Security Issues and Resolutions

Andy Pepperdine

The first part of this paper is about the types of threat to your data and PC. The second part is about what you have to protect and why. The final part describes the steps you can take to ward off these threats.

In all matters of security, there is one essential question: Do you trust the other side of the transaction? It is ALL about TRUST.

But do not go overboard. Locking things up means using keys to open it every time, and that can be a pain. So think before you put your data in a safe, and protect only what you really have to (or you are paranoid about). But if it is worth protecting, do not skimp on the technique, nor just hope for the best.

There are two other important questions to ask: What will happen if I mislaid the key and lost the contents of the box? What will happen if someone else obtained the key and used the contents of the box?

Types of threats

Problems of security can be classified in various ways, but for this paper, we will consider them to be divided into those which are external threats to your PC and it's local data, threats which can infiltrate themselves onto your machine, and threats which are purely external to your machine.

Sometimes you may hear the term "malware", which is software that is running where you do not want it and doing things you do not want to happen. They are like weeds, and like weeds the same program can be unwanted in one situation, but a valuable item in another.

External threats to your machine

This is the situation where your data is compromised by something else penetrating your defences without any action on your part. It is represented by malware known as "worms". You can think of them as burglars who come round checking whether you have left any doors or windows open, but will not do any damage if everything is locked up. Firewalls prevent this type of intrusion.

Infiltrated threats

This category consists of most malware. Some of it is given names that reflect the manner in which it is transferred to your machine, such as "virus" or "trojan".

They may arrive via e-mail, and the message may be disguised as one from a well-known correspondent, but who did not in fact send it.

Or they can arrive from a website when you visit a compromised site. Web pages deliver content to your PC. This is largely data, but more and more frequently, some script is also being downloaded to execute on your machine in order to present the page correctly. This is a dangerous hole in the security of the Internet and has been there ever since Javascript was invented. It is technically a bad idea, but there is no hope now of removing it. We will have to live with it.

Payloads

However malware gets onto your machine, it will carry a “payload”, which is the piece of software that will do the damage, whatever that is. The vector that distributed it is like the mosquito, the payload is like the disease, say malaria, that is conveyed by the mosquito.

Payloads are also categorised, and can go under the names of “keylogger”, “spyware”, unwanted “adware”, “rootkit” or a number of other names that appear from time to time.

Some of it is designed to damage you (e.g. steal your passwords, or address lists), and others are designed to use your machine to damage others (e.g. send out spam or attack a website). The latter type are particularly insidious as, if it is possible to track the harm to a website back to its source, it will be your machine that will be accused of doing the harm – not a desirable outcome on your part.

Execution

In order that any payload can do any damage at all, it must “execute” some code. That means that your PC will do what the payload requests. In order for this to happen, something must be started on your machine. If it is started with administrator permissions, then it has access to everything – all the data and could take advantage of all the features that you have installed. If, on the other hand, it starts under the permissions granted to a lesser account, then it will be restricted to only what that account can do. Typically, installation of software needs administrator permissions, so any request you see for the password for administration is a warning sign, and should be taken seriously.

What do you have to protect?

Your own data

When you think about your data, you will be surprised how much there is which must not be compromised. Imagine someone rummaging through your filing cabinet, your diary, your address book; and learning about your financial transactions, details of all your accounts, and about your life and work. That is what is exposed if a piece of malware gains entry to your PC. Less damage can be caused should a website be attacked, since all the information will relate to that site. Only the data between you and the site is affected, but that may be bad enough.

Are there any documents on your hard disk you really want to keep private, or at least control the release of? Think copyright on books, pictures, ideas, etc.

Passwords

Your passwords to web sites are essential to your access, and are worth every bit as much as various keys to equipment and rooms. Think what might happen if someone got into your Amazon account and ordered various books on your account; or worse, changed you password so you could not get in again. What about your banking arrangements?

When dealing with a web site, it is a matter of how much you trust the site to keep your details safe from interference. If you do not trust them, do not use them.

Another thing to consider is this: Do all your rooms use the same key? Different keys can allow separation of risks, so if a burglar gets into one room, he still cannot get to the others unless he works hard again to crack the next lock. In the same way, if one password is lost, can it be used

elsewhere? If it can, to what effect?

Finally, what sort of password should be used? How long should it be? What sort of characters should it contain?

