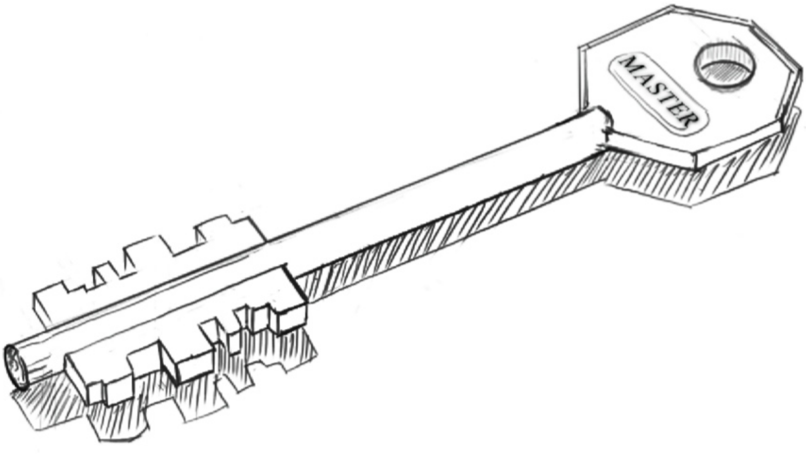
the CryptoParty handbook



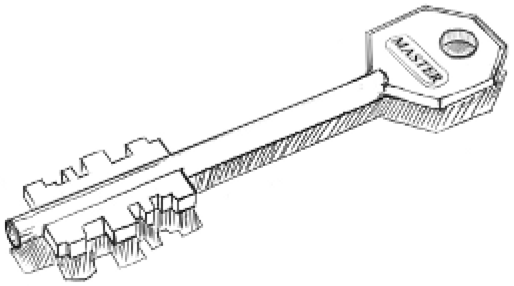
v1.1

The CryptoParty Handbook

ed. Version 1

Contents

CryptoParty Handbook



A CryptoParty History: Party Like It's 1984

Because everything sounds better when someone promises there'll be beer.

What is CryptoParty?

Interested parties with computers, devices, and the willingness to learn how to use the most basic crypto programs and the fundamental concepts of their operation! CryptoParties are free to attend, public and commercially non-aligned.

CryptoParty is a decentralized, global initiative to introduce basic cryptography tools - such as the Tor anonymity network, public key encryption (PGP/GPG), and OTR (Off The Record messaging) - to the general public.

The CryptoParty idea was conceived on August 22nd 2012 as the result of a casual Twitter conversation between information activist and Twitter identity Asher Wolf and computer security experts in the wake of the Australian Cybercrime Legislation Amendment Bill 2011.

"The DIY, self-organizing movement immediately went viral, with a dozen autonomous CryptoParties being organized within hours in cities throughout Australia, the US, the UK, and Germany."

Currently sixteen CryptoParties have been held in a dozen different countries worldwide, and many more are planned. Tor usage in Australia has spiked after four CryptoParties, and the London CryptoParty had to be moved from London Hackspace to the Google Campus to accommodate the large number of eager participants, with 125 ticketed guests and 40 people on the waiting list. Similarly, CryptoParty Melbourne found interest outstripped venue capacity - originally planned for approximately 30 participants - over 70 people turned up.

CryptoParty has received messages of support from the Electronic Frontier Foundation, AnonyOps, NSA whistleblower Thomas Drake, former Wikileaks

Central editor Heather Marsh, and Wired reporter Quinn Norton. Eric Hughes, the author of *A Cypherpunk's Manifesto* twenty years ago, delivered a keynote address at Amsterdam's first CryptoParty. And we're just getting started.

A CryptoParty Manifesto

"Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth." - Oscar Wilde

In 1996, John Perry Barlow, co-founder of the Electronic Frontier Foundation (EFF, https://www.eff.org/), wrote 'A Declaration of the Independence of Cyberspace'. It includes the following passage:

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Sixteen years later, and the Internet has changed the way we live our lives. It has given us the combined knowledge of humankind at our fingertips. We can form new relationships and share our thoughts and lives with friends worldwide. We can organise, communicate and collaborate in ways never thought possible. This is the world we want to hand down to our children, a world with a free internet.

Unfortunately, not all of John Perry Barlow's vision has come to pass. Without access to online anonymity, we can not be free from privilege or prejudice. Without privacy, free expression is not possible.

The problems we face in the 21st Century require all of humanity to work together. The issues we face are are serious: climate change, energy crises, state censorship, mass surveillance and on-going wars. We must be free to communicate and associate without fear. We need to support free and open source projects which aim to increase the commons' knowledge of technologies that we all depend on. [Contribute!]

To realise our right to privacy and anonymity online, we need peer-reviewed, crowd-sourced solutions. CryptoParties provide the opportunity to meet up and learn how to use these solutions to give us all the means with which to assert our right to privacy and anonymity online.

- We are all users, we fight for the user and we strive to empower the user. We assert *user requests* are the reason why computers exist. We trust in the collective wisdom of human beings, over the interest of software vendors, corporations or governments. We refuse the shackles of digital Gulags, lorded over by vassal interests of governments and corporations. We are the CypherPunk Revolutionaries.

- *The right to personal anonymity, pseudonymity and privacy is a basic human right.* These rights include life, liberty, dignity, security, right to a family, and the right to live without fear or intimidation. No government, organisation or individual should prevent people from accessing the technology which underscores these basic human rights.

- Privacy is the absolute right of the individual. Transparency is a requirement of governments and corporations who act in the name of the people.

- The individual alone owns the right to their identity. Only the individual may choose what they share. Coercive attempts to gain access to personal information without explicit consent is a breach of human rights.

- All people are entitled to cryptography and the human rights crypto tools afford, regardless of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, political, jurisdictional or international status of the country or territory in which a person resides.

- Just as governments should exist only to serve their citizens - so too, cryptography should belong to the people.Technology should not be locked away from the people.

- Surveillance cannot be separated from censorship, and the slavery it entails. No machine shall be held in servitude to surveillance and censorship. Crypto is a key to our collective freedom.

- Code is speech: code is human created language. To ban, censor or lock cryptography away from the people is to deprive human beings from a human right, the freedom of speech.

- Those who would seek to stop the spread of cryptography are akin to the XV century clergy seeking to ban the printing press, afraid their monopoly on knowledge will be undermined.

How To CryptoParty

- Throw a party. All you need is a time, a date and a location. Add it to the wiki: cryptoparty.org.

- Make sure you have Internet connectivity and enough power sources for all devices. If you do not have a place to hold a CryptoParty, find a pub or park where you can meet and squeeze the public bandwidth. That will really hone your skills!

- Bring USB sticks and printed handouts for those who need them, and set up old computers for people to fiddle with and try out new skills.

- Talk about Linux to everyone you meet at your CryptoParty. If you are new to CryptoParties - ask someone "what is Linux?" ASAP.

- Make entry free for all if possible - CryptoParties are not-for-profit, not commercially aligned and especially important for those without other resources.

- Teach basic cryptographic tools to the masses. Crowd-source the best crypto. We suggest starting with PGP, OTR, and Tor as the first tools to install.

- Invite experts and non-experts from all fields. Invite graphic designers and illustrators to contribute new ways to understand crypto. Everyone is an expert on something. Let them share their skills.

- Decentralize. Organize organically and chaotically. Avoid clear leadership. Urge different people to take different leads- take a tutorial, fix the wifi, update the wiki, or organize the next CryptoParty in their place. If someone claims others are doing it wrong - invite them to do it better.

- Ask for feedback. Assimilate critics - ask them for their help in creating a better CryptoParty. Do not be scared to troll the trolls back or boot them from your space. Share feedback on the wiki. Iterate.

- A successful CryptoParty can have as many or as few as two people. Size doesn't count, it's what you do with it that matters. The criterion for success should be that everyone had fun, learned something and wants to come to the next party.

- Think of the CryptoParty movement as a huge Twitter hive ready to swarm at any moment. Tweet a lot, and make sure your tweets are meaningful. Retweet other CryptoPartiers frequently.

- Make sure the way crypto is taught at your party could be understood by a 10-year-old. Then have the 10-year-old teach it to an 80-year-old. Breach the digital divide with random acts of awesomeness such as unfettered use of images of kittens in all CryptoParty literature.

- Consider hosting private, off-the-radar CryptoParties for activists, journalists and individuals working in dangerous locations.

- Don't scare non-technical people. Don't teach command lines before people know where the on-off buttons are located on their laptops. Encourage advanced users to help not-so advanced ones. Delegate.

- Doing excellent stuff at CryptoParty does not require permission or an official consensus decision. If you're uncertain about the excellence of something you want to do, you should ask someone else what they think.
  Do not be afraid bounce people who breach CryptoParty's anti-harassment policy.

- CryptoParty is dedicated to providing a harassment-free sharing experience for everyone, regardless of gender, sexual orientation, disability, physical appearance, body size, heritage, or religion. Behaving like a moron may mean you are permanently uninvited to CryptoParties events. Harassment includes:

  -Hurtful or offensive comments
  -Deliberate intimidation
  -Direct or indirect threats
  -Stalking
  -Inappropriate physical contact
  -Unwelcome sexual attention

- Use online meeting platforms like mumble (e.g. #cryptoparty room on http://occupytalk.org/) when physical meetups are not possible or impractical.

- Copy from other Cryptoparties. Remix, Reuse and Share. Create a basket of old devices people are willing to donate to other CryptoPartiers in need.

- No one's coming? Get the word out! Print posters and/or flyers and distribute them in your neighbourhood, post online versions to social networks and mail them to friends.

- Don't sell out to sponsors for pizza and beer money. Ask people to bring food and drink to share. Host CryptoPicnics as often as possible. Make friends with librarians. They wield power over keys to local, public meeting rooms that may be free of charge to utilize.

- Invite all the people. Bring people together who have a wide range of skills and interests - musicians, political pundits, activists, hackers, programmers, journalists, artists and philosophers. Spread the love.

- Seed CryptoParties in your local communities - at nursing homes, scout groups, music festivals, universities, and schools. Take CryptoParty to isolated and remote communities. Make friends in far away places and travel whenever possible. Ask people in rural farming communities if they'd like to CryptoParty.

- Have fun! Share music, beers, & chips. Bond together over eclectic music, cheeseballs, installing GPG, TrueCrypt, OTR and Tor, as well as watching movies together. We recommend Hackers, The Matrix, Bladerunner, Tron, Wargames, Sneakers, and The Net.

Why Privacy Matters

Privacy is a fundamental human right. It is recognized in many countries to be as central to individual human dignity and social values as Freedom of Association and Freedom of Speech. Simply put, privacy is the border where we draw a line between how far a society can intrude into our personal lives.

Countries differ in how they define privacy. In the UK for example, privacy laws can be traced back to the 1300s when the English monarchy created laws protecting people from eavesdroppers and peeping toms. These regulations referred to the intrusion of a persons comfort and not even the King of England could enter into a poor person's house without their permission. From this perspective, privacy is defined in terms of personal space and private property. In 1880, American lawyers Samuel Warren and Louis Brandeis described privacy as the 'right to be left alone.' In this case, privacy is synonymous with notions of solitude and the right for a private life. In 1948, the Universal Declaration of Human Rights specifically protected territorial and communications privacy which by that became part of constitutions worldwide. The European Commission on Human Rights and the European Court of Human Rights also noted in 1978 that privacy encompasses the right to establish relationships with others and develop emotional well-being.

Today, a further facet of privacy increasingly perceived is the personal data we provide to organizations, online as well as offline. How our personal data is used and accessed drives the debate about the laws that govern our behaviour and society. This in turn has knock-on effects on the public services we access and how businesses interact with us. It even has effects on how we define ourselves. If privacy is about who we give permission to watch us and track aspects of our lives, then the amount and type of personal information gathered, disseminated and processed is paramount to our basic civil liberties.

And yet, we often give away such rights ourselves, thinking “I only do boring stuff. Nobody will be interested in it anyway," or, "I have nothing to hide." These are the most common arguments for giving up our privacy, but these arguements are naive.

Firstly, a lot of companies are very interested in what boring things you do precisely so that they have the opportunity to offer "excellent" products fitting those interests. In this way their advertising becomes much more efficient - they are able to tailor specifically to assumed needs and desires. Secondly you DO have lots to hide. Maybe you do not express it in explicitly stated messages to friends and colleagues, but your browsing - if not protected by the applications and techniques described in this book - will divulge a lot of things you might rather keep secret: the ex-partner you search for using Google, illnesses you research or movies you watch are just a few examples.

Another consideration is that, just because you might not have something to hide right now, you may very well in future, as governments and legislation become more controlling. Putting together all the tools and skills to protect yourself from surveillance takes practice, trust and some effort. These are things you might not be able to do and configure right when you need them most. An obsessed, persistent stalker, for example, is enough to heavily disrupt your life. The more you follow the suggestions given in this book, the less impact attacks like this will have on you. Companies may also stalk you, finding more and more ways to reach into your daily life as the reach of computer networking itself deepens.

Finally, a lack of anonymity and privacy does not just affect you, but all the people around you. If a third party, like your Internet Service Provider, reads your email, it is also violating the privacy of all the people in your address book. This problem starts to look even more dramatic when you look at the issues of social networking websites like Facebook. It is increasingly common to see photos uploaded and tagged without the knowledge or permission of the people affected. Maintaining privacy on the Internet is also a personal responsibility.

While we encourage you to actively defend your right to privacy against corporations, governments and criminals, we wrote this book in order to help you develop the habit of protecting your communications wherever you go and whatever you do. We hope these chapters will help you reach a point where you can feel that you have some control over how much other people know about you. Each of us has the right to a private life, a right to explore, browse and communicate with others as one wishes, without living in fear of prying eyes.

About this book

V1.0

The CryptoParty Handbook was born from a suggestion by Marta Peirano and Adam Hyde after the first Berlin CryptoParty, held on the 29th of August, 2012. Julian Oliver and Danja Vasiliev, co-organisers of the Berlin CryptoParty along with Marta were very enthusiastic about the idea, seeing a need for a practical working book with a low entry-barrier to use in subsequent parties. Asher Wolf, originator of the Crypto Party movement, was then invited to run along and the project was born.

The 1st draft (v1.0) was written in the first 3 days of October 2012 at Studio Weise7, Berlin, surrounded by fine food and a small ocean of coffee. The BookSprint System was used, in conjunction with the open source browser-based publishing and book authoring system BookType (http://www.sourcefabric.org/en/booktype/).

Approximately 20 people were involved in its creation, some more than others, some local and some far. It was released by midnight October the 3rd, GMT+1.

Core Team: Adam Hyde (facilitator), Marta Peirano, Julian Oliver, Danja Vasiliev, Asher Wolf, Jan Gerber, Malte Dik, Brian Newbold, Brendan Howell, AT, Carola Hesse, Chris Pinchen. Cover art (illustrations to come) by Emile Denichaud.

V1.1

This a bugfix and merge release, attempting to consolidate different efforts and exporting to e-pub formats (as promised) before the Handbook finally leaves BookType and continues on in GitHub (http://github.com).

Enthusiasm around the book resulted in a need for revision-control and merging and so 'yuvadm' went through the entire BookType version and imported it into GitHub (https://github.com/cryptoparty/handbook).

While GitHub is a closed source platform for code repositories and revision control, it has a large community of users and powerful tools, including in-browser text editing. Many changes were made to the GitHub version ('pettter', Daniel Kinsman, qbi, Jens Kubieziel et al) at the same time changes were made to the BookType (and then http://booki.cc/cryptoparty-handbook/) version. This release is an attempt to merge these disparate edits and marks the last release before it is all imported into GitHub for continued development. The work is ongoing, including coming up with an equivalent to the exporter(s) that BookType has, to e-pub and ODT formats.

Help us improve this book

If you see areas that need improvement or simply come across a typo, create a GitHub account and get editing here:

https://github.com/cryptoparty/handbook

CryptoParty HandBook Credits

Adam Hyde
Marta Peirano
Asher Wolf
Julian Oliver
Danja Vasiliev
Malte Dik
Jan Gerber
Brian Newbold
Brendan Howell
Teresa Dillon
AT
Carola Hesse
Chris Pinchen
'LiamO'
'l3lackEyedAngels'
'Story89'
Travis Tueffel
'yuvadm'
'schnuffus'
'qbi'
'pettter'
Jens Kubieziel
Daniel Kinsman
'Stooj'
'jmorahan'
'Punkbob'

Cover Image
Emile Denichaud

Other material included:

https://www.flossmanuals.net/bypassing-censorship

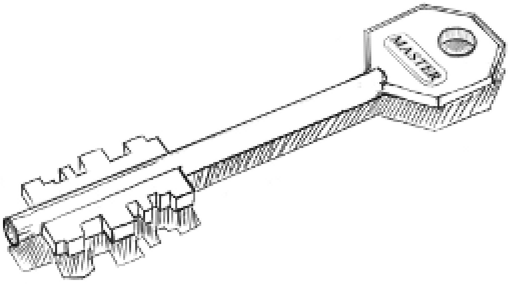
The manuals used in the second half of this book borrow from 2 books sprinted by FLOSS Manuals :

"How to Bypass Internet Censorship" 2008 & 2010
Adam Hyde (Facilitator), Alice Miller, Edward Cherlin, Freerk Ohling, Janet Swisher, Niels Elgaard Larsen, Sam Tennyson, Seth Schoen, Tomas Krag, Tom Boyle, Nart Villeneuve, Ronald Deibert, Zorrino Zorrinno, Austin Martin, Ben Weissmann, Ariel Viera, Niels Elgaard Larsen, Steven Murdoch, Ross Anderson, helen varley jamieson, Roberto Rastapopoulos, Karen Reilly, Erinn Clark, Samuel L. Tennyson, A Ravi

"Basic Internet Security" 2011
Adam Hyde (Facilitator), Jan Gerber, Dan Hassan, Erik Stein, Sacha van Geffen, Mart van Santen, Lonneke van der Velden, Emile den Tex and Douwe Schmidt

All chapters © the contributors unless otherwise noted below.

Understanding Email



Types of Email

The use of email almost always comes in two forms:

1. Email read, written and sent in the browser (webmail)
2. Email read, written and sent using an email program, like Mozilla Thunderbird, Mail.App or Outlook Express

Remotely hosted email ('webmail'), resourced using a web browser

Email sent and received using the browser, sometimes referred to as *webmail*, typically assumes an account with a remote email host like Google (Gmail), Microsoft (Hotmail) or Yahoo (Yahoo Mail). The business opportunities opened up by hosting other people's email are many: contact with other services offered by the company, brand exposure and most importantly, mining your email for patterns that can be used to evaluate your interests – something of great value to the advertising industry (alongside certain Governments).

Because the email entirely resides on the server, there is a basic risk of email loss. An attacker gaining access to the account might delete email or the service itself could disappear or be attacked.

Remotely hosted email, resourced using an email program or using a web browser

Email written and send from an email program like Outlook, Thunderbird, Mail.App can also be used with a webmail service like Gmail or your company's email service. In either case, email may still be downloaded onto your computer but is retained on the email server (e.g. Gmail). Done this way, your use of email doesn't *depend* on the browser, but you are still using Gmail or Hotmail as a service.

The difference between storing email on your computer with an email program and having it stored remotely on an email server (like Hotmail, Gmail or your University's service) on the Internet can appear confusing at first. Nonetheless it provides several advantages:

Using webmail alongside a local email program obviously allows the freedom of logging in from any computer connected to the Internet (great for travellers) but also provides the option for local backups onto a machine you control and own. This approach adds what's referred to as *data redundancy*. Having both local and remote copies of your email is absolutely recommended for content sensitive information. Most importantly however, when using an email program we have the option of using encryption (see section **Email Encryption**), stopping unwanted eyes from reading the email. This is not always easily done using webmail alone.

If you do download the email alongside viewing it in your browser, disk encryption on the local machine is highly advisable (section **Disk Encryption**). That way if the machine is stolen or detained, the email cannot be read by the thief.

Email sent and received using an email program, not stored on the remote machine

Finally, email can also be sent to an email server but not stored there at all, merely volleyed onto its destination as soon as the email reaches the email forwarding server. Google and Microsoft do not allow for this sort of setup. Rather this is typically something your university or company will provide for you. Bear in mind that this comes with an implicit risk: the email administrator on that system still has access to your email as it reaches and leaves the server.

Context considerations

You may be a server administrator yourself and run your own email service. Or your email could be stored on your company or bosses' server. Finally you may be using a service provided by a corporation, like Google (Gmail) or Microsoft (Hotmail). Each comes with its own interesting mix of considerations that relate precisely to the basic fact that unless the email *itself* is encrypted, the administrator of the email server can still secretly copy the email the moment it reaches the server. It doesn't matter that you may be using a secure login provided by *TLS/SSL* to login and check your email as this only protects the connection between your local machine and the server itself. Simply put, never send sensitive email unencrypted, let alone using a service you don't fully trust.

Employer/Organisation

Your employer or an organisation that you are involved with is in a very good position to take advantage of your trust and read the emails of your business email account that is stored on their email server, perhaps in an effort to learn about you, your motivations, agendas and interests. Such cases of employer->employee spying are so typical they do not bear mention. Your only measure against it is to use an email encryption solution like *GPG* (see **Email Encryption**).

Self-administered email server

Generally speaking this is the ideal hosting configuration, but requires a higher level of technical skill. Here, in general, the risks to privacy are not only in protecting your own email against attempts at exploit (poor passwords, no SSL) but in that you have a responsibility, and perhaps a temptation, to read the emails of those you provide a service for.

'Free' email services

As mentioned above the risks of storing and sending your email using a service provided by a corporation are rather high if respect of your civil right to privacy is valued. The companies hosting your love letters, random expressions and diaries are always at risk of yielding to pressures from political, economic and law enforcement interests of the country to which they are legally subject. A Malaysian Gmail user, for instance, risks exposing her interests and intents to a government she *did not elect*, not to mention business partners of Google interested in expanding their market reach.

Non-profit

Several non-profit web hosts offer free email accounts to organisations that are themselves non-profit or philanthropic. Some of them even offer wikis, mailing lists, chats and social networks. A consideration for organisations working in a political field may be differences of interests between the state in which the email is hosted and the political interests of the organisation using that service. Such risks would ideally be reflected in the End User License Agreement.

Notes on email forwarding

Email forwarding services provide the great convenience of 'linking' one email account to another as the user sees fit. This of course is most commonly used when an account holder is on holiday and would like email forwarded from their work account to another used during travel or otherwise inaccessible outside the workplace. The risk with any external email forwarding service is the same as with remotely hosted emails through Gmail for instance: it can be copied and stored. Here email encryption using a system such as GPG (section **Email Encryption**) will ensure that if it is copied at least it cannot be read.

Basic Tips on Email

Just as with other forms of communication on the Web, some basic precautions always ought to be taken to ensure you have the best chance at protecting your privacy.

In brief:

- Passwords shouldn't relate to personal details and should contain a mix of more than 8 letters and other characters.
- Always be sure your connection is secure when reading email on a wireless network, especially in Internet cafes.
- Temporary files (e.g. the 'cache' and History) on the computer that you use to check your email can present some risks. Clear them often.
- Create and maintain separate email accounts for different tasks and interests.
- Encrypt any message you wouldn't feel comfortable sending on a postcard.
- Be aware of the risks of having your email hosted by a company or organization.

Passwords

Passwords are a primary point of vulnerability in email communication. Even a secure password can be read in transit unless the connection is secure (see *TLS/SSL* in the glossary). In addition, just because a password is long doesn't mean it cannot be guessed by using knowledge of you and your life to determine likely words and numbers.

The general rule for creating passwords is that it should be long (8 characters or more) and have a mix of letters and other characters (numbers and symbols, which means you could just choose a short sentence). Combining your birthday with that of a family name is however a great example of how *not* to do it. This kind of information is easy to find using public resources. A popular trick is to base it on a favourite phrase and then, just to throw people off, sprinkle it with a few numbers. Best of all is to use a password generator, either on your local system or online.

Often such passwords are difficult to remember and a second point of vulnerability is opened up – physical discovery. Since there is no better means of storing a password than in your own brain, services like *OnlinePasswordGenerator* (http://www.onlinepasswordgenerator.com/) offer a great compromise by randomly generating passwords that vaguely resemble words and present you with a list to choose from.

If you do choose to store your password outside your head, you have the choice to either write it down or use *keychain* software. This can be a risky decision, especially if the email account and password are on the same device like your phone or computer.

Keychain software, like *Keepass*, consolidates various passwords and passphrases in one place and makes them accessible through a master password or passphrase. This puts a lot of pressure on the master password. If you do decide to use a keychain software, remember to choose a secure password.

Finally, you should use a different password for different accounts. In that way, if one of them gets hijacked, your other accounts remain safe. Never use the same password for your work and private email accounts. See section **Passwords** to learn more about how to secure yourself.

Reading Email in Public Places

One of the great conveniences of wireless networking and 'cloud computing' is the ability to work anywhere. You may often want to check your email in an Internet cafe or public location. Spies, criminals and mischievous types are known to visit these locations in order to take advantage of the rich opportunities offered for ID theft, email snooping and hijacking bank accounts.

Here we find ourselves within an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone joins *the same* encrypted network, s/he can easily capture and read all *unsecured* (see chapter **Secure Connections**) traffic of all of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives those that know how to capture and read network packets the chance to read your password while you check your email.

Here a simple general rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

Cache Cunning

Here again convenience quickly paves the road to bad places. Due to the general annoyance of having to type in your password over and over again, you ask the browser or local mail client to store it for you. This is not bad in itself, but when a laptop or phone gets stolen, it enables the thief to access the owner's email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One basic precaution can justify you holding onto your convenient cache: disk encryption. If your laptop is stolen and the thief reboots the machine, they'll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing browsing session, it cannot be accessed.

Securing your communication

Whenever you write and send email in a browser or use an email program (Outlook Express, Mozilla Thunderbird, Mail.app or Mutt), you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TLS/SSL* (Secure Socket Layer) connections by email servers (**See glossary TLS/SSL**).

If you are using a browser to check your email, check to see if the mail server supports SSL sessions by looking for **https://** at the beginning of the URL. If not, be sure to turn it on in your email account settings, such as Gmail or Hotmail.This ensures that not just the login part of your email session is encrypted but also the writing and sending of emails.

At the time of writing, Google's Gmail uses TLS/SSL by default whereas Hotmail does not. If your email service does not appear to provide TLS/SSL, then it is advised to stop using it. Even if your emails are not important, you might find yourself 'locked out' of your account one day with a changed password!

When using an email program to check your email, be sure that you are using TLS/SSL in the program options. For instance in Mozilla Thunderbird the option for securing your outgoing email is found in **Tools -> Account Settings -> Outgoing Server (SMTP)** and for incoming email in **Tools -> Account Settings -> Server Settings**. This ensures that the downloading and sending of email is encrypted, making it very difficult for someone on your network, or on any of the networks between you and the server, to read or log your comunications.

Encrypting the email itself

Even if the line itself is encrypted using a system such as SSL, the email service provider still has full access to the email because they own and have full access to the storage device where you host your email. If you want to use a web service and be sure that your provider cannot read your messages, you need to use something like *GPG* (**Appendix for GnuPG**) with which you can encrypt your email. The *header* of the email however will still contain the IP (Internet address) that the email was sent from alongside other compromising details. Worth mentioning here is that the use of *GPG* in webmail is not as comfortable as with a locally installed mail client, such as *Thunderbird* or *Outlook Express*.

Account Separation

Due to the convenience of services like Gmail, it is increasingly typical for people to have only one email account. This considerably centralises the potential damage done by a compromised account. More so, there is nothing to stop a disgruntled Google employee from deleting or stealing your email, let alone Google itself getting hacked. It has happened before.

A practical strategy is to keep your personal email personal. If you have a work email then create a new account if your employers haven't already done it for you. The same should go for any clubs or organisations you belong to, each with a unique password. Not only does this improve security, by reducing the risk of whole identity theft, but greatly reduces the likelihood of spam dominating your inbox.

A note about hosted email

Those that provide you with the service to host, send, download and read email are not encumbered by the use of TLS/SSL. As hosts, they can read and log your email in plain text. They can comply with requests by local law enforcement agencies who wish to access email. They may also study your email for patterns, keywords or signs of sentiment for or against brands, ideologies or political groups. It is important to read the EULA (End-user license agreement) of your email service provider and do some background research on their affiliations and interests before choosing what kind of email content they have access to. These concerns also apply to the hosts of your messages' recipients.

Email Privacy Fears

Who can read the email messages that I have already sent or received?
Who can read the emails I send when they travel across the Internet?
Can the people I send emails to share them with anybody?

Emails that are sent "in the clear" without any encryption (which means the vast majority of email sent and received today) can be read, logged, and indexed by any server or router along the path the message travels from sender to receiver. Assuming you use an encrypted connection (see glossary for **TLS/SSL**) between your devices and your email service provider (you should!), this means in practice that the following people can still read any message you send or receive:

1. You
2. Your email service provider
3. The operators and owners of any intermediate network connections (often ambiguous multinational conglomerates or even sovereign states)
4. The recipient's email service provider
5. The intended recipient

Many webmail providers (like Gmail) automatically inspect all of the messages sent and received by their users to feed their targeted advertisements. While this may be a reasonable compromise for some users most of the time (free email!), it is disturbing for many that even their most private communications are inspected and indexed as part of a hidden and potentially very insightful profile maintained by a powerful corporate giant.

Additionally, somebody who can legally pressure the groups above could request or demand:

1. Logged meta-data about email (lists of messages sent or received by any user, subject lines, recipients), in some jurisdictions even without a warrant.
2. Messages sent and received by a specific user or group, with a warrant or court order in some jurisdictions.
3. A dedicated connection to siphon off *all* messages and traffic, to be analyzed and indexed off site.

In cases where a user has a business or service relationship with their email provider, most governments will defend the privacy rights of the user against unauthorized and unwarranted reading or sharing of messages, but often it is the government itself seeking information, and frequently users agree to waive some of these rights as part of their service agreement. However, when the email provider is the user's employer or academic institution, privacy rights frequently do not apply. Depending on jurisdiction, businesses generally have the legal right to read all of the messages sent and received by their employees from their corporate accounts and computers, even personal messages sent after hours or on vacation.

Historically, it was possible to "get away" with using clear text email because the cost and effort to store and index the growing volume of messages was too high: it was hard enough just to get messages delivered reliably. This is why many email systems do not contain mechanisms to preserve the privacy of their contents. Now the cost of monitoring has dropped much faster than the growth of Internet traffic and large-scale monitoring and indexing of all messages (either on the sender or receiving side) is reasonable to expect even for the most innocuous messages and users.

For updated examples to illustrate this point, search for corporate email archiving/spying, blue coat, Syrian monitoring, USA Utah data center, USA intercept scandals. For more about legal protections of email messages "at rest" (technical term for messages stored on a server after having been delivered), especially regarding government access to your email messages, see:

- https://ssd.eff.org/3rdparties/govt/stronger-protection (USA)
- http://en.wikipedia.org/wiki/Data_Protection_Directive (EU)

Just like there are certain photos, letters and credentials that you would not post "in the clear" on the Internet because you would not want that information to get indexed accidentally and show up in search results, you should never send email messages in the clear that you would not want an employer or disgruntled airport security officer to have easy access to.

Random abuse and theft by malicious hackers

What if somebody gets complete control of my email account?
I logged in from an insecure location... how do I know now if my account has been hacked?
I've done nothing wrong... what do I have to hide?
Why would anybody care about me?

Unfortunately, there are many practical, social, and economic incentives for malicious hackers to break into the accounts of random Internet individuals. The most obvious incentive is identity and financial theft, when the attacker may be trying to get access to credit card numbers, shopping site credentials, or banking information to steal money. A hacker has no way to know ahead of time which users might be better targets than others, so they just try to break into all accounts, even if the user doesn't have anything to take or is careful not to expose his information.

Less obvious are attacks to gain access to valid and trusted user accounts to collect contact email addresses and distribute mass spam, or to gain access to particular services tied to an email account, or to use as a "stepping stone" in sophisticated social engineering attacks. For example, once in control of your account, a hacker could rapidly send emails to your associates or co-workers requesting emergency access to more secured computer systems.

A final unexpected problem affecting even low-profile email users, is the mass hijacking of accounts on large service providers, when hackers gain access to the hosting infrastructure itself and extract passwords and private information in large chunks, then sell or publish lists of login information in online markets.

Targeted abuse, harassment, and spying

Something I wrote upset a person in power... how do I protect myself?

If you find yourself the individual target of attention from powerful organizations, governments, or determined individuals, then the same techniques and principles apply to keeping your email safe and private, but additional care must be taken to protect against hackers who might use sophisticated techniques to undermine your devices and accounts. If a hacker gains control of any of your computing devices or gets access to any of your email accounts, they will likely gain immediate access both to all of your correspondence, and to any external services linked to your email account.

Efforts to protect yourself against such attacks can quickly escalate into a battle of wills and resources, but a few basic guidelines can go a long way. Use specific devices for specific communication tasks, and use them only for those tasks. Log out and shutdown your devices immediately when you are done using them. Use open software encryption tools, web browsers, and operating systems as they can be publicly reviewed for security problems and keep up to date with security fixes.

Be wary of opening PDF files using Adobe Reader or other proprietary PDF readers. Closed source PDF readers have been known to be used to execute malign code embedded in the PDF body. If you receive a .pdf as an attachment you should first consider if you know the supposed sender and if you are expecting a document from him. Secondly, you can use PDF readers which have been tested for known vulnerabilities and do not execute code via java script.

Linux: Evince, Sumatra PDF

OS X: Preview

Windows: Evince

Use short-term anonymous throw away accounts with randomly generated passwords whenever possible.

When Encryption Goes Wrong

What happens if I lose my "keys"? Do I lose my email?

Rigorous GPG encryption of email is not without its own problems.

If you store your email encrypted and lose all copies of your private key, you will be absolutely unable to read the old stored emails, and if you do not have a copy of your revocation certificate for the private key it could be difficult to prove that any new key you generate is truly the valid one, at least until the original private key expires.

If you sign a message with your private key, you will have great difficulty convincing anybody that you did not sign if the recipient of the message ever reveals the message and signature publicly. The term for this is *non-repudiation*: any message you send signed is excellent evidence in court. Relatedly, if your private key is ever compromised, it could be used to read all encrypted messages ever sent to you using your public key: the messages may be safe when they are in transit and just when they are received, but any copies are a liability and a gamble that the private key will never be revealed. In particular, even if you destroy every message just after reading it, anybody who snooped the message on the wire would keep a copy and attempt to decrypt it later if they obtained the private key.

The solution is to use a messaging protocol that provides *perfect forward secrecy* by generating a new unique session key for every conversation of exchange of messages in a random way such that the session keys could not be re-generated after the fact even if the private keys were known. The OTR chat protocol provides perfect forward secrecy (http://en.wikipedia.org/wiki/-Perfect_forward_secrecy) for real time instant messaging, and the SSH protocol provides it for remote shell connections, but there is no equivalent system for email yet.

It can be difficult to balance the convenience of mobile access to your private keys with the fact that mobile devices are much more likely to be lost, stolen or inspected and exploited than stationary machines. An emergency or unexpected time of need might be exactly the moment when you would most want to send a confidential message or a signed message to verify your identity, but these are also the moments when you might be without access to your private keys if your mobile device was seized or not loaded with all your keys.

Secure Connections

Can other people read along when I check my email?

As discussed in the chapter **Email: Basic Tips**, whether you use webmail or an email program you should always be sure to use encryption for the entire session, from login to logout. This will keep anyone from spying on your communication with your email provider. Thankfully, this is easily done due to the popular use of *TLS/SSL* connections on email servers.

A TLS/SSL connection in the browser, when using webmail, will appear with '*http***s**' in the URL instead of the standard '*http*', like so:

https://gogglemail.com

If your webmail host does not provide a TLS/SSL service then you should consider discontinuing use of that account; even if your emails themselves are not especially private or important, your account can very easily be hacked by "sniffing" your password! If it is not enabled already be sure to turn it on in your account options. At the time of writing, Google's Gmail and Hotmail / Microsoft Live both automatically switch your browser to using a secure connection.

If you are using an email program like Thunderbird, Mail.app or Outlook, be sure to check that you are using TLS/SSL in the options of the program. (See the chapter **Setting Up Secure Connections** in the section **Email Security)**.

Notes

It's important to note that the administrators at providers like Hotmail or Google, that host, receive or forward your email, can read your email even if you are using secure connections. It is also worth nothing that the private keys that Certificate Authorities sell to web site owners can sometimes end up in the hands of governments or hackers, making it much easier for a *Man In The Middle Attack* on connections using TLS/SSL (See Glossary for **Man in the Middle Attack**). An example is here, implicating America's NSA and several email providers: http://cryptome.info/0001/nsa-ssl-email.htm

We also note here that a *Virtual Private Network* is also a good way of securing your connections when sending and reading email but requires using a *VPN* client on your local machine connecting to a server. (See the chapter **VPN** in the **Browsing** section).

Secure Emails

It is possible to send and receive secure email using standard current email programs by adding a few add-ons or extensions. The essential function of these add-ons is to make the message body (but not the *To:*, *From:*, *CC:* and *Subject:* fields) unreadable by any 3rd party that intercepts or otherwise gains access to your email or that of your conversation partner. This process is known as *encryption.*

Secure email is generally done using a technique called *Public-Key Cryptography*. Public-Key Cryptography is a clever technique that uses two code keys to send a message. Each user has a *public key*, which can only be used to encrypt a message but not to decrypt it. The public keys are quite safe to pass around without worrying that somebody might discover them. The *private keys* are kept secret by the person who receives the message and can be used to decode the messages that are encoded with the matching public key.

In practice, that means if Rosa wants to send Heinz a secure message, she only needs his public key which encodes the text. Upon receiving the email, Heinz then uses his private key to decrypt the message. If he wants to respond, he will need to use Rosa's public key to encrypt the response, and so on.

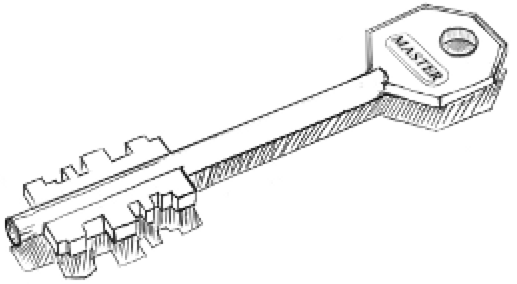
What software can I use to encrypt my email?

The most popular setup for public-key cryptography is to use *Gnu Privacy Guard* (GPG) to create and manage keys and an add-on to integrate it with standard email software. Using GPG will give you the option of encrypting sensitive mail and decoding incoming mail that has been encrypted but it will not force you to use it all the time. In years past, it was quite difficult to install and set up email encryption but recent advances have made this process relatively simple.

See section **Email Encryption** for working with GPG in the scope of your operating system and email program.

If you use a *webmail* service and wish to encrypt your email this is more difficult. You can use a GPG program on your computer to encrypt the text using your public key or you can use an add-on, like *Lock The Text* (http://lockthetext.sourceforge.net/). If you want to keep your messages private, we suggest using a dedicated email program like Thunderbird instead of webmail.

Understanding Browsing



What happens when you browse

Browsing the web is communicating. You might not send as much text in terms of number of words, but it is always the browser which initiates and maintains the communication by requesting the bits and pieces which are woven into what is eventually displayed on your screen.

Browsers like Mozilla Firefox, Google Chrome, Opera, Safari & Internet Explorer all work in a similar manner. When we type a URL (e.g. "http://happybunnies.com") in the address bar, the browser requests the page (which is just a special kind of text) from a remote server and then transforms it into colored blocks, text and images to be displayed in the browser window. To see the text the way the browser sees it, one just has to click on the *View* --> *Page source* menu entry in the browser. What comes up is the same webpage but in HTML – a language mainly concerned with content, context and links to other resources (CSS and JavaScript) which govern the way these contents are displayed and behave.

When the browser tries to open a webpage – and assuming there are no proxies involved – the first thing it does is to check its own cache. If there are no past memories of such website, it tries to resolve the name into an address it can actually use. It is an internet program, so it needs an Internet Protocol address (IP address or just IP). To get this address it asks a DNS Server (a kind of phonebook for internet programs) which is installed in the router of your internet access by default. The IP address is a numerical label assigned to every device in the (global) network, like the address of a house in the postal system – and as the address of your home, you should be very careful to whom you hand out the IP address you are browsing from, though by default it is visible to everyone.

Once the IP address has been received, the browser opens a TCP (just a communication protocol) connection to the destination host and starts sending packages to a port at this address, typically no. 80, unless another path is specified (ports are like doors to the servers, there are many but usually only a few are open). These packages travel through a number of servers on the internet (up to a couple of dozen depending on where the target address is located). The server then looks for the requested page and, if found, delivers it using the HTTP protocol.

When the HTTP response arrives, the browser can close the TCP connection or reuse it for subsequent requests. The response can be one of many things, from some sort of redirection to a classic Internal Server Error (500). Provided the response proceeds as expected and we get to the happy bunnies, the browser will store the whole page in a cache for further use, decode it (uncompress it if compressed, rendered if video codec, etc) and display/play it according to instructions.

Now, the process can be illustrated in a little conversation between browser (B) and server (S):

B: "Hallo."

S: "Hey!"

B: "May I get that page with the happy bunnies, please?"

S: "Well, here you are."

B: "Oh, maybe you could also give me a big version of that picture of that bunny baby cuddling a teddy bear."

S: "Sure, why not."

[...]

B: "That's all for now. Thank you. Bye."

But this is not the only thing that happens when you browse; there are lots of activities happening in the background that you might not be aware of. Depending on how you have configured its options, your browser will probably be adding the page to browser history, saving cookies, checking for plugins, checking for RSS updates and communicating with a variety of servers, all while you're looking at bunnies.

A topography of you: footprints

Most important: you will leave footprints. Some of them will be left on your own computer – a collection of cache data, browsing history and naughty little files with elephantine memory called cookies. They are all very convenient; speed up your browser's performance, reduce your data download or remember your passwords and preferences from your favorite Social Networks. They also snitch on your browsing habits and compile a record of everywhere you go and everything you do. This should bother you in any case, but especially if you are using a public computer station at a library, work at a cybercafe, or share your apartment with a nosey partner!

Even if you configure your browser to not keep a history record, reject cookies and delete cached files (or allocate zero MB of space for the cache), you would still leave a trail of breadcrumbs all over the Internet. Your IP address is recorded by default everywhere, by everyone, and the packets sent and received are monitored by an increasing number of entities - commercial, governmental or criminal, along with creeps and potential stalkers.

Democratic governments everywhere are redesigning regulations to make Internet providers keep a copy of everything so they can have later access to it. In the USA, section 215 of the American PATRIOT act *'prohibits an individual or organization from revealing that it has given records to the federal government, following an investigation'*. That means that the company you pay every month as a customer to provide you with Internet access can be ordered to turn over your browsing and email records, and the law bans them from letting you know about it.

Most of the time, though, surveillance is not a *1984* affair. Google collects your searches along with your browser identification (*user agent*), your IP and a whole bunch of data that can eventually lead to your doorstep, but the ultimate aim is usually not political repression but market research. Advertisers don't fuss about advertising space any more, they just want to know everything about you. They want to know your dietary and medication habits, how many children you have and where you take them on holidays, how you make your money, how much you earn and how you like to spend it. Even more: they want to know how you *feel* about stuff. They want to know if your friends respect those feelings enough so that you can convince them to change *their* consumption habits. This is not a conspiracy, but rather the nature of Information Age capitalism. To paraphrase a famous observation of the current situation, *the best minds of our generation are thinking about how to make people click ads.*[4]

Some people think ads can be ignored or that having advertisers cater for our specific needs is a win-win situation, because at least we are spammed with things we may actually want. Even if that was the case (it isn't): should we trust Google with such reports of our life? Even if we trust Google to 'do no evil', it can still be bought by someone evil; benevolent Larry Page and Sergey Brin could be overruled by their own board, their data base be sequestered by a fascistic government. One of their 30,000 employees worldwide could cut loose and run with our data. Their servers can be hacked. In any case, their priority will always be their real customers, *the companies paying for advertising*. We are just the product being sold.

Moreover, in the Social Networks our browsing habits are generating a Permanent Record, a collection of data so vast that the information that Facebook keeps about a given user alone can fill a thousand pages. Nobody will be surprised to learn that Facebook's purpose is not to make us happy – again: if you are not paying for it, you're not the customer, you're the product. But even if you don't care about their commercial goals, consider this: the platform has publicly admitted hackers break into hundreds of thousands of Facebook accounts every day.

For a taste of what lurks behind the curtains of the websites you visit, install a plugin/add-on called *Ghostery* to your browser. It's like an x-ray-machine that reveals all the surveillance technology which might be (and often *is*) embedded in a web page, normally invisible to the user. In the same line, *Do Not Track Plus* and *Trackerblock* will give you further control over online tracking, through cookie blocking, persistent opt-out cookies, etc. Our following chapter *Tracking* will equip you with expertise in such topics.

Even in between your computer and the router, your packages can easily be intercepted by anyone using the same wireless network in the casual environment of a cafe. It is a jungle out there, but still we choose passwords like "password" and "123456", perform economic transactions and buy tickets on public wireless networks and click on links from unsolicited emails. It is not only our right to preserve our privacy but also our responsibility to defend that right against the intrusions of governments, corporations and anyone who attempts to dispossess us. If we do not exercise those rights today, we deserve whatever happens tomorrow.

---

1. If you are a Unix user, you can use the tcpdump command in the bash and view real time dns traffic. It's loads of fun! (and disturbing)
2. See list of TCP and UDP port numbers (http://en.wikipedia.org/wiki/-List_of_TCP_and_UDP_port_numbers)
3. If this exchange is happening under an HTTPS connection, the process is much more complicated and also much safer, but you will find out more about that in a most fascinating chapter called Encryption.
4. *This Tech Bubble Is Different (http://www.businessweek.com/magazine/-content/11_17/b4225060960537.htm)*, Ashlee Vance (Businessweek magazine)

Basic Tips on Browsing Privacy

In Brief

- When you visit a website you give away information about yourself to the site owner, unless precautions are taken.
- Your browsing on the Internet may be tracked by the sites you visit and partners of those sites. Use anti-tracking software.
- Visiting a website on the Internet is never a direct connection. Many computers, owned by many different people are involved. Use a secure connection to ensure your browsing can not be recorded.
- What you search for is of great interest to search providers. Use search anonymising software to protect your privacy.
- It is wiser to trust Open Source browsers like Mozilla Firefox as they can be more readily security audited.

Your browser talks about you behind your back

All browsers communicate information to the web server serving you a web page. This information includes name and version of the browser, referral information (a link on another site, for instance) and the operating system used.

Websites often use this information to customise your browsing experience, suggesting downloads for your operating system and formatting the web page to better fit your browser. Naturally however, this presents an issue as regards the user's own anonymity as this information becomes part of a larger body of data that can be used to identify you individually.

Stopping the chatter of your browser is not easily done. You can, however, falsify some of the informtion sent to web servers while you browse by altering data contained in the *User Agent*, the browser's identity. There is a very useful plugin for Firefox, for instance, called *User Agent Switcher* that allows you to set the browser identity to another profile selected from a drop down list of options.

Web sites can track you as you browse

Small files, called *cookies*, are often written onto your computer by web sites. Cookies present certain conveniences, like caching login data, session information and other data that makes your browsing experience smoother. These small pieces of data however present a significant risk to your right to anonymity on the web: they can be used to identify you if you return to a site and also to track you as you move from site to site. Coupled with the User-Agent, they present a powerful and covert means of remotely identifying your person.

The ideal solution to this problem is deny all website attempts to write cookies onto your system but this can greatly reduce the quality of your experience on the web.

See the chapter **Tracking** for guides as to how to stop web servers tracking you.

Searching online can give away information about you

When we search online using services like Bing or Google our right to privacy is already at risk, vastly more so than asking a person at an Information Desk in an airport, for instance.

Combined with the use of cookies and User Agent data this information can be used to build an evolving portrait of you over time. Advertisers consider this information very valuable, use it to make assumptions about your interests and market you products in a targeted fashion.

While some customers may sing the praises of targeted advertising and others may not care, the risks are often misunderstood. Firstly, the information collected about you may be requested by a government, even a government you did not elect (Google, for instance, is an American company and so must comply with American judicial processes and political interests). Secondly there is the risk that merely searching for information can be misconstrued as intent or political endorsement. For instance an artist studying the aesthetics of different forms of Religious Extremism might find him or herself in danger of being associated with support for the organisations studied. Finally there is the risk that this hidden profile of you may be sold on to insurance agents, provided to potential employers or other customers of the company whose search service you are using.

Even once you've ensured your cookies are cleared, your *User Agent* has been changed (see above and chapter **Tracking**) you are still giving away one crucial bit of information: the Internet Address you are connecting from (see chapter **What Happens When You Browse**). To avoid this you can use an anonymising service like *Tor* (see chapter **Anonymity**). If you are a Firefox user (recommended) be sure to install the excellent *Google Sharing* add-on, an anonymiser for Google search. Even if you don't consciously use Google, a vast number of web sites use a customised Google Search bar as a means of exploring their content.

With the above said, there are no reasons to trust Google, Yahoo or Bing. We recommend switching to a search service that takes your right to privacy seriously: DuckDuckGo (http://duckduckgo.com/).

More eyes than you can see

The Internet is a big place and is not one network but a greater network of many smaller interconnected networks. So it follows that when you request a page from a server on the Internet your request must traverse many machines before it reaches the server hosting the page. This journey is known as a *route* and typically includes at least 10 machines along the path. As packets move from machine to machine they are necessarily copied into memory, re-written and passed on.

Each of the machines along a network route belongs to someone, normally a company or organisation and may be in entirely different countries. While there are efforts to standardise communication laws across countries, the situation is currently one of significant jurisdictional variation. So, while there may not be a law requiring the logging of your web browsing in your country, such laws may be in place elsewhere along your packet's route.

The only means of protecting the traffic along your route from being recorded or tampered with is using *end to end encryption* like that provided by

TLS/Secure Socket Layer (SSL) or a *Virtual Private Network* (See chapter **VPN**). Online banking websites and webmail services like GMail use SSL to secure connections between your browser and the server. A TLS/SSL connection in the browser, when using webmail, will appear with ***https*** in the URL instead of the standard *http*, like so:

> https://gogglemail.com

Your right to be unknown

Beyond the desire to minimise privacy leakage to specific service providers, you should consider obscuring the Internet Address you are connecting from more generally (see chapter **What Happens When You Browse**). The desire to achieve such anonymity spurred the creation of the *Tor Project.*

Tor uses an ever evolving network of nodes to route your connection to a site in a way that cannot be traced back to you. It is a very robust means of ensuring your Internet address cannot be logged by a remote server. See the chapter **Anonymity** for more information about how this works and how to get started with Tor.

Browsing Privacy Fears

Social Networking - what are the dangers?

The phenomenon of Internet based Social Networking has changed not just how people use the Internet but its very shape. Large data centers around the world, particularly in the US, have been built to cater to the sudden and vast desire for people to upload content about themselves, their interests and their lives in order to participate in the digital society.

Social Networking as we know it with Facebook, Twitter (and earlier MySpace) are certainly far from 'free'. Rather, these are businesses that seek to develop upon, and then exploit, a very basic anxiety: the fear of social irrelevance. As social animals we can't bear the idea of missing out and so many find themselves placing their most intimate expressions onto a businessman's hard-disk, buried deep in a data center in another country - one they will never be allowed to visit.

Despite this many would argue that the social warmth and personal validation acquired through engagement with Social Networks well out-weighs the potential loss of privacy. Such a statement however is only valid when the *full* extent of the risks are known.

The risks of Social Networking on a person's basic right to privacy are defined by:

The scope and intimacy of the user's individual contributions.

- A user posting frequently and including many personal details constructs a body of information of greater use for targeted marketing.

The preparedness of the user to take social risks.

- A user making social connections uncritically is at greater risk from predators and social engineering attacks.

The economic interests and partners of the organisation providing the service.

- Commissioned studies from clients, data mining, sentiment analysis.

Political/legal demands exerted by the State against the organisation in the jurisdiction(s) in which it is resident.

- Court orders for data on a particular user (whether civilian or foreigner).
- Surveillance agendas by law enforcement or partners of the organisation.
- Sentiment analysis: projections of political intent.

With these things in mind it is possible to chart a sliding scale between projects like Diaspora and Facebook: the former promises some level of organisational transparency, a commitment to privacy and a general openness, whereas Facebook proves to be an opaque company economically able to gamble with the privacy of their users and manage civil lawsuits in the interests of looking after their clients. As such there is more likelihood of your interactions with a large Social Network service affecting how an Insurance company or potential employer considers you than a smaller, more transparent company.

Who can steal my identity?

This question depends on the context you are working within as you browse. A weak and universal password presents a danger of multiple services from Social Networking, Banking, WebMail etc being account hijacked. A strong and universal password on a wireless network shared with others (whether open or encrypted) is just as vulnerable. The general rule is to ensure you have a strong password (see section on **Passwords**).

Wireless networks

Here we find ourselves amidst an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone uses the same encrypted network, he can easily capture and read all unsecured traffic of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives those that know how to capture and read network packets the chance to read your password while you check your email.

A simple rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

The browser cache

Due to the general annoyance of having to type in your password repeatedly, you allow the browser or local mail client to store it for you. This is not bad in itself, but when a laptop or phone gets stolen, this enables the thief to access the owner's email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One precaution can justify you holding onto your convenient cache: disk encryption. If your laptop is stolen and the thief reboots the machine, they'll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing user session, it cannot be accessed.

Securing your line

Whenever you log into any service you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TLS/SSL* (Secure Socket Layer).

Check to see the service you're using (whether Email, Social Networking or online-banking) supports TLS/SSL sessions by looking for **https://** at the beginning of the URL. If not, be sure to turn it on in any settings provided by the service. To better understand how browsing the World Wide Web works, see the chapter **What happens when you browse.**

Can I get in trouble for Googling weird stuff?

Google and other search companies may comply with court orders and warrants targeting certain individuals. A web site using a customised Google Search field to find content on their site may be forced to log and supply all search queries to organisations within their local jurisdiction. Academics, artists and researchers are particularly at risk of being misunderstood, assumed to have motivations just by virtue of their apparent interests.

Who is keeping a record of my browsing and am I allowed to hide from them?

It is absolutely within your basic human rights, and commonly constitutionally protected, to visit web sites anonymously. Just as you're allowed to visit a public library, skim through books and put them back on the shelf without someone noting the pages and titles of your interest, you are free to browse anonymously on the Internet.

How to not reveal my Identity?

See the chapter on **Anonymity**.

How to avoid being tracked?

See the chapter on **Tracking**.

Accounts and Security

When you browse, you may be logged into various services, sometimes at the same time. It may be a company website, your email or a social networking site. Our accounts are important to us because highly sensitive information about us and others is stored on machines elsewhere on the Internet.

Keeping your accounts secure requires more than just a strong password (see section ***Passwords***) and a secure communication link with the server via TLS/SSL (see chapter ***Secure Connections***). Unless specified otherwise, most browsers will store your login data in tiny files called *cookies*, reducing the need for you re-type your password when you reconnect to those sites. This means that someone with access to your computer or phone may be able to access your accounts without having to steal your password or do sophisticated snooping.

As smartphones have become more popular there has been a dramatic rise in account hijacking with stolen phones. Laptops theft presents a similar risk. If you do choose to have the browser save your passwords then you have a few options to protect yourself:

- Use a screen lock. If you have a phone and prefer an unlock pattern system get in the habit of wiping the screen so an attacker can not guess the pattern from finger smears. On a Laptop, you should set your screensaver to require a password as well as a password on start-up.
- Encrypt your hard disk. TrueCrypt is an open and secure disk encryption system for Windows 7/Vista/XP, Mac OS X and Linux. OSX and most Linux distributions provide the option for disk encryption on install.
- Android Developers: do not enable USB debugging on your phone by default. This allows an attacker using the Android *adb shell* on a computer to access your phone's hard disk without unlocking the phone.

Can malicious web sites take over my accounts?

Those special cookies that contain your login data are a primary point of vulnerability. One particularly popular technique for stealing login data is called *click-jacking*, where the user is tricked into clicking on a seemingly innocuous link, executing a script that takes advantage of the fact you are logged in. The login data can then be stolen, giving the remote attacker access to your account. While this is a very complicated technique, it has proven effective on several occasions. Both Twitter and Facebook have seen cases of login sessions being stolen using these techniques.

It is important to develop a habit for thinking before you click on links to sites while logged into your accounts. One technique is to use another browser entirely that is not logged into your accounts as a tool for testing the safety of a link. Always confirm the address (URL) in the link to make sure it is spelled correctly. It may be a site with a name very similar to one you already trust. Note that links using URL shorteners (like http://is.gd and http://bit.ly) present a risk as you cannot see the actual link you are requesting data from.

If using Firefox on your device, use the add-on *NoScript* http://noscript.net as it mitigates many of the *Cross Site Scripting* techniques that allow for your cookie to be hijacked but it will disable many fancy features on some web sites.

Tracking

When you browse the web tiny digital traces of your presence are left behind. Many web sites harmlessly use this data to compile statistics and see how many people are looking at their site and which pages are popular, but some sites go further and use various techniques to track individual users, even going as far as trying to identify them personally. It doesn't stop there however. Some firms store data in your web browser which can be used to track you on other web sites. This information can be compiled and passed on to other organizations without your knowledge or permission.

This all sounds ominous but really who cares if some big company knows about a few web sites that we have looked at? Big web sites compile and use this data for "behavioral advertising" where ads are tailored to fit your interests exactly. That's why after looking at say, the Wikipedia entry for Majorca, one may suddenly start seeing lots of ads for packaged vacations and party hats. This may seem innocent enough, but after doing a search for "Herpes Treatments" or "Fetish Communities" and suddenly seeing listings for relevant products, one may start to feel that the web is getting a bit too familiar.

Such information is also of interest to other parties, like your insurance company. If they know you have been looking at skydiving sites or forums for congenital diseases, your premiums may mysteriously start going up. Potential employers or landlords may turn you down based on their concerns about your web interests. In extreme instances, the police or tax authorities may develop an interest without you ever having committed a crime, simply based on suspicious surfing.

How do they track us?

Every time you load a web page, the server software on the web site generates a record of the page viewed in a log file. This is not always a bad thing. When you log in to a website, there is a need for a way to establish your identity and keep track of who you are in order to save your preferences, or present you with customized information. It does this by passing a small file to your browser and storing a corresponding reference on the web server. This file is called a *cookie*. It sounds tasty but the problem is that this information stays on your computer even after leaving the web site and may phone home to tell the owner of the cookie about other web sites you are visiting. Some major sites, like Facebook and Google have been caught using them to keep track of your browsing even after you have logged out.

Supercookies / Evercookie / Zombie Cookies?

How can I prevent tracking?

The simplest and most direct way to deal with tracking is to delete the cookie files in your browser:

[show how in Firefox (tools->Clear Recent History...), chrome, IE, etc.]

The limitation to this approach is that you will receive new cookies as soon as you return to these sites or go to any other pages with tracking components. The other disadvantage is that you will lose all of your current login sessions for any open tabs, forcing you to type in usernames and passwords again. A more convenient option, supported by current browsers is *private browsing* or *incognito mode*. This opens a temporary browser window that does not save the history of pages viewed, passwords, downloaded files or cookies. Upon closing the private browsing window, all of this information is deleted. You can enable private browsing:

[show how in Firefox (tools->Start Private Browsing), chrome, IE, etc.]

This solution also has it's limitations. We cannot save bookmarks, remember passwords, or take advantage of much of convenience offered by modern browsers. Thankfully, there are several plugins specially designed to address the problems of tracking. The most extensive, in terms of features and flexibility, is Ghostery. The plugin allows you to block categories or individual services that track users. Here's how you install Ghostery:

[screenshots here installing the plugin]

Another option is to install an ad-blocking plugin like AdBlockPlus. This will automatically block many of the tracking cookies sent by advertising companies but not those used by Google, Facebook and other web analytics companies. [expand on this maybe, explain "web analytics"]

How can I see who is tracking me?

The easiest way to see who is tracking you is to use the Ghostery plugin. There is a small icon on the upper right or lower right corner of your browser window that will tell you which services are tracking you on particular web sites.

{ Suggestion: Add Abine.com's Do Not Track add-on. I suggest using both Ghosterly and DNT, as occasionally they block a different cookie. Abine also has Privacy Suite, recently developed which can give a proxy telephone and proxy email, similar to 10 Minute Mail or Guerrilla Mail for fill- in emails for forms. }

A word of warning.

If you block trackers, you will have a higher level of privacy when surfing the net. However, government agencies, bosses, hackers and unscrupulous network administrators will still be able to intercept your traffic and see what you are looking at. If you want to secure your connections you will need to read the chapter on encryption. Your identity may also be visible to other people on the internet. If you want to thoroughly protect your identity while browsing, you will need to take steps toward online anonymity which is explained in another section of this book.

Anonymity

Intro

Article 2 of the Universal Declaration of Human Rights states:

"Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.".

You can read the entire Declaration on the UN website here: http://www.un.org/en/documents/udhr/index.shtml

One way of enforcing this basic right in hostile environments is by means of anonymity, where attempts to connect an active agent to a specific person are blocked.

Acting anonymously is also a great way to help others with a high need for protection – the bigger the herd of sheep, the harder it is to target a specific one. An easy way to do so is by using TOR, a technique which routes internet traffic between users of a special software, thus making it untraceable to any specific IP address or person without having control over the whole network (and nobody has that yet in the case of the internet). A highly functional means to protect ones own identity is by using anonymous proxy servers and Virtual Private Networks (VPN).

Proxy

*"An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable. It is a proxy [server] computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information." (http://en.wikipedia.org/wiki/Anonymizer)*

The main purpose behind using a proxy is to hide or to change Internet address (IP address) assigned to user's computer. There can be a few reasons for needing to do so, for example:

- To anonymize access to particular server(s) and/or to obfuscate traces left in the log files of a web-server. For instance a user might need/want to access sensitive materials online (special materials, research topics or else) without triggering authorities attention.
- To break through firewalls of corporations or repressive regimes. A corporation/government can limit or completely restrict Internet access for a particular IP address or a range of IP addresses. Hiding behind a proxy will help to trick these filters and access otherwise forbidden sites.
- To watch online video and streams banned in your country due to legal issues.
- To access websites and/or materials available only for IP addresses belonging to a specific country. For example, a user wants to watch a BBC video stream (UK-only) while not residing in the UK.
- To access the Internet from a partially banned/blocked IP address. Public IP addresses can often have "bad reputation" (bandwidth abuse, scam or unsolicited email distribution) and be blocked by some web-sites and servers.

While a usual scenario would be to use proxy for accessing the Web (HTTP), practically Internet protocol can be proxied - i.e. sent via a remote server. Unlike a router, proxy server is not directly forwarding remote user requests but rather mediates those requests and echos responses back to remote user's computer.

Proxy (unless setup as "transparent") does not allow direct communication to the Internet thus applications such as browsers, chat-clients or download applications need to be made aware of the proxy server (see *Safer Browsing/Proxy settings* chapter)

Tor

"- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android."
(https://www.torproject.org)

Tor is a system intended to enable online anonymity, composed of client software and a network of servers which can hide information about users' locations and other factors which might identify them. Imagine a message being wrapped in several layers of protection: every server needs to take off one layer, thereby immediately deleting the sender information of the previous server.

Use of this system makes it more difficult to trace Internet traffic to the user, including visits to Web sites, online posts, instant messages, and other communication forms. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business, by keeping their internet activities from being monitored. The software is open-source and the network is free of charge to use.

Tor cannot and does not attempt to protect against monitoring the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation). *End-to-End Correlation* is a way of matching an online identity with a real person.

A recent case of this involved the FBI wanting to prove that the man Jeremy Hammon was behind an alias known to be responsible for several Anonymous attacks. Sitting outside his house, the FBI were monitoring his wireless traffic alongside a chat channel the alias was known to visit. When Jeremy went online in his apartment, inspection of the wireless packets revealed he was using Tor at the same moment the suspected alias associated with him came online in the surveilled chat channel. This was enough to incriminate Jeremy and he was arrested.

See chapter *Using Tor* in the *Safer Browsing* section for setup instructions.

VPN

The way your data makes it to the desired server and back to your laptop computer or a mobile device is not as straightforward as it might seem. Suppose you are connected to a wireless network at home and opening a wikipedia.org page. The path your request (data) takes will consist of multiple middle points, or *"hops"* in network-architect terminology. At each of these hops (likely to be more then 5) your data can be scooped, copied and potentially modified. For example:

- Your wireless network (your data can be sniffed from the air)
- Your ISP (in most countries they are obliged to keep detailed logs of user activity)
- Internet Exchange Point (IXP) somewhere on another continent (usually more secure then any other *hop*)
- ISP of the hosting company that hosts the site (is probably keeping logs)
- Internal network to which the server is connected
- And multiple hops between...

Any person with physical access to the computers or the networks which are on the way from you to the remote server, intentionally or not, can collect and reveal the data that's passing from you to the remote server and back. This is especially true for the few last leaps that an internet connection makes to reach a user - so called 'last mile' situations. That includes domestic and public wireless or wired networks, telephone and mobile networks, networks in libraries, homes, schools, hotels. Your ISP can not be considered a safe, or 'data-neutral' instance either. In many countries state agencies do not require a warrant to access your data, and there is always the risk of intrusion by paid attackers working for adversaries with deep pockets.

VPN - a Virtual Private Network - is a solution for this 'last-mile' leakage. VPN is a technology that allows the creation of a virtual network on top of an existing infrastructure. Such a VPN network operates using the same protocols and standards as the underlying physical network. Programs and operating systems use it transparently, as if it were a separate network connection. But its topology - how network nodes (you, the VPN server and, potentially, other members or services available on VPN) are interconnected in relation to the physical space - is entirely redefined.

Imagine that instead of having to entrust your data to a series of middle-man (your local network, ISP, the state) you have the choice to instead pass it via a server of a trusted VPN (recommendation or research can help here). Your data will start its journey here to the remote location. VPN allows you to re-create your local and geo-political context altogether - from the moment your data leaves your computer and gets into the VPN network it is fully secured with TLS/SSL type encryption. As such it will appear as random noise to any node who might be spying after you. It is as if your data were traveling inside an independent titanium-alloy pipe, unbreakable all the way from your laptop to the VPN server. Of course one could argue that eventually, once your data is outside the safe harbour of VPN, it becomes vulnerable again, but this is only partially true. Once your data exits the VPN server it is far away from you - beyond the reach of creeps sniffing on the local wireless network, your venal ISP or a government obsessed with anti-terrorism laws. A serious VPN provider will have their servers installed at a high-security Internet exchange location, rendering any physical human access, tapping or logging a difficult task.

> *"Today everything you do on the Internet is monitored and we want to change that. With our fast VPN service you get totally anonymous on the Internet. It's also possible to surf censored web sites, that your school, ISP, work or country are blocking. [DarkVPN] will not only help people to surf anonymously, it also helps people in countries like China to be able to surf censored web pages. Which is your democratic right. DarknetVPN gives all VPN users an anonymous IP address. All electronic tracks will end up with us. We do not save any log files in order to achieve maximum anonymity. With us you always surfing anonymously, secure and encrypted."*
> *(http://www.darknetvpn.com/about.php)*

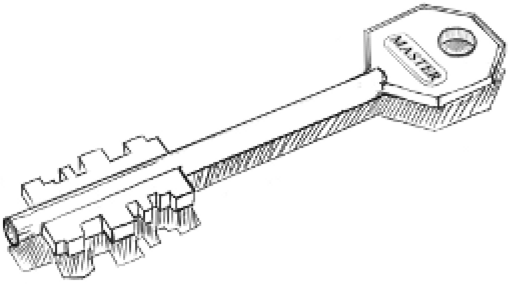
Another interesting and often underrated features of VPN is encoded in its name - besides being **V**irtual and **P**rivate it is also a **N**etwork. VPN allows not only connection via the VPN server to the rest of the world but also communication with other members of the same VPN network, without ever having to leave the safety of encrypted space. Through this functionality Virtual Private Network becomes something like a *DarkNet* (in a broader sense of the definition) - a network isolated from the Internet and inaccessible to uninvited guests. A connection to VPN server, and thus the private network it facilitates, require a key or a *certificate*, and so only "invited" users are allowed. There is no chance that an Internet stranger can gain access to what's on a VPN without enrolling as a user or stealing someone's keys. While not usually referred to as such, any corporate *Intranet* type of network is technically a DarkNet too.

"A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.." (http://en.wikipedia.org/wiki/Virtual_private_network)

Many commercial VPN providers stress the *anonymity* that their service provides. Quoting Ipredator.org page (a VPN service started by the people behind The Pirate Bay project): *"You'll exchange the IP address you get from your ISP for an anonymous IP address. You get a safe/encrypted connection between your computer and the Internet"*. Indeed, when you access the Internet via a VPN connection it does appear as if the connection is originating from the IP address of IPredator servers.

"You'll exchange the IP address you get from your ISP for an anonymous IP address. You get a safe/encrypted connection between your computer and the Internet."
(https://www.ipredator.se)

Publishing and Distribution



Publishing Anonymously

Whether you are an activist operating under a totalitarian regime, an employee determined to expose some wrongdoings in your company or a vengeful writer composing a bitchy portrait of your ex-wife, you need to protect your identity. If you are not collaborating with others, the focus lies on anonymity and not encryption or privacy.

If the message is urgent and the stakes are high, one easy way to just get it out quickly is going to an internet cafe one usually does not frequent, create accounts specifically set up for the task, deliver the data and discard those accounts right after that. If you are in a hurry, consider MintEmail (http://www.mintemail.com/) or FilzMail (http://www.filzmail.com/), where your address will expire from 3 to 24 hours respectively. Do not do anything else while you're there; don't check your gmail account, do not have a quick one on Facebook and clear all cache, cookies and history and close the browser before you leave.

If you keep these basic rules, the worst – though highly improbable – thing that could happen would be that the offered computer is compromised and logging keystrokes, revealing passwords or even your face, in case an attached webcam is remotely operated. Don't do this at work or in a place where you are a registered member or a regular visitor, like a club or a library.

If you want to maintain a constant stream of communication and maybe even establish an audience, this method quickly becomes quite cumbersome, and you might also run out of unused internet cafes. In this case you can use a machine you own, but, if you cannot dedicate one especially to this purpose, boot your computer with a different operating system (OS). This can be easily done by using a USB stick to boot a live operating system like TAILS, which comes with TOR enabled by default and includes state-of-the-art cryptographic tools. In any case, use Tor to disguise your IP.

Turn off all cookies, history and cache options and never use the same profile or the same browser for other activities. Not only would that add data to your topography as a user in the Net, but it also opens a very wide window for mistakes. If you want extra support, install *Do Not Track Plus* and *Trackerblock* or *Ghostery* in your browser add-ons menu.

Use passwords for different accounts and choose proper passwords or even passphrases (more about that in the basic tips section). Protect your entire system with a general password, change it often and do not share it with anyone, especially not your lover. Install a keystroke logger to see if someone sneaks into your email, *especially* your lover. Set up your preferences everywhere to log out of every service and platform after 5 minutes of non-use. Keep your superhero identity to yourself.

If you can mantain such level of discipline, you should even be capable of using your own internet connection. But consider this: not using a dedicated system makes it incredibly difficult to keep all the different identities separated in a safe way, and the feeling of safety often leads to carelessness. Keep a healthy level of neurosis.

Today there are many publishing possibilities, from cost-free blogging sites (Blogspot, Tumblr, WordPress, Identi.ca) to PasteBins (see glossary) and some specifically catered to anonymous users like BlogACause. Global Voices Advocacy recommends using WordPress through the Tor network. Keep a sane level of cynicism; they all act in commercial interests that you use for 'free' and so cannot be trusted at all, especially in that they may be bound to the demands of a legal juristiction that is not your own. All providers are, when it comes down to it, traitors.

If registration with these services requires a working email address, create one dedicated solely to this purpose. Avoid Gmail, Yahoo, Hotmail and other big commercial platforms with a history of turning over their users and go for an specialized service like Hushmail (https://www.hushmail.com/). For more on anonymous email, please find the chapter Anonymous email in the previous section.

Several Don'ts

Don't register a domain. There are services that will protect your identity from a simple who is query, like Anonymous Speech or Silent Register, but they will know who you are through your payment data. Unless you have the chance to purchase one in BitCoins, limit yourself to one of the domains offered by your blogging platform like yourblogname.blogspot.com and choose a setting outside your native country. Also, find a name that doesn't give you away easily. If you have problems with that, use a blog name generator online.

Don't open a social network account associated to your blog. If you must, keep the level of hygiene that you keep for blogging and never ever login while using your regular browser. If you have a public social network life, avoid it all together. You will eventually make a mistake.

Don't upload video, photo or audio files without using an editor to modify or erase all the meta data (photos contain information up to the GPS coordinates of the location the photo was taken at) that standard digital cameras, SmartPhones, recorders and other devices add by default. The *Metadata Anonymisation Toolkit* might help you with that.

Don't leave a history. Add X-Robots-Tag to your http headers to stop the searching spiders from indexing your website. That should include repositories like the Wayback Machine from archive.org. If you don't know how to do this, search along the lines of "Robots Text File Generator".

Don't leave comments. If you must, maintain the levels of hygiene that you use for blogging and always logout when you're done and for god sakes do not troll around. Hell hath no fury like a blogger scorned.

Don't expect it to last. If you hit the pot and become a blogging sensation (like *Belle de Jour*, the British PhD candidate who became a sensation and sold a book and mused two TV shows about her double life as a high escort) there will be a legion of journalists, tax auditors and obsessive fans scrutinizing your every move. You are only human: they will get to you.

Don't linger. If you realize you have already made any mistakes but nobody has caught you yet, do close all your accounts, uncover your tracks and start a totally new identity. The Internet has infinite memory: one strike, and you're out of the closet.

Anonymous Email

Every data packet travelling through the Internet contains information about its sender and its recipient. This applies to email as well as any other network communication. There are several ways to reduce identifying information but no way to remove it completely.

The issue of anonymous email has been in the media often, most recently in the case surrounding the resignation of the Director of the CIA, David Petreus. You can find out all about the case by using your favourite search engine, but the quick version is that Petreus and his lover were using the draft folder of a Gmail account to leave each other messages.

The Electronic Frontier Foundation reports that,

> "According to press reports, Broadwell and Petraeus used pseudonymous webmail accounts to talk to each other. That was a prudent first step, but it was ineffectual once the government examined Google's logs to find the IP address that Broadwell was using to log into her pseudonymous account, and then checked to see what other, non-pseudonymous accounts had been used from the same IP address. Under current US law, much of this information receives inadequate protection, and could be obtained from a webmail provider by the FBI without even requiring a warrant.
>
> Because webmail providers like Google choose to keep extremely extensive logs, protecting your pseudonymous webmail against this kind of de-anonymization attack requires forethought and discipline."
>
> (https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts)

It has also been suggested that due to these messages being stored in the draft folder, but not actually sent, that they were not subject to legislation covering email communication. In the same post the EFF provide a tutorial on Anonymous Email Accounts using Tor and Hushmail, explaining the issues therein. (https://www.eff.org/deeplinks/2012/11/when-will-our-email-betray-us-email-privacy-primer-light-petraeus-saga)

Sending From Throw-away Email Accounts

One option is to use a throw-away email account. This is an account set up at a service like Gmail or Hotmail, used once or twice for anonymous exchange. When signing up for the account, you will need to provide fake information about your name and location. After using the account for a short amount of time, say 24 hours, you should never log in again. If you need to communicate further, then create a new account.

It is very important to keep in mind that these services keep logs of the IP addresses of those using them. If you are sending highly sensitive information, you will need to combine a throw away email account with Tor in order keep your IP address hidden.

If you are not expecting a reply, then an anonymous remailer like AnonEmail or Silentsender may be a useful solution. A remailer is a server that receives messages with instructions on where to send the data and acts as a relay, forwarding it from a generic address without revealing the identity of the original sender. This works best when combined with an email provider like Hushmail or RiseUp who are specially set up for secure email connections.

Both of these methods are useful, but only if you always remember that the intermediary himself knows where the original message came from and can read the messages as they come in. Despite their claims to protect your identity, these services often have user agreements that indicate their right "to disclose to third parties certain registration data about you" or they are suspected to be compromised by secret services. The only way to safely use this technique is to not trust these services at all, and apply extra security measures: send via Tor using a throw-away email address.

If you only need to receive email, services like Mailinator and MintEmail give you an email address that destroys itself after a few hours. When signing up for any account, you should provide fake information about your name and location and protect yourself by using Tor.

Be Careful about what you say!

The content of your message can give away your identity. If you mention details about your life, your geography, social relations or personal appearance, people may be able to determine who is sending the message. Even word choice and style of writing can be used to guess who might be behind anonymous emails.

You should not use the same user name for different accounts or use a name that you are already linked to like a childhood nickname or a favourite book character. You should never use your secret email for normal personal communication. If someone knows your secrets, do not communicate with that person using this email address. If your life depends on it, change your secret email address often as well as between providers.

Finally, once you have your whole your email set up to protect your identity, vanity is your worst enemy. You need to avoid being distinct. Don't try to be clever, flamboyant or unique. Even the way you break your paragraphs is valuable data for identification, especially these days when every school essay and blog post you have written is available in the Internet. Powerful organizations can actually use these texts to build up a database that can "fingerprint" writing.

File Sharing

The term *File Sharing* refers to the practice of sharing files on a network, often with widest possible distribution in mind. Unfortunately in recent years the term has come to be popularly associated with the distribution of content registered under certain copyright licenses that disallow the distribution of copies (eg. supposed criminal activity). Regardless of this new association, file sharing remains a vital tool for many world wide: from academic groups to scientific networks and open source software communities.

In this book we wish to help you learn to privately distribute files, with other consenting people, without the content of that exchange known to others or the transaction stopped by an external party. Your basic right to anonymity and to not be spied upon protects that. Suspicions that those things *might* have been stolen and are not yours to give does not undermine that same and original right to privacy.

The history of the internet is littered with attacks of different types on publication and distribution nodes, conducted by different means (court order, Distributed Denial of Service attacks). What such events have demonstrated is that if one wants information to be persistently available and robust against attack, it is a mistake to rely upon a single node which can be neutralised.

This has recently been demonstrated by the takedown of the direct download service Megaupload, whose disappearance led to the loss of massive amounts of its users' data, much of it extraneous even to the alleged copyright infringements which formed the pretext for its closure. In similar vein ISPs will often take down web sites containing disputed material merely because it is cheaper for them to do so than to go to court and have a judge decide. Such policies leave the door open to groundless bullying by all manner of companies, organisations and individuals ready and willing to make aggressive use of legal letters. Both direct download services and ISPs are examples of centralised structures which cannot be relied upon both because they are a single point of failure for attack, and because their commercial interests are not aligned with those of their users.

Spreading files through distribution, decentralising the data, is the best way to defend against such attacks. In the following section two realms of filesharing are profiled. The first are standard p2p technologies whose technical design is determined by the efficiency of the networks in enabling speed of distribution and discovery of content through associated search mechanisms. The second focuses on I2P as an example of a so-called darknet, its design prioritises security and anonymity over other criteria offering a robust, if less resource efficient, path to persistent availability.

The means of sharing files mentioned below are just some examples of the many P2P technologies that were developed since 1999. BitTorrent and Soulseek have very different approaches, both however were designed for easy usability by a wide public and have significant user communities. I2P is of more recent development, has a small user base.

BitTorrent has become the most popular P2P file-sharing system. The controversy that surrounds it nowadays ironically seems to help the community grow, while police, lobbied by powerful copyright holders seize torrent-tracker server hardware and pursue their operators, sometimes to the point of jailing them as in the case of The Pirate Bay.

Soulseek - while it has never been the most popular file-sharing platform, neither did it ever have the ambition. Soulseek focuses on the exchange of music between enthusiasts, underground producers, fans and researchers. The system and the community around it is completely isolated from the Web: Soulseek files can't be linked to. They are kept exclusively on the hard-disks of Soulseek users. The content of the network fully depends on how many members are connected and what they share. Files are transferred only between two users at a time and nobody but those two users are involved. Because of this 'introverted' character - and the specificity of its content - Soulseek has stayed out of sight of legislation and non-pro-copy copyright advocates.

I2P is one of several systems developed to resist censorship (others include FreeNet and Tor) and has a much smaller user community, it is highlighted here because of its inclusion of Bit Torrent functionality within its basic installation. These systems can also be used to provide hidden services, amongst others, enabling you to publish web pages within their environments.

