Global Information Assurance Certification Paper

Ray Stirbei

GIAC GSEC Practical
Version 1.4b
Option 1

Achieving personal information security through functionality

[abstract]

When it comes to home computing, information security and privacy are generally misunderstood concepts and subsequently neglected. A possible remedy to make security more easily understood and palatable is to make it more transparent and inline with user functionality. This document provides some general guidelines for integrating the function of security with daily computing tasks with a minimal degree of inconvenience. An example is also provided to give some technical details on how it can be accomplished.

Introduction

The evolution of personal computing came about from the shift away from mainframes and terminals to the decentralized and distributed model of today. The introduction of automobiles in society is vaguely similar in the sense there was an initial lack of concern with security and safety, possibly due to their initial slow speed, but as adoption grew safety mechanisms were added to mitigate some of the risks. The safety curve has generally lagged the progression of performance. In other words, seatbelts, structural improvements and other safety measures have been a reaction to the casualties of automobiles.

Passenger safety in airplanes, however, was always extremely obvious and the safety model in that industry has been proactive from the start. The need for safety in computers is not obvious as flying, certainly not at the same visceral level and I fear the argument for information security will be perpetually difficult. After countless automobile casualties drunk and aggressive driving remains a problem. It is an economic cost to society of approximately 230.6 billion dollars in 2000 [1]. Moreover, unlike driving computer operation is not licensed by the government.

Like morality, security is centered on limiting action and scope. Technology however gives the opportunity to incorporate some aspects of security transparently in the context of home computing. It does not replace the need for understanding one's actions. An informed and diligent user base is one of the best defenses and it is the best solution to achieving information security.

This document focuses on the more tractable goal of making home computing as secure as possible supporting daily tasks with the smallest degree of inconvenience. It complements other papers and books on the subject and attempts to place their suggestions in context. The target audience is any personal computer user.

What is privacy? What is security?

The root of privacy lies in the question of identity, one best answered with individual reading of Plato, John Stuart Mill, Spinoza, Decartes, Locke, Freud and plenty of others. For the purposes of this document, we define privacy as an individual's personal information and freedom of action not being observed by others. That is to say, it consists of your files and your computing habits or behavior.

There is much discussion of personal information such as social security numbers, birth date, mother's maiden name, etc. Rarely mentioned are one's documents such as email, letters, work files, financial information, MP3 collection, etc. Everyone has documents, even if its just Internet cookies or system log files. That is part of his or her identity or behavior.

Security can be defined as measures taken to protect our privacy from hostile acts.

Why should we protect our privacy?

Security is now a basic requirement because general Internet computing is inherently insecure. Every computer may be under some sort of attack and home computers are prime targets.

A likely scenario due to a nonchalant security attitude is a malicious individual hacking your computer and then using it to launch an attack on a military or government agency or to propagate illegal software or pornography. Much more sophisticated attacks are possible: if your browser saves your passwords to web sites for convenience, a hacker can use them to impersonate you to say email a death threat to the president or someone from your address book. Another possibility is to log onto to your brokerage and execute online trades. Or simply collect more personal information to do identity theft. Espionage could be subtler still. The threat increases if victim has a large public profile, such as senior executives or an outspoken activist for a controversial position. Living in relative obscurity diminishes the risk but does not purchase immunity to these kinds of attacks. A basic understanding of the risks goes beyond saving you time from explaining to the Secret Service agents that you did not write that death threat to the president, for example. It is simple neglect to endanger yourself and others.

Thinking your computer would be of no value to an attacker, because you don't have any valuable data or because you simply surf the web is a fallacy. Most trojans, worms and viruses do not discriminate. And human attackers are usually more interested in your computer to launch attacks or to cover their tracks, not to read your email. My home computer connected to the Internet is scanned at least a few times a day; if you are connected you need to be protected.

I propose a small initial investment that will provide dividends in terms of time saving, risk reduction and the intangible good Internet etiquette. All with a minimal impact on your computing experience, resources and wallet. Realistically, like most aspects of life, spending money makes things a lot easier and it is inverse to spending time. However, you can accomplish a great deal of security without spending a dollar.

How we protect our privacy?

