OVERVIEW GUIDE TO COMPUTER SECURITY

The issues of computer security cover a vast terrain. For a broad understanding, you can usefully divide these issues into two general categories:

1. Protecting data on your computer
2. Protecting data while in transit (Internet, Email, etc.)

This Guide will look at both these categories (Section 1 and Section 2, respectively), and will conclude by offering some useful links (Section 3).

Contents

Section 1: Protecting data stored on your hard drive

- 1.1. Locking down Windows
- 1.2. Avoiding Malware
- 1.3. Cleaning / Erasing
- 1.4. Encryption
- 1.5. Security Note on USB Drives and Wear-Leveling
- 1.6. Other Methods
  - 1.6.1. Live CDs
  - 1.6.2. Portable Applications
  - 1.6.3. System Drive Emulation software
  - 1.6.4. Virtual Machines

Section 2: Protecting data while in transit over networks (Internet, Email, etc).

- 2.1. Email
  - 2.1.1. PGP
- 2.2. Web-Surfing
  - 2.2.1. Free proxies
  - 2.2.2. Commercial software
  - 2.2.3. Tor
- 2.3. Other Network Usage (Chat, Anonymous Remailers, File-Sharing)

Section 3: Useful Links

SECTION 1: Protecting Data on Your Computer

1.1. Locking Down Windows

Windows at its default settings is an insecure operating system. Having been designed for mass consumer/commercial usage, it tries to be all things to all people. Consequently, it has a tendency to run unnecessary services, store/hide private information in numerous, often hidden, locations, and exposes your PC to unnecessary security risks. There are various measures you can take to tighten up Windows security:

a) Disable unneeded services: Many of the services in Windows are unnecessary, and some are security risks (e.g. the 'Remote Registry' service, which permits third party network access to the computer's system settings). There are numerous online guides giving advice as to which services you can safely disable (see, e.g. http://www.optimizingpc.com/optimize/windowsservices.html or http://www.prestwood.com/aspsuite/kb/document_view.asp?qid=100274

b) System Restore points: by default, Windows saves a backup of your system settings at regular intervals (and therefore may store information that is ideally kept sensitive) in case you need to roll-back the system to an earlier point in time. Most computer problems can be fixed via other methods however, and if you don't use/need System Restore you can disable it (via Control Panel / System / System Properties / System Restore tab).

c) Hibernation: if you don't use hibernation, ensure that this is disabled, since otherwise it will intermittently save anything that you are currently working on to your hard drive in plain text form – even encrypted documents – which could later be retrieved. (Control Panel / Power Options / Hibernate tab / uncheck 'Enable Hibernation').

d) Pagefile/Swapfile: by default, Windows creates a file on your hard drive (pagefile.sys) which it uses as additional computer memory, and it shifts running processes to this file on the hard drive when necessary. Many modern PCs have sufficient RAM (e.g. over 1 GB) not to need this file. You can disable it via Control Panel / System / Advanced tab / select 'Settings' button under the 'Performance' heading / Advanced tab / Virtual Memory / Change / select 'No Paging File' / click 'Set' / click 'Ok'. .

   NOTE: Disabling the pagefile is contentious, and the debate around this is unresolved (see, e.g. http://www.codinghorror.com/blog/archives/000422.html for a discussion). Provided you have a reasonably fast CPU and a decent amount of RAM, you should not encounter any problems. If you do need the paging file for some reason, or your RAM capacity is not sufficient to do without it, you should at least ensure that it is securely wiped when the computer powers off (see Section 1.3.1., below). In addition, the pagefile can be encrypted using a dedicated encryption product, such *BestCrypt* (http://www.jetico.com).

e) Windows Security Center: The built-in Security Center and Windows Firewall are highly ineffective. Disable them via the Control Panel, and use a third party Firewall instead (see Section 1.2, below).

f) Windows Privacy Tools: In addition to the above steps, you can utilize easy-to-use, one-off, privacy tools to tighten up Windows settings. See, e.g. *Security and Privacy Complete* (http://cmia.backtrace.org/index_en.html) and *XP Anti-Spy* (http://www.xp-antispy.org/).

g) Alternative Software: Avoid using Microsoft software (e.g. Office, Outlook Express, Internet Explorer, Windows Media Player) so far as possible. Since they are designed to collaborate with one another, most of them leak

personal information all over the place. Use open-source alternatives so far as possible (which typically also have the added benefit of being much less resource-hungry). For example, consider using:

- *Open Office suite* (http://www.openoffice.org) instead of MS Office (Word, Excel, etc). Particularly important for office software is to remember to disable 'auto-save' in the program options – since if you are working on an encrypted file the document may be saved to your drive as plain text during an auto-save.
- *Thunderbird* (http://www.mozilla.com) or *Eudora* (http://www.eudora.com/email/features/windows/) instead of Outlook Express
- *Firefox* (http://www.mozilla.com) or *Opera* (http://www.opera.com/) instead of Internet Explorer
- *VLC Media Player* (http://www.videolan.org/) or *Media Player Classic* (http://sourceforge.net/projects/guliverkli/) instead of Windows Media Player
- *Foxit PDF Reader* (http://www.foxitsoftware.com/pdf/reader_2/down_reader.htm) instead of Adobe Acrobat Reader.

1.2. Avoiding Malware

The commonly talked about threats to computer data surround the execution of malevolent code on your PC, in the form of viruses, trojans, spyware, etc. Discussion of this topic usually revolves around damage to your data or identity theft by cyber-criminals for financial gain; but it is also crucial to ensure that you are protected from malware that could benefit other adversaries. One obvious aspect is keylogging software: you can come up with the most complex passwords to protect your data, but if there is a keylogger on your PC capturing each keystroke you enter, the password might become worthless. Equally insidious is the use of 'copware' – malware planted on your PC via LEA specifically targeting you (for an example of this, see, e.g. http://www.infiltrated.net/cipav.pimp). Such software frequently arrives on the target's PC via email attachments. Standard email advice applies, e.g:

- Disable HTML in your emails – in most webmail and desktop email clients there is an option to do this in the settings (eg. in *Thunderbird*: 'View' menu / uncheck 'Display attachments inline' and check 'View message body as...plain text');
- Use Anti-Virus software that scans emails as well as files;
- Don't open attachments from unknown sources.