BitTorrent

BitTorrent is a peer-to-peer (P2P) protocol that facilitates distribution of data stored across multiple nodes/participants of the network. There are no central servers or hubs, each node is capable of exchanging data with any other node, sometimes hundreds of them simultaneously. The fact that data is exchanged in parts between numerous nodes allows for great download speeds for popular content on BitTorrent networks, making it quickly the de facto P2P file-sharing platform.

If you are using BitTorrent to circulate material of ambiguous legality, you should know that enforcement agents typically collect information on allegedly infringing peers by participating in torrent swarms, observing and documenting the behaviour of other peers. The large number of users creates a difficulty for the enforcement system simply at the level of scaling up - there simply are not the resources to pursue every user. Any court case will require actual evidence of data transfer between your client and another (and usually evidence of you uploading), it is enough that you provide even part of the file, not the file in its entirety, for a prosecution to have legs. But if you prefer to lean towards greater caution, you should use a VPN to route your BitTorrent traffic, as detailed in the *Using VPN* chapter.

Leeching (downloading) of a file from BitTorrent network begins with a *torrent file* or *magnet link*. A torrent file is a small file containing information on the larger files you want to download. The torrent file tells your torrent client the names of the files being shared, a URL for the *tracker* and a *hash* code, which is a unique code representing, and derived from, the underlying file - kind of like an ID or catalog number. The client can use that *hash* to find others seeding (uploading) those files, so you can download from their computers and check the authenticity of the chunks as they arrive.

A *Magnet Link* does away with the need for a torrent file and is essentially a hyperlink containing a description for that torrent, which your torrent client can immediately use to start finding people sharing the file you are willing to download. Magnet links don't require a tracker, instead they rely on *Dis-*

tributed Hash Table (DHT) -which you can read more about in the *Glossary*- and *Peer Exchange*. Magnet links do not refer to a file by its location (e.g. by IP addresses of people who have the file, or URL) but rather defines search parameters by which this file can be found. When a magnet link is loaded, the torrent client initiates an availability search which is broadcast to other nodes and is basically a shout-out "who's got anything matching this hash?!". Torrent client then connects to the nodes which responded to the shout-out and begins to download the file.

BitTorrent uses encryption to prevent providers and other man-in-the-middle from blocking and sniffing your traffic based on the content you exchange. Since BitTorrent swarms (flocks of seeders and leechers) are free for everyone to join it is possible for anyone to join a swarm and gather information about all connected peers. Using magnet links will not prevent you from being seen in a swarm; any of the nodes sharing the same file must communicate between each-other and thus, if just one of the nodes in your swarm is rogue, it will be able to see your IP address. It will also be able to determine if you are seeding the data by sending your node a download request.

One important aspect of using BitTorrent is worth a special mention. Every chunk of data that you receive (leech) is being instantly shared (seeded) with other BitTorrent users. Thus, a process of downloading transforms into a process of (involuntary) publishing, using a legal term - *making available* of that data, before the download is even complete. While BitTorrent is often used to re-distribute freely available and legitimate software, moves, music and other materials, its "making available" capacity created a lot of controversy and led to endless legal battles between copyright holders and facilitators of BitTorrent platforms. At the moment of writing this text, the co-founder of *The Pirate Bay* Gottfrid Svartholm is being detained by Swedish police after an international warrant was issued against him.

For these reasons, and a public relations campaign by copyright holders, use of BitTorrent platforms has become practically analogous to piracy. And while the meaning of terms such as *piracy, copyright* and *ownership* in digital context is yet to be settled, many ordinary BitTorrent users have been already prosecuted on the basis of breaking copyright laws.

Most torrent clients allow you to block IP addresses of known copyright trolls using blacklists. Instead of using public torrents one can also join closed trackers or use BitTorrent over VPN or Tor.

In situations when you feel that you should be worried about your BitTorrent traffic and it's anonymity go through the following check-list:

- Check if your torrent client supports peer-blacklists.
- Check if the peer-blacklist definitions are updated on a daily basis.
- Make sure your client supports all recent protocols - DHT, PEX and Magnet links.
- Choose a torrent client that supports encrypted peers and enable it.
- Upgrade or change your torrent client if any of the above mentioned options is not available.
- Use VPN connection to disguise your BitTorrent traffic from your ISP. Make sure your VPN provider allows P2P traffic. See more tips and recommendations in *Using VPN* chapter.
- Do not leech and seed stuff you don't know much about.
- Be suspicious of high ratings and overly-positive comments regarding particular torrent link.

SoulSeek

As a peer to peer (P2P) file sharing program, the content available is determined by the users of the Soulseek client, and what files they choose to share. The network has historically had a diverse mix of music, including underground and independent artists, unreleased music, such as demos and mix-tapes, bootlegs, etc. It is is entirely financed by donations, with no advertising or user fees.

"Soulseek does not endorse nor condone the sharing of copyrighted materials. You should only share and download files which you are legally allowed to, or have otherwise received permission to, share." (http://www.soulseekqt.net)

Soulseek network depends on a pair of central servers. One server supports the original client and network, and the other supporting the newer network. While these central servers are key to coordinating searches and hosting chat rooms, they do not actually play a part in the transfer of files between users, which takes place directly between the users concerned.

Users can search for items; the results returned being a list of files whose names match the search term used. Searches may be explicit or may use wildcards/patterns or terms to be excluded. A feature specific to the Soulseek search engine is the inclusion of the folder names and file paths in the search list. This allows users to search by folder name.

The list of search results shows details, such as the full name and path of the file, its size, the user who is hosting the file, together with that users' average transfer rate, and, in the case of mp3 files, brief details about the encoded track itself, such as bit rate, length, etc. The resulting search list may then be sorted in a variety of ways and individual files (or folders) chosen for download.

Unlike BitTorrent, Soulseek does not support multi-source downloading or "swarming" like other post-Napster clients, and must fetch a requested file from a single source.

While the Soulseek software is free, a donation scheme exists to support the programming effort and cost of maintaining the servers. In return for donations, users are granted the privilege of being able to jump ahead of non-donating users in a queue when downloading files (but only if the files are not shared over a local area network). The Soulseek protocol search algorithms are not published, as those algorithms run on the server. However several Open Source implementations of server and client software exits for Linux, OS X and Windows.

Regarding privacy and copyright issues Soulseek stand quite far away from BitTorrent too. Soulseek has been taken to court only once, in 2008, but even that did not go anywhere. There are no indications of Soulseek users ever being brought to court or accused of illegal distribution of copyrighted materials or any other 'digital-millenium' crimes.

If you want to use the Soulseek network with some degree of real anonymity, you will need to use it over a VPN.

I2P

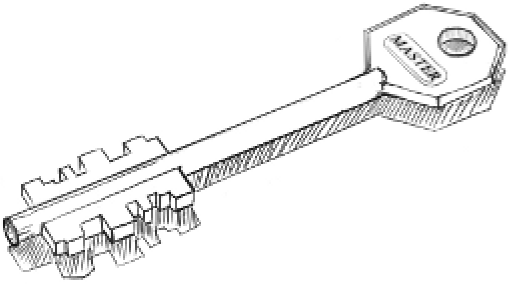
I2P began as a fork from the Freenet project, originally conceived as a mathod for censorship-resistant publishing and distribution. From their website:

> The I2P project was formed in 2003 to support the efforts of those trying to build a more free society by offering them an uncensorable, anonymous, and secure communication system. I2P is a development effort producing a low latency, fully distributed, autonomous, scalable, anonymous, resilient, and secure network. The goal is to operate successfully in hostile environments - even when an organization with substantial financial or political resources attacks it. All aspects of the network are open source and available without cost, as this should both assure the people using it that the software does what it claims, as well as enable others to contribute and improve upon it to defeat aggressive attempts to stifle free speech.

http://www.i2p2.de/

For a guide to installing the software and configuring your browser see the chapter on ***Installing I2P*** in section ***Secure Filesharing*** (Ubuntu only for now). Once complete, on launch you will be brought to a console page containing links to popular sites and services. In addition to the usual webpages (referred to as eePsites) there are a range of applications services available ranging from the blogging tool Syndie to a built in BitTorrent client which functions through a web interface.

Secure Calls and SMS



Secure Calls

Phone calls made over the normal telecommunications system have some forms of protection from third party interception, i.e. GSM mobile phones calls are encrypted. GSM calls are not encrypted end-to-end however and telephone providers are increasingly forced to give governments and law enforement organisations access to your calls. In addition to this the encryption used in GSM has been cracked and now anyone with enough interest and capital can buy the equipment to intercept calls. A GSM Interceptor (http://en.intercept.ws/catalog/2087.html) is an off the shelf device to record mobile phone conversations when in the vicinity of the call. Centralised or proprietary systems like Skype also encrypt calls but have built in backdoors for secret services and governments and are at the behest of their owner (in Skype's case Microsoft).

A solution to this problem is to make encrypted calls using Voice over IP (VoIP) through an Internet connection. Both WiFi or mobile data networks can be used: cracking the GSM or Wireless password will not mean that your call can be intercepted.

As regards platforms, Android has a wider range of open source VoIP software, largely because Apple's AppStore licensing model prohibits distribution of software released under the *General Public License* (approximately 60% of all open source software released). The GPL is very popular in the security and networking community.

At the time of writing iPhone users have only non-open-source options available for purchase, like *Groundwire* (http://www.acrobits.cz/11/acrobits-groundwire-for-iphone). **Warning: as it is not open, the security of Groundwire cannot be assured!**

Android users head over to the section **Call Encryption** to get started making secure VoIP calls.

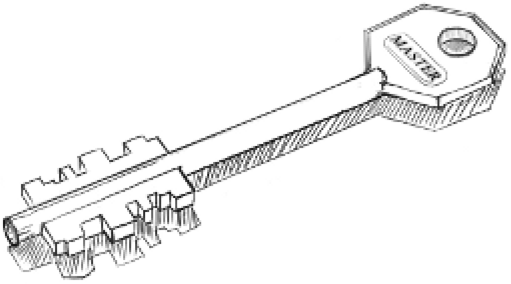
Secure Messaging

SMS are short messages sent between mobile phones. The text is sent without encryption and can be read and stored by mobile phone providers and other parties with access to the network infrastructure to which you're connected. To protect your messages from interception you have to use a *chat protocol* over your data connection. Thankfully this is not at all difficult. Many Instant Messaging providers use the *Extensible Messaging and Presence Protocol* (XMPP) that allows users to use various clients to send and receive messages and exchange message with other providers.

Although XMPP uses TLS/SSL (see glossary entry TLS/SSL) encryption to prevent 3rd party interception, your provider can still read your messages and hand them over to other entities. *Off-the-Record* (OTR) Messaging however allows you encrypt your messages. The messages you send do *not* have digital signatures that can be verified by a third party, consequently the identity of their author is *repudiable afterwards.* Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured of the *integrity* of the messages - what s/he sees is authentic and unmodified.

See the section **Instant Messaging Encryption**

Basic Email Security



Start Using Thunderbird

In upcoming sections, we will be using Mozilla's Thunderbird e-mail program to show you how to configure your e-mail client for maximum security. Similar to Mozilla's Firefox browser, Thunderbird has many security advantages over its counterparts like Apple Mail and Outlook.

Thunderbird is a so-called "mail user agent" (MUA). This is different from web-based e-mail services like Google's Gmail. You must install the Thunderbird application on your computer. Thunderbird has a nice interface and features that enable you to manage multiple mailboxes, organize messages into folders, and search through mails easily.

Thunderbird can be configured to work with your existing e-mail account, whether that account is through your Internet Service Provider (such as Comcast) or through an web-based email provider (such as Gmail).

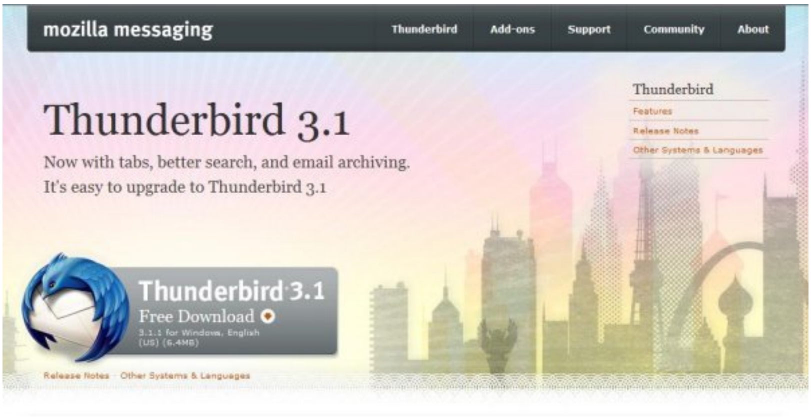
Using Thunderbird has many advantages over using web-based e-mail interfaces. These will be discussed in the following chapter. To summarize, though, Thunderbird enables much greater privacy and security than web-based e-mail services.

This section provides information on how to install Thunderbird on Windows, Mac OS X, and Ubuntu.

Installing Thunderbird on Windows

Installing Thunderbird involves two steps: first, download the software and then run the installation program.

1. Use your web browser to visit the Thunderbird download page at http://www.mozillamessaging.com/en-US/thunderbird/. This page detects your computer's operating system and language, and recommends the best version of Thunderbird for you to use.

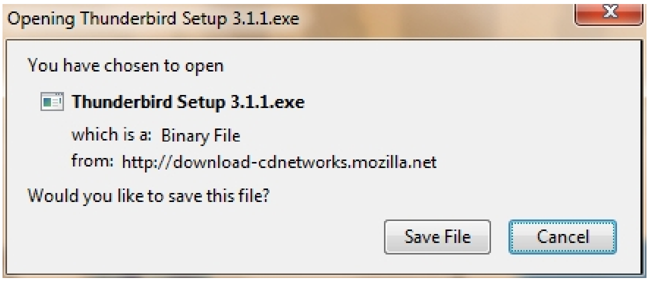


Thunderbird 3.1

Now with tabs, better search, and email archiving.
It's easy to upgrade to Thunderbird 3.1

If you want to use Thunderbird in a different language or with a different operating system, click the *Other Systems and Languages* link on the right side of the page and select the version that you need.

2. Click the download button to save the installation program to your computer.



Opening Thunderbird Setup 3.1.1.exe

You have chosen to open

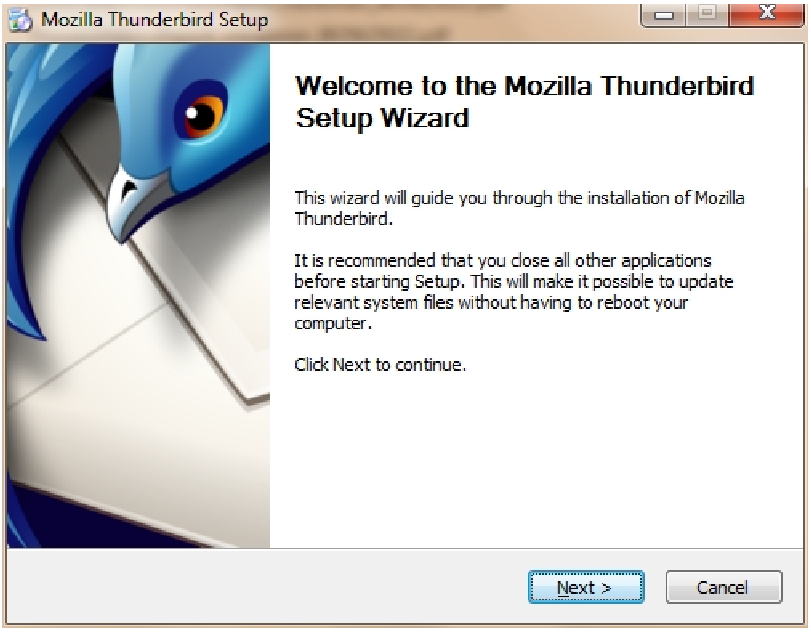
Thunderbird Setup 3.1.1.exe

which is a: Binary File
from: http://download-cdnetworks.mozilla.net

Would you like to save this file?

Click the **Save** button to save the Thunderbird Setup file to your computer.

3. Close all applications running on your computer.
4. Find the setup file on your computer (it's usually in the Downloads folder or on your desktop) and then double-click it to start the installation. The first thing that the installer does is display the **Welcome to the Mozilla Thunderbird Setup Wizard**screen.



Mozilla Thunderbird Setup

Welcome to the Mozilla Thunderbird Setup Wizard

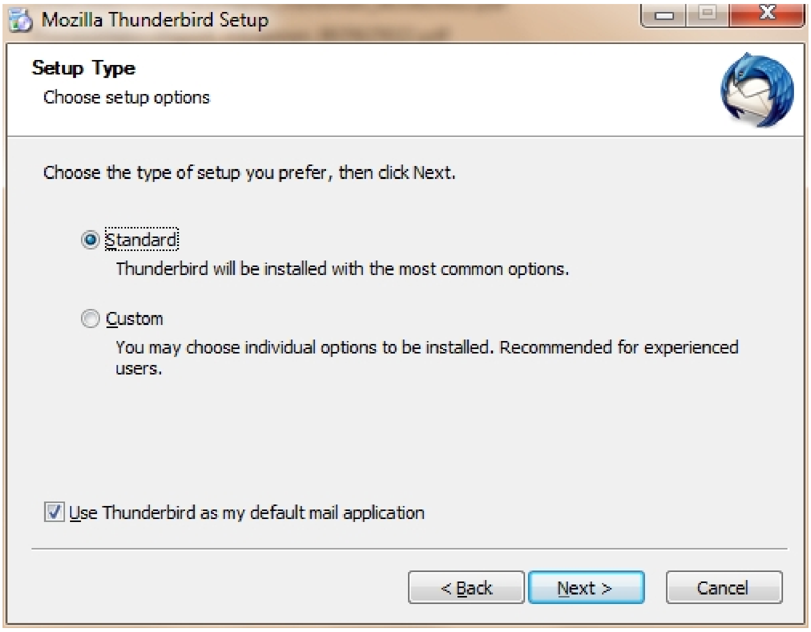
This wizard will guide you through the installation of Mozilla Thunderbird.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Click the **Next** button to start the installation. If you want to cancel it, click the **Cancel** button.

5. The next thing that you see is the **Setup Type** screen. For most users the Standard setup option is good enough for their needs. The Custom setup option is recommended for experienced users only. Note that Thunderbird installs itself as your default mail application. If you do not want this, clear the checkbox labeled **Use Thunderbird as my default mail application**.



Mozilla Thunderbird Setup

Setup Type

Choose setup options

Choose the type of setup you prefer, then click Next.

● Standard

Thunderbird will be installed with the most common options.

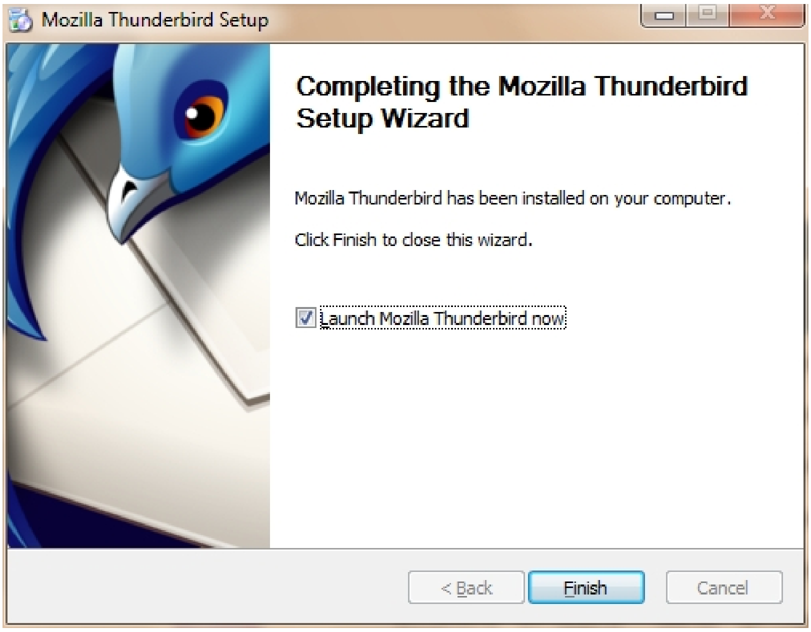
○ Custom

You may choose individual options to be installed. Recommended for experienced users.

☑ Use Thunderbird as my default mail application

Click the **Next** button to continue the installation.

6. After Thunderbird has been installed, click the **Finish** button to close the setup wizard.



Mozilla Thunderbird Setup

Completing the Mozilla Thunderbird Setup Wizard

Mozilla Thunderbird has been installed on your computer.

Click Finish to close this wizard.

☑ Launch Mozilla Thunderbird now

If the **Launch Mozilla Thunderbird now** checkbox is selected, Thunderbird starts after it has been installed.

Installing Thunderbird on Ubuntu

There are two different procedures for installing Thunderbird on Ubuntu: one for version 10.04 or later, and one for earlier versions of Ubuntu. We describe both below.

Thunderbird will not run without the following libraries or packages installed on your computer:

- GTK+ 2.10 or higher
- GLib 2.12 or higher
- Pango 1.14 or higher
- X.Org 1.0 or higher

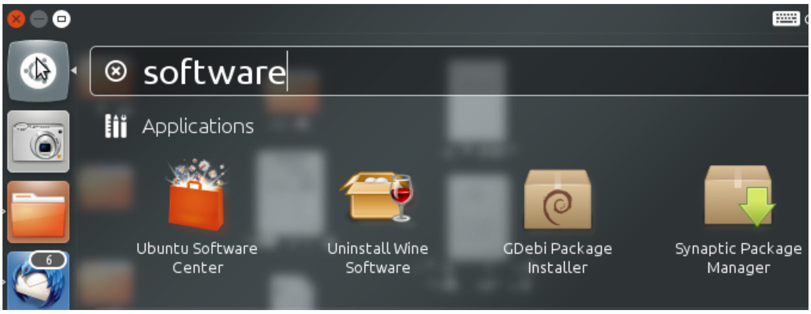
Mozilla recommends that a Linux system also has the following libraries or packages installed:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- HAL 0.5.8 or higher
- GNOME 2.16 or higher

Installing Thunderbird on Ubuntu 12.04 or newer

If you're using Ubuntu 12.04 or newer, the easiest way to install Thunderbird is through the Ubuntu Software Center.

1. Type **Software** in the Untiy search window.

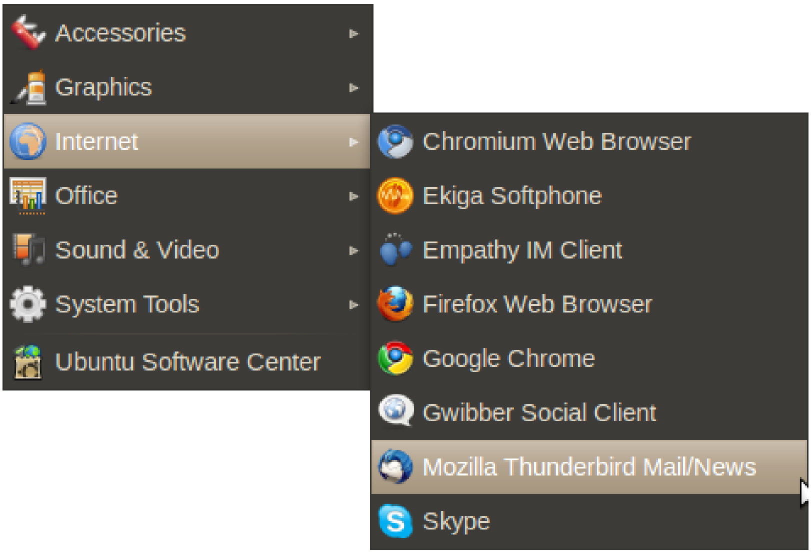


2. Click on 'Ubuntu Software Center'
3. Type "Thunderbird" in the search box and press the Enter on your keyboard. The Ubuntu Software Center finds Thunderbird in its list of available

software.

4. Click the **Install** button. If Thunderbird needs any additional libraries, the Ubuntu Software Center alerts you and installs them along with Thunderbird.

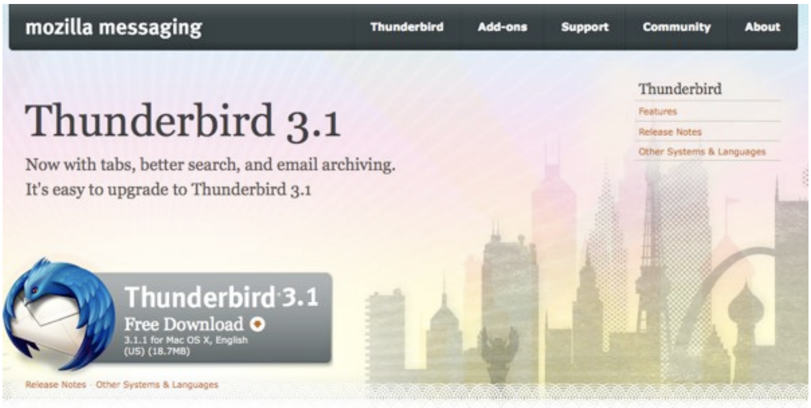
You can find the shortcut to start Thunderbird in the Internet option under the Applications menu:



Installing Thunderbird on Mac OS X

To install Thunderbird on your Mac, follow these steps:

1. Use your web browser to visit the Thunderbird download page at http://www.mozillamessaging.com/en-US/thunderbird/. This page detects your computer's operating system and language, and it recommends the best version of Thunderbird for you to use.

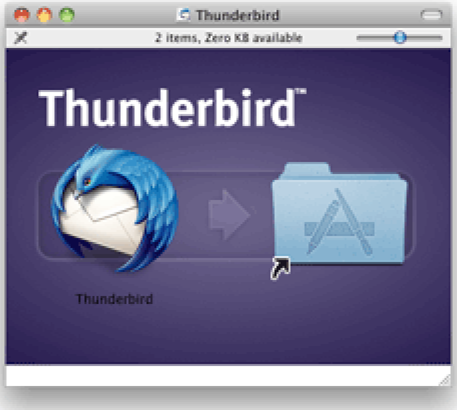


Thunderbird 3.1

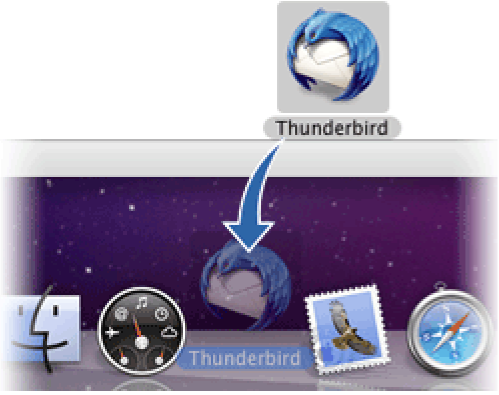
Now with tabs, better search, and email archiving.
It's easy to upgrade to Thunderbird 3.1

2. Download the Thunderbird disk image. When the download is complete, the disk image may automatically open and mount a new volume called *Thunderbird.*

   If the volume did not mount automatically, open the Download folder and double-click the disk image to mount it. A Finder window appears:

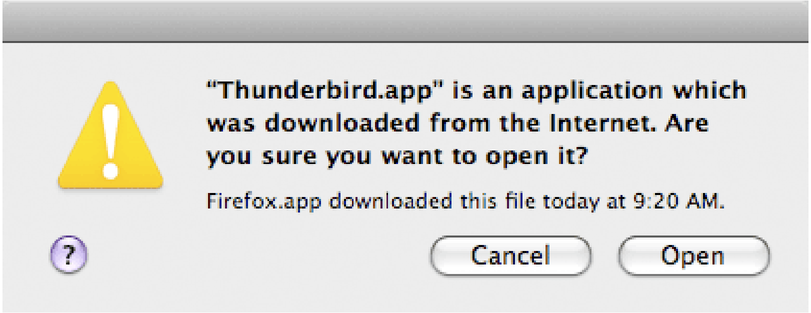


3. Drag the Thunderbird icon into your Applications folder. You've installed Thunderbird!
4. Optionally, drag the Thunderbird icon from the Applications folder into the Dock. Choosing the Thunderbird icon from the Dock lets you quickly open Thunderbird from there.



Note: When you run Thunderbird for the first time, newer versions of Mac OS X (10.5 or later) will warn you that the application Thunderbird.app was downloaded from the Internet.

If you downloaded Thunderbird from the Mozilla site, click the **Open** button.



"Thunderbird.app" is an application which was downloaded from the Internet. Are you sure you want to open it?

Firefox.app downloaded this file today at 9:20 AM.

Starting Thunderbird for the first time

After you have installed Thunderbird for the first time you will be guided through the configuration of your mail account. These settings are defined by your e-mail provider (your Internet Service Provider or web-based e-mail service provider). The next chapter describes how to set up your account and configure it for maximum security.

Setting up secure connections

There is a right (secure) way to configure your connection to your provider's mail servers and a wrong (insecure) way. The most fundamental aspect of e-mail security is the type of connection that you make to your e-mail provider's mail server.

Whenever possible, you should connect using the **SSL** (Secure Socket Layer) and **TLS** (Transport Layer Security) protocols. (**STARTTLS**, which is another option available when configuring an account, is a variation of SSL / TLS.) These protocols prevent your own system (beyond Thunderbird) and any points between your system and the mail server from intercepting and obtaining your password. SSL / TLS also prevent eavesdroppers from reading the content of your messages.

These protocols, however, only secure the connection between your computer and the mail server. They do not secure the information channel all the way to the message recipient. Once the mail servers forward the message for delivery, the message may be intercepted and read by points in between the mail server and the recipient.

This is where **PGP** (Pretty Good Privacy) comes in, which is described in the next chapter.

The first step in establishing e-mail security is a secure connection between your system and the mail servers. This chapter describes how to set up your e-mail account the right way.

Configuration requirements

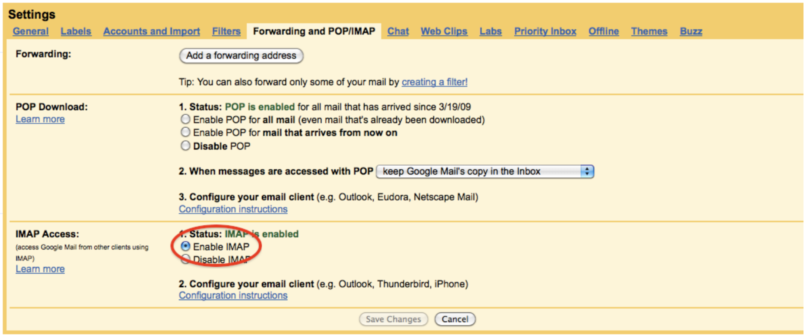
When you configure an account, Thunderbird attempts to determine (from the email account and the account details that you provide) the connection parameters to your email provider. While Thunderbird knows the connection parameters for many email providers, it does not know them all. If the parameters are not known to Thunderbird, you will need to provide the following information to configure your account:

- **Your username**
- **Your password**
- **Incoming server**: name (such as "imap.example.com"), protocol (POP or IMAP), port (by default, 110), and security protocol
- **Outgoing server**: name (such as "smtp.example.com"), port (by default, 25), and security protocol

You should have received this information from your hosting provider. Alternatively, you can usually find this information on the support pages on the website of your hosting provider. In our example we will be using the Gmail server configuration. You can use Thunderbird with your Gmail account. To do so, you must change a configuration setting in your account. If you are not using a Gmail account, skip the next section.

Preparing a Gmail account for use with Thunderbird

Log in to your Gmail account in your browser. Select **Settings** from options in the top right, then go to the tab **Forwarding and POP/IMAP**. Click **Enable IMAP** and then **Save Changes**.



Forwarding:

Tip: You can also forward only some of your mail by creating a filter!

POP Download:

1. Status: POP is enabled for all mail that has arrived since 3/19/09
○ Enable POP for **all mail** (even mail that's already been downloaded)
○ Enable POP for **mail that arrives from now on**
○ **Disable** POP

2. When messages are accessed with POP: keep Google Mail's copy in the Inbox

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)

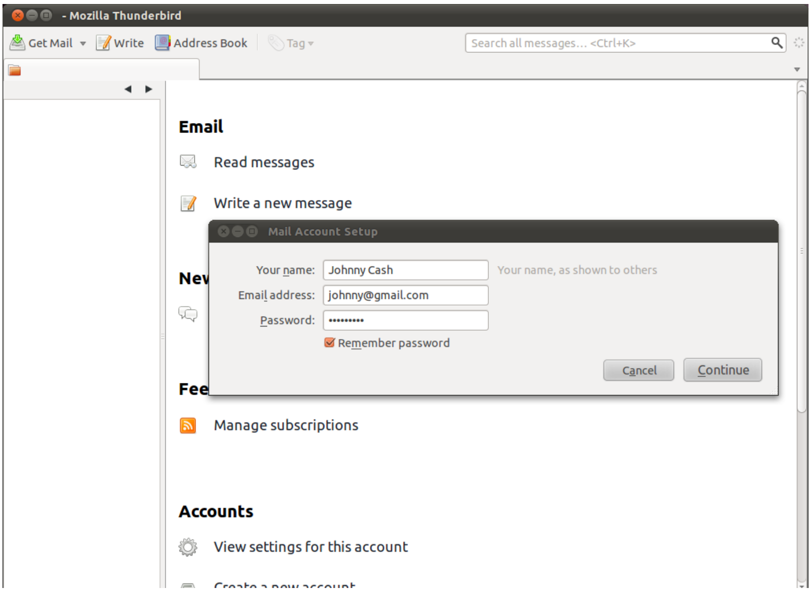
IMAP Access:
(access Google Mail from other clients using IMAP)

1. Status: IMAP is enabled
● Enable IMAP
○ Disable IMAP

2. Configure your email client (e.g. Outlook, Thunderbird, iPhone)

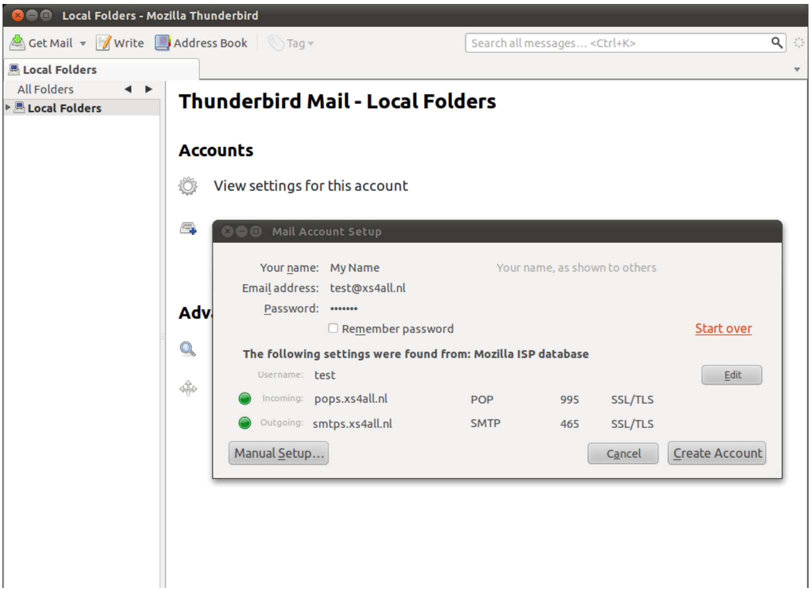
Configuring Thunderbird to use SSL/TLS

When you start up Thunderbird for the first time, you will enter a step-by-step configuration procedure for setting up your first account. (You can invoke the account setup interface any time by selecting **File | New | Mail Account**). On the first screen, you will be asked for your name, your email-address and your password. The value you enter for your name does not have to be your real name. It will be shown to the recipient of your messages. Enter the information and click **Continue**.



Your name: Johnny Cash — Your name, as shown to others
Email address: johnny@gmail.com
Password: •••••••••
☑ Remember password

On the next screen, Thunderbird will attempt to determine the server names based on your email address. This may take some time, and will only work if Thunderbird knows the settings for the mail servers for your email provider. In either case you will be presented with a window where you can modify the settings. In the example below, Thunderbird has detected the settings automatically. You can see the protocol at the right side of the server names. *This should be either **SSL/TLS** or **STARTTLS**. Otherwise your connection is insecure and you should attempt manual setup.*


Local Folders - Mozilla Thunderbird
Get Mail
Write
Address Book
Tag
Search all messages... <Ctrl+K>
Local Folders
All Folders
Local Folders
Thunderbird Mail - Local Folders
Accounts
View settings for this account
Adv
Mail Account Setup
Your name, as shown to others
Start over
Edit
Manual Setup...
Cancel
Create Account

Your name: My Name

Email address: test@xs4all.nl

Password: •••••••

□ Remember password

The following settings were found from: Mozilla ISP database

Username: test

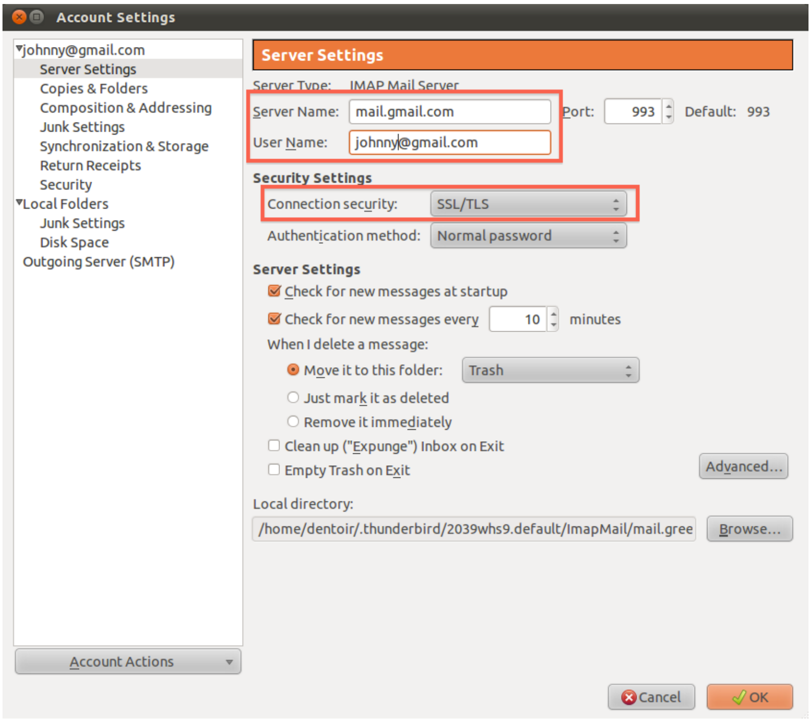
Incoming: pops.xs4all.nl POP 995 SSL/TLS

Outgoing: smtps.xs4all.nl SMTP 465 SSL/TLS

When you are finished, click **Create account**. If Thunderbird could not determine your server settings, click on **Manual setup** to configure the server names yourself.

Manual setup

Use the Account Settings interface to manually configure accounts in Thunderbird. The Account Settings dialog will automatically open if you select **Manual setup** in the configuration wizard. In this case we are only interested in the incoming and outgoing mail server names, and the protocol we use to connect with them. As you can see in the examples below, we enter the Gmail server names and we force them to use **TLS/SSL**, a secure method to connect to the servers.



Server Settings

Server Type: IMAP Mail Server

Server Name: mail.gmail.com Port: 993 Default: 993

User Name: johnny@gmail.com

Security Settings

Connection security: SSL/TLS

Authentication method: Normal password

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

When I delete a message:

● Move it to this folder: Trash

○ Just mark it as deleted

○ Remove it immediately

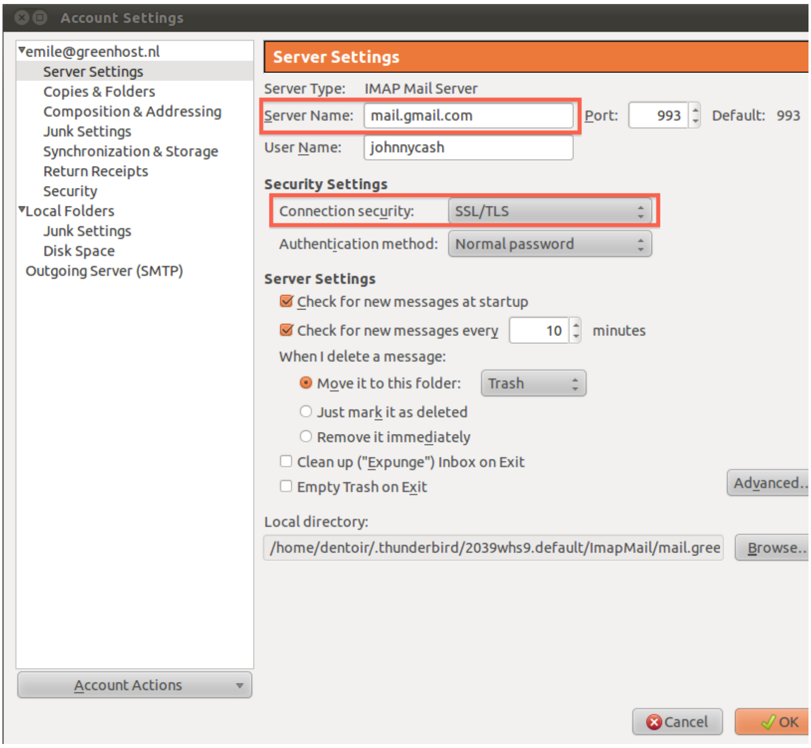
□ Clean up ("Expunge") Inbox on Exit

□ Empty Trash on Exit

Local directory:

/home/dentoir/.thunderbird/2039whs9.default/ImapMail/mail.gree

Under 'Server Settings', we will find only the incoming (**IMAP**) server and its settings for that specific account.



Server Settings

Server Type: IMAP Mail Server

Server Name: mail.gmail.com Port: 993 Default: 993

User Name: johnnycash

Security Settings

Connection security: SSL/TLS

Authentication method: Normal password

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

When I delete a message:

● Move it to this folder: Trash

○ Just mark it as deleted

○ Remove it immediately

□ Clean up ("Expunge") Inbox on Exit

□ Empty Trash on Exit

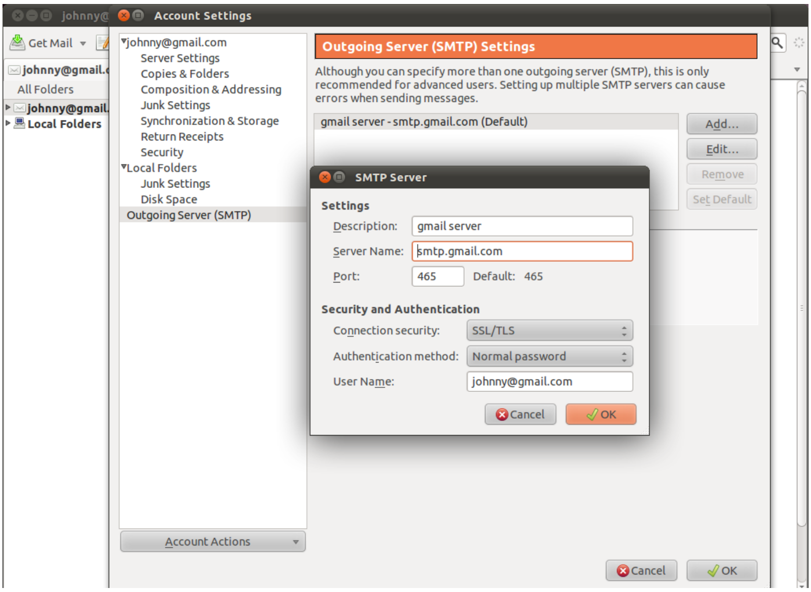
Local directory:

/home/dentoir/.thunderbird/2039whs9.default/ImapMail/mail.gree

After **Server Name** enter the name of the IMAP server, in this case mail.gmail.com

As you can see we have selected '**SSL/TLS**' *under the connection security setting. This enforces encryption.* Do not be scared by the authentication method **Normal password**. The password will be automatically encrypted due to our secured connections to the server.

Finally, configure the outgoing server for the account. Click on **Outgoing Server (SMTP)** in the left panel.



Outgoing Server (SMTP) Settings

Although you can specify more than one outgoing server (SMTP), this is only recommended for advanced users. Setting up multiple SMTP servers can cause errors when sending messages.

gmail server - smtp.gmail.com (Default)

SMTP Server

Settings

Description: gmail server

Server Name: smtp.gmail.com

Port: 465 Default: 465

Security and Authentication

Connection security: SSL/TLS

Authentication method: Normal password

User Name: johnny@gmail.com

Again, we have selected **SSL/TLS** under **Connection security**. The port will default to 465 and this should generally not have to be changed.

Finishing the setup, different encryption methods

Test your Thunderbird setup by trying to send and receive mails. Some email hosting providers may not support the SSL/TLS protocol, which is the preferred choice. You will get an error message saying the authentication protocol is not supported by the server. You may then switch to using STARTTLS instead. In the above two screens, select 'STARTTLS' under 'Connection security'. If this method also fails, contact your email hosting provider and ask them if they provide another way to securely connect to their servers. If they do not allow you to securely connect to their servers, then you should complain and seriously consider switching to a different provider.

Returning to the configuration screens

At any time you can reconfigure your email accounts by going to the Thunderbird menu bar and clicking **Edit** | **Account Settings** (Linux), **Tools** | **Account Settings** (Windows and Mac OS X).

Some Additional Security Settings

Thunderbird provides additional security measures to protect you from junk mail, identity theft, viruses (with the help of your anti-virus software, of course), intellectual property theft, and malicious web sites.

We will look at the following Thunderbird security features. First a little background on why you need to consider some of these measures:

- **Adaptive junk mail controls**
  Adaptive junk mail controls allow you to train Thunderbird to identify junk email (SPAM) and remove it from your inbox. You can also mark messages as junk mail manually if your email provider's system misses the junk mail and lets it go through.
- **Integration with anti-virus software**
  If your anti-virus software supports Thunderbird, you can use that software to quarantine messages that contain viruses or other malicious content. If you're wondering what anti-virus software works with Thunderbird, you can find a list here: http://kb.mozillazine.org/Antivirus_software.
- **Master password**
  For your convenience, you can have Thunderbird remember each of your individual passwords of your e-mail accounts. You can specify a master password that you enter each time you start Thunderbird. This will enable Thunderbird to open all your email accounts with your saved passwords.
- **Restrictions on cookies**
  Some blogs and websites attempt to send cookies (a piece of text that stores information from Web sites on your computer) with their RSS feeds. These cookies are often used by content providers to provide targeted advertising. Thunderbird rejects cookies by default, but you can configure Thunderbird to accept some or all cookies.

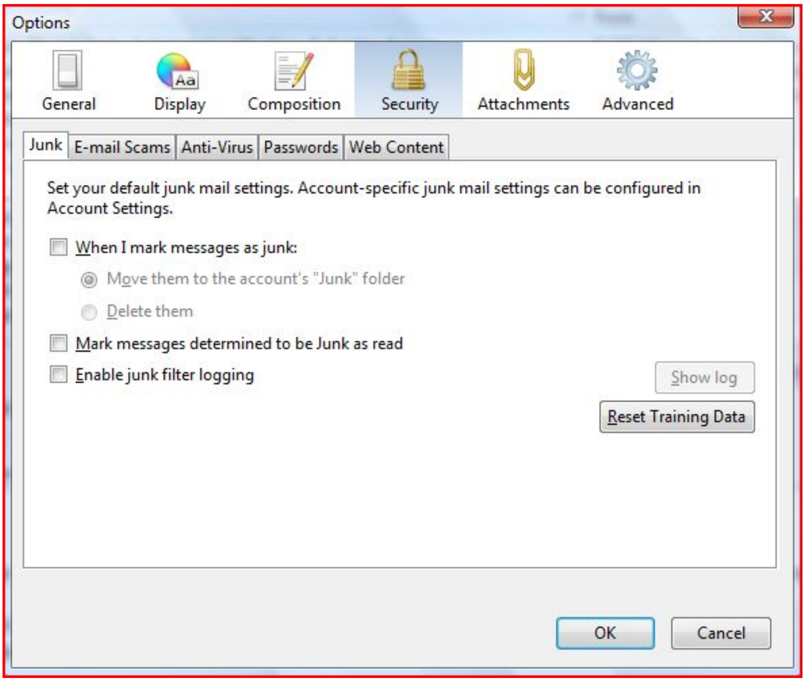
In the Security Preferences section of Thunderbird's Options/Preferences dialog box you can set up the preferences for these features.

- In Windows and Mac OS X, go to the 'Tools' menu and click 'Options'.
- On Ubuntu or other versions of Linux, go to the 'Edit' menu and click 'Pre-

ferences'.

JUNK MAIL SETTINGS

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Junk' tab.



Set your default junk mail settings. Account-specific junk mail settings can be configured in Account Settings.

□ When I mark messages as junk:

● Move them to the account's "Junk" folder

○ Delete them

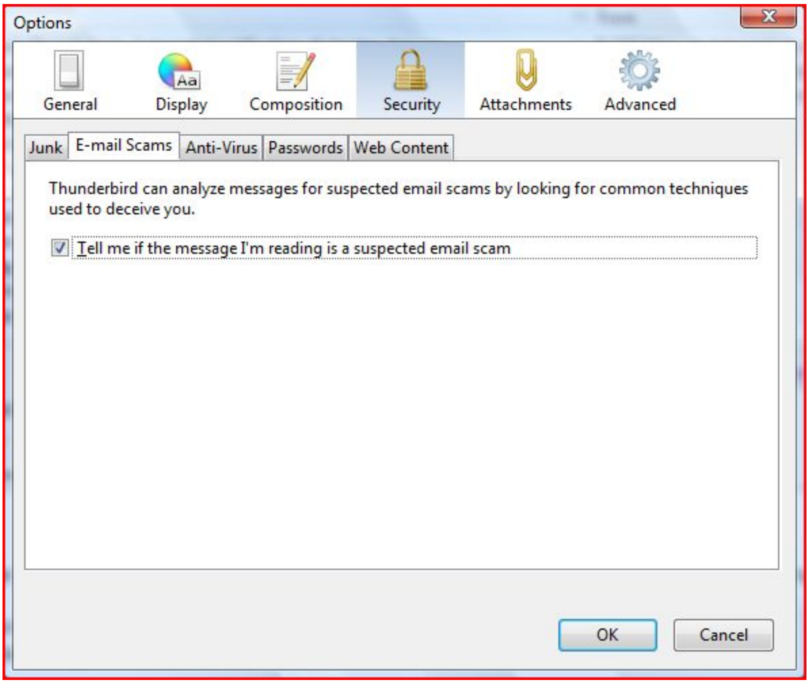
□ Mark messages determined to be Junk as read

□ Enable junk filter logging

2. Do the following:
   - To tell Thunderbird that it should handle messages marked as junk, select the check box labelled 'When I mark message as junk'.
   - To have Thunderbird move these messages to a junk folder, select the 'Move them to account's 'Junk' folder' radio button.
   - To have Thunderbird delete junk mail upon receiving it, select the 'Delete them' radio button.
3. Thunderbird will mark junk message as read if you select the check box labeled 'Mark messages determined to be Junk as read'.
4. If you want to keep a log of junk mail received, select the 'Enable junk filter logging' check box.
5. Click the 'OK' button to close the 'Options/Preferences' dialog box.

Scam detection and warning system

1. In the Preferences/Options dialog box, click 'Security' and then click the 'E-mail Scams' tab.



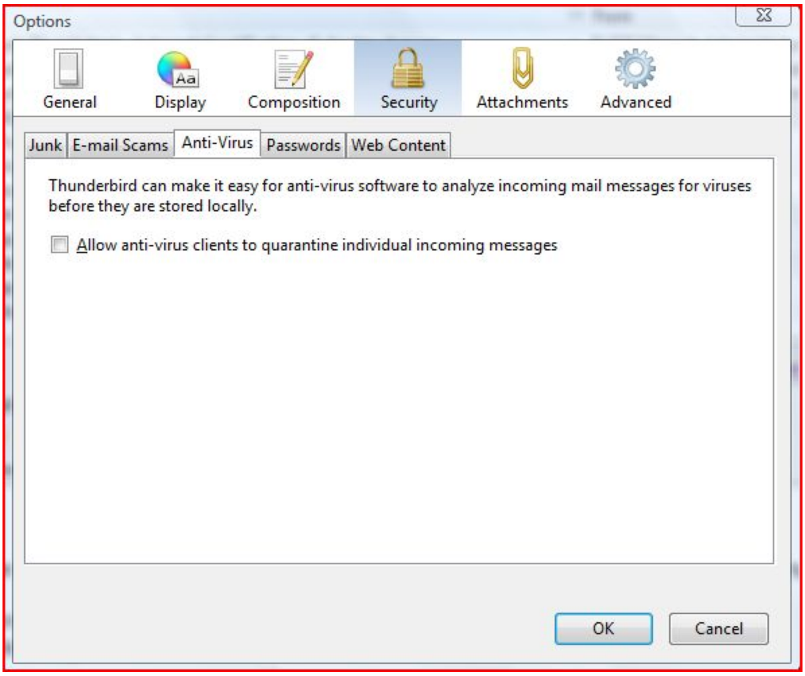
Thunderbird can analyze messages for suspected email scams by looking for common techniques used to deceive you.

☑ Tell me if the message I'm reading is a suspected email scam

2. To have Thunderbird warn you about possible email scams, select the check box labelled 'Tell me if the message I'm read is a suspected email scam'. To turn off this feature, deselect this check box.
3. Click the 'OK' button to close the 'Options/Preferences' dialog box.

Anti-virus integration

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Anti-Virus' tab.



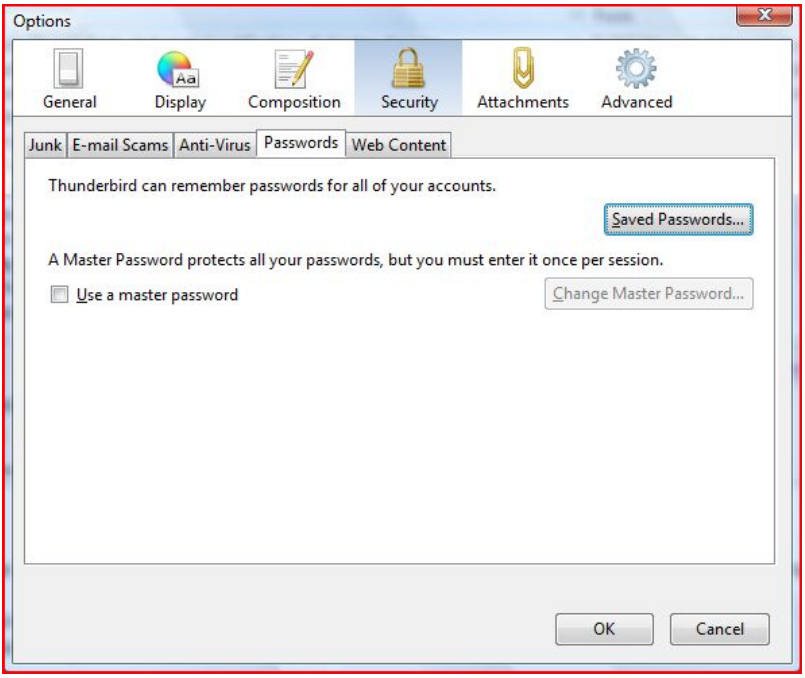
Thunderbird can make it easy for anti-virus software to analyze incoming mail messages for viruses before they are stored locally.

□ Allow anti-virus clients to quarantine individual incoming messages

2. To turn on anti-virus integration, select the check box labeled 'Allow anti-virus clients to quarantine individual incoming messages'. To turn off this feature, deselect this check box.
3. Click the 'OK' button to close the 'Options/Preferences' dialog box.

Set a master password

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Passwords' tab.



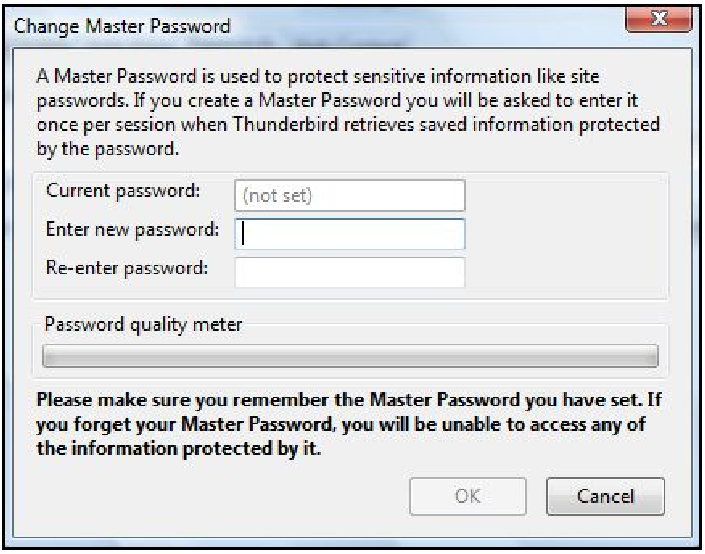
Options

Thunderbird can remember passwords for all of your accounts.

A Master Password protects all your passwords, but you must enter it once per session.

□ Use a master password

2. Select the check box labeled 'Use a master password'.
3. Enter your password into the 'Enter new password' and 'Re-enter password' fields.



Change Master Password

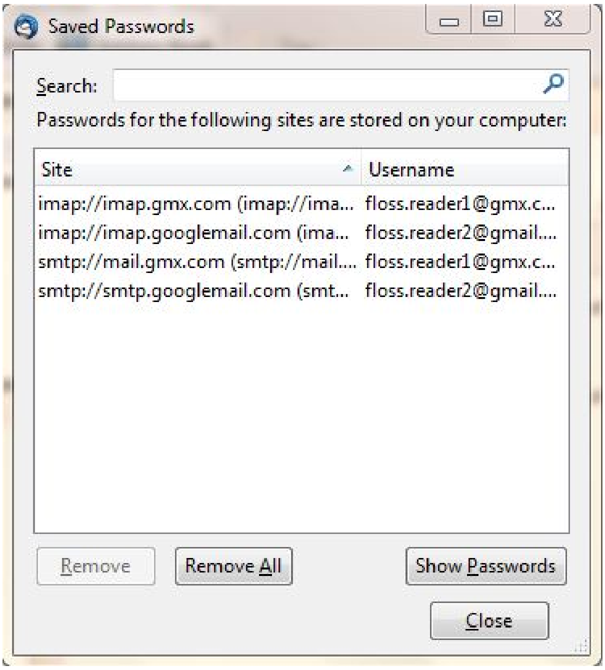
A Master Password is used to protect sensitive information like site passwords. If you create a Master Password you will be asked to enter it once per session when Thunderbird retrieves saved information protected by the password.

Current password: (not set)
Enter new password:
Re-enter password:

Password quality meter

Please make sure you remember the Master Password you have set. If you forget your Master Password, you will be unable to access any of the information protected by it.

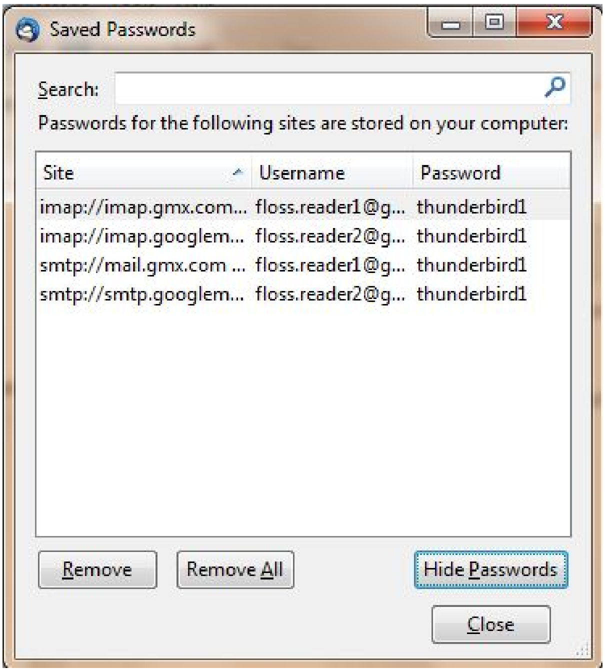
4. Click the 'OK' button to close the Change Master Password dialog box.
5. If you want to see the passwords that you have saved in Thunderbird, click the 'Saved Passwords' button. This will open the 'Saved Passwords' dialog box.



Passwords for the following sites are stored on your computer:

Site	Username
imap://imap.gmx.com (imap://ima...	floss.reader1@gmx.c...
imap://imap.googlemail.com (ima...	floss.reader2@gmail....
smtp://mail.gmx.com (smtp://mail....	floss.reader1@gmx.c...
smtp://smtp.googlemail.com (smt...	floss.reader2@gmail....

6. To see the passwords, click the 'Show Passwords' button.



Passwords for the following sites are stored on your computer:

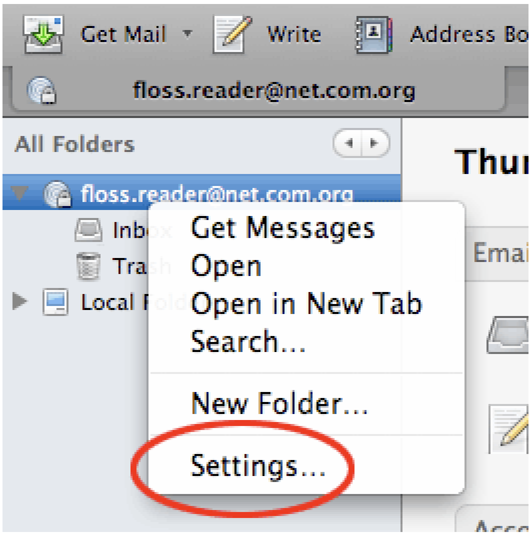
Site	Username	Password
imap://imap.gmx.com...	floss.reader1@g...	thunderbird1
imap://imap.googlem...	floss.reader2@g...	thunderbird1
smtp://mail.gmx.com ...	floss.reader1@g...	thunderbird1
smtp://smtp.googlem...	floss.reader2@g...	thunderbird1

7. Click the 'Close' button to close 'Saved Passwords' dialog box.
8. Click the 'OK' button to close the 'Options/Preferences' dialog box.

Adaptive junk mail controls

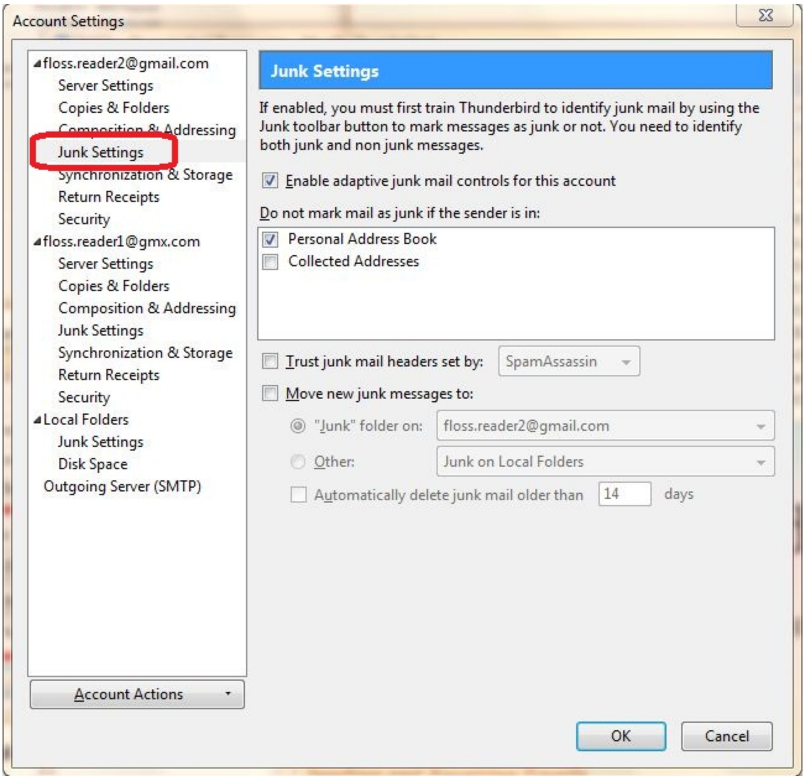
You need to first open Account Settings window. Note that settings configured in the Account Settings window apply only to the account that you select in the Folders pane. You must configure local folders separately.

1. In the Folders pane right-click on an account name and select 'Settings'.



2. In Windows or Mac go to the 'Tools' menu and select 'Account Settings'. In Linux, go to the 'Edit menu' and select 'Account Settings'.

1. To set adaptive junk mail controls for a specific account, pick an account and click 'Junk Settings'.



Junk Settings

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages.

☑ Enable adaptive junk mail controls for this account

Do not mark mail as junk if the sender is in:

☑ Personal Address Book
□ Collected Addresses

□ Trust junk mail headers set by: SpamAssassin

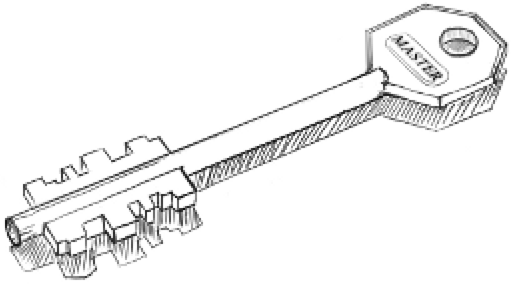
□ Move new junk messages to:

● "Junk" folder on: floss.reader2@gmail.com
○ Other: Junk on Local Folders

□ Automatically delete junk mail older than 14 days

2. To turn on the controls, select the check box labeled 'Enable adaptive junk mail controls for this account'. To turn them off, deselect this check box.
3. If you want the controls to ignore mail from senders in your Address Book, select the check boxes next to any of the listed address books.
4. To use a mail filter such as SpamAssassin or SpamPal, select the check box labelled 'Trust junk mail headers sent by:' and pick a filter from the menu.
5. Select the check box labeled 'Move new junk messages to' if you want to move junk mail to a specified folder. Then select the destination folder to be either at your email provider or a local folder on your computer.
6. Select the 'Automatically delete junk mail other 14 days' check box to have Thunderbird regularly remove junk mail. To change the time period for this process, enter a different number (in days) in the text box.
7. Click 'OK' to save your changes.

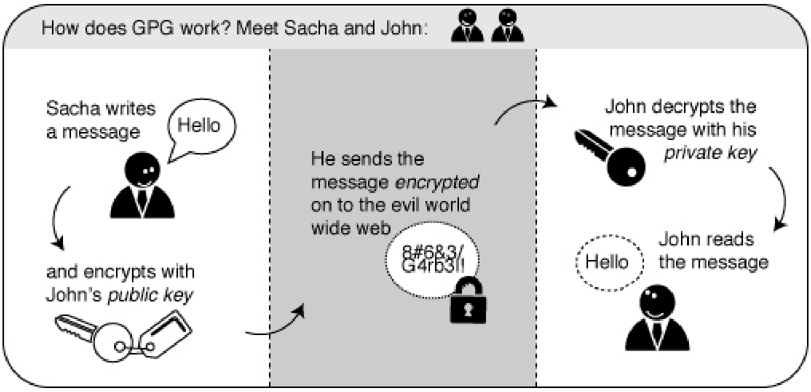
Email Encryption



INTRODUCING MAIL ENCRYPTION (PGP)

This chapter will introduce you to some basic concepts behind mail encryption. It is important to read to get some feeling of how mail encryption actually works and what its caveats and limitations are. **PGP** (Pretty Good Privacy) is the protocol we shall use for e-mail encryption. This protocol allows us to digitally sign and encrypt mail messages. It works on an end-to-end basis: messages will be encrypted on your own computer and will only be decrypted by the recipient of the message. There is no possibility for a 'man-in-the-middle' to decipher the contents of your encrypted message. This *excludes* the subject lines and the 'from' and 'to' addresses, which unfortunately are not encrypted in this protocol.

After having introduced these basic concepts, the next chapters will give you a hands-on guide to install the necessary tools on your operating system and get encryption up and running. We will focus on using Enigmail which is an extension for Thunderbird that helps you manage PGP encryption for your email. The installation process for Enigmail / PGP is different for Mac OSX, Windows and Ubuntu so please see the appropriate chapters in this section for instructions.


How does GPG work? Meet Sacha and John:
Sacha writes a message
Hello
and encrypts with John's *public key*
He sends the message *encrypted* on to the evil world wide web
8#6&3/ G4rb3!l
John decrypts the message with his *private key*
Hello
John reads the message

Using a key-pair to encrypt your mail

A crucial concept in mail encryption is the usage of so-called *key-pairs*. A key-pair is just two separate files sitting on your harddisk or USB stick. Whenever you want to encrypt mails for a certain mail-account, you will need to have these files available to yourself in some form. If they are sitting at home on your computer, you will not be able to decrypt mail at the office. Putting them on a USB stick should provide a solution to this problem.

A key-pair consists of the two different keys: a public key and a secret key.

The public key: you can give this key to other people, so they can send you encrypted mails. This file does not have to be kept secret.

The secret key: this basically is your secret file to decrypt emails people send to you. It should *never* be given to someone else.

Sending encrypted mails to other people: you need their public key

I have five colleagues at work and I want to send encrypted mails to them. I need to have public keys for each of their addresses. They can send me these keys using ordinary mail, or they can give them to me in person, or put them on a USB stick, or they can have their keys on a website. It doesn't matter, as long as I can trust those keys really belong to the person I want to correspond with. My software puts the keys on my `keyring', so my mail application knows how to send them encrypted mails.

Receiving encrypted mails from other people: they need *my* public key

For my five (or thirty) colleagues to be able to send *me* encrypted mails, the process goes the other way around. I need to distribute my public key to each of them.

Conclusion: encryption requires public key distribution!

All the people in a network of friends or colleagues wanting to send each other encrypted emails, need to distribute their public keys to each other, while keeping their secret keys a closely guarded secret. The software described in this chapter will help you do this key management.

Installing PGP on Windows

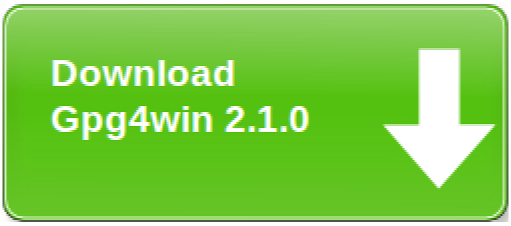
To complicate matters a little - PGP is the protocol used for encrypting e-mail by various softwares. To get PGP to work with Thunderbird we need to install GPG - a free software implementation of PGP *and* Enigmail - an extension of Thunderbird that allows you to use GPG... Confused?! Don't worry about it, all you have to know is how to encrypt your email with PGP and you need to install *both* GPG and Enigmail. Here is how to do it...

Installing PGP (GPG) on Microsoft Windows

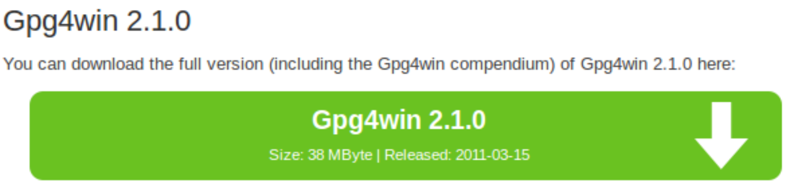
The GNU Privacy Guard (GnuPG) is software which is required to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption.

Head to the website of the Gpg4win project. Go to http://gpg4win.org/

On the left side of the website, you will find a 'Download' link. Click on it.



This will take you to a page where you can download the Gpg4Win. Click on the button which offers you the latest stable version (not beta) of Gpg4Win.


Gpg4win 2.1.0

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.1.0 here:

This will download you an .exe file. Depending on your browser, you may have to double-click on this downloaded file (which will be called something like gpg4qin-2.1.0.exe) before something happens. Windows will ask you if you are sure you want to install this program. Answer yes.

Then complete the installation by agreeing to the license, choosing appropriate language and accepting the default options by clicking 'Next', unless you have a particular reason not to.

The installer will ask you where to put the application on your computer. The default setting should be fine but make a note of it as we may need this later. Click on 'Next' when you agree.

Installing with the Enigmail extension

After you have successfully installed the **PGP** software as we described above you are now ready to install the **Enigmail** add-on.

Enigmail is a Thunderbird add-on that lets you protect the privacy of your email conversations. Enigmail is simply an interface that lets you use PGP encryption from within Thunderbird.

Enigmail is based on public-key cryptography. In this method, each individual must generate her/his own personal key pair. The first key is known as the private key. It is protected by a password or passphrase, guarded and never shared with anyone.

The second key is known as the public key. This key can be shared with any of your correspondents. Once you have a correspondent's public key you can begin sending encrypted e-mails to this person. Only she will be able to decrypt and read your emails, because she is the only person who has access to the matching private key.

Similarly, if you send a copy of your own public key to your e-mail contacts and keep the matching private key secret, only you will be able to read encrypted messages from those contacts.

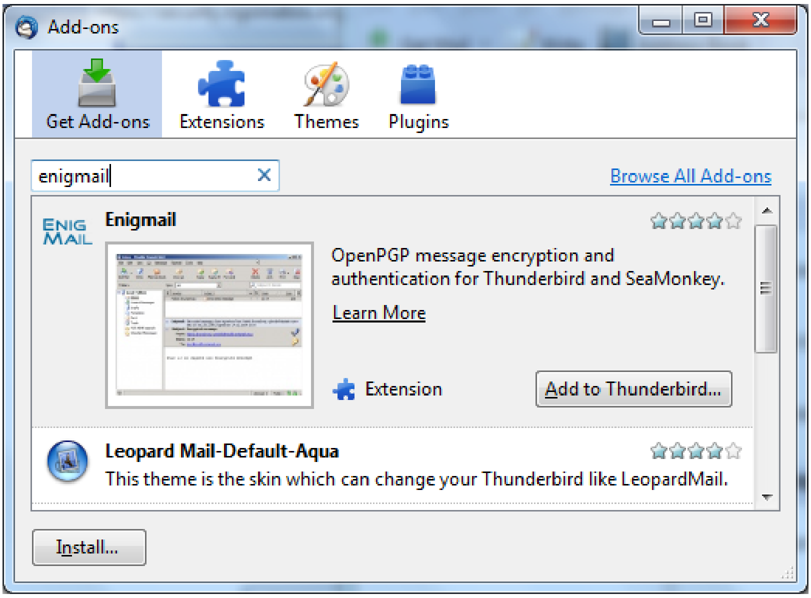
Enigmail also lets you attach digital signatures to your messages. The recipient of your message who has a genuine copy of your public key will be able to verify that the e-mail comes from you, and that its content was not tampered with on the way. Similarly, if you have a correspondent's public key, you can verify the digital signatures on her messages.

Installation steps

To begin installing **Enigmail**, perform the following steps:

Step 1. Open Thunderbird, then **Select Tools** > **Add-ons** to activate the *Add-ons* window; the *Add-ons* window will appear with the default *Get Add-ons* pane enabled.

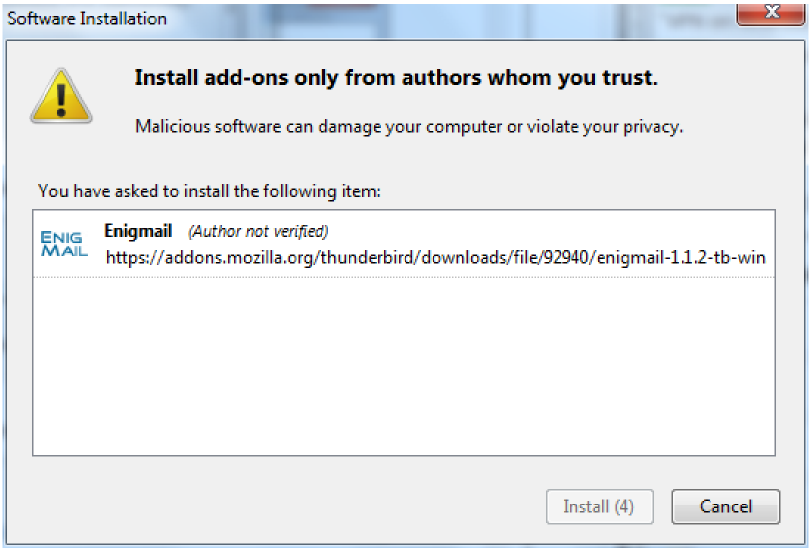
Step 2. Enter enigmail in the search bar, like below, and click on the search icon.



Add-ons
Get Add-ons
Extensions
Themes
Plugins
enigmail
Browse All Add-ons
ENIG MAIL
Enigmail
OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.
Learn More
Extension
Add to Thunderbird...
Leopard Mail-Default-Aqua
This theme is the skin which can change your Thunderbird like LeopardMail.
Install...

Step 3. Simply click on the 'Add to Thunderbird' button to start the installation.

Step 4. Thunderbird will ask you if you are certain you want to install this add-on. We trust this application so we should click on the 'Install now' button.



Software Installation

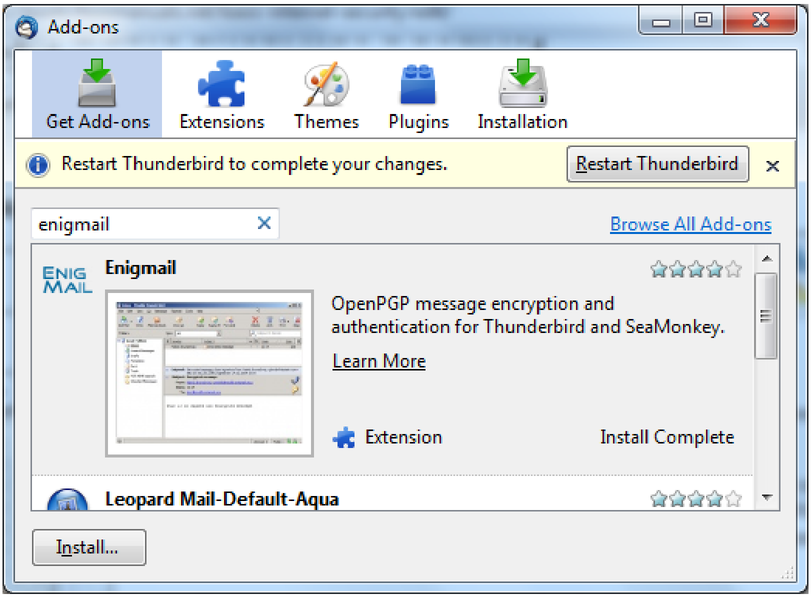
Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Enigmail *(Author not verified)*
https://addons.mozilla.org/thunderbird/downloads/file/92940/enigmail-1.1.2-tb-win

Step 5. After some time the installation should be completed and the following window should appear. Please click on the 'Restart Thunderbird' button.



Add-ons

Restart Thunderbird to complete your changes.

enigmail

Enigmail

OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.

Learn More

Extension Install Complete

Leopard Mail-Default-Aqua

Installing PGP on OSX

The GNU Privacy Guard (GnuPG) is software which enables you to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption. This chapter covers the installation steps required to install GnuPG on Mac OSX.

Getting started

For this chapter we assume you have the latest version of:

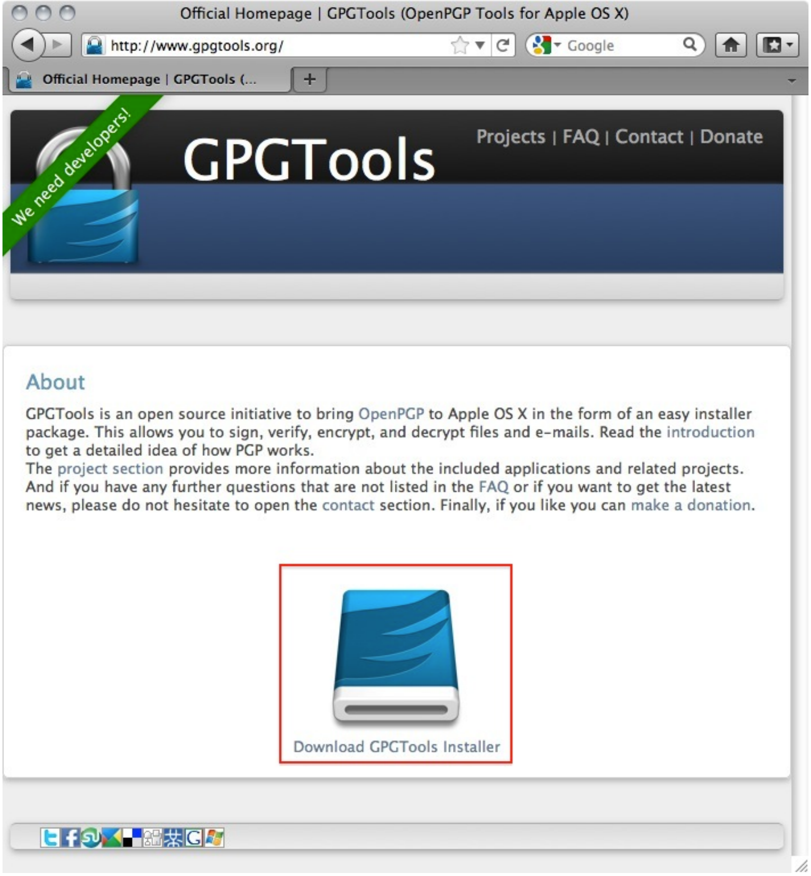
- OSX installed (10.6.7)
- Thunderbird (3.1.10)

> **Note on OSX Mail**: It is possible to use PGP with the build-in mail program of OSX. But we do not recommend this because this option relies on a hack of the program which is neither open or supported by its developer and breaks with every update of the mail program. So unless you really have no other option we advice you to switch to Mozilla Thunderbird as your default mail program if you want to use PGP.