There are many resources [2,3,5,6,7,8] dedicated to answering this question in detail and they should be a starting point. This document will assume a familiarity with those resources, especially Brian Porters's work [3] as it is a great introduction to this topic. It also explains some of the technical terms used in this document.

There is no absolute level of security protection; there are only relative degrees of resistance against specific risk. Risk is generally defined as vulnerability x threat x cost. Simply stated the vulnerability is exposure, the threat is the likelihood of attack and cost is the level of negative impact (in time and money) a successful attack can create.

There are many types of attacks to defend against but we can simplify them under three attack modalities: interference, interception, and impersonation. Lets look at how we can defend from these attacks by protecting our privacy.

Protecting computers

To protect our documents we must protect the computers that hold those files. The major tools to abate, not eliminate, the attacks above are personal firewalls, anti-virus scanners, encryption and strong passwords, respectively.

The idea is to:
1.secure the computer
2.create a baseline
3.create a system for continuous auditing against this baseline

Our first task is confirming the computer hasn't already been infected or hacked. A personal firewall and an anti-virus scanner should be installed on every computer connected to the Internet. That is the equivalent to wearing a safety belt.

There are many sources [2, 3, 5, 7, 8] where great information can be gathered regarding these two technologies, like various types of scans, inoculation, updating, etc. For Window users not interested in spending any money, I recommend ZoneAlarm firewall and AVG Antivirus. Both are solid products available at no monetary cost. The URL (the Internet address) for these products is listed in the Resources section of this document.

Run a complete virus scan on all files and memory, and I suggest using more than one anti-virus scanner. There are no cost online scanners that are kept up to date to complement your program. One such example is TrendMicro's HouseCall (URL found in the Resources section)

Once certain the computer is not infected, we can run a formal risk evaluation. Various sites like shields up! (www.grc.com), HackerWacker (www.hackerwacker.com), Symantec Security Check (security.norton.com) provide this service at no cost. Some also suggest ways to remedy the security problems they uncover.

We can commence securing (also called hardening or armoring) our computer with these suggestions. The objective is to make our computer more resistant to attacks. A basic tenet of information security is to use only what you need. So lets remove all superfluous programs and services. These are the programs you have never used or do not plan to use often. An example might be the Alerter service on Windows 2000 or the Universal Plug and Play on Windows XP. Some Windows services allow remote users to access your registry, or view your clipbook or browse your directory; all gaping security holes. You can find guides and articles [11, 12, 13] online that will aid the process of identifying and removing services. Please be very careful when turning off anything as they might render the operating system inoperable. Implement changes one by one to easily revert back in

case of a problem and always backup at every step. Rest assured that your effort will be rewarded with a more secure computer as well as a faster one. I cleared up over 15MB of memory simply by disabling services I never used.

There are many other steps on the road to a secure computer. Some of these steps are:
- apply the proper file permissions (especially for critical data files)
- remove unnecessary user accounts (like the guest account)
- enable system auditing and logging (like logon events, object access, privilege use)
- configure network security (like network protocols, bindings)

There are some detailed guides found in the Resources section at the end of this document. A search on google.com for 'securing Windows 2000' produced thousands of results. But so many checklists with numerous steps can be easily overwhelming. One can spend months reading and learning about each step and registry setting suggested. How do we know we have achieved an adequate level of security? We made a promise earlier to make security more convenient. We need some automation and luckily there are tools to help us. One such tool is the Microsoft Baseline Security Analyzer (check under Resources). An even better one is the SANS Gold Standard Security Benchmark.

As soon as we have a secure baseline for our computer(s) we can create a system that integrates security with minimal hassle. Most operating systems have automated ways of downloading and installing security patches and updates. It is not without risks, but for the home user this feature is recommended. On Windows 2000 you can configure this by going to Control Panel and clicking on the Windows Update icon. The anti-virus and firewall programs should also be set to automatically update themselves whenever a new release is available. Virus scans should be automated as well and ran frequently, at least once a week.

Now that we don't have to worry about the latest security hole listed in our operating system, we can deal with large hassle of password management. With so many websites requiring a username and password it is very convenient to choose a simple password and use it everywhere. It is also very wrong. User trust is based on recognizing identity and passwords the most common technique to recognize you. Passwords are the access keys to personal information. The importance of using strong passwords cannot be overstated.