In addition, further advice includes:

a) Check regularly for the presence of hardware keyloggers (a small device fitted to your PC designed to record keystrokes as an alternative to software keyloggers). The device will appear inconspicuous, and could, for example, resemble a traditional USB-type plug. Also consider applying a drop of paint (or, e.g. correction fluid) to the screws in the back of keyboards, making it easier to see if the hardware has been tampered with.

b) When encrypting data, and where given the option to do so, use 'keyfiles' in addition to passwords. This is an available option with some encryption programs, which enables you to specify a file(s) on your hard-drive (perhaps a photo, for example) that must be entered in addition to a password. This will help protect against keyloggers (though not against malware that also captures mouse-movements).

c) If practicable, you could also use an on screen keyboard (OSK) to enter passwords (thereby using the mouse rather

than the keyboard).

d) Zero-emission pads: Surveillance teams can remotely scan the electromagnetic emissions from your computer monitor, e.g. as you type a passphrase (google TEMPEST for technical details). You can use a replacement text editor that enables you to view and/or edit text in a special font and screen that allegedly 'diffuses the emissions from your computer monitor efficiently enough to defeat TEMPEST surveillance equipment'. Such a pad can be downloaded at: http://geocities.com/phosphor2013/zep.zip

e) So far as security software is concerned, you should have one Firewall, one Anti-Virus (AV) program, and one Anti-Spyware (AS) program, all providing 'real-time' protection. For completeness, you could also install a second AV and/or AS program and/or dedicated anti-trojan software (e.g. *TrojanHunter* http://www.misec.net/) – not to operate in 'real-time' (since a software conflict is possible) but just to perform regular scanning of your PC.

Firewalls, AV and AS vary considerably in effectiveness (as well as in the amount of your PC's resources that they use). Check PC magazines for test results, or check online sources for the most effective protection. Good sources of information are sites such as Wilders Security Forums (http://www.wilderssecurity.com) and Matousec (for firewall comparisons: http://www.matousec.com/projects/firewall-challenge/results.php).

It is sometimes rumored – though to what extent this is likely is debatable – that major AV/AS companies may turn a 'blind-eye' to copware. Here is one advantage of using standalone products, e.g. separate AV, AS and Firewall software each from a different company, rather than the easier option of relying on a single security suite such as Norton or McAfee. In addition, some software is notorious for 'phoning home' regularly – Zone Alarm, for instance, frequently (more so than necessary) contacts its company's servers without notifying the user. It may therefore be desirable to turn off 'automatic updating', and manually update software at (say) daily intervals; and for persistent software (e.g. Zone Alarm) you can prevent it from contacting its servers by making simple changes to the Windows 'hosts' file (for instructions, see, e.g. http://labnol.blogspot.com/2006/02/prevent-zonealarm-from-phoning-home.html).

f) In counteracting malware, you should also keep an eye on which programs are running on your PC, and whether any software has set itself to startup when you boot Windows. Both can be checked via Windows' built-in tools:-

- to view running processes, open Task Manager by right-clicking on the taskbar and selecting the 'processes' tab. You can identify any processes you do not recognize online, by looking them up at sites such as (http://www.whatsrunning.net/whatsrunning/ProcessInfoCentral.aspx).
- to check which programs are set to start when you boot Windows, go to Start / Run... then enter “msconfig” in the box (without the quote marks). In the window that appears, the last tab marked 'Startup' lists these items. Many of these are inserted by software, and are unnecessary. To check whether it needs to run at startup, identify the program at the following site: http://www.sysinfo.org/startuplist.php and uncheck any that are not needed. (Note, this has the added advantage of substantially reducing the PC's boot time).

As an alternative to these built-in Windows tools, you could use a freeware program to keep a closer eye on running processes and startup items, e.g. *What's Running* (http://www.whatsrunning.net/whatsrunning/main.aspx), *Process Explorer* (http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx) or *CurrProcess* (http://www.nirsoft.net/utils/cprocess.html)

g) Keep up-to-date all your software that uses network connections, such as your browser, anti-virus software, and all security products.

1.3. Cleaning and Erasing

Windows stores a vast amount of information about your activities, which should be cleaned up on a regular basis. Note that such traces, along with any files that you chose to get rid of, should be securely erased rather than just deleted. This distinction between 'deleting' and 'erasing/wiping' is a crucial one. Deleting data in the standard way merely makes the data invisible to Windows – it remains on the hard disk until it is overwritten by other data. Instead of deleting, data should be securely 'erased' or 'wiped' (i.e. it is overwritten a number of times with random data so that it becomes unrecoverable).

1.3.1. Erasing files

There are numerous tools available for securely erasing files. One simple, freeware, tool is [Heidi] *Eraser* (http://www.heidi.ie/node/6). This has various features, one of which is to insert itself into your context menu, such that when you right-click a file, you just select 'Erase', and it will wipe the file according to the number of 'passes' that you specify. Another useful feature is 'Erase Secure Move': usually when you move files from one place to another, behind-the-scenes Windows actually copies the file to the new location, then deletes the existing file – which suffers from the above-mentioned issue of the deleted file being recoverable. With the Erase Secure Move option, after the file is copied to the new location, the existing file will be wiped, rather than just deleted.

NOTE: *Eraser* can also be set to erase the Windows 'pagefile' on shutdown/restart (see 'Locking down Windows', Section 1.1, above).