Downloading and installing the Software

For OSX there is a bundle available which will install everything you need in one installation. You can get it by directing your browser to http://www.gpgtools.org/ and clicking on the big blue disk with "Download GPGTools Installer" written under it. It will redirect you to another page on http://www.gpgtools.org/installer/index.html where you can actually download the software.

(*nb. We are using the latest version Firefox for this manual, so the screens might look a little bit different if you are using a different browser*)

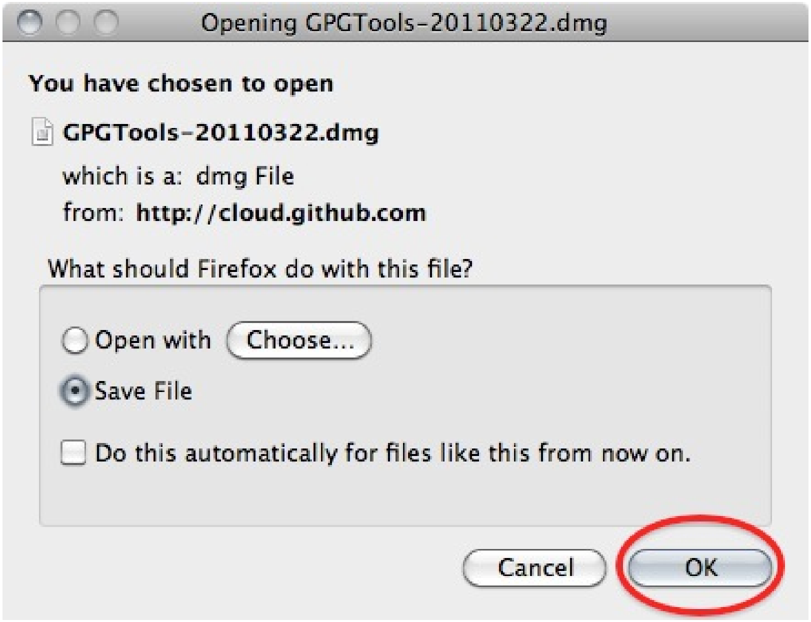


Official Homepage | GPGTools (OpenPGP Tools for Apple OS X)
http://www.gpgtools.org/
Google
Official Homepage | GPGTools (...
We need developers!
GPGTools
Projects | FAQ | Contact | Donate
Download GPGTools Installer

About

GPGTools is an open source initiative to bring OpenPGP to Apple OS X in the form of an easy installer package. This allows you to sign, verify, encrypt, and decrypt files and e-mails. Read the introduction to get a detailed idea of how PGP works.
The project section provides more information about the included applications and related projects. And if you have any further questions that are not listed in the FAQ or if you want to get the latest news, please do not hesitate to open the contact section. Finally, if you like you can make a donation.

2. Download the software by choosing 'Save File' and clicking 'OK' in the dialogue.



Opening GPGTools-20110322.dmg

You have chosen to open

GPGTools-20110322.dmg

which is a: dmg File

from: **http://cloud.github.com**

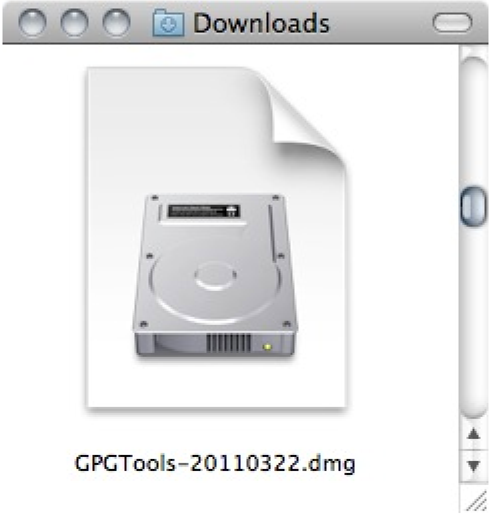
What should Firefox do with this file?

○ Open with

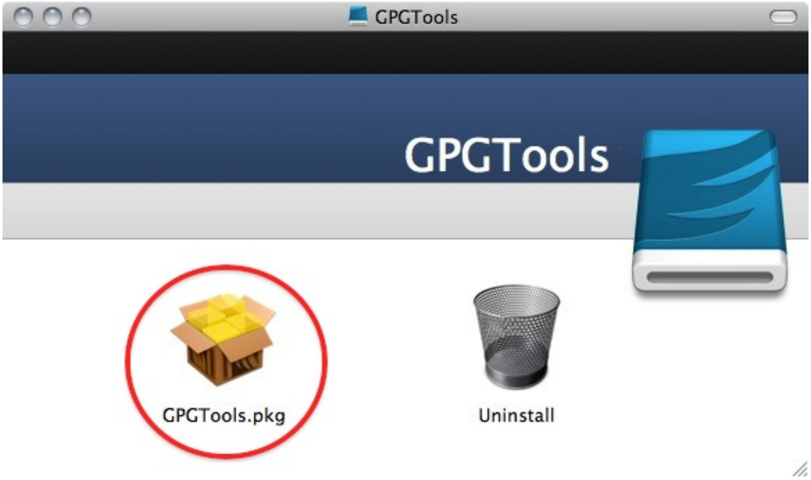
● Save File

□ Do this automatically for files like this from now on.

3. Navigate to the folder where you normally store your downloads (Mostly the desktop or the downloads folder surprisingly) en double click the '.DMG' file to open the virtual disk containing the installer.

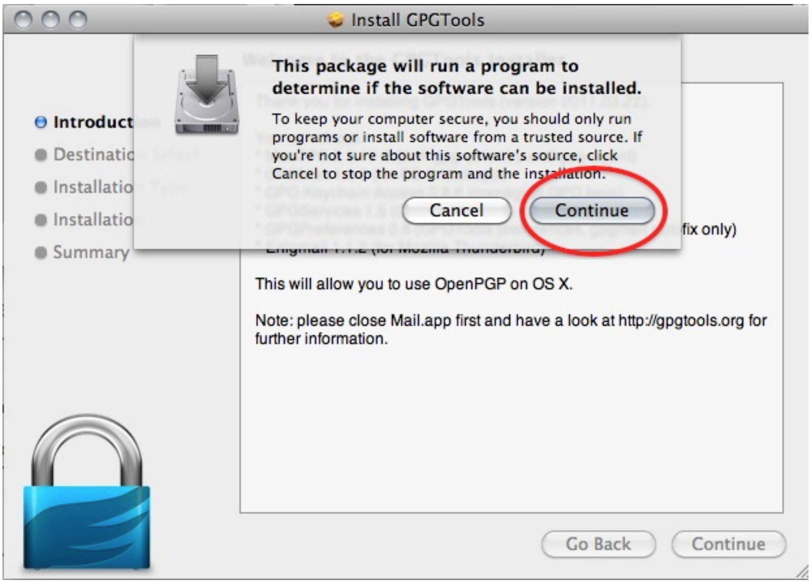


4. Open the installer by double-clicking on the icon.



5. The program will check your computer to see if it can run on the computer.

(Note, if you're Mac is bought before 2006 it will not have an intel processor required to run this software and the installation will fail. Sadly it is beyond the scope op this manual to also take into account computers over five year old)



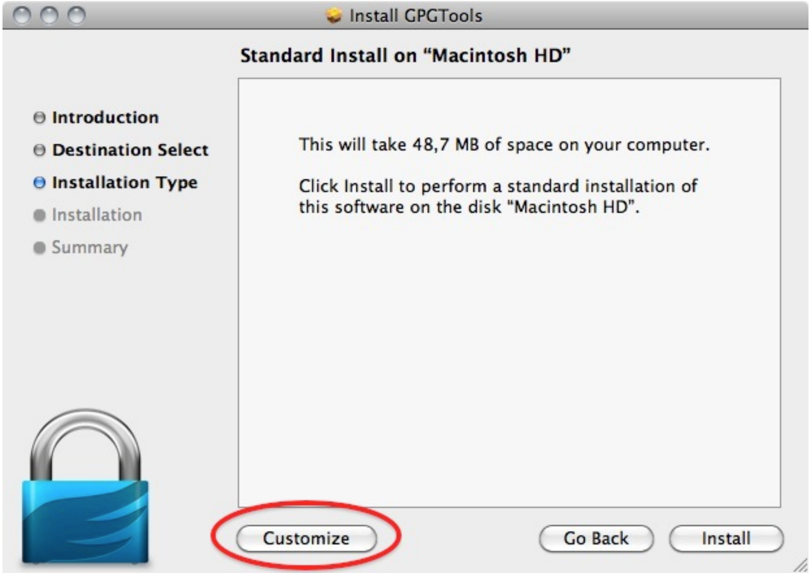
This package will run a program to determine if the software can be installed.

To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.

This will allow you to use OpenPGP on OS X.

Note: please close Mail.app first and have a look at http://gpgtools.org for further information.

You will be guided by the program through the next steps like accepting the license agreement. But stop pressing all the OK's and Agrees as soon as you come to the 'Installation Type' screen:

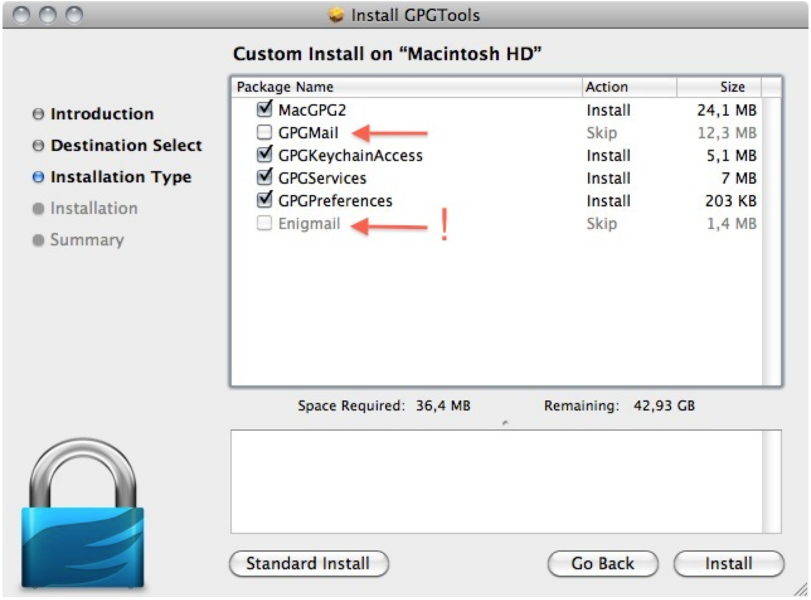


Standard Install on "Macintosh HD"

This will take 48,7 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

6. Clicking 'Customize' will open this screen where you several options of programs and software to install. You can click on each one of them to get a little bit of information on what is is, what it does and why you might need it.



Custom Install on "Macintosh HD"

Package Name	Action	Size
☑ MacGPG2	Install	24,1 MB
□ GPGMail	Skip	12,3 MB
☑ GPGKeychainAccess	Install	5,1 MB
☑ GPGServices	Install	7 MB
☑ GPGPreferences	Install	203 KB
□ Enigmail	Skip	1,4 MB

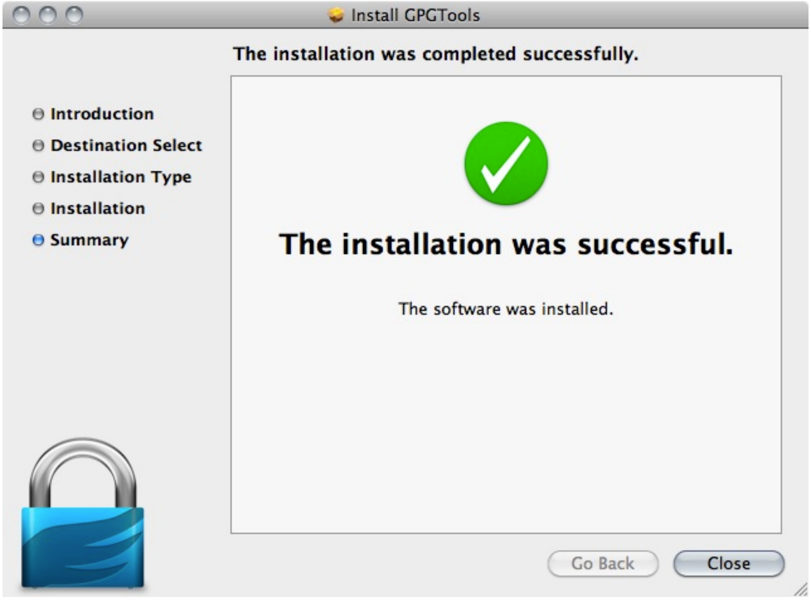
Space Required: 36,4 MB   Remaining: 42,93 GB

As said in the intro; we advise against using Apple Mail in combination with PGP. Therefore you won't be needing 'GPGMail', as this enables PGP on Apple Mail, and you can uncheck it.

'**Enigmail**' on the other hand is very important as it is the component that will enable Thunderbird to use PGP. In the screen shot here it is greyed out as the installer wasn't able to identify my installation of Thunderbird. Since this seems to be a bug. You can also install Enigmail from within Thunderbird as is explained in another chapter.

If the option is not greyed out in your installation, you should tick it.

After you checked all the components you want to install click 'Install' to proceed. The installer will ask you for your password and after you enter that the installation will run and complete; Hooray!



Install GPGTools

The installation was completed successfully.

The installation was successful.

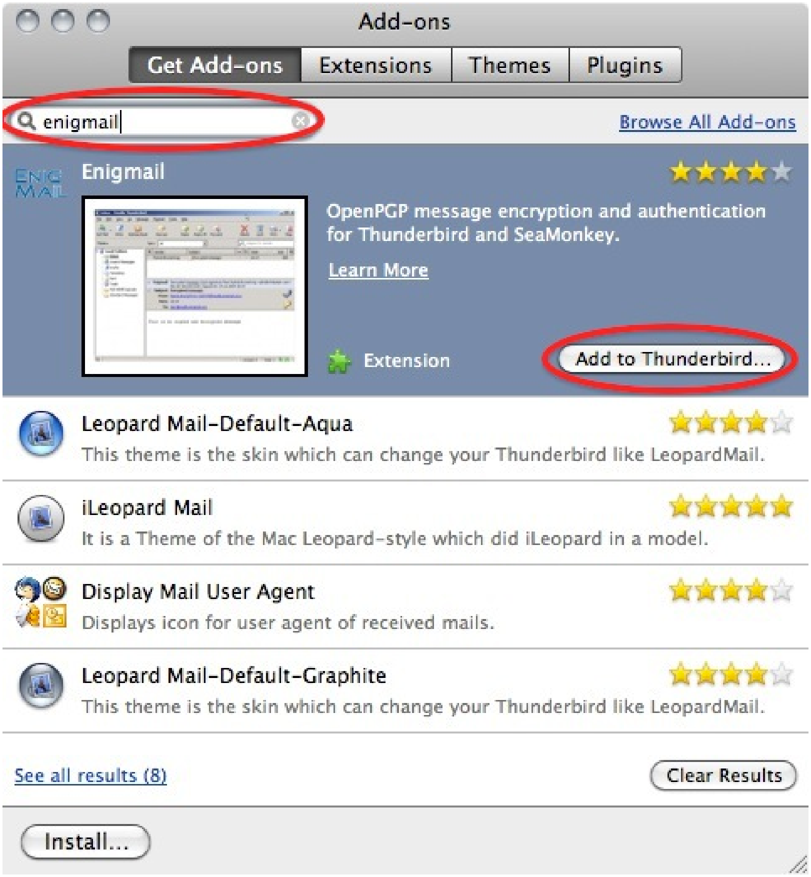
The software was installed.

Installing up Engimail

Step 1. **Open Thunderbird**, then **Select Tools** > **Add-ons** to activate the *Add-ons* window; the *Add-ons* window will appear with the default *Get Add-ons* pane enabled.

In the Add-On window, you can search for 'Enigmail' and install the extension by clicking 'Add to Thunderbird ...'

2. After you open the Add-On window, you can search for 'Enigmail' and install the extension by clicking 'Add to Thunderbird ...'



Enigmail

OpenPGP message encryption and authentication for Thunderbird and SeaMonkey.

Leopard Mail-Default-Aqua

This theme is the skin which can change your Thunderbird like LeopardMail.

iLeopard Mail

It is a Theme of the Mac Leopard-style which did iLeopard in a model.

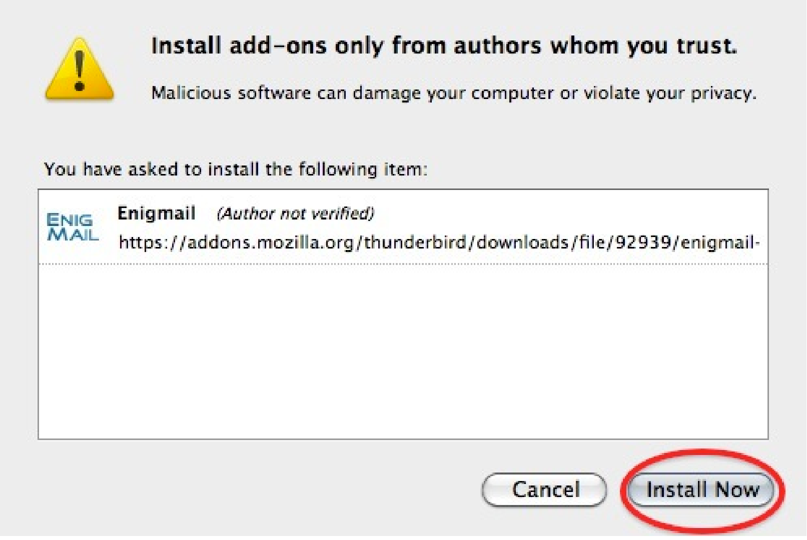
Display Mail User Agent

Displays icon for user agent of received mails.

Leopard Mail-Default-Graphite

This theme is the skin which can change your Thunderbird like LeopardMail.

3. Click on 'Install Now' to download and install the extension.



Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Enigmail *(Author not verified)*
https://addons.mozilla.org/thunderbird/downloads/file/92939/enigmail-

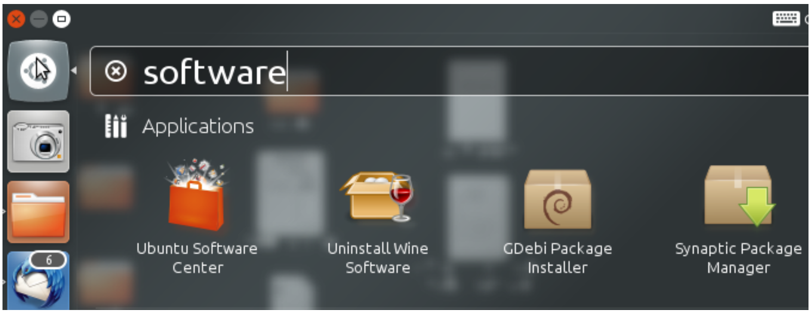
Be aware that you will have to restart Thunderbird to use the func-

tionality of this extension!

Now that you have successfully downloaded and installed Enigmail and PGP you can go on to the Chapter that deals with setting up the software for use.

Installing PGP on Ubuntu

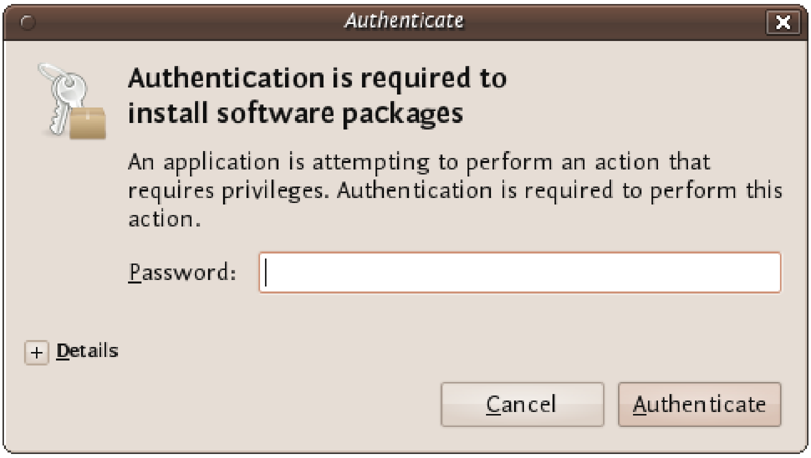
We will use the Ubuntu Software Centre for installing PGP (Enigmail and accessories). First open the Ubuntu Software Center through the Unity menu by typing 'software' into the Unity search area



Click on the 'Ubuntu Software Center'.

Type into the search field 'Enigmail' and search results should be returned automatically:

Highlight the Enigmail item (it should be highlighted by default) and click 'Install' and you will be asked to authenticate the installation process.



Authenticate

Authentication is required to install software packages

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

Enter your password and click 'Authenticate'. The installation process will begin.

When the process is completed you get very little feedback from Ubuntu. The progress bar at the top left disappears. The 'In Progress' text on the right also disappears. Enigmail should now be installed.

With the growing usage of mobile phones for e-mail, it's interesting to be able to use GPG also on your mobile. This way you can still read the messages sent to you in GPG on your phone and not only on your computer.

Installing GPG on Android

Install the *Android Privacy Guard* (APG) and *K-9 Mail* applications to your Android device from the Google Play Store or another trusted source.

1. Generate a new private key that uses DSA-Elgamal with your PC's GPG installation (You can only create keys with up to 1024bit key length on Android itself).
2. Copy the private key to your Android device.
3. Import the private key to APG. You may wish to have APG automatically delete the plaintext copy of your private key from your Android device's filesystem.
4. Set-up your e-mail accounts in *K-9 Mail*.
5. In the settings for each account, under *Cryptography*, make sure that *K-9 Mail* knows to use APG. You can also find options here to make *K-9 Mail* automatically sign your messages and/or encrypt them if APG can find a public key for the recipient(s).
6. Try it out.

APG

This is a small tool which makes GPG encryption possible on the phone. You can use APG to manage your private and public keys. The options in the application are quite straightforward if you are a little knowledge of GPG in general.

Management of keys is not very well implemented yet. The best way is to manually copy all your public keys to the SD card in the APG folder. Then it's easy to import your keys. After you've imported your public and private keys, GPG encrypting, signing and decrypting will be available for other applications as long as these applications have integrated encryption/GPG.

GPG enabled e-mail on Android: K-9 Mail

The default mail application does not support GPG. Luckily there is an excellent alternative: K-9 Mail. This application is based on the original Android mail application but with some improvements. The application can use APG as it's GPG provider. Setting up K-9 Mail is straightforward and similar to setting up mail in the Android default mail application. In the settings menu there is an option to enable "Cryptography" for GPG mail signing.

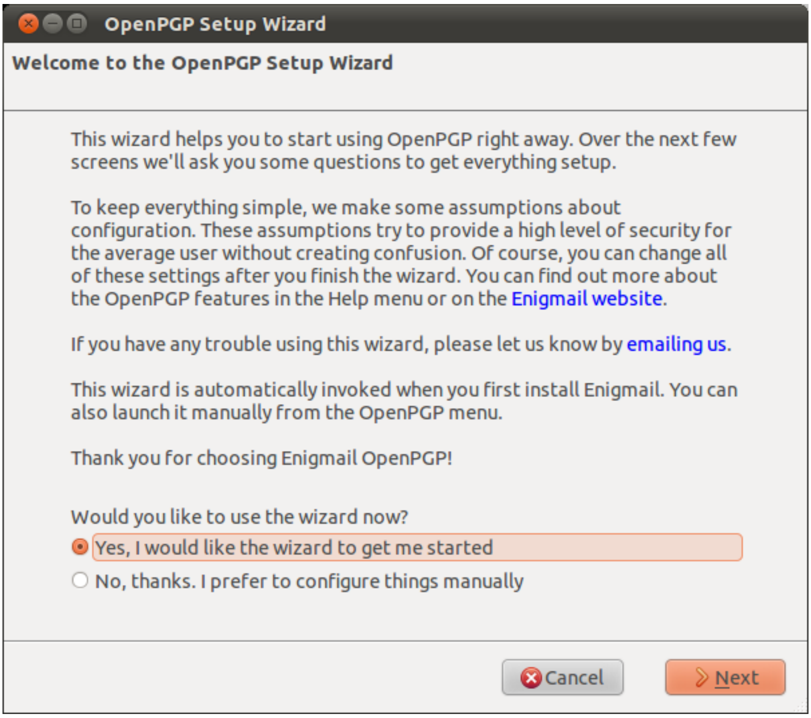
If you want to access your GPG mails on your phone this application is a must have.

Please note, due to some small bugs in K-9 Mail and/or APG, it's very advisable to disable HTML mail and use only Plain text. HTML mails are not encrypted nicely and are often not readable.

Creating GPG keys in Thunderbird

You are now ready to start encryption your mails with GPG. You can do this by using Enigmail *within* Thunderbird. Enigmail comes with a nice wizard to help you with the creation of a public/private key pair (see the chapter introducing GPG for an explanation). You can start the wizard at any time within Thunderbird by selecting **OpenPGP** > **Setup Wizard** from the menu on top.

Step 1. This is what the wizard looks like. Please read the text on every window carefully. It provides useful information and helps you setup GPG to your personal preferences. In the first screen, click on Next to start the configuration.



Welcome to the OpenPGP Setup Wizard

This wizard helps you to start using OpenPGP right away. Over the next few screens we'll ask you some questions to get everything setup.

To keep everything simple, we make some assumptions about configuration. These assumptions try to provide a high level of security for the average user without creating confusion. Of course, you can change all of these settings after you finish the wizard. You can find out more about the OpenPGP features in the Help menu or on the Enigmail website.

If you have any trouble using this wizard, please let us know by emailing us.

This wizard is automatically invoked when you first install Enigmail. You can also launch it manually from the OpenPGP menu.

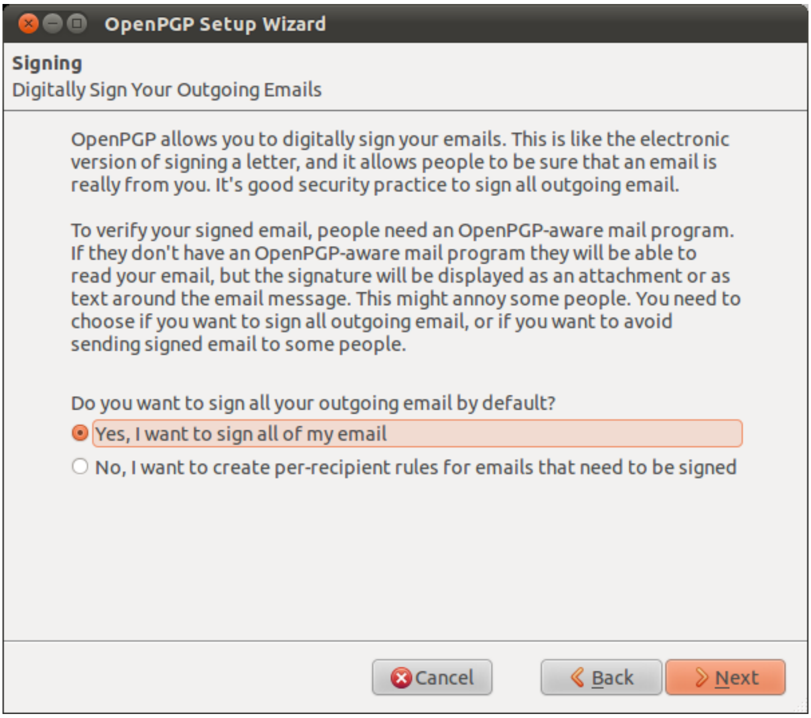
Thank you for choosing Enigmail OpenPGP!

Would you like to use the wizard now?

● Yes, I would like the wizard to get me started

○ No, thanks. I prefer to configure things manually

Step 2. The wizard asks you whether you want to sign all your outgoing mail messages. Signing all your messages is a good choice. If you choose not to, you can still manually decide to sign a message when you are composing it. Click on the 'Next' button after you have made a decision.



Signing

Digitally Sign Your Outgoing Emails

OpenPGP allows you to digitally sign your emails. This is like the electronic version of signing a letter, and it allows people to be sure that an email is really from you. It's good security practice to sign all outgoing email.

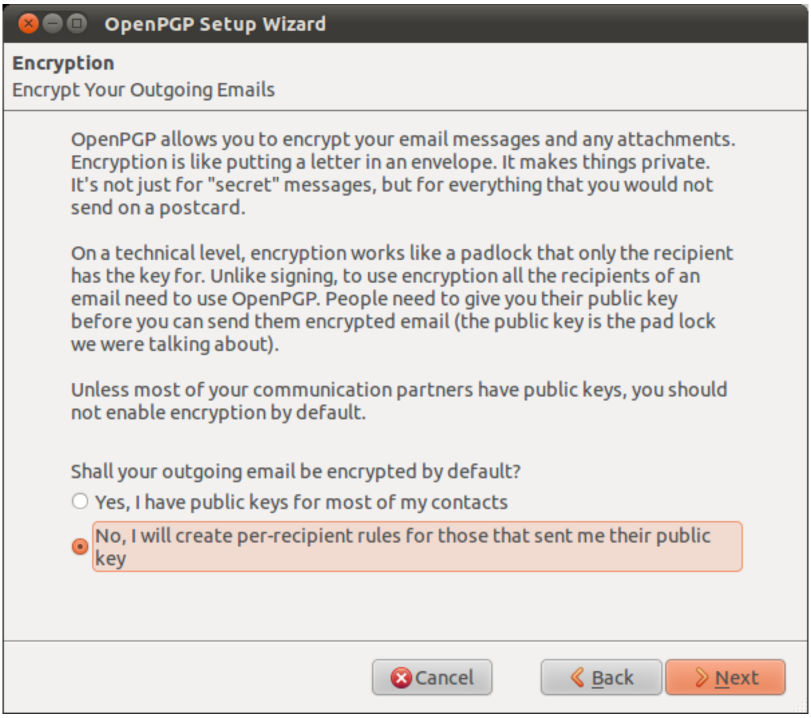
To verify your signed email, people need an OpenPGP-aware mail program. If they don't have an OpenPGP-aware mail program they will be able to read your email, but the signature will be displayed as an attachment or as text around the email message. This might annoy some people. You need to choose if you want to sign all outgoing email, or if you want to avoid sending signed email to some people.

Do you want to sign all your outgoing email by default?

● Yes, I want to sign all of my email

○ No, I want to create per-recipient rules for emails that need to be signed

Step 3. On the following screen, the wizard asks you whether you want to encrypt *all* your outgoing mail messages by default. Unlike with signing of mails, encryption requires the recipient to have GPG software installed as well. Therefore you should probably answer 'no' to this question, so that you will send normal (unencrypted) mail by default. After you have made your decision, click on the 'Next' button.



Encryption

Encrypt Your Outgoing Emails

OpenPGP allows you to encrypt your email messages and any attachments. Encryption is like putting a letter in an envelope. It makes things private. It's not just for "secret" messages, but for everything that you would not send on a postcard.

On a technical level, encryption works like a padlock that only the recipient has the key for. Unlike signing, to use encryption all the recipients of an email need to use OpenPGP. People need to give you their public key before you can send them encrypted email (the public key is the pad lock we were talking about).

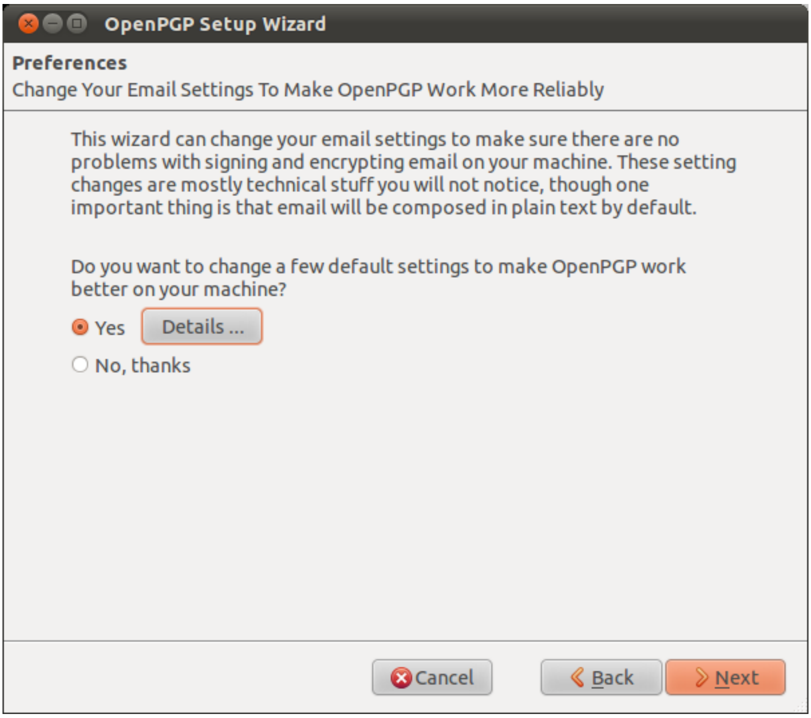
Unless most of your communication partners have public keys, you should not enable encryption by default.

Shall your outgoing email be encrypted by default?

○ Yes, I have public keys for most of my contacts

● No, I will create per-recipient rules for those that sent me their public key

Step 4: On the following screen the wizard asks if it should change some of your mail formatting settings to better work with PGP. It is a good choice to answer 'Yes' because it means that by default, your mail will be composed in plain text rather than HTML. Click on the 'Next' button after you have made your decision.



Preferences
Change Your Email Settings To Make OpenPGP Work More Reliably

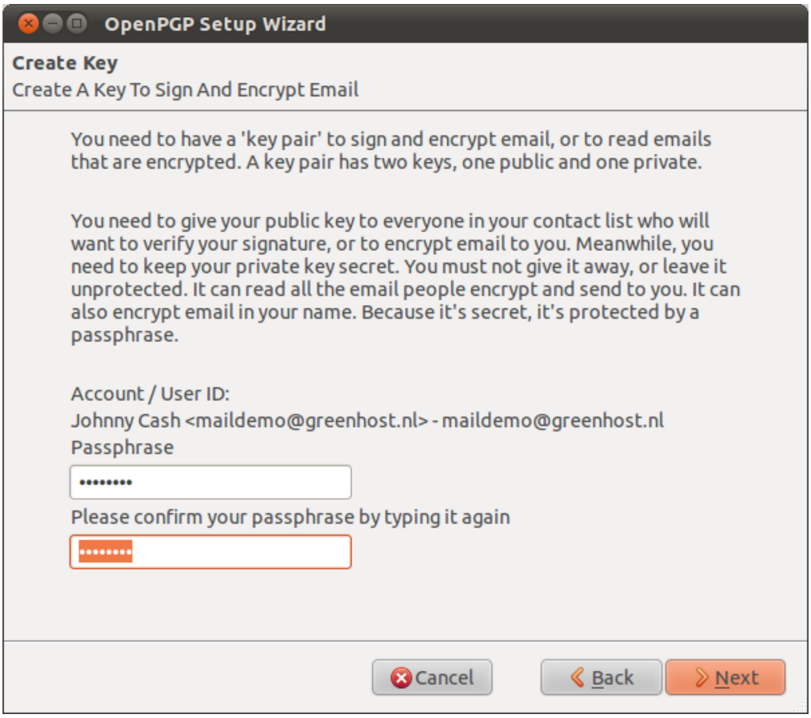
This wizard can change your email settings to make sure there are no problems with signing and encrypting email on your machine. These setting changes are mostly technical stuff you will not notice, though one important thing is that email will be composed in plain text by default.

Do you want to change a few default settings to make OpenPGP work better on your machine?

● Yes Details ...

○ No, thanks

Step 5: In the following screen, select one of your mail accounts; the default is selected for you if you only have one. In the 'Passphrase' text box you must enter a password. This is a *new* password which is used to protect your private key. It is **very important** to remember this password, because you cannot read your own encrypted emails if you forget it. Make it a **strong** password, ideally 20 characters or longer. Please see the chapter on passwords for help on creating unique, long and easy to remember passwords. After you have selected your account and created a passphrase, click on the 'Next' button.



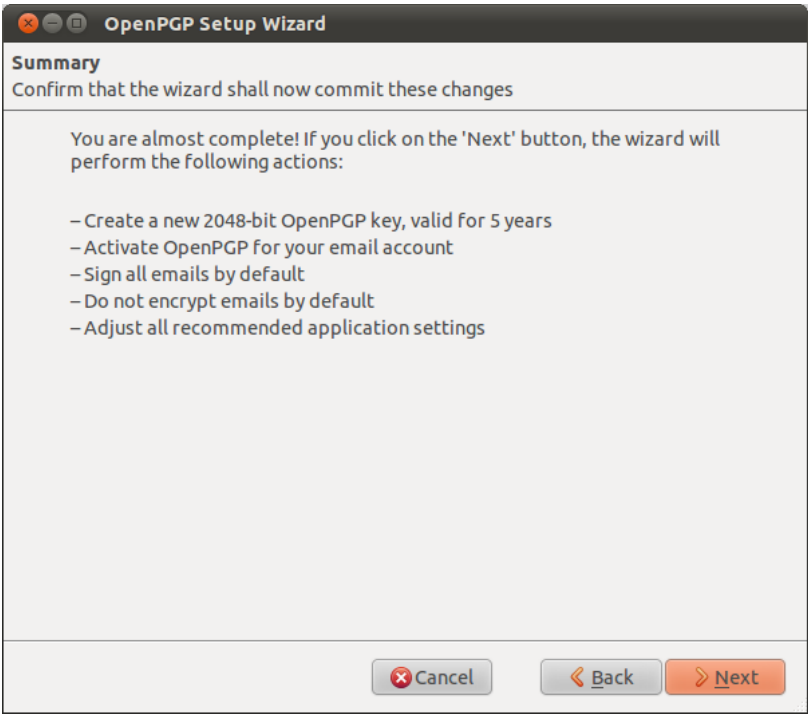
Create Key
Create A Key To Sign And Encrypt Email

You need to have a 'key pair' to sign and encrypt email, or to read emails that are encrypted. A key pair has two keys, one public and one private.

You need to give your public key to everyone in your contact list who will want to verify your signature, or to encrypt email to you. Meanwhile, you need to keep your private key secret. You must not give it away, or leave it unprotected. It can read all the email people encrypt and send to you. It can also encrypt email in your name. Because it's secret, it's protected by a passphrase.

Account / User ID:
Johnny Cash <maildemo@greenhost.nl> - maildemo@greenhost.nl
Passphrase
••••••••
Please confirm your passphrase by typing it again
••••••••

Step 6: In the following screen the wizard summarizes the actions it will take to enable PGP encryption for your account. If you are satisfied, click the 'Next' button.



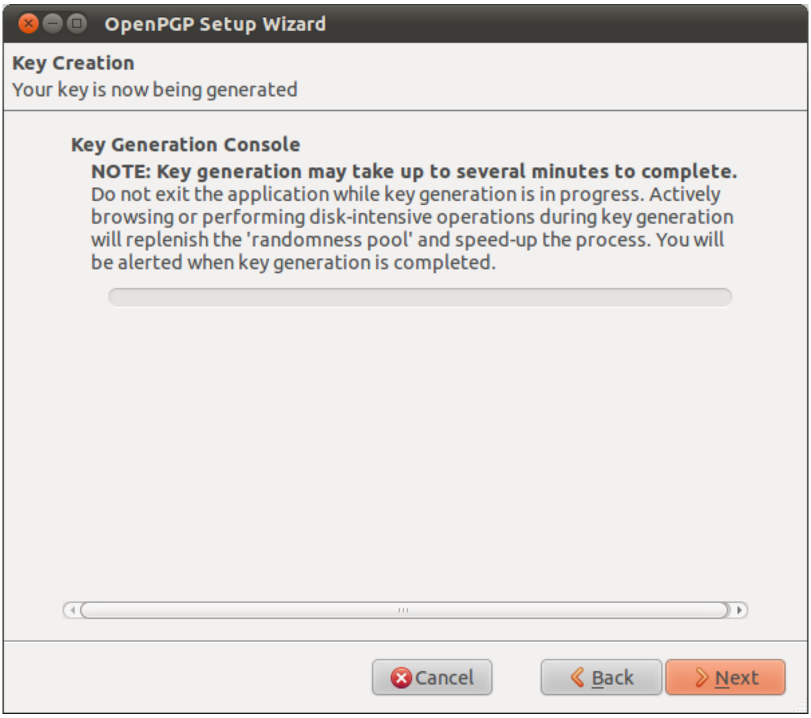
Summary

Confirm that the wizard shall now commit these changes

You are almost complete! If you click on the 'Next' button, the wizard will perform the following actions:

– Create a new 2048-bit OpenPGP key, valid for 5 years
– Activate OpenPGP for your email account
– Sign all emails by default
– Do not encrypt emails by default
– Adjust all recommended application settings

Step 7: Your keys will be created by the wizard, which will take some time (you can speed it up by doing random stuff, like moving your mouse, browsing the web or something else). When completed, click on the 'Next' button.



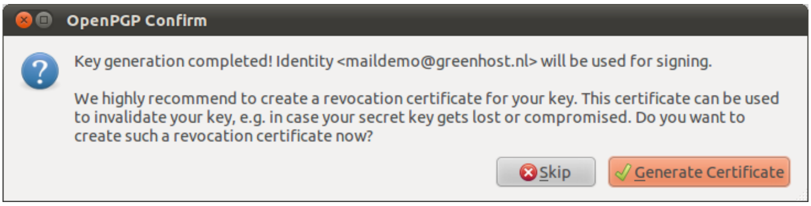
Key Creation

Your key is now being generated

Key Generation Console

NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

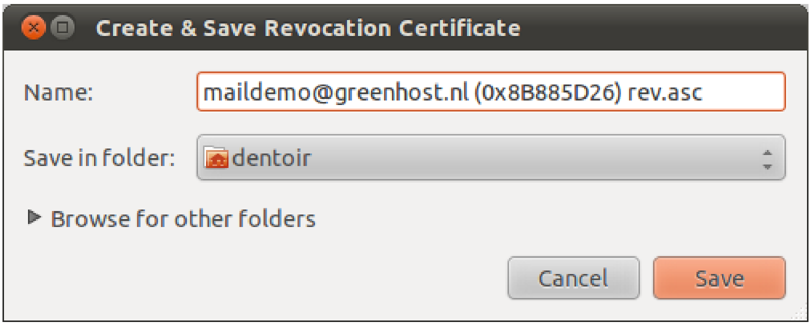
Step 8: You now have your own GPG key-pair. The wizard will ask you if you also want to create a 'Revocation certificate'. This is a file which can be used to inform everyone if your private key is compromised, for example if your laptop is stolen. Think of it as a 'kill switch' for your GPG identity. You may also wish to revoke the key simply because you have generated a new one, and the old one is obsolete.



Key generation completed! Identity <maildemo@greenhost.nl> will be used for signing.

We highly recommend to create a revocation certificate for your key. This certificate can be used to invalidate your key, e.g. in case your secret key gets lost or compromised. Do you want to create such a revocation certificate now?

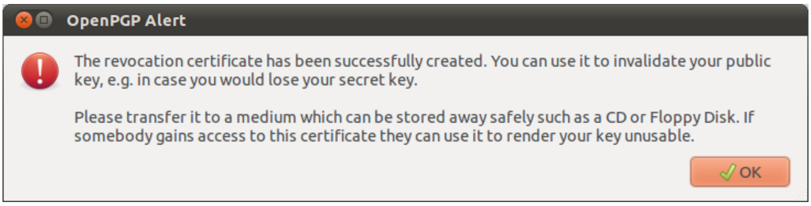
Step 9: If you decided to generate a revocation certificate, the wizard will ask you where the file should be saved. The dialog will look different depending on which operating system you use. It is a good idea to rename the file to something sensible like 'my_revocation_certificate'. Click on 'Save' when you you have decided on a location.



Name: maildemo@greenhost.nl (0x8B885D26) rev.asc

Save in folder: dentoir

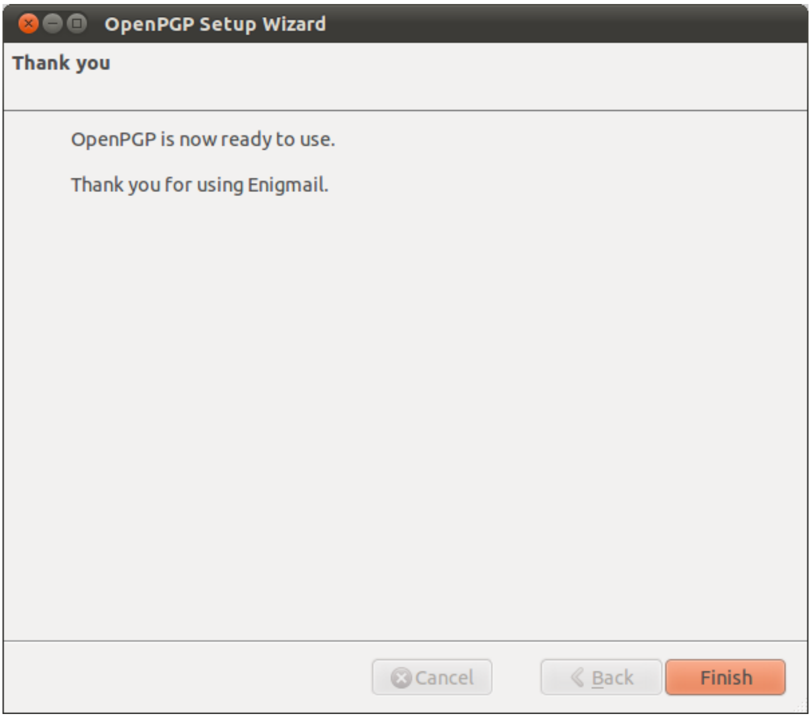
Step 10: If you decided to generate a revocation certificate, the wizard informs you it has been successfully stored. You may want to print it out or burn it to a CD and keep it in a safe place.



The revocation certificate has been successfully created. You can use it to invalidate your public key, e.g. in case you would lose your secret key.

Please transfer it to a medium which can be stored away safely such as a CD or Floppy Disk. If somebody gains access to this certificate they can use it to render your key unusable.

Step 11: The wizard will inform you it has completed the setup.



OpenPGP is now ready to use.

Thank you for using Enigmail.

Congratulations, you now have a fully PGP-configured mail client. In the next chapter we will explain how to manage your keys, sign messages and do encryption. Thunderbird can help you do a lot of these things automatically.

DAILY PGP USAGE

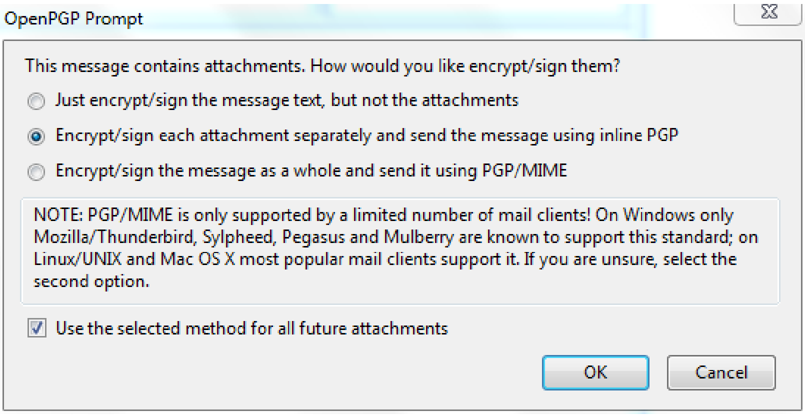
In the previous chapters we have have explained how to set up a secure mail environment using Thunderbird, GPG and Enigmail. We assume you have installed the software and have successfully followed the wizard instructions to generate an encryption key-pair as described in the previous chapter. This chapter will describe how to use your secured Thunderbird in daily life to protect your e-mail communication. In particular we will focus on:

1. Encrypting attachments
2. Entering your pass-phrase
3. Receiving encrypted e-mail
4. Sending and receiving public keys
5. Receiving public keys and adding them to your key ring
6. Using public key servers
7. Signing e-mails to an individual
8. Sending encrypted e-mails to an individual
9. Automating encryption to certain recipients
10. Verifying incoming e-mails
11. Revoking your GPG key pair
12. What to do when you have lost your secret key, or forgot your passphrase
13. What to do when your secret key has been stolen, or compromised
14. Backing up your keys

First we shall explain two dialog windows that will inevitably appear after you start using Thunderbird to encrypt your emails.

ENCRYPTING ATTACHMENTS

The dialog window below will pop-up whenever you are sending an encrypted email with attachments for the first time. Thunderbird asks a technical question on how to encrypt attachments to your mail. The second (default) option is the best choice, because it combines security with the highest compatibility. You should also select the 'Use the selected method for all future attachments' option. Then click 'OK' and your mail should be sent with no further delay.



OpenPGP Prompt

This message contains attachments. How would you like encrypt/sign them?

○ Just encrypt/sign the message text, but not the attachments

● Encrypt/sign each attachment separately and send the message using inline PGP

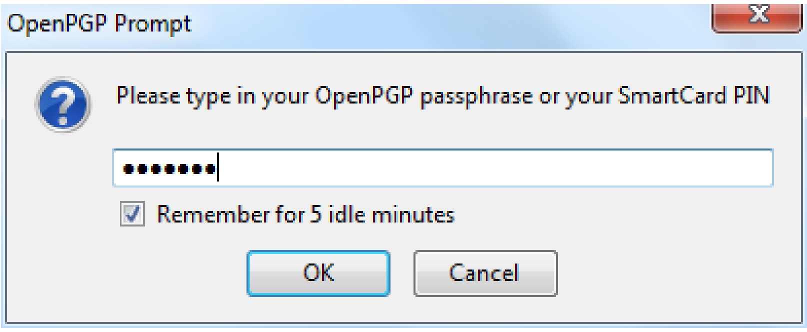
○ Encrypt/sign the message as a whole and send it using PGP/MIME

NOTE: PGP/MIME is only supported by a limited number of mail clients! On Windows only Mozilla/Thunderbird, Sylpheed, Pegasus and Mulberry are known to support this standard; on Linux/UNIX and Mac OS X most popular mail clients support it. If you are unsure, select the second option.

☑ Use the selected method for all future attachments

Entering your pass-phrase

For security reasons, the pass-phrase to your secret key is stored temporarily in memory. Every now and then the dialog window below will pop-up. Thunderbird asks you for the pass-phrase to your secret key. This should be different from your normal email password. It was the pass-phrase you have entered when creating your key-pair in the previous chapter. Enter the pass-phrase in the text-box and click on 'OK'



OpenPGP Prompt

Please type in your OpenPGP passphrase or your SmartCard PIN

•••••••

☑ Remember for 5 idle minutes

Receiving encrypted e-mails

The decryption of e-mails is handled automatically by Enigmail, the only action that may be needed on your behalf is to enter the pass-phrase to your secret key. However, in order to have any kind of encrypted correspondence with somebody, you will first need to exchange public keys.

Sending and receiving public keys

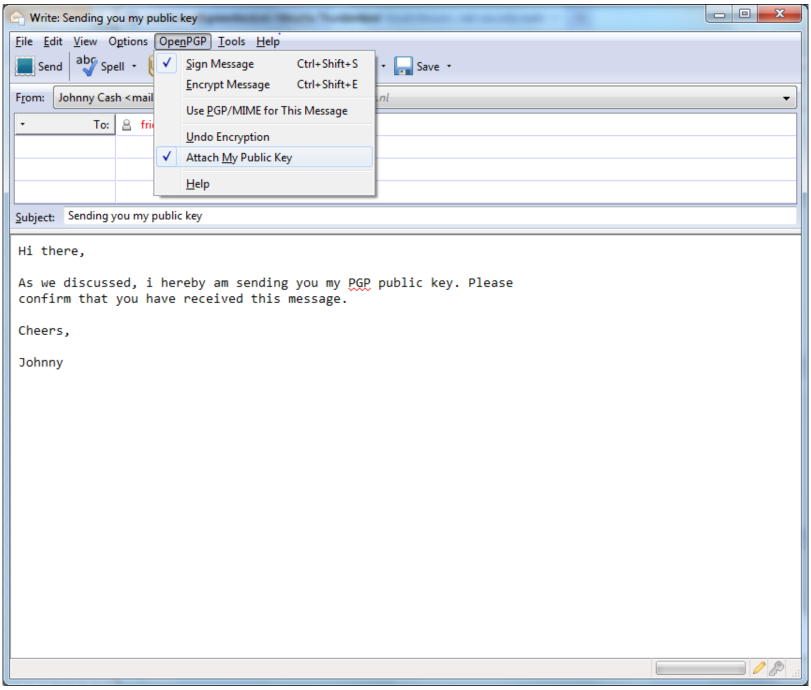
There are multiple ways to distribute your public key to friends or colleagues. By far the simplest way is to attach the key to a mail. In order for your friend to be able to *trust* that the message actually came from you, you should inform them in person (if possible) and also require them to reply to your mail. This should at least prevent easy forgeries. You have to decide for yourself what level of validation is necessary. This is also true when receiving emails from third-parties containing public keys. Contact your correspondent through some means of communication other than e-mail. You can use a telephone, text messages, Voice over Internet Protocol (VoIP) or any other method, but you must be absolutely certain that you are really talking to the right person. As a result, telephone conversations and face-to-face meetings work best, if they are convenient and if they can be arranged safely.

Sending your public key is easy.

1. In Thunderbird, click on the Write icon.

2. Compose a mail to your friend or colleague and tell them you are sending them your PGP public key. If your friend does not know what that means, you may have to explain them and point them to this documentation.

3. Before actually sending the mail, click to **OpenPGP > Attach My Public Key** option on the menu bar of the mail compose window. Next to this option a marked sign ✓ will appear. See the example below.


Write: Sending you my public key
File
Edit
View
Options
OpenPGP
Tools
Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
✓ Attach My Public Key
Help
To:

From: Johnny Cash <mail

To: fri

Subject: Sending you my public key

```
Hi there,

As we discussed, i hereby am sending you my PGP public key. Please
confirm that you have received this message.

Cheers,

Johnny
```

4. Send your mail by clicking on the Send button.

Receiving public keys and adding them to your keyring

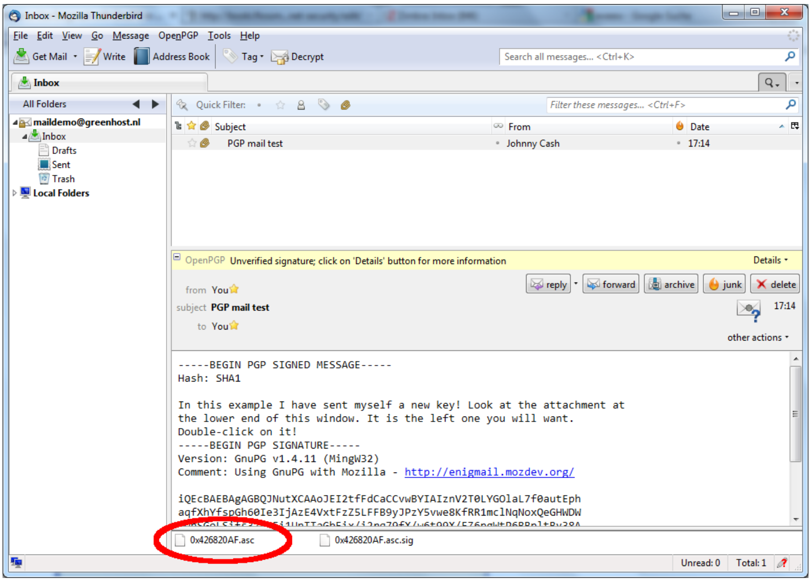
Lets say we receive a public key from a friend by mail. The key will show up in Thunderbird as an *attached file*. Scroll down the message and below you will find tabs with one or two file names. The extension of this public key file will be .asc, different from the extension of an attached GPG signature, which ends with .asc.sig

Look at the example email in the next image, which is a received, signed GPG message containing an attached public key. We notice a yellow bar with a warning message: 'OpenPGP: Unverified signature, click on 'Details' button for more information'. Thunderbird warns us that the sender is not known yet, which is correct. This will change once we have accepted the public key.

What are all those strange characters doing in the mail message? Because Thunderbird does not yet recognize the signature as valid, it prints out the entire raw signature, just as it has received it. This is how digitally signed

GPG messages will appear to those recipients who do not have your public key.

The most important thing in this example is to find the attached GPG public key. We mentioned it is a file that ends with .asc. In this example it's the first attachment on the left, in the red circle. Double-clicking on this attachment will make Thunderbird recognize the key.



Subject	From	Date
PGP mail test	Johnny Cash	17:14

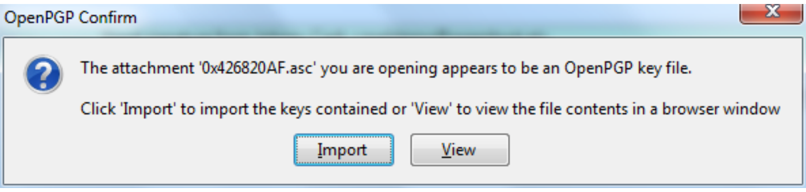
OpenPGP Unverified signature; click on 'Details' button for more information

from You
subject **PGP mail test**
to You
17:14

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

In this example I have sent myself a new key! Look at the attachment at
the lower end of this window. It is the left one you will want.
Double-click on it!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

iQEcBAEBAgAGBQJNutXCAAoJEI2tfFdCaCCvwBYIAIznV2T0LYGOlaL7f0autEph
aqfXhYfspGh60Ie3IjAzE4VxtFzZ5LFFB9yJPzY5vwe8KfRR1mclNqNoxQeGHWDW
```

0x426820AF.asc
0x426820AF.asc.sig

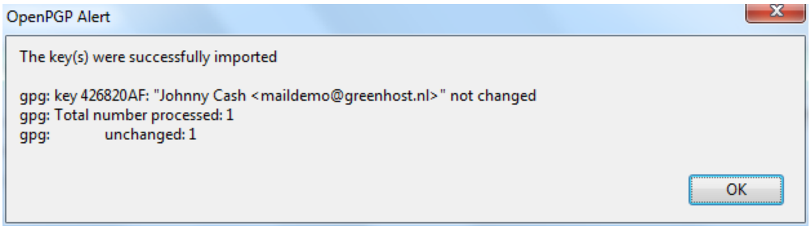
After we have clicked on the attachment, the following pop-up will appear.



The attachment '0x426820AF.asc' you are opening appears to be an OpenPGP key file.

Click 'Import' to import the keys contained or 'View' to view the file contents in a browser window

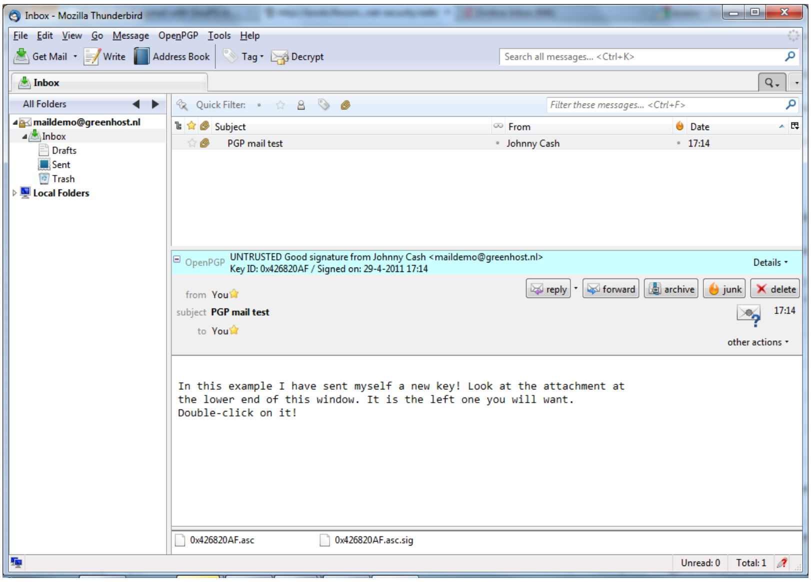
Thunderbird has recognized the GPG public key file. Click on 'Import' to add this key to your keyring. The following pop-up should appear. Thunderbird says the operation was successful. Click on 'OK' and you are almost done.



The key(s) were successfully imported

```
gpg: key 426820AF: "Johnny Cash <maildemo@greenhost.nl>" not changed
gpg: Total number processed: 1
gpg:           unchanged: 1
```

We are back in the main Thunderbird screen and we refresh the view on this particular example message, by clicking on some other message and back for example. Now the body of the message looks different (see below). This time Thunderbird *does* recognize the signature, because we have added the public key of the sender.



Subject	From	Date
PGP mail test	Johnny Cash	17:14

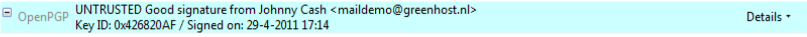
OpenPGP UNTRUSTED Good signature from Johnny Cash <maildemo@greenhost.nl>
Key ID: 0x426820AF / Signed on: 29-4-2011 17:14

from You
subject **PGP mail test**
to You
17:14

```
In this example I have sent myself a new key! Look at the attachment at
the lower end of this window. It is the left one you will want.
Double-click on it!
```

0x426820AF.asc
0x426820AF.asc.sig

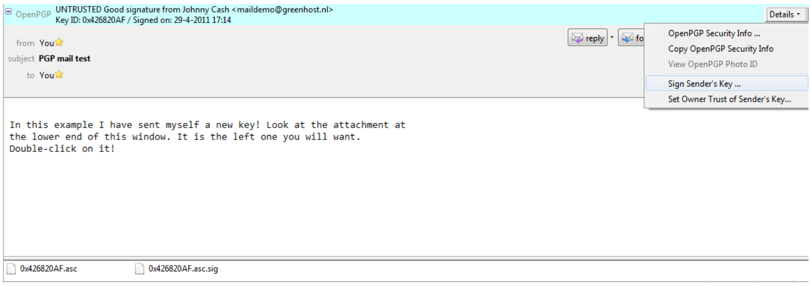
There is still one thing that remains. While Thunderbird now recognizes the signature, we should explicitly *trust* that the public key really belongs to the sender in real life. We realize this when we take a closer look at the green bar (see below). While the signature is good, it is still UNTRUSTED.



OpenPGP UNTRUSTED Good signature from Johnny Cash <maildemo@greenhost.nl>
Key ID: 0x426820AF / Signed on: 29-4-2011 17:14

We will now decide to trust this particular public key and the signatures made by it. We can do this immediately by clicking on 'Details'. A small menu will appear (see below). From this menu we should click on the option 'Sign

Sender's Key ...'.

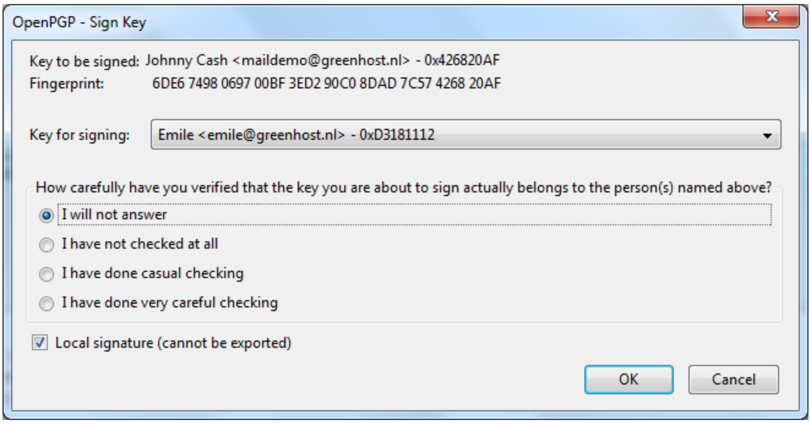


OpenPGP UNTRUSTED Good signature from Johnny Cash <maildemo@greenhost.nl>
Key ID: 0x426820AF / Signed on: 29-4-2011 17:14

from You
subject PGP mail test
to You

```
In this example I have sent myself a new key! Look at the attachment at
the lower end of this window. It is the left one you will want.
Double-click on it!
```

After we have selected 'Sign Sender's Key ...' we will get another selection window (see below). We are requested to state how carefully we have checked this key for validity. The explanation of levels of trust and trust networks in GPG falls outside the scope of this document. We will not use this information, therefore we will just select the option 'I will not answer'. Also select the option 'Local signature (cannot be exported)'. Click on the 'OK' button to finishing signing this key. This finishes accepting the public key. You can now send encrypted mail to this individual.



OpenPGP - Sign Key

Key to be signed: Johnny Cash <maildemo@greenhost.nl> - 0x426820AF
Fingerprint: 6DE6 7498 0697 00BF 3ED2 90C0 8DAD 7C57 4268 20AF

Key for signing: Emile <emile@greenhost.nl> - 0xD3181112

How carefully have you verified that the key you are about to sign actually belongs to the person(s) named above?

● I will not answer
○ I have not checked at all
○ I have done casual checking
○ I have done very careful checking

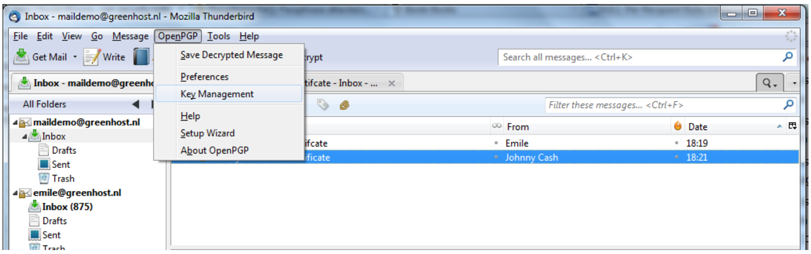
☑ Local signature (cannot be exported)

Using public key servers

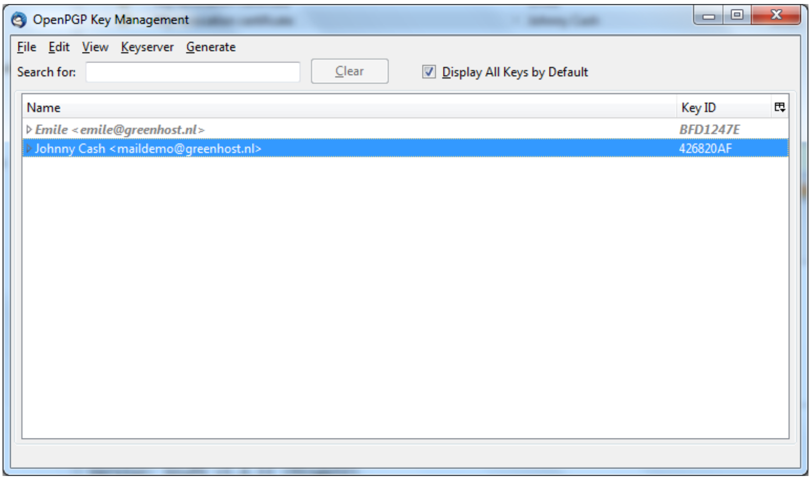
Another method of distributing public keys is by putting them on a public key server. This allows anyone to check whether your email address has GPG support, and then download your public key.

To put your own key on a keyserver, take the following steps.

1. Head to the key manager by using the Thunderbird menu and click on **OpenPGP > Key Management**

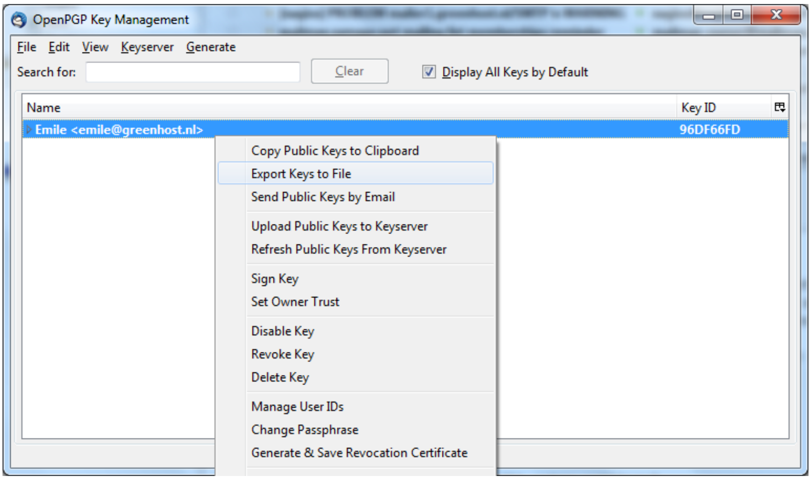


2. The key management window will be displayed and looks like this:


OpenPGP Key Management
File Edit View Keyserver Generate
Search for:
Clear
☑ Display All Keys by Default

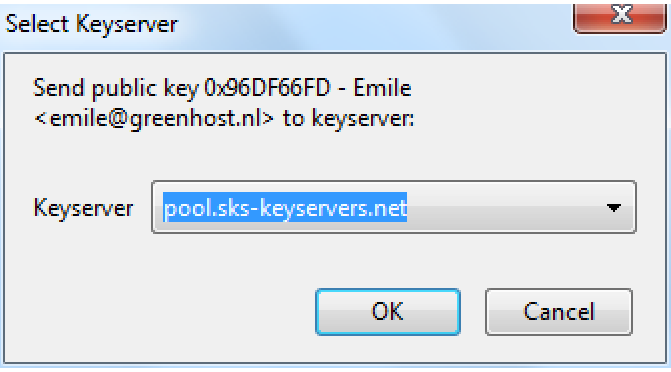
Name	Key ID
Emile <emile@greenhost.nl>	BFD1247E
Johnny Cash <maildemo@greenhost.nl>	426820AF

3. You need to have selected the 'Display All Keys by Default' option to get a list of all your keys. Look up your own email address in the list and right click on the address. A selection window will appear with some options. Select the option 'Upload Public Keys to Keyserver'.


OpenPGP Key Management
File
Edit
View
Keyserver
Generate
Search for:
Clear
☑ Display All Keys by Default
Copy Public Keys to Clipboard
Export Keys to File
Send Public Keys by Email
Upload Public Keys to Keyserver
Refresh Public Keys From Keyserver
Sign Key
Set Owner Trust
Disable Key
Revoke Key
Delete Key
Manage User IDs
Change Passphrase
Generate & Save Revocation Certificate

Name	Key ID
Emile <emile@greenhost.nl>	96DF66FD

4. You will see a small dialog window like below. The default server to distribute your keys to is good. Press 'OK" and distribute your public key to the world.



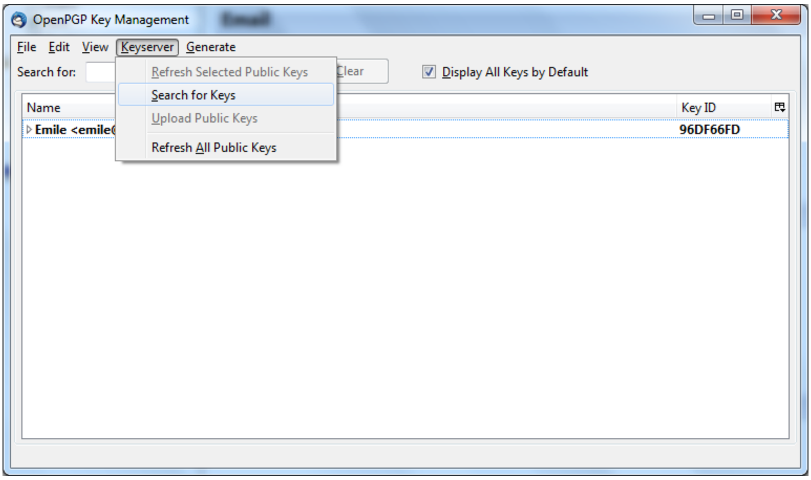
Send public key 0x96DF66FD - Emile <emile@greenhost.nl> to keyserver:

Keyserver pool.sks-keyservers.net

To look up whether some email address has a public key available on a server, take the following steps.

1. Head to the key manager by using the Thunderbird menu and click on **OpenPGP > Key Management**

2. In the key manager window menu bar, select **Keyserver > Search for Keys**

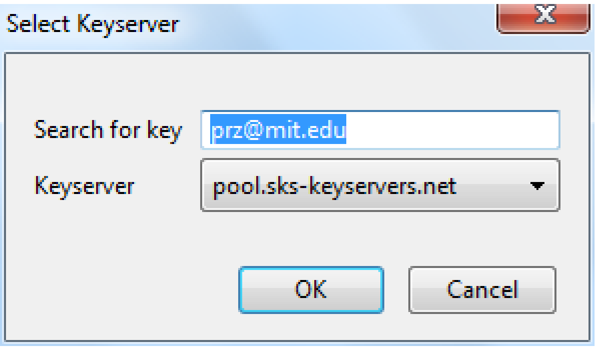


Search for:

☑ Display All Keys by Default

Name	Key ID
Emile <emile(	96DF66FD

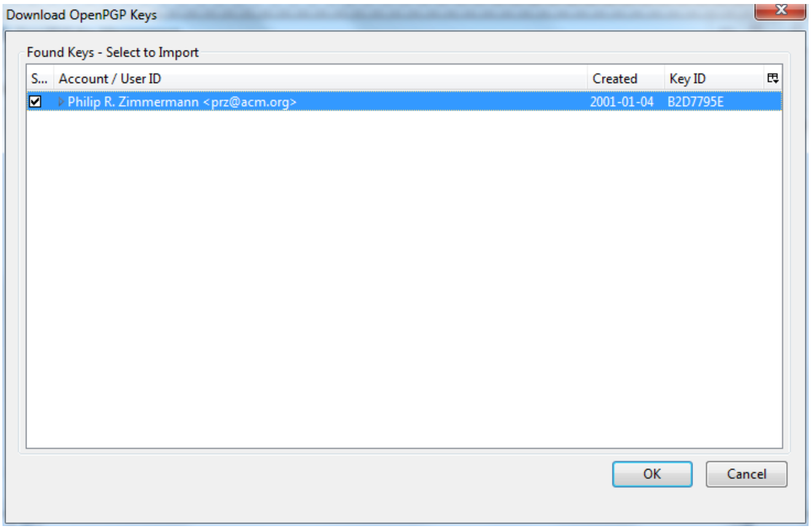
3. In this example we will look-up up the key for the creator of PGP software, Philip Zimmermann. After we have entered the email address, we click on 'OK'.



Search for key: prz@mit.edu

Keyserver: pool.sks-keyservers.net

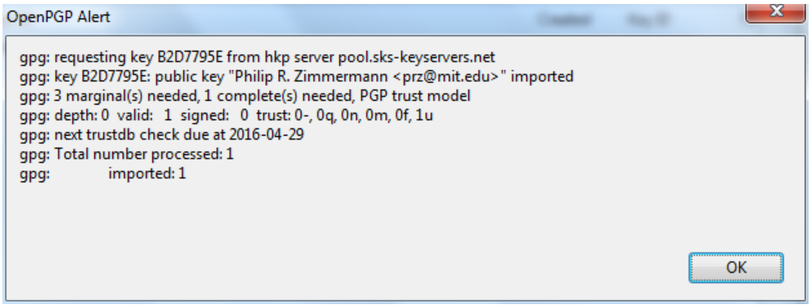
4, The next window displays the result of our search. We have found the public key. It is automatically selected. Just click on 'OK' to import the key.



Found Keys - Select to Import

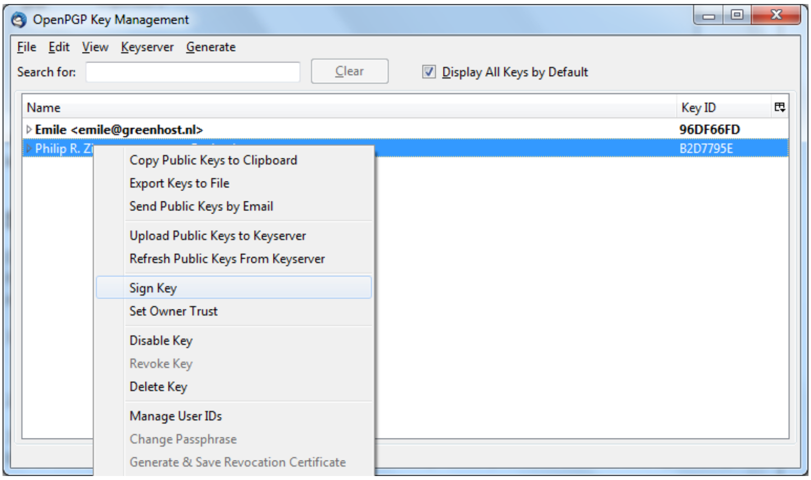
S...	Account / User ID	Created	Key ID
☑	Philip R. Zimmermann <prz@acm.org>	2001-01-04	B2D7795E

5. Importing the key will take some time. On completion you should see a pop-up window like below.

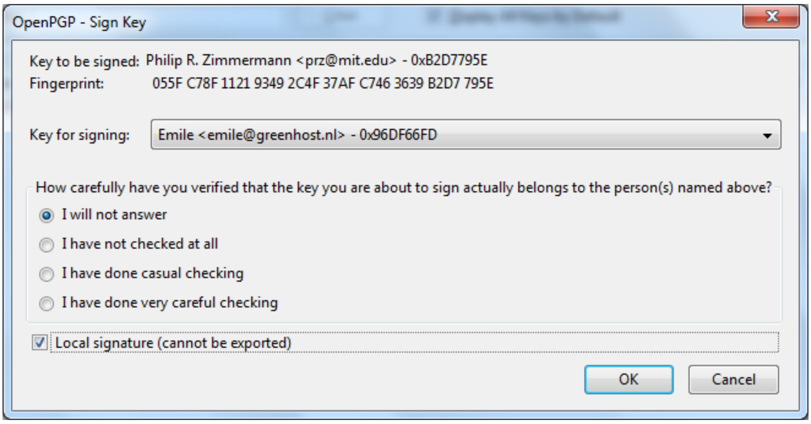