The general guidelines:
- avoid reusing the same password twice
- make the passwords long
- can be typed quickly
- mix characters, case, numbers to avoid dictionary words
- change them frequently

Keeping track of these numerous passwords and usernames with the goal of convenience we turn again to automated tools. A password generator can be used to mitigate the difficulty of creating good passwords. And a repository can be used to keep track of them.

Such a repository might be a database or a program made for this purpose or even a text file. The ease and speed of retrieval are the important elements here as well as a reasonable security. To keep things simple (and safe) no other repository should be used. This includes saving passwords in browsers, unless you are planning to use the browser's password program as your repository. The Mozilla browser comes with such a password manager (mozilla.org)

Special caution should be employed if a text file is used. Plaintext does not provide any protection for your passwords. No matter how esoteric the file name or directory might be, strong encryption should be employed. You can imagine the damage caused if an attacker finds this information on a compromised computer.

A best practice on the topic of passwords is implementing account lockout policies. These measures prevent attackers from trying to keep guessing your passwords. I recommend the lockout duration be set to 45 minutes, the lockout threshold to 5 invalid login attempts and the reset counter to 45 minutes. On Windows 2000, you can set these options in the Local Security Policy (Start -> Settings -> Control Panel -> Administrative Tools -> Local Security Policy -> Account Policy -> Account Lockout Policy) but note these settings do not affect the Administrator account, so a very strong password for this account is critical.

In short, computer security includes proper configuration, system maintenance and monitoring.

Managing personal files

Once we have a clean and secure computing environment, the focus is a system to protect and manage personal documents and data. The idea is to:
1.identify the files we need to protect
2.centralize the location of these files
3.apply proper security controls and
4.copying them to other trusted computers or media (for backup purposes)

For step one, identify all the documents and files you care about. Examine what programs are being used and where they store their data. Some versions of Windows have a folder called 'My Documents' so most of this work has already been completed. In Linux, all your personal information (including settings) is saved automatically in your home directory.

If all you use is Microsoft Word or Excel and all your documents are under 'My Documents' you are done. Some programs, such as Quicken, will let you specify a folder to save its data files. Other programs might not be as flexible in such a case I recommend moving the whole program to your documents folder. If that is not possible either keep track of the folder where your data files are.

It might be helpful to create a folder structure that accommodates your needs, as opposed to ad hoc folders placed by various applications. Such a structure should be based on

your personality and habits and it is completely up to you. The objective is convenience so choose whatever works for you.

Once the first two steps have been completed, we can think about securing this root folder. File permissions should be stringent: only you should have access. If you are not able to set permissions in Windows 2000, you most likely need to change your file system to NTFS. Go to Start > Run and at the command line type in "*convert c: /fs:ntfs"*. Replace "c:" with your drive letter, if different.

If there is any concern for physical security, encryption should be used. For a laptop, the risk (as defined earlier in this document) is very high. This is due to the likelihood of loss or theft. A PDA (personal digital assistant) with your critical information requires even less effort to lose, misplace or steal. Consider the physical security for your desktop computer as well. If other people have access to your computer, they can circumvent your file security permissions.

Once we calculate the risk, we can apply the technology. Windows 2000 has a file encryption system (EFS) that is very convenient and transparent to use. You can enable it by right clicking on Properties of the folder you wish to secure. Then click on the Advanced tab and then on the checkbox that states "Encrypt contents to secure data". A cross platform alternative to EFS is Pretty Good Privacy (PGP).

The last step is backup. If you have just one computer then the root folder containing all your files should be copied to a CD or another media on a regular basis. Keep it somewhere safe and it should be encrypted (unless you plan to keep in a bank safe).

In the case you have more than one computer, you can use the additional computers for backup purposes. I still recommend copying your files to a CD, to protect against a fire or other physical harm. However, it doesn't have to be as often. Between two computers, backup can be conveniently facilitated by replication or synchronization. Replication involves a bulk copy of data from one computer to another. This is suitable if only one of the computers is primarily used, or if you only have a handful of files.

A synchronization mechanism is recommended for anything beyond the above scenario. A common case is a laptop for school or work and a desktop computer at home. A secure medium is required regardless whether we replicate or synchronize the data.