E-mail

How do you really know the sender of an e-mail message is really who they say they are? Is this message really from my brother? How does my brother know a message I send is really from me? How much are you willing to invest to ensure that these questions have good answers? Is there any sensitive information in the messages themselves?

What should I do?

We will look at the various places that you have control over and how best to protect them.

Router

You have access to the Internet through some device called a modem or router. This section applies only to routers. Modems on their own typically have no independent protection as part of their operation.

A router allows messages to flow between the Internet and your PC. Nowadays these are computers in their own right, but are devoted to a specialised task. You want any transactions to take place that you initiate, but refuse all transactions that are initiated from outside. It is not sufficient to ban all incoming data, because you would then not be able to receive any web pages you asked for!

When a message starts to ask another site for an answer, it first “knocks on the door” at a specific place to ask for a suitable service. You need to prevent anyone answering the door, but you want to able to open the door yourself to go out and look for the postman.

The technical term for the door is a “port”.

This control is the function of a “firewall”. It sets up the rules that specify what sort of transactions are allowed, in other words, which doors are to be left unlocked.

Routers have firewalls, and the default settings for modern routers are almost certainly acceptable for a personal computer at home, in that they will by default suppress all incoming messages, but allow almost all outgoing messages. Somewhere in the administration of the router you will find the tables which identify which ports can be opened by whom – that is where you want to go if you do need to change the settings.

Your desktop PC

If your PC always sits behind a router and never strays onto another network, then you will not need a firewall, except in unusual circumstances, like a break-in by a piece of malware you are trying to eradicate. Different systems have different types of firewalls, but the same rules apply as for routers, except when you have your own internal network.

Laptops and Netbooks

Laptops and other portable devices are intended to be connected to any network that is suitable. You

will then not have control over the administration of the network you are connecting to. In this case, it is essential you have your own firewall in the device. Do not rely on the other guy getting it right for you. Systems these days all come with a firewall. Learn how to access it and check the settings.

If you take a laptop away, then consider what would happen if you left it somewhere. Any data that does not need a password to get to is at risk. If there is any danger at all that it might be lost, then consider encrypting the file system containing your data. Or at least protect any sensitive information via passwords on the individual files.

Even if you have a password on your log in on the laptop, it will not prevent someone else who has the machine from reading the hard drive in some other way. It is not necessary to log on to read a file. You cannot rely on log in passwords to protect your files.

Internal networks

If you have no internal network, and you have a router, you will not need to set up a firewall on your PC. The router will have one for you.

If you do not have a router, then you should ensure your PC has a firewall as it has no extra line of defence facing the Internet.

Even if you have a router, if you have a network with more than one machine on it, then it may be advisable to set firewalls on each and every machine. This is especially true if you are in the habit of allowing others to plug into your broadband (e.g. via your wifi) – you cannot control what they might bring in. Malware on your internal network is bad news, especially worms which can spread themselves from one machine to another along the internal network.

There are various reasons why you may have an internal network. You may be sharing files between computers, you may have a printer on a computer you want to allow others to access, you may have a printer which is attached directly to the network. In these cases, each device has to allow access to the services it provides. In our analogy, which doors should be left unlocked. Computer B cannot access files on computer A, unless A lets it happen and listens on the appropriate port. The firewall has to be set up so it will accept incoming messages on that port.

These days, the rules are normally relaxed automatically when the sharing process is set up. If things do not seem to work, it is one area where there may be a problem – the firewall may be blocking the service that you should allow.

A special word is in order about self-contained devices, like printers, stuck on the local network. If you ever do get a worm on your network, in theory it could affect your printer while it is turned on. The first thing to do when clearing the worm out is to turn off the printer and leave it off until you are sure you are clean. If you have any doubts about the printer, then do a factory reset on it and re-configure it from the beginning. Your printer documentation will help. Of course any other device attached to your network should be treated the same way, including any data stores.

E-mail

To prevent the ingress of nasty elements via your e-mail client, you can ensure you have up to date anti-virus software. These days, almost all ISPs that deliver e-mail to you have already scanned the e-mail to remove the malware they know about, which helps enormously. But some may still get through.

However, anti-virus programs work only after the fact. If they detect something, it is like taking

antibiotics when you are ill. It is much better to get inoculated before you enter anywhere that might infect you. Nothing is perfect here, but there are some pointers.