1.3.2. Erasing disk space

Files that are deleted automatically by Windows (e.g. temporary files which it has created), or files that have been deleted by the standard method without having been wiped as above, will be simply be hidden in 'free disk space' until overwritten. To ensure that these have been removed, regularly wipe the 'free disk space' on your hard drive – again, *Eraser* (above) is good for this purpose.

1.3.3. Cleaning traces

Most software stores information about your usage – e.g. Internet browsers keep a record of details such as your browsing history, downloads, and cookies; PDF readers store a history of the last few files you've read; Office products keep a record of recently opened documents and perhaps unusual words used therein; media players store details of recently played files; Windows itself stores temporary files, prefetch data, memory dumps, and so on. A simple way to erase all such tracks in one go is to use dedicated 'cleaning' software. For example, *CCleaner* (http://www.ccleaner.com/) is a decent freeware program which will erase these tracks for you. In the settings options, you can select the number of times such traces should be 'wiped', rather than simply deleted.

NOTE (1): All decent erasing/wiping/shredding software will allow you to specify the number of times that the data will be overwritten – typically, you can choose to overwrite data once, three times, seven times or thirty-five times, depending on the sensitivity of the data. There is some debate as to whether modern hard drives require as many passes to irrevocably destroy data – Googling this issue will produce much discussion. To be on the safe side, a minimum of three 'passes' is suggested. Naturally, the more 'passes' over the data you select, the longer it will take. Be aware that,

say, shredding the entire free disk space on a hard drive (which may be hundreds of gigabytes) will take a significant amount of time.

NOTE (2): If wiping data on flash memory (e.g. USB sticks), wiping individual files is insufficient to make them irrecoverable, due to the way such memory writes data. See the special section on USB drives (Section 1.5, below).

1.4. Encryption

Broadly-speaking, "computer forensics" involves inspection of the computer hard drive for evidence as part of a legal investigation. In the event that your PC is seized, investigators or other adversaries will search it for the 'activity traces' referred to in the previous section, as well as stored files and documents, and other evidence of how the PC has been used (e.g. checking the Windows Registry for evidence of which USB drives have been used – since details of such devices, including their serial numbers, are stored there). The goal of encryption is to make data unintelligible, so that, even if your data is seized, it cannot be read.

A brief note on the medium which you may be using: first, there is the hard drive. Typically, Windows will be installed onto partition C of the hard drive (and unless you have created other partitions, this may make up the entire physical drive). Data may also be stored on external, USB hard drives; on flash memory drives (USB sticks / pen drives); on floppy disks, CDs and DVDs. It is important that, on whichever medium you store sensitive data, that data are encrypted.

1.4.1. Individual Files

There are numerous tools available to encrypt data, offering various different options. Some software will simply encrypt individual files – they will still be visible on the hard disk, but a password will be required to open them. Other software offers a greater range of options, such as creating a 'vault' on your hard drive of a specific size, into which you can place sensitive files without having to encrypt each file individually.

TrueCrypt (http://www.truecrypt.org) is highly recommended for your encryption needs. It enables both the creation of encrypted files, as well as the ability to encrypt an entire hard drive partition, or an entire device (e.g. a USB stick). It also allows for the creation of 'hidden volumes' – a partition/device can be encrypted, then within this encrypted container a *second*, encrypted contained is created. This is primarily so that if you are forced to decrypt the 'outer' volume, on which you might store a few sensitive-looking, but unimportant files, it will not be evident (and cannot be proved) that there is a second, hidden volume.

NB. For various security reasons, encrypting partitions or devices is preferable to encrypting individual files – the *TrueCrypt* manual explains these in detail.

The advantage of the open-source *TrueCrypt* over most other encryption software is the 'plausible deniability' aspect. It is impossible to prove that a partition or device encrypted with *TrueCrypt* is in fact encrypted. Upon forensic analysis, the partition or device appears to simply be filled with random data – as though there is nothing on the partition or device. This is crucial in authoritarian regimes, e.g. the United Kingdom, which has enacted a criminal offense (punishable by up to 2 years, or 10 years in terrorism cases) of 'failing to decrypt' (or provide the password to enable decryption) when demanded by the authorities. Obviously for such a law to be used against you, it would have to be established that you had some encrypted material in the first place. With a *TrueCrypt*-encrypted device or partition,

this should be impossible to prove.

NOTE: If you are working with individual encrypted files (rather than storing files in a container or partition) and are using USB flash drives, see Section 1.5 on USB drives below.

1.4.2. System Drive / Full Disk / Whole Disk Encryption

The disadvantage of only encrypting individual files or external devices is that computer forensics can still reveal much about your computer usage from the system partition (the drive on which Windows is installed) and – importantly – sensitive details such as your browsing history, bookmarks, emails, and email contacts addresses, may be accessible. Details of your contacts is one of the first things an adversary will check for, which they will use to 'broaden' their investigation, perhaps by targeting those contacts. There is therefore an obligation to protect not only yourself, but also those with whom you correspond.

Computer forensics is essentially rendered ineffective by encrypting your entire system drive (typically the C: drive in Windows). This is the ideal position: if the adversary cannot access your hard drive to begin with, you have gone a long way to defending your data. The latest versions of *TrueCrypt* (versions 5.0 and upwards) have an option for encryption of the system drive (or the entire hard drive, if it has more than one partition). It is very simple to use, and will ensure that no one can access your hard drive without first entering the correct password prior to the computer booting (and also makes it more difficult for adversaries to plant data on your hard drive). A detailed reading of the *TrueCrypt* manual is essential in order to encrypt the system drive effectively.

One consideration for those in countries in which failure to disclose a password is a criminal offense (just the UK at present, though this will undoubtedly be extended to other countries), is that where your entire hard drive (or just the system drive) is completely encrypted, you lose an element of plausible deniability. *TrueCrypt* system encryption, for example, stores its 'boot loader' (the information necessary for the computer to boot) on the first cylinder of the hard disk – which will obviously be visible to a forensics team. It is possible to remove the boot loader and instead boot from a CD which has the TC boot loader installed, though obviously this is more inconvenient.