```
gpg: requesting key B2D7795E from hkp server pool.sks-keyservers.net
gpg: key B2D7795E: public key "Philip R. Zimmermann <prz@mit.edu>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-04-29
gpg: Total number processed: 1
gpg:               imported: 1
```

6. The final step is to locally sign this key, to indicate that we trust it. When you are back in the key manager, make sure you have selected the 'Display All Keys by Default' option. You should now see the newly imported key in the list. Right-click on the address and select the option 'Sign Key' from the list.


OpenPGP Key Management
File Edit View Keyserver Generate
Search for:
Clear
☑ Display All Keys by Default
Name
Key ID
Emile <emile@greenhost.nl> 96DF66FD
Philip R. Zi B2D7795E
Copy Public Keys to Clipboard
Export Keys to File
Send Public Keys by Email
Upload Public Keys to Keyserver
Refresh Public Keys From Keyserver
Sign Key
Set Owner Trust
Disable Key
Revoke Key
Delete Key
Manage User IDs
Change Passphrase
Generate & Save Revocation Certificate

7. Select the options 'I will not answer' and 'Local signature (cannot be exported)', then click on 'OK'. You are now finished and can send Philip Zimmermann encrypted mail.


OpenPGP - Sign Key

Key to be signed: Philip R. Zimmermann <prz@mit.edu> - 0xB2D7795E

Fingerprint: 055F C78F 1121 9349 2C4F 37AF C746 3639 B2D7 795E

Key for signing: Emile <emile@greenhost.nl> - 0x96DF66FD

How carefully have you verified that the key you are about to sign actually belongs to the person(s) named above?

● I will not answer

○ I have not checked at all

○ I have done casual checking

○ I have done very careful checking

☑ Local signature (cannot be exported)

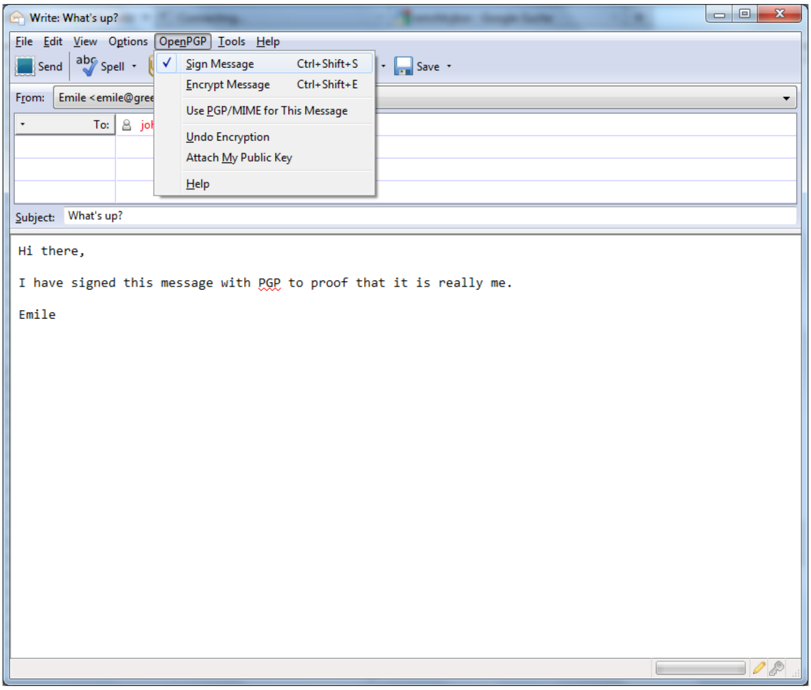
Signing emails to an individual

Digitally signing email messages is a way to prove to recipients that you are the actual sender of a mail message. Those recipients who have received your public key will be able to *verify* that your message is authentic.

1. Offer your friend your public key, using the method described earlier in this chapter.

2. In Thunderbird, click on the Write icon.

3. Before actually sending the mail, enable the **OpenPGP > Sign Message** option via the menu bar of the mail compose window, if it is not enable already. Once you have enabled this option, by clicking on it, a marked sign ✓ will appear. Clicking again should disable encryption again. See the example below.


Write: What's up?
File Edit View Options OpenPGP Tools Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
Attach My Public Key
Help
From: Emile <emile@gree
To:
Subject: What's up?

Hi there,

I have signed this message with PGP to proof that it is really me.

Emile

4. Click on the Send button and your signed mail will be sent.

Sending encrypted mails to an individual

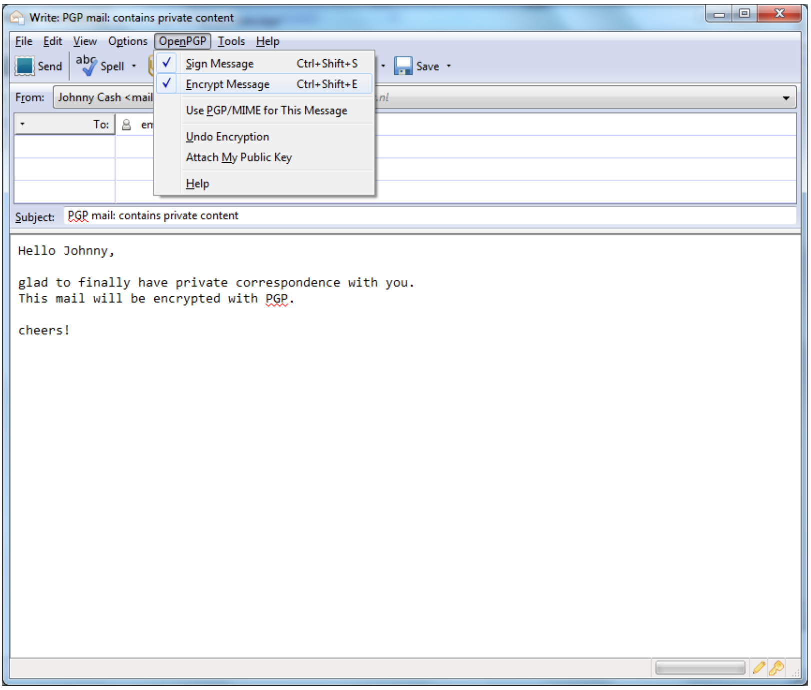
1. You should have received the public key from the friend or colleague you want to email and you should have accepted their public key, using the method describe earlier in this chapter.

2. In Thunderbird, click on the Write icon.

3. Compose a mail to the friend or colleague, from who you have previously received their public key. **Remember the subject line of the message will**

not be encrypted, only the message body itself, and any attachments.

4. Before actually sending the mail, enable the **OpenPGP** > **Encrypt Message** option via the menu bar of the mail compose window, if it is not enabled already. Once you have enabled this option, by clicking on it, a marked sign ✓ will appear. Clicking again should disable encryption again. See the example below.



Write: PGP mail: contains private content
File
Edit
View
Options
OpenPGP
Tools
Help
Send
Spell
Save
✓ Sign Message Ctrl+Shift+S
✓ Encrypt Message Ctrl+Shift+E
Use PGP/MIME for This Message
Undo Encryption
Attach My Public Key
Help
To:

From: Johnny Cash <mail

Subject: PGP mail: contains private content

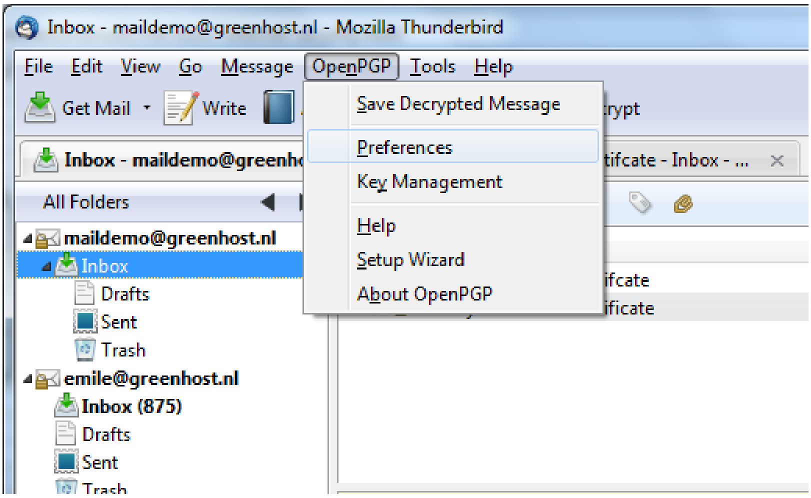
```
Hello Johnny,

glad to finally have private correspondence with you.
This mail will be encrypted with PGP.

cheers!
```

5. Click on the Send button and your encrypted mail will be sent.

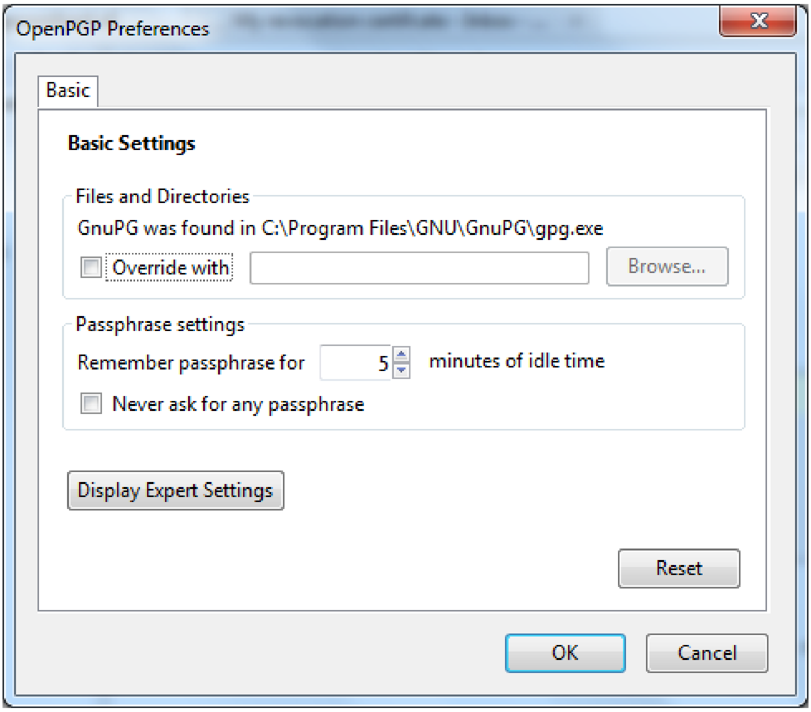
Automating encryption to certain recipients

You will often want to make sure *all* your messages to a certain colleague or friend are signed and encrypted. This is good practice, because you may forget to enable the encryption manually. You can do this by editing the per-recipient rules. To do this we access the OpenPGP per-recipient rule editor.

Select **OpenPGP** > **Preferences** from the Thunderbird menu bar.



The preferences window will appear like below. We need to click on 'Display Expert Settings'.



OpenPGP Preferences

Basic

Basic Settings

Files and Directories

GnuPG was found in C:\Program Files\GNU\GnuPG\gpg.exe

□ Override with [ ] Browse...

Passphrase settings

Remember passphrase for 5 minutes of idle time

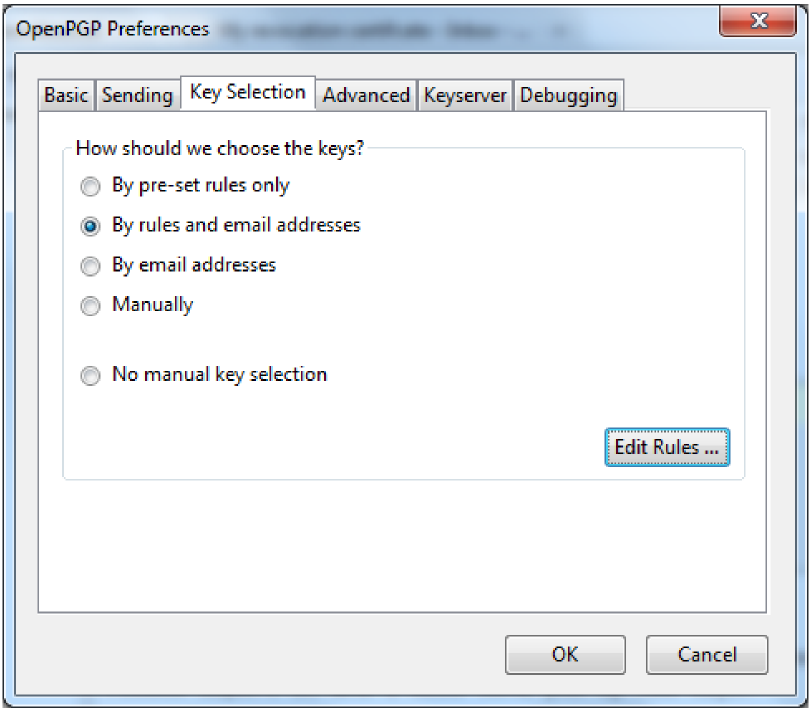
□ Never ask for any passphrase

Display Expert Settings

Reset

OK Cancel

New menu tabs will appear in the window. Go to the tab 'Key Selection' and then click on the button labeled 'Edit Rules ...'



How should we choose the keys?

○ By pre-set rules only

● By rules and email addresses

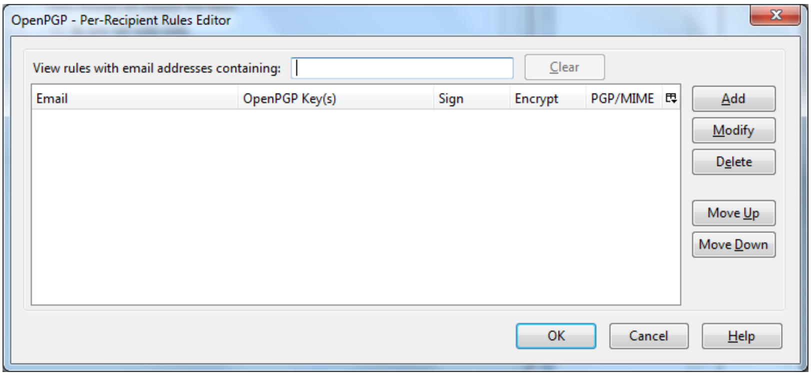
○ By email addresses

○ Manually

○ No manual key selection

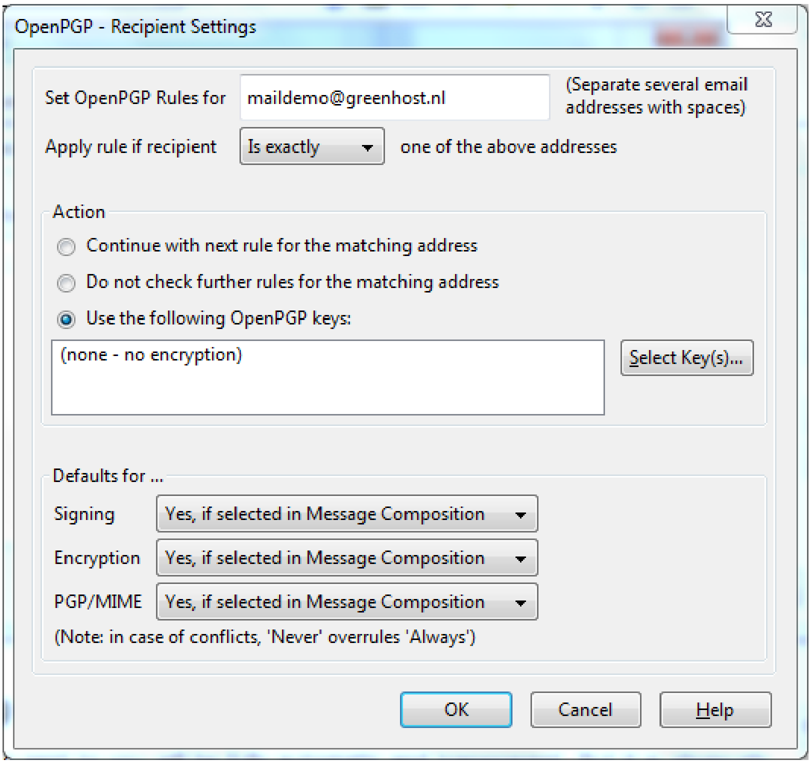
We are now shown the per-recipient rules editor (see below). This editor can be used to specify the way how messages to certain recipients are sent. We will now add a rule saying we want to encrypt and sign all mail messages to maildemo@greenhost.nl

First click on the 'Add' button.



Now the window to add a new rule will be shown.

The first thing we should enter is the email address of the recipient. In the example below we have entered maildemo@greenhost.nl



OpenPGP - Recipient Settings

Set OpenPGP Rules for: maildemo@greenhost.nl (Separate several email addresses with spaces)

Apply rule if recipient: Is exactly — one of the above addresses

Action

○ Continue with next rule for the matching address

○ Do not check further rules for the matching address

● Use the following OpenPGP keys:

(none - no encryption)

Defaults for ...

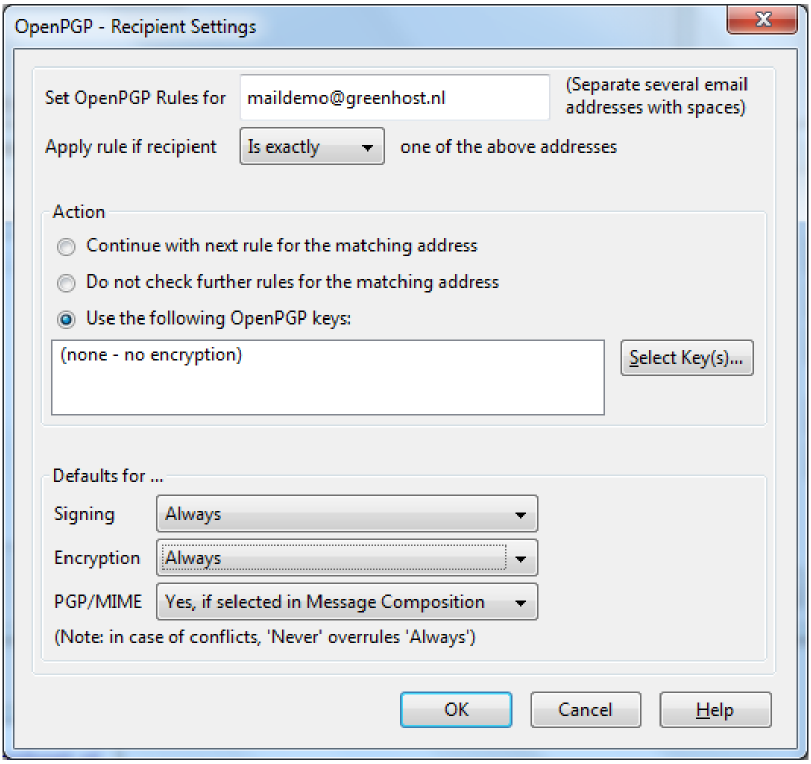
Signing: Yes, if selected in Message Composition

Encryption: Yes, if selected in Message Composition

PGP/MIME: Yes, if selected in Message Composition

(Note: in case of conflicts, 'Never' overrules 'Always')

Now we will set the encryption defaults by using the drop-downs below. For Signing select 'Always'. For Encryption also select 'Always'.



OpenPGP - Recipient Settings

Set OpenPGP Rules for: maildemo@greenhost.nl (Separate several email addresses with spaces)

Apply rule if recipient: Is exactly one of the above addresses

Action

○ Continue with next rule for the matching address

○ Do not check further rules for the matching address

● Use the following OpenPGP keys:

(none - no encryption)

Defaults for ...

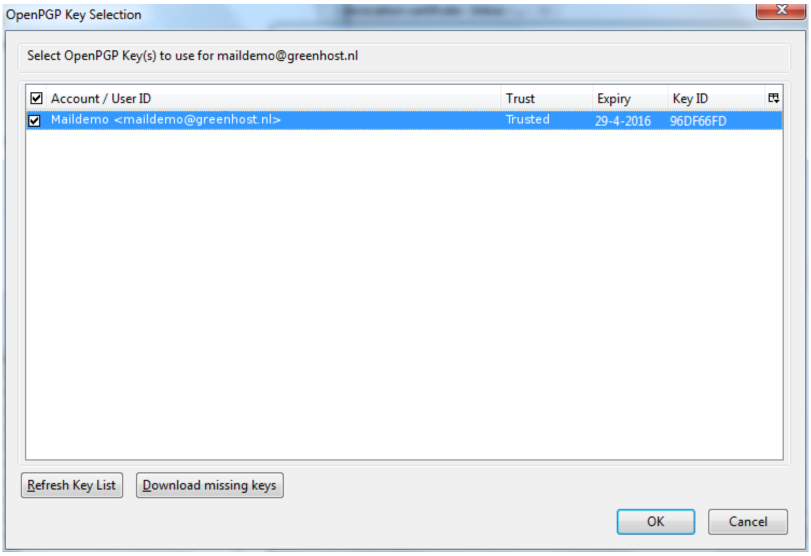
Signing: Always

Encryption: Always

PGP/MIME: Yes, if selected in Message Composition

(Note: in case of conflicts, 'Never' overrules 'Always')

Finally we have to select the *public key* of the recipient, with which to encrypt our messages. Do not forget this important step, otherwise the e-mail will not be encrypted. Click on the button labeled 'Select Key(s)...'. The key selection window will show up. The most obvious key will be selected by default. In the example below, we only have one public key available. We can select keys by clicking on the small box next to the address. Then we click 'OK' and close all relevant windows and we are finished.


OpenPGP Key Selection

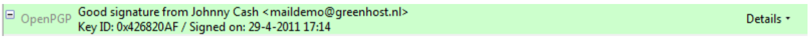
Select OpenPGP Key(s) to use for maildemo@greenhost.nl

☑ Account / User ID	Trust	Expiry	Key ID
☑ Maildemo <maildemo@greenhost.nl>	Trusted	29-4-2016	96DF66FD

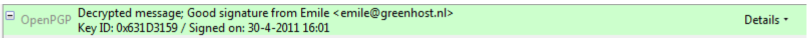
Verifying incoming e-mails

Decrypting email messages sent to you will be fully automatic and transparent. But it is obviously important to see whether or not a message to you *has* in fact been encrypted or signed. This information is available by looking at the special bar above the message body.

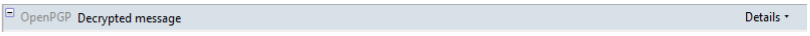
A valid signature will be recognized by a green bar above the mail message like the example image below.


Good signature from Johnny Cash <maildemo@greenhost.nl>
Key ID: 0x426820AF / Signed on: 29-4-2011 17:14

The last example message was signed but *not* encrypted. If the message had been encrypted, it would show like this:

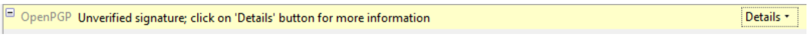

Decrypted message; Good signature from Emile <emile@greenhost.nl>
Key ID: 0x631D3159 / Signed on: 30-4-2011 16:01

When a message which has been encrypted, but *not* signed, it could have been a forgery by someone. The status bar will become gray like in the image below and tells you that while the message was sent securely (encrypted), the sender could have been someone else than the person behind the email address you will see in the 'From' header. The signature is neccessaty to verify the real sender of the message. Of course it is perfectly possible that you have published your public key on the Internet and you allow people to send you emails anonymously. But is it also possible that someone is trying to impersonate one of your friends.



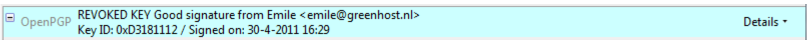
Decrypted message

Similarly if you receive a *signed* email from somebody you know, and you have this persons public key, but still the status bar becomes yellow and displays a warning message, it is likely that someone is attempting to send you forged emails!



Unverified signature; click on 'Details' button for more information

Sometimes secret keys get stolen or lost. The owner of the key will inform his friends and send them a so-called revocation certificate (more explanation of this in the next paragraph). Revocation means that we no longer trust the old key. The thief may afterwards still try his luck and send you a falsely signed mail message. The status bar will now look like this:



REVOKED KEY Good signature from Emile <emile@greenhost.nl>
Key ID: 0xD3181112 / Signed on: 30-4-2011 16:29

Strangely enough Thunderbird in this situation will still display a green status bar! It is important to look at the contents of the status bar in order to understand the encryption aspects of a message. GPG allows for strong security and privacy, but only if you are familiar with its use and concepts. Pay attention to warnings in the status bar.

Revoking your GPG key-pair

Your secret key has been stolen by somebody. Your harddisk crashed and you have lost all your data. If your key is lost, you can no longer decrypt messages. If your key has been stolen, somebody else can decrypt your communication. You need to make a new set of keys. The process of creating keys, using the OpenPGP wizard in Thunderbird, has been described in this manual. But first you want to tell the world that your old public key is now worthless, or even dangerous to use.

What to do when you have lost your secret key, or forgot your passphrase

During the creation of your key-pair, the OpenPGP wizard offered you the possibility to create a so-called revocation certificate. This is a special file you send to others in the advent you have to disable your key. If you have a copy of this file, sending the revocation key is simply sending the file as an attachment to all your friends. You can no longer send signed mails (obviously, because you have lost your secret key). That doesn't matter. Send it as a normal mail. The revocation certificate file could only have been created by the owner of the secret key and proofs he or she wants to revoke it. That's why it should normally be kept hidden from others.

If you do not have the revocation certificate, there exists no other option than for you to contact your friends personally and convince them your key is lost and that they should no longer trust it.

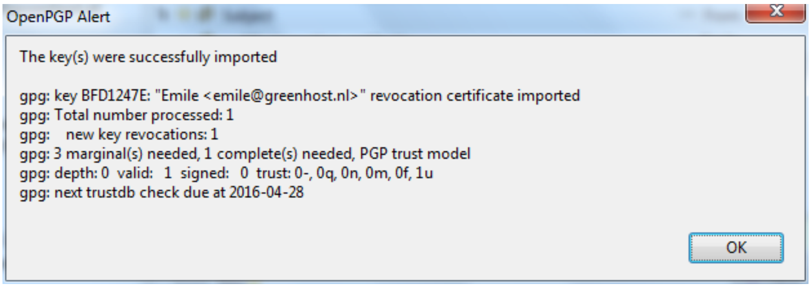
What to do when your secret key has been stolen, or compromised

If you have reason to believe your secret key has been compromised, or worse your secret key *and* passphrase, it is very important to contact others that they should stop sending you encrypted messages. With your secret key, other persons will be able to break the encryption of your e-mail messages if they also have your passphrase. This is also true for those messages you have send in the past. Cracking the passphrase is not trivial, but it may be possible if the party has lots of resources, like a state or a big organization for example, or if your passphrase is too weak. In any case you should assume the worst and assume your passphrase may have been compromised. Send a revocation certificate file to all your friends or contact them personally and inform them of the situation.

Even after you have revoked your old key pair, the stolen key may still be used to decrypt your previous correspondence. You should consider other ways to protect that old correspondence, for instance by re-encrypting it with a new key. The latter operation will not be discussed in this manual. If you are uncertain you should seek assistance from experts or look up more information on the web.

Receiving a revocation certificate

If one of your friends sends you a revocation certificate, s/he asks you to distrust his public key from now on. You should always accept such a request and 'import' the certificate to disable their key. The process of accepting a revocation certificate is exactly the same as accepting a public key, as has already been described in the chapter. Thunderbird will ask you if you want to import the 'OpenPGP key file'. Once you have done so, a confirmation pop-up should be displayed like below.



The key(s) were successfully imported

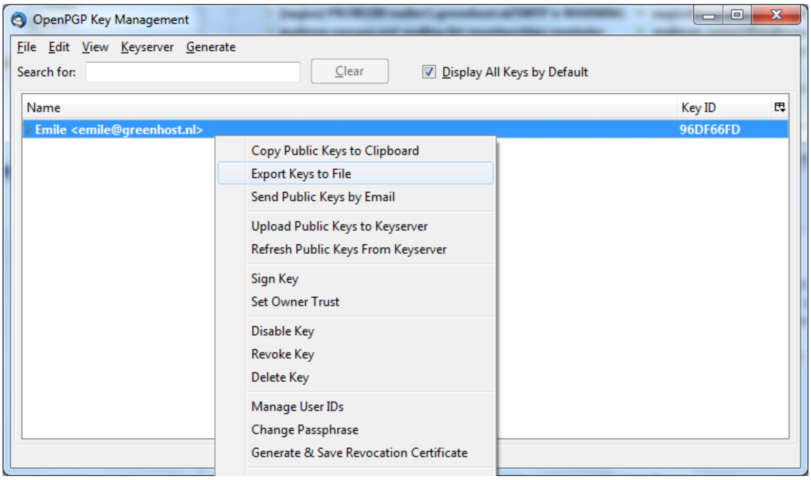
```
gpg: key BFD1247E: "Emile <emile@greenhost.nl>" revocation certificate imported
gpg: Total number processed: 1
gpg:    new key revocations: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:  1  signed:  0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-04-28
```

Preparing for the worst: backup your keys

Your keys are usually stored on your hard disk as normal files. They may get lost if your computer gets damaged. It is strongly advised to keep a backup of your keys in a safe place, like a vault. Making a a backup of your secret key has another security advantage as well. Whenever you fear your laptop or computer is in immediate danger of being confiscated, you can safely delete your key-pair. Your email will be rendered unreadable immediately. At a later stage, you can retrieve your keys from the vault and re-import them in Thunderbird.

To make a backup of your key-pair, first head to the key manager by using the Thunderbird menu and click on **OpenPGP > Key Management**.

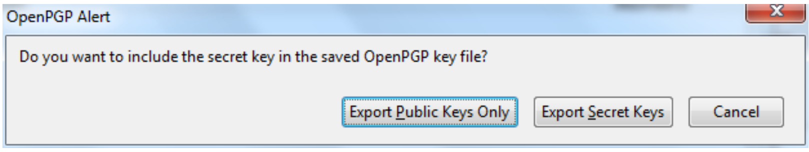
You need to have selected the 'Display All Keys by Default' option to get a list of all your keys. Lookup your own email address in the list and right click on the address. A selection window will appear with some options. Select the option 'Export Keys to File'.


OpenPGP Key Management
File
Edit
View
Keyserver
Generate
Search for:
Clear
Display All Keys by Default
Name
Key ID
Copy Public Keys to Clipboard
Export Keys to File
Send Public Keys by Email
Upload Public Keys to Keyserver
Refresh Public Keys From Keyserver
Sign Key
Set Owner Trust
Disable Key
Revoke Key
Delete Key
Manage User IDs
Change Passphrase
Generate & Save Revocation Certificate

☑ Display All Keys by Default

Name	Key ID
Emile <emile@greenhost.nl>	96DF66FD

Now we will save the key-pair to a file. Thunderbird asks us if we want to include the secret key as well. We do want to include the secret key, therefore we select 'Export Secret Keys'.



Do you want to include the secret key in the saved OpenPGP key file?

Finally Thunderbird asks us for the location of the key file. You can store the file anywhere you like, network disk, USB-stick. Just remember to hide it away from other people.

Further reading

More documentation on using GPG with Thunderbird can be found on the website of the Enigmail plugin. The Enigmail handbook is the guide you will want to use.

http://enigmail.mozdev.org/documentation/handbook.php.html

WEBMAIL AND GPG

The only safe way of encrypting email inside of the browser window is to encypt it outside and then copy&paste the encrypted text into the browser window.

For example, write the text in a text editor like gedit, vim or kate and save it as .txt file (in this example "message.txt". Then type

```
gpg -ase -r the.recipients.email.address@or.gpg.id
-r your.gpg.id message.txt
```

A new file called "message.asc" will be created. It contains the encrypted message and can thus be either attached to an email or its content safely copy&-pasted into the browser window.

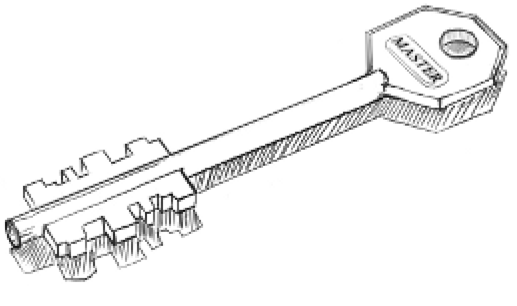
To decrypt a message from the browser window, simply type

```
gpg
```

into the commandline and hit Enter. Then copy&paste the message to be decrpyted into the commandline window and after being asked for your passphrase hit Ctrl+D (this enters a end-of-file character and prompts gpg to output the cleartext message).

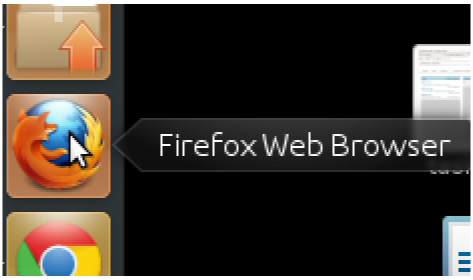
If using the commandline seems too cumbersome to you, you might consider installing a helper application like gpgApplet, kgpg or whatever application ships with your operating system.

Safer Browsing

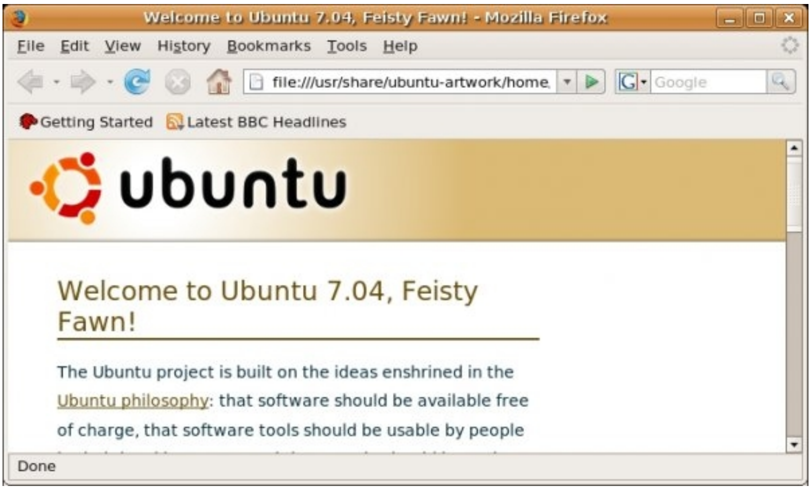


Accessing Firefox on Ubuntu

Firefox is already installed on Ubuntu by default. To open it, click on the Unity side bar where you see the Firefox icon:



Firefox starts and a welcome window opens:

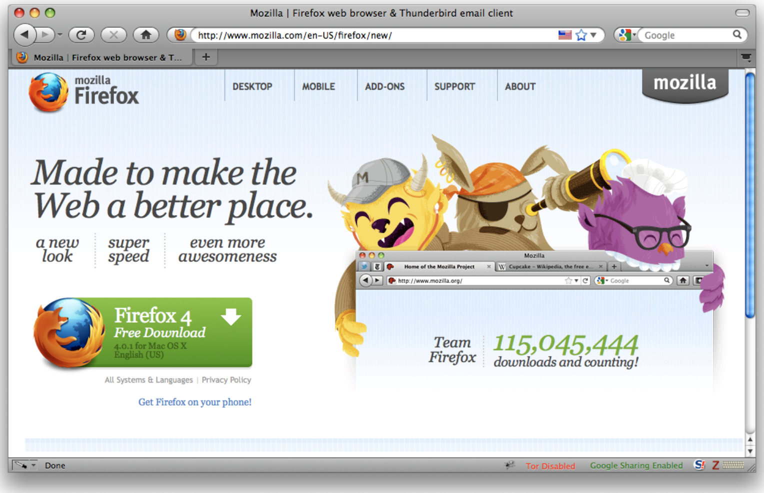

Welcome to Ubuntu 7.04, Feisty Fawn! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///usr/share/ubuntu-artwork/home
Google
Getting Started
Latest BBC Headlines
ubuntu
Done

Welcome to Ubuntu 7.04, Feisty Fawn!

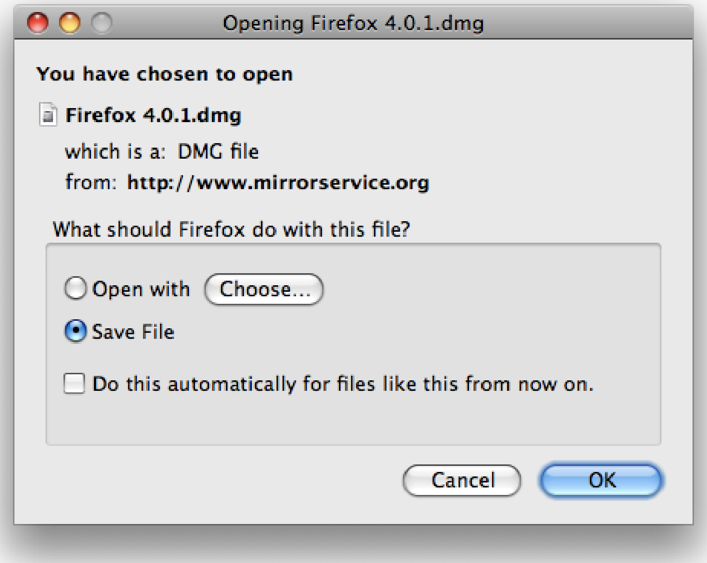
The Ubuntu project is built on the ideas enshrined in the Ubuntu philosophy: that software should be available free of charge, that software tools should be usable by people

Installing on Mac OS X

1. To download Firefox, visit https://www.mozilla.org/firefox and click on the big green button labeled "Firefox Free Download". The download should start automatically, if it does not, click the link to download it manually.


Mozilla | Firefox web browser & Thunderbird email client
http://www.mozilla.com/en-US/firefox/new/
Google
Mozilla | Firefox web browser & T...
mozilla Firefox
DESKTOP
MOBILE
ADD-ONS
SUPPORT
ABOUT
mozilla
Made to make the Web a better place.
a new look
super speed
even more awesomeness
Firefox 4 Free Download
4.0.1 for Mac OS X English (US)
All Systems & Languages | Privacy Policy
Get Firefox on your phone!
Team Firefox
115,045,444 downloads and counting!
Done
Tor Disabled
Google Sharing Enabled

2. When prompted, click **OK**.


Opening Firefox 4.0.1.dmg

You have chosen to open

Firefox 4.0.1.dmg

which is a: DMG file

from: http://www.mirrorservice.org

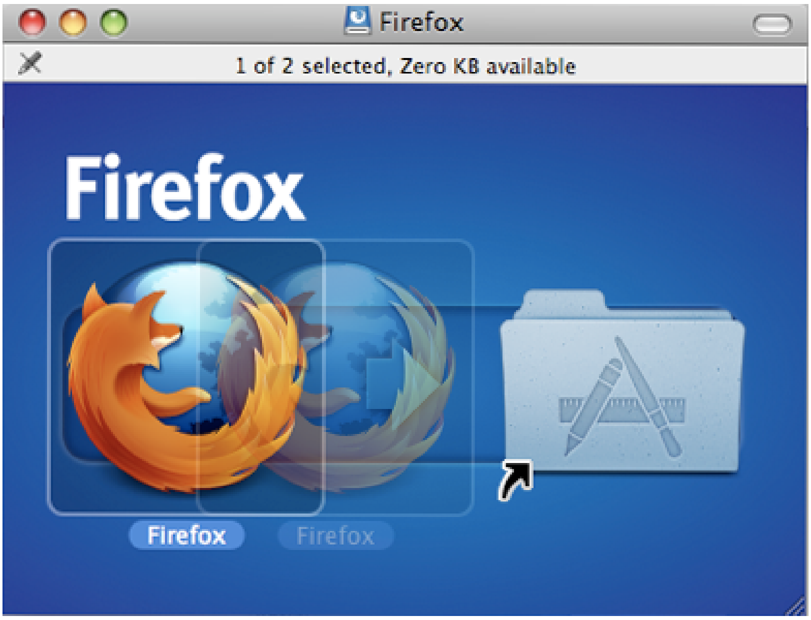
What should Firefox do with this file?

○ Open with Choose...

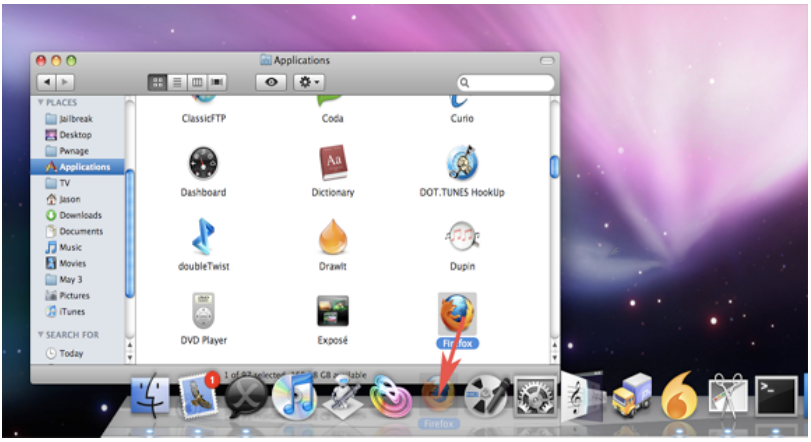
● Save File

□ Do this automatically for files like this from now on.

Once the download is complete a window similar to this appears:

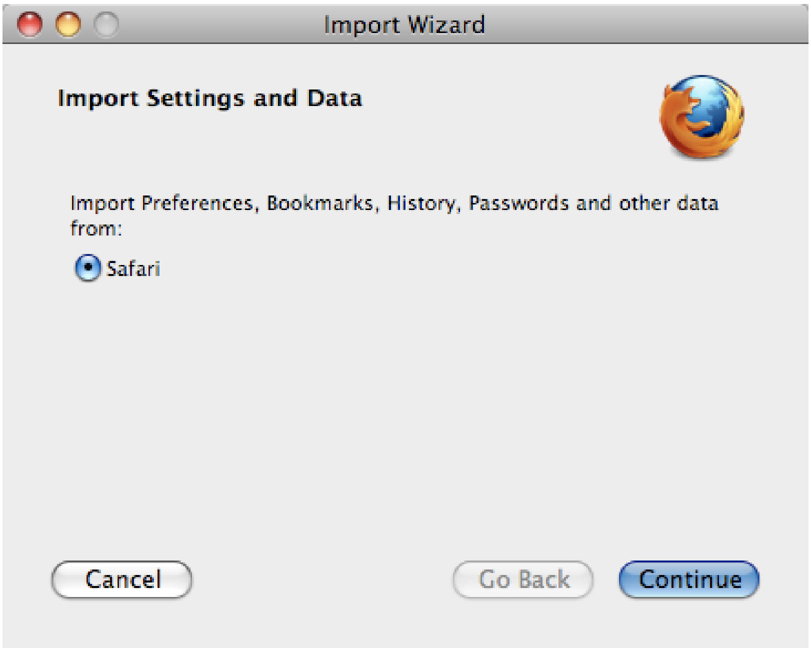


3. Click and drag the **Firefox** icon on top of the **Applications** icon. This starts copying the program files to the Applications directory on your computer.
4. When the installation is finished, close the two small Firefox windows.
5. Eject the Firefox disk image. If this does not work by normal means, select the disk image icon and then, in the Finder menu, select *File > Eject Firefox.*
6. Now, open the **Applications** directory and drag the **Firefox** icon to the dock:



7. Click the **Firefox** icon in the Dock to start Firefox. The Import Wizard di-

alog box appears:



Import Wizard

Import Settings and Data

Import Preferences, Bookmarks, History, Passwords and other data from:

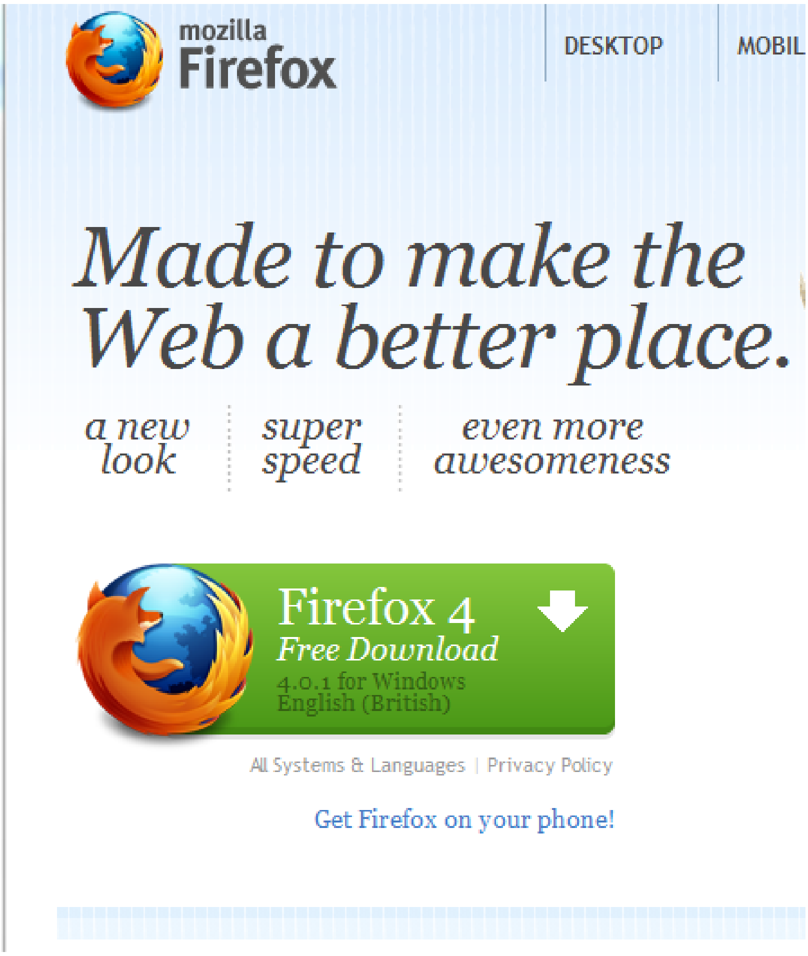
● Safari

8. To import your bookmarks, passwords and other data from Safari, click **Continue**. If you don't want to import anything, just select **Cancel**.

Congratulations, you are now ready to use Firefox!

Installing Firefox on Windows

1. To download Firefox, visit https://www.mozilla.com/firefox/.



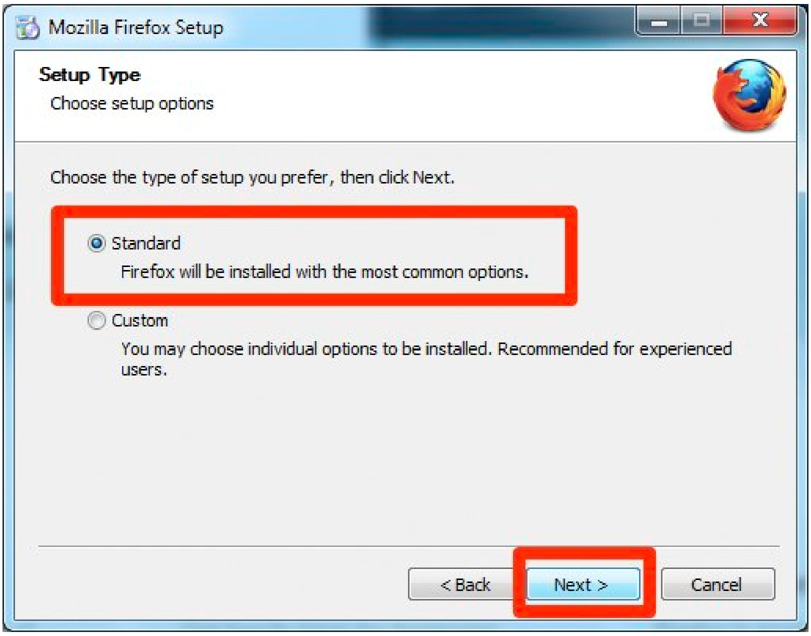
2. Click the download button and the installation file will begin to download to your computer.
3. Once the download is complete, double-click the installation file to start the Firefox installation wizard.

   - If you are running Windows Vista, you may get a User Account Control prompt. In this case, allow the setup to run by clicking **Continue**.
   - If you are running Windows 7, you will be asked whether to

allow Firefox to make changes to your computer. Click on **Yes.**

A welcome screen appears.

4. Click 'Next' to continue. You will be asked if you would like the standard installation, or whether you would like to customize it. Choose the standard installation and click 'Next'.



Setup Type

Choose setup options

Choose the type of setup you prefer, then click Next.

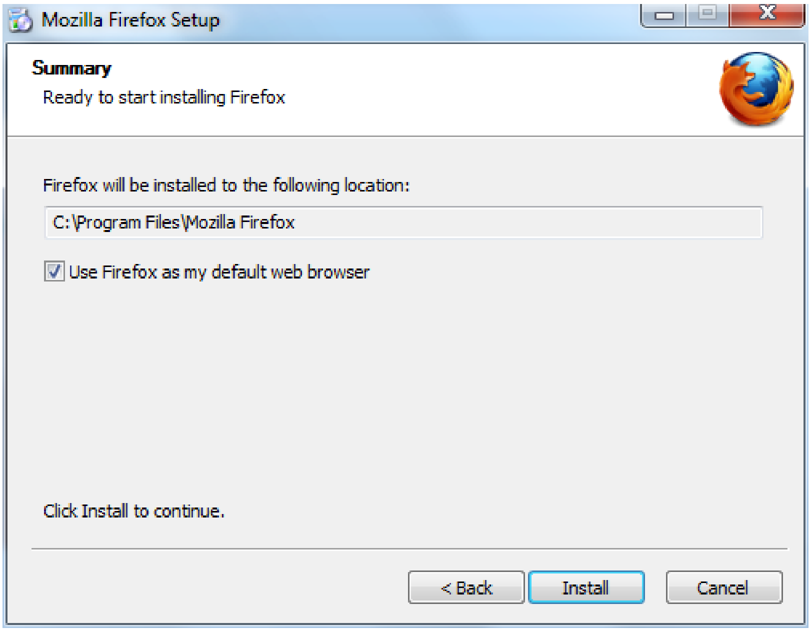
● Standard

Firefox will be installed with the most common options.

○ Custom

You may choose individual options to be installed. Recommended for experienced users.

5. You will be asked if you want Firefox to be your default browser. This is recommended.



Mozilla Firefox Setup

Summary

Ready to start installing Firefox

Firefox will be installed to the following location:

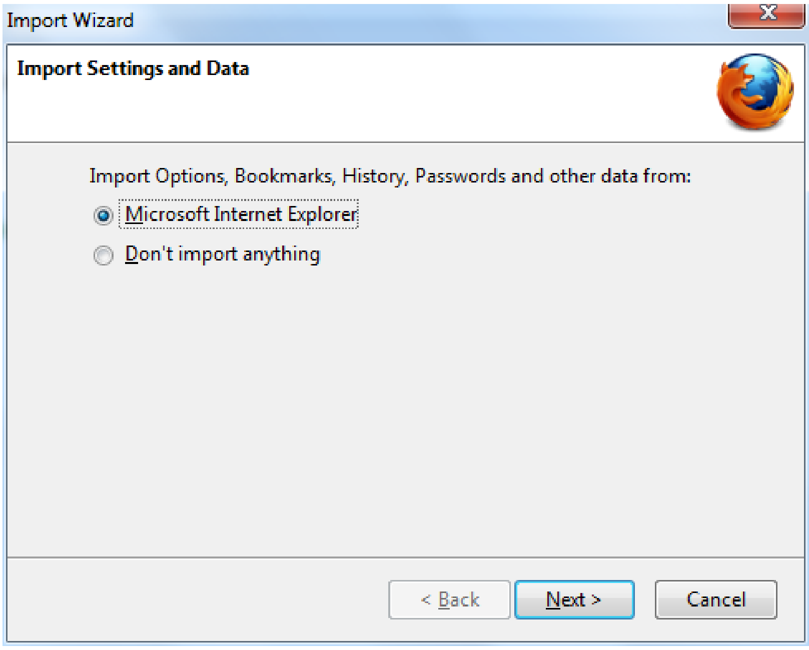
C:\Program Files\Mozilla Firefox

☑ Use Firefox as my default web browser

Click Install to continue.

6. Click **Install**.

7. To import your bookmarks and other data from other browsers (for example Internet Explorer), click **Continue**. If you don't want to import anything, just select **Cancel**.



Import Wizard

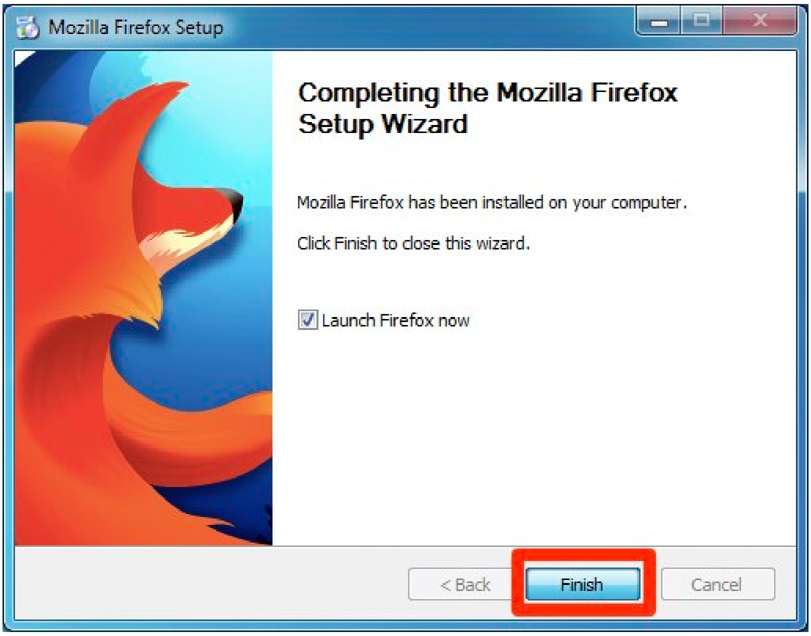
Import Settings and Data

Import Options, Bookmarks, History, Passwords and other data from:

● Microsoft Internet Explorer

○ Don't import anything

8. Once Firefox has been installed, click **Finish** to close the setup wizard.



Mozilla Firefox Setup

Completing the Mozilla Firefox Setup Wizard

Mozilla Firefox has been installed on your computer.

Click Finish to close this wizard.

☑ Launch Firefox now

If the **Launch Firefox now** check box is checked, Firefox will start after you click **Finish**. Otherwise you can launch Firefox through the start menu.

Windows Vista Users:

If at any time throughout the installation process you are prompted with a User Account Control (UAC) window, press Continue, Allow, or Accept.

Troubleshooting

If you have problems starting Firefox, see https://support.mozilla.com/kb/Firefox+will+not+start)

Extending Firefox

When you first download and install Firefox, it can handle basic browser tasks immediately. You can also add extra capabilities or change the way Firefox behaves by installing add-ons, small additions that extend Firefox's power.

Firefox extensions can pimp your browser, but they can also collect and transmit information about you. Before you install any add-on, keep in mind to choose add-ons from trusted sources. Otherwise, an add-on might share information about you without your knowing, keep a record on the sites you have visited, or even harm your computer.

There are several kinds of add-ons:

- *Extensions* add functionality to Firefox
- *Themes* change the appearance of Firefox.
- *Plugins* help Firefox handle things it normally can't process (i.e. Flash movies, Java applications).

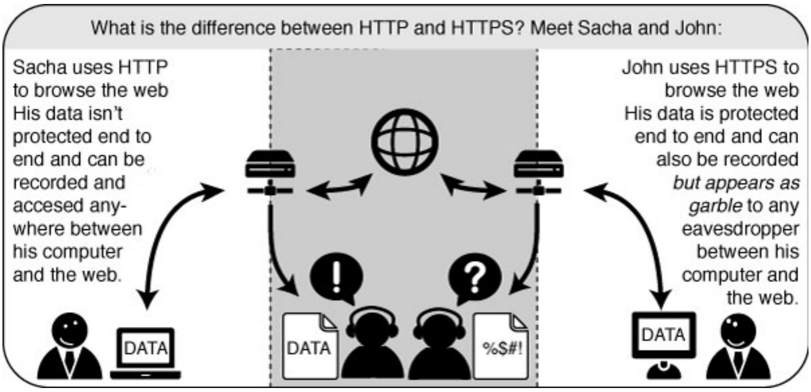
For the topics covered in this book we are only going to need extensions. We will look at some add-ons that are particularly relevant for dealing with Internet security. The variety of available extensions is enormous. You can add dictionaries for different languages, track the weather in other countries, get suggestions for Web sites that are similar to the one you are currently viewing, and much more. Firefox keeps a list of current extensions on its site (https://addons.mozilla.org/firefox), or you can browse them by category at https://addons.mozilla.org/firefox/browse.

Caution: We recommend that you never install an add-on for Firefox unless it is available from the Firefox add-on pages. You should also never install Firefox unless you get the installation files from a trusted source. It is important to note that using Firefox on someone else's computer or in an Internet caf increases your potential vulnerability. Know that you can take Firefox on a CD or USB-stick (check our chapter on that issue).

While no tool can protect you completely against all threats to your online privacy and security, the Firefox extensions described in this chapter can significantly reduce your exposure to the most common ones, and increase your chances of remaining anonymous.

HTTPS Everywhere

HTTP is considered unsafe, because communication is transmitted in plain text. Many sites on the Web offer some support for encryption over HTTPS, but make it difficult to use. For instance, they may connect you to HTTP by default, even when HTTPS is available, or they may fill encrypted pages with links that go back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS. Although the extension is called "HTTPS Everywhere", it only activates HTTPS on a particular list of sites and can only use HTTPS on sites that have chosen to support it. It cannot make your connection to a site secure if that site does not offer HTTPS as an option.


What is the difference between HTTP and HTTPS? Meet Sacha and John:
Sacha uses HTTP to browse the web His data isn't protected end to end and can be recorded and accesed anywhere between his computer and the web.
John uses HTTPS to browse the web His data is protected end to end and can also be recorded *but appears as garble* to any eavesdropper between his computer and the web.
DATA
DATA
%$#!
DATA

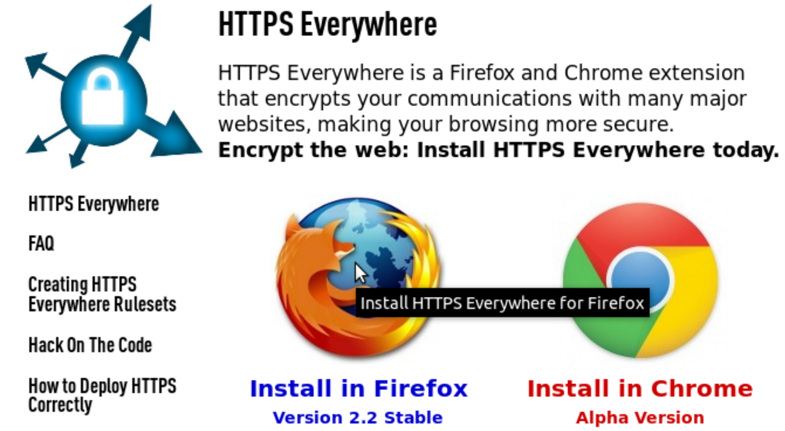
Please note that some of those sites still include a lot of content, such as images or icons, from third party domains that are not available over HTTPS. As always, if the browser's lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis. However, the effort required to monitor your browsing should still be usefully increased.

Some Web sites (such as Gmail) provide HTTPS support automatically, but using HTTPS Everywhere will also protect you from TLS/SSL-stripping attacks, in which an attacker hides the HTTPS version of the site from your computer if you initially try to access the HTTP version.

Additional information can be found at: https://www.eff.org/https-everywhere.

Installation

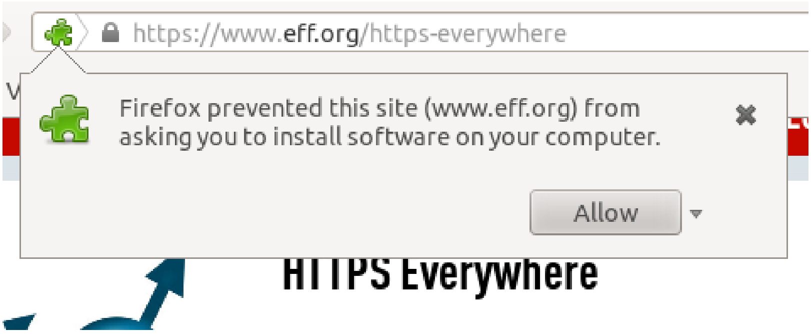
First, download the HTTPS Everywhere extension from the official Web site: https://www.eff.org/https-everywhere



HTTPS Everywhere

HTTPS Everywhere is a Firefox and Chrome extension that encrypts your communications with many major websites, making your browsing more secure.
Encrypt the web: Install HTTPS Everywhere today.

Select the newest release. In the example below, version 2.2 of HTTPS Everywhere was used. (A newer version may be available now.)

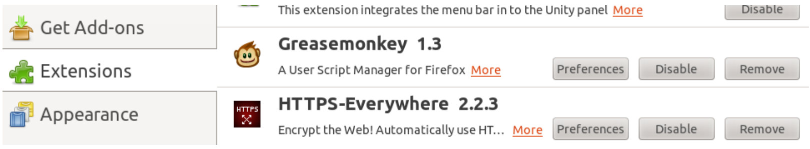


Firefox prevented this site (www.eff.org) from asking you to install software on your computer.

Click on "Allow". You will then have to restart Firefox by clicking on the "Restart Now" button. HTTPS Everywhere is now installed.

Configuration

To access the HTTPS Everywhere settings panel in Firefox 4 (Linux), click on the Tools menu at the top of your screen and then select Add-ons. (Note that in different versions of Firefox and different operating systems, the Add-ons Manager may be located in different places in the interface.)



This extension integrates the menu bar in to the Unity panel More

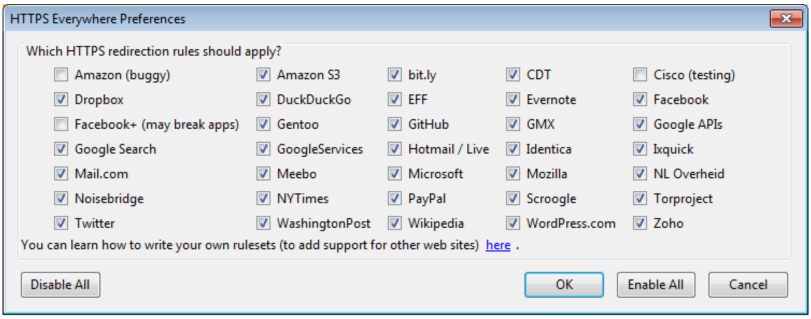
Greasemonkey 1.3

A User Script Manager for Firefox More

HTTPS-Everywhere 2.2.3

Encrypt the Web! Automatically use HT... More

Click on the Preferences button.



HTTPS Everywhere Preferences

Which HTTPS redirection rules should apply?

☐ Amazon (buggy)
☑ Dropbox
☐ Facebook+ (may break apps)
☑ Google Search
☑ Mail.com
☑ Noisebridge
☑ Twitter

☑ Amazon S3
☑ DuckDuckGo
☑ Gentoo
☑ GoogleServices
☑ Meebo
☑ NYTimes
☑ WashingtonPost

☑ bit.ly
☑ EFF
☑ GitHub
☑ Hotmail / Live
☑ Microsoft
☑ PayPal
☑ Wikipedia

☑ CDT
☑ Evernote
☑ GMX
☑ Identica
☑ Mozilla
☑ Scroogle
☑ WordPress.com

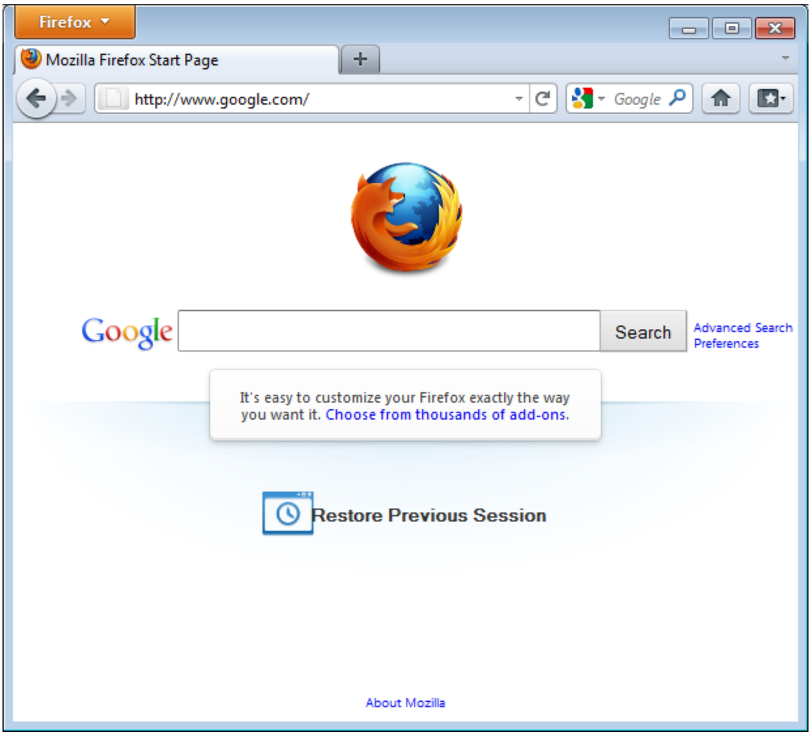
☐ Cisco (testing)
☑ Facebook
☑ Google APIs
☑ Ixquick
☑ NL Overheid
☑ Torproject
☑ Zoho

You can learn how to write your own rulesets (to add support for other web sites) here .

A list of all supported Web sites where HTTPS redirection rules should be applied will be displayed. If you have problems with a specific redirection rule, you can uncheck it here. In that case, HTTPS Everywhere will no longer modify your connections to that specific site.

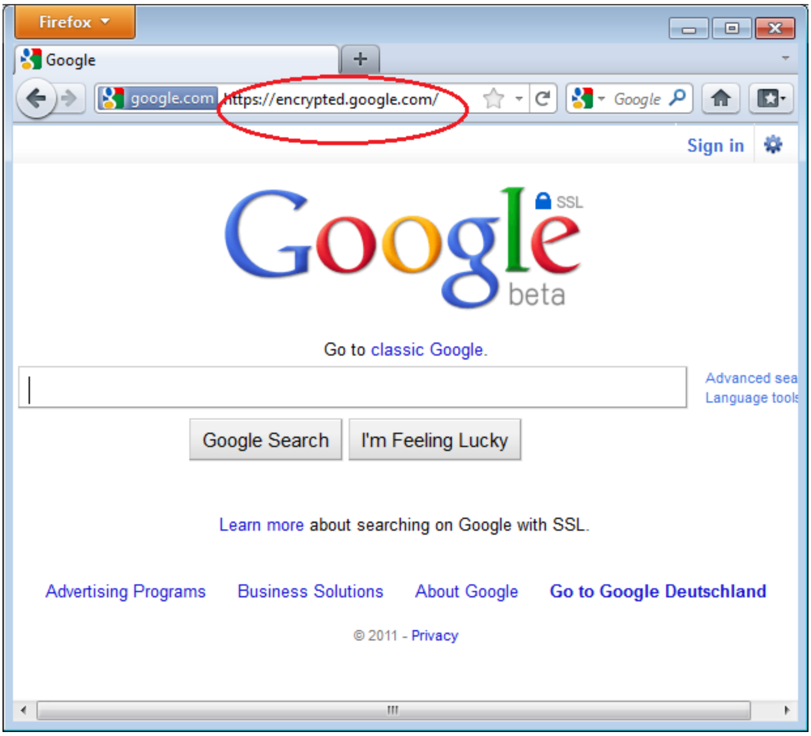
Usage

Once enabled and configured, HTTPS Everywhere is very easy and transparent to use. Type an insecure HTTP URL (for example, http://www.google.com).



It's easy to customize your Firefox exactly the way you want it. Choose from thousands of add-ons.

Press Enter. You will be automatically redirected to the secure HTTPS encrypted Web site (in this example: https://encrypted.google.com). No other action is needed.



https://encrypted.google.com/

Go to classic Google.

Learn more about searching on Google with SSL.

If networks block HTTPS

Your network operator may decide to block the secure versions of Web sites in order to increase its ability to spy on what you do. In such cases, HTTPS Everywhere could prevent you from using these sites because it forces your browser to use only the secure version of these sites, never the insecure version. (For example, we heard about an airport WiFi network where all HTTP connections were permitted, but not HTTPS connections. Perhaps the WiFi operators were interested in watching what users did. At that airport, users with HTTPS Everywhere were not able to use certain Web sites unless they temporarily disabled HTTPS Everywhere.)

In this scenario, you might choose to use HTTPS Everywhere together with a circumvention technology such as Tor or a VPN in order to bypass the network's blocking of secure access to Web sites.

Adding support for additional sites in HTTPS Everywhere

You can add your own rules to the HTTPS Everywhere add-on for your favorite Web sites. You can find out how to do that at: https://www.eff.org/https-everywhere/rulesets. The benefit of adding rules is that they teach HTTPS Everywhere how to ensure that your access to these sites is secure. But remember: HTTPS Everywhere does *not* allow you to access sites securely unless the site operators have already chosen to make their sites available through HTTPS. If a site does not support HTTPS, there is no benefit to adding a ruleset for it.

If you are managing a Web site and have made an HTTPS version of the site available, a good practice would be to submit your Web site to the official HTTPS Everywhere release.

Adblock Plus

Adblock Plus (http://www.adblockplus.org) is mainly known for blocking advertisements on websites. But it also can be used to block other content that may try to track you. To keep current with the latest threats, Adblock Plus relies on blacklists maintained by volunteers.

Extra Geek info: How does Adblock Plus block addresses?

The hard work here is actually done by Gecko, the engine on top of which Firefox, Thunderbird and other applications are built. It allows something called "content policies". A content policy is simply a JavaScript (or C++) object that gets called whenever the browser needs to load something. It can then look at the address that should be loaded and some other data and decide whether it should be allowed. There is a number of built-in content policies (when you define which sites shouldn't be allowed to load images in Firefox or SeaMonkey, you are actually configuring one of these built-in content policies) and any extension can register one. So all that Adblock Plus has to do is to register its content policy, other than that there is only application logic to decide which addresses to block and user interface code to allow configuration of filters.

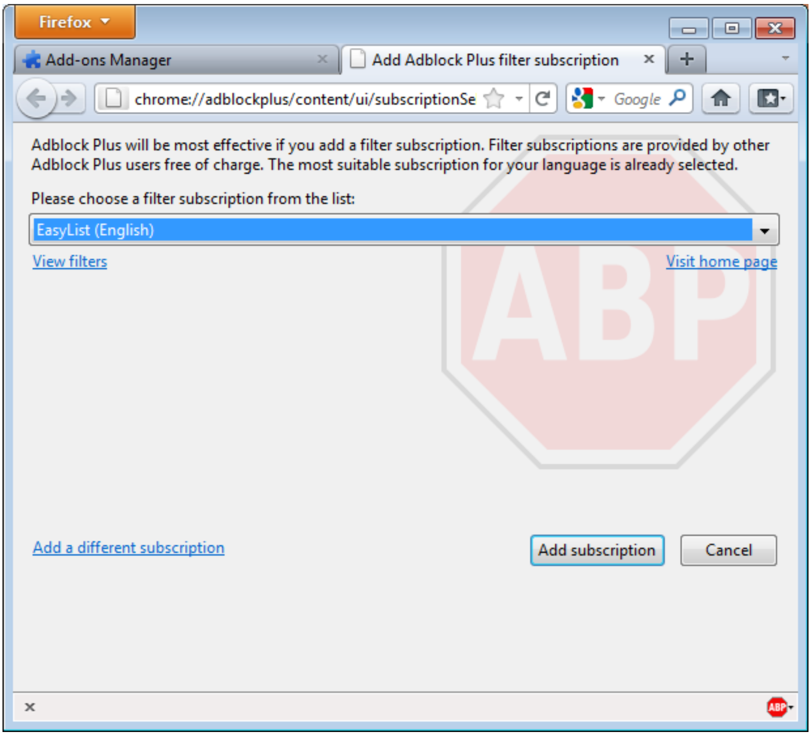
Getting started with Adblock Plus

Once you have Firefox installed:

1. Download the latest version of Adblock Plus from the Add-On database of Firefox
2. Confirm that your want Adblock Plus by clicking "Install Now".
3. After Adblock Plus has been installed, Firefox will ask to restart.

Choosing a filter subscription

Adblock Plus by itself doesn't do anything. It can see each element that a Web site attempts to load, but it doesn't know which ones should be blocked. This is what Adblock's filters are for. After restarting Firefox, you will be asked to choose a filter subscription (free).



chrome://adblockplus/content/ui/subscriptionSe

Adblock Plus will be most effective if you add a filter subscription. Filter subscriptions are provided by other Adblock Plus users free of charge. The most suitable subscription for your language is already selected.

Please choose a filter subscription from the list:

EasyList (English)

Which filter subscription should you choose? Adblock Plus offers a few in its dropdown menu and you may wish to learn about the strengths of each. A good filter to start protecting your privacy is EasyList (also available at http://easylist.adblockplus.org/en).

As tempting as it may seem, don't add as many subscriptions as you can get, since some may overlap, resulting in unexpected outcomes. EasyList (mainly targeted at English-language sites) works well with other EasyList extensions (such as region-specific lists like RuAdList or thematic lists like EasyPrivacy). But it collides with Fanboy's List (another list with main focus on English-language sites).

You can always change your filter subscriptions at any time within preferences. Once you've made your changes, click OK.

Creating personalized filters

AdBlock Plus also lets you create your own filters, if you are so inclined. To add a filter, start with Adblock Plus preferences and click on "Add Filter" at the bottom left corner of the window. Personalized filters may not replace the benefits of well-maintained blacklists like EasyList, but they're very useful for blocking specific content that isn't covered in the public lists. For example, if you wanted to prevent interaction with Facebook from other Web sites, you could add the following filter:

```
||facebook.*$domain=~facebook.com|~127.0.0.1
```

The first part (||facebook.*) will initially block everything coming from Facebook's domain. The second part ($domain=~facebook.com|~127.0.0.1) is an exception that tells the filter to allow Facebook requests only when you are in Facebook or if the Facebook requests come from 127.0.0.1 (your own computer) in order to keep certain features of Facebook working.

A guide on how to create your own Adblock Plus filters can be found at http://adblockplus.org/en/filters.

Enabling and disabling AdBlock Plus for specific elements or Web sites

You can see the elements identified by AdBlock Plus by clicking on the ABP icon in your browser (usually next to the search bar) and selecting "Open blockable items". A window at the bottom of your browser will let you enable or disable each element on a case-by-case basis. Alternatively, you can disable AdBlock Plus for a specific domain or page by clicking on the ABP icon and ticking the option "Disable on [domain name]" or "Disable on this page only".

Other extensions that can improve your security

Below is a short list of extensions that are not covered in this book but are helpful to further protect you.

Flagfox - puts a flag in the location bar telling you where the server you are visiting is most probably located. https://addons.mozilla.org/en-US/firefox/addon/flagfox/

BetterPrivacy - manages "cookies" used to track you while visiting websites. Cookies are small bits of information stored in your browser. Some of them are used to track the sites you are visiting by advertisers. https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/

GoogleSharing - If you are worried that google knows your search history, this extension will help you prevent that. https://addons.mozilla.org/en-us/firefox/addon/googlesharing/

Extending Chrome

Chrome is Google's browser. Here are some useful tips and extensions:

Disabling Instant Search

Chrome can search as you type. The advantage of this is that you get search suggestions and can use Google's predictions - but the disadvantage is that every character you type is sent to Google's servers, where it may be logged.

To disable, open Chrome's settings by clicking the menu button at the right of
the address bar and clicking Settings. Or, simply type `chrome://settings/` in your address bar.

Ensure that the *Enable Instant for faster searching (omnibox input may be logged)* checkbox is unchecked.

AdBlock for Chrome

Just like Firefox, AdBlock removes ads. Install it from Chrome Webstore.

HTTPS Everywhere

Forces encrypted https connections wherever possible. Installation link can be found on the EFFs *HTTPS Everywhere* homepage (https://www.eff.org/https-everywhere).

PrivacyFix

PrivacyFix (beta) gives you a dashboard view of your privacy settings on Facebook and Google, as well as Do-Not-Track headers and tracking cookies. It
provides links to quickly change these privacy settings without digging through
many drilldown pages. Install from the Chrome Webstore.

Proxy Settings

A proxy server allows you to reach a Web site or other Internet location even when direct access is blocked in your country or by your ISP. There are many different kinds of proxies, including:

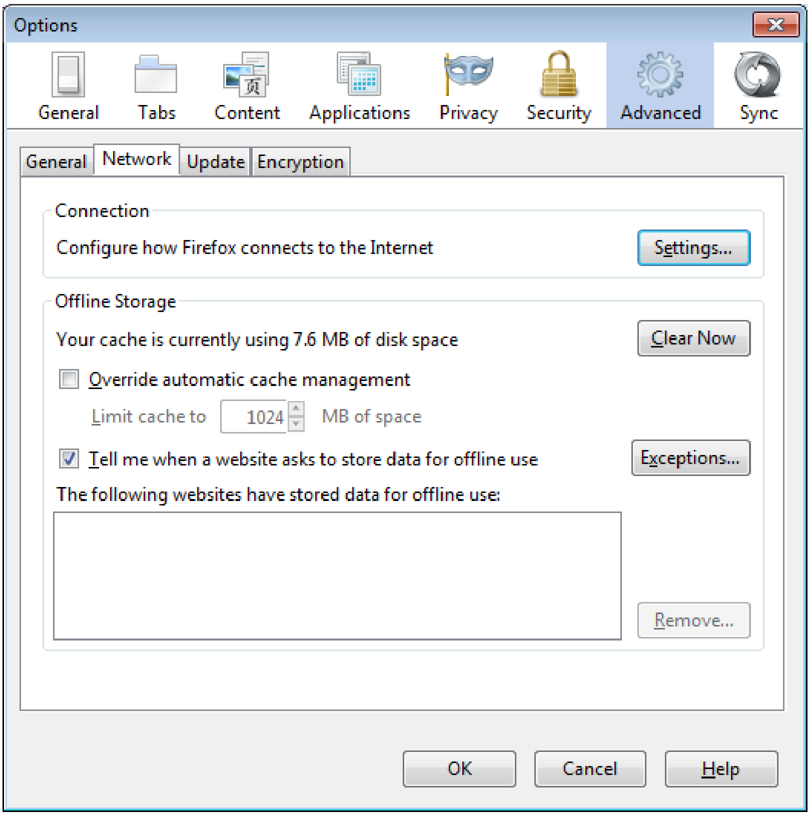
- Web proxies, which only require that you know the proxy Web site's address. A Web proxy URL may look like http://www.example.com/cgi-bin/nph-proxy.cgi
- HTTP proxies, which require that you modify your Browser settings. HTTP proxies only work for Web content. You may get the information about a HTTP proxy in the format "proxy.example.com:3128" or "192.168.0.1:8080".
- SOCKS proxies, which also require that you modify your Browser settings. SOCKS proxies work for many different Internet applications, including e-mail and instant messaging tools. The SOCKS proxy information looks just like HTTP proxy information.

You can use a Web proxy directly without any configuration by typing in the URL. The HTTP and SOCKS proxies, however, have to be configured in your Web browser.

Default Firefox proxy configuration

In Firefox you can change the settings for using a proxy. You'll need to open the Options or Preferences window of Firefox. You can find this in the menu, by clicking on the top of the Window and selecting **Edit** > **Preferences** on Linux or **Tools** > **Options** on Windows.

Go to the Network section and open the Advanced tab.



Connection

Configure how Firefox connects to the Internet

Offline Storage

Your cache is currently using 7.6 MB of disk space

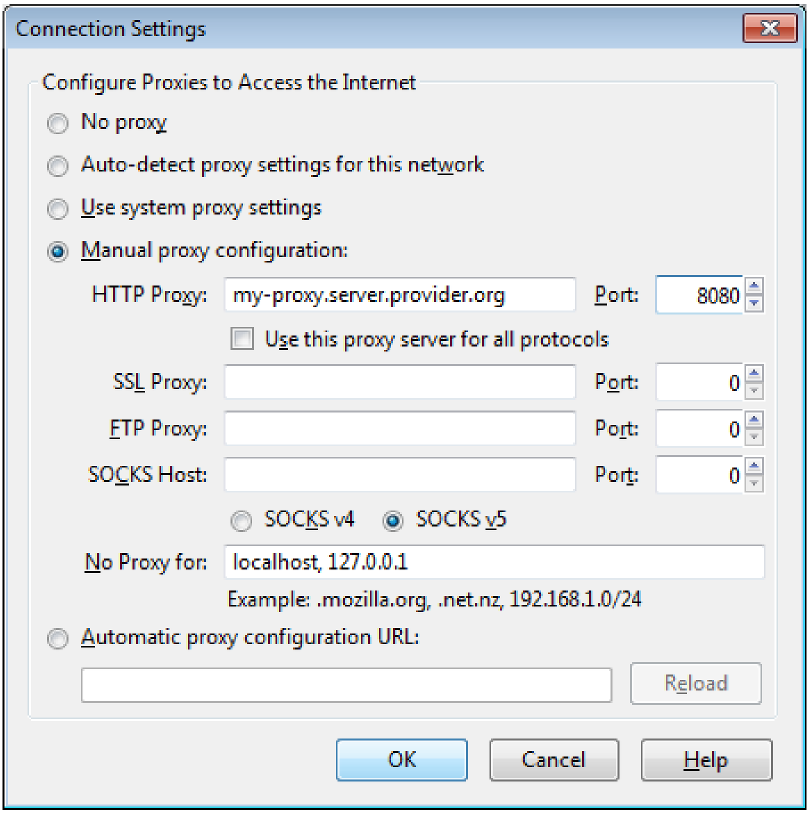
☐ Override automatic cache management

Limit cache to 1024 MB of space

☑ Tell me when a website asks to store data for offline use

The following websites have stored data for offline use:

Select Settings, click on "Manual proxy configuration" and enter the information of the proxy server you want to use. Please remember that HTTP proxies and SOCKS proxies work differently and have to be entered in the corresponding fields. If there is a colon (:) in your proxy information, that is the separator between the proxy address and the port number. Your screen should look like this:



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: my-proxy.server.provider.org Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

After you click OK, your configuration will be saved and your Web browser will automatically connect through that proxy on all future connections. If you get an error message such as, "The proxy server is refusing connections" or "Unable to find the proxy server", there is a problem with your proxy configuration. In that case, repeat the steps above and select "No proxy" in the last screen to deactivate the proxy.

Using Tor?

Tor is a system intended to enable online anonymity, composed of client software and a network of servers which can hide information about users' locations and other factors which might identify them. Imagine a message being wrapped in several layers of protection: every server needs to take off one layer, thereby immediately deleting the sender information of the previous server.

Use of this system makes it more difficult to trace internet traffic to the user, including visits to Web sites, online posts, instant messages, and other communication forms. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business, by keeping their internet activities from being monitored. The software is open-source and the network is free of charge to use.

Like all current low latency anonymity networks, Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network, i.e., the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation)

Caution: As Tor does not, and by design cannot, encrypt the traffic between an exit node and the target server, any exit node is in a position to capture any traffic passing through it which does not use end-to-end encryption such as TLS. (If your postman is corrupt he might still open the envelope and read the content). While this may or may not inherently violate the anonymity of the source, if users mistake Tor's anonymity for end-to-end encryption they may be subject to additional risk of data interception by third parties. So: the location of the user remains hidden; however, in some cases content is vulnerable for analysis through which also information about the user may be gained.

Using Tor Browser Bundle

The Tor Browser Bundle lets you use Tor on Windows, OSX and/or Linux without requiring you to configure a Web browser. Even better, it's also a portable application that can be run from a USB flash drive, allowing you to carry it to any PC without installing it on each computer's hard drive.

Downloading Tor Browser Bundle

You can download the Tor Browser Bundle from the torproject.org Web site (https://www.torproject.org), either as a single file (13MB) or a split version that is multiple files of 1.4 MB each which may proof easier to download on slow connections.

If the torproject.org Web site is filtered from where you are, type "tor mirrors" in your favorite Web search engine: The results probably include some alternative addresses to download the Tor Browser Bundle.

Caution: When you download Tor Bundle (plain or split versions), you should check the signatures of the files, especially if you are downloading the files from a mirror site. This step ensures that the files have not been tampered with. To learn more about signature files and how to check them, read https://www.torproject.org/docs/verifying-signatures

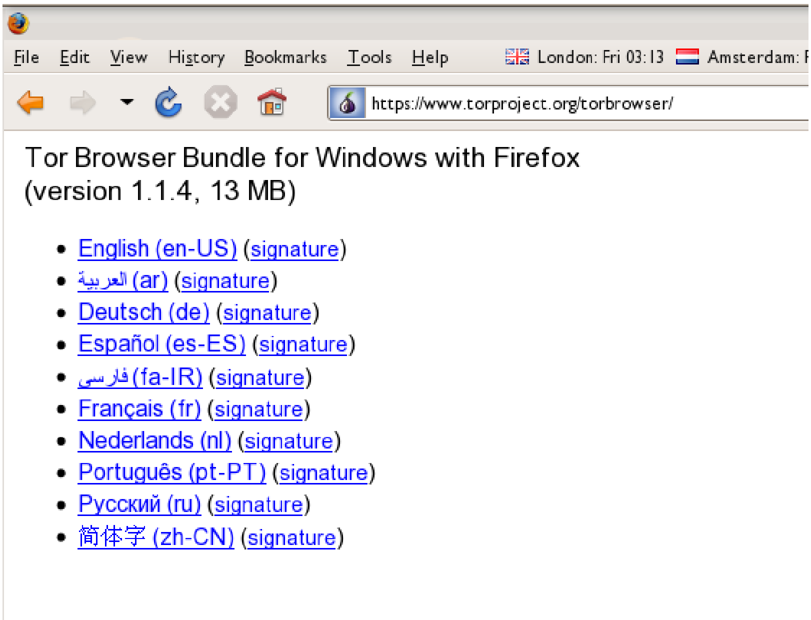
(You can also download the GnuPG software that you will need to check the signature here: http://www.gnupg.org/download/index.en.html#auto-ref-2)

The instructions below refer to installing Tor Browser on Microsoft Windows. If you are using a different operating system, refer to the torproject.org website for download links and instructions.

Installing from a single file

1. In your Web browser, enter the download URL for Tor Browser:

https://www.torproject.org/download/download

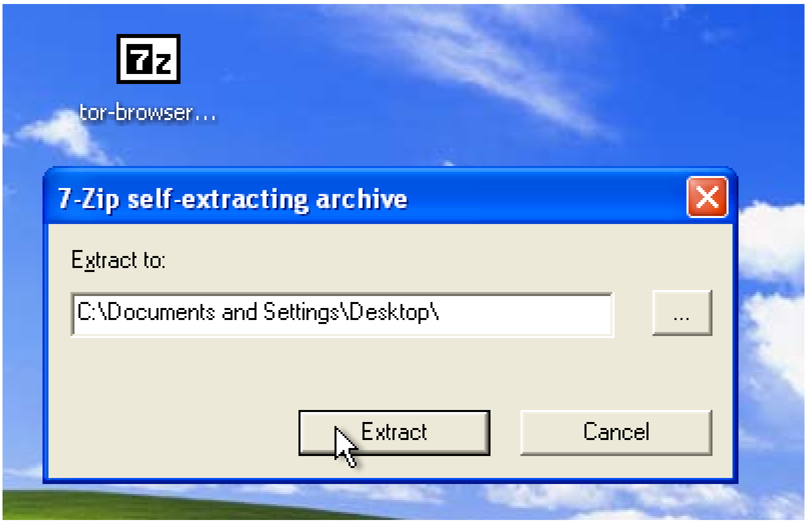


Tor Browser Bundle for Windows with Firefox (version 1.1.4, 13 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa-IR) (signature)
- Français (fr) (signature)
- Nederlands (nl) (signature)
- Português (pt-PT) (signature)
- Русский (ru) (signature)
- 简体字 (zh-CN) (signature)

2. Click the link for your language to download the installation file.

3. On windows double-click the .EXE file you just downloaded. A "7-Zip self-extracting archive" window appears.

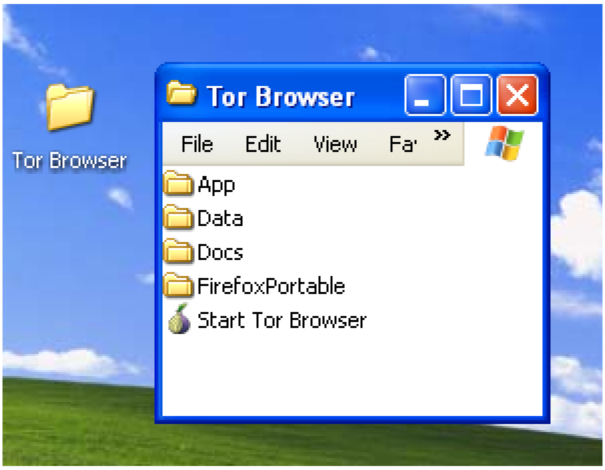


Extract to: C:\Documents and Settings\Desktop\

4. Choose a folder into which you want to extract the files and click "Extract".

Note: You can choose to extract the files directly onto a USB key or memory stick if you want to use Tor Browser on different computers (for instance on public computers in Internet cafes).

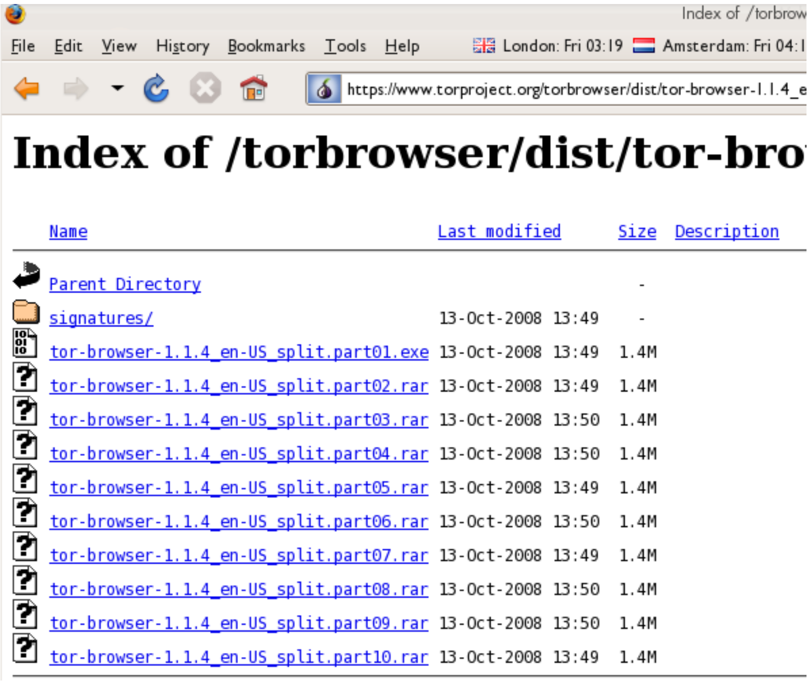
5. When the extraction is completed, open the folder and check that the contents match the image below:



6. To clean up, delete the .EXE file you originally downloaded.

Installing from split files

1. In your Web browser, enter the URL for the split version of the Tor Browser Bundle (https://www.torproject.org/torbrowser/split.html), then click the link for your language to get to a page that looks like the one for English below:


Index of /torbrow
File Edit View History Bookmarks Tools Help
London: Fri 03:19 Amsterdam: Fri 04:1

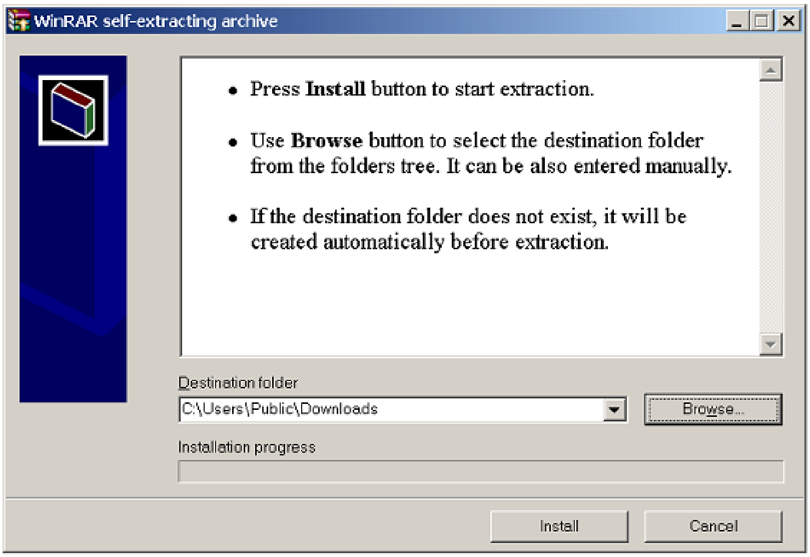
https://www.torproject.org/torbrowser/dist/tor-browser-1.1.4_e

Index of /torbrowser/dist/tor-bro

```
Name                                   Last modified      Size  Description
Parent Directory                                            -
signatures/                            13-Oct-2008 13:49    -
tor-browser-1.1.4_en-US_split.part01.exe 13-Oct-2008 13:49  1.4M
tor-browser-1.1.4_en-US_split.part02.rar 13-Oct-2008 13:49  1.4M
tor-browser-1.1.4_en-US_split.part03.rar 13-Oct-2008 13:50  1.4M
tor-browser-1.1.4_en-US_split.part04.rar 13-Oct-2008 13:50  1.4M
tor-browser-1.1.4_en-US_split.part05.rar 13-Oct-2008 13:49  1.4M
tor-browser-1.1.4_en-US_split.part06.rar 13-Oct-2008 13:50  1.4M
tor-browser-1.1.4_en-US_split.part07.rar 13-Oct-2008 13:49  1.4M
tor-browser-1.1.4_en-US_split.part08.rar 13-Oct-2008 13:50  1.4M
tor-browser-1.1.4_en-US_split.part09.rar 13-Oct-2008 13:50  1.4M
tor-browser-1.1.4_en-US_split.part10.rar 13-Oct-2008 13:49  1.4M
```

2. Click each file to download it (one ending in ".exe" and nine others ending in ".rar"), one after the other, and save them all in one folder on your hard- or USB-drive.

3. Double-click the first part (the file whose name ends in ".exe"). This runs a program to gather all the parts together.



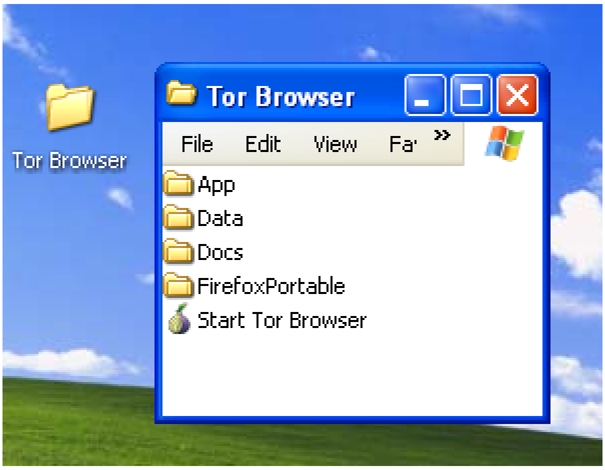
- Press **Install** button to start extraction.
- Use **Browse** button to select the destination folder from the folders tree. It can be also entered manually.
- If the destination folder does not exist, it will be created automatically before extraction.

Destination folder: C:\Users\Public\Downloads

4. Choose a folder where you want to install the files, and click "Install". The

program displays messages about its progress while it's running, and then quits.

5. When the extraction is completed, open the folder and check that the contents match the image below:



6. To clean up, delete all the files you originally downloaded.

Using Tor Browser

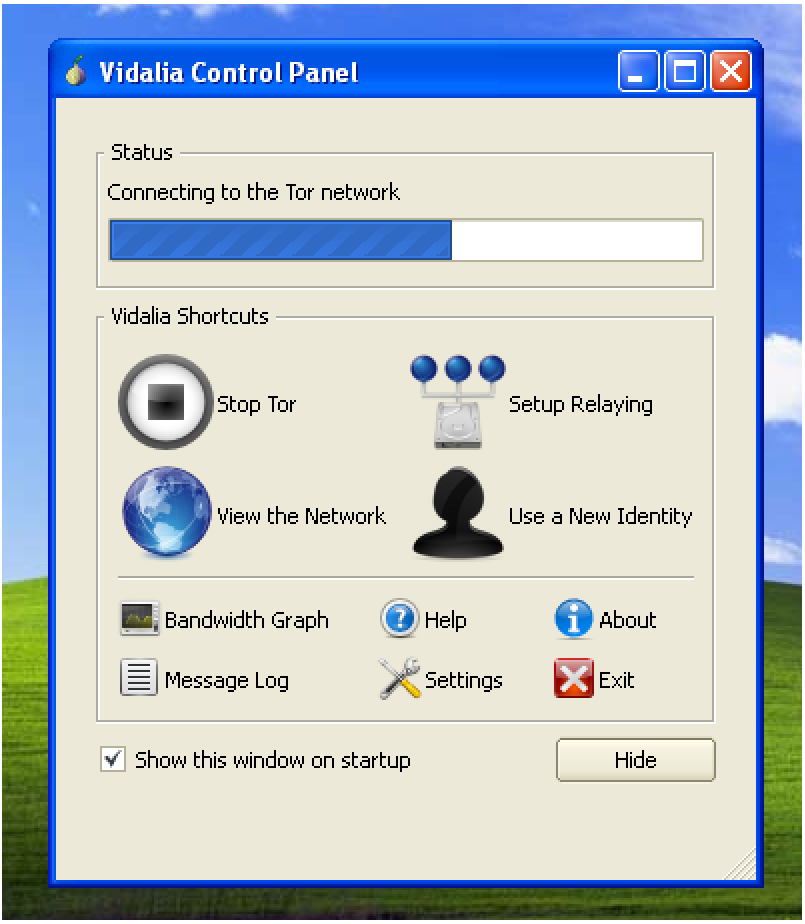
Before you start:

- **Close Firefox.** If Firefox is installed on your computer, make sure it is not currently running.

- **Close Tor.** If Tor is already installed on your computer, make sure it is not currently running.

Launch Tor Browser:

- In the "Tor Browser" folder, double-click "Start Tor Browser". The Tor control panel ("Vidalia") opens and Tor starts to connect to the Tor network.

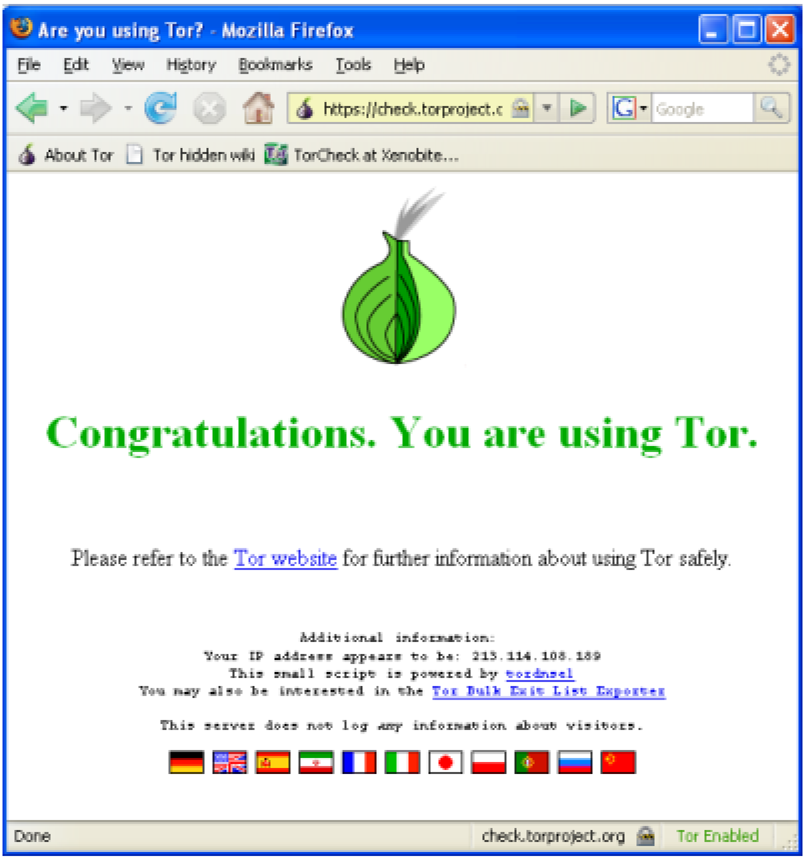


Status

Connecting to the Tor network

☑ Show this window on startup

When a connection is established, Firefox automatically connects to the TorCheck page and then confirms if you are connected to the Tor network. This may take some time, depending on the quality of your Internet connection.


Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.c
Google
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Done
check.torproject.org
Tor Enabled

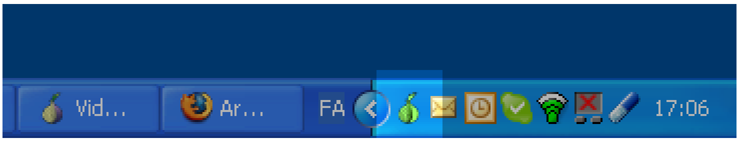
Congratulations. You are using Tor.

Please refer to the Tor website for further information about using Tor safely.

Additional information:
Your IP address appears to be: 213.114.108.189
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If you are connected to the Tor network, a green onion icon appears in the System Tray on the lower-right-hand corner of your screen:

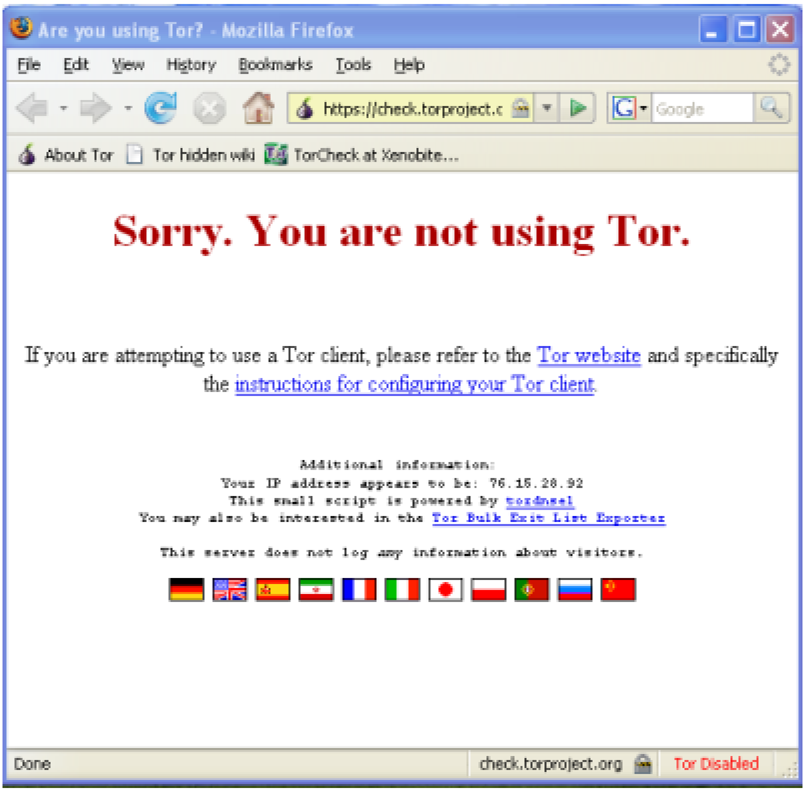


Browsing the Web using Tor Browser

Try viewing a few Web sites, and see whether they display. The sites are likely to load more slowly than usual because your connection is being routed through several relays.

If this does not work

If the onion in the Vidalia Control Panel never turns green or if Firefox opened, but displayed a page saying "Sorry. You are not using Tor", as in the image below, then you are not using Tor.


Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.c
Google
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Done
check.torproject.org
Tor Disabled

Sorry. You are not using Tor.

If you are attempting to use a Tor client, please refer to the Tor website and specifically the instructions for configuring your Tor client.

Additional information:
Your IP address appears to be: 76.15.28.92
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If you see this message, close Firefox and Tor Browser and then repeat the steps above. You can perform this check to ensure that you are using tor, at any time by clicking the bookmark button labelled "TorCheck at Xenobite..." in the Firefox toolbar.

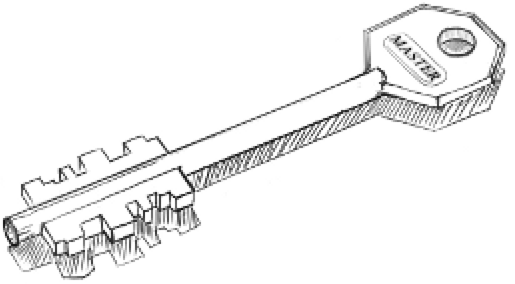
If Firefox browser does not launch, another instance of the browser may be interfering with Tor Browser. To fix this:

1. Open the Windows Task Manager. How you do this depends on how your computer is set up. On most systems, you can right-click in the Task Bar and then click "Task Manager".
2. Click the "Processes" tab.
3. Look for a process in the list named "firefox.exe".

4. If you find one, select the entry and click "End Process".
5. Repeat the steps above to launch Tor Browser.

If Tor Browser still doesn't work after two or three tries, Tor may be partly blocked by your ISP and you should try using the *bridge* feature of Tor.

Passwords



Keeping passwords safe

Passwords are like keys in the physical world. If you lose a password you will not be able to get in, and if others copy or steal it they can use it to enter. A good password should not be easy for others to guess and not easy to crack with computers, while still being easy for you to remember.

Password length and complexity

To protect your passwords from being guessed, length and complexity are important. Passwords like the name of your pet or a birth date are very unsafe, as is using single word that can be found in a dictionary. Do not use a password containing only numbers. Most importantly a secure password is long. Using combinations of lower case letters, capitals, numbers and special characters can improve the security, but length is still the most important factor.

For use with important accounts like the pass phrase which protects your PGP/GPG or TrueCrypt encrypted data, or the password for your main email account, use 20 characters or more, the longer the better. See the xkcd cartoons no. 936 example “correct horse battery staple” vis-à-vis “Tr0ub4dor&3” for an explanation (https://xkcd.com/936/).

Easy to remember and secure passwords

One way to create strong and easy to remember passwords is to use sentences.

A few examples:

- “IloveDouglasAdamsbecausehe'sreallyawesome.”,
- “Peoplelovemachinesin2029A.D.” or – if blank spaces are allowed –
- “Barney from How I Met Your Mother is AWESOME!”

Sentences are easy to remember, even if they are 50 characters long and contain uppercase characters, lowercase characters, symbols and numbers.

Minimizing damage

It is important to minimize the damage if one of your passwords is ever compromised. Use different passwords for different websites or accounts, that way if one is compromised, the others are not. Change your passwords from time to time, especially for accounts you consider to be sensitive. By doing this you can block access to an attacker who may have learned your old password.

Using a password manager

Remembering a lot of different passwords can be difficult. One solution is to use a dedicated application to manage most of your passwords. The next section in this chapter will discuss *Keepass*, a free and open source password manager with no known vulnerabilities, so long as you chose a sufficiently long and complex "master password" to secure it with.

For website passwords only, another option is the built-in password manager of the Firefox browser. Make sure to set a master password, otherwise this is very insecure!

Physical protection

When using a public computer such as at a library, an internet cafe, or any computer you do not own, there are several dangers. Using "over the shoulder" surveillance, someone, possibly with a camera, can watch your actions and may see the account you log in to and the password you type. A less obvious threat is software programs or hardware devices called "keystroke logggers" that record what you type. They can be hidden inside a computer or a keyboard and are not easily spotted. Do not use public computers to log in to your private accounts, such as email. If you do, change your passwords as soon as you get back to a computer you own and trust.

Other caveats

Some applications such as chat or mail programs may ask you to save or "remember" your username and password, so that you don't have to type them every time the program is opened. Doing so may mean that your password can be retrieved by other programs running on the machine, or directly from your hard disk by someone with physical access to it.

If your login information is sent over an insecure connection or channel, it might fall into the wrong hands. See the chapters on secure browsing for more information.

Installing KeePass

We will cover installing KeePass on Ubuntu and Windows.

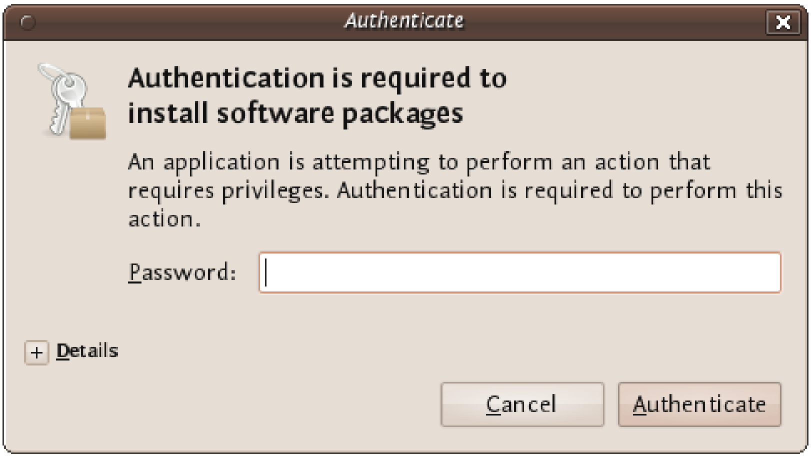
Mac OSX comes with an excellent built-in password manager called **Keychain** that is just as safe. Downsides are that it isn't Open Source and doesn't work on other systems. If you'd need to take your passwords from one Operating System to another it is better to stick with Keepass after all. How to use **Keychain** is covered in the next chapter.

Installing KeePassX on Ubuntu

To install on Ubuntu we will use the Ubuntu Software Center

Type KeePass in the search field at the top right and the application KeePassX should automatically appear in the listing.

Highlight the item (it may already be highlighted by default) and then press 'Install'. You will be asked to Authorise the installation process:



Authenticate

Authentication is required to install software packages

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

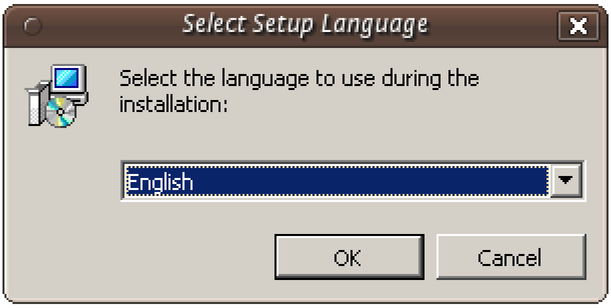
Enter your password and press 'Authenticate' the installation process will then begin.

Ubuntu does not offer very good feedback to show the software is installed. If the green progress indicator on the left has gone and the progress bar on the right has gone then you can assumed the software is installed.

Installing KeePass on Windows

First visit the KeePass download webpage (http://keepass.info/download.html) and choose the appropriate installer. For this chapter we are using the current installer (KeePass-2.15-Setup.exe which can also be directly downloaded from here http://downloads.sourceforge.net/keepass/KeePass-2.15-Setup.exe).

Download this to your computer then double click on the installer. You will first be asked to select a language, we will choose English:

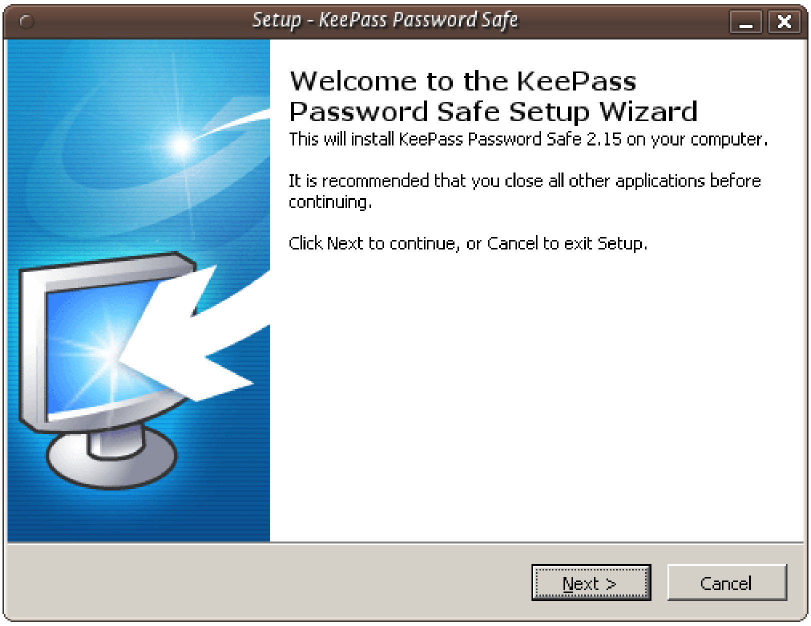


Select Setup Language

Select the language to use during the installation:

English

Press 'OK' and you will be shown the following screen:



Setup - KeePass Password Safe

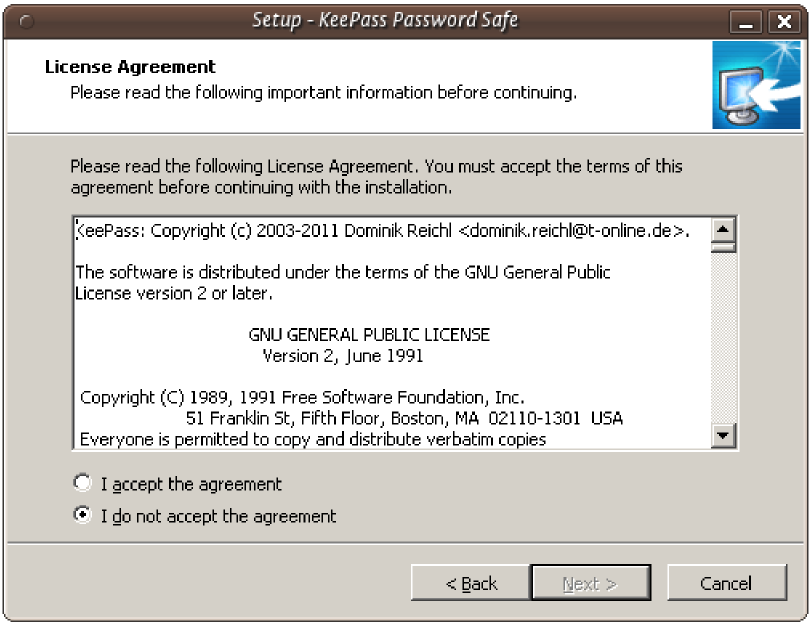
Welcome to the KeePass Password Safe Setup Wizard

This will install KeePass Password Safe 2.15 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Just press 'Next >' and go to the next screen :



Setup - KeePass Password Safe

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

KeePass: Copyright (c) 2003-2011 Dominik Reichl <dominik.reichl@t-online.de>.

The software is distributed under the terms of the GNU General Public License version 2 or later.

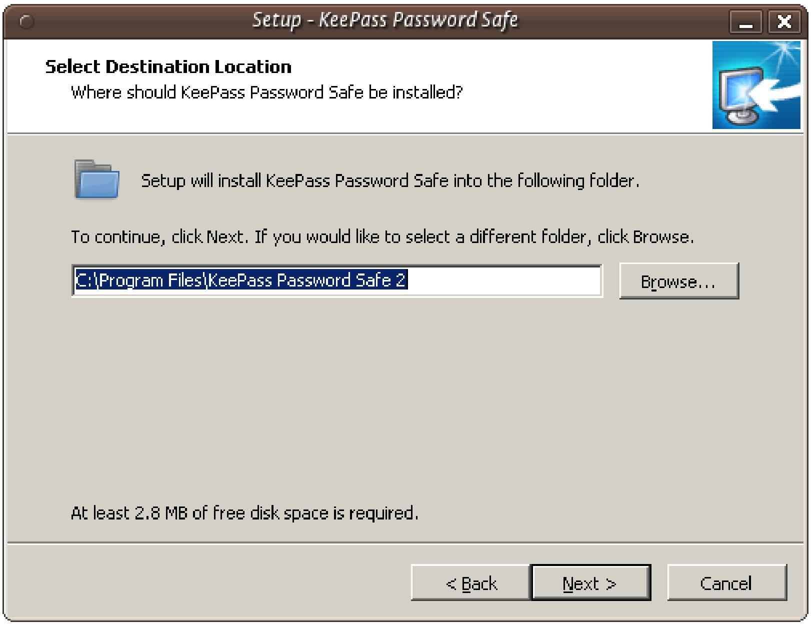
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies

○ I accept the agreement

● I do not accept the agreement

In the screen shown above we must select 'I accept the agreement' otherwise we will not be able to install the software. Choose this option and then press 'Next >'. In the next screen you will be asked to determine the installation location. You can leave this with the defaults unless you have good reason to change them.



Setup - KeePass Password Safe

Select Destination Location

Where should KeePass Password Safe be installed?

Setup will install KeePass Password Safe into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

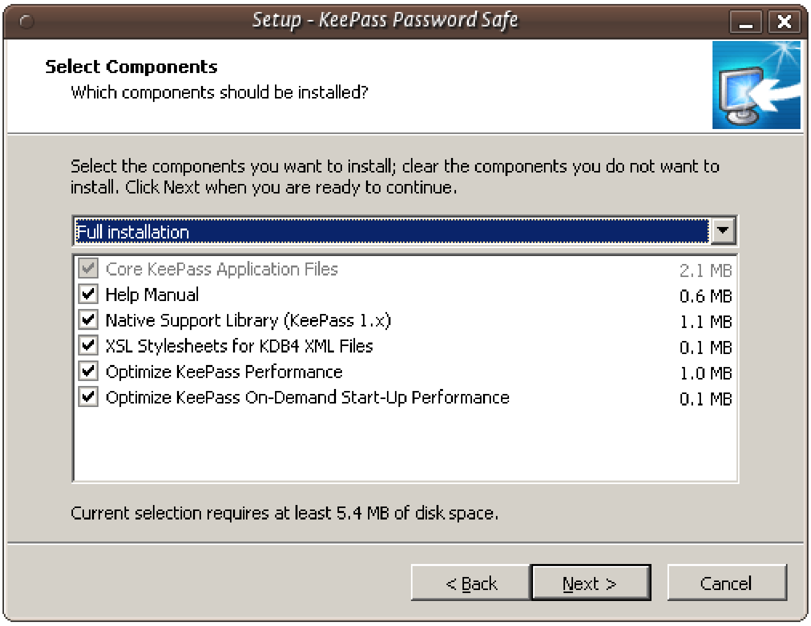
C:\Program Files\KeePass Password Safe 2

Browse...

At least 2.8 MB of free disk space is required.

< Back | Next > | Cancel

Click on 'Next >' and continue.



Setup - KeePass Password Safe

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

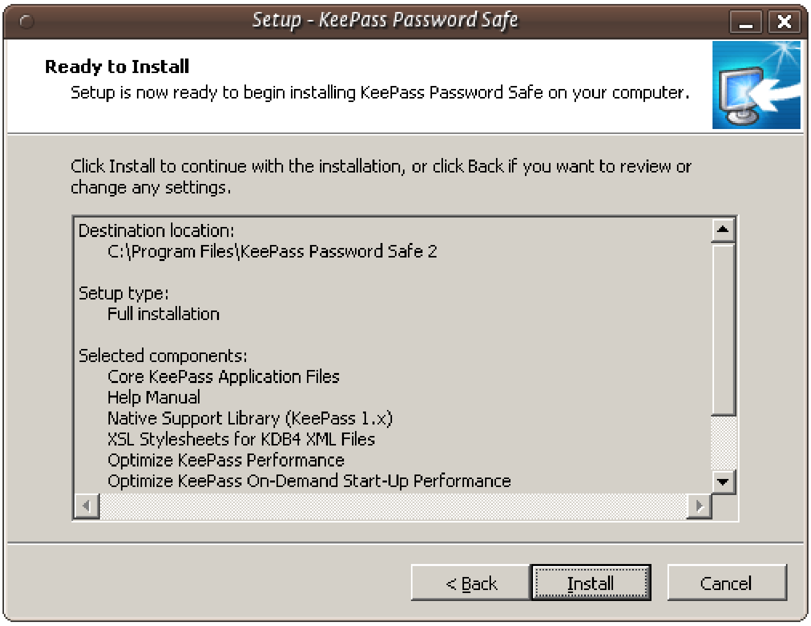
Full installation

☑ Core KeePass Application Files 2.1 MB
☑ Help Manual 0.6 MB
☑ Native Support Library (KeePass 1.x) 1.1 MB
☑ XSL Stylesheets for KDB4 XML Files 0.1 MB
☑ Optimize KeePass Performance 1.0 MB
☑ Optimize KeePass On-Demand Start-Up Performance 0.1 MB

Current selection requires at least 5.4 MB of disk space.

< Back | Next > | Cancel

The above image shows the KeePass components you can choose from. Just leave the defaults as they are and press 'Next >'. You will come to a new screen:



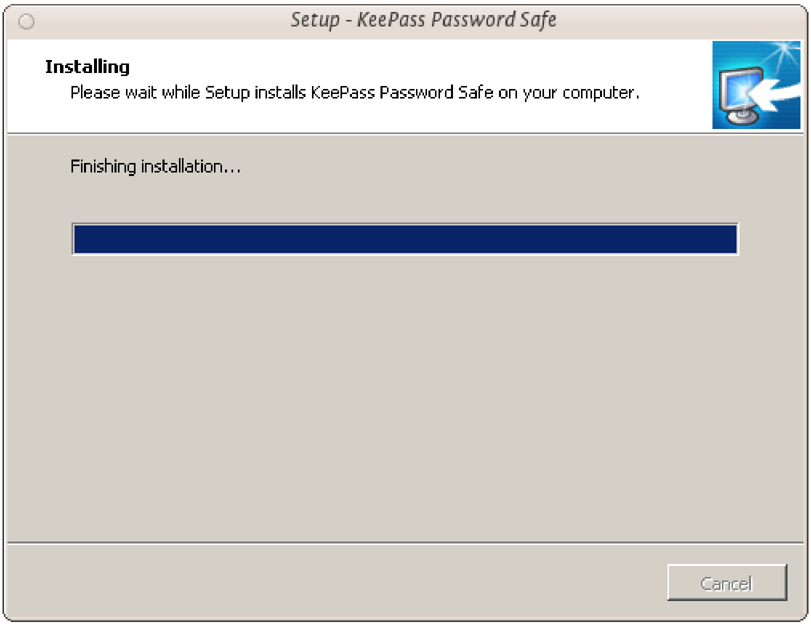
Ready to Install

Setup is now ready to begin installing KeePass Password Safe on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
     C:\Program Files\KeePass Password Safe 2

Setup type:
     Full installation

Selected components:
     Core KeePass Application Files
     Help Manual
     Native Support Library (KeePass 1.x)
     XSL Stylesheets for KDB4 XML Files
     Optimize KeePass Performance
     Optimize KeePass On-Demand Start-Up Performance
```

This doesn't do anything but give you a summary of your options. Press 'Install' and the installation process will begin.



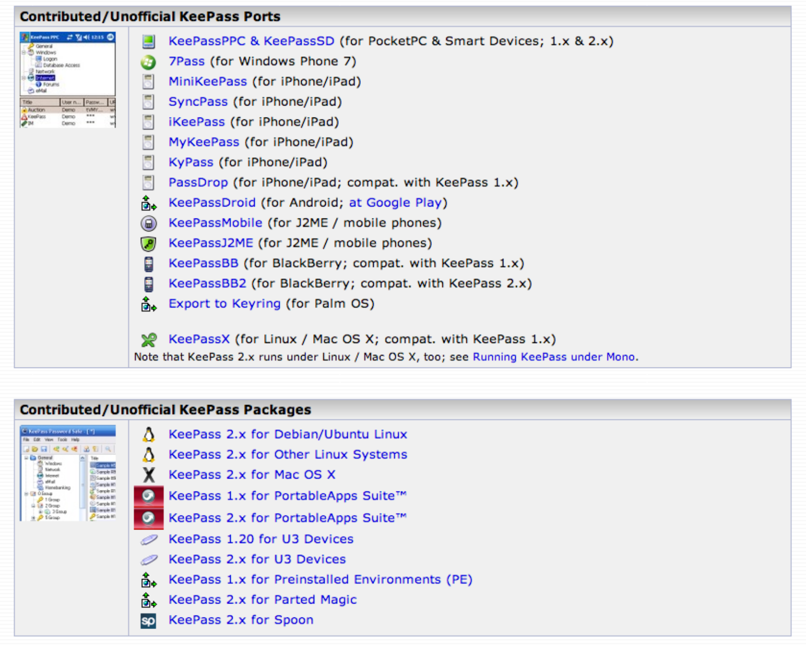
Installing

Please wait while Setup installs KeePass Password Safe on your computer.

Finishing installation...

Installing KeePass on Mac OS X

Although Keychain in Mac OS X does an excellent job of storing your passwords, you may want to run your own password database and manager. KeePass allows this added flexibility. First visit the KeePass download webpage (http://keepass.info/download.html) and choose the appropriate installer. Although the official installers are listed at the top of the page, there are unofficial/contributed installers further down. Scroll down to find KeePass 2.x for Mac OS X:



Contributed/Unofficial KeePass Ports

- KeePassPPC & KeePassSD (for PocketPC & Smart Devices; 1.x & 2.x)
- 7Pass (for Windows Phone 7)
- MiniKeePass (for iPhone/iPad)
- SyncPass (for iPhone/iPad)
- iKeePass (for iPhone/iPad)
- MyKeePass (for iPhone/iPad)
- KyPass (for iPhone/iPad)
- PassDrop (for iPhone/iPad; compat. with KeePass 1.x)
- KeePassDroid (for Android; at Google Play)
- KeePassMobile (for J2ME / mobile phones)
- KeePassJ2ME (for J2ME / mobile phones)
- KeePassBB (for BlackBerry; compat. with KeePass 1.x)
- KeePassBB2 (for BlackBerry; compat. with KeePass 2.x)
- Export to Keyring (for Palm OS)

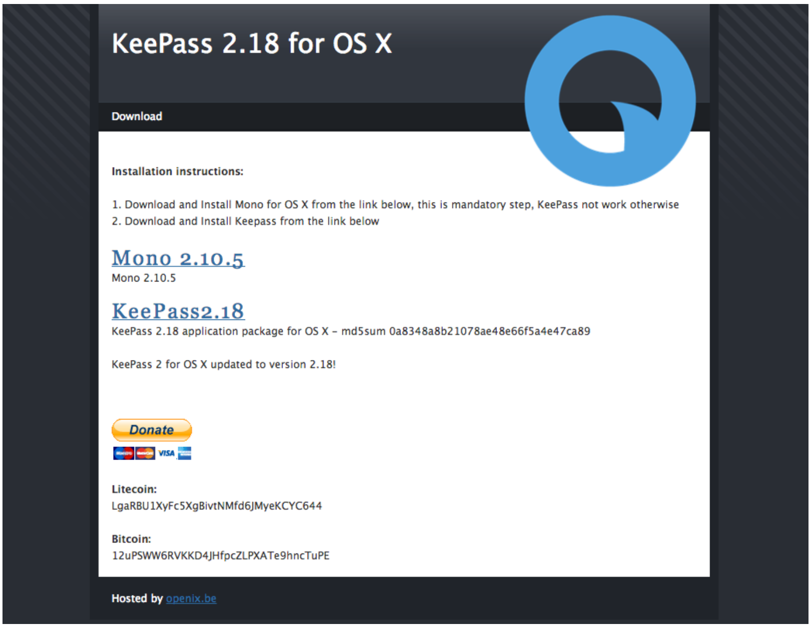
- KeePassX (for Linux / Mac OS X; compat. with KeePass 1.x)

Note that KeePass 2.x runs under Linux / Mac OS X, too; see Running KeePass under Mono.

Contributed/Unofficial KeePass Packages

- KeePass 2.x for Debian/Ubuntu Linux
- KeePass 2.x for Other Linux Systems
- KeePass 2.x for Mac OS X
- KeePass 1.x for PortableApps Suite™
- KeePass 2.x for PortableApps Suite™
- KeePass 1.20 for U3 Devices
- KeePass 2.x for U3 Devices
- KeePass 1.x for Preinstalled Environments (PE)
- KeePass 2.x for Parted Magic
- KeePass 2.x for Spoon

As this is an external link, your browser will be redirected to http://keepass2.openix.be/:



KeePass 2.18 for OS X

Download

Installation instructions:

1. Download and Install Mono for OS X from the link below, this is mandatory step, KeePass not work otherwise
2. Download and Install Keepass from the link below

Mono 2.10.5

Mono 2.10.5

KeePass2.18

KeePass 2.18 application package for OS X – md5sum 0a8348a8b21078ae48e66f5a4e47ca89

KeePass 2 for OS X updated to version 2.18!

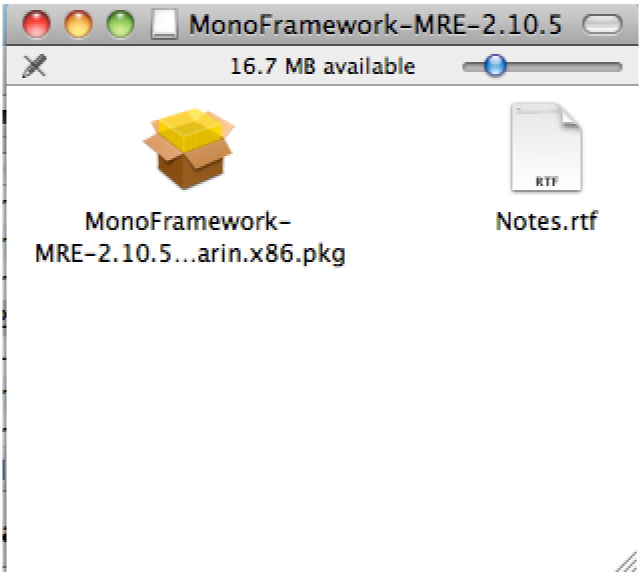
Litecoin:
LgaRBU1XyFc5XgBivtNMfd6JMyeKCYC644

Bitcoin:
12uPSWW6RVKKD4JHfpcZLPXATe9hncTuPE

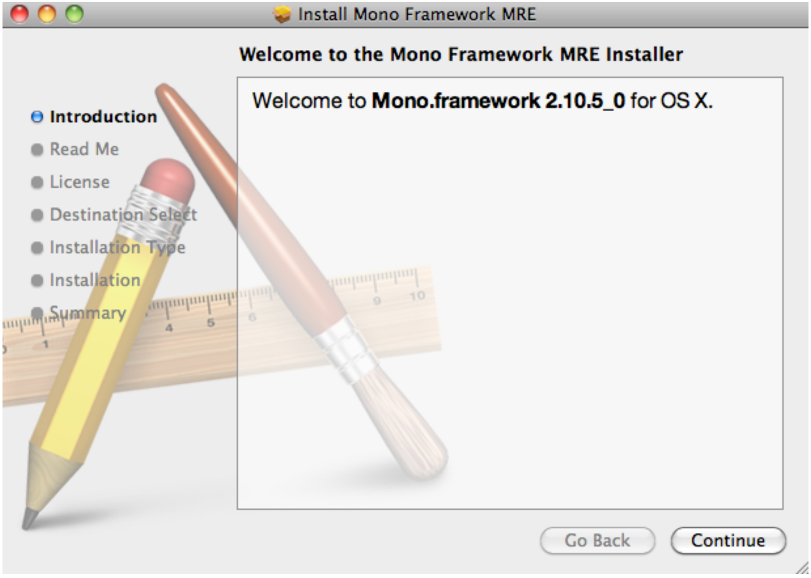
Hosted by openix.be

Note here that you must install the Mono framework first, so that KeePass can run in OS X. So click on each of the links Mono 2.10.5 and KeePass2.18 to download the DMG files to your computer. Double-click on each of the DMGs in your downloads folder to unpack the volumes to your desktop.

The Mono Package installer is called 'MonoFramework-MRE-2.10.5_0.macos10.xamarin.x86.pkg', so double-click on this document in the MonoFramework volume on your desktop:

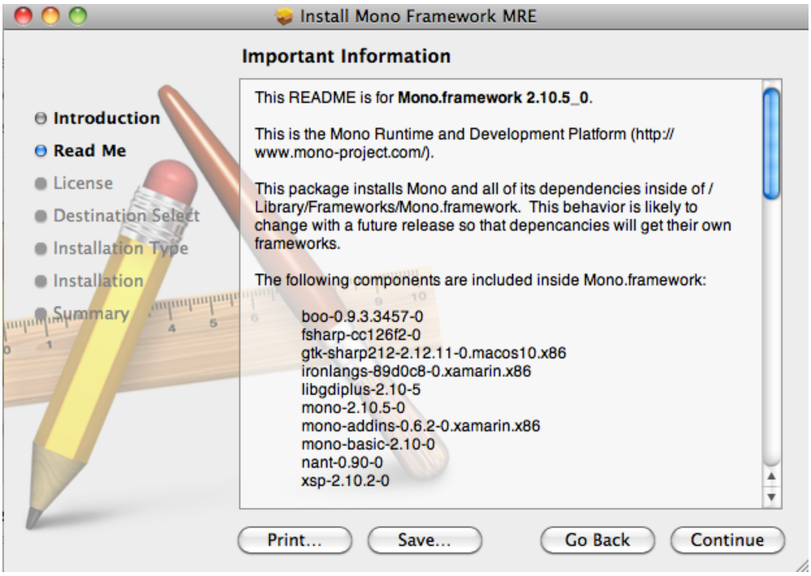


The installer will open and run:



Welcome to **Mono.framework 2.10.5_0** for OS X.

Follow each of the steps by clicking 'Continue', the next step being 'Read Me'. Inhere is important information such as all of the files that the package will install, including information on how to uninstall Mono:



Important Information

This README is for **Mono.framework 2.10.5_0**.

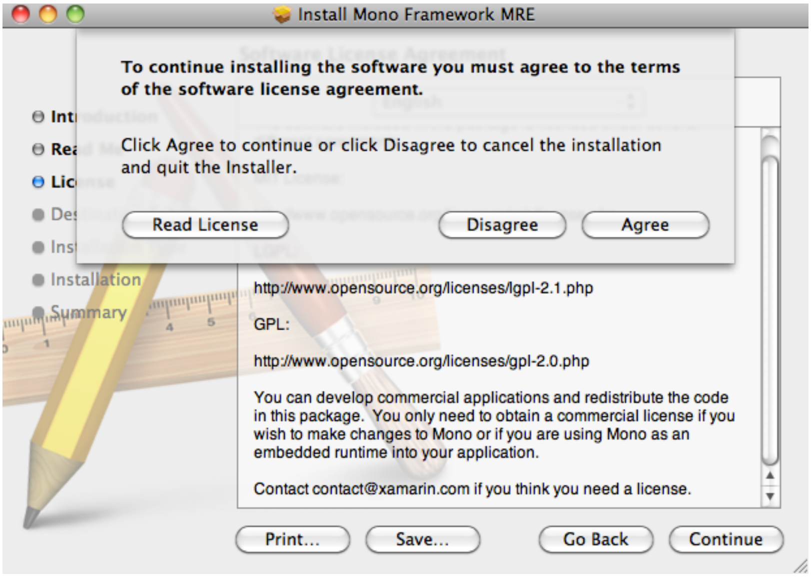
This is the Mono Runtime and Development Platform (http://www.mono-project.com/).

This package installs Mono and all of its dependencies inside of /Library/Frameworks/Mono.framework. This behavior is likely to change with a future release so that depencancies will get their own frameworks.

The following components are included inside Mono.framework:

boo-0.9.3.3457-0
fsharp-cc126f2-0
gtk-sharp212-2.12.11-0.macos10.x86
ironlangs-89d0c8-0.xamarin.x86
libgdiplus-2.10-5
mono-2.10.5-0
mono-addins-0.6.2-0.xamarin.x86
mono-basic-2.10-0
nant-0.90-0
xsp-2.10.2-0

Click 'Continue' to the next screen, the license. Clicking 'Continue' on the license screen pops up the agree/disagree dialogue box. If you agree with the license conditions, the installation will continue:



To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

http://www.opensource.org/licenses/lgpl-2.1.php

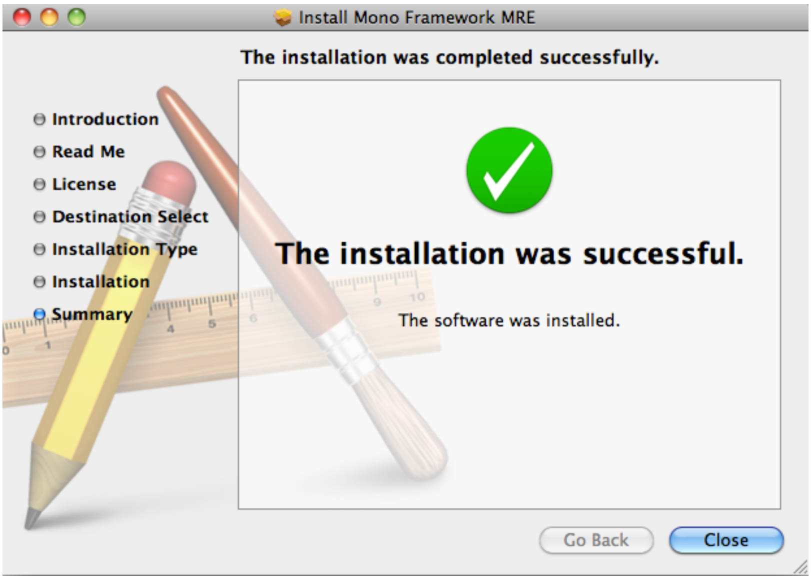
GPL:

http://www.opensource.org/licenses/gpl-2.0.php

You can develop commercial applications and redistribute the code in this package. You only need to obtain a commercial license if you wish to make changes to Mono or if you are using Mono as an embedded runtime into your application.

Contact contact@xamarin.com if you think you need a license.

The following two steps in the installation ask you to choose an installation destination, and check there is enough space on the install disk. When the installation has completed, you will see this screen:



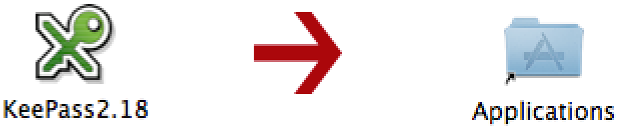
Install Mono Framework MRE

The installation was completed successfully.

The installation was successful.

The software was installed.

Now you can quit the installer. Next take a look at the KeePass disk image, double-click to open it, and drag the KeePass application into your Applications folder:



Now KeePass is ready to use for Mac OS X.

Encrypting Passwords with a Password Manager

To encrypt password we use KeePass on Windows and KeePassX Ubuntu, and Keychain on OSX. The basic principle is the same; you have a file on your computer which is encrypted with *one single very secure password.* This is sometimes referred to as a 'Master Password', 'Admin-Password', 'Root-Password' etc. but they are all *the ultimate key* to all your other keys and secure data. For this reason you can't and shouldn't think to light about creating this password.

If a password manager is part of your OS (like it is with OSX) it unlocks automatically for you after you login to your account and so opening secure information like passwords. For this, and other, reasons you should disable 'Automatically Login'. When you start-up your computer you should always have to login and, even better, set your computer to automatically logout or lock the screen after a set amount of time.

Encrypting Passwords with KeePassX on Ubuntu

First open KeePassX from the Applications->Accessories -> KeePassX menu.

The first time you use KeePassX you need to set up a new database to store your passwords. Click on File->New Database

You will be asked to set a master key (password).

Choose a strong password for this field - refer to the chapter about passwords if you would like some tips on how to do this. Enter the password and press 'OK'. You then are asked to enter the password again. Do so and press 'OK'. If the passwords are the same you will see a new KeePassX 'database' ready for you to use.

Now you have a place to store all your passwords and protect them by the 'master' password you just set. You will see two default categories 'Internet' and 'Email' - you can store passwords just under these two categories, you can delete categories, add sub-groups, or create new categories. For now we just want to stay with these two and add a password for our email to the email group. Right click on the email category and choose 'Add New Entry...':

So now fill this form out with the details so you can correctly identify which email account the passwords are associated with. You need to fill out the fields 'Title' and the password fields. All else is optional.

KeePassX gives some indication if the passwords you are using are 'strong' or 'weak'...you should try and make passwords stronger and for advice on this read the chapter about creating good passwords. Press 'OK' when you are done and you will see something like this:

To recover the passwords (see them) you must double click on the enter and you will see the same window you used for recording the information. If you click on the 'eye' icon to the right of the passwords they will be converted from stars (***) to the plain text so you can read it.

Now you you can use KeePassX to store your passwords. However before getting too excited you must do one last thing. When you close KeePassX (choose File->Quit) it asks you if you would like to save the changes you have made.

Press 'Yes'. If it is the first time you used KeePassX (or you have just created a new database) you must choose a place to store your passwords. Otherwise it will save the updated information in the file you have previously created.

When you want to access the passwords you must then open KeePassX and you will be asked for the master key. After typing this in you can add all your passwords to the database and see all your entries. It is *not* a good idea to open KeePassX and have it open permanently as then anyone could see your passwords if they can access your computer. Instead get into the practice of just opening it when you need it and then closing it again.

Encrypting Passwords with KeePass on Windows

After you installed KeePass on Windows you can find it in the application menu. Launch the application and the following window should appear.

You start by making a database, the file which will contain your key. From the menu select **File > New.** You have to chose the name and the location of the file in the dialog window below. In this example we call our database 'my_password_database'.

The next screen will ask you for the master password. Enter the password and click on 'OK'. You will not need to select anything else.

The next window allows you to add special configuration settings for your new database. We do not need to edit anything. Just click on 'OK'.

Now the main window appears again and we see some default password categories on the left side. Lets add a new password in the category 'Internet'. First click on the word 'Internet', then click on the add entry icon under the menu bar.

A widow will appear like below. Use the fields to give a description of this particular password, and of course, enter the password itself. When done, click on 'OK'.

Encrypting Passwords with Keychain on Mac OSX

Mac OSX comes pre-installed with the build in password manager 'Keychain'. Because of it's tight integration with the OS most of the time you will hardly know it exists. But every now and then you will have a pop-up window in almost any application asking 'do you want to store this password in your keychain?'. This happens when you add new email accounts to your mail client, login to a protected wireless network, enter your details in your chat client etc. etc. etc.

Basically what happens is that Mac OSX offers you to store all that login data and different passwords in an encrypted file which it unlocks as soon as you login to your account. You can then check your mail, logon to your WiFi and use your chat client without having to enter your login data all the time over and over again. This is a fully automated process, but if you want to see what is stored where and alter passwords, or lookup a password you will have to open the Keychain program.

You can find the Keychain program in the Utilities folder which lives in the Applications folder.

When you open it you will see that your 'Login' keychain is unlocked and see all the items contained in it on the right bottom side of the window.

(note: the window here is empty because it seemed to be deceiving the purpose of this manual to make a screenshot of my personal keychain items and share it here with you)

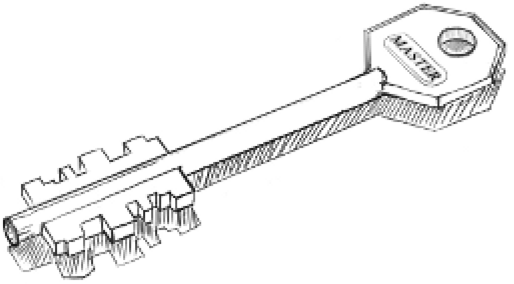
You can double click any of the items in the Keychain to view it's details and tick 'Show password:' to see the password associated with the item.

You will note that it will ask you for your master or login password to view the item.

You can access modify any of the items and also use the Keychain to securely save any bits and pieces of text using the notes. To do this click on notes and than choose 'New secure Note item' from the file menu.

That's it

Using VPN



GETTING, SETTING-UP AND TESTING A VPN ACCOUNT

In all the VPN systems, there is one computer set up as a server (in an unrestricted location), to which one or more clients connect. The set up of the server is out of the scope of this manual and the set up of this system is in general covered by your VPN provider. This server is one of the two ends of the encrypted tunnel. It is important that the company running this server can be trusted and is located in an area you trust. So to run a VPN, an account is needed at such a trusted server.

Please keep in mind that an account can often only be used on one device at a time. If you want to use a VPN with both your mobile and laptop concurrently, it is very well possible you need two accounts.

AN ACCOUNT FROM A COMMERCIAL VPN PROVIDER

There are multiple VPN providers out there. Some will give you free trial time, others will begin charging right away at an approximate rate of €5 per month. Look for a VPN provider that offers OpenVPN accounts - it is an Open Source, trusted solution available for Linux, OS X, and Windows, as well as Android and iOS.

When choosing a VPN provider you need to consider the following points:

- Information that is required from you to register an account - the less that is needed the better. A truly privacy concerned VPN provider would only ask you for email address (make a temporary one!), username and password. More isn't required unless the provider creates a user database which you probably don't want to be a part of.
- Payment method to be used to pay for your subscription. Cash-transfer is probably the most privacy-prone method, since it does not link your bank account and your VPN network ID. Paypal can also be an acceptable option assuming that you can register and use a temporary account for every payment. Payment via a bank transfer or by a credit card can severely undermine your anonymity on and beyond the VPN.
- Avoid VPN providers that require you to install their own proprietary client

software. There is a perfect open source solution for any platform, and having to run a "special" client is a clear sign of a phony service.
- **Avoid using PPTP based VPNs, as several security vulnerabilities exist in that protocol.** In fact, if two providers are otherwise equal, choose the one _not_ offering PPTP if feasible.
- Look for a VPN provider that's using OpenVPN - an open source, multi-platform VPN solution.
- Exit gateways in countries of your interest. Having a choice of several countries allows you to change your geo-political context and appears to come from a different part of the world. You need to be aware of legislation details and privacy laws in that particular country.
- Anonymity policy regarding your traffic - a safe VPN provider will have a non-disclosure policy. Personal information, such as username and times of connection, should not be logged either.
- Allowed protocols to use within VPN and protocols that are routed to the Internet. You probably want most of the protocols to be available
- Price vs. quality of the service and its reliability.
- Any known issues in regard to anonymity of the users the VPN provider might have had in the past. Look online, read forums and ask around. Don't be tempted by unknown, new, cheap or dodgy offers.

There are several VPN review oriented places online that can help you make the right choice:

http://www.bestvpnservice.com/vpn-providers.php
http://vpncreative.com/complete-list-of-vpn-providers
http://en.cship.org/wiki/VPN

Setting up your VPN client

"OpenVPN [..] is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate GNu/Linux, OSX, Windows and environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/or private cloud network resources and applications with fine-grained access control."
(http://openvpn.net/index.php/access-server/overview.html)

There are a number of different standards for setting up VPNs, including PPTP, LL2P/IPSec and **OpenVPN**. They vary in complexity, the level of security they provide, and which operating systems they are available for. **Do not use PPTP as it has several security vulnerabilities.** In this text we will concentrate on OpenVPN. It works on most versions of GNU/Linux, OSX, Windows. OpenVPN is TLS/SSL-based - it uses the same type of **encryption** that is used in HTTPS (Secure HTTP) and a myriad of other encrypted protocols. OpenVPN encryption is based on ***RSA*** key exchange algorithm. For this to work and in order to communicate, both the server and the client need to have *public and private* RSA keys.

Once you obtain access to your VPN account the server generates those keys and you simply need to download those from the website of your VPN provider or have them sent to your email address. Together with your keys you will receive a *root certificate (*.ca)* and a main *configuration file (*.conf or *.ovpn)*. In most cases only the following files will be needed to configure and run an OpenVPN client:

- **client.conf** (or **client.ovpn**) - configuration file that includes all necessary parameters and settings. NOTE: in some cases certificates and keys can come embedded inside the main configuration file. In such a case the below mentioned files are not necessary.
- **ca.crt** (unless in configuration file) - root authority certificate of your VPN server, used to sign and check other keys issued by the provider.
- **client.crt** (unless in configuration file) - your client certificate, allows you

to communicate with VPN server.

Based on a particular configuration, your VPN provider might require a username/password pair to authenticate your connection. Often, for convenience, the username and password can be saved into a separate file or added to the main configuration file. In other cases, *key-based authentication* is used, and the key is stored in a separate file:

- **client.key** (unless in configuration file) - client authentication key, used to authenticate to the VPN server and establish an encrypted data channel.

In most cases, unless otherwise necessary, you don't need to change anything in the configuration file and (surely!) do not edit key or certificate files! All VPN providers have thorough instructions regarding the setup. Read and follow those guidelines to make sure your VPN client is configured correctly.

NOTE: Usually it's only allowed to use one key per one connection, so you probably shouldn't be using the same keys on different devices at the same time. Get a new set of keys for each device you plan to use with a VPN, or attempt to set up a local VPN gateway (advanced, not covered here).

Download your OpenVPN *configuration* and *key* files copy them to a safe place and proceed to the following chapter.

Setting up OpenVPN client

In the following chapters some examples are given for setting up OpenVPN client software. On any flavor of GNU/Linux use your favorite package manager and install ***openvpn*** or ***openvpn-client*** package.

If you want to use OpenVPN on Windows or OSX, have look at:

http://openvpn.se (Windows interface)
http://code.google.com/p/tunnelblick (OSX interface)

VPN on Ubuntu

If you use Ubuntu as your operating system, you can connect to a VPN by using the built-in *NetworkManager*. This application is able to set up networks with OpenVPN. PPTP should not be used for security reasons. Unfortunately at the time of writing a L2TP interface is not available in Ubuntu. (It can be done manually, but it goes beyond the scope of this document).

The following example will explain how to connect with an OpenVPN-server. Under all situations we assume you already have a VPN account as described earlier in this section.

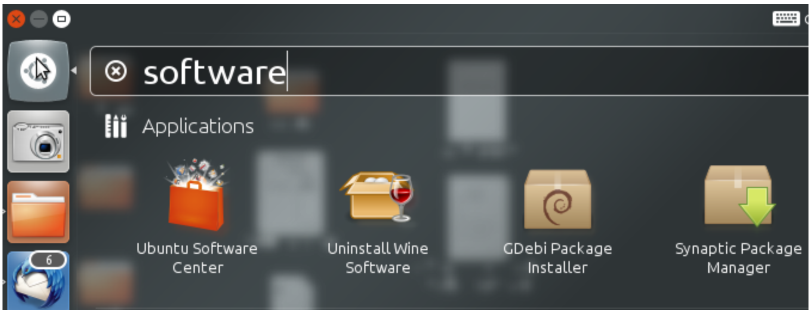
1. Preparing Network Manager for VPN networks

For Ubuntu there is an excellent network utility: Network Manager. This is the same utility you use to set up your Wireless (or wired) network and is normally in the upper right corner of your screen (next to the clock). This tools is also capable of managing your VPNs, but before it can do so, it's necessary to install some extensions.

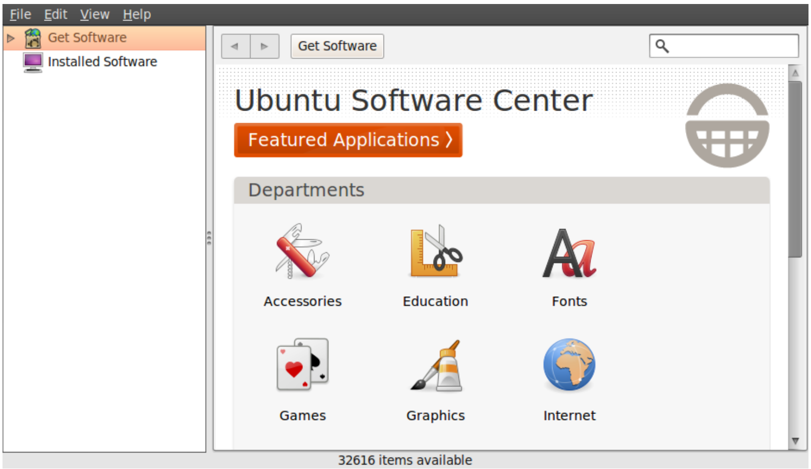
Installing OpenVPN extension for Network Manager

To install the plugins for Network Manager we will use the Ubuntu Software Center.

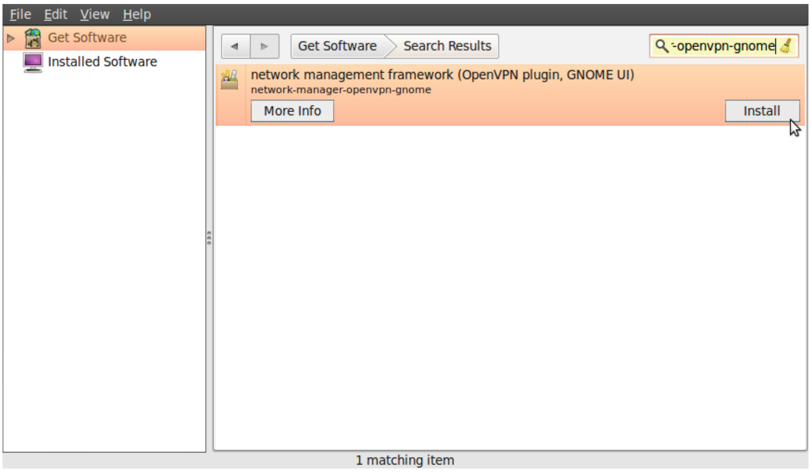
1. Open the Ubuntu Software Center by typing software in the Unity search bar



2. The Ubuntu Software Center enables you to search, install and remove software on your computer. Click on the search box at the top right of the window.



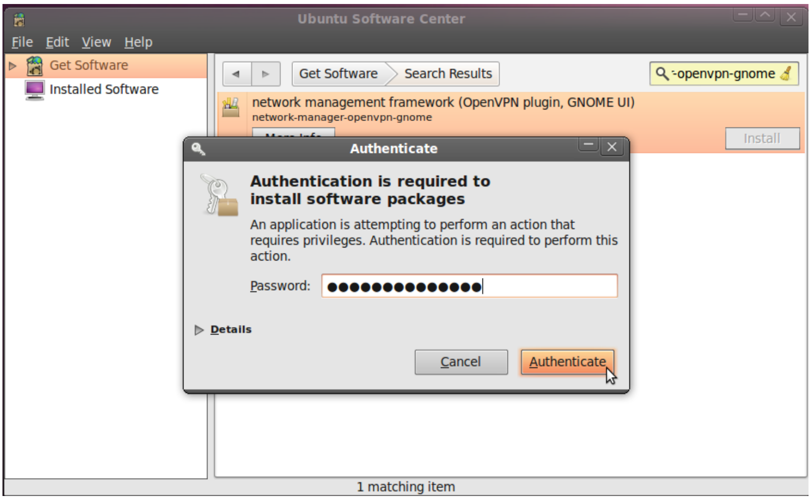
3. In the search box, type in "network-manager-openvpn-gnome" (which is the extension that will enable OpenVPN). It's necessary to type the full names because the packages are classified as "technical" and don't pop-up earlier. These packages include all the files you need to establish a VPN connection successfully.



-openvpn-gnome

network management framework (OpenVPN plugin, GNOME UI)
network-manager-openvpn-gnome

4. Ubuntu may ask you for additional permissions to install the program. If that is the case, type in your password and click Authenticate. Once the package is installed, you can close the Software Center window.



-openvpn-gnome

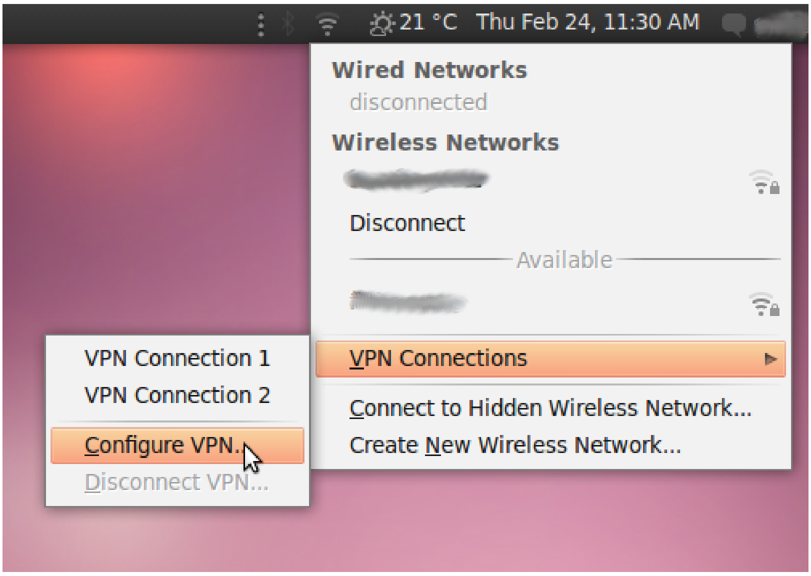
network management framework (OpenVPN plugin, GNOME UI)
network-manager-openvpn-gnome

Authentication is required to install software packages

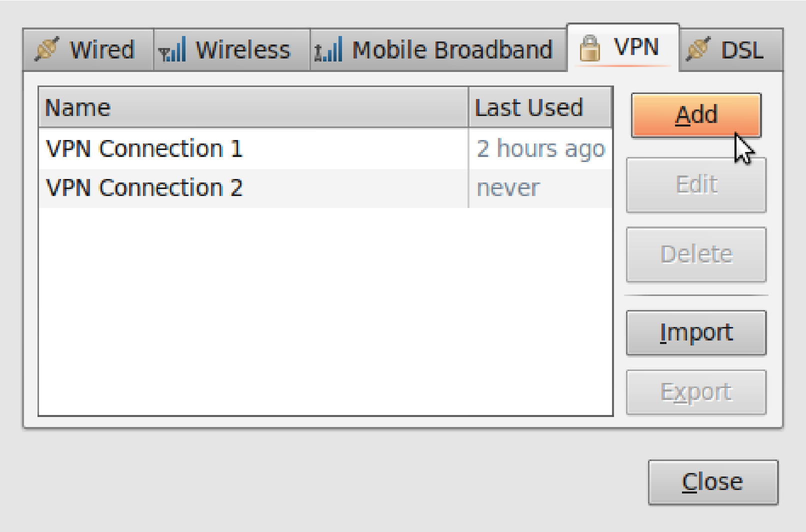
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password: ●●●●●●●●●●●●●●

5. To check if the extensions are correctly installed, click on the NetworkManager (the icon at the left of your system clock) and select VPN Connections > Configure VPN.

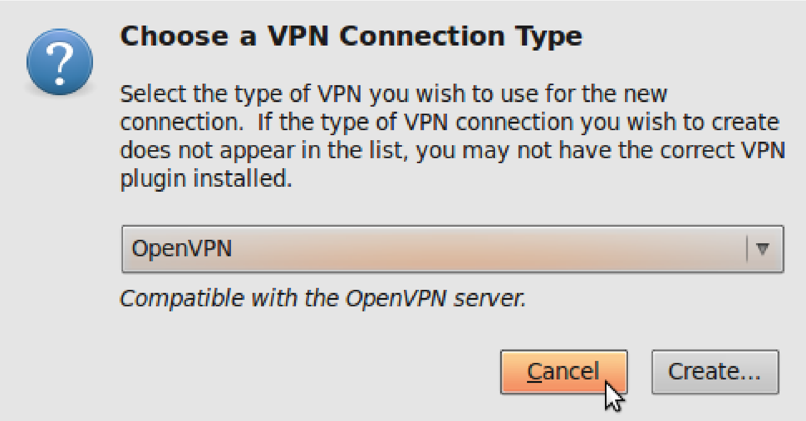


6. Click Add under the VPN tab.



Name	Last Used
VPN Connection 1	2 hours ago
VPN Connection 2	never

7. If you see a pop-up asking for the type of VPN and the tunnel technology (OpenVPN) option is available, this means that you have installed the VPN extension in Ubuntu correctly. If you have your VPN login information ready, you can continue right away, else you first have to get a VPN account from a VPN-provider. If this is the case, click cancel to close the Network Manager.



Choose a VPN Connection Type

Select the type of VPN you wish to use for the new connection. If the type of VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

OpenVPN

Compatible with the OpenVPN server.

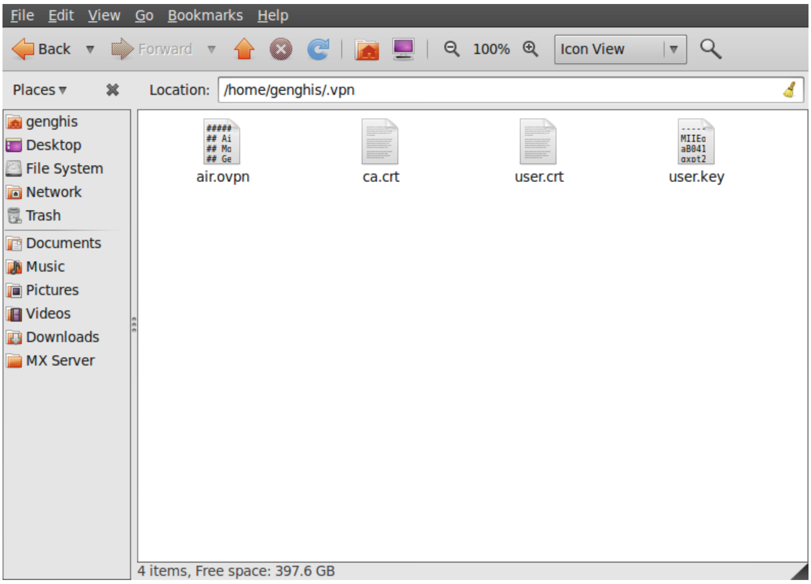
2. Configuring an OpenVPN network

Let's assume you received your configuration files and credentials from your VPN provider. This information should contain the following

- an *.ovpn file, ex. air.ovpn
- The file: ca.crt (this file is specific for every OpenVPN provider)
- The file: user.crt (this file is your personal certificate, used for encryption of data)
- The file: user.key (this file contains your private key. It should be protected in a good manner. Losing this file will make your connection insecure)

In most cases your provider will send these files to you in a zip file. Some openvpn providers use username and password authentication which will not be covered.

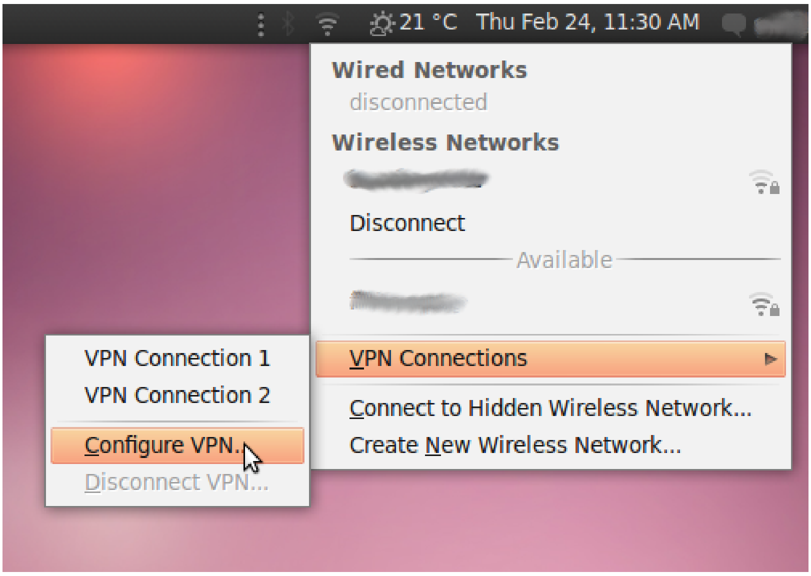
1. Unzip the file you have downloaded to a folder on your hard drive (e.g.: "/home/[yourusername]/.vpn"). You should now have four files. The file "air.ovpn" is the configuration file that you need to import into NetworkManager.