Throw out Outlook Express. It has got better recently, but only as a result of pressure from email clients that have taken sensible defaults, like Thunderbird – but there are others. These will not execute anything automatically on receipt of a message. That way you at least have a chance of checking the content before allowing it to go ahead and display.

You can turn off the interpretation of HTML in messages. HTML was always an atrocious idea for email, but also is here to stay. It's another gaping security hole because of the ability to execute code you did not know about. A lot of messages nowadays come in both HTML and plain text, and you can then get the chance whether to look at the pretty pictures, or not. The vast majority of messages do not need pictures.

If you have anti-virus software, then let it do a scan of the whole disk regularly. One a week is probably fine, but make your own decisions about the reliability of your working practices.

Signing e-mail

It is possible to digitally sign your e-mail messages. If everyone did this, you would know immediately and accurately who actually sent each message and spam would vanish. It will take some work on your part to understand how to do this as the security brotherhood has not made it easy to do and have complicated it unnecessarily for the ordinary (wo)man in the street. We do not need the paranoid complexity inherent in the theoretical situations they cover, but enough can be done by simply creating your own public and private key pair and signing every message you send. The more people who do this, the easier it will get for everyone, and the easier to use the system will become.

I would warn against using a certificate system for signatures, as it is introduces another third party, and that is always bad for security no matter who they are.

E-mail content

When writing an e-mail message, always remember that it is like sending a postcard. The postman can read it, and if there is a bent postman, then your content could be misused. Never put anything unencrypted in a message that you need to keep safe.

The easiest way to encrypt a message in fact is to write it in a word processor like MS Word, or OpenOffice Writer, which will allow it to be saved with a password. This is then sent as an attachment, and then phone your correspondent to tell them what the password is. pdf documents can also be protected with passwords, but some interfaces make it less than obvious how to do this. Look for a Security tab in the dialogs.

Websites & Browsing

When browsing the web, most browsers now give you the ability not to execute any scripts that are downloaded as part of the page. Some have this facility built-in (like IE9) and some via an add-on (like Firefox's – NoScript). You can then selectively turn on those sites you trust enough to send you scripts, either temporarily for the one visit, or permanently if you will re-visit frequently.

Another source of annoyance, and potentially malware, are advertisements attached to websites. Firefox has another add-on (AdBlock Plus) that can be used to suppress selected advertisement

sites. Fortunately, most of the annoying adverts come from relatively few independent sites and can be filtered out by this add-on.

When you use a website, especially for shopping, the site will drop onto your machine little bits of data called “cookies”. These are necessary for technical reasons to enable the dialogue with the site to take place. Some unpopular sites also use them to harass you each time you go back to the site. In addition, you cannot know whether there are other sites that will read those cookies and use the information for their own benefit, not your benefit. They are a minor security hole, but potentially a major annoyance.

You can avoid this by suppressing the saving of cookies from one invocation of the browser to the next, as most browsers have a way of deleting the cookies after the session. Look in the preferences, or options, for the appropriate option. Sometimes it is referred to as “private browsing” or some such term. Firefox also has an add-on (TACO) which will tell you more about cookies and enable you to save only those for sites you trust not to abuse their use of them.

If you use an Internet café or another person’s machine, you might also wish to remove the history the browser would keep, in order to preserve your own privacy. The same private browser options will normally allow you to delete the history after the session is complete.

Note that any options that take effect at the end of a session, will only do so when the browser is closed down normally. They will not be obeyed if you merely close the system down directly, or put a laptop into suspend or hibernate mode.

Browsers and Extensions

Some browsers have extensions or “add-ons” which will enhance their security features. These can be very valuable to aid in alerting you to problems, and keeping you as safe as pure technology could. The main issue with each add-on is whether it can be trusted to do what it says. The developers of the add-on presumably have done it for some purpose, which more often than not is honest and for their own use as well. There have been cases of add-ons being themselves a form of malware, but these are usually very quickly spotted and withdrawn. Add-ons from the official site of the browser are supported by the reputation of the browser, and can be considered safe. If you get them from elsewhere, then let the user beware.

In any case, recommendations from others is the best way to ensure that what you get is good and safe, and will not create more trouble.

Since I use Firefox, I will give a summary of which ones I’ve installed and why.