In any event, whether or not the boot loader is present, it remains the case that it cannot be proved that the hard drive itself is encrypted – the remainder of the drive will still appear as random data. So from this point of view, you are still protected from 'failure to disclose password' laws. Nonetheless, having to explain away an internal hard drive with a TC boot loader, and "nothing else" on it, will be tedious (depending on how convincing you can be that you had "coincidentally, just recently wiped the hard drive"). Therefore it may be felt preferable to use other tactics to increase plausibility.

One such tactic is to install Windows to an external hard drive, or to a USB stick, and encrypt it with *TrueCrypt*. You can then keep your 'dummy' Windows installation with no compromising data on the PC's internal hard drive, and boot to the external hard drive or USB stick to use your 'real' Windows. Technically, Windows does not want to be installed to external devices – but it can be achieved. There are numerous guides available on the web; one of the most succinct set of instructions is available at http://www.ngine.de/index.jsp?pageid=4176 – and the project also has a useful forum for resolving issues. For installing Windows to an external device to work, it is necessary that your PC's BIOS is capable of booting to external devices – most recent computers (built in the last few years) can do this, but if you have an older PC, check its ability to do so by doing a web search on its model.

If utilizing this method, your 'computer' effectively lives on your external device, while you maintain a dummy system on the internal drive. This has the added advantage of portability – your Windows installation can be kept in a secure place when not in use, etc. Again, the *TrueCrypt* boot loader will reside on the first cylinder of the external device – but it is certainly more plausible to have an external device with "nothing on it" than an internal drive (particularly if you take the extra step of removing the *TrueCrypt* boot loader and booting the device from a CD).

NOTE: While the latest version of *TrueCrypt* (6.0 and upwards) now enables the creation of a hidden, encrypted system drive – by utilizing a 'dummy' system partition, with the real system partition hidden – at the time of writing it is not ideal: to ensure complete plausible deniability it has very stringent requirements, e.g. the real system partition should not be used to access the Internet (which partly defeats the object), files cannot be copied from the real partition to other media, the dummy partition must be accessed regularly to make it appear plausible, etc. It may be felt that until a more substantive hidden operating system is available, this latest feature should be used circumspectly.

1.5. Security Note: USB Drives and Wear Leveling

When writing data to a USB flash drive, a PC uses a 'logical address' on the drive. However, this logical address is distinct from the flash drive's 'physical block address' – since most USB flash drives use a 'wear leveling' technique. Wear leveling – i.e. shifting data around the physical blocks of the flash drive – prevents the same physical block being used over and over (in order to preserve the life of the USB drive).

Consequently, any time updated or new data are written to the flash drive, such data will be written to a new physical block, regardless of the address of the old block, and any old/amended data is just deleted (not wiped).

This raises a number of security issues, e.g:–

(1) 'Securely wiping' (e.g. with Eraser) an individual file on a flash drive is potentially ineffective, since the random data that is used to overwrite could be written to a different physical block; the existing data will simply be deleted, rather than wiped.

(2) Encrypting individual files could potentially suffer similar problems – e.g. when decrypting a file, amending it, then re-encrypting it.

These issues can be resolved by either securely wiping the entire flash drive (not just wiping individual files) or by encrypting the entire flash drive (rather than encrypting individual files on it) – since then it makes no difference to which physical block the new data is being written.

Ideally the latter approach should be used for all USB flash drives on which sensitive data is placed – encrypt or wipe the entire USB drive – as necessary. For any existing USB flash drives on which this approach has not been taken, it would be advisable to format and wipe the USB drive completely, then start using it afresh with this 'entire USB drive' approach.

1.6. Other Methods

There are of course many, many alternatives to the security suggestions outlined above, such as using any or all of the following:

1.6.1. Live CDs

Live CDs are an excellent alternative to encrypting the entire system drive. Essentially, an entire operating system (usually Linux-based) is on the CD, and whenever you want to boot to your OS, you simply boot the CD rather than booting to your hard disk. Should you not want to encrypt your hard drive, you could use the OS on there for all non-sensitive tasks, and use the Live CD for Internet access / other sensitive tasks.

Running an operating system from a Live CD means that the PC's hard drive does not get used at all – and is therefore not subject to problems of leaving behind 'traces' to be recovered by forensics. There are some limitations with Live CDs e.g. a limited range of software can be run from them, and since the CD is read-only (as the point is *not* to save any data, which could be recovered!) any data you do want to save while working within the CD, or settings you want to keep, should be saved to an (encrypted) USB drive. Its simplicity ensures that this remains an attractive alternative, and it is worth keeping an eye on developments in this area. For some examples of Live CDs, see *Bart's PE* on how to create your own live bootable Windows CD (http://www.nu2.nu/pebuilder/) or see http://www.livecdlist.com/ for a list of pre-built, mostly Linux-based alternatives.

An excellent example of a pre-built option is the *Incognito* Live CD – this an operating system on a CD which is pre-configured to use the Tor network for all Internet access – including emails and web browsing (for urther details, see: http://www.browseanonymouslyanywhere.com.

1.6.2. Portable applications

If installing an entire operating system to an external drive/USB stick, or using a Live CD, are not desired options, another alternative is to use 'portable applications' – standalone versions of existing software that can be run from a USB stick and do not save files or settings to your hard drive in the way that regular applications do. The idea is simply to prevent data being saved to your hard drive – the application files and data (including settings such as bookmarks, emails, etc), will be stored entirely on the USB device (which could be encrypted using a program such as TrueCrypt). See, for example, http://portableapps.com/ for an entire portable suite of software (including commonly-used programs such as *Firefox*, *Thunderbird*, *Open Office*, etc.).