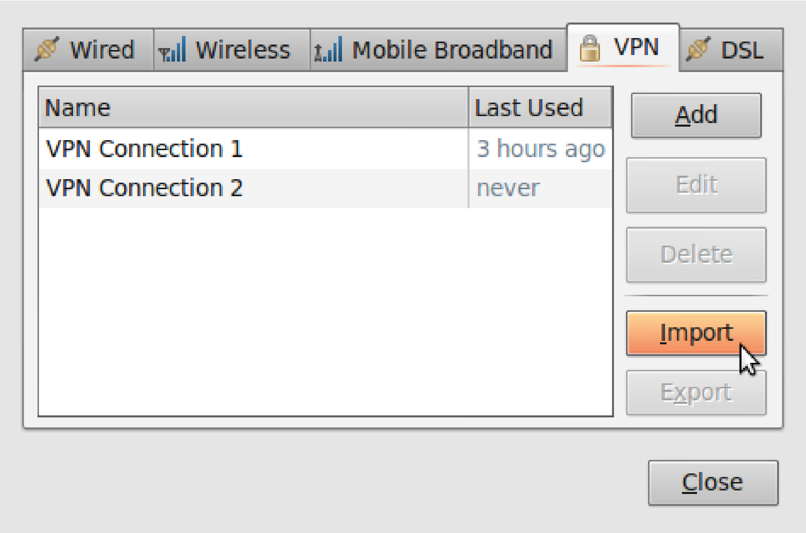
Location: /home/genghis/.vpn

4 items, Free space: 397.6 GB

2. To import the configuration file, open NetworkManager and go to VPN Connections > Configure VPN.

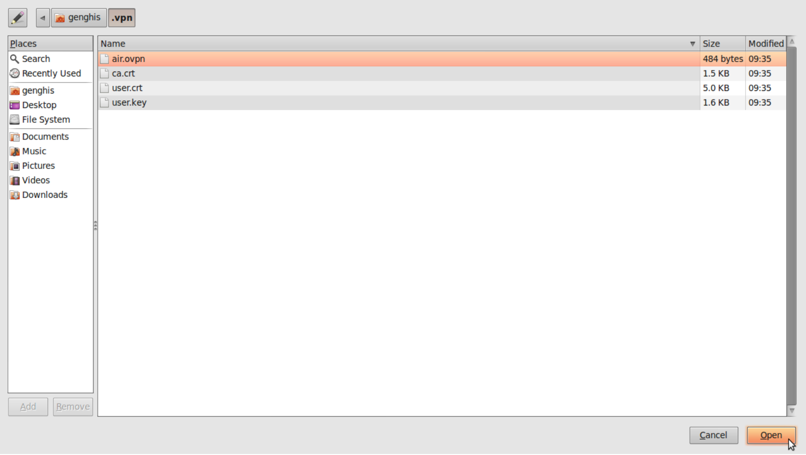


3. Under the VPN tab, click Import.



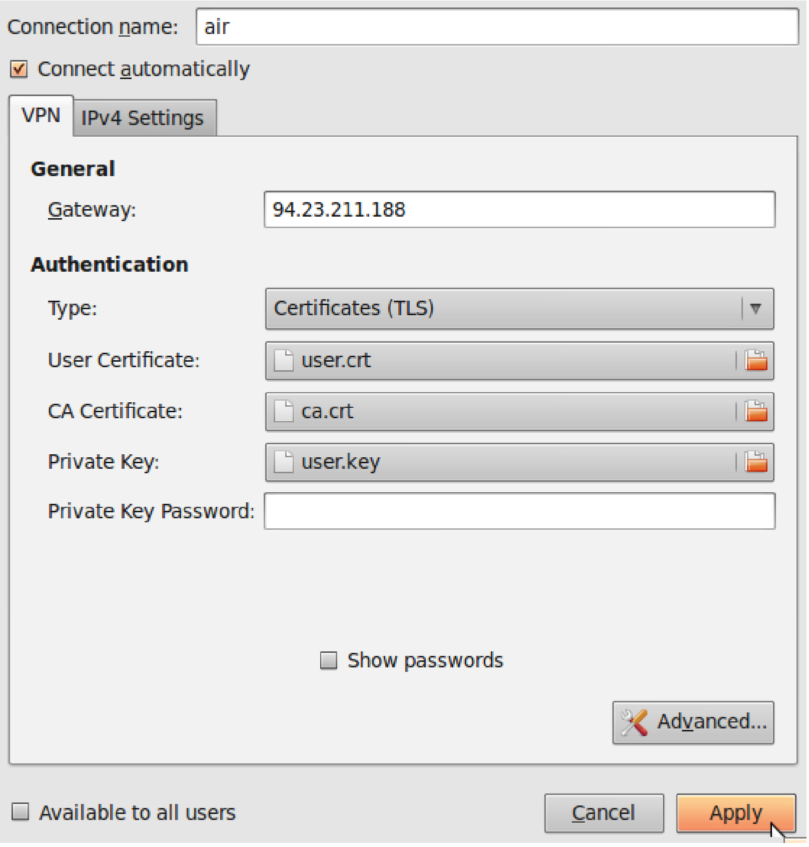
Name	Last Used
VPN Connection 1	3 hours ago
VPN Connection 2	never

4. Locate the file air.ovpn that you have just unzipped. Click Open.



Name	Size	Modified
air.ovpn	484 bytes	09:35
ca.crt	1.5 KB	09:35
user.crt	5.0 KB	09:35
user.key	1.6 KB	09:35

5. A new window will open. Leave everything as it is and click Apply.



Connection name: air

☑ Connect automatically

General

Gateway: 94.23.211.188

Authentication

Type: Certificates (TLS)

User Certificate: user.crt

CA Certificate: ca.crt

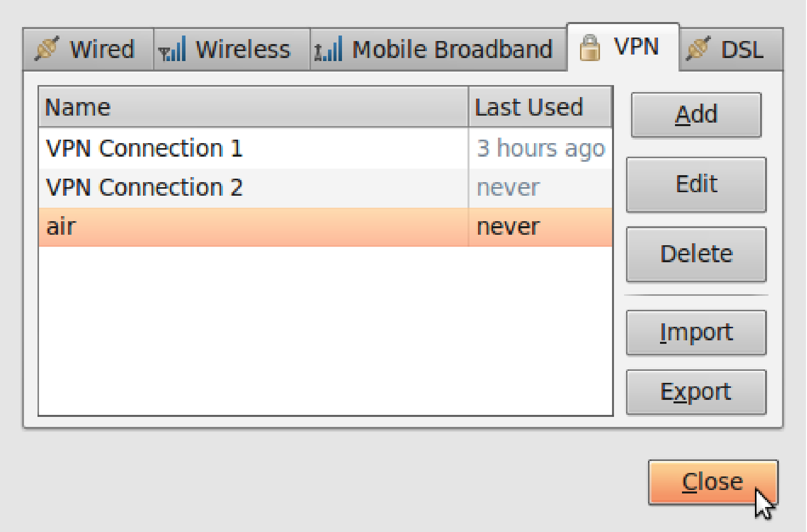
Private Key: user.key

Private Key Password:

□ Show passwords

□ Available to all users

6. Congratulations! Your VPN connection is ready to be used and should appear on the list of connections under the VPN tab. You can now close NetworkManager.

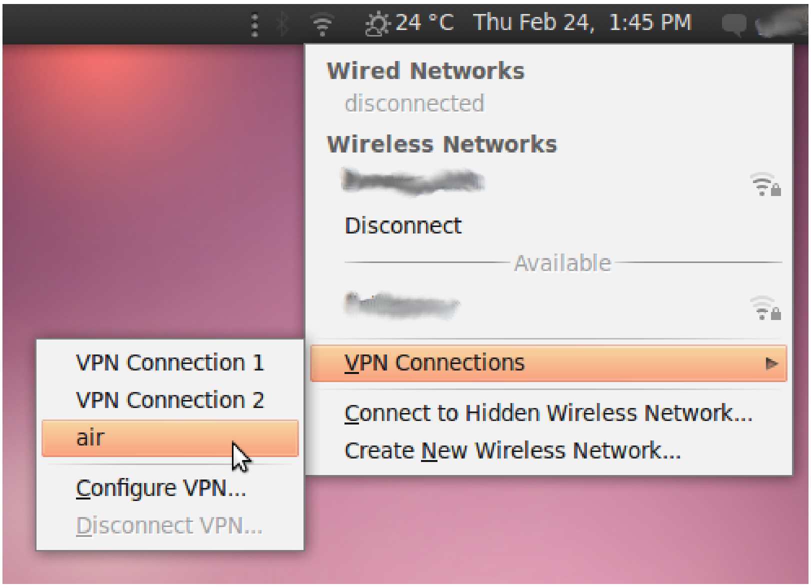


Name	Last Used
VPN Connection 1	3 hours ago
VPN Connection 2	never
air	never

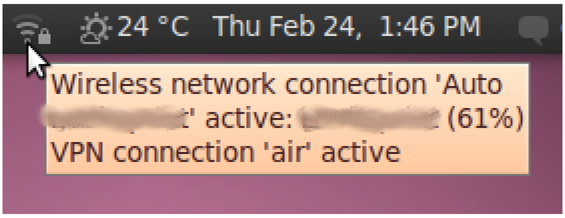
Using your new VPN connection

Now that you configured NetworkManager to connect to a VPN service using the OpenVPN client, you can use your new VPN connection to circumvent Internet censorship. To get started, follow these steps:

1. In the NetworkManager menu, select your new connection from VPN Connections.



2. Wait for the VPN connection to be established. When connected, a small padlock should appear right next to your NetworkManager icon, indicating that you are now using a secure connection. Move your cursor over the icon to confirm that the VPN connection is active.

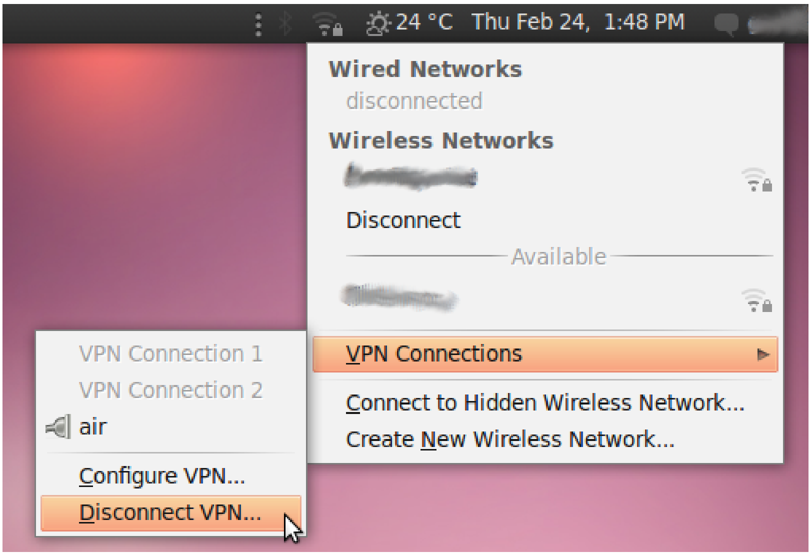


Wireless network connection 'Auto [redacted]' active: [redacted] (61%)
VPN connection 'air' active

3. Test your connection, using the method described in the "Make sure it works" section of this chapter.

4. To disconnect from your VPN, select VPN Connections > Disconnect VPN in

the NetworkManager menu. You are now using your normal connection again.

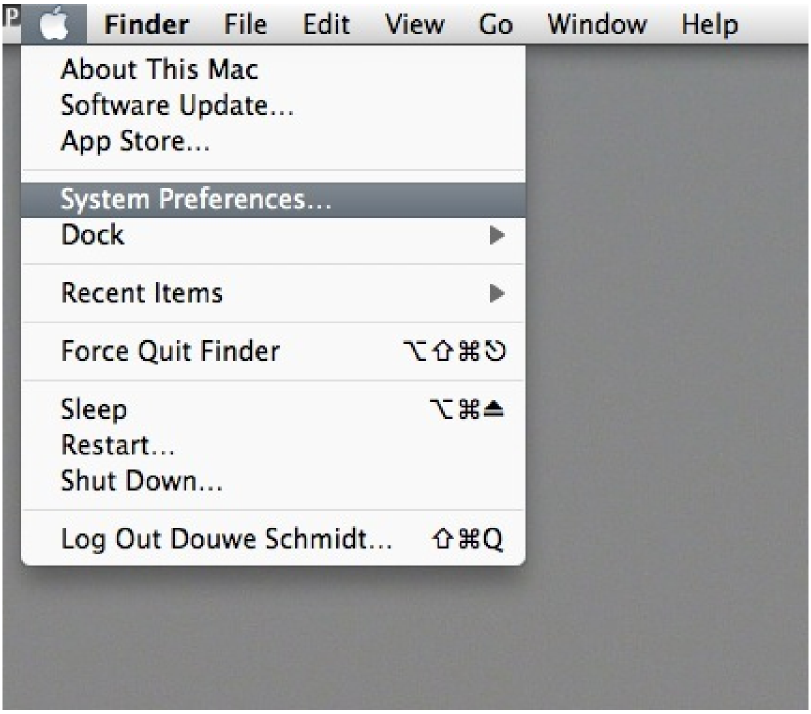


VPN on MacOSX

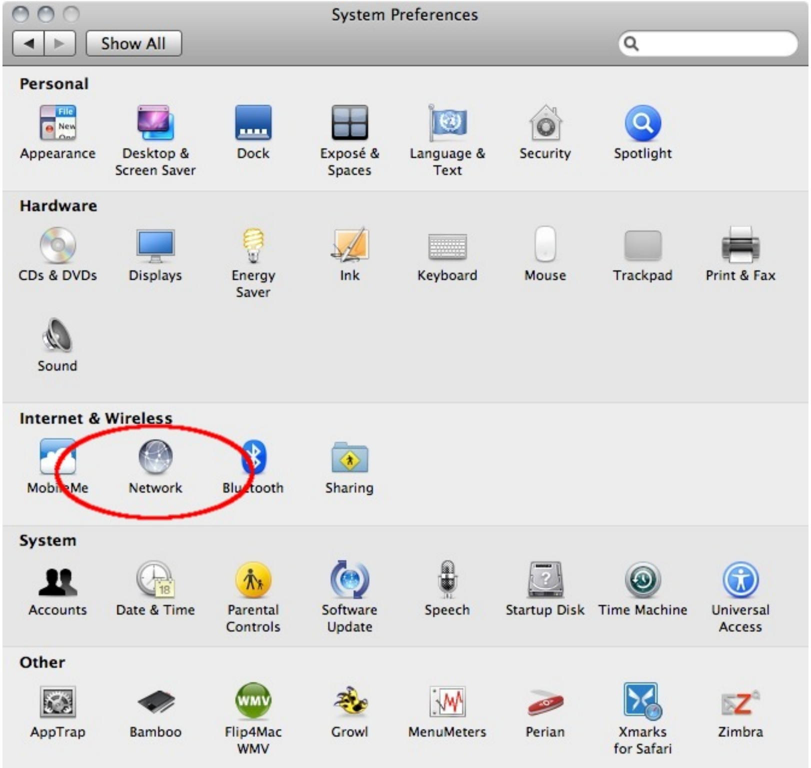
Setting up a VPN on MacOSX is very easy once you have your account details ready, Let's assume have your credentials from your VPN provider for L2TP/IPSec connection ready. This information should contain the following:

- Username, ex. bill2
- Password, ex. verysecretpassword
- VPN server, ex. tunnel.greenhost.nl
- A Pre-Shared-Key or Machine-certificate

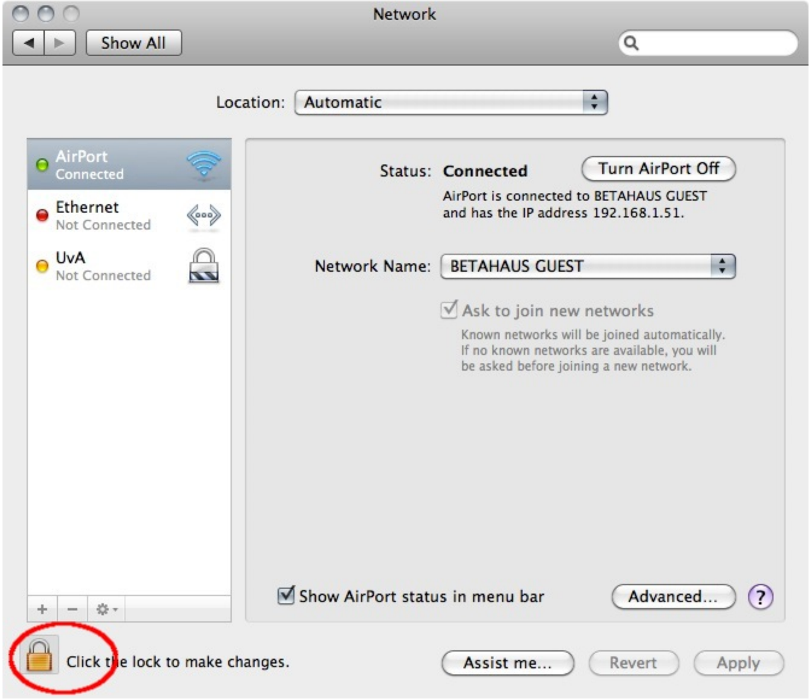
1. Before getting started, please be sure you've read the paragraph "testing before and after account set up", this way you will be able to validate if your connection is actually working after set up.
2. A VPN is configured in the network settings, that are accessible via "System Preferences.." in the Apple menu.



3. Next, open the Network preferences .



4. OSX uses this nifty system to lock windows. To add a VPN it is necessary to unlock the screen: you can do this by clicking on the lock on the left bottom of the screen.



Location: Automatic

AirPort Connected

Ethernet Not Connected

UvA Not Connected

Status: Connected

AirPort is connected to BETAHAUS GUEST and has the IP address 192.168.1.51.

Network Name: BETAHAUS GUEST

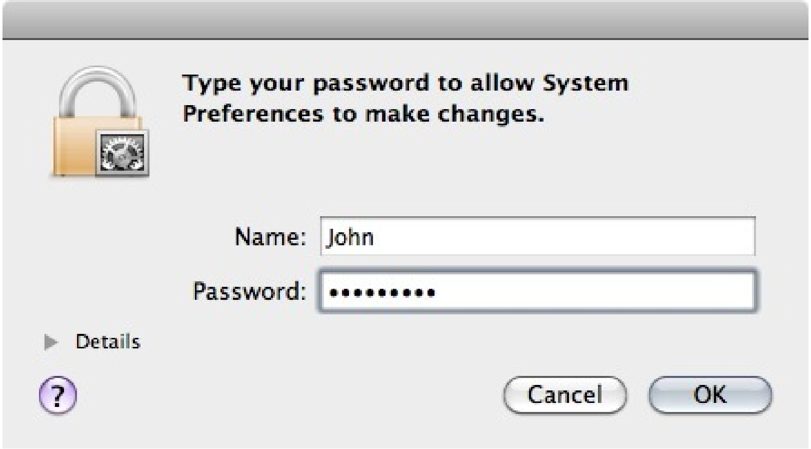
☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show AirPort status in menu bar

Click the lock to make changes.

5. Enter our user credentials

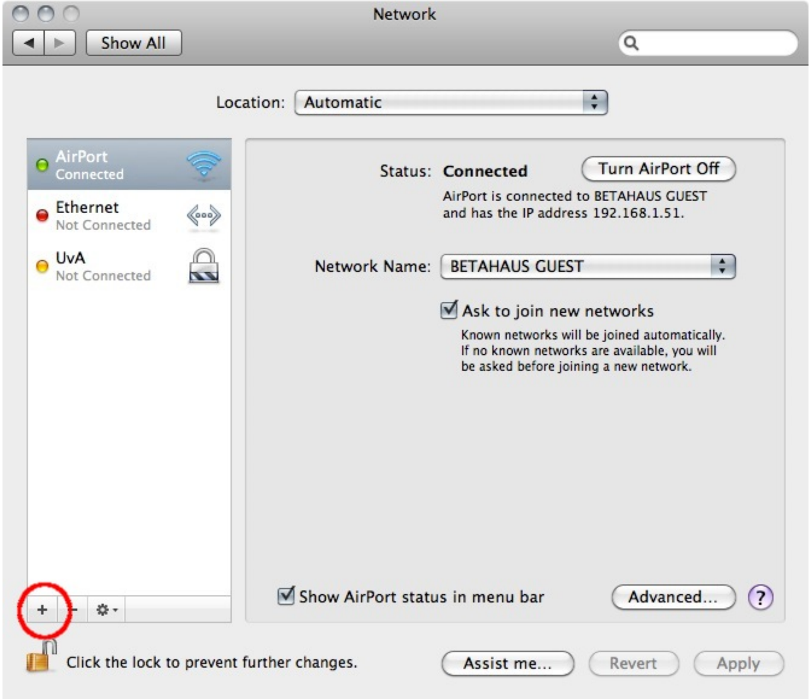


Type your password to allow System Preferences to make changes.

Name: John

Password: ••••••••••

6. Now we can add a new network. Do this by clicking on the "+" sign



Location: Automatic

Status: Connected

AirPort is connected to BETAHAUS GUEST and has the IP address 192.168.1.51.

Network Name: BETAHAUS GUEST

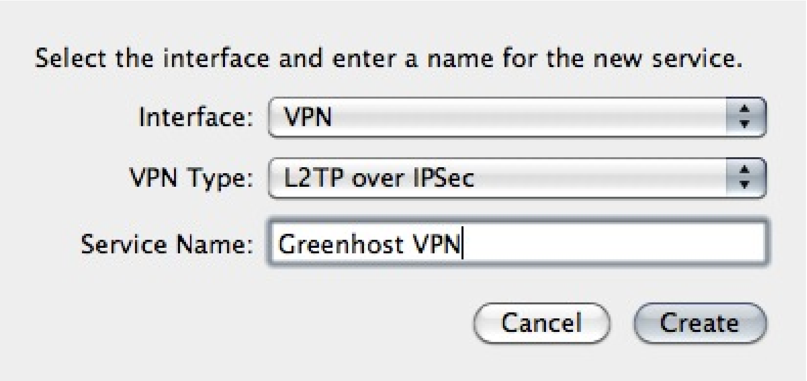
☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

7. In the pop-up you need to specify the type of connection. In this case choose an VPN interface with L2TP over IPSec. This is the most common system. Also don't forget to give the connection a nice name.



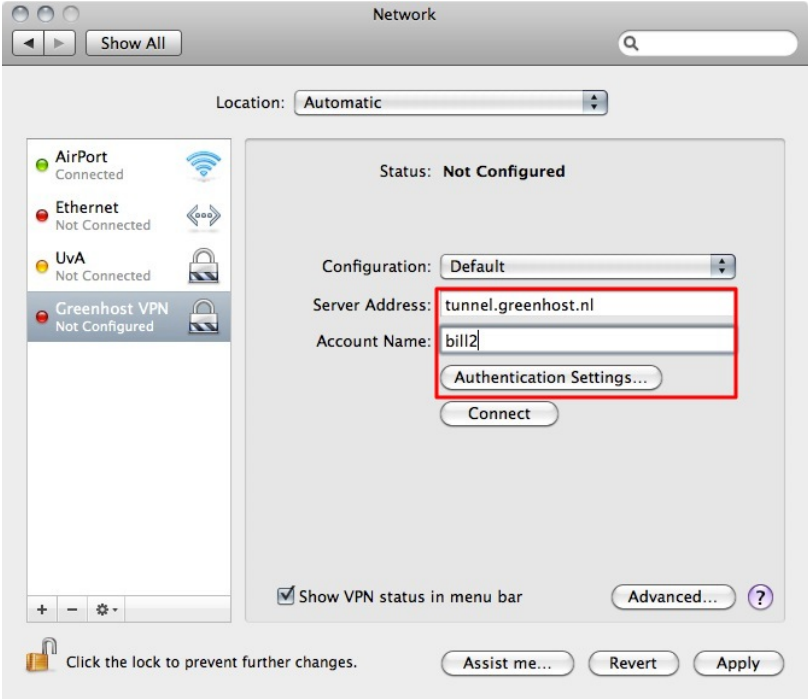
Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: L2TP over IPSec

Service Name: Greenhost VPN

8. Next comes the connection data. Please fill in the provided server name and user name (called 'Account Name'). If this is done, click on the "Authentication Settings..." button



Location: Automatic

AirPort Connected

Ethernet Not Connected

UvA Not Connected

Greenhost VPN Not Configured

Status: Not Configured

Configuration: Default

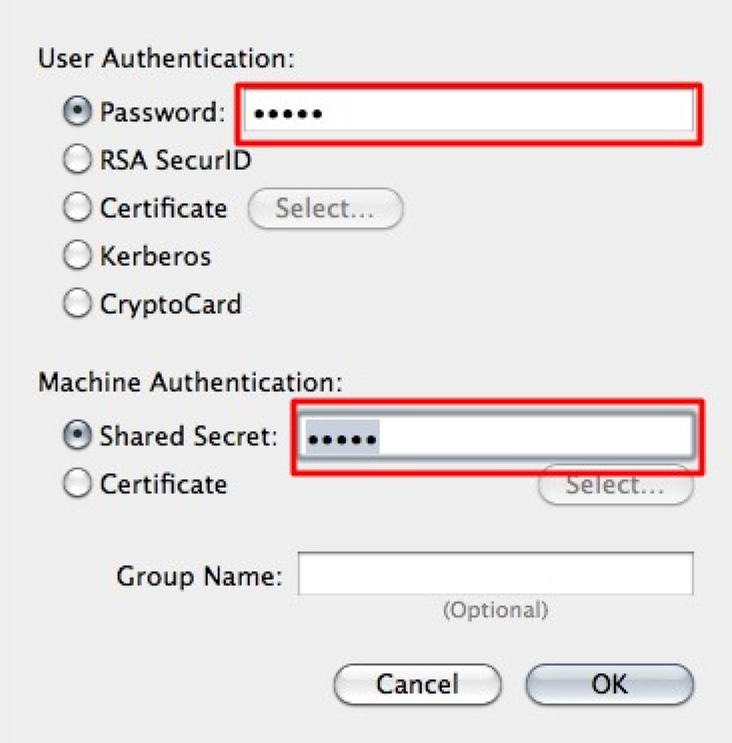
Server Address: tunnel.greenhost.nl

Account Name: bill2

☑ Show VPN status in menu bar

Click the lock to prevent further changes.

9. In the new pop-up you can specify connection specific information. This is the way the user is authenticated and how the machine is authenticated. The user is very commonly authenticated by using a password, although other methods are possible. Machine authentication is often done by a Shared Secret (Pre-Shared-Key/PSK), but also quite often by using a certificate. In this case we use the Shared Secret method. When this is done click OK.



User Authentication:

● Password: •••••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Machine Authentication:

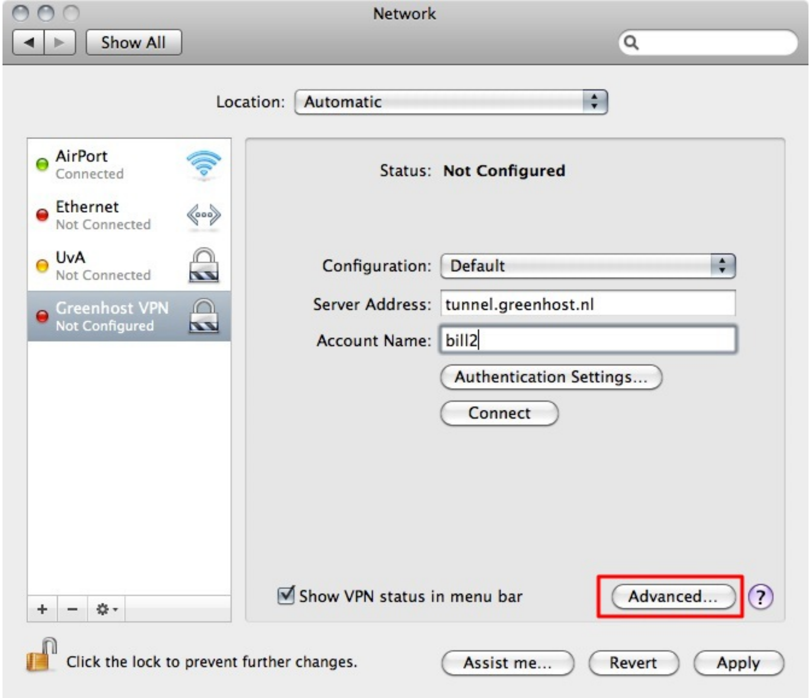
● Shared Secret: •••••

○ Certificate

Group Name:

(Optional)

10. Now you return back to the network screen. The next step is very important, so click on "Advanced..."



Network

Location: Automatic

AirPort Connected

Ethernet Not Connected

UvA Not Connected

Greenhost VPN Not Configured

Status: Not Configured

Configuration: Default

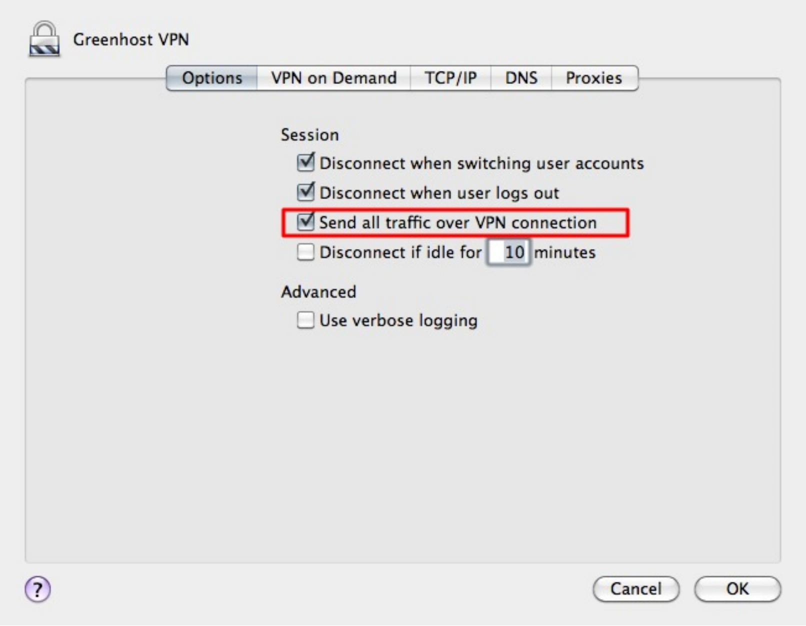
Server Address: tunnel.greenhost.nl

Account Name: bill2

☑ Show VPN status in menu bar

Click the lock to prevent further changes.

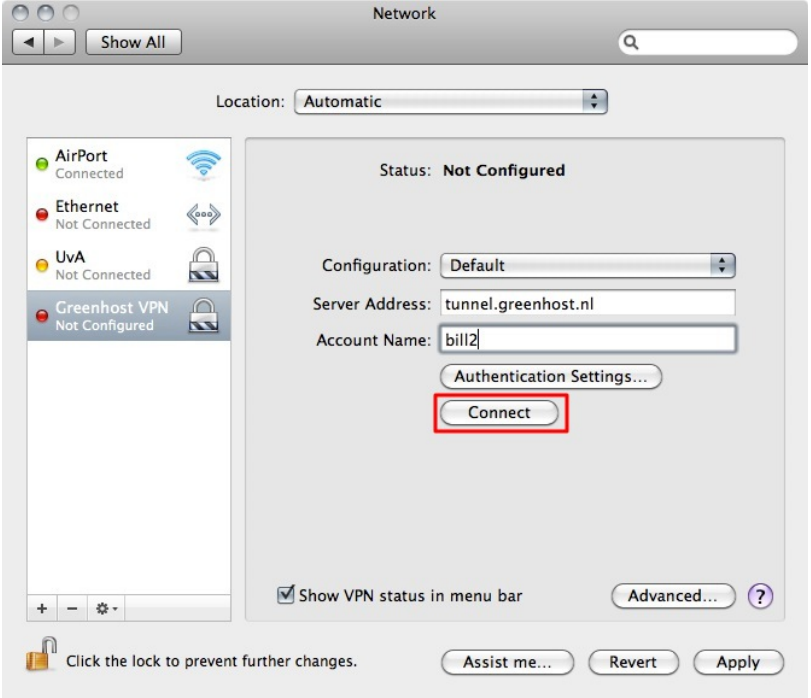
11. In the new pop up you will see an option to route all traffic through the VPN connection. We want to enable this, so all our traffic is encrypted.



Session
☑ Disconnect when switching user accounts
☑ Disconnect when user logs out
☑ Send all traffic over VPN connection
□ Disconnect if idle for 10 minutes

Advanced
□ Use verbose logging

12. Well, all is done. Now hit the Connect button!



Location: Automatic

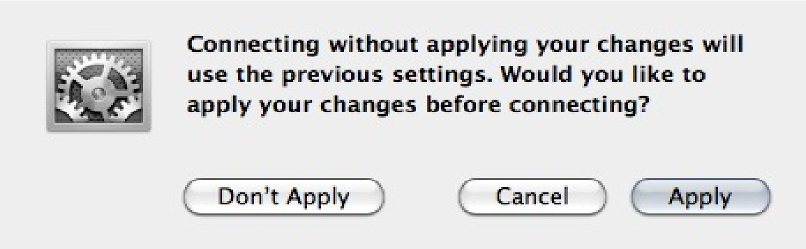
Status: Not Configured

Configuration: Default
Server Address: tunnel.greenhost.nl
Account Name: bill2

☑ Show VPN status in menu bar

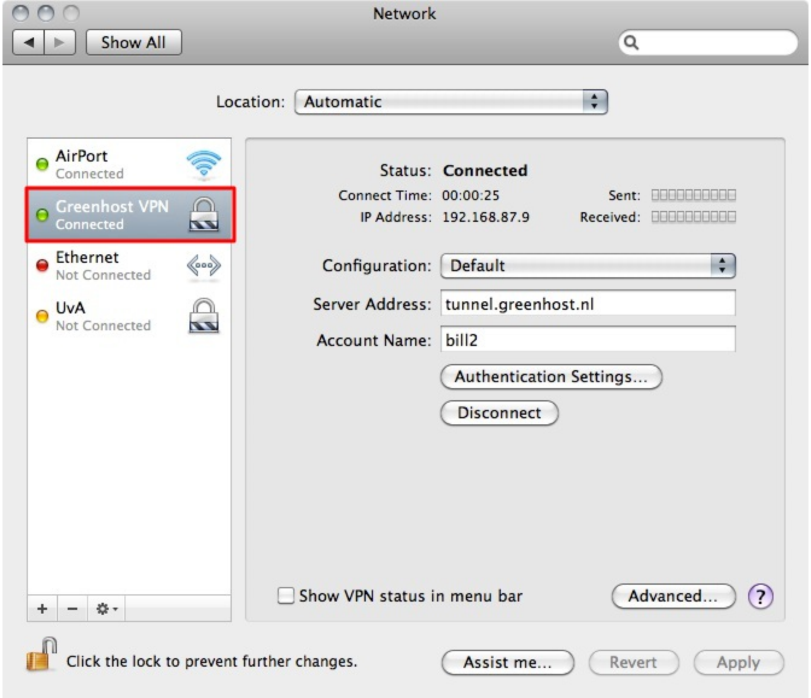
Click the lock to prevent further changes.

13. A pop-up appears. You need to confirm your changes, just hit "Apply"



Connecting without applying your changes will use the previous settings. Would you like to apply your changes before connecting?

14. After a few seconds, on the left side the connection should turn green. If so, you are connected!



Status: Connected

Connect Time: 00:00:25

IP Address: 192.168.87.9

Configuration: Default

Server Address: tunnel.greenhost.nl

Account Name: bill2

□ Show VPN status in menu bar

15. Ok, now test your connection!

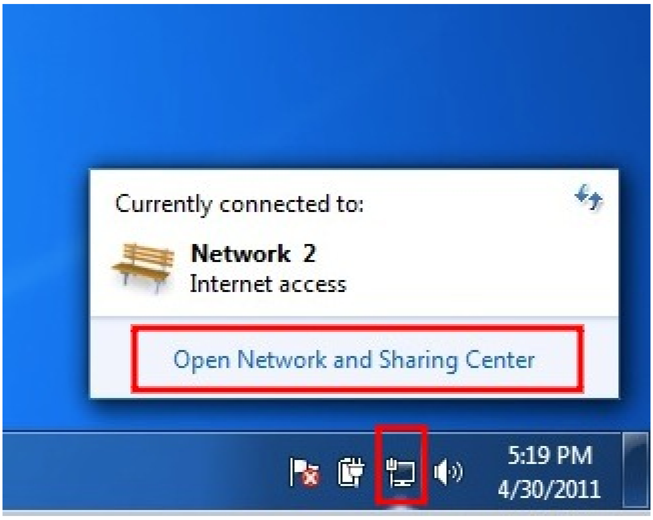
VPN on Windows

Setting up a VPN on Windows is very easy once you have your account details ready. Let's assume have your credentials from your VPN provider for L2TP/IPSec connection ready. This information should contain the following:

- Username, ex. bill2
- Password, ex. verysecretpassword
- VPN server, ex. tunnel.greenhost.nl
- A Pre-Shared-Key or Machine-certificate

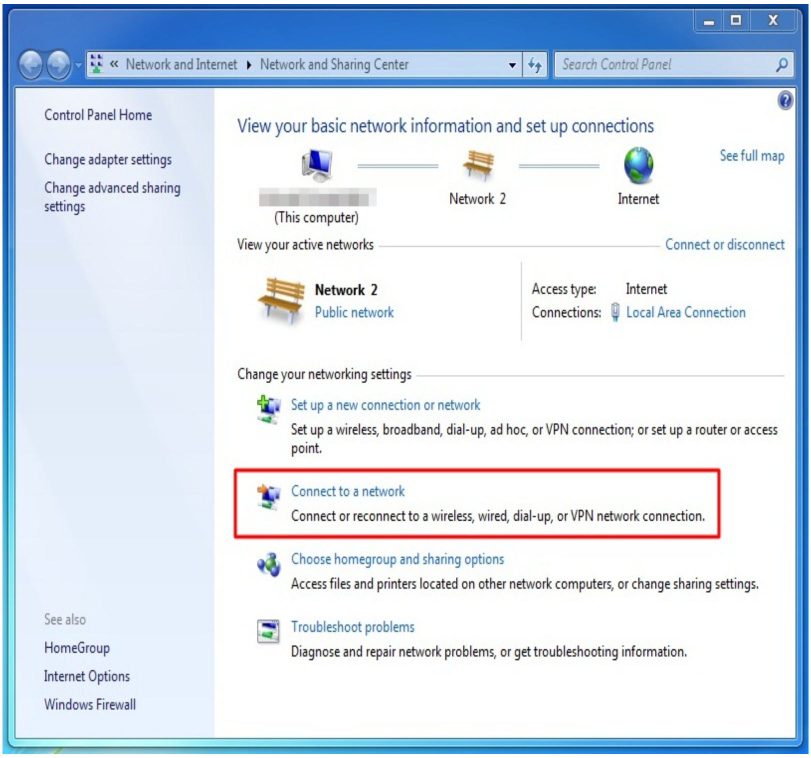
1. Before getting started, please be sure you've read the paragraph "testing before and after account set up", this way you will be able to validate if your connection is actually working after set up.

2. We need to go to the "Network and Sharing Center" of Windows to create a new VPN connection. We can access this center easily by clicking on the network icon next to the systemclock en click on "open Network and Sharing Center"



3. The "Network and Sharing Center" will popup. You will see some information about your current network. Click on "Connect to a network" to

add a VPN connection.



View your basic network information and set up connections

View your active networks

Change your networking settings

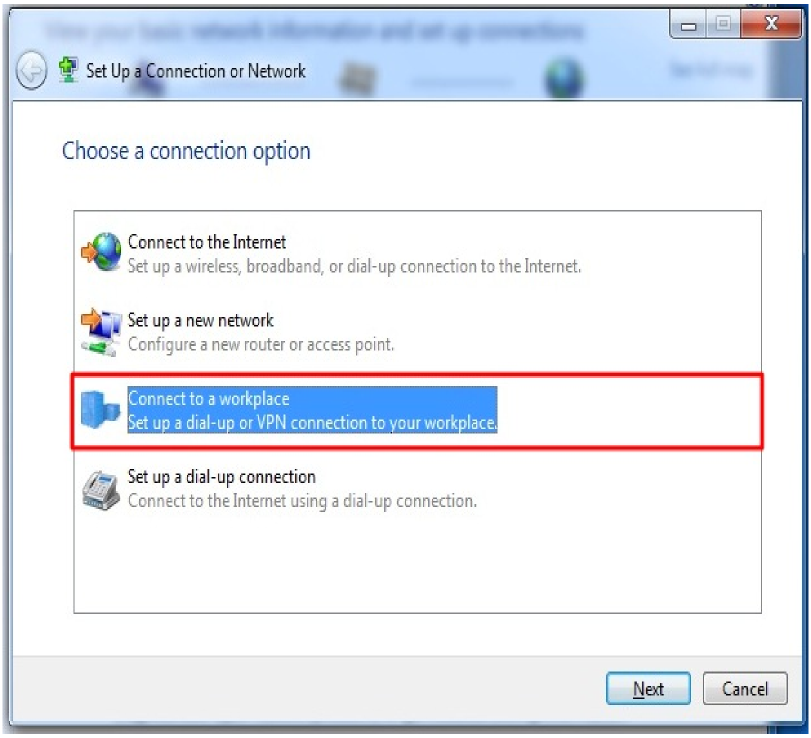
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Access files and printers located on other network computers, or change sharing settings.

Diagnose and repair network problems, or get troubleshooting information.

4. The wizard to setup a connection will popup. Choose the option to "connect to a workplace", which is Microsoft's way of naming a VPN connection.



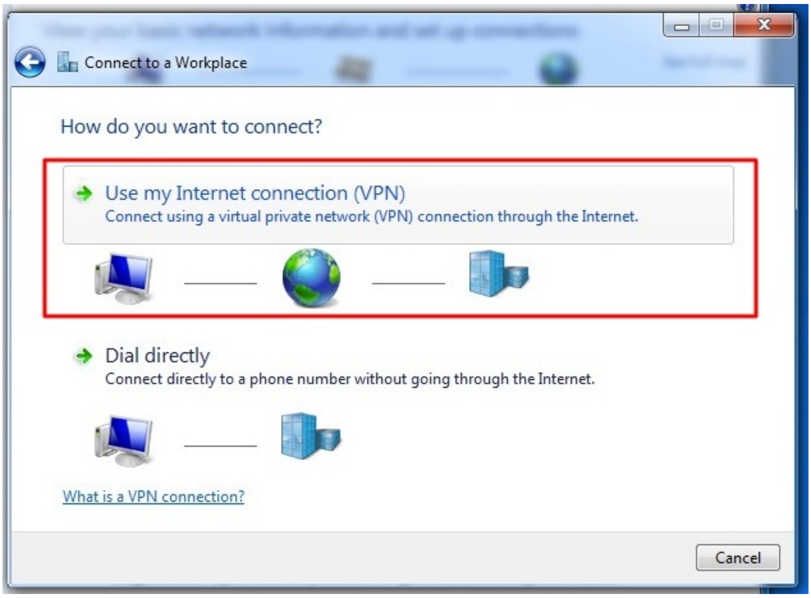
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

5. The next screen asks us if we want to use our Internet connection or an old-skool phone line to connect to the VPN. Just choose the first option then.

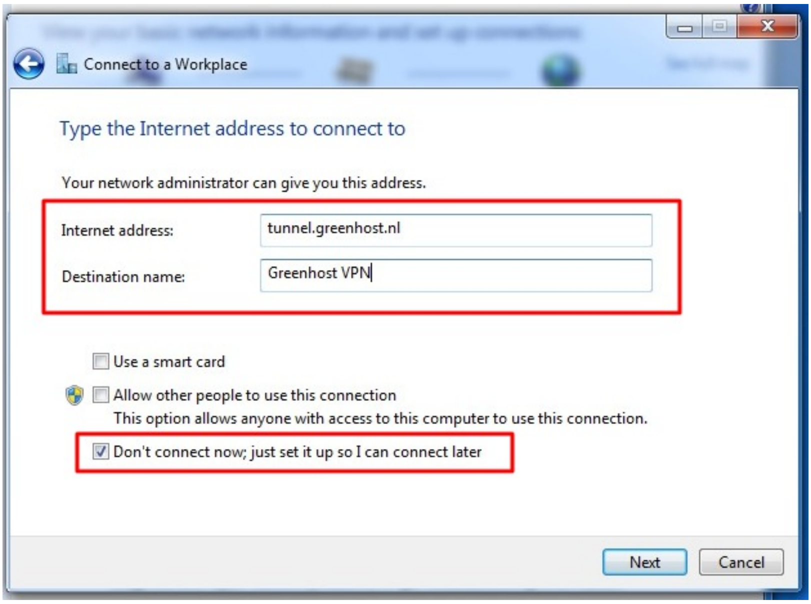


Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

6. The next screen asks for the connection details. Enter here the server of

your VPN-provider (called "Internet address" in this dialog). On the bottom please check the box "Don't connect now; just set it up". Using this option the connection will be automatically saved and it's easier to control extra settings. If this is all done, hit the "next" button



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: tunnel.greenhost.nl

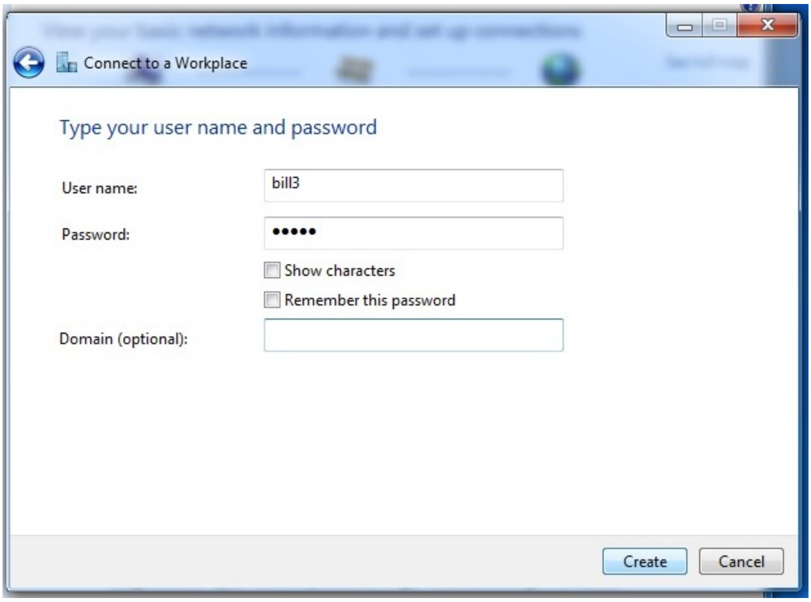
Destination name: Greenhost VPN

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

7. Next up are your username and password. Just give them like you received them from your VPN-provider. If the connection fails, Windows forgets them. So keep them with you, you maybe need them later. If this is done. Click "create".



Type your user name and password

User name: bill3

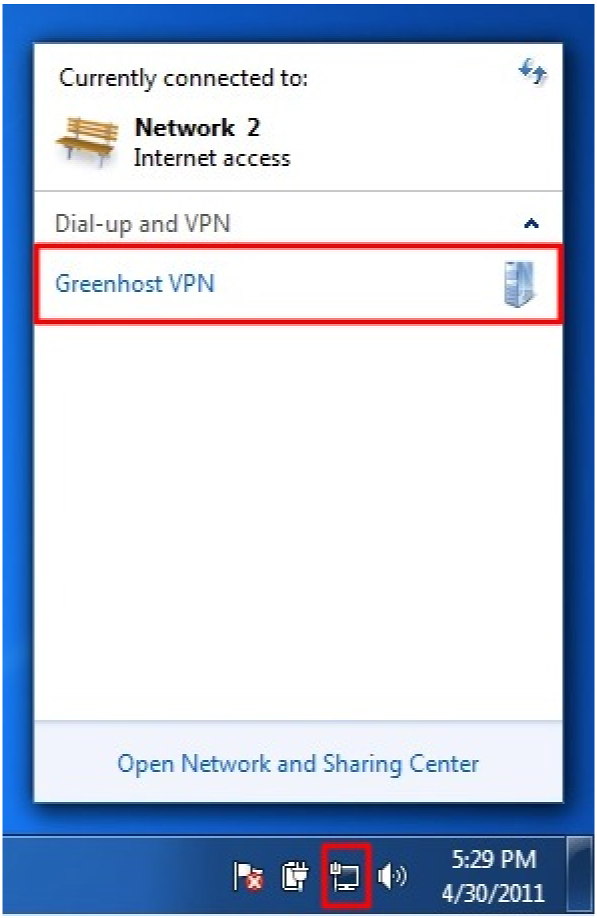
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

8. Your connection is now available, if you click the the network icon again, you will see a new option in the network menu, the name of your VPN connection, just click it to connect.



Currently connected to:

Network 2
Internet access

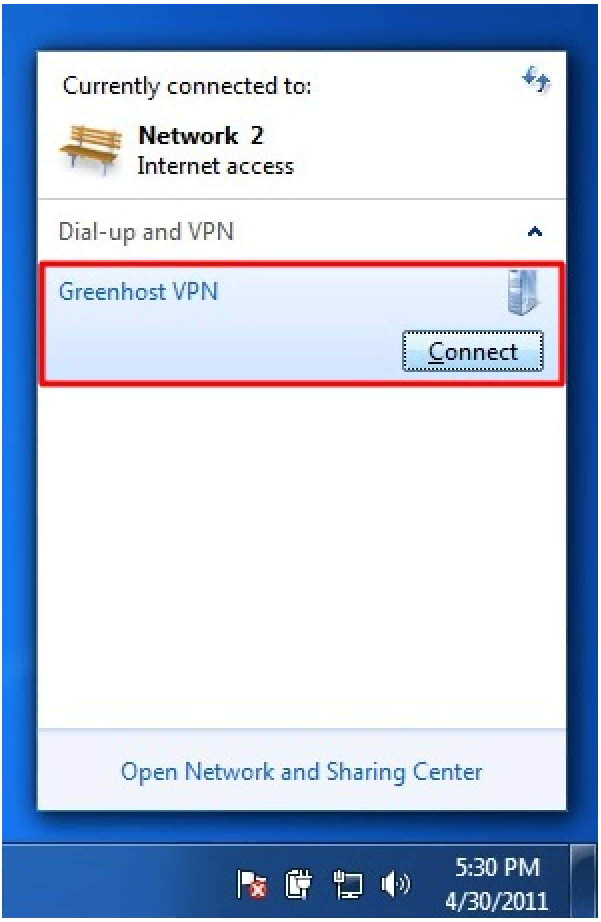
Dial-up and VPN

Greenhost VPN

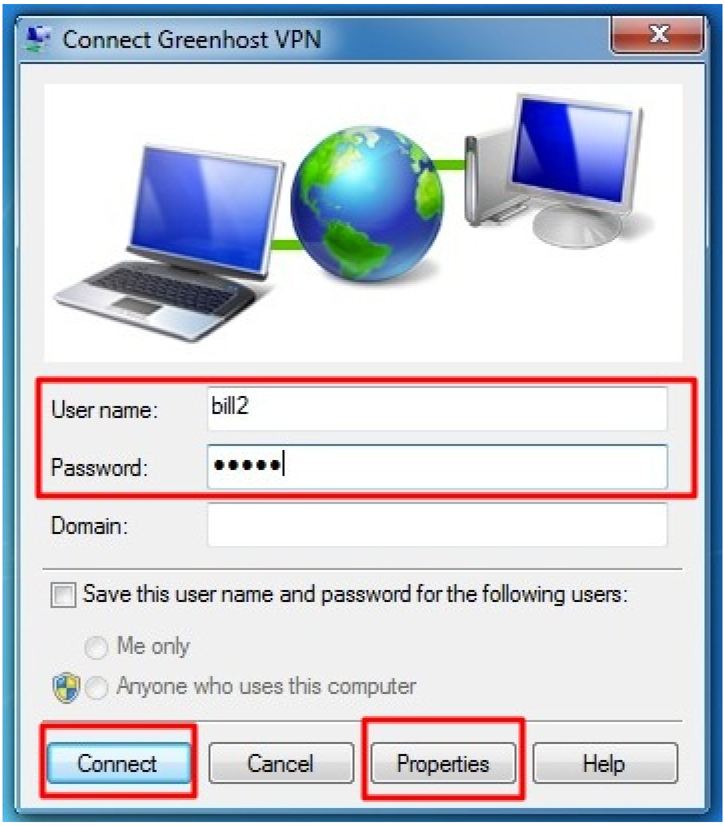
Open Network and Sharing Center

5:29 PM
4/30/2011

9. And click "connect"



10. A VPN connection dialog appears. This give us the opportunity to review our settings and to connect. You can try to connect, Windows will try to discover all other settings automatically. Unfortunately, this does not always work, so if this is not working for you, hit the "properties" button.



User name: bill2

Password: •••••

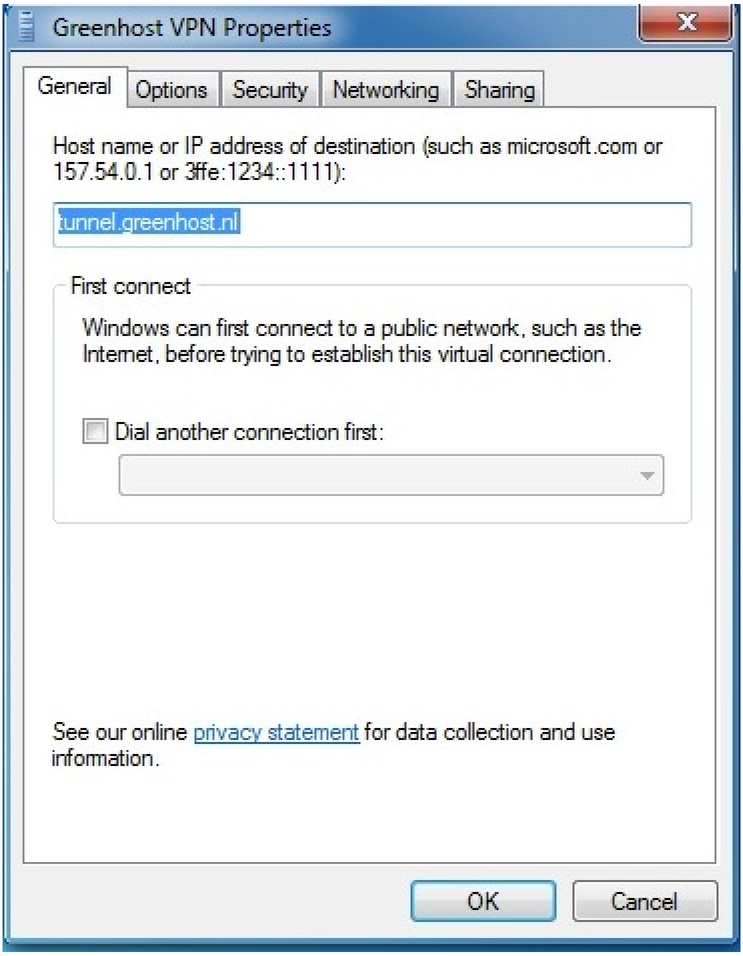
Domain:

□ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

11. The properties windows appear. The most important page is the "Security" page, click on the Security tab to open it.



Greenhost VPN Properties

Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

tunnel.greenhost.nl

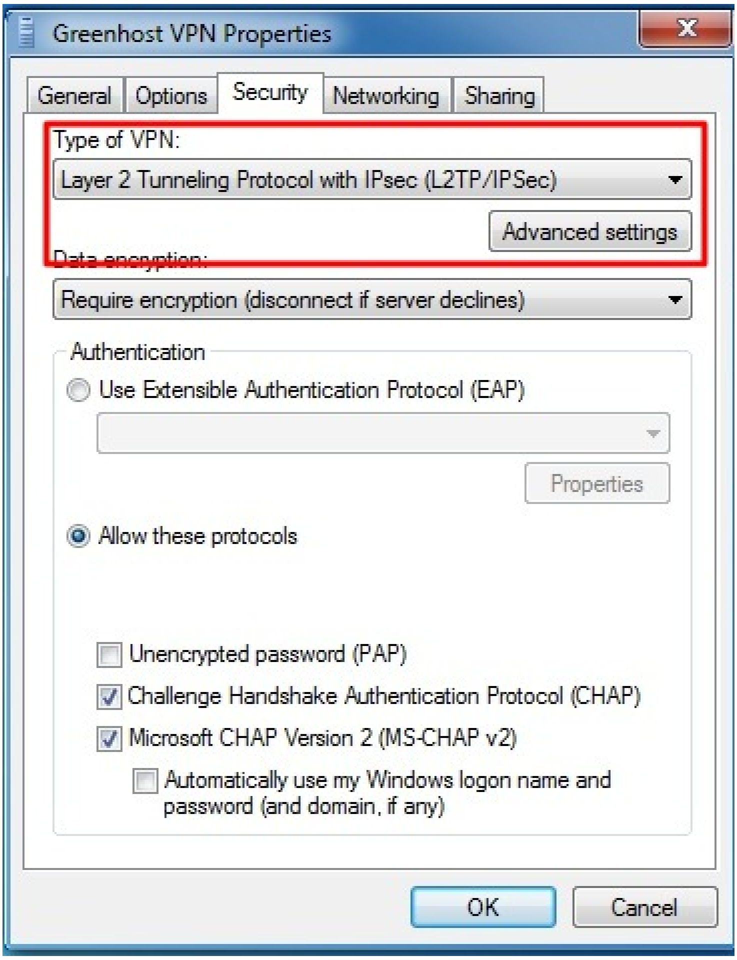
First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:

See our online privacy statement for data collection and use information.

12. In the security tab you can specify VPN type, normally L2TP/IPSec. Do not use PPTP as it has several security vulnerabilities. For L2TP/IPSec also have a look at the Advanced settings.



Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

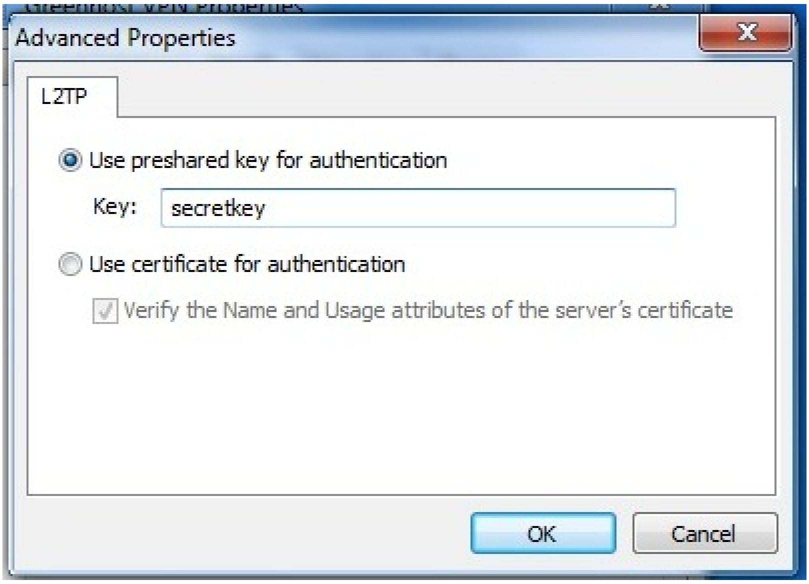
□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

13. In the Advanced Settings window, you can specify if you are using a pre-shared key or a certificate. This depends on your VPN-provider. If you have received a pre-shared-key, Select this option and fill in this key. Hit ok afterwards. You will return to the previous window, click ok there also



Advanced Properties

L2TP

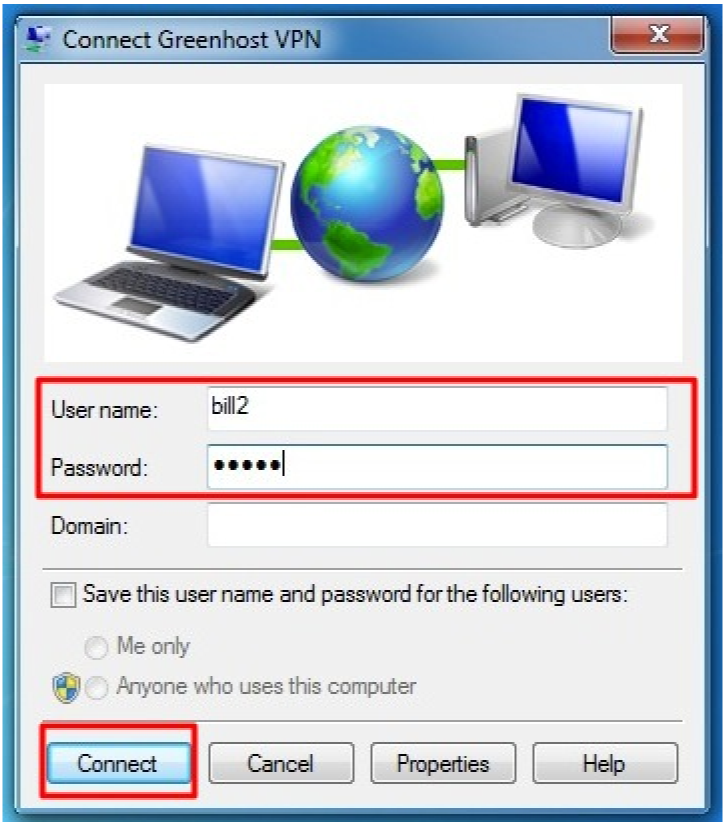
● Use preshared key for authentication

Key: secretkey

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

14. Back in to connection window try to connect now. Please be sure your username and password are filled out.



Connect Greenhost VPN

User name: bill2

Password: ●●●●●

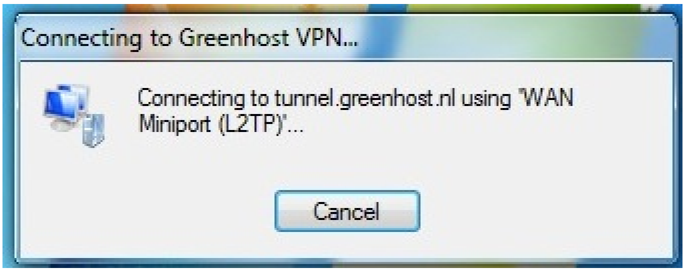
Domain:

□ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

15. A connection popup will appear



Connecting to Greenhost VPN...

Connecting to tunnel.greenhost.nl using 'WAN Miniport (L2TP)'...

16. Online! Don't forget to check if your VPN is working properly.

Make sure it works

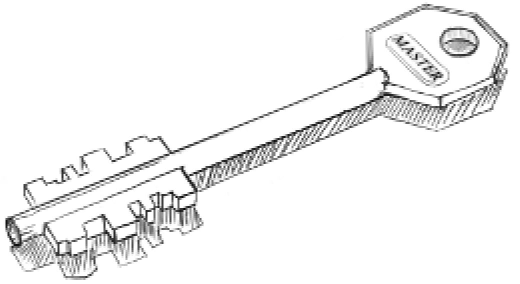
Probably one of the first things that you would like to make sure of right after your VPN connection has been set up is whether your data is actually passing via the VPN network. The simplest (and reliable) test is to check what your "external" IP address is, the address which you are exposing to the Internet. There are numerous websites online that can report your IP address and its geo-location.

One of such services is: http://www.myip.se (and try using others too!)

Hoping that you have followed our advice and chose a VPN provider from a foreign country (rather then the country you are in) you will see that your IP geo-location reported as a remote location. Nowadays, almost any online search engine will report your IP address if you search for "my ip". To be absolutely sure that your traffic is redirected via the VPN simply search for "my ip" before connecting to VPN and beyond.. The results should differ.

Once you know that your external IP has been changed to the IP of your VPN server you can rest assured your communication is encrypted - VPN connection would not succeed were there any errors.

Disk Encryption



Installing TrueCrypt

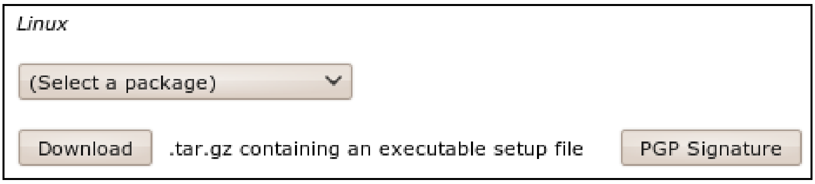
TrueCrypt can be installed on Windows, Linux, or Mac OSX. The installation files are available here: http://www.truecrypt.org/downloads

The following gives complete detail on how to install TrueCrypt on your computer for each of these Operating Systems, starting with Ubuntu.

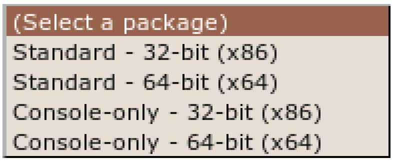
Installing on Ubuntu

TrueCrypt is not available in the standard Ubuntu repositories. This means you cannot use the Ubuntu Software Center or *apt-get* (a command line method for installing software on Ubuntu) to install it. Instead you must first visit the TrueCrypt downloads page (http://www.truecrypt.org/downloads).

You will see a drop-down menu under the heading *Linux*.



From the '(Select a package)' drop down menu you can choose from four options:



This is a little technical - the console version is the one you choose if you are either very technical and don't like Graphical User Interfaces or you wish to run this on a machine that you have only a terminal (command line or 'shell') access to (like a remote server for example).

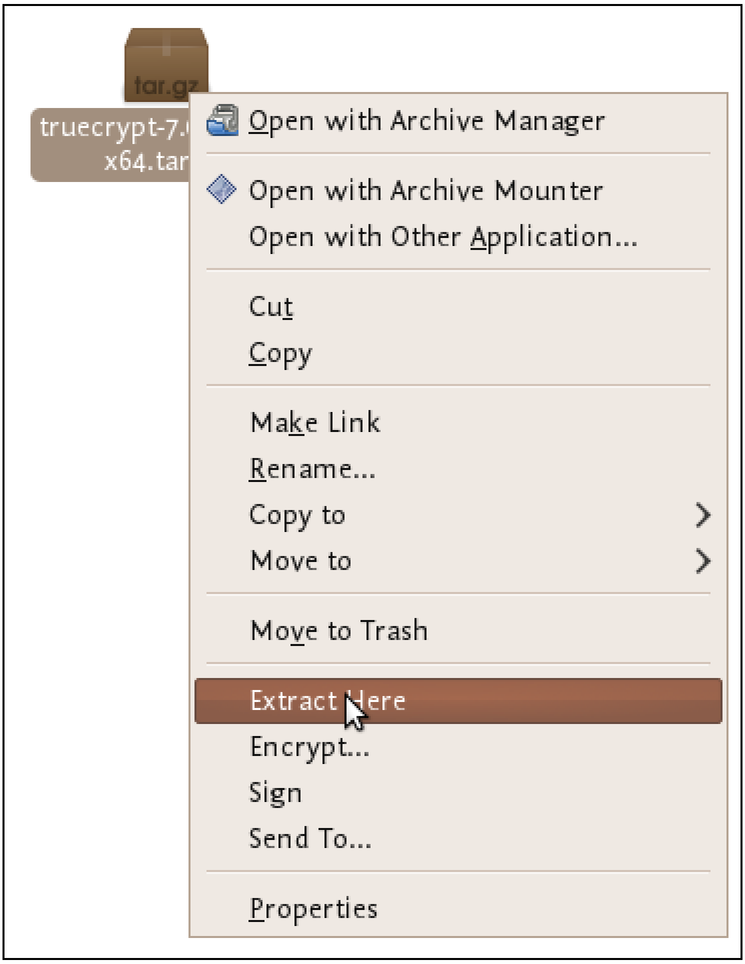
Assuming you are running this in your laptop its best to choose the easy 'standard' option - this will give you a nice user interface to use. From these two options you need to choose the one most suitable for the *architecture* of your machine. Don't know what this means? Well, it basically comes down to the type of hardware (processor) running on your computer, the options are 32-bit or 64-bit. Unfortunately Ubuntu does not make it easy for you to find this information if you don't already know it. You need to open a 'terminal' from the Applications->Accessories menu and type the following, followed by the [enter] key

```
uname -a
```

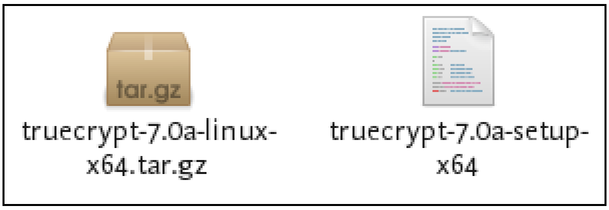
The output will be something like 'Linux bigsy 2.6.32-30-generic #59-Ubuntu SMP Tue Mar 1 21:30:46 UTC 2011 **x86_64** GNU/Linux'. In this instance you can see the architecture is 64-bit ('x86_64'). In this example I would choose the 'Standard - 64-bit (x64)' option. If you see 'i686' somewhere in the output of the uname command then you would choose the other standard option to download.

Once selected press the 'download' button and save the file to somewhere on your computer.

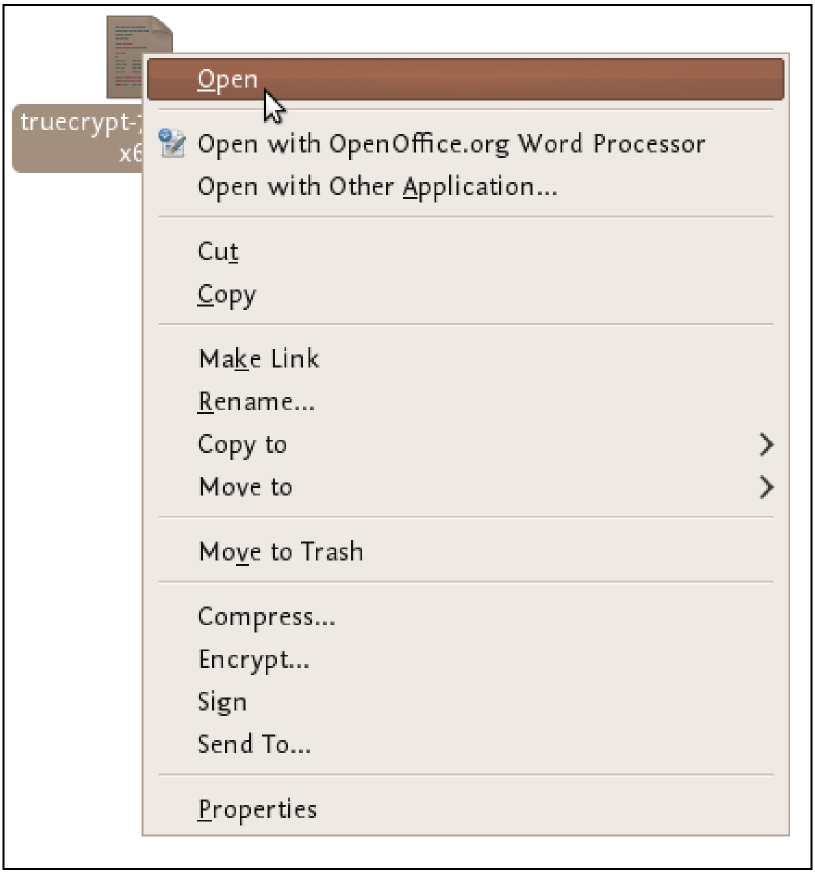
So the installation process is still not over. The file you downloaded is a compressed file (to make downloading it is faster) and you need to first de-compress the file before you install it. Fortunately Ubuntu makes this easy - simply browse to the file on your computer and right click on it and choose 'Extract Here'.



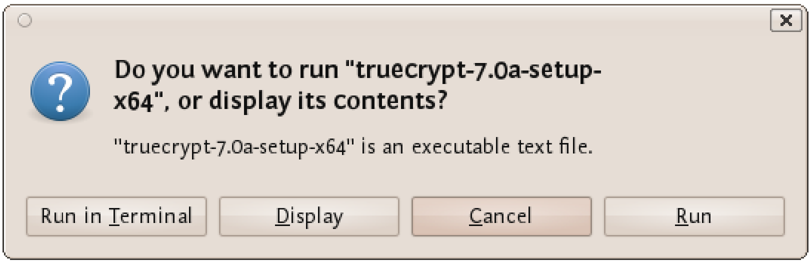
You will see a new file appear next to the compressed file:



Nearly done! Now right click on the new file and choose 'open' :

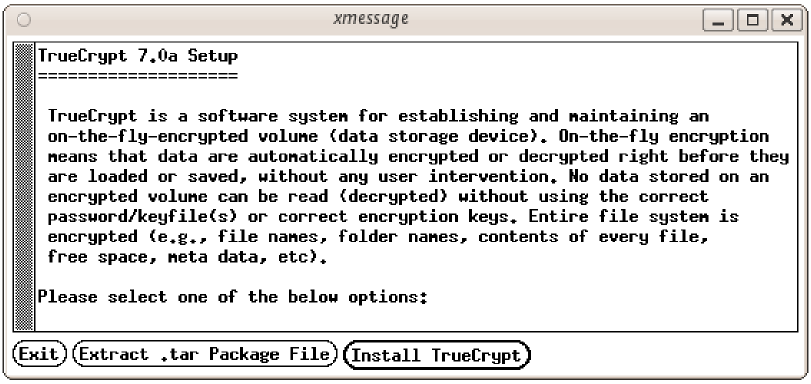


If all is well you will see a window open like this:


Do you want to run "truecrypt-7.0a-setup-x64", or display its contents?

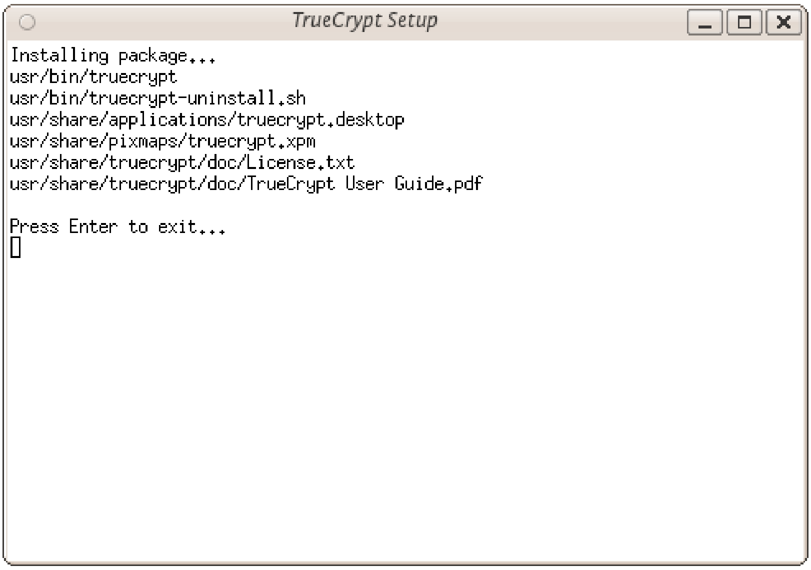
"truecrypt-7.0a-setup-x64" is an executable text file.

Choose 'run' and you see the following:



```
TrueCrypt 7.0a Setup
====================

 TrueCrypt is a software system for establishing and maintaining an
 on-the-fly-encrypted volume (data storage device). On-the-fly encryption
 means that data are automatically encrypted or decrypted right before they
 are loaded or saved, without any user intervention. No data stored on an
 encrypted volume can be read (decrypted) without using the correct
 password/keyfile(s) or correct encryption keys. Entire file system is
 encrypted (e.g., file names, folder names, contents of every file,
 free space, meta data, etc).

Please select one of the below options:
```

Now we are getting somewhere...press 'Install TrueCrypt'. You will be displayed a user agreement. At the bottom press 'I accept and agree to be bound by the license terms' (sounds serious). You will then be shown another info screen telling you you can uninstall TrueCrypt. Press 'OK' then you will be asked for your password to install software on your computer. Enter your password and then you will finally see a screen like this:

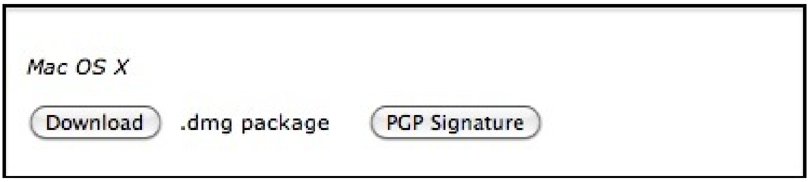


```
Installing package...
usr/bin/truecrypt
usr/bin/truecrypt-uninstall.sh
usr/share/applications/truecrypt.desktop
usr/share/pixmaps/truecrypt.xpm
usr/share/truecrypt/doc/License.txt
usr/share/truecrypt/doc/TrueCrypt User Guide.pdf

Press Enter to exit...
```

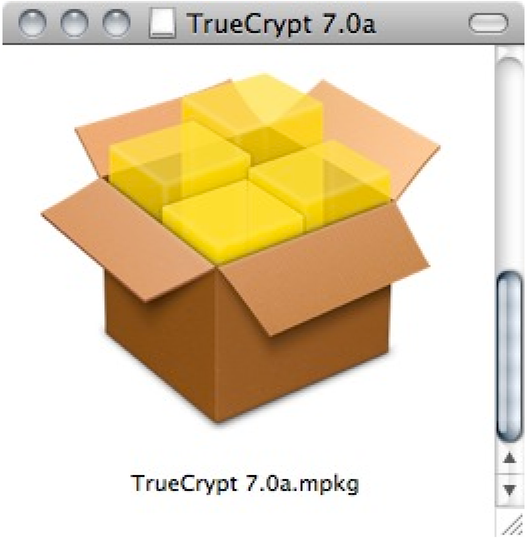
Believe it or now your are done...TrueCrypt is installed and you can access it from the Applications->accessories menu...close the setup window. Now proceed to the chapter on Using TrueCrypt.

Installing on OSX

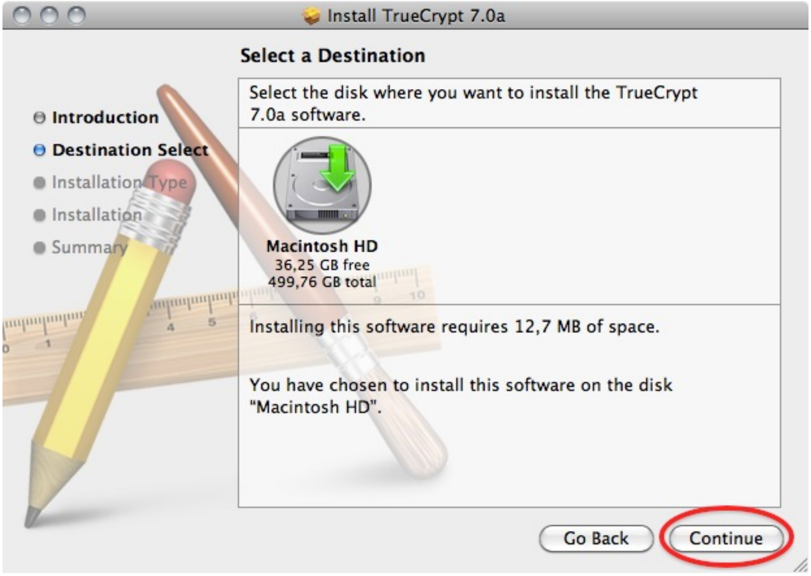
1. To install TrueCrypt on OSX first visit the download page (http://www.truecrypt.org/downloads) and press the download button under the *OSX* section.