To see what you have already installed on Firefox, go to Tools → Add-ons and then hit the Extensions icon. You will then see the list of what is installed with your version of Firefox. To get more hit the Get Add-ons icon and put a suitable keyword into the search box. Installation has been straightforward for all those I’ve ever used.

NoScript

This add-on suppresses all scripts from executing for websites by default. In this mode you cannot suffer from any of the malware a website might send you since it cannot be installed.

However, there are plenty of websites that need you to execute a script in order to perform the functions you want. In these cases, NoScript gives you the ability to enable script execution for the site either temporarily (for this occasion only) or permanently (when it will remember the site from

session to session). Of course, you can always revert the options whenever you wish.

A side-effect of this is that a lot of sites become faster to load because they are not fetching adverts, and other detritus, from sundry other places.

Adblock Plus

Advertisers often use one of a small number of sites that deliver advertisements to your screen. Adblock Plus will suppress all these sites and not allow the browser to fetch from them.

This primarily helps you to concentrate on the content of the website you are trying to read rather than the adverts that get in the way, but it is also safer in that you are access fewer sites which could lead to malware. Advertisers only want to sell, security of their site is not of paramount importance to them, and all those adverts in one place make the sites honeypots attracting the malware brigade to try to crack them open to install their own nefarious scripts.

When you install this, you will be offered a choice of lists of banned sites. Which one suits will depend on the type of browsing you do. Try them until you find one that gives good results.

TACO with Abine

There are a few varieties of TACO, and I use one of them. These will keep your cookies under control. It allows you to record sites that you wish to keep cookies from between sessions, and will delete cookies from all the others sites.

Certificate Patrol

This add-on records the certificates in use by sites that you visit via https, the secure version of browsing. If these certificates change, it means that the site has changed its identification. There are several valid reasons why this may happen, but there is also the possibility that the change is not planned. If it changes unexpectedly, it may presage a man-in-the-middle attack on your details.

The certificates are issued and held by third party companies, and their servers are prime targets for anyone interested in cracking log-ins at other sites. Around 15 March 2011 there was a break-in into Comodo which compromised a number of certificates. Fortunately, this was identified and fixed quickly, and Comodo are to be commended for being open with the browser suppliers to help their rapid fixes to be done. The Certificate Patrol Firefox add-on would have given warnings in exactly this case and alerted you to the danger.

ShowIP

This is a simple add-on that displays on the status bar at the bottom the actual IP address that you are visiting, by numerical address, not by readable name. It is not especially useful for security purposes while browsing, although it would enable you to check that a site is where you think it is after any issues are brought to your attention. By comparing against a where-is service you can gain confidence in whether it is what it claims.

Plug-ins

Plug-ins are also additional things added to your browser to help it perform certain functions for you. They are very similar to extensions, but are concerned with the interpretation of websites, like codecs to enable you to view videos or listen to sound tracks. Most of these are produced by

proprietary organisations, like Sun, now Oracle, (for Java), Adobe (for Flash and pdf readers) etc. Which you will need will depend on what sites you refer to. I would say that they can be trusted in so far as they will not introduce malware, but they may have unfortunate side-effects that will become apparent in the news and among friends by word of mouth. One recent discovery was that Adobe Flash plug-in dumped cookies on your machine in places that were not normally cleared out after you've finished. This was found by others, who then started to keep their own cookies in that hidden location, too. We always have to keep an eye on this sort of antisocial behaviour and guard against as best we can.

Free software can now replace some of these proprietary plug-ins in Firefox and they will usually not have these drawbacks.

User accounts, logging in and screen savers

Since the dangers from malware can occur only when something has to execute, and will be constrained by the permissions it has, it is always safer to do anything while logged into a "normal" user account. It is always a bad move to browse the web when logged in as Administrator, or root, or some other account with extensive abilities. It is always worthwhile creating a user account, and using that except when doing things like installing software, configuring devices, or managing a network. How strong a password you decide to use when logging in to each account depends on whether anyone else may get access to the machine. In any event, do not use the same password for all the accounts, and make the administrator password fairly strong and unique.

If you ever are requested for the administration password, make sure you understand why it asking. If you don't know, refuse it until you can check with someone else.