The use of portable applications may prove a practical and easy method of protecting your most sensitive data without going to the lengths of full disk encryption. One drawback is that there will still be traces of the USB drive having been used on that PC, and any monitoring software (firewalls, AV, etc.) is likely to have a record of an application on the USB drive (eg *Firefox*) having been run, which you might be called upon to explain. Nevertheless, this is an inconvenience more than anything, and so long as the USB stick itself is encrypted, the data will be safe. To increase the protection, this method could be combined with the following option.

1.6.3. System drive emulation software

Such software effectively prevents data being written to your hard drive by creating a clone of the system partition (typically drive C: in Windows – which includes system files, page file, registry files, application data and program files, etc.) as it looks when it is booted, in the computer's RAM. Once the system is shut down/restarted, this clone will be restored, thereby returning your system drive to the position it was before any data was written. An example of such software is the freeware program *Returnil* (http://www.returnilvirtualsystem.com/index_files/rvspersonal.htm). Simple to use, it is 'switched on' when necessary, and from that moment nothing that takes place (programs installed, software

used, etc.) is permanently recorded; all normal computer operations appear to take place, but in fact these changes only take place for the duration of the session – upon restarting the PC there is no evidence that any such activity has occurred.

With reference to the previous item – Portable Applications – an advantage of using combining drive emulation software with running portable apps from a USB drive would be that, once the PC was shut down/restarted, there would be no evidence of the applications on the USB stick (eg *Firefox*) ever having been run (and further, no evidence that the USB stick was ever plugged into that computer).

1.6.4. Virtual machines

Another alternative to running a separate installation of Windows on an encrypted device is to employ a virtual machine. Such software (e.g. *VirtualBox*, at www.virtualbox.org) enables you to create a virtual operating system on your existing computer. In this way, you could run a dummy copy of Windows (or any other OS) on the main hard drive, then boot to a virtual copy of Windows which could reside in an encrypted file or partition on the hard drive. One drawback of this technique (other than the additional system resources / RAM consumption it requires) is that it is not guaranteed that traces of the virtual systems may not still appear in the 'real' system, since the two systems share some resources (and frequently, a network connection).

SECTION 2: Protecting Data While in Transit Over Networks (Internet, Email, etc).

Whenever data is on the move – whether in the form of sending/receiving email, surfing the web, chat, downloading via P2P, viewing streaming media files, etc – it is at risk of interception. Data is transferred via different protocols (e.g. 'http' for web traffic, 'pop3' or 'smtp' for email, 'ftp' for some file uploads/downloads, etc). All the 'standard' forms of protocol (including those just mentioned) are sent over networks in plain text format – meaning that the data is visible to anyone who intercepts the traffic (your ISP, crackers, LEA, etc). The goal is therefore to utilize methods of secure communication so far as possible, irrespective of the data that is being transferred.

2.1. Email

Most commercial email addresses (including any email addresses supplied by your ISP) typically use insecure protocols. This will be apparent by checking the ports they use to communicate. If you use a desktop email client (eg. *Outlook*, *Outlook Express*, *Eudora*, *Thunderbird*) you will find this information under the 'Settings' option. If your email communicates via standard ports (usually port 110 for POP3 (i.e. incoming email) and port 25 for SMTP (i.e. outgoing email), it is being transmitted unencrypted – and therefore potentially visible to everyone.

There are various techniques that can be employed to enhance the security of your emails:

- Check your email provider's website to see if they offer an encrypted option (i.e. sending and receiving email via SSL (secure socket layer)). Usually this will simply be a matter of changing the port used in your email client's account settings – e.g. changing the ports to ports 995 (SSL POP) and 465 (SSL SMTP).
- Avoid using email addresses provided by an ISP, and instead use dedicated email providers, such as *Fastmail*, *Hushmail*, *SafeMail*, and so on. Examples of such providers can be found in Section 3 below, or at EPIC's website: http://epic.org/privacy/tools.html. Specialized email providers enhance your security by limiting the amount of information transferred to the recipient in the hidden email 'header' – which in the case of standard email providers (ISPs, *Hotmail*, etc) provide the recipient with far too much information, such as the IP address of your computer, the operating system that you use, and even which email client you used to send the email).
- Use a dedicated form of email encryption, such as *PGP*. This utilizes public key encryption – the drawback being that the people with whom you communicate must also use public key encryption. Encourage others that you correspond with to do this. See 2.1.1. for more information.
- Anonymous Remailers can be used to conceal from the recipient the origin of the email (see Section 2.3 for further details).

2.1.1. PGP

In 'public key' cryptography, two different keys are used: one key is secret and the other is made public. Anybody sending you an email simply encrypts their message to you using your public key. The public key is obviously not secret – in fact it may be spread widely so that anybody can find it if they wish to send you encrypted email (you can upload the key to a public key server to do this; though you may prefer just to give your public key to specific

correspondents). The only way to decrypt an incoming message is with your secret key. The process works in reverse when sending email: you encrypt an email using the recipient's public key, which only they can decrypt using their private key.

The original, and most well-known, program of this type is *PGP*, invented by Phil Zimmerman. There is now an OpenPGP standard, with which all software using public key cryptography should comply. Consequently, other programs are becoming popular, such as the open-source *GNU Privacy Guard* (GnuPG) (http://www.gnupg.org), which is OpenPGP compliant and compatible with other Open PGP tools (including PGP itself).

After downloading the software, you simply use it to create a pair of keys – one public and one secret key. The public key can then be given to your correspondents which they will use to encrypt messages to you, which you can then decrypt using your private key. There are some programs which make the process of encrypting/decrypting easier via the use of 'add-ons'. Some email clients (e.g. *Thunderbird*) have add-ons (e.g. *Enigmail*, http://enigmail.mozdev.org/home/index.php) which takes care of the encryption/decryption process on your behalf; the *Firefox* browser also has an add-on (see *FireGPG*: http://getfiregpg.org/) which enables you to easily encrypt text for pasting into a website, for example.