2. Download this to your computer find the .dmg file and open it to access the installation package.



3. Open the installation package, and click away through the dialogues.



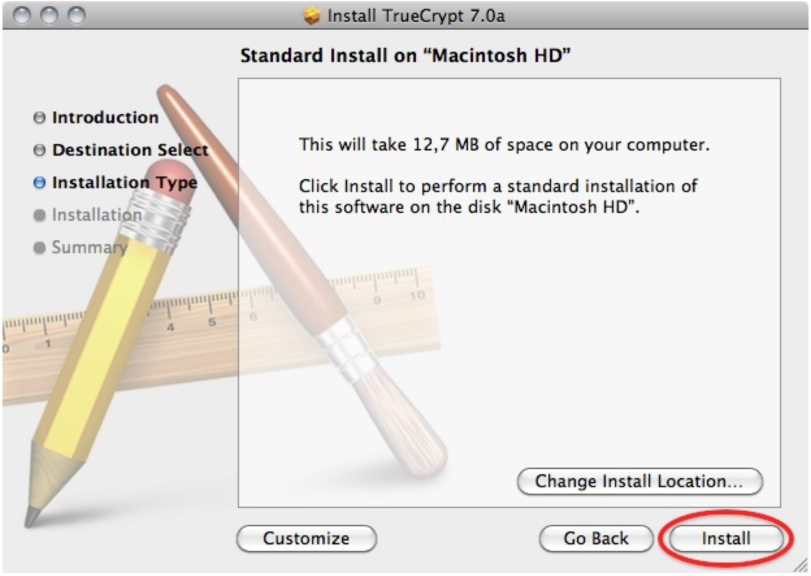
Select a Destination

Select the disk where you want to install the TrueCrypt 7.0a software.

Installing this software requires 12,7 MB of space.

You have chosen to install this software on the disk "Macintosh HD".

4. Choose the standard installation. (you can choose to do a customized installation and deselect FUSE, but why would you? You need it!)

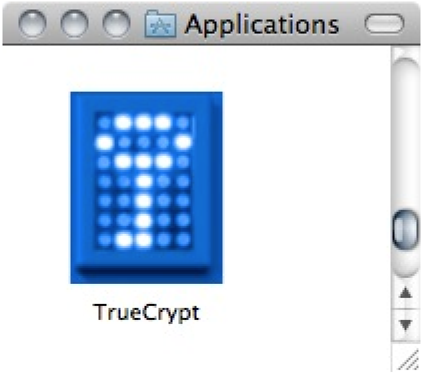


Standard Install on “Macintosh HD”

This will take 12,7 MB of space on your computer.

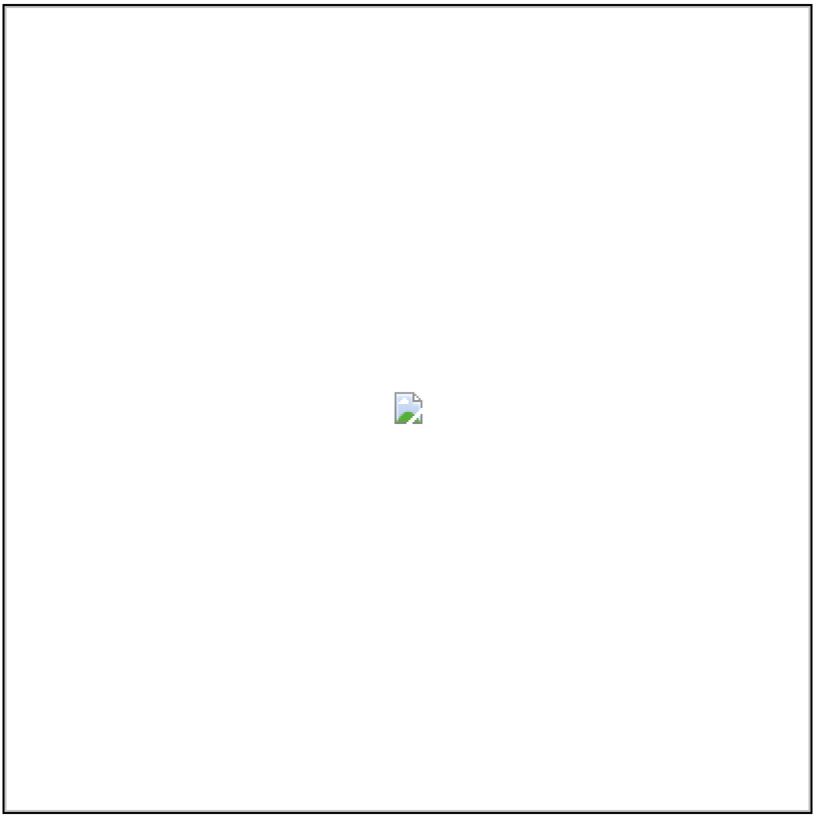
Click Install to perform a standard installation of this software on the disk “Macintosh HD”.

6. After the installation finishes you can find the program in your Applications folder



Installing on Windows

To install TrueCrypt on Windows first visit the download page (http://www.truecrypt.org/downloads) and press the download button under the *Windows* section.



Download this to your computer and then double click on the file. You will see a license agreement.

Click on 'I accept and agree to be bound by the license terms' and then click 'Accept'.

Leave the above screen with the defaults and press 'Next >' and you will be taken to the Setup Options window:

You can leave this with the defaults. If you want to set up TrueCrypt just for yourself then consider not selecting the 'Install for all users'. However if you are installing this on your own machine and no one else uses the computer then this is not necessary. You may also wish to consider installing TrueCrypt in a folder other than the default. In which case click 'Browse' and choose another location. When you are done click 'Install' and the process will proceed:

When the installation is complete you will get a verification popup that it was successful. Close this window and click 'Finish' and all is done. Now proceed to the chapter on Using TrueCrypt.

USING TRUECRYPT

The following are step-by-step instructions on how to create, mount, and use a TrueCrypt volume.

CREATING A TRUECRYPT CONTAINER

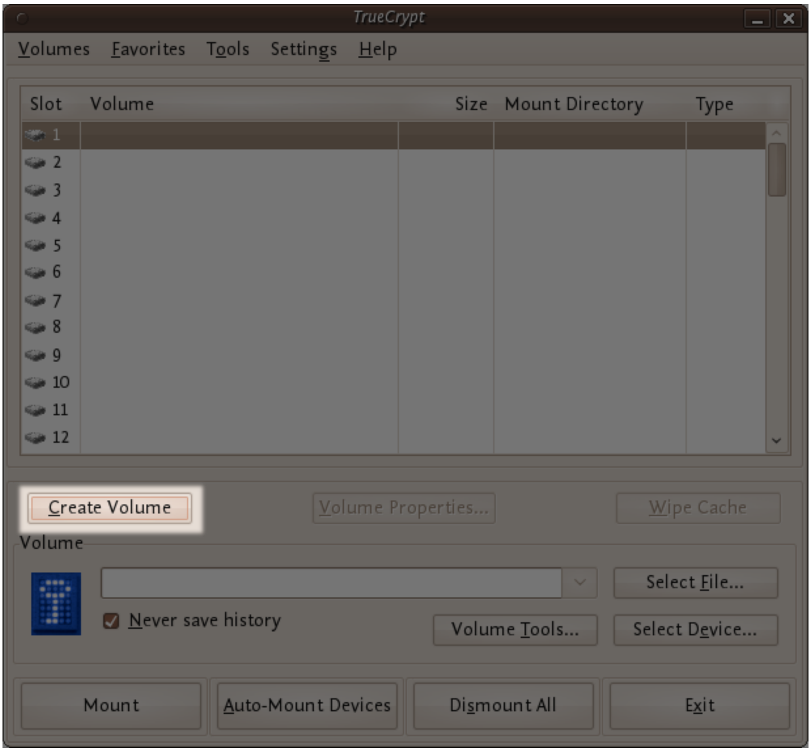
Step 1:

Install TrueCrypt. Then launch TrueCrypt by

- double-clicking the file TrueCrypt.exe in **Windows**
- opening Applications->Accessories->TrueCrypt in **Ubuntu**
- on **MacOSX** open it by clicking Go > Applications. Find TrueCrypt in the Applications folder and double click on it.

Step 2:

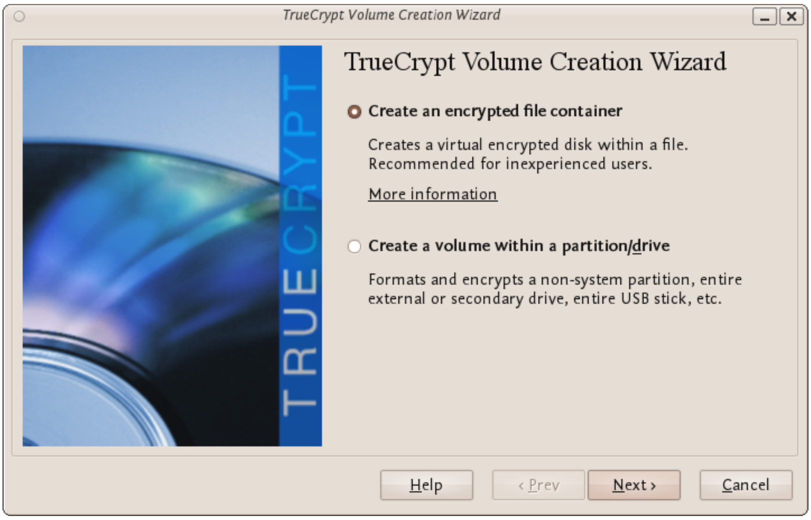
When the main TrueCrypt window appears. Click Create Volume.



☑ Never save history

Step 3:

You should see the TrueCrypt Volume Creation Wizard window appear on screen.



TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file.
Recommended for inexperienced users.

More information

○ Create a volume within a partition/drive

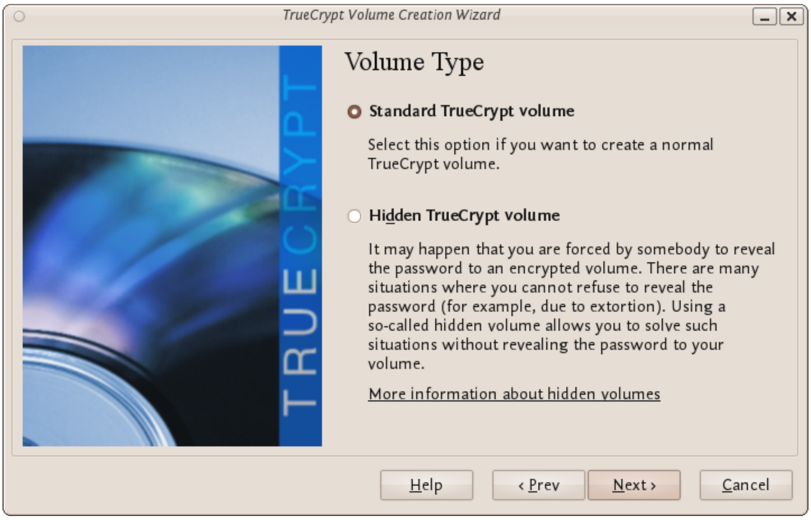
Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.

Where do you want to create the TrueCrypt volume? You need to choose now. This can be in a file, which is also called a container, in a partition or drive. The following steps will take you through the first option creating a TrueCrypt volume within a file.

You can just click Next, as the option is selected by default,

Step 4:

Next you need to choose whether to create a standard or hidden TrueCrypt volume. We will walk you through the former option and create a standard TrueCrypt volume.



TrueCrypt Volume Creation Wizard

Volume Type

● Standard TrueCrypt volume

Select this option if you want to create a normal TrueCrypt volume.

○ Hidden TrueCrypt volume

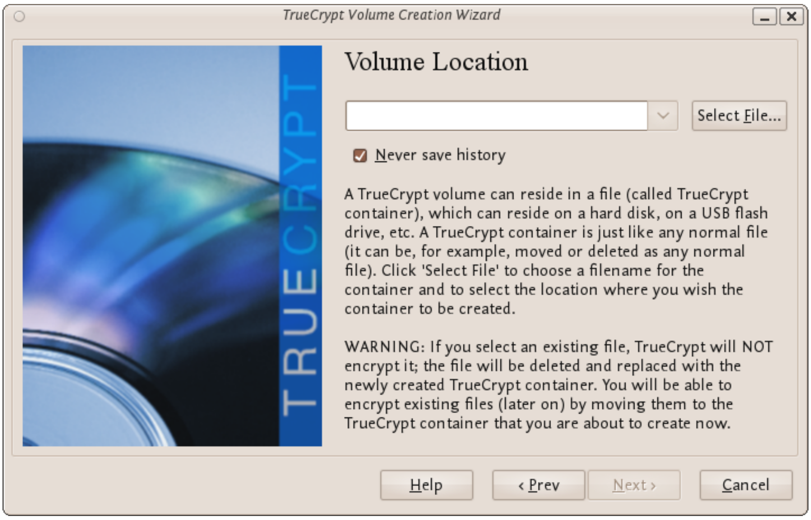
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

You can just click Next, as the option is selected by default.

Step 5:

Now you have to specify where to have the TrueCrypt volume (file container) created. Note that a TrueCrypt container behaves like any normal file. It can be moved or deleted as any normal file.



Volume Location

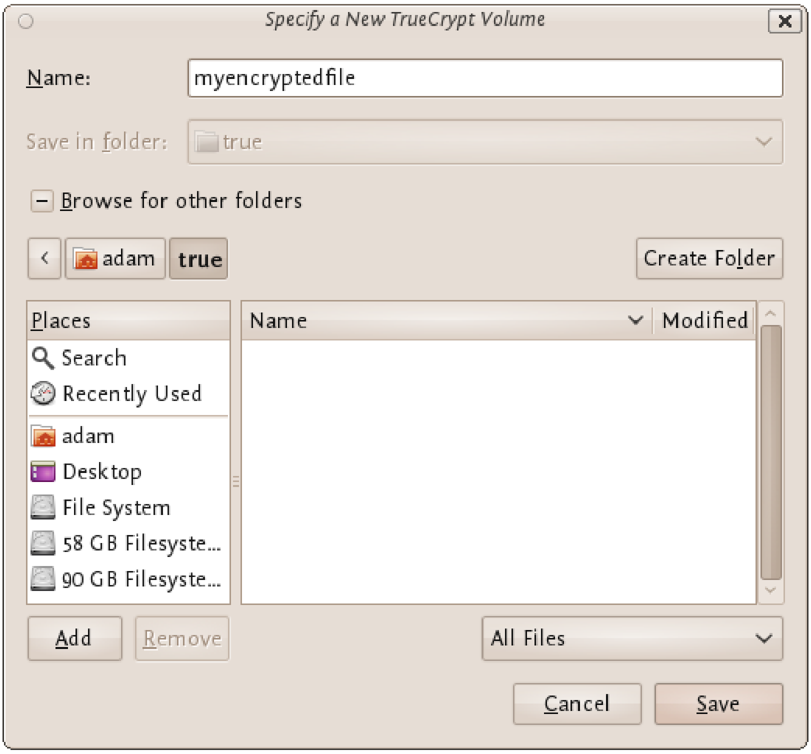
☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Click Select File.

The standard file selector will now appear on screen (the TrueCrypt Volume Creation Wizard remains open in the background). You need to browse to the folder that the file should be created in and then type into the 'name' field the name for the file you wish to create.



Name: myencryptedfile

Save in folder: true

We will create our TrueCrypt volume in the folder 'adam/true' and the filename of the volume (container) will be 'myencryptedfile'. You may, of course, choose any other filename and location you like (for example, on a USB stick). Note that the file 'myencryptedfile' does not exist yet - TrueCrypt will create it. Press 'Save' when you are ready. The file selector window should close.

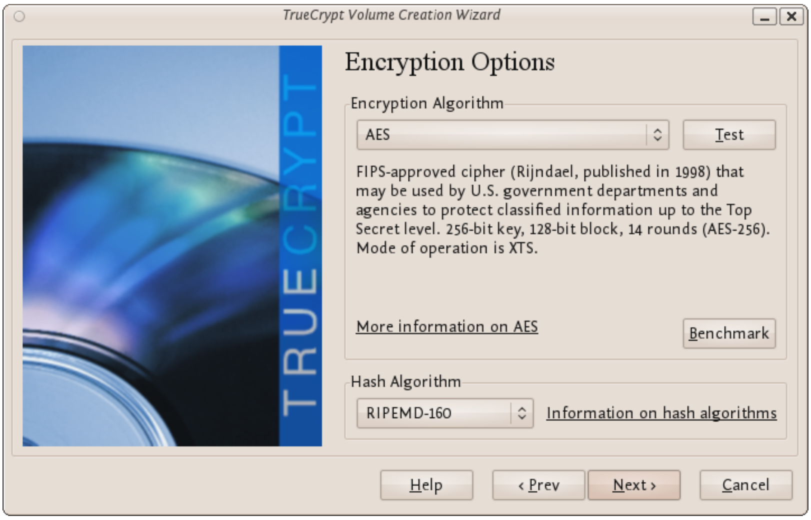
IMPORTANT: Note that TrueCrypt will not encrypt any existing files. If an existing file is selected in this step, it will be overwritten and replaced by the newly created volume (the contents of the existing file will be lost). You will be able to encrypt existing files later on by moving them to the TrueCrypt volume that we are creating now.

Step 6:

In the Volume Creation Wizard window (which was previously running in the background), click Next.

Step 7:

Here you can choose an encryption algorithm and a hash algorithm for the volume.



Encryption Options

Encryption Algorithm: AES

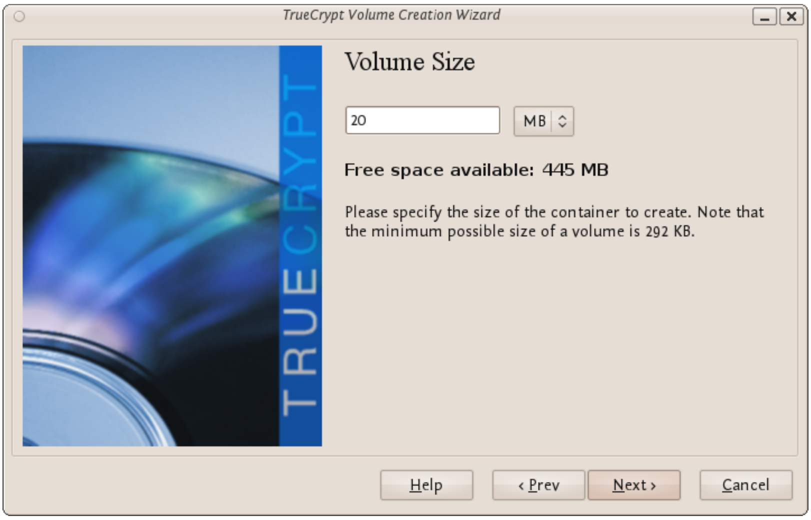
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: RIPEMD-160

The TrueCrypt manual suggests that if you are not sure what to select here, you can use the default settings and click Next (for more information about each setting have a look at the TrueCrypt documentation website).

Step 8:

Now choose the size of your container. You should be fine with 1 megabyte but for this example we will enter '20' into the available field.



Volume Size

20 MB

Free space available: 445 MB

Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.

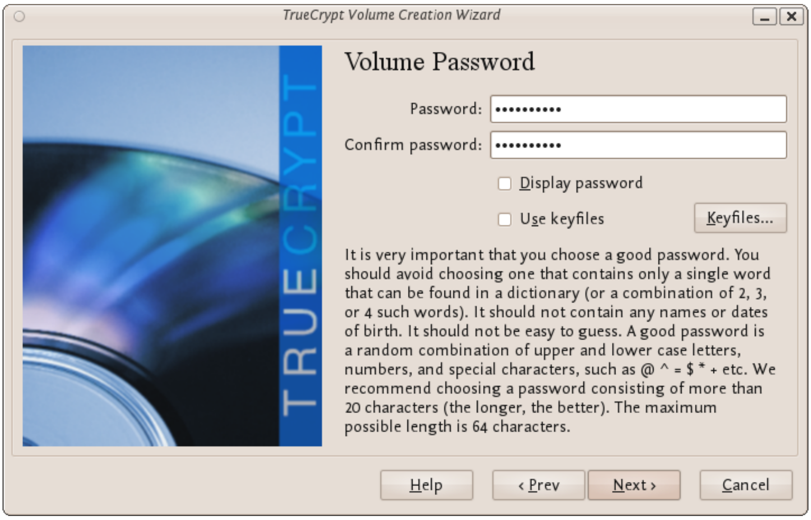
You may, of course, specify a different size. After you type the desired size in the input field, click Next.

Step 9:

This step is really important, choosing a password.

The information displayed in the Wizard window about what is considered a good password, should be read carefully.

Choose a strong password, type it in the first input field. Then re-type it in the input field below the first one.



Volume Password

Password: ••••••••••

Confirm password: ••••••••••

□ Display password

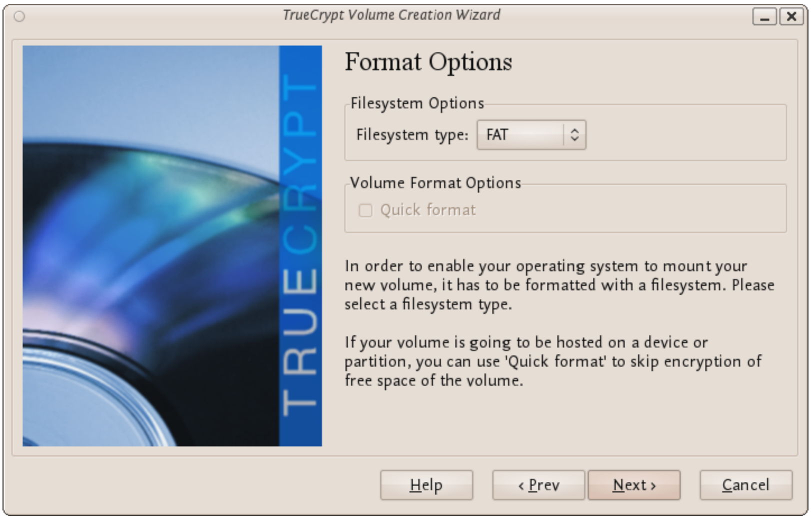
□ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

When you are done click Next.

Step 10:

Now you must choose the format of your partition (this step may not be available for you under windows or OSX). If using Ubuntu you can choose a Linux file type or FAT (Windows) for simplicity leave it at the default.



Format Options

Filesystem Options

Filesystem type: FAT

Volume Format Options

□ Quick format

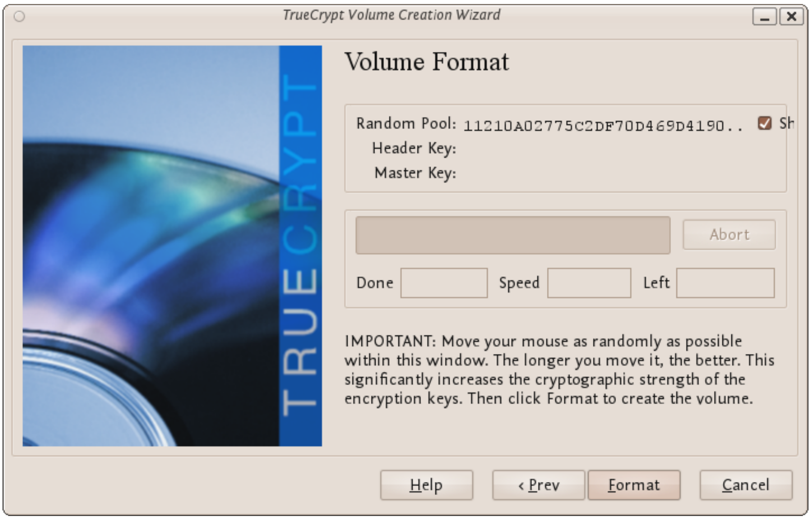
In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.

If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.

Then press Next.

Step 11:

Next TrueCrypt tries to generate random information to help encrypt your container. For 30 seconds move your mouse as randomly as possible within the Volume Creation Wizard window. Move the mouse as much as possible for up to a minute. This significantly increases security by increasing the cryptographic strength of the encryption keys. security). Move your mouse around until you are bored.



TrueCrypt Volume Creation Wizard

Volume Format

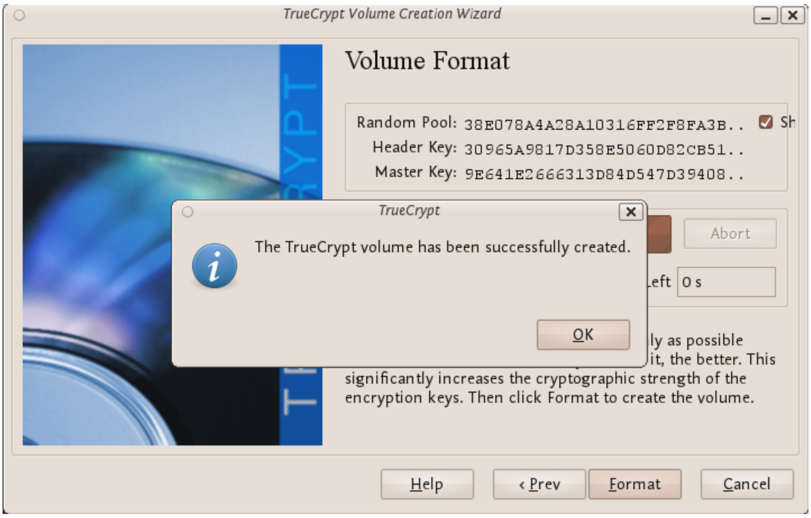
Random Pool: 11210A02775C2DF70D469D4190.. ☑ Sh
Header Key:
Master Key:

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Then Click Format.

TrueCrypt will now create a file in the folder you selected with the name you chose. This file will be a TrueCrypt container, containing the encrypted TrueCrypt volume. This may take some time depending on the size of the volume. When it finishes this should appear:



TrueCrypt Volume Creation Wizard

Volume Format

Random Pool: 38E078A4A28A10316FF2F8FA3B.. ☑ Sh
Header Key: 30965A9817D358E5060D82CB51..
Master Key: 9E641E2666313D84D547D39408..

TrueCrypt

The TrueCrypt volume has been successfully created.

ly as possible
it, the better. This
significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Click OK to close the dialog box.

Step 11:

Well done! You've just successfully created a TrueCrypt volume (file container).

In the TrueCrypt Volume Creation Wizard window, click Exit.

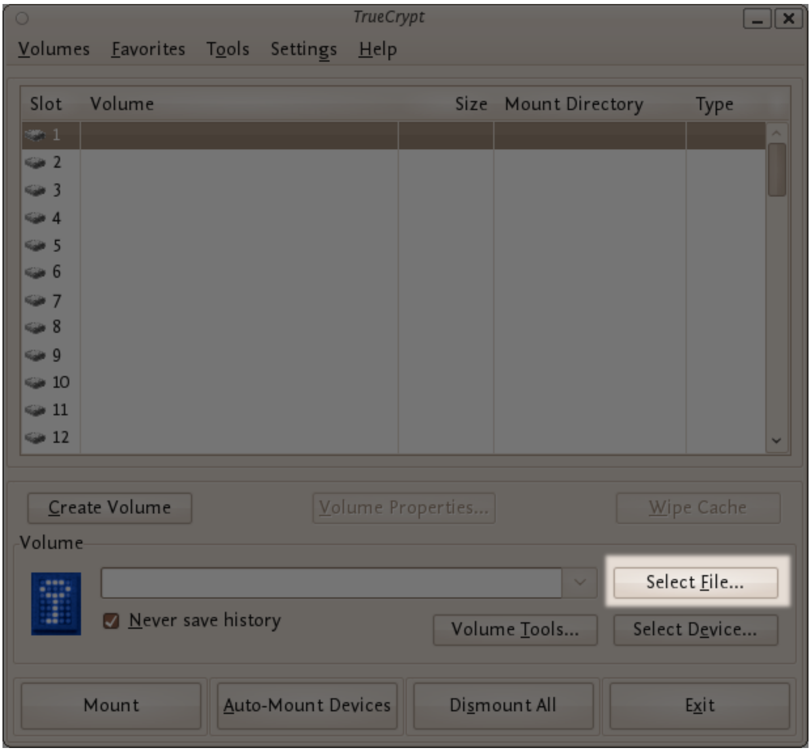
Mounting the Encrypted Volume

Step 1:

Open up TrueCrypt again.

Step 2:

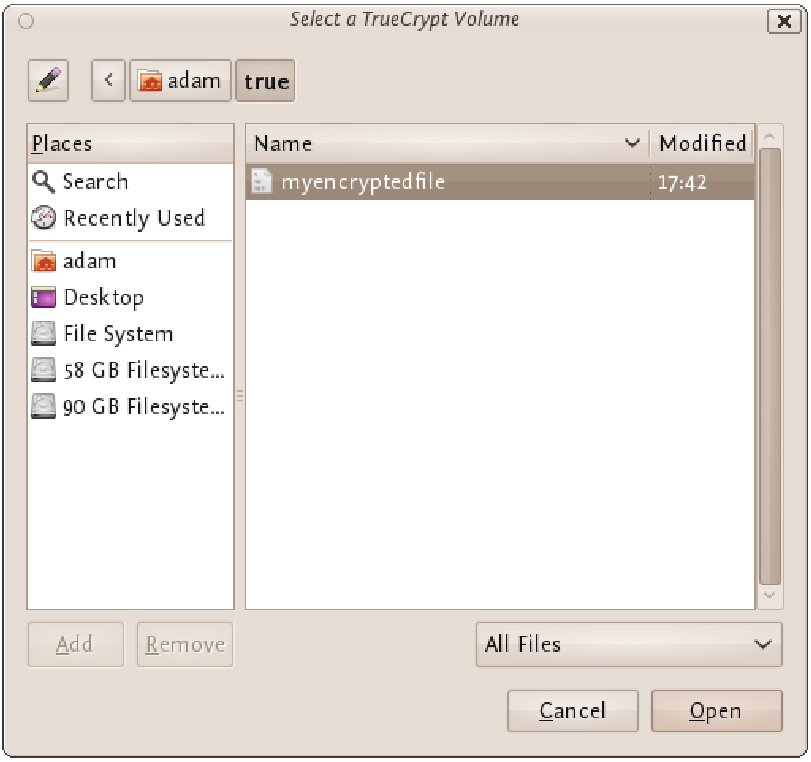
Make sure one of the 'Slots' is chosen (it doesn't matter which - you can leave at the default first item in the list). Click Select File.



The standard file selector window should appear.

Step 3:

In the file selector, browse to the container file (which we created earlier) and select it.

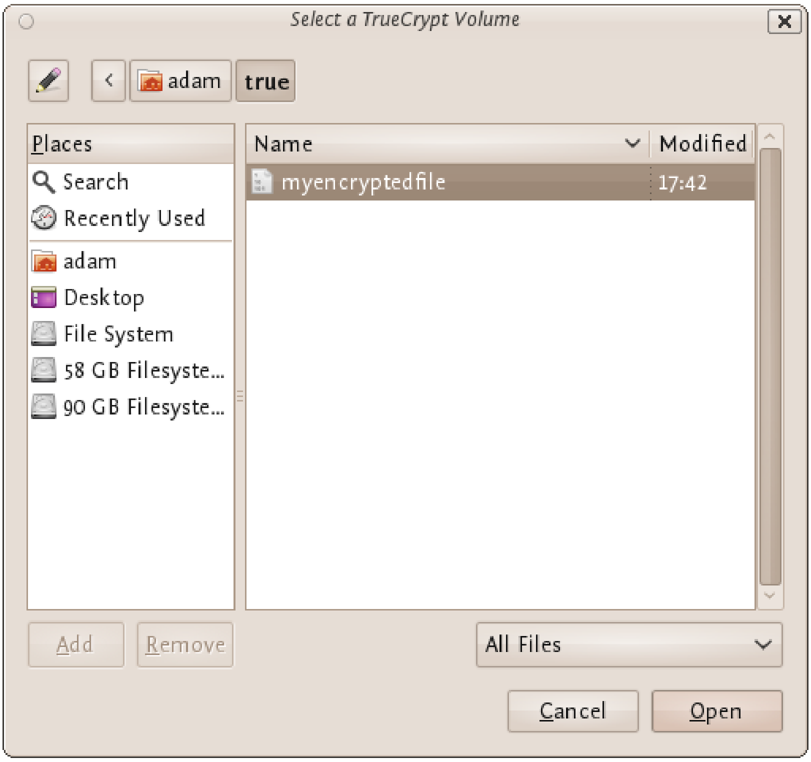


Click Open (in the file selector window).

The file selector window should disappear.

Step 4:

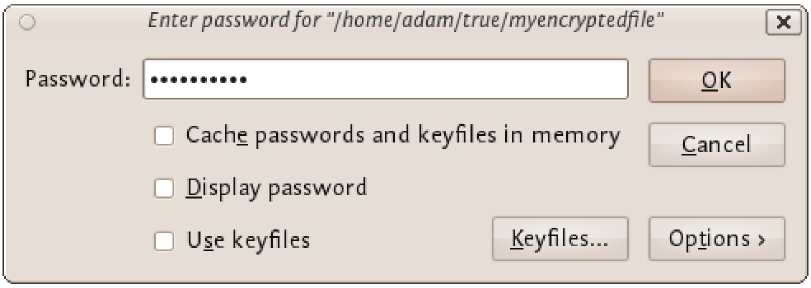
In the main TrueCrypt window, click Mount.



Password prompt dialog window should appear.

Step 5:

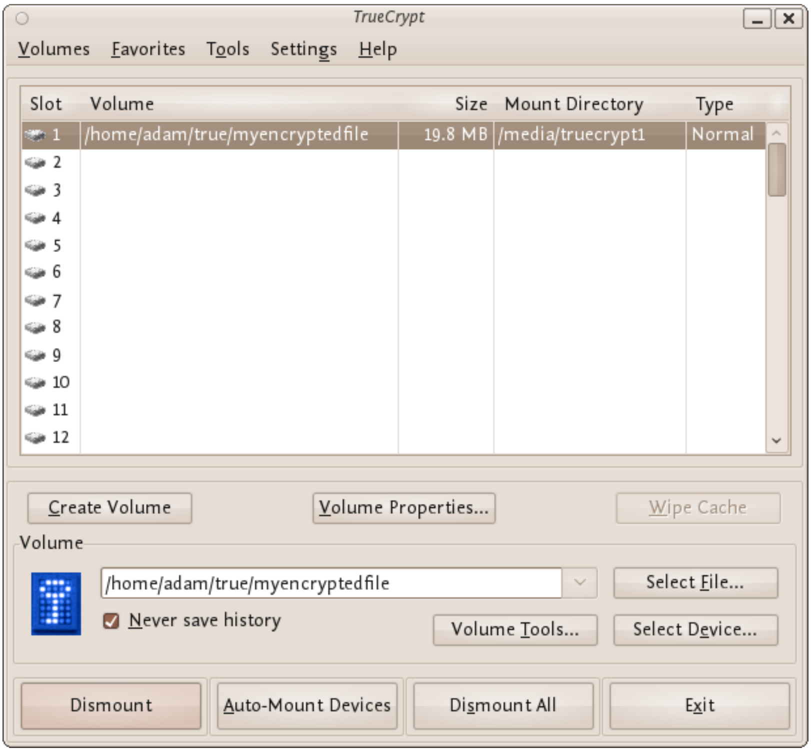
Type the password in the password input field.


Enter password for "/home/adam/true/myencryptedfile"
Password:
••••••••••
OK
□ Cache passwords and keyfiles in memory
Cancel
□ Display password
□ Use keyfiles
Keyfiles...
Options ›

Step 6:

Click OK in the password prompt window.

TrueCrypt will now attempt to mount the volume. If the password is correct, the volume will be mounted.



Slot	Volume	Size	Mount Directory	Type
1	/home/adam/true/myencryptedfile	19.8 MB	/media/truecrypt1	Normal
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

/home/adam/true/myencryptedfile

☑ Never save history

If the password is incorrect (for example, if you typed it incorrectly), TrueCrypt will notify you and you will need to repeat the previous step (type the password again and click OK).

Step 7:

We have just successfully mounted the container as a virtual disk 1. The container will appear on your Desktop or you will see it in your file browser.

What does this mean?

The disk that you have just created is completely encrypted and behaves like a real disk. Saving (moving, copying, etc) files to this disk will allow you to encrypt files on the fly.

You'll be able to open a file which is stored on a TrueCrypt volume, which will automatically be decrypted to RAM while it is being read, and you won't need to enter your password each time. You'll only need to enter this when your mounting the volume.

Remember to dismount!

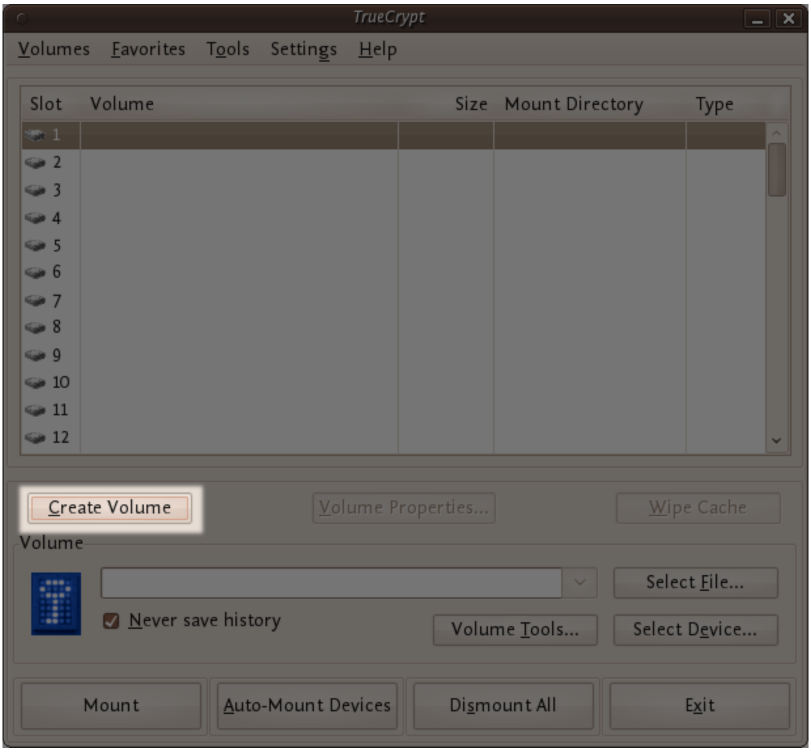
To do this right click on the drive and select unmount. This will automatically happen when you turn off your computer but will not happen if you just put the computer on sleep.

Setting up a hidden volume

A TrueCrypt hidden volume exists within the free space of a typical TrueCrypt volume. Given then the 'outer volume' is accessed it is (almost) impossible to determine if there is a hidden volume within it. This is because TrueCrypt *always* fills the empty space of an encrypted volume with random data. So a hidden volume looks the same as an empty TrueCrypt volume.

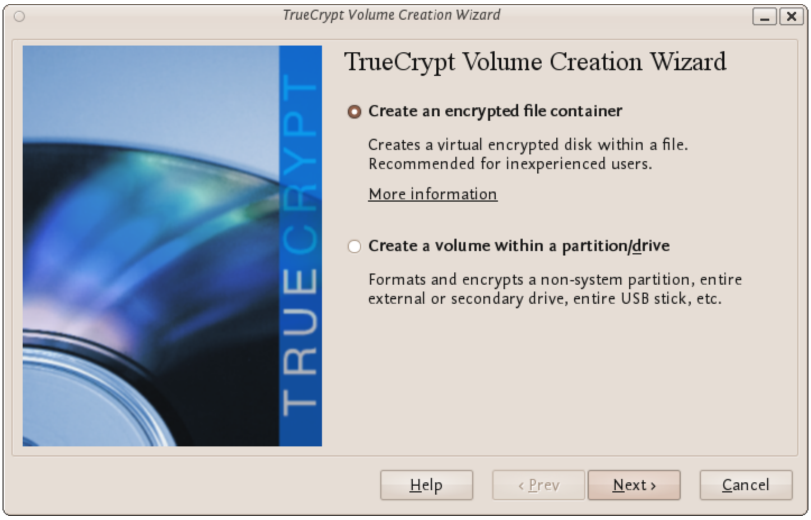
To create and use a hidden volume you need two passwords - one each for the outer and inner (hidden) volumes. When you mount (open) the volume you can use either password and that will determine which of the two is opened. If you want to open just the hidden volume you use one password, and if you want to access just the non-hidden encrypted volume you use the other password.

To create a hidden volume open TrueCrypt and press the 'Create Volume' button:



☑ Never save history

The options for half of this process are *almost* the same as for setting up a standard TrueCrypt volume and then the process continues for setting up the hidden volume but lets go through the entire process step by step anyway. In the screen shown below you just want to stay with the default setting 'Create an encrypted file container':



TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

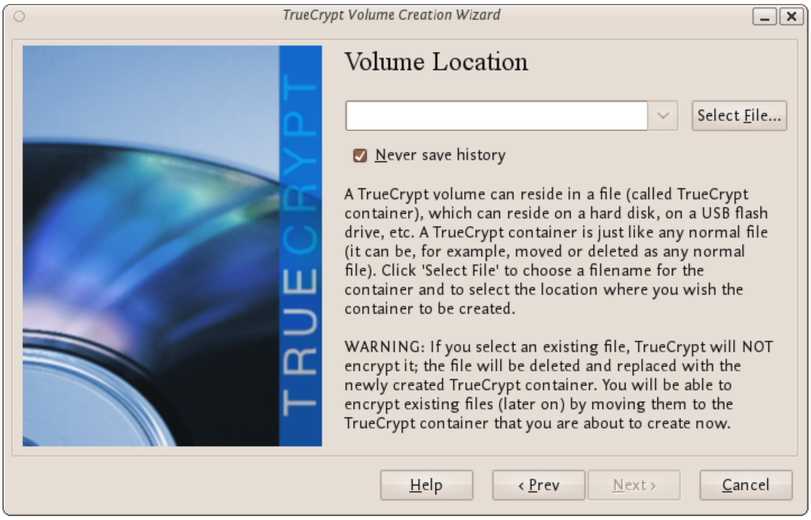
More information

○ Create a volume within a partition/drive

Formats and encrypts a non-system partition, entire external or secondary drive, entire USB stick, etc.

Press 'Next >' and continue to the next screen.

In the above screen you want to be sure that you choose the second option 'Hidden TrueCrypt Volume'. Select this and click on 'Next >' you will then be asked to choose the location and name of the TrueCrypt *outer* volume.



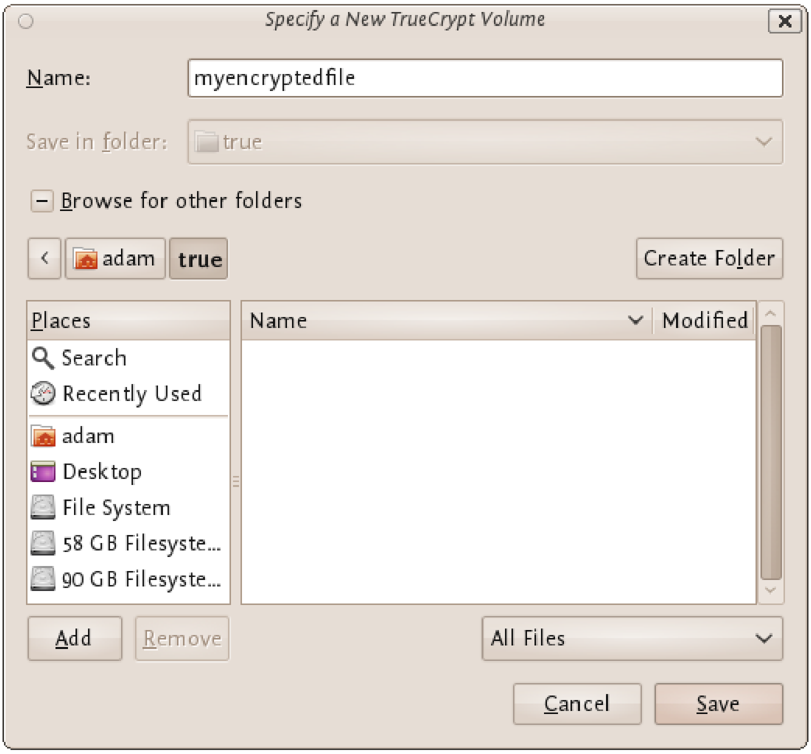
Volume Location

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Click 'Select File...' and browse to a location for a new TrueCrypt volume. We will use the name 'myencryptedfile' in this example. Its the same name as we used in the last example so be aware that if you have just followed those instructions you must now create a new volume with a new name.

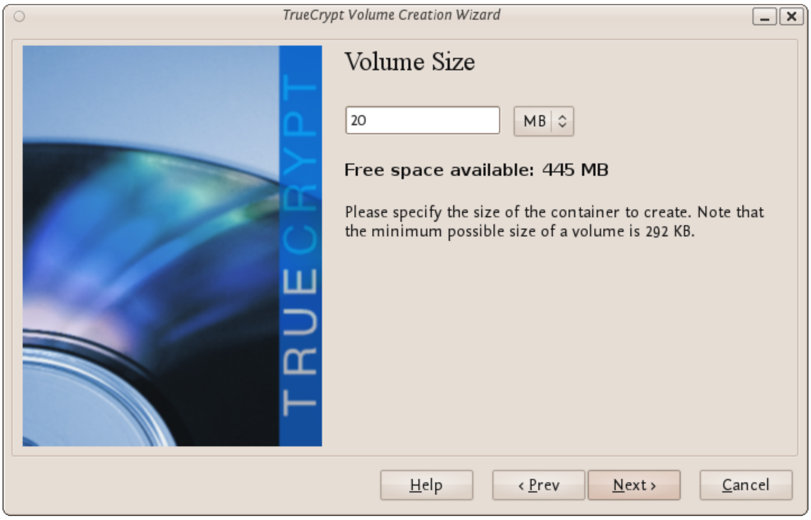


Name: myencryptedfile

Save in folder: true

Browse to the directory where you want to put the outer volume and enter the name of the volume in the field named 'Name' as in the example above. When you are satisfied all is well click on 'Save'. The file browser will close and you return to the Wizard. Click 'Next >'. Here you are presented with some very technical choices. Don't worry about them. Leave them at the defaults and click 'Next >'. The next screen asks you to determine the size of the outer volume. Note that when you do this the maximum inner 'hidden' volume size is determined by TrueCrypt. This maximum size will of course be smaller that the size you are setting on this screen. If you are not sure what the ratio of outer volume size to inner (hidden) volume size is then go through the process now as a 'dummy' run - you can always trash the encrypted volume and start again (no harm done).

So choose the size of the outer volume, I will choose 20MB as shown below:



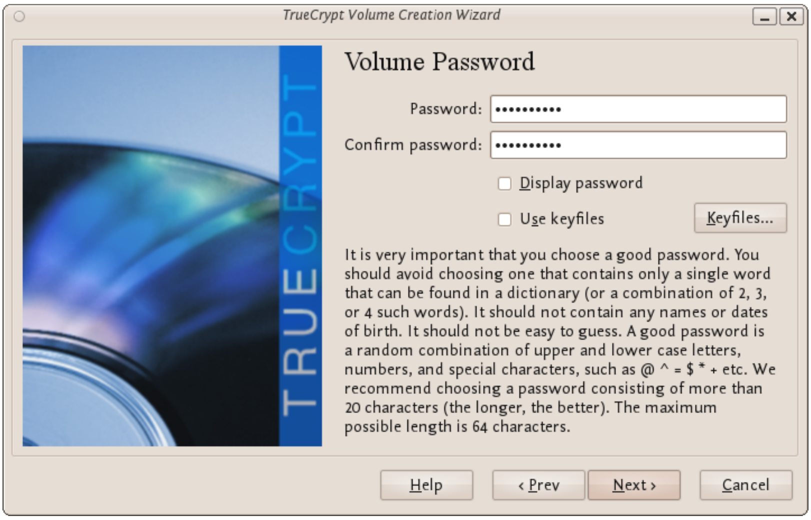
Volume Size

20 MB

Free space available: 445 MB

Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.

You cannot set the outer volume size to be larger than the amount of free space you have available on your disk. TrueCrypt tells you the maximum possible size in bold letters so create a volume size smaller than that. Then click 'Next >' and you will be taken to a screen asking you to set a password for the *outer* (not the hidden, this comes later) volume.



Volume Password

Password: ••••••••••

Confirm password: ••••••••••

□ Display password

□ Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Enter a password that is strong (see the chapter on creating good passwords) and press 'Next >'. Next TrueCrypt wants you to help it create the random data it will fill the volume up with. So wave your mouse around, browse the web, and do whatever you want for as long as you can. When you feel TrueCrypt should be happy then press 'Format'. You will see a progress bar zip by and then you will be presented with the next screen:

You can open the outer volume if you like but for this chapter we will skip that and go ahead to create the hidden volume. Press 'Next >' and TrueCrypt will work out how the maximum possible size of the hidden volume.

When you see the above screen just press 'Next >'. Now you must choose the encryption type for the hidden volume. Leave it at the defaults and press 'Next >'.

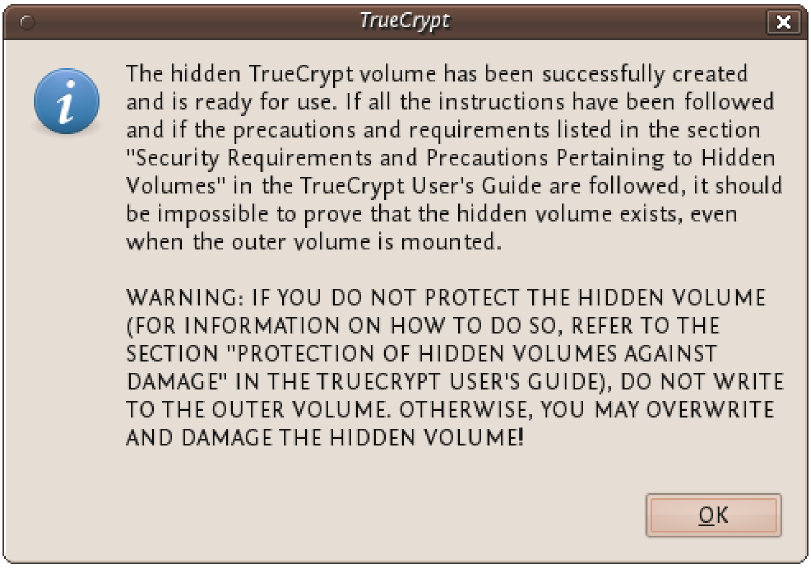
Now you will be asked to choose the size of the hidden volume.

I have set (as you see above) the maximum size as 10MB. When you have set your maximum size press 'Next >' and you will be promoted to create a password for the hidden volume.

When creating the password for the hidden volume make sure you make it substantially different fro the password for the outer volume. If someone really does access your drive and finds out the password for the outer volume they might try variations on this password to see if there is also a hidden volume. So make sure the two passwords are not alike.

Enter your password in the two fields and press 'Next >'.

Leave this window at the defaults and press 'Next >' and you will be presented with the same screen you have seen before to generate random data for TrueCrypt. When you are happy click 'Format' and you should see the following :



The hidden TrueCrypt volume has been successfully created and is ready for use. If all the instructions have been followed and if the precautions and requirements listed in the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the TrueCrypt User's Guide are followed, it should be impossible to prove that the hidden volume exists, even when the outer volume is mounted.

WARNING: IF YOU DO NOT PROTECT THE HIDDEN VOLUME (FOR INFORMATION ON HOW TO DO SO, REFER TO THE SECTION "PROTECTION OF HIDDEN VOLUMES AGAINST DAMAGE" IN THE TRUECRYPT USER'S GUIDE), DO NOT WRITE TO THE OUTER VOLUME. OTHERWISE, YOU MAY OVERWRITE AND DAMAGE THE HIDDEN VOLUME!

The TrueCrypt manual it is referring to is *not* this manual. They mean this manual : http://www.truecrypt.org/docs/

Click 'OK' and keep and exit TrueCrypt. You can now mount the volume as noted in the previous chapter.

SECURELY DESTROYING DATA

Just hit the delete button and you are done! No it's not that easy. To understand how to securely delete data, we have to understand how data is stored. In an analogy to the real world, an explanation of how data is stored follows:

Assume you have a small notebook with 10 pages and you want to write some data in this notebook. You just start writing on the first page up to the end of the notebook. Maybe you decide the information on page 5 must be destroyed. Probably you will just take out the page and burn it.

Unfortunately data on a harddisk doesn't work this way. A harddisk contains not ten but thousands or maybe even millions of pages. Also it's impossible to take out a "page" of a harddisk and destroy it. To explain how a harddisk work, we will continue with our 10-page notebook example. But now we will work a little bit different with it. We will work in a way similar to how a harddisk works.

This time we use the first page of our notebook as an index. Assume we write a piece about "WikiLeaks", then on the first page we write a line "piece about WikiLeaks: see page 2". The actual piece is then written on page 2.

For the next document, a piece about "Goldman Sachs" we add a line on page 1, "Goldman Sachs: see page 3". We can continue this way till our notebook is full. Let's assume the first page will look like this:

- WikiLeaks -> see page 2
- Goldman Sachs -> see page 3
- Monstanto scandal -> see page 4
- Holiday pictures -> see page 5
- KGB Investigation -> see page 6
- Al Jazeeraa contacts -> see page 7
- Iran nuclear program -> see page 8
- Sudan investigation -> see page 9
- Infiltration in EU-politics -> see page 10

Now, let's decide you want to wipe the "Goldman Sachs" piece, what a harddisk will do, it will only remove the entry on the first page, but not the actual data, your index will be:

- WikiLeaks -> see page 2
- Monstanto scandal -> see page 4
- Holiday pictures -> see page 5
- KGB Investigation -> see page 6
- Al Jazeeraa contacts -> see page 7
- Iran nuclear program -> see page 8
- Sudan investigation -> see page 9
- Infiltration in EU-politics -> see page 10

What we did, we removed only the reference to the article, but if we open page 3, we will still able to read the Goldman Sachs piece. This is exactly the way what a harddisk does when your "delete" a file. With specialized software it still able to "recover" page 3.

To securely delete data, we should do the following:

1. Open the "Goldman Sachs" page (page 3)
2. Use an eraser to remove the article there, if done return to page 1
3. Delete the reference in the index on page 1

Well you will be surprised by the similarity between this example and the real world. You know when you removed the article on page 3 with an eraser, it is still possible to read the article slightly. The pencil leaves a track on the paper because of the pressure of the pencil on the paper and also you will be unable to erase all of the graphite. Small traces are left behind on the paper. If you really need this article, you can reconstruct (parts) of it, even if it's erased.

With a harddisk this is very similar. Even if you erased every piece of data, it is sometimes possible with (very) specialized hardware to recover pieces of the data. If the data is very confidential and must be erased with the greatest care, you can use software to "overwrite" all pieces of data with random data. When this is done multiple times, this will make the data untraceable.

An important note on Solid State Hard Drives

The instructions below explain how to use file deletion tools to securely delete files from your hard drives. These tools rely on the Operating System you are using being able to directly address every byte on the hard drive in order to tell the drive "set byte number X to 0". Unfortunately, due to a number of advanced technologies used by *Solid State Drives* (SSDs) such as *TRIM*, it is not always possible to ensure with 100% certainty that every part of a file on an SSD has been erased using the tools below.

An important note on Journaled File Systems

Data Journaling is a feature of several modern file systems and presents a risk to secure data deletion. File-systems of this type include *Ext3* and *Ext4* (Linux), compressed file systems and *RAID*-based file systems.

The manual page for the deletion program *Wipe* says:

No secure deletion program that does filesystem-level calls can sanitize files on such filesystems, because sensitive data and metadata can be written to the journal, which cannot be readily accessed. Per-file secure deletion is better implemented in the operating system.

The manual page for the deletion program *Shred* says:

CAUTION: Note that shred relies on a very important assumption: that the file system overwrites data in place. This is the traditional way to do things, but many modern file system designs do not satisfy this assumption.

The following are examples of file systems on which shred is not effective, or is not guaranteed to be effective in all file system modes:

- log-structured or journaled file systems, such as those supplied with AIX and Solaris (and JFS, ReiserFS, XFS, Ext3, etc.)
- file systems that write redundant data and carry on even if some writes fail, such as RAID-based file systems * file systems that make snapshots, such as Network Appliance's NFS server
- file systems that cache in temporary locations, such as NFS version 3

clients

- compressed file systems In the case of ext3 file systems, the above disclaimer applies (and shred is thus of limited effectiveness) only in data=journal mode, which journals file data in addition to just metadata. In both the data=ordered (default) and data=writeback modes, shred works as usual. Ext3 journaling modes can be changed by adding the data=something option to the mount options for a particular file system in the /etc/fstab file, as documented in the mount man page (man mount).

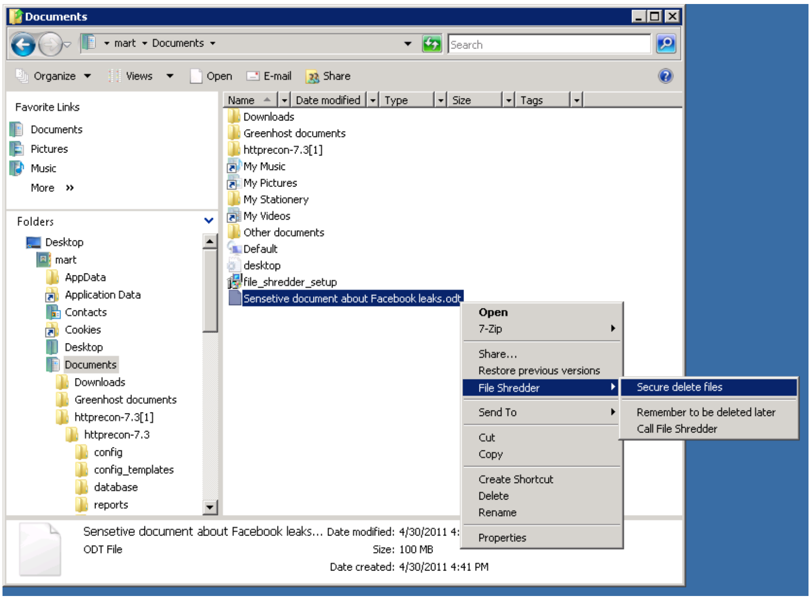
If you wish to delete data from a journaled file-system on Linux (mounted in *data=journal* mode) you should remount it in another mode. To be sure, remount your disk in Linux in *data=ordered* mode. See the manual page for the program *mount* on your system. Solaris users or those with RAID systems are outside of the scope of this manual. Please see the relevant documentation and/or research your special case in order to be sure you are securely deleting your data.

Securely delete data under Windows

For Windows there is a good open source tool called "File Shredder". This tool can be downloaded from http://www.fileshredder.org

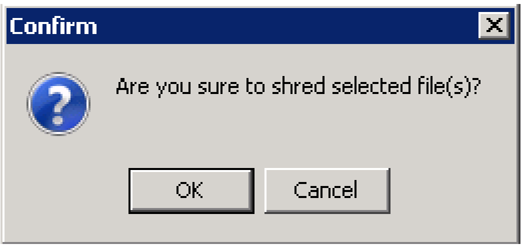
The installation is very straightforward, just download the application and install it by hitting the next button. After installation this application will automatically start. You can then start using it for shredding files. However the best part of the program is that you can use it from within windows itself by right clicking on a file.

1. Click right on the file you want to shred, and choose File Shredder -> Secure delete files



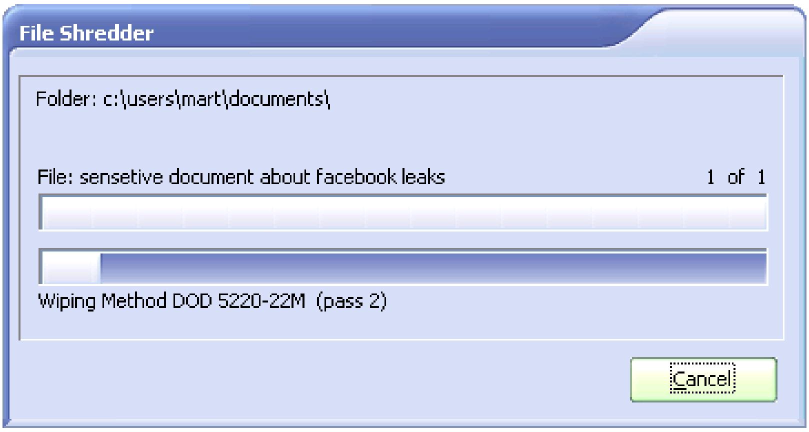
Sensetive document about Facebook leaks... Date modified: 4/30/2011 4:
ODT File Size: 100 MB
Date created: 4/30/2011 4:41 PM

2. A pop-up asks if you really want to shred this file



Are you sure to shred selected file(s)?

3. After confirming, there your file goes. Depending on the size of the file this can take a while



Folder: c:\users\mart\documents\

File: sensetive document about facebook leaks 1 of 1

Wiping Method DOD 5220-22M (pass 2)

Securely delete data under MacOSX

There are basically to build-in steps to make to securely delete your data on Mac OSX.

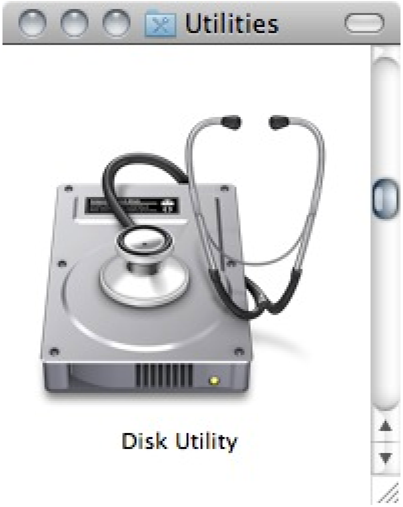
1. Erase the free-space on your hard-drive containing all the data of items which are deleted in an insecure way.

2. Make sure that every file from then on is always securely deleted.

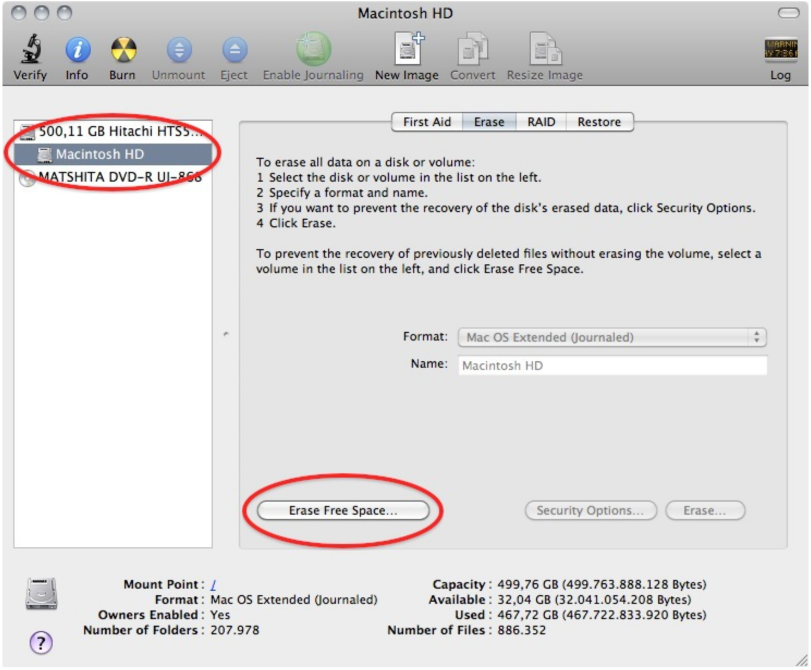
We start with the first one:

Erasing Free Space

1. Open Disk-Utility which resides in the Utilities folder inside the Applications folder.



2. Select your hard drive and click on 'Erase Free Space'.



To erase all data on a disk or volume:
1 Select the disk or volume in the list on the left.
2 Specify a format and name.
3 If you want to prevent the recovery of the disk's erased data, click Security Options.
4 Click Erase.

To prevent the recovery of previously deleted files without erasing the volume, select a volume in the list on the left, and click Erase Free Space.

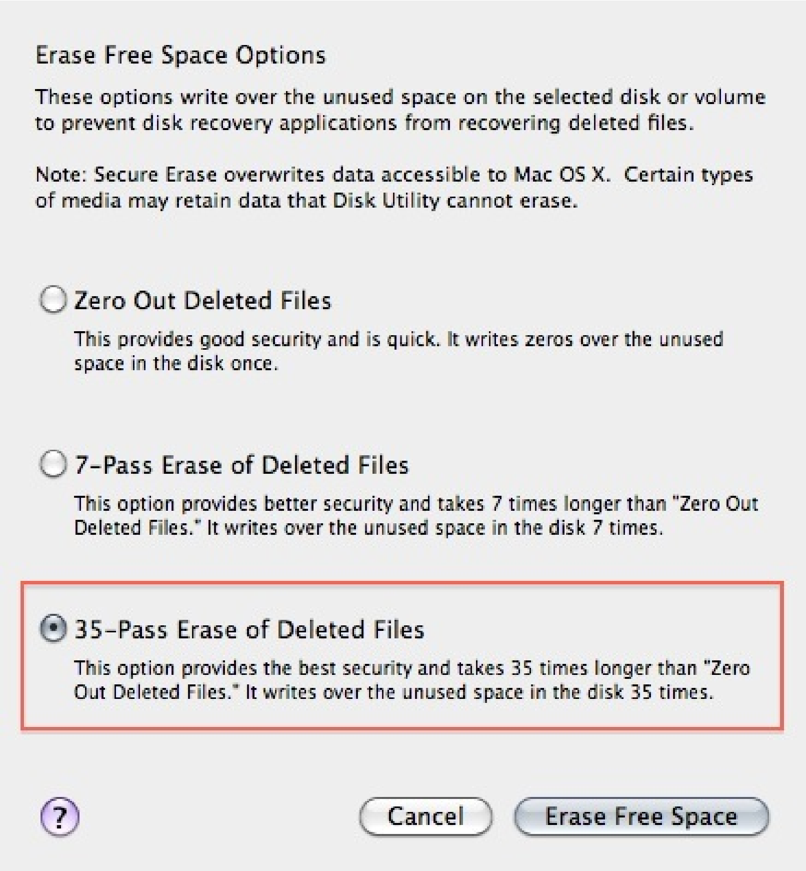
Format: Mac OS Extended (Journaled)
Name: Macintosh HD

Mount Point : /
Format : Mac OS Extended (Journaled)
Owners Enabled : Yes
Number of Folders : 207.978

Capacity : 499,76 GB (499.763.888.128 Bytes)
Available : 32,04 GB (32.041.054.208 Bytes)
Used : 467,72 GB (467.722.833.920 Bytes)
Number of Files : 886.352

3. Three options will appear, from top to bottom more secure, but also they take much more time to complete. Read the descriptions on each one of them to get an idea from what will happen if you use them and then choose which one might suite your needs the best and click 'Erase free Space'.

If time is no issue, then use the most secure method and enjoy your free time to get a good coffee while you Mac crunches away on this task. If the crooks are already knocking on your front-door you might want to use the fastest way.



Erase Free Space Options

These options write over the unused space on the selected disk or volume to prevent disk recovery applications from recovering deleted files.

Note: Secure Erase overwrites data accessible to Mac OS X. Certain types of media may retain data that Disk Utility cannot erase.

○ Zero Out Deleted Files

This provides good security and is quick. It writes zeros over the unused space in the disk once.

○ 7-Pass Erase of Deleted Files

This option provides better security and takes 7 times longer than "Zero Out Deleted Files." It writes over the unused space in the disk 7 times.

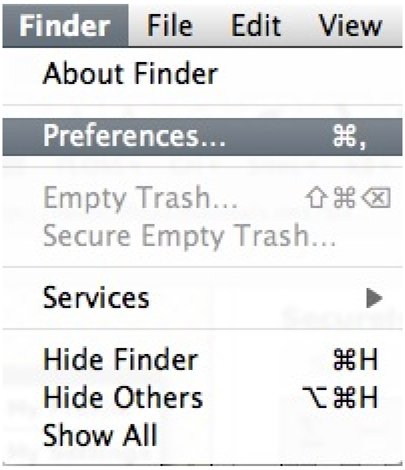
● 35-Pass Erase of Deleted Files

This option provides the best security and takes 35 times longer than "Zero Out Deleted Files." It writes over the unused space in the disk 35 times.

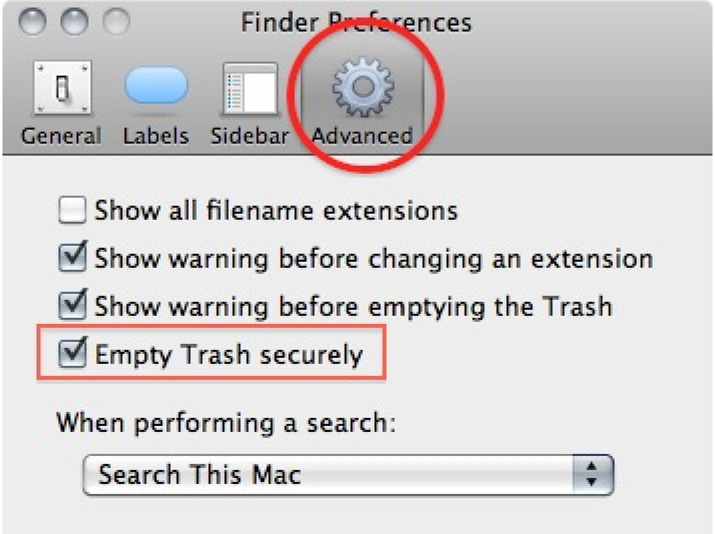
Securely Erasing Files

Now that your previously deleted data is once and for ever securely erased you should make sure that you don't create any new data that might be recovered at a later date.

1. To do this open the finder preferences under the Finder Menu.



2. Go to the advanced tab and tick 'Empty trash securely'. This will make sure that *every time* you empty your trash all the items in it will be securely deleted and are *really gone!*



□ Show all filename extensions
☑ Show warning before changing an extension
☑ Show warning before emptying the Trash
☑ Empty Trash securely

When performing a search:
Search This Mac

Note 1: Deleting your files securely will take longer then just deleting them. If you have to erase big portions of unimportant data (say your movie and mp3 collection) you may wanna untick this option before doing so.

Securely delete data under Ubuntu/Linux

Before we start, please see *An important note on Journaled File Systems*, above.

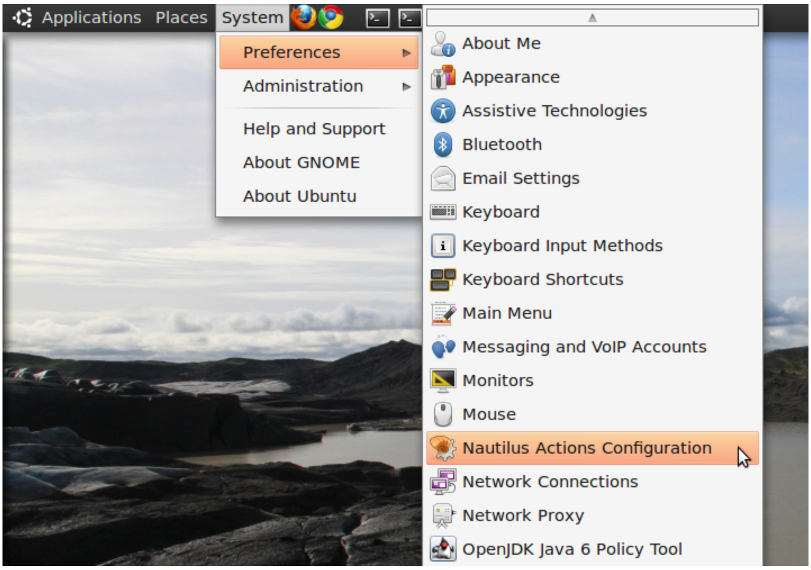
Unfortunately currently there is no graphical user interface available for Ubuntu to delete files secure. There are two command-line programs available though.

- *shred*
- *wipe*

Shred is installed in Ubuntu by default and can delete single files. Wipe is not installed by default but can easily be installed with using Ubuntu Software Center or if you understand the command line you can install it with *apt-get install wipe.* Wipe is a little more secure and has nicer options.

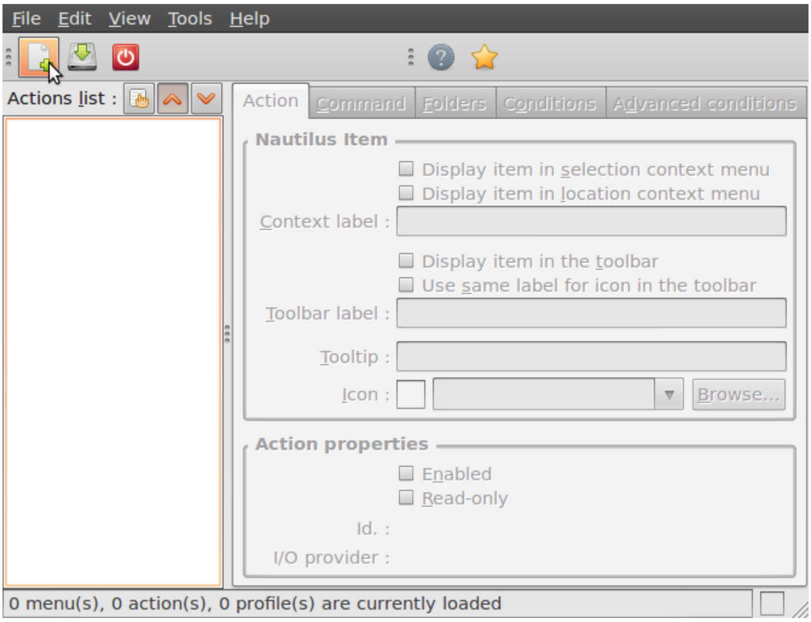
It is possible make access to these program's easy by adding it as an extra menu option

1. We assume you are familiar with the Ubuntu Software Center. To add the securely wipe option, it's required to install these two programs *wipe* and *nautilus-actions*
   If the two programs are installed follow the following steps. If they are not installed use the Ubuntu Software Center to install them or on the command line simply type *apt-get install nautilus-actions wipe*
2. Open the "Nautilus Actions Configuration" from the System -> Preferences menu



3. We have to add a new action. To do this, start clicking on the "create

new action button", the first option in the toolbar



Nautilus Item

□ Display item in selection context menu
□ Display item in location context menu

Context label :

□ Display item in the toolbar
□ Use same label for icon in the toolbar

Toolbar label :

Tooltip :

Icon :

Action properties

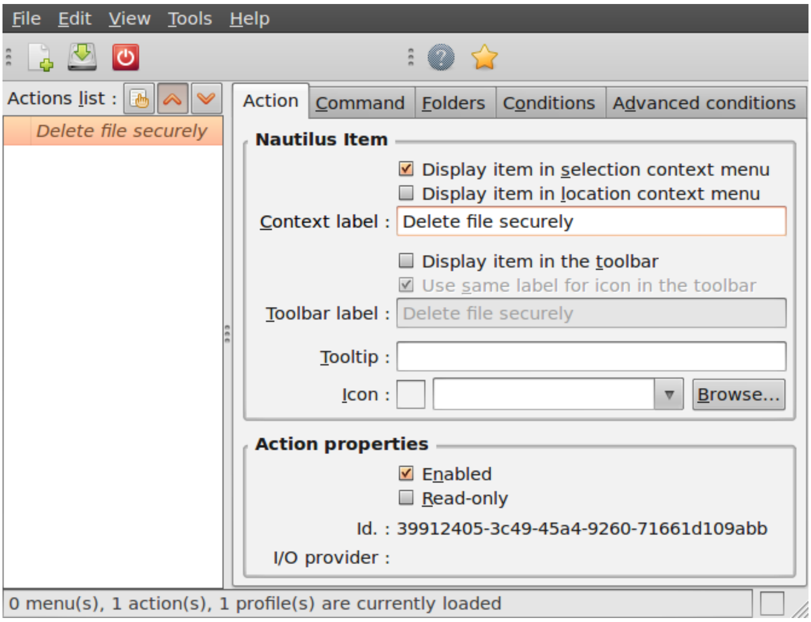
□ Enabled
□ Read-only

Id. :

I/O provider :

0 menu(s), 0 action(s), 0 profile(s) are currently loaded

4. Next is describing the new action. You can give the action every name you wish. Fill out this title in the "Context label" field. In this example we used "Delete file securely"



Delete file securely

Nautilus Item

☑ Display item in selection context menu
□ Display item in location context menu

Context label : Delete file securely

□ Display item in the toolbar
☑ Use same label for icon in the toolbar

Toolbar label : Delete file securely

Tooltip :

Icon :

Action properties

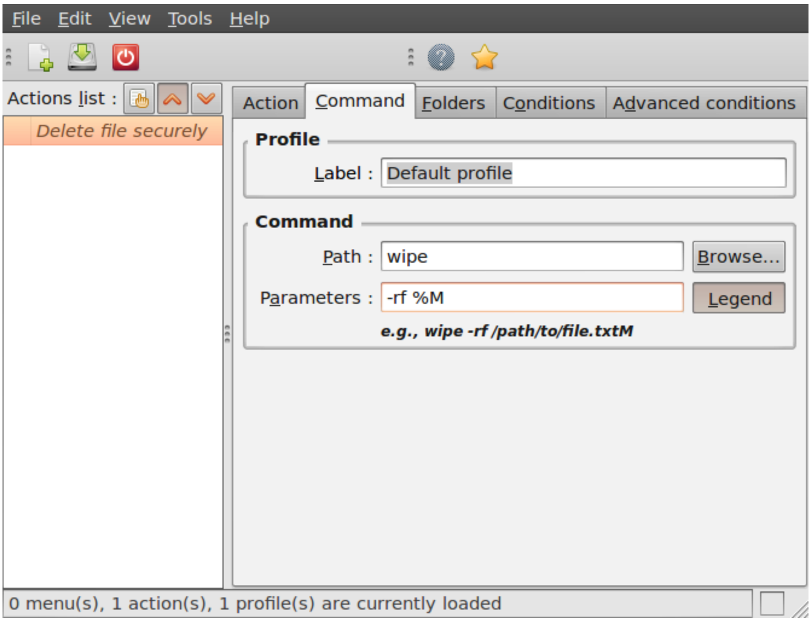
☑ Enabled
□ Read-only

Id. : 39912405-3c49-45a4-9260-71661d109abb

I/O provider :

0 menu(s), 1 action(s), 1 profile(s) are currently loaded

5. Click on the second tab ("Command"), here is how we specify the action we want. In the field "Path", type "wipe", in the field parameters type "-rf %M", please be sure about the capitalisation of all characters here, this is very important.