If you have a portable machine, then ask yourself whether it may ever be left unattended anywhere. If there is a chance of that, then make sure you know how to lock the screen before leaving it. At the least, let the screen saver lock it for you so it will automatically protect itself eventually. The same question applies to desk non-portable PCs whenever there is a possibility of inquisitive little fingers reaching the keyboard. If you are concerned, then also make sure you have to log in to an account when the machine is booted. Otherwise, anyone could re-boot into an account even if the screen was locked.

Passwords

Selecting a password is worth serious consideration; it is not something to be treated as an annoyance, and the same one to be used for everything, because then if one goes, then they all go, and it is easy to get into your account at a hundred websites, each wanting a password.

It is impossible to remember 100 different strong ones, but there are ways of keeping them on record so you can get to them, but others cannot. For example, you can keep all the information about each site (and also e-mail access details, ISP passwords, etc.) in a text document, either in OpenOffice (.odt format) or Microsoft Office (.doc format), but when you save it initially give it a password. It cannot then be accessed without that password. This means you will have one password which you make easier to remember, to keep all the others. This is like using one key to a keysafe, where you keep all the other keys. If you do decide to do this, **keep backups of the file in more than one place**. It is no use if the list is lost, so use memory sticks as well as the usual backups for your data.

Saving the file as a .pdf file also gives you the chance to set a password; it is harder to edit, but can

be read in more places, on more machines. This is a good format to use when carrying it around on attached to your physical keyring.

Firefox has the ability to save passwords in its own safe, and you have the ability to set your own master password to cover the safe. Chromium can save the passwords, too, but you cannot set a master password, which makes it unsuitable for use on laptops that are taken away. However, neither of these can save the passwords from some sites that use a specially crafted script to hide the login process – banks are especially prone to this sort of manipulation of the website protocols, but I've found only very few that are troublesome this way.

Password Strength

The strength of a password is akin to the difficulty of picking a lock. How important is the content of the place you are locking up?

These days, with the advent of very powerful machines that can sit on a desktop, and also the ability to create networks of machines, it is not good enough any more to use eight alphabetic / numeric characters. Strong passwords should now be at least 13 characters long and contain not only upper and lower case letter, numbers, but also some punctuation marks. Unfortunately, there are still some websites that do not allow punctuation characters, in which case, the passwords should probably be 15 characters long to be as safe as possible.

But temper that with the question: How important is my data to whoever may wish to take it? How hard will anyone try to crack your password? In most cases, I suggest that it is not going to be worth anyone's trouble to crack your web passwords if it takes serious effort. But it is still important to keep a decent lock on your data. Avoid the obvious things like names of friends or pets, or dates, or publicly known registration numbers, etc. See further information below for a generator of good passwords.

Data

Your own data may be precious, in which case it is worth considering encrypting the whole disk on which it is kept. However, the downside is that if you lose the password, you lose the lot. It can also make backups difficult and you may have to make special arrangements to save disk images, instead of just the files that have changed, etc. Remember, what is the point of encrypting the disk, if the backups are not encrypted too?

And talking of backups, there is no point in protecting your working data if a hardware failure could leave you without any at all, so a regime of frequent and regular backups is also essential.

If your data is kept at home on a desk machine, or server, then it will remain there unless the machine itself is removed, or someone takes a copy. How likely is that in your case? If you think it is a real risk, then encrypt your whole drive, or at least the whole directory where you keep all your stuff. Backups will also have to be encrypted for the same reason – just bear in mind what will happen when your descendants want to read it all. The same applies to a laptop that contains all the valuable data on it. (UK Government: please note!)

If, however, most of it is less important, then perhaps just encrypting the particular files is adequate. If you are taking the data elsewhere, think about how you will read it at the remote location. If you have your own laptop, you can supply your own decrypting software; but if you are taking it on a memory stick for use on another machine, then do they have the means to read what you have? In the latter case, protecting individual files like pdfs and odts and docs with their own passwords is a

good way to go, since the files are transferable to anywhere, and the application will request the unlocking password. You will not need file system control of the encryption.

Cloud data

“Cloud Computing” is getting more popular, and is certainly useful when travelling. All of the data is stored “on-line” and held by some other party for you, and all you need to do is access it via a username and password. For some hosts, you can encrypt the connection so that no one can intercept the transfer of the documents between the cloud and your own machine.