2.2. Web Surfing

Whenever you request a web page via your Internet browser, in very basic terms what is happening is this: your browser sends the request for data to the server hosting that website, which then replies, and transfers the data to your computer, which is then recreated in your browser. Consequently, any request you make (whether by clicking on a link, or manually entering the site address) is transferred over the Internet via standard protocols (see introduction to this section, above) – typically for the Internet this will be http.

Accordingly, this request for a particular web page is sent over the networks in *plain text* and so will be visible to anyone who is monitoring your activity (e.g. your ISP or other adversaries), and also reveals to the site you are visiting information about who you are (your computer's unique IP address) and information about your computer (which browser you use, what language/location settings you use, what the current time is on your PC, etc). In addition, in order to find that site, your browser needs to translate the address of the web page (e.g. (“amazon.com”) into its numeric equivalent – which it does by consulting a domain name (DNS) server. In a standard home Internet connection, the DNS server will be owned by your ISP – so the ISP has a second method of recording which sites you visit. Note that you can change your DNS server to one not owned by your ISP: see OpenDNS (http://www.opendns.com/) for the relevant address to use.

The upshot of the above is clear: both the site you visit, and your ISP (and anyone intercepting), knows the unique IP address assigned to your computer, and what data you are viewing. To avoid this, various options are available to 'anonymize' and/or encrypt your web surfing:

2.2.1. Free proxies

This is the weakest level of 'anonymity' – these are sites (e.g. http://www.w3privacy.com) which enable you to access another site, without that latter site seeing your IP address, i.e. your request is sent to the 'end' site using the proxy site as a intermediary. In such a case, the site you ultimately visit sees the request for data as emanating from the

proxy site, not from *your* computer. This does not protect you against surveillance by your ISP, and the data transferred is typically unencrypted and therefore visible to anyone else monitoring your connections.

2.2.2. Commercial (paid-for) software

These are companies (e.g. *Anonymizer*, see Section 3 for an extensive list) which provide software which effectively bypasses surveillance from your ISP by creating an encrypted 'tunnel' between your computer and that company's server. In practice, this means that before making the data transfer from your PC (in the form of, say, a request for a web page), the software will encrypt this request, and then direct it to be forwarded from your ISP's servers to the proxy company's server. When it reaches the latter, the request will be decrypted and forwarded on to the relevant website. When that website returns the data, the reverse will take place. The effect of this is that:

(a) your ISP cannot see which websites you are accessing – all it can see is that you are communicating with the company's server, not which websites you visit thereafter. (So if you were surfing the web for (say) 3 hours, from your ISP's point of view, they could see that traffic was passing back and forwards to your PC, but you would only appear to be receiving traffic from one address (the proxy company's server), and the contents of that traffic would be encrypted);

(b) the website you are visiting cannot see who you are – since as far as they know, they are receiving the request for data from the proxy company's server, and simply return it to that server.

The weak link in this chain will be apparent. While you are protected from your ISP, and from the websites you visit, the commercial proxy company knows who you are and (potentially, if they keep logs, what you are doing). The significance of this will vary according to the circumstance. If the sites you are visiting are merely sensitive (rather than illegal in your jurisdiction), the fact that the commercial proxy knows what you are doing is of little importance (particularly if – as recommended – you chose one in a different jurisdiction to your home country). You may, for example, simply not want your ISP to know that you visit boychat.org. The commercial proxy would be adequate for such uses.

Check the terms and conditions of the commercial proxy company – in particular, whether they keep logs of your activity (for example, some log everything; some do not log origin and destination, but only record the quantity of data passing through, etc). Also, check which forms of data they will support – some commercial proxies will only encrypt Internet traffic (the http protocol), others (genuine 'VPNs') will encrypt *all* forms of protocol (whether it is Internet, email, file-sharing, etc). For additional security, look for a commercial proxy that offers anonymous payment methods and, ideally, is outside the US/EU.

In summary: the advantage of using a commercial proxy is that it gives you a level of protection from monitoring by your ISP, and from the sites you visit, and generally you suffer little or no loss of speed in browsing. A potential disadvantage is that the commercial proxy knows who you are. For this reason, when accessing more sensitive sites, you may wish to employ other methods, such as *Tor*.

2.2.3. Tor

The basic idea of *Tor* (http://www.torproject.org/) is to protect your privacy by disguising the route of data to and from your PC, as well as encrypting the traffic.

Broadly-speaking, the *Tor* software will create a chain of at least 3 proxies, through which your data will pass – each interim stage in this chain only knows who sent the data to it (the previous proxy) and who it should forward data to (the next proxy in the chain).

Effectively, this means that if you want to visit, say, Site A, *Tor* will encrypt this request, and pass it to the first link in the chain (Proxy 1), with encrypted instructions on where to send it thereafter. Proxy 1 will forward the encrypted request to Proxy 2, Proxy 2 will forward it to Proxy 3, etc. Thus, Proxy 1 only knows Proxy 2, Proxy 2 only knows Proxy 1 and Proxy 3, Proxy 3 only knows Proxy 2. The final link in this chain (known as the 'exit node') transfers the request to your ultimate destination (Site A). The process is then repeated in reverse. From the point of view of the user, this process happens invisibly – once the software is up and running, you merely use your browser as normal.

(It should be noted at this point that once the data leaves the final link in the chain, it is no longer encrypted – at least until data is returned from your final destination to the first link in the return journey. This is only really significant if you are providing identifying information, e.g. entering a password into a webmail server – since then it is apparent that the request has come from you).

The obvious advantage of this procedure is that there is no commercial proxy in the middle. No single point in the chain knows both you *and* your ultimate destination. This is arguably the most secure form of anonymizing web traffic. Some disadvantages are:

(a) There is an initial learning curve with *Tor* – nevertheless, there is extensive documentation on the *Tor* website to assist with this, and once you have set it up and used it a few times, it becomes second nature.