Delete file securely

Label : Default profile

Command

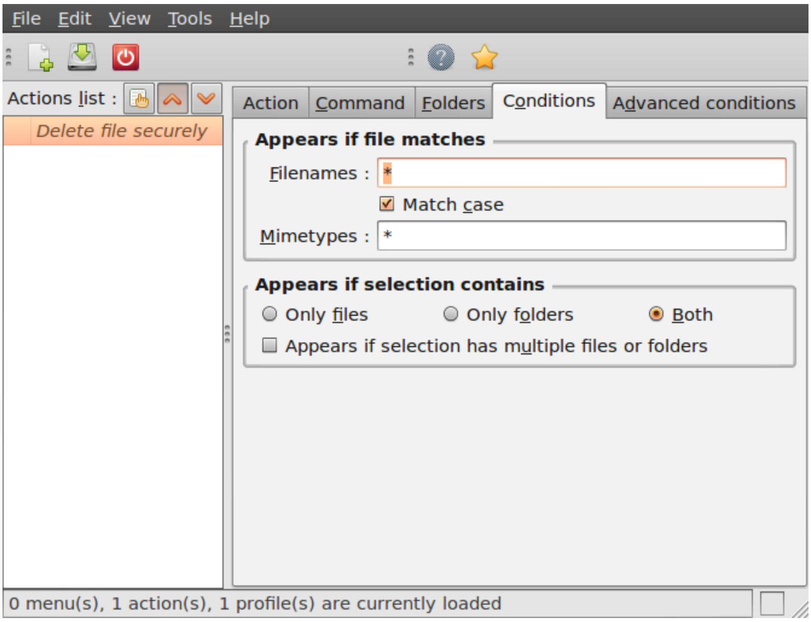
Path : wipe

Parameters : -rf %M

e.g., wipe -rf /path/to/file.txtM

0 menu(s), 1 action(s), 1 profile(s) are currently loaded

6. Next is specifying the conditions, click on the conditions tab and choose the option "Both" in the "Appears if selection contains..." box. With this option you can wipe both files and folders securely. If done, click the save button (second item on the icon bottom toolbar) or use the menu File->Save



Appears if file matches

Filenames : *

☑ Match case

Mimetypes : *

Appears if selection contains

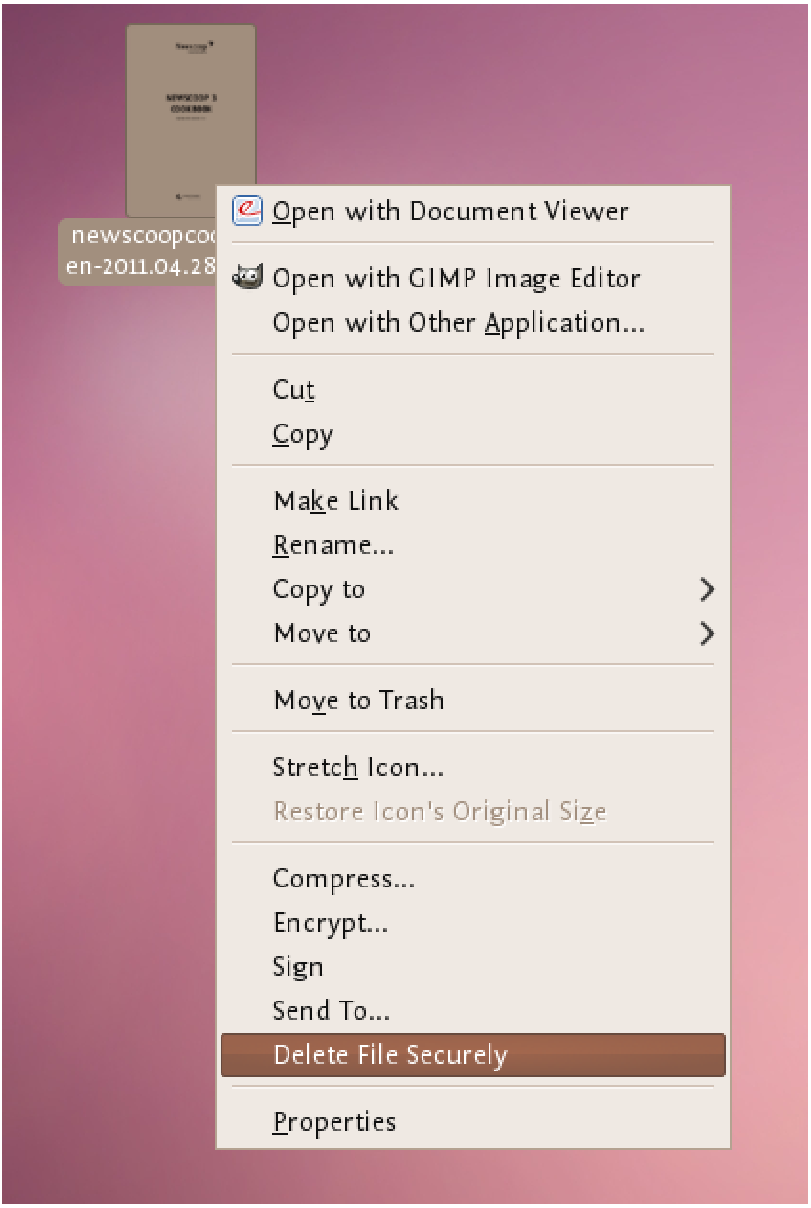
○ Only files ○ Only folders ● Both

□ Appears if selection has multiple files or folders

0 menu(s), 1 action(s), 1 profile(s) are currently loaded

7. Now close the Nautilus Actions Configuration tool. Unfortunately, after this, you have to re-login into your system, so ether reboot or logout/login.

8. Now browse to the file you want to securely delete and right click:

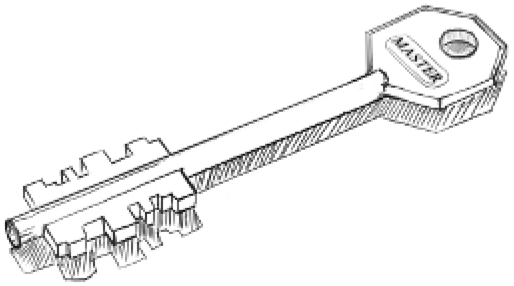


Choose 'Delete File Securely'. The file will then be wiped 'quietly' - you do not get any feedback or notice that the process has started or stopped. However the process *is* underway. It takes some time to securely delete data and the bigger the file the longer it takes. When it is complete the icon for the file to be wiped will disappear. If you would like to add some feedback you can change the parameters field in Nautilius Actions Configuration tool to this:

```
-rf %M | zenity --info --text "your wipe is underway please be patient.
The icon of the file to be wiped will disappear shortly."
```

The above line will tell you the process is underway but you will not know the file is deleted until the icon disappears.

Call Encryption



INSTALLING CSIPSIMPLE

CSipSimple is a program for Android devices that allows for making encrypted calls. Naturally the calling software isn't enough on its own and we need a communication network to enable us to make calls.

INTRODUCING THE OSTN NETWORK

If you already know about OSTN and have an account, you can skip this section.

OSTN (Open {Secure, Source, Standards} Telephony Network - https://guardianproject.info/wiki/OSTN) is an attempt to define a standard Voice over IP (VoIP) setup using the Session Initiation Protocol (SIP) that enables end-to-end encrypted calls. Similar to e-mail, SIP allows people to choose their service provider while still being able to call each other even if they are not using the same provider. Yet, not all SIP providers offer OSTN and both providers have to support OSTN for the call to be secure. Once a connection between two people is established, the audio data is exchanged directly between the two parties. Data is encrypted according to the Secure Real-time Transport Protocol (SRTP).

A majority of encrypting VoIP applications currently use Session Description Protocol Security Descriptions for Media Streams (SDES) with hop-by-hop Transport Layer Security (TLS) to exchange secret master keys for SRTP. This method is not end-to-end secure as the SRTP keys are visible in plaintext to any SIP proxy or provider involved in the call.

ZRTP is a cryptographic key-agreement protocol to negotiate the keys for encryption between two parties. ZRTP end points use the media stream rather than the signaling stream to establish the SRTP encryption keys. Since the media stream is a direct connection between the calling parties, there is no way for the SIP providers or proxies to intercept the SRTP keys. ZRTP provides a useful reassurance to end-users that they have a secure line. By reading and comparing a word pair, users can be certain that the key exchange has completed.

Open Secure Telephony (https://ostel.me/) is a testbed for OSTN that worked well at the time of writing this book. At https://ostel.me/users/sign_up you can sign up and create an account. You can also check the OSTN page listed above for other providers.

CSipSimple

CSipSimple is a free and open source client for Android that works well with OSTN. You can find it at https://market.android.com/details?id=com.csipsimple

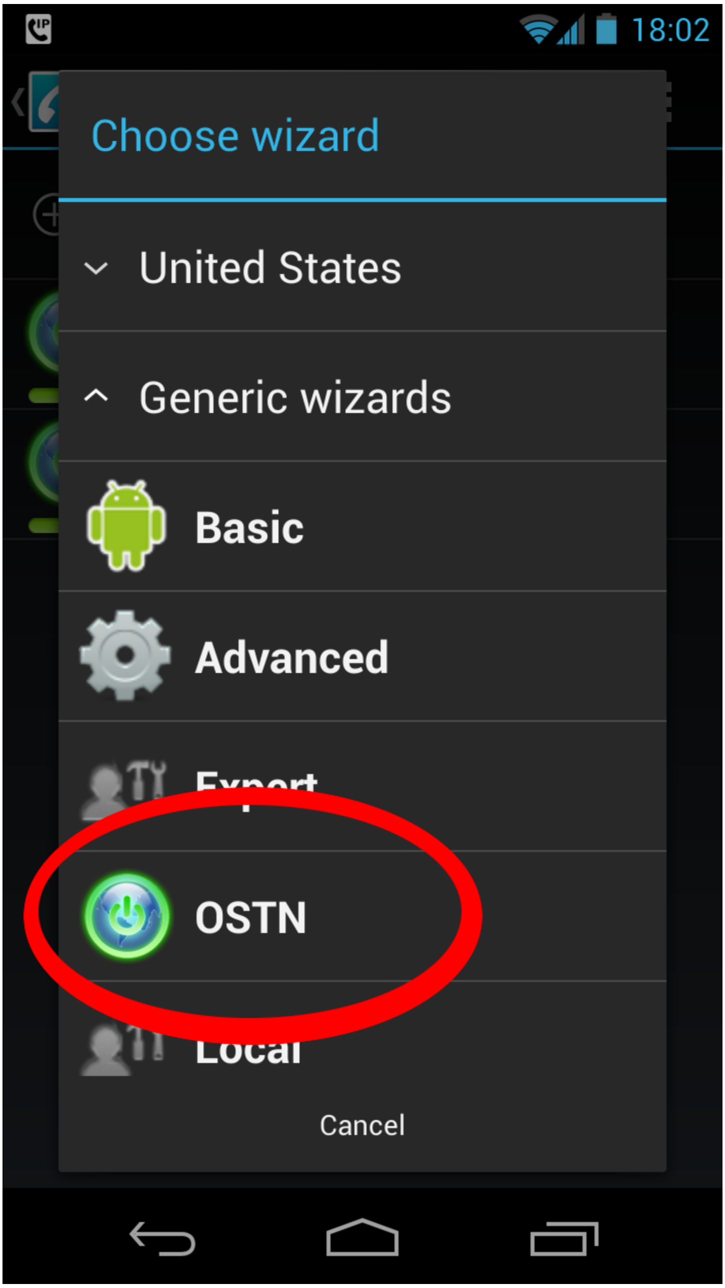
To use CSipSimple with ostel.me, select OSTN in the generic wizards when creating an account and enter username, password and server as provided after signing up at https://ostel.me/users/sign_up

Once you call another party with CSipSimple you see a yellow bar with ZRTP and the verification word pair. You now have established a secure voice connection that cannot be intercepted. Still, you should be aware that your phone or the phone of the other party could be set up to record the conversation.

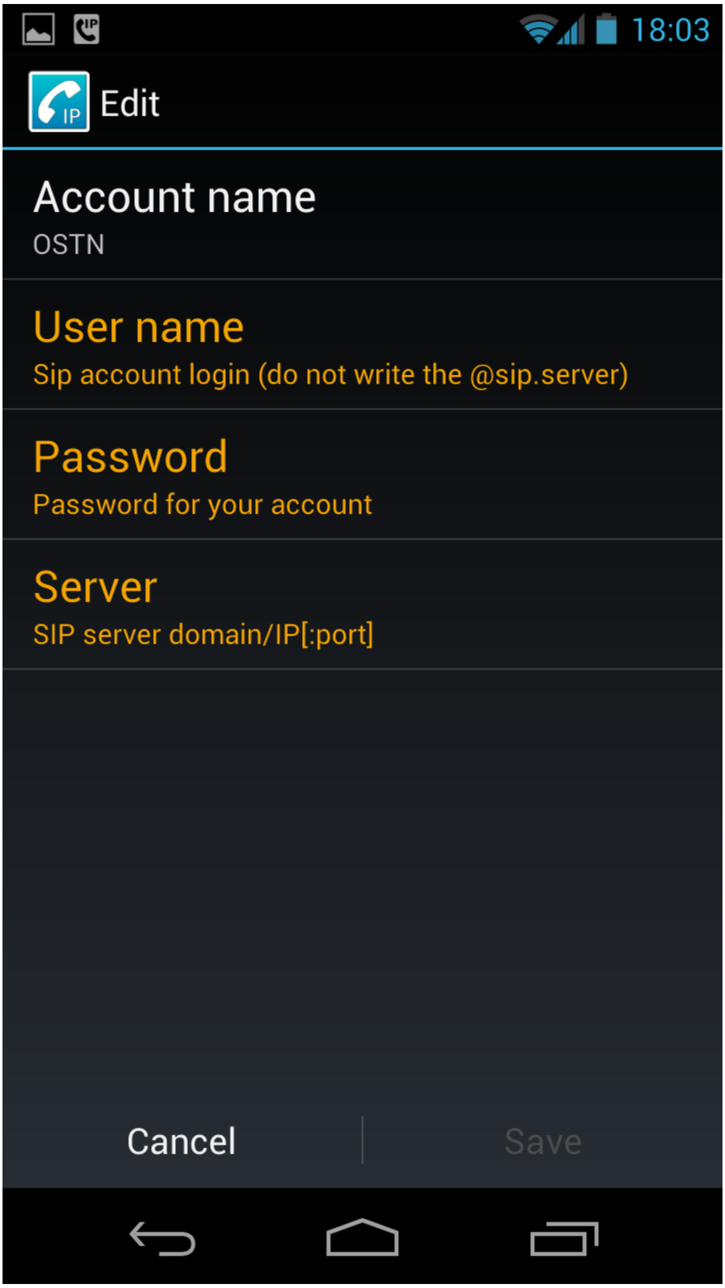
Basic steps:

1. Install CSipSimple from Google Play store or other trusted source
2. Start it up and choose if you want to make SIP calls via data connection or only WiFi
3. Configure your account

To use CSipSimple with ostel.me, select OSTN in the Generic Wizards section when creating an account. You can toggle off the "United States" providers by clicking on "United States". Now select **OSTN**:



Now you can enter your username (number), password and server (ostel.me) as provided after signing up at https://ostel.me/users/sign_up.



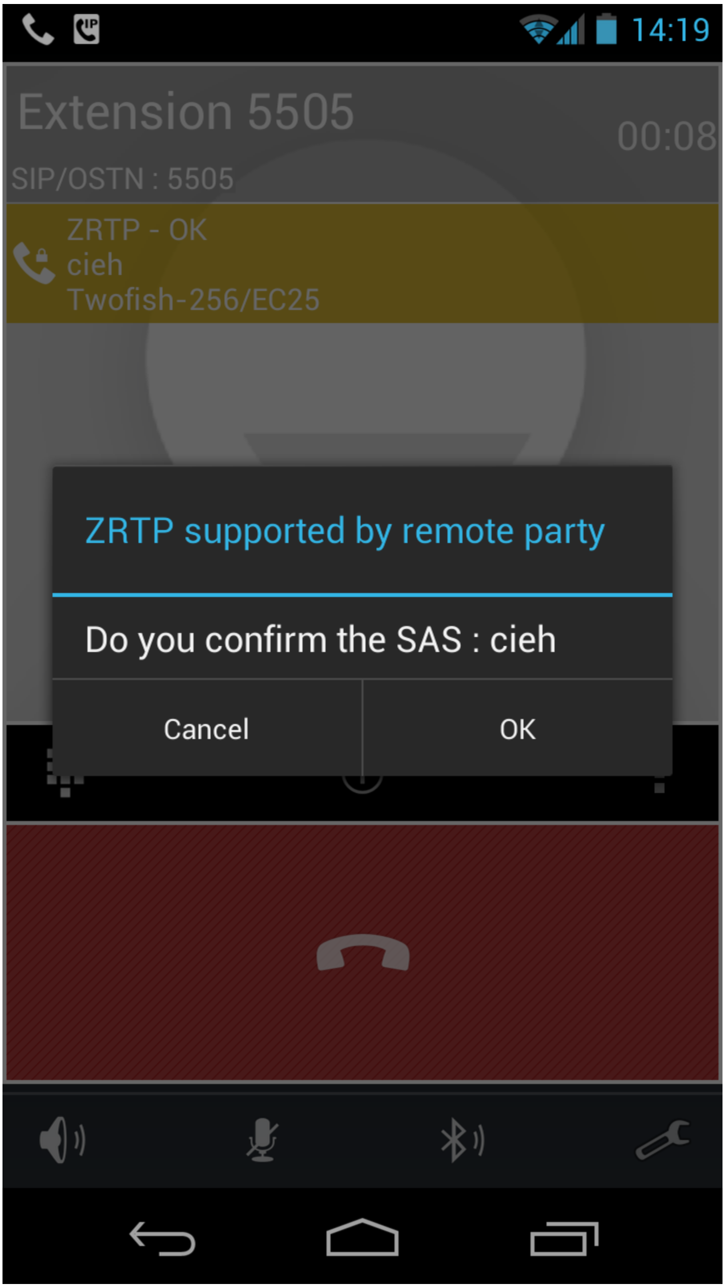
Account name
OSTN

User name
Sip account login (do not write the @sip.server)

Password
Password for your account

Server
SIP server domain/IP[:port]

Now you can make a call. The first time you connect to someone with ZRTP you have to verify that the key exchange was successful. In the example below the confirmation word is "**cieh**", you can already talk to the other party and make sure you both see the same word. Once done, press ok.



14:19

Extension 5505

00:08

SIP/OSTN : 5505

ZRTP - OK
cieh
Twofish-256/EC25

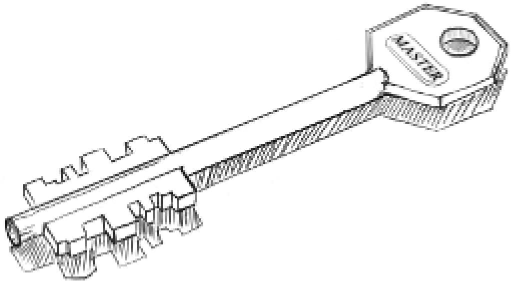
ZRTP supported by remote party

Do you confirm the SAS : cieh

You now have established a secure voice connection that cannot be intercepted. Beware that your or the phone of the other party could be recording your conversation.

Instant Messaging

Encryption



Setting up Encrypted Instant Messaging

Android - Installing Gibberbot

https://guardianproject.info/apps/gibber/

Gibberbot is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Gibberbot uses the Off-The-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install Gibberbot through the Google Play store or from another trusted source.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

iOS - Installing ChatSecure

http://chrisballinger.info/apps/chatsecure/

ChatSecure is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. ChatSecure uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install ChatSecure through the iTunes store

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

Ubuntu - Installing Pidgin

http://pidgin.im/

Pidgin is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Pidgin uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install via Ubuntu Software Center, search for pidgin-otr to install pidgin and the pidgin otr plugin.

Once installed you can enable otr for any account you setup in pidgin.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

OS X - Installing Adium

http://www.adium.im/

Adium is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Adium uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

Installing Adium is similar to installing most Mac OS X applications.

1. Download the Adium disk image from http://www.adium.im/.
2. If an Adium window doesn't open automatically, double click the downloaded file
3. Drag the Adium application to your Applications folder.
4. "Eject" the Adium disk image, which has an icon of a drive
5. The Adium disk image will still be present in your download folder (probably on your desktop). You can drag this file to the trash, as it is no longer needed.
6. To load Adium, locate it in the Applications folder and double click.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

Windows - Installing Pidgin

http://pidgin.in/

Pidgin is a secure chat client capable of end-to-end encryption. It works with

Google, Facebook, any Jabber or XMPP server. Pidgin uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

To use Pidgin with OTR on Windows, you have to install Pidgin and the OTR plugin for Pidgin.

1. Download the latest version of Pidgin from http://www.pidgin.im/download/windows/
2. Run the Pidgin Installer
3. Download the latest version of "OTR plugin for Pidgin" from http://www.cypherpunks.ca/otr/#downloads
4. Run the OTR Plugin Installer

Now you can use OTR with any account you setup in Pidgin.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

ALL OS - CRYPTO.CAT

https://crypto.cat

Cryptocat is an open source web application intended to allow secure, encrypted online chatting. Cryptocat encrypts chats on the client side, only trusting the server with data that is already encrypted. Cryptocat is delivered as a browser extension and offers plugins for Google Chrome, Mozilla Firefox and Apple Safari.

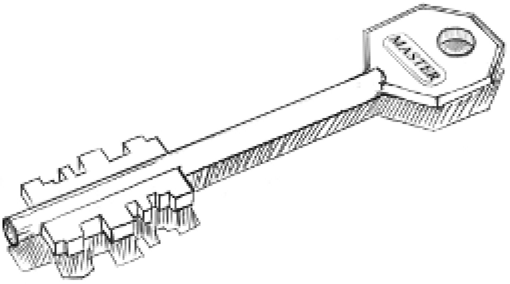
Cryptocat intends to provide means for impromptu, encrypted communications that offer more privacy than services such as Google Talk, while maintaining a higher level of accessibility than other high-level encryption platforms, and furthermore allows for multiple users in one chat room.

Chat Log Files

Some of the Chat Clients listed above e.g. Adium, store plaintext, unencrypted Chat Logs, often **by default**, even when the OTR "security / privacy" plug-in is installed.

If you are taking OTR precautions to protect your chats from snoopers over the wire or over the air, you should either double check that you have manually switched off Chat Session Logging, or ensure that the Chat Logs you deliberately intend to keep are created on an encrypted disk drive or volume, in case your computer is lost, stolen or seized. It is also worth asking the person you are chatting with if they are inadvertently logging the chat with their own Chat Client software.

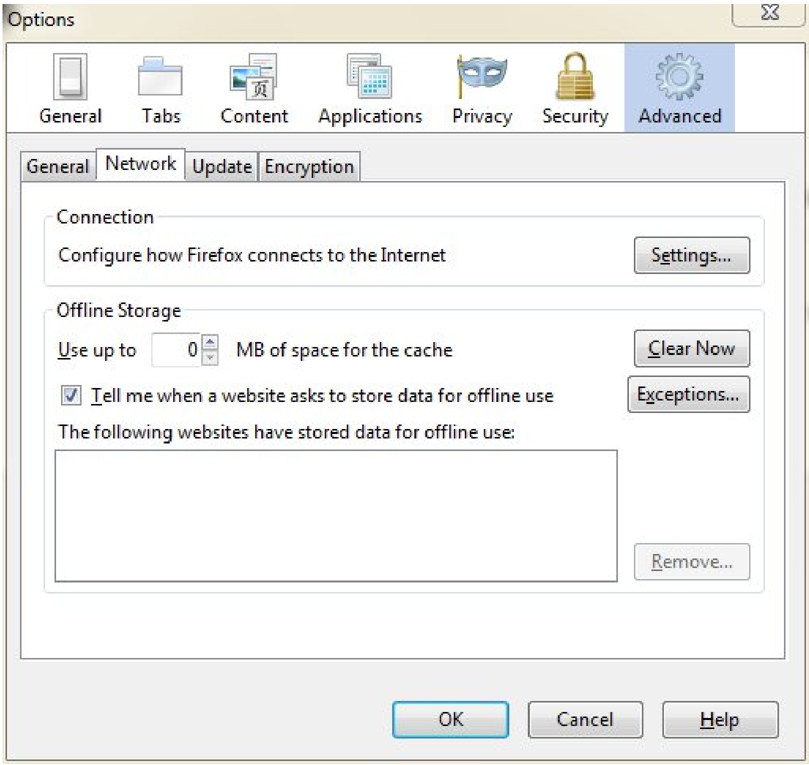
Secure File Sharing



Installing I2P on Ubuntu

1. Open a terminal and enter:
   ```
   sudo apt-add-repository ppa:i2p-maintainers/i2p
   ```
   This command will add the PPA to /etc/apt/sources.list.d and fetch the gpg key that the repository has been signed with. The GPG key ensures that the packages have not been tampered with since being built.
2. Notify your package manager of the new PPA by entering
   ```
   sudo apt-get update
   ```
   This command will retrieve the latest list of software from each repository that is enabled on your system, including the I2P PPA that was added with the earlier command.
3. You are now ready to install I2P!
   ```
   sudo apt-get install i2p
   ```
4. Your browse should open up with your local I2P router console, to browse i2p domains you have to configure your browser to use the i2p proxy. Also check your connection status on the left side on the router console. If your status is **Network: Firewalled** your connection will be rather slow. The first time you start I2P it may take a few minutes to integrate you into the network and find additional peers to optimize your integration, so please be patient.

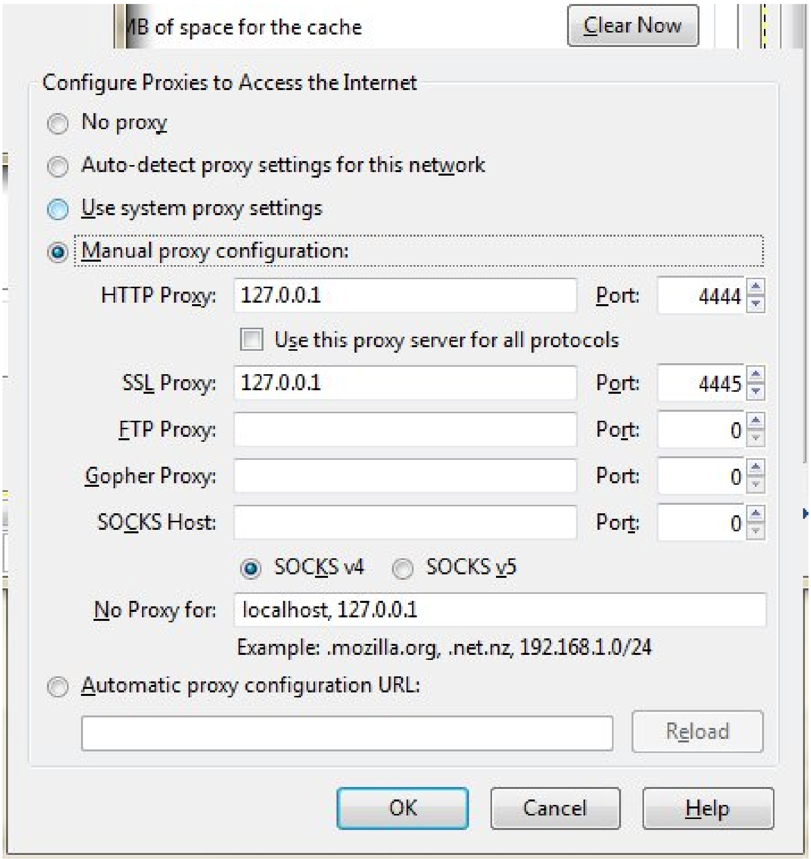
From the Tools menu, select Options to bring up the Firefox settings panel. Click the icon labelled *Advanced*, then click on the *Network* tab. In the *Connections* section, click on the Settings button. You'll see a Window like the following:



Use up to 0 MB of space for the cache

☑ Tell me when a website asks to store data for offline use

In the *Connection Settings* window, click the circle next to *Manual proxy configuration*, then enter 127.0.0.1, port 4444 in the HTTP Proxy field. Enter 127.0.0.1, port 4445 in the SSL Proxy field. Be sure to enter localhost and 127.0.0.1 into the "No Proxy for" box.



IB of space for the cache

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 4444

□ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 4445

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

● SOCKS v4 ○ SOCKS v5

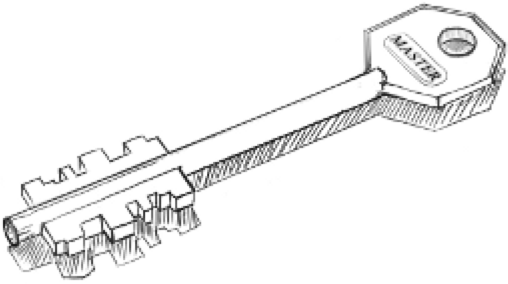
No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

For more information and proxy settings for other browsers check http://www.i2p2.de/htproxyports.htm

Appendices



The necessity of Open Source

The last 20 years have seen network technology reaching ever more deeply into our lives, informing how we communicate and act within the world. With this come inherent risks: the less we understand the network environment we depend upon, the more vulnerable we are to exploitation.

This ignorance is something traditionally enjoyed by criminals. In recent years however some corporations and governments have exploited civilian ignorance in a quest for increased control. This flagrant and often covert denial of dignity breaches many basic rights, the right to privacy, in particular.

Closed source software has been a great boon to such exploitation – primarily due to the fact there is no code available for open, decentralised security auditing by the community . Under the auspices of hiding trade secrets, closed-source software developers have proven to be unwilling to explain to users how their programs work. This might not always be an issue were it not for the high stakes: identity theft, the distribution of deeply personal opinion and sentiment, a persons diverse interests and even his/her home increasingly come into close contact with software in a world-wide network context. As such, many people find themselves using software for personal purposes with full trust that it are secure. The Windows operating system itself is the most obvious real-world example. Apple's OS X follows close behind, with large portions of the operating system's inner-workings barred from public inspection.

In Cryptography there is a strong principle, established in the 19th century by *Auguste Kerckhoff* (and hence named after him) which demands that

"[the encryption method] must not be required to be secret, and it must
be able to fall into the hands of the enemy without inconvenience".

While this principle has been taken further by most scientific and (of course) open source communities – publishing their methods and inner-workings upfront, so potential weaknesses can be pointed out and fixed before further distribution – most distributors of proprietary software rely on obfuscation to hide the weaknesses of their software. As such they often prove to address newly discovered vulnerabilities in a non-transparent way – leaving many trusting users at risk of exploitation.

Of course it must be said that Open Source Software is as secure as you make it (and there is a lot of OSS written by beginners). However there are many good examples of well written, well managed software which have such a large (and concerned) user base that even the tiniest of mistakes are quickly found and dealt with. This is especially the case with software depended upon in a network context.

To use closed source software in a network context is not only to be a minority, it is to be overlooked by a vast community of concerned researchers and specialists that have your privacy and safety in mind.

N.B. There is also a more cynical view of Open Source Software, which points out that since nobody is paid full time to constantly review and regression test the latest tinkering by unskilled or deliberately malicious programmers, it can also suffer from major security weaknesses which go undetected for long periods of time in complicated software, leaving it vulnerable to hackers, criminals and intelligence agencies etc. e.g. the (now fixed) Debian Linux predictable random number generator problem which led to the creation of lots of weak cryptographic keys.

Cryptography and Encryption

Cryptography and encryption are similar terms, the former being the science and latter the implementation of it. The history of the subject can be traced back to ancient civilisations, when the first humans began to organise themselves into groups. This was driven in part by the realisation that we were in competition for resources and tribal organisation, warfare and so forth were necessary, so as to keep on top of the heap. In this respect cryptography and encryption are rooted in warfare, progression and resource management, where it was necessary to send secret messages to each other without the enemy deciphering ones moves.

Writing is actually one of the earliest forms of cryptography as not everyone could read. The word cryptography stems from the Greek words kryptos (hidden) and graphein (writing). In this respect cryptography and encryption in their simplest form refer to the writing of hidden messages, which require a system or rule to decode and read them. Essentially this enables you to protect your privacy by scrambling information in a way that it is only recoverable with certain knowledge (passwords or passphrases) or possession (a key).

Put in another way, encryption is the translation of information written in plaintext into a non-readable form (ciphertext) using algorithmic schemes (ciphers). The goal is to use the right key to unlock the ciphertext and return it back into its original plain text form so it becomes readable again.

Although most encryption methods refer to written word, during World War Two, the US military used Navajo Indians, who traveled between camps sending messages in their native tongue. The reason the army used the Navajo tribe was to protect the information they were sending from the Japanese troops, who famously could not decipher the Navajo's spoken language. This is a very simple example of using a language to send messages that you do not want people to listen into or know what you're discussing.

Why is encryption important?

Computer and telecommunication networks store digital echoes or footprints of our thoughts and records of personal lives.

From banking, to booking, to socialising: we submit a variety of detailed, personalised information, which is driving new modes of business, social interaction and behavior. We have now become accustomed to giving away what was (and still is) considered private information in exchange for what is presented as more personalised and tailored services, which might meet our needs, but cater to our greed.

But how do we protect who sees, controls and uses this information?

Lets consider a scenario whereby we all thought it was fine to send all our communication on open handwritten postcards. From conversations with your doctor, to intimate moments with our lovers, to legal discussions you may have with lawyers or accountants. It's unlikely that we would want all people to be able to read such communications. So instead we have written letters in sealed envelopes, tracking methods for sending post, closed offices and confidential agreements, which help to keep such communication private. However given the shift in how we communicate, much more of this type of interaction is taking place online. More importantly it is taking place through online spaces, which are not private by default and open to people with little technical skills to snoop into the matters that can mean the most to our lives.

Online privacy and encryption is something we therefore need to be aware of and practice daily. In the same way we would put an important letter into an envelope or have a conversation behind a closed door. Given that so much of our private communication is now happening in networked and online spaces, we should consider the interface, like envelopes or seals, which protect this material as a basic necessity and human right.

Encryption examples

Throughout history we can find examples of cipher methods, which have been used to keep messages private and secret.

A Warning!

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files" - Bruce Schneier, Applied Cryptography, 1996

This chapter first explains a number of historical cryptographic systems and then provides a summary of modern techniques. The historical examples illustrate how cryptography emerged, but are considered **broken** in the face of modern computers. They can be fun to learn, but please don't use them for anything sensitive!

Historical ciphers

Classical ciphers refer to historical ciphers, which are now out of popular use or no longer applicable. There are two general categories of classical ciphers: transposition and substitution ciphers.

In a transposition cipher, the letters themselves are kept unchanged, but the order within the message is scrambled according to some well-defined scheme. An example of a transposition cipher is Skytale, which was used in ancient Rome and Greece. A paperstrip was wrapped around a stick and the message written across it. That way the message could not be read unless wound around a stick of similar diameter again.

Image: Skytale taken from Wikimedia Commons (3.10.12)

A substitution cipher is a form of classical cipher whereby letters or groups of letters are systematically replaced throughout the message for other letters (or groups of letters). Substitution ciphers are divided into monoalphabetic and polyalphabetic substitutions. The Caesar Shift cipher is common example of amonoalphabetic substitution ciphers, where the letters in the alphabet are shifted in one direction or another.

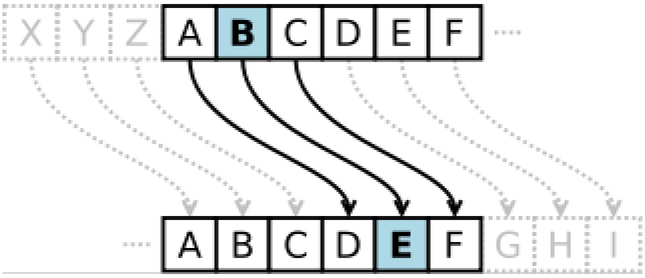
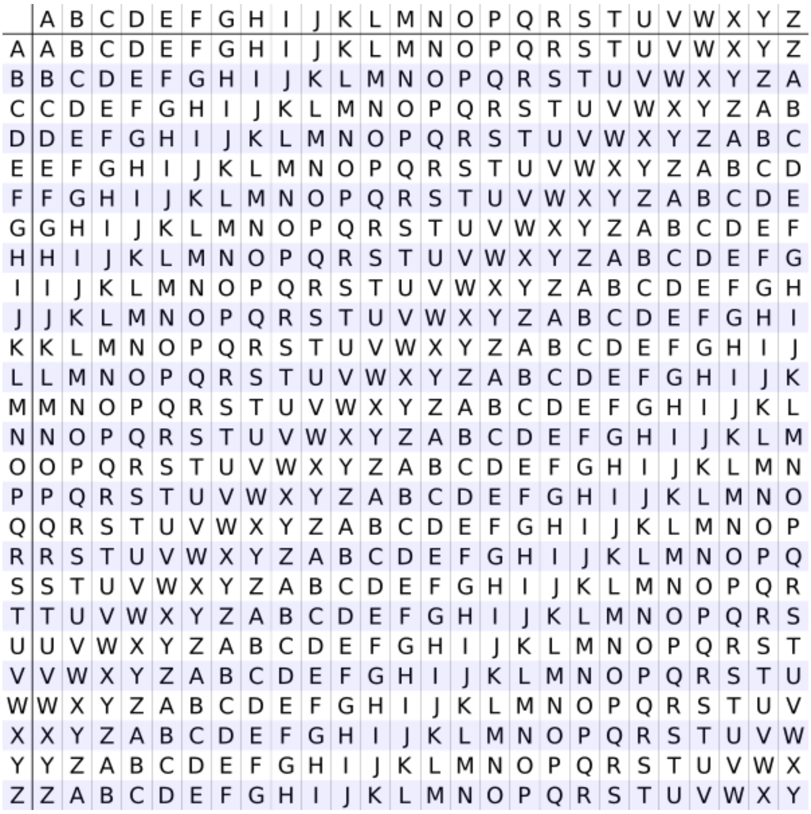


Image: Caesar Shift Cipher taken from Wikimedia Commons (3.10.12)

Polyalphabetic substitutions are more complex than substitution ciphers as they use more than one alphabet and rotate them. For example, The Alberti cipher, which was the first polyalphabetic cipher was created by Leon Battista Alberti, a 15th century Italian, Renaissance polymath and humanist who is also credited as the godfather of western cryptography. His cipher is similar to the Vigenère cipher, where every letter of the alphabet gets a unique number (e.g. 1-26). The message is then encrypted by writing down the message along with the password repeatedly written beneath it.

In the Vigenère cipher the corresponding numbers of the letters of message and key are summed up (with numbers exceeding the alphabet being dragged around the back) making the message so unreadable that it couldn't be deciphered for centuries (nowadays, with the help of computers, this obviously isn't true anymore).



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Image: Vigenère cipher taken from Wikimedia Commons (3.10.12)

During World War 2 there was a surge in crypography, which lead to the development of new algorithms such as the one-time pad (OTP). The OTP algorithm combines plaintext with a random key that is as long as the plaintext so that each character is only used once. To use it you need two copies of the pad, which are kept by each user and exchanged via a secure channel. Once the message is encoded with the pad, the pad is destroyed and the encoded message is sent. On the recipient's side, the encoded message has a duplicate copy of the pad from which the plaintext message is generated. A good way to look at OTP is to think of it as a 100% noise source, which is used to mask the message. Since both parties of the communication have copies of the noise source they are the only people who can filter it out.

OTP lies behind modern day stream ciphers, which are explained below. Claude Shannon, (a key player in modern cryptography and information theory), in his seminal 1949 paper "Communication Theory of Secrecy

Systems" demonstrated that theoretically all unbreakable ciphers should include the OTP encryption, which if used correctly are impossible to crack.

Modern ciphers

Post the World Wars the field of cryptography became less of a public service and fell more within the domain of governance. Major advances in the field began to reemerge in the mid-1970s with the advent of personalised computers and the introduction of the Data Encryption Standard (DES, developed at IBM in 1977 and later adopted by the U.S government). Since 2001 we now use the AES, Advanced Encryption Standard), which is based on symmetric cryptography forms.

Contemporary cryptography can be generally divided into what is called symmetric, asymmetric and quantum cryptography.

Symmetric cryptography, or secret key, cryptography refers to ciphers where the same key is used to both encrypt and decrypt the text or information involved. In this class of ciphers the key is shared and kept secret within a restricted group and therefore it is not possible to view the encrypted information without having the key. A simple analogy to secret key cryptography is having access to a community garden, which has one key to open gate, which is shared by the community. You cannot open the gate, unless you have the key. Obviously the issue here with the garden key and with symmetric cryptography is if the key falls into the wrong hands, then an intruder or attacker can get in and the security of the garden, or the data or information is compromised. Consequently one of the main issues with this form of cryptography is the issue of key management. As a result this method is best employed within single-user contexts or small group environments.

Despite this limitation symmetric key methods are considerably faster than asymmetric methods and so are the preferred mechanism for encrypting large chunks of text.

Symmetric ciphers are usually implemented using **block ciphers** or **stream ciphers**.

Block ciphers work by looking at the input data in 8 or 16 or 32 byte blocks at a time and spreading the input and key within those blocks. Different modes of operation are performed on the data in order to transform and spread the data between blocks. Such ciphers use a secret key to convert a fixed block of plain text into cipher text. The same key is then used to decrypt the cipher text.

In comparison stream ciphers (also known as state cipher) work on each plaintext digit by creating a corresponding keystream which forms the ciphertext. The keystream refers to a stream of random characters (bits, bytes, numbers or letters) on which various additive or subtractive functions are performed and combined to a character in the plaintext message, which then produces the ciphertext. Although this method is very secure, it is not always practical, since the key of the same length as the message needs to be transmitted in some secure way so that receiver can decypher the message. Another limitation is that the key can only be used once and then its discarded. Although this can mean almost watertight security, it does limit the use of the cipher.

Asymmetric ciphers work much more complex mathematical problems with back doors, enabling faster solutions on smaller, highly important pieces of data. They also work on fixed data sizes, typically 1024-2048 bits and and 384 bits. What makes them special is that they help solve some of the issues with key distribution by allocating one public and one private pair per person, so that everyone just needs to know everyone else's public portion. Asymmetric ciphers are also used for digital signatures. Where as symmetric ciphers are generally used for message authenticity. Symmetric ciphers cannot non-repudiation signatures (i.e., signatures that you cannot later deny that you did not sign). Digital signatures are very important in modern day cryptography. They are similar to wax seals in that they verify who the message is from and like seals are unique to that person. Digital signatures are one of the methods used within public key systems, which have transformed the field of cryptography are central to modern day Internet security and online transactions.

Quantum Cryptography

Quantum cryptography is the term used to describe the type of cryptography that is now necessary to deal with the speed at which we now process information and the related security measures that are necessary. Essentially it deals with how we use quantum communication to securely exchange a key and its associated distribution. As the machines we use become faster the possible combinations of public-key encryption and digital signatures becomes easier to break and quantum cryptography deals with the types of algorithms that are necessary to keep pace with more advanced networks.

Challenges & Implications

At the heart of cryptography lies the challenge of how we use and communicate information. The above methods describe how we encrypt written communication but obviously as shown in the Navajo example other forms of communication (speech, sound, image etc) can also be encrypted using different methods.

The main goal and skill of encryption is to apply the right methods to support trustworthy communication. This is achieved by understanding the tradeoffs, strengths and weaknesses of different cipher methods and how they relate to the level of security and privacy required. Getting this right depends on the task and context.

Importantly when we speak about communication, we are speaking about trust. Traditionally cryptography dealt with the hypothetical scenarios, where the challenge was to address how 'Bob' could speak to 'Alice' in a private and secure manner.

Our lives are now heavily mediated via computers and the Internet. So the boundaries between Bob, Alice + the 'other' (Eve, Oscar, Big Brother, your boss, ex-boyfriend or the government) are a lot more blurred. Given the quantum leaps in computer processing, in order for 'us', Bob's and Alice's to have trust in the system, we need to know who we are talking too, we need to know who is listening and importantly who has the potential to eavesdrop. What becomes important is how we navigate this complexity and feel in control and secure, so that you can engage and communicate in a trustful manner, which respects our individual freedoms and privacy.

Threat Modeling

Threat Modeling is the practice of building an abstract description of how an attack may proceed and cause damage in order to define strategies and means to defend against it. It is an important part of working toward protecting an *Information System* (like your computer, or a network you are responsible for), especially if there are many points of potential vulnerability.

Introduction

Before we begin, it's important to define what a threat is, in an Information System (IS) context. A succint description from the National Information Assurance Glossary defines a *threat* as:

> *Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.*

Their more comprehensive (read "absurdly long") definition is:

> *The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. Categorize and classify threats as follows: Categories Classes Human Intentional Unintentional Environmental Natural Fabricated 2. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification or data, and/or denial of service. 3. Any circumstance or event with the potential to cause harm to the ADP system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities regardless of the amount of fire protection available. 4. Types of computer systems related adverse events (i. e. , perils) that may result in losses. Examples are flooding, sabotage and fraud. 5. An assertion primarily concerning entities of the external environment (agents); we say that an agent (or class of agents) poses a threat to one or more assets; we write: T(e;i) where: e is an external entity; i is an internal entity or an empty set. 6. An undesirable occurrence that might be anticipated but is not*

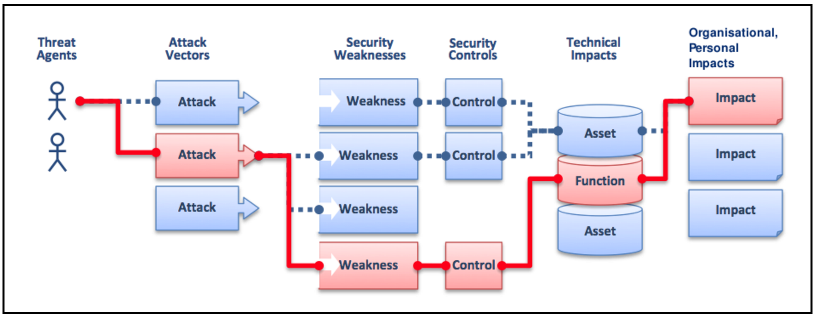
> *the result of a conscious act or decision. In threat analysis, a threat is defined as an ordered pair, , suggesting the nature of these occurrences but not the details (details are specific to events). 7. A potential violation of security. 8. A set of properties of a specific external entity (which may be either an individual or class of entities) that, in union with a set of properties of a specific internal entity, implies a risk (according to some body of knowledge).*

Broadly speaking, a threat implies *vulnerability,* this can come in the form of a person directly spying on your communications or in the form of an automated system (malware or software on the network). It can also come from environmental phenomena, such as fire. In the context of this handbook we'll consider threats as coming from an *agent* attacking with a *motivation* rather than environmental phenomena or 'Acts of God'.

An attack is *active* when it is attempting to manipulate and/or affect a system's resources and/or its general operation. In this way it can be said to compromise the *Integrity* or *Availability* of a system. A *passive attack* however is something that is commonly done as part of an attempt to learn about a system and/or access information on the system but does not actually affect the general running or availability of that system (text adapted from *RFC2828*).

Successful attacks can be *known* or *unknown.* All successful attacks *exploit* a *weakness.* While neither are desirable, knowledge of a successful attack *exposes* one or more weaknesses, providing an opportunity for *hardening* the *defense strategy.* Attacks that manipulate a system often take *control* of *functions* on the system.

Not all attacks are strictly related to the system itself. A highly sophisticated attack may deploy *Social Engineering* strategies to manipulate a person to give the attacker access to a system or to important information. Some of these attacks can themselves be automated. *Phishing* and *Pretexting* are two such examples.



Modeling Threats

Here are three often-cited frames for the modeling of threats:

Asset-centric: Here the model begins with looking at the assets (personal information, bank account data, for instance) that are stored on a trusted system. From there particular strategies for accessing those assets might be determined. For instance, a strong passphrase used for logging into an online banking service is of little use if the user of that account is vulnerable to *Phishing* attacks. Similarly, valued data assets stored on an *Encrypted File System* on a laptop might be safe from prying eyes but are still are vulnerable to kinds of attacks whose goal is to destroy that data (from malware, to an axe or a cup of spilled coffee), unless secured backups are in place.

Attacker-centric: This model starts with trying to determine the motivations and goals of an attacker in order to isolate their method and means of attack. An example might be that an attacker might want to listen into an important phone call in order to determine the time and place of a special meeting. From there we would look at how they might do this based on how (landline, cellular phone or Voice Over IP) and in what context. Does attacker have access to the service being used (wiretapping)? What hardware is the caller using? What software (if any) is the caller using and what are its known vulnerabilities?

System-centric: System-centric modeling considers threat from the perspective of the system itself, most typically the design of the software in use. Each element of the system is studied for vulnerabilities, resulting in determination of an overall *attack surface*.

Threat Agents

Attacks have a *motivation*. Typically they are to spy, steal identities, aquire/destroy data (assets), control a system or render a system dysfunctional. There are many different means to achieve these outcomes, each of which relates directly to the conditions the attacker is working with at the time. These conditions might comprise social, psychological, network, operating system and application security factors all the same time.

Risk Management Insight LLC published a paper in 2006 (http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf) that defines five kinds of *Threat Agents*:

- Access – simple unauthorized access
- Misuse – unauthorized use of assets (e.g., identity theft, setting up a porn distribution service on a compromised server, etc.)
- Disclose – the threat agent illicitly discloses sensitive information
- Modify – unauthorized changes to an asset
- Deny access – includes destruction, theft of a non-data asset, etc.

Threat Consequences

It's often very useful to have the particular consequences of a successful attack in mind when modeling threats. This can help us to get closer to isolating the particular strategies an attacker might deploy in search of their goal.

The Internet Engineering Task Force defines *Threat Consequences* in RFC2828 (http://tools.ietf.org/html/rfc2828). Here is an adaptation of that definition, with references to the (extensive) glossary and natural disaster removed:

A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation. The following subentries describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

1. "(Unauthorized) Disclosure": A circumstance or event whereby an entity gains access to data for which the entity is not authorized. (See: data confidentiality.) The following threat actions can cause unauthorized disclosure:

a. *Exposure*: A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:

- *Deliberate Exposure*: Intentional release of sensitive data to an unauthorized entity.
- *Scavenging*: Searching through data residue in a system to gain unauthorized knowledge of sensitive data.
- **Human error*: Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data.
- **Hardware/software error*: System failure that results in an entity gaining unauthorized knowledge of sensitive data.

b. *Interception*: A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. This includes:

- *Theft*: Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
- *Wiretapping (passive)*: Monitoring and recording data that is flowing between two points in a communication system. (See: wiretapping.)
- *Emanations analysis*: Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: emanation.)

c. *Inference*: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. This includes:

- *Traffic analysis*: Gaining knowledge of data by observing the characteristics of communications that carry the data.
- *Signals analysis*: Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and

that contains the data but is not intended to communicate the data. (See: emanation.)

d. *Intrusion*: A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. This includes:

- *Trespass*: Gaining unauthorized physical access to sensitive data by circumventing a system's protections.
- *Penetration*: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
- *Reverse engineering*: Acquiring sensitive data by disassembling and analyzing the design of a system component.
- *Cryptanalysis*: Transforming encrypted data into plaintext without having prior knowledge of encryption parameters or processes.

2. "Deception": A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. The following threat actions can cause deception:

a. Masquerade: A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.

- *Spoof*: Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
- *Malicious logic*: In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

b. *Falsification*: A threat action whereby false data deceives an authorized entity. (See: active wiretapping.)

- *Substitution*: Altering or replacing valid data with false data that serves to deceive an authorized entity.
- *Insertion*: Introducing false data that serves to deceive an authorized entity.

c. *Repudiation*: A threat action whereby an entity deceives another by falsely denying responsibility for an act. (See: non-repudiation service).

- *False denial of origin*: Action whereby the originator of data denies responsibility for its generation.
- *False denial of receipt*: Action whereby the recipient of data denies receiving and possessing the data.

3. "Disruption": A circumstance or event that interrupts or prevents the correct operation of system services and functions. (See: denial of service.) The following threat actions can cause disruption:

a. *Incapacitation*: A threat action that prevents or interrupts system operation by disabling a system component.

- *Malicious logic*: In context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources.
- *Physical destruction*: Deliberate destruction of a system component to interrupt or prevent system operation.
- *Human error*: Action or inaction that unintentionally disables a system component.
- *Hardware or software error*: Error that causes failure of a system component and leads to disruption of system operation.

b. *Corruption*: A threat action that undesirably alters system operation by adversely modifying system functions or data.

- *Tamper*: In context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.
- *Malicious logic*: In context of corruption, any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data.
- *Human error*: Human action or inaction that unintentionally results in the alteration of system functions or data.
- *Hardware or software error*: Error that results in the alteration of system functions or data.

c. *Obstruction*: A threat action that interrupts delivery of system services by hindering system operations.

- *Interference*: Disruption of system operations by blocking communications or user data or control information.
- *Overload*: Hindrance of system operation by placing excess burden on the performance capabilities of a system component. (See: flooding.)

4. "Usurpation": A circumstance or event that results in control of system services or functions by an unauthorized entity. The following threat actions can cause usurpation:

a. *Misappropriation*: A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.

- *Theft of service*: Unauthorized use of service by an entity.
- *Theft of functionality*: Unauthorized acquisition of actual hardware, software, or firmware of a system component.
- *Theft of data*: Unauthorized acquisition and use of data.

b. *Misuse*: A threat action that causes a system component to perform a function or service that is detrimental to system security.

- *Tamper*: In context of misuse, deliberate alteration of a system's logic, data, or control information to cause the system to perform unauthorized functions or services.
- *Malicious logic*: In context of misuse, any hardware, software, or firmware intentionally introduced into a system to perform or control execution of an unauthorized function or service.
- *Violation of permissions*: Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.

Glossary

Much of this content is based on http://en.cship.org/wiki/Special:Allpages

AGGREGATOR

An aggregator is a service that gathers syndicated information from one or many sites and makes it available at a different address. Sometimes called an RSS aggregator, a feed aggregator, a feed reader, or a news reader. (Not to be confused with a **Usenet** News reader.)

ANONYMITY

(Not be confused with privacy, pseudonymity, security, or confidentiality.)

Anonymity on the Internet is the ability to use services without leaving clues to one's identity or being spied upon. The level of protection depends on the anonymity techniques used and the extent of monitoring. The strongest techniques in use to protect anonymity involve creating a chain of communication using a random process to select some of the links, in which each link has access to only partial information about the process. The first knows the user's Internet address (IP) but not the content, destination, or purpose of the communication, because the message contents and destination information are encrypted. The last knows the identity of the site being contacted, but not the source of the session. One or more steps in between prevents the first and last links from sharing their partial knowledge in order to connect the user and the target site.

ANONYMOUS REMAILER

An anonymous remailer is a service that accepts e-mail messages containing instructions for delivery, and sends them out without revealing their sources. Since the remailer has access to the user's address, the content of the message, and the destination of the message, remailers should be used as part of a chain of *multiple* remailers so that no one remailer knows all this information.

ASP (Application service provider)

An ASP is an organization that offers software services over the Internet, allowing the software to be upgraded and maintained centrally.

BACKBONE

A backbone is one of the high-bandwidth communications links that tie together networks in different countries and organizations around the world to form the Internet.

BADWARE

See **malware**.

BANDWIDTH

The bandwidth of a connection is the maximum rate of data transfer on that connection, limited by its capacity and the capabilities of the computers at both ends of the connection.

BASH (Bourne-again shell)

The bash shell is a command-line interface for Linux/Unix operating systems, based on the Bourne shell.

BitTorrent

BitTorrent is a **peer-to-peer** file-sharing **protocol** invented by Bram Cohen in 2001. It allows individuals to cheaply and effectively distribute large files, such as CD images, video, or music files.

BLACKLIST

A blacklist is a list of forbidden things. In Internet censorship, lists of forbidden Web sites or the IP addresses of computers may be used as blacklists; **censorware** may allow access to all sites except for those specifically listed on its blacklist. An alternative to a blacklist is a **whitelist**, or a list of permitted things. A whitelist system blocks access to all sites except for those specifically listed on the whitelist. This is a less common approach to Internet censorship. It is possible to combine both approaches, using string matching or other conditional techniques on **URL**s that do not match either list.

BLUEBAR

The blue **URL** bar (called the Bluebar in Psiphon lingo) is the form at the top of your Psiphon node browser window, which allows you to access blocked site by typing its URL inside.

See also **Psiphon node**

BLOCK

To block is to prevent access to an Internet resource, using any number of methods.

BOOKMARK

A bookmark is a placeholder within software that contains a reference to an external resource. In a browser, a bookmark is a reference to a Web page – by choosing the bookmark you can quickly load the Web site without needing to type in the full **URL**.

BRIDGE

See **Tor bridge**.

BRUTE-FORCE ATTACK

A brute force attack consists of trying every possible code, combination, or password until you find the right one. These are some of the most trivial hacking attacks.

CACHE

A cache is a part of an information-processing system used to store recently used or frequently used data to speed up repeated access to it. A Web cache holds copies of Web page files.

CENSOR

To censor is to prevent publication or retrieval of information, or take action, legal or otherwise, against publishers and readers.

CENSORWARE

Censorware is software used to **filter** or **block** access to the Internet. This term is most often used to refer to Internet filtering or blocking software installed on the client machine (the PC which is used to access the Internet). Most such client-side censorware is used for parental control purposes.

Sometimes the term censorware is also used to refer to software used for the same purpose installed on a network server or **router**.

CGI (Common Gateway Interface)

CGI is a common standard used to let programs on a Web server run as Web applications. Many Web-based proxies use CGI and thus are also called "CGI proxies". (One popular CGI proxy application written by James Marshall using the Perl programming language is called CGIProxy.)

CHAT

Chat, also called **instant messaging**, is a common method of communication among two or more people in which each line typed by a participant in a session is echoed to all of the others. There are numerous chat protocols, including those created by specific companies (AOL, Yahoo!, Microsoft, Google, and others) and publicly defined protocols. Some chat client software uses only one of these protocols, while others use a range of popular protocols.

CIPHER

In cryptography, a **cipher** (or **cypher**) is an algorithm for performing encryption or decryption

CIRCUMVENTION

Circumvention is publishing or accessing content in spite of attempts at censorship.

COMMON GATEWAY INTERFACE

See CGI.

COMMAND-LINE INTERFACE

A method of controlling the execution of software using commands entered on a keyboard, such as a Unix shell or the Windows command line.

COOKIE

A cookie is a text string sent by a Web server to the user's browser to store on the user's computer, containing information needed to maintain continuity in sessions across multiple Web pages, or across multiple sessions. Some Web sites cannot be used without accepting and storing a cookie. Some people consider this an invasion of privacy or a security risk.

COUNTRY CODE TOP-LEVEL DOMAIN (CCTLD)

Each country has a two-letter country code, and a TLD (**top-level domain**) based on it, such as .ca for Canada; this domain is called a country code top-level domain. Each such ccTLD has a DNS server that lists all second-level domains within the TLD. The Internet root servers point to all TLDs, and cache frequently-used information on lower-level domains.

CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

DARPA (DEFENSE ADVANCED PROJECTS RESEARCH AGENCY)

DARPA is the successor to ARPA, which funded the Internet and its predecessor, the ARPAnet.

DECRYPTION

Decryption is recovering plain text or other messages from encrypted data with the use of a key.

See also **encryption**.

DISK ENCRYPTION

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. **Disk encryption** uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

DOMAIN

A domain can be a **Top-Level Domain** (TLD) or secondary domain on the Internet.

See also **Top-Level Domain**, **country code Top-Level Domain** and **secondary domain**.

DNS (Domain Name System)

The Domain Name System (DNS) converts domain names, made up of easy-to-remember combinations of letters, to IP addresses, which are hard-to-remember strings of numbers. Every computer on the Internet has a unique address (a little bit like an area code+telephone number).

DNS leak

A DNS leak occurs when a computer configured to use a **proxy** for its Internet connection nonetheless makes DNS queries without using the proxy, thus exposing the user's attempts to connect with blocked sites. Some Web browsers have configuration options to force the use of the proxy.

DNS server

A DNS server, or name server, is a server that provides the look-up function of the Domain Name System. It does this either by accessing an existing cached record of the IP address of a specific **domain**, or by sending a request for information to another name server.

DNS tunnel

A DNS tunnel is a way to **tunnel** almost everything over DNS/Nameservers.

Because you "abuse" the DNS system for an unintended purpose, it only allows a very slow connection of about 3 kb/s which is even less than the speed of an analog modem. That is not enough for YouTube or **file sharing**, but should be sufficient for instant messengers like ICQ or MSN Messenger and also for plain text e-mail.

On the connection you want to use a DNS tunnel, you only need port 53 to be open; therefore it even works on many commercial Wi-Fi providers without the need to pay.

The main problem is that there are no public modified nameservers that you can use. You have to set up your own. You need a server with a permanent connection to the Internet running Linux. There you can install the free software OzymanDNS and in combination with SSH and a proxy like Squid you can use the tunnel. More Information on this on http://www.dnstunnel.de.

EAVESDROPPING

Eavesdropping is listening to voice traffic or reading or filtering data traffic on a telephone line or digital data connection, usually to detect or prevent illegal or unwanted activities or to control or monitor what people are talking about.

E-MAIL

E-mail, short for electronic mail, is a method to send and receive messages over the Internet. It is possible to use a Web mail service or to send e-mails with the SMTP protocol and receive them with the POP3 protocol by using an e-mail client such as Outlook Express or Thunderbird. It is comparatively rare for a government to block e-mail, but e-mail surveillance is common. If e-mail is not encrypted, it could be read easily by a network operator or government.

EMBEDDED SCRIPT

An embedded script is a piece of software code.

ENCRYPTION

Encryption is any method for recoding and scrambling data or transforming it mathematically to make it unreadable to a third party who doesn't know the secret key to decrypt it. It is possible to encrypt data on your local hard drive using software like TrueCrypt (http://www.truecrypt.org) or to encrypt Internet traffic with **TLS/SSL** or SSH.

See also **decryption**.

EXIT NODE

An exit node is a Tor node that forwards data outside the Tor network.

See also **middleman node**.

FILE SHARING

File sharing refers to any computer system where multiple people can use the same information, but often refers to making music, films or other materials available to others free of charge over the Internet.

FILE SPREADING ENGINE

A file spreading engine is a Web site a publisher can use to get around censorship. A user only has to upload a file to publish once and the file spreading engine uploads that file to some set of sharehosting services (like Rapidshare or Megaupload).

FILTER

To filter is to search in various ways for specific data patterns to **block** or permit communications.

FIREFOX

Firefox is the most popular free and open source Web browser, developed by the Mozilla Foundation.

FORUM

On a Web site, a forum is a place for discussion, where users can post messages and comment on previously posted messages. It is distinguished from a mailing list or a **Usenet** newsgroup by the persistence of the pages containing the message threads. Newsgroup and mailing list archives, in contrast, typically display messages one per page, with navigation pages listing only the headers of the messages in a thread.

FRAME

A frame is a portion of a Web page with its own separate **URL**. For example, frames are frequently used to place a static menu next to a scrolling text window.

FTP (File Transfer Protocol)

The FTP **protocol** is used for file transfers. Many people use it mostly for downloads; it can also be used to upload Web pages and scripts to some Web servers. It normally uses ports 20 and 21, which are sometimes blocked. Some FTP servers listen to an uncommon port, which can evade port-based blocking.

A popular free and open source FTP client for Windows and Mac OS is FileZilla. There are also some Web-based FTP clients that you can use with a normal Web browser like Firefox.

FULL DISK ENCRYPTION

see **disk encryption**.

GATEWAY

A gateway is a **node** connecting two networks on the Internet. An important example is a national gateway that requires all incoming or outgoing traffic to go through it.

GNU Privacy Guard

GNU Privacy Guard (**GnuPG** or **GPG**) is a GPL Licensed alternative to the PGP suite of cryptographic software. GnuPG is compliant with RFC 4880, which is the current IETF standards track specification of OpenPGP.

see also **Pretty Good Privacy** (**PGP**).

GPG

see **GNU Privacy Guard.**

HONEYPOT

A honeypot is a site that pretends to offer a service in order to entice potential users to use it, and to capture information about them or their activities.

HOP

A hop is a link in a chain of **packet** transfers from one computer to another, or any computer along the route. The number of hops between computers can give a rough measure of the delay (**latency**) in communications between them. Each individual hop is also an entity that has the ability to eavesdrop on, block, or tamper with communications.

HTTP (Hypertext Transfer Protocol)

HTTP is the fundamental **protocol** of the World Wide Web, providing methods for requesting and serving Web pages, querying and generating answers to queries, and accessing a wide range of services.

HTTPS (Secure HTTP)

Secure HTTP is a **protocol** for secure communication using **encrypted** HTTP messages. Messages between client and server are encrypted in both directions, using keys generated when the connection is requested and exchanged securely. Source and destination IP addresses are in the headers of every **packet**, so HTTPS cannot hide the fact of the communication, just the contents of the data transmitted and received.

IANA (Internet Assigned Numbers Authority)

IANA is the organization responsible for technical work in managing the infrastructure of the Internet, including assigning blocks of IP addresses for **top-level domains** and licensing domain registrars for ccTLDs and for the generic TLDs, running the root name servers of the Internet, and other duties.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is a corporation created by the US Department of Commerce to manage the highest levels of the Internet. Its technical work is performed by IANA.

Instant Messaging (IM)

Instant messaging is either certain proprietary forms of chat using proprietary protocols, or chat in general. Common instant messaging clients include MSN Messenger, ICQ, AIM or Yahoo! Messenger.

intermediary

See **man in the middle**.

Internet

The Internet is a network of networks interconnected using TCP/IP and other communication **protocols**.

IP (Internet Protocol) Address

An IP address is a number identifying a particular computer on the Internet. In the previous version 4 of the Internet Protocol an IP address consisted of four bytes (32 bits), often represented as four integers in the range 0-255 separated by dots, such as 74.54.30.85. In IPv6, which the Net is currently switching to, an IP address is four times longer, and consists of 16 bytes (128 bits). It can be written as 8 groups of 4 hex digits separated by colons, such as `2001:0db8:85a3:0000:0000:8a2e:0370:7334.`

IRC (Internet relay chat)

IRC is a more than 20-year-old Internet **protocol** used for real-time text conversations (chat or **instant messaging**). There exist several IRC networks -- the largest have more than 50 000 users.

ISP (Internet Service Provider)

An ISP (Internet service provider) is a business or organization that provides access to the Internet for its customers.

JavaScript

JavaScript is a scripting language, commonly used in Web pages to provide interactive functions.

KeePass, KeePassX

KeePass and KeePassX are types of **Password Manager**.

KEYCHAIN SOFTWARE

see **Password Manager**.

KEYWORD FILTER

A keyword filter scans all Internet traffic going through a server for forbidden words or terms to **block**.

LATENCY

Latency is a measure of time delay experienced in a system, here in a computer network. It is measured by the time between the *start* of **packet** *transmission* to the *start* of packet *reception*, between one network end (e.g. you) to the other end (e.g. the Web server). One very powerful way of Web filtering is maintaining a very high latency, which makes lots of **circumvention** tools very difficult to use.

LOG FILE

A log file is a file that records a sequence of messages from a software process, which can be an application or a component of the operating system. For example, Web servers or proxies may keep log files containing records about which IP addresses used these services when and what pages were accessed.

LOW-BANDWIDTH FILTER

A low-bandwidth filter is a Web service that removes extraneous elements such as advertising and images from a Web page and otherwise compresses it, making page download much quicker.

MALWARE

Malware is a general term for malicious software, including viruses, that may be installed or executed without your knowledge. Malware may take control of your computer for purposes such as sending spam. (Malware is also sometimes called badware.)

MAN IN THE MIDDLE

A man in the middle or man-in-the-middle is a person or computer capturing traffic on a communication channel, especially to selectively change or **block** content in a way that undermines cryptographic security. Generally the man-in-the-middle attack involves impersonating a Web site, service, or individual in order to record or alter communications. Governments can run man-in-the-middle attacks at country **gateways** where all traffic entering or leaving the country must pass.

MIDDLEMAN NODE

A middleman node is a **Tor node** that is not an **exit node**. Running a middleman node can be safer than running an exit node because a middleman node will not show up in third parties' log files. (A middleman node is sometimes called a non-exit node.)

MONITOR

To monitor is to check a data stream continuously for unwanted activity.

NETWORK ADDRESS TRANSLATION (NAT)

NAT is a **router** function for hiding an address space by remapping. All traffic going out from the router then uses the router's IP address, and the router knows how to route incoming traffic to the requestor. NAT is frequently implemented by firewalls. Because incoming connections are normally forbidden by NAT, NAT makes it difficult to offer a service to the general public, such as a Web site or public proxy. On a network where NAT is in use, offering such a service requires some kind of firewall configuration or NAT traversal method.

NETWORK OPERATOR

A network operator is a person or organization who runs or controls a network and thus is in a position to **monitor**, **block**, or alter communications passing through that network.

NODE

A node is an active device on a network. A **router** is an example of a node. In the Psiphon and Tor networks, a server is referred to as a node.

NON-EXIT NODE

See **middleman node**.

OBFUSCATION

Obfuscation means obscuring text using easily-understood and easily-reversed transformation techniques that will withstand casual inspection but not cryptanalysis, or making minor changes in text strings to prevent simple matches. **Web proxies** often use obfuscation to hide certain names and addresses from simple text filters that might be fooled by the obfuscation. As another example, any **domain** name can optionally contain a final dot, as in "somewhere.com.", but some filters might search only for "somewhere.com" (without the final dot).

OPEN NODE

An open node is a specific **Psiphon node** which can be used without logging in. It automatically loads a particular homepage, and presents itself in a particular language, but can then be used to browse elsewhere.

See also **Psiphon node**.

OTR/Off-the-Record messaging

Off-the-Record Messaging, commonly referred to as **OTR**, is a cryptographic protocol that provides strong encryption for instant messaging conversations.

PACKET

A packet is a data structure defined by a communication **protocol** to contain specific information in specific forms, together with arbitrary data to be communicated from one point to another. Messages are broken into pieces that will fit in a packet for transmission, and reassembled at the other end of the link.

PASSWORD MANAGER

A **password manager** is software that helps a user organize passwords and PIN codes. The software typically has a local database or a file that holds the encrypted password data for secure logon onto computers, networks, web sites and application data files. KeePass http://keepass.info/ is an example of a password manager.

PASTEBIN

A web service where any kind of text can be dumped and read without registration. All text will be visible publicly.

PEER-TO-PEER

A peer-to-peer (or P2P) network is a computer network between equal peers. Unlike client-server networks there is no central server and so the traffic is distributed only among the clients.This technology is mostly applied to **file sharing** programs like **BitTorrent**, eMule and Gnutella. But also the very old **Usenet** technology or the **VoIP** program Skype can be categorized as peer-to-peer systems.

See also **file sharing**.

PERFECT FORWARD SECRECY

In an authenticated key-agreement protocol that uses public key cryptography, **perfect forward secrecy** (or **PFS**) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

Pretty Good Privacy (PGP)

Pretty Good Privacy (**PGP**) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

PHP

PHP is a scripting language designed to create dynamic Web sites and web applications. It is installed on a Web server. For example, the popular **Web proxy** PHProxy uses this technology.

PLAIN TEXT

Plain text is unformatted text consisting of a sequence of character codes, as in ASCII plain text or Unicode plain text.

PLAINTEXT

Plaintext is unencrypted text, or decrypted text.

See also **encryption**, **TLS/SSL**, **SSH**.

PRIVACY

Protection of personal privacy means preventing disclosure of personal information without the permission of the person concerned. In the context of **circumvention**, it means preventing observers from finding out that a person has sought or received information that has been **blocked** or is illegal in the country where that person is at the time.

PRIVATE KEY

see **public key encryption/public-key cryptography.**

POP3

Post Office Protocol version 3 is used to receive mail from a server, by default on port 110 with an e-mail program such as Outlook Express or Thunderbird.

PORT

A hardware port on a computer is a physical connector for a specific purpose, using a particular hardware **protocol**. Examples are a VGA display port or a USB connector.

Software ports also connect computers and other devices over networks using various protocols, but they exist in software only as numbers. Ports are somewhat like numbered doors into different rooms, each for a special service on a server or PC. They are identified by numbers from 0 to 65535.

PROTOCOL

A formal definition of a method of communication, and the form of data to be transmitted to accomplish it. Also, the purpose of such a method of communication. For example, Internet Protocol (IP) for transmitting data **packets** on the Internet, or Hypertext Transfer Protocol for interactions on the World Wide Web.

PROXY SERVER

A proxy server is a server, a computer system or an application program which acts as a **gateway** between a client and a Web server. A client connects to the proxy server to request a Web page from a different server. Then the proxy server accesses the resource by connecting to the specified server, and returns the information to the requesting site. Proxy servers can serve many different purposes, including restricting Web access or helping users route around obstacles.

PSIPHON NODE

A Psiphon node is a secured **web proxy** designed to evade Internet censorship. It is developed by Psiphon inc. Psiphon nodes can be open or private.

PRIVATE NODE

A private node is a **Psiphon node** working with authentication, which means that you have to register before you can use it. Once registered, you will be able to send invitations to your friends and relatives to use this specific node.

See also **Psiphon node**.

PUBLIC KEY

see **public key encryption/public-key cryptography.**

PUBLIC KEY ENCRYPTION/PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

Public-key cryptography uses asymmetric key algorithms (such as RSA), and can also be referred to by the more generic term "asymmetric key cryptography."

PUBLICLY ROUTABLE IP ADDRESS

Publicly routable IP addresses (sometimes called public IP addresses) are those reachable in the normal way on the Internet, through a chain of **routers**. Some IP addresses are private, such as the 192.168.x.x block, and many are unassigned.

REGULAR EXPRESSION

A regular expression (also called a regexp or RE) is a text pattern that specifies a set of text strings in a particular regular expression implementation such as the UNIX grep utility. A text string "matches" a regular expression if the string conforms to the pattern, as defined by the regular expression syntax. In each RE syntax, some characters have special meanings, to allow one pattern to match multiple other strings. For example, the regular expression `lo+se` matches `lose, loose,` and `looose.`

REMAILER

An anonymous remailer is a service which allows users to send **e-mails** anonymously. The remailer receives messages via e-mail and forwards them to their intended recipient after removing information that would identify the original sender. Some also provide an anonymous return address that can be used to reply to the original sender without disclosing her identity. Well-known Remailer services include Cypherpunk, Mixmaster and Nym.

ROUTER

A router is a computer that determines the route for forwarding **packets**. It uses address information in the packet header and cached information on the server to match address numbers with hardware connections.

ROOT NAME SERVER

A root name server or root server is any of thirteen server clusters run by **IANA** to direct traffic to all of the **TLD**s, as the core of the **DNS** system.

RSS (Real Simple Syndication)

RSS is a method and protocol for allowing Internet users to subscribe to content from a Web page, and receive updates as soon as they are posted.

SCHEME

On the Web, a scheme is a mapping from a name to a **protocol**. Thus the HTTP scheme maps **URL**s that begin with HTTP: to the Hypertext Transfer Protocol. The protocol determines the interpretation of the rest of the URL, so that http://www.example.com/dir/content.html identifies a Web site and a specific file in a specific directory, and mailto:user@somewhere.com is an **e-mail** address of a specific person or group at a specific **domain**.

SHELL

A UNIX **shell** is the traditional **command line** user interface for the UNIX/Linux operating systems. The most common shells are sh and **bash**.

SOCKS

A **SOCKS** proxy is a special kind of **proxy server**. In the ISO/OSI model it operates between the application layer and the transport layer. The standard **port** for SOCKS proxies is 1080, but they can also run on different ports. Many programs support a connection through a SOCKS proxy. If not you can install a SOCKS client like FreeCap, ProxyCap or SocksCap which can force programs to run through the Socks proxy using dynamic port forwarding. It is also possible to use **SSH** tools such as OpenSSH as a SOCKS proxy server.

SCREENLOGGER

A screenlogger is software able to record everything your computer displays on the screen. The main feature of a screenlogger is to capture the screen and log it into files to view at any time in the future. Screen loggers can be used as powerful **monitoring** tool. You should be aware of any screen logger running on any computer you are using, anytime.

SCRIPT

A script is a program, usually written in an interpreted, non-compiled language such as JavaScript, Java, or a command interpreter language such as bash. Many Web pages include scripts to manage user interaction with a Web page, so that the server does not have to send a new page for each change.

SMARTPHONE

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone, such as Web access, ability to run elaborated operating systems and run built-in applications.

SPAM

Spam is messages that overwhelm a communications channel used by people, most notably commercial advertising sent to large numbers of individuals or discussion groups. Most spam advertises products or services that are illegal in one or more ways, almost always including fraud. Content **filtering** of **e-mail** to **block** spam, with the permission of the recipient, is almost universally approved of.

SSH (Secure Shell)

SSH or Secure Shell is a network protocol that allows **encrypted** communication between computers. It was invented as a successor of the unencrypted Telnet **protocol** and is also used to access a **shell** on a remote server.

The standard SSH **port** is 22. It can be used to bypass Internet censorship with port forwarding or it can be used to **tunnel** other programs like VNC.

SSL (Secure Sockets Layer)

SSL (or Secure Sockets Layer), is one of several cryptographic standards used to make Internet transactions secure. It is was used as the basis for the creation of the related Transport Layer Security (**TLS**). You can easily see if you are using **SSL** by looking at the **URL** in your Browser (like Firefox or Internet Explorer): If it starts with https instead of http, your connection is **encrypted**.

STEGANOGRAPHY

Steganography, from the Greek for *hidden writing*, refers to a variety of methods of sending hidden messages where not only the content of the message is hidden but the very fact that something covert is being sent is also concealed. Usually this is done by concealing something within something else, like a picture or a text about something innocent or completely unrelated. Unlike cryptography, where it is clear that a secret message is being transmitted, steganography does not attract attention to the fact that someone is trying to conceal or **encrypt** a message.

SUBDOMAIN

A subdomain is part of a larger **domain**. If for example "wikipedia.org" is the domain for the Wikipedia, "en.wikipedia.org" is the subdomain for the English version of the Wikipedia.

THREAT ANALYSIS

A security threat analysis is properly a detailed, formal study of all known ways of attacking the security of servers or **protocols**, or of methods for using them for a particular purpose such as **circumvention**. Threats can be technical, such as code-breaking or exploiting software bugs, or social, such as stealing passwords or bribing someone who has special knowledge. Few companies or individuals have the knowledge and skill to do a comprehensive threat analysis, but everybody involved in circumvention has to make some estimate of the issues.

Top-Level Domain (TLD)

In Internet names, the TLD is the last component of the **domain** name. There are several generic TLDs, most notably .com, .org, .edu, .net, .gov, .mil, .int, and one two-letter country code (**ccTLD**) for each country in the system, such as .ca for Canada. The European Union also has the two-letter code .eu.

TLS (Transport Layer Security)

TLS or Transport Layer Security is a cryptographic standard based on **SSL**, used to make Internet transactions secure.

TCP/IP (Transmission Control Protocol over Internet Protocol)

TCP and IP are the fundamental **protocols** of the Internet, handling **packet** transmission and routing. There are a few alternative protocols that are used at this level of Internet structure, such as **UDP**.

Tor bridge

A bridge is a middleman Tor **node** that is not listed in the main public Tor directory, and so is possibly useful in countries where the public relays are **blocked**. Unlike the case of **exit nodes**, IP addresses of bridge nodes never appear in server log files and never pass through monitoring nodes in a way that can be connected with **circumvention**.

TRAFFIC ANALYSIS

Traffic analysis is statistical analysis of **encrypted** communications. In some circumstances traffic analysis can reveal information about the people communicating and the information being communicated.

TUNNEL

A tunnel is an alternate route from one computer to another, usually including a **protocol** that specifies **encryption** of messages.

UDP (User Datagram Packet)

UDP is an alternate **protocol** used with IP. Most Internet services can be accessed using either **TCP** or UDP, but there are some that are defined to use only one of these alternatives. UDP is especially useful for real-time multimedia applications like Internet phone calls (**VoIP**).

URL (Uniform Resource Locator)

The URL (Uniform Resource Locator) is the address of a Web site. For example, the URL for the World News section of the NY Times is http://www.nytimes.com/pages/world/index.html. Many censoring systems can **block** a single URL. Sometimes an easy way to bypass the block is to obscure the URL. It is for example possible to add a dot after the site name, so the URL http://en.cship.org/wiki/URL becomes http://en.cship.org./wiki/URL. If you are lucky with this little trick you can access blocked Web sites.

Usenet

Usenet is a more than 20-year-old discussion forum system accessed using the NNTP **protocol**. The messages are not stored on one server but on many servers which distribute their content constantly. Because of that it is impossible to censor Usenet as a whole, however *access* to Usenet can and is often **blocked**, and any particular server is likely to carry only a subset of locally-acceptable Usenet newsgroups. Google archives the entire available history of Usenet messages for searching.

VoIP (Voice over Internet Protocol)

VoIP refers to any of several **protocols** for real-time two-way voice communication on the Internet, which is usually much less expensive than calling over telephone company voice networks. It is not subject to the kinds of wiretapping practiced on telephone networks, but can be monitored using digital technology. Many companies produce software and equipment to **eavesdrop** on VoIP calls; securely **encrypted** VoIP technologies have only recently begun to emerge.

VPN (VIRTUAL PRIVATE NETWORK)

A VPN (virtual private network) is a private communication network used by many companies and organizations to connect securely over a public network. Usually on the Internet it is **encrypted** and so nobody except the endpoints of the communication can look at the data traffic. There are various standards like IPSec, **SSL** and **TLS**. The use of a VPN provider is a very fast, secure and convenient method to bypass Internet censorship with little risks but it generally costs money every month.Further, note that the VPN standard PPTP is no longer considered secure, and should be avoided.

WHITELIST

A whitelist is a list of sites specifically authorized for a particular form of communication. Filtering traffic can be done either by a whitelist (**block** everything but the sites on the list), a **blacklist** (allow everything but the sites on the list), a combination of the two, or by other policies based on specific rules and conditions.

WORLD WIDE WEB (WWW)

The World Wide Web is the network of hyperlinked **domains** and content pages accessible using the Hypertext Transfer Protocol and its numerous extensions. The World Wide Web is the most famous part of the Internet.

WEBMAIL

Webmail is **e-mail** service through a Web site. The service sends and receives mail messages for users in the usual way, but provides a Web interface for reading and managing messages, as an alternative to running a mail client such as Outlook Express or Thunderbird on the user's computer. For example a popular and free webmail service is https://mail.google.com/

Web proxy

A Web proxy is a script running on a Web server which acts as a **proxy/gateway**. Users can access such a Web proxy with their normal Web browser (like Firefox) and enter any **URL** in the form located on that Web site. Then the Web proxy program on the server receives that Web content and displays it to the user. This way the **ISP** only sees a connection to the server with the Web proxy since there is no direct connection.

WHOIS

WHOIS (who is) is the aptly named Internet function that allows one to query remote WHOIS databases for **domain** registration information. By performing a simple WHOIS search you can discover when and by whom a domain was registered, contact information, and more.

A WHOIS search can also reveal the name or network mapped to a numerical IP address