When selecting a host, the things you need to consider are:

1. How secure is the site where the data is stored?
2. Where is it stored, which country? Does that country have adequate data protection laws?
3. How frequent is the back-up of all your data?
4. What happens if the business is taken over, or goes bankrupt? Who owns the data stored there?
5. Is it kept in encrypted form? What technique is used, and who has access to the keys?
6. Is the transfer between the storage and my working machine encrypted?

But that is not all that you need to think about, you also have to consider the effect on your own data and how you can work with it. Some further questions:

1. If I lost access, like a server failing, could I continue? How long a break is supportable?
2. Can I still continue if I have to use an untrusted machine, like in an Internet Café?

So before you make a decision about using cloud computing, read the terms and conditions, and think how you will use it BEFORE taking the plunge.

My own opinion is that within two, maybe three, years, there will be readily available boxes where you can store all the stuff you want accessible from everywhere, but residing in your own home under your own control. The technology exists, it just needs putting together in a package that anyone can use easily.

Data longevity

Although this is not strictly a security matter, it is something you may wish to ponder when selecting the applications you will use to create your documents, and the format you save them in. If you want your descendants to have access, then they must be provided with any and all tools they need:

1. Have you made provision for that?
2. Have you updated your will?
3. Can they find the passwords?
4. Will they have programs that can read the data you have saved?

Wireless connections

Wireless connections, whether to your own local WAP (wireless access point) to access your

broadband line, or via a mobile phone connection, are necessarily open to anyone to listen in. If the data transmitted over such a link is not encrypted, then it could be intercepted and understood.

The only safe data over a wireless link when browsing, is when you are accessing a site via an https:// connection, when a padlock will appear somewhere on your browser's window. If you cannot access via https, then the link is not secure. More and more websites are moving to https, first optionally, and then obligatorily, and this security hole may eventually disappear. Meanwhile treat any wireless link circumspectly.

In any case, you should always protect your own wireless access point with a password to prevent any passer by from logging in to it and misusing bandwidth. These days, routers come set up with passwords already established and the documentation tells you what it is. The safest methods for home use are WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key) or WPA2-PSK. These use the password both to authenticate the access initially, and to generate keys for the encryption of the data as it is transmitted to prevent snooping in the aether. Only more recent devices will support WPA2, so if you start to use it, check that everything that you wish to connect can cope with it.

Applications

However hard software developers try, it is impossible not to have some bugs in a large piece of software. These bugs may be exploitable for malware purposes. However, that can only happen when the bug is found and an exploit created.

If there is a danger, the providers of the application will supply updates. These are always worth installing. It is important to keep abreast of what updates are available, so establish a routine whereby you will check for them regularly. On some systems, you can set them up so they will do this according to a time schedule you define, but make sure that the machine is switched on when the schedule comes round!

Occasionally an update fails, but that is a smaller risk usually than not updating. In any case, you should check what the update is for and what it will do, before accepting it. If in doubt ask someone or search on-line for others' opinions and experiences.

Finding out what has failed

While this topic is not strictly about safety and security, it may affect how well you recover from any hardware failures. Things can go wrong without you doing anything; hardware wears out; power units expire; disks crash; and any number of other things. It is important that you have the information and ability to distinguish what has failed so it can be replaced – repairing is often impractical these days.

When things start to behave differently, the first things that needs to be asked is: What was the last change made to the system? Then to ask: when was the change made relative to when the problem started to occur?

To aid this, it is immensely useful to keep a logbook for each machine separately in which you record all changes made to software – what was installed, how and when, including system and application updates; what hardware changes have been made to anything connected to the machine; anything else at all that might conceivably relate to the machine.

Such a logbook must be in the old-fashioned format of real paper with legible writing in it, with dates. It's no use if you cannot boot to say the logbook is held on the disk!

Conclusion

There appear to be a lot of things to think about, but they all come down to one basic rule: Ask yourself at all times: “Do I trust this site / software / application / hardware?” Find good sources of all the items you want and keep a check on their reputations. There is no substitute for integrity to form the basis of a good reputation.

Further information

There are some websites that can be used to generate random passwords of differing strengths. For example: http://www.mytsoftware.com/dailyproject/PassGen/PassGen.html

The Comodo certificate break-in is analysed at https://lwn.net/Articles/435214/

There are a number of utilities on the net to check out the ownership of sites. One such is http://www.whatismyip.com/tools/ip-whois-lookup.asp

Your own personal cloud at home is being worked on: http://freedomboxfoundation.org/