(b) As part of this learning curve, it is crucial that you configure your browser correctly, and a second piece of software – e.g. *Privoxy* – should be used to filter data such as your computer's DNS requests (see above) over the Tor network. Again: this is not as complicated as it sounds in abstract, and is made easier for Windows users by the GUI package (*Vidalia*) which includes all the necessary software (including Privoxy, and a quick-configuration button for Firefox users).

(c) It should also be pointed out that when using *Tor*, your browsing will be slowed considerably – which is to an extent inevitable given the number of different servers the traffic passes through, each of which may have different bandwidth allotments. *Tor* will therefore be unsuitable for downloading large files (and possibly streaming data, such as Youtube or other streaming media). Its primary use will be for visiting particularly sensitive websites.

(d) Related to the previous point, at the present time *Tor* only encrypts limited forms of protocol – primarily http traffic – which effectively limits its use to visiting web sites.

(e) There have been a number of stories about breaching *Tor's* anonymity. Such instances tend to be a consequence of user implementation, rather than any flaw in *Tor* itself. More specifically, when using *Tor*, ensure that Javascript is disabled in your browser (since it is due to malicious scripts that Tor can be compromised. This can be done manually (in *Firefox*, go to Tools / Options / Content / uncheck 'enable Javascript'), or through the use of an Add-on such as *NoScript* (http://noscript.net/), which automatically blocks scripts unless you permit them on a sire-by-site basis.

It will be clear from the above consideration of Email and Web Surfing that there is no 'perfect' solution to online anonymity. Experts would say that 'true' anonymity is impossible. As long as you are transferring data from one

computer to another over a network, there will be attempts made to intercept or track that data content and movement. Nonetheless, utilizing a combination of the above methods, depending on the circumstances and the sensitivity of your activities, offers significant protection against surveillance.

NOTE: Regardless of whether an anonymous connection is used, your browser should be as secure as possible, since there are numerous browser vulnerabilities that can expose your PC to malware. Javascript, Flash, Shockwave objects – all of these can compromise your anonymity. *Firefox* is highly recommended as a more secure browser than Internet Explorer, and can be further customized with Add-ons to increase security. *NoScript*, referred to above, is particularly desirable. Other security-related Add-ons are referred to in the Links section, below.

2.3. Other Network Usage

Similar anonymity considerations apply to any form of network activity, including Chat, P2P/File-Sharing, Usenet, etc. Typically, all such traffic is carried unencrypted over public networks, and is therefore capable of surveillance by the ISP and interception from other adversaries. Wherever possible, utilize security and anonymity tools to protect the privacy of such data.

- For chat/IM, *OTR* (Off The Record), http://www.cypherpunks.ca/otr/ is an excellent plugin. Even if your contacts' private keys are determined, your private conversations are not compromised.
- For posting messages on Usenet, consider using an anonymous remailer, which forwards messages without revealing where they originally came from. Anonymous remailers utilize the same 'onion router' principle behind *Tor*: they remove personal data from the message, encrypt it, and pass it through a chain of 'post offices' until the last remailer in the chain forwards the message to the recipient. As with *Tor*, the idea is to make the message untraceable to the sender.

  The main issue with remailers is whether/how a recipient can reply to the message, given that its source is untraceable. Different types of remailers handle this differently. 'Pseudonymous remailers' are the most basic: they are typically unencrypted, and merely apply a pseudonym to the sender and forward the message to the recipient, who can then reply via the remailer. 'Cypherpunk remailers' typically encrypt the message and pass it through numerous hops on the chain to the recipient; generally the recipient cannot reply to such messages. 'Mixmaster' and 'Mixminion' remailers offer more advanced features, and seek to address issues such as the capacity for the recipient to reply to a message that has come from an 'untraceable' source. These generally require dedicated software.

  One example of such software is *OmniMix*: http://www.danner-net.de/om.htm, which is designed for Windows, and can be used to send email and Usenet postings through the Mixmaster anonymous remailer network. *OmniMix* is straightforward to install, and can also be run from a removable device such as a USB stick.
- When downloading from file-sharing networks (e.g. Limewire, Shareaza, etc.), it is important to know that not only is the traffic unencrypted (and therefore visible to, e.g. your ISP), your IP address is made available to anyone you are sharing with – and there is every possibility that the latter could be LEA or other adversary. A new breed of 'anonymous' networks are continually being developed, which generally seek to utilize the onion routing principle – traffic is encrypted and the origin/destination of the requested file are proxied. For examples of these, see:

- *Freenet:* http://freenetproject.org/
- *GNU Net:* http://www.gnunet.org/
- *Ants:* http://antsp2p.sourceforge.net/
- *StealthNet:* http://www.stealthnet.de/en_index.php

For a more detailed comparison of the different programs available, see http://www.zeropaid.com/software/file-sharing/ and http://www.anonymous-p2p.org/programs.html

SECTION 3: Useful Links

NOTE: inclusion of links should not be taken to imply endorsement of particular software.

3.1 Cleaning Traces, Erasing and general Encryption software

- *CCleaner*: http://www.ccleaner.com/ - shreds/wipes sensitive traces of activity
- *Heidi Eraser*: http://www.heidi.ie/node/6 - secure erasing software for individual files and free disk space
- *Darik's Boot and Nuke* (DBAN): http://www.dban.org/ - a boot disk that does a government-standard wipe of hard drives
- *TrueCrypt*: http://www.truecrypt.org - open-source encryption software
- *BestCrypt*: http://www.jetico.com - commercial encryption software

3.2 Email providers, Remailers, and Email Encryption

- *Fastmail*: http://www.fastmail.fm/ - email provider
- *Hushmail*: http://www.hushmail.com - email provider
- *Alice Mail*: http://www.alicemail.net - email provider
- *Anonymous Speech*: http://www.anonymousspeech.com - email provider
- *Cotse*: http://www.cotse.net - email and SSH provider
- Beginner's Guide to PGP: http://www.stack.nl/~galactus/remailers/bg2pgp.txt - email encryption guide
- PGP for beginners: http://axion.physics.ubc.ca/pgp-begin.html#index - email encryption guide
- The PGP Faq: http://www.cryptography.org/getpgp.txt - email encryption guide
- *PGP*: http://www.pgpi.org/ - email encryption software
- *GnuPG*: http://www.gnupg.org - Linux/Windows email encryption
- *GPG4Win*: http://www.gpg4win.org/ - Windows-based email encryption
- *Enigmail*: http://enigmail.mozdev.org - plugin for Thunderbird Email client to manage encryption
- *QuickSilver*: http://quicksilvermail.net - email remailer client
- *OmniMix*: http://www.danner-net.de/om.htm - anonymous remailer
- *OTR (Off The Record)*: http://www.cypherpunks.ca/otr/ - a plugin for encyrpting chat/IM

3.3 Anonymity online

- *Tor*: http://www.torproject.org/ - open source anonymity project
- *I2P*: http://www.i2p2.de/index – Anonymity, similar to Tor
- *JanusVM*: http://www.janusvm.com/ - Anonymity, similar to Tor
- *Relakks*: https://www.relakks.com – commercial VPN
- *Goldens*: http://goldens.com/ - commercial VPN
- *Xerobank*: http://xerobank.com/ - commercial VPN

- *ShadowVPN*: http://shadowvpn.com/ – commercial VPN (consumer version of Xerobank)
- *JonDos*: http://www.jondos.de/en/ - commercial VPN
- *Steganos*: http://www.steganos.com – commercial VPN
- *SwissVPN*: http://www.swissvpn.net/ – commercial VPN
- *CryptoTunnel*: http://www.cryptotunnel.com – commercial VPN
- *Anonymizer*: https://www.anonymizer.com – commercial VPN
- *TrilightZone*: http://www.trilightzone.org/index.html – commercial VPN
- *Privoxy*:http://www.privoxy.org/ - web filter proxy
- *Proxomitron*: http://www.proxomitron.info/index.html - web filter proxy
- *OpenDNS*: http://www.opendns.com/ - set your DNS addresses using OpenDNS, instead of using your ISP's DNSs.
- *Stunnel*: http://www.stunnel.org/ - use in conjunction with SSL-equipped connections

NOTE: When purchasing commercial products, ensure you check the providers' terms & conditions, particularly regarding their jurisdiction, privacy, reporting and logging policies. Do some research on the different companies' products, e.g. by searching their name at Wilders Security Forums. Use alternative methods of payment wherever possible, such as using prepaid web money/debit cards that you don't need ID to buy.

3.4 Firefox Add-ons

- *NoScript*: http://noscript.net/ - Many browser security holes are related to Javascript. Block scripts entirely, until expressedly permitted on a site-by-site basis.
- *CoookieCuller*: http://cookieculler.mozdev.org/ - can be set up to delete all cookies, or just but keep cookies for trusted sites
- *FlashBlock*: http://flashblock.mozdev.org/ - blocks flash content until you permit it
- *SwitchProxy*: https://addons.mozilla.org/en-US/firefox/addon/125 - Manage and switch between proxies
- *FireGPG*: http://getfiregpg.org/ - a Firefox plugin that facilitates the use of GnuPGP encryption
- *Refcontrol*: https://addons.mozilla.org/en-US/firefox/addon/953 - blocks or fakes your referrer ID

3.5 Miscellaneous Privacy / Security Software

- *Security and Privacy Complete* : http://cmia.backtrace.org/index_en.html - tighten up Windows security
- *XP Anti-Spy*: http://www.xp-antispy.org/ - tighten up Windows security
- *KeePass*: http://keepass.info/ - an open-source password manager
- *TweakUI*: http://www.microsoft.com/windowsxp/Downloads/powertoys/Xppowertoys.mspx - change some hidden Windows settings
- *CurrPorts*: http://www.nirsoft.net/utils/cports.html - see your open ports
- *CurrProcess*:http://www.nirsoft.net/utils/cprocess.html - See info about processes running in your computer
- *WinDirStat*: http://windirstat.info/ - disk usage statistics viewer and cleanup tool
- *PeerGuardian 2*: http://phoenixlabs.org/pg2/ - open-source software for blocking anti-p2p organizations, but could also block known governments' and corporations' IP addresses for non-p2p purposes

- *7-zip*: http://www.7-zip.org/ - compression & encryption tool
- *PeaZip*: http://peazip.sourceforge.net/ - open-source compression & encryption tool
- *PAQ*: http://www.cs.fit.edu/~mmahoney/compression/#paq – open-source high-compression tool
- *Sandboxie*: http://www.sandboxie.com – run your browser inside a 'sandbox' to prevent malware from gaining access to your system
- Pre-paid debit cards / Anonymous web money: see http://www.card444.com and http://www.money-around-the-world.com/ (US), *PaySafeCard* http://www.paysafecard.com (EU)

3.6 Sources for Technical Advice / Support

- Wilders Security Forums: http://www.wilderssecurity.com - forums for information relating to security matters and a vast range of security/privacy software
- EPIC 'Online Guide to Practical Privacy Tools': http://epic.org/privacy/tools.html - a vast array of links to privacy software
- Sommersault's Technical Forums: http://www.somersaultforums.org/techforum/ – a friendly forum for advice on computers matters
- *TrueCrypt* Forums: http://forums.truecrypt.org (or any other software site for product-specific information)
- An old BoyChat post with useful advice on how not to accidentally out yourself: https://www.boychat.org/messages/1107524.htm

FINAL NOTE: If you follow the procedures outlined in this Guide, you will be a long way to protecting yourself - but please remember that there is no such thing as 100% computer security. Stay safe.

Disclaimer: All material provided in this Guide is intended as introductory guidance only, and should not be used as an alternative to undertaking your own research. No representation is made as to the current accuracy of the information and links provided.

Date of compilation: September 08, 2008.