If access to the other computer(s) is required from the Internet, we need secure communication to ensure the confidentiality of this precious information. If both computers are at home on the local area network, we are already using a secure medium. For an extra layer of transparent security, IPSec can be used in this scenario.

A plethora of vendors offer secure communication, or file synchronization or a combination of both. PCAnywhere, laplink and gotomypc.com are complete packages with lots of functionality. But I recommend a specialized synchronization program that can be automated as much as possible.

Our objective remains convenience and security by using only what we need. Transparent secure communication can be enabled through various types of VPNs (virtual private networks) or through ssh (tool suite).

You can find both commercial and open source (read: free) solutions for communication and synchronization. It is an individual choice based on your needs, technical ability and environment. A good choice should enable automated backup and availability of your files with little hassle. Availability is one of goals of information security.

Protecting behavior

Protecting online and offline actions are more difficult and is beyond the typical prescription: cookie management, blocking spy ware and spam. Awareness and knowledge is essential if you are to protect yourself from the barrage of attempts to track and analyze your actions, either from corporate or government endeavors.

Individual privacy is constantly being eroded due to three major trends:
1. Technology improvements make it feasible to store and analyze massive amounts of data and as society is becoming increasingly digital. (i.e. credit cards, e-commerce)
2. Commercial enterprises aggressively using technology to better market their products and services (i.e. demographics, data-mining, swapping customer lists)
3. Increased government interest and powers in tracking criminals and terrorists (i.e. Carnivore, better integration of government databases)

It is not a question of being watched so much as being logged and tracked. In my area, supermarkets give our cards that enable discount sale items in exchange for a customer's name, address, phone number and maybe other details. Then they effectively analyze this information to measure product demand and buying patterns. However, the cost to individual privacy is enormous: every time you buy an item with the card, your information is being written to a database.

“Give every man thine ear but few thy voice” was Polonius' advice to his son in Shakespeare's Hamlet and it is an effective way to mitigate social engineering attacks among other things.

Every action on the Internet is logged, most likely in several places. Public proxies will remove your computer's information when visiting other sites, usually at a small performance cost.

Multiple email addresses are a good idea for discrete functions, like work or personal correspondence. Keep an email address from a reliable provider (like yahoo) so you don’t become reliable on your ISP connection or employee account.

In a personal experiment to illustrate the degree of spam, I have created an account on yahoo, turned off all marketing preferences and used it to send mail regularly to my colleagues. During the course of one year, ending last month (December 2002), I have not

received any spam at all. Not even one message. The lesson? Using an email account solely for private communication can significantly reduce spam.

In the unfortunate case you are already deluged by massive amounts of spam, here is a plausible transitioning plan:

1. create an email account for friends and family and another for everything else.
2. put your new private email address in the reply-to field of your existing account
3. send emails to friends and family from the old account and their reply will be received at the new email address.
4. use the other new email account for everything else

In the meantime you can use heavy-duty spam-filtering tools like proxies. These can run on your computer. SpamPal is such a tool that runs on Windows. It is available from www.spampal.us and it is free.

General Guidelines

This document assumes most of your computing uses are creating documents, games, email, and surfing. If there is intent to serve a website from your computer, I recommend using (ISP) Internet service provider. Most people don't cut their own hair, they go to a specialist. The seemingly simple act of downloading and running a web server is a very complex security proposition.

Likewise, programs like instant messaging or IRC chatting have their own risks and threat models.

File and print sharing should be turned off, no matter what operating system you are running. File sharing is convenient but at a high cost to general security: it makes a computer more susceptible to attack and your files are vulnerable during transport. File sharing approaches (such as NFS for Unix or NETBIOS shares for Windows) have a long history of security problems. I disable NETBIOS altogether, not just shares, for my Windows systems. Besides added security, removing unnecessary bindings will increase the performance of your computer.

If your network consists of more than one computer, synchronizing your files over a secure medium is preferable to the rudimentary file sharing approach of copying files from one computer to another. If a printer must absolutely be shared, a solution might be use NETBUI instead. NETBUI is an alternative to the standard Windows networking protocol (NETBIOS). It is a protocol that is not being routed, that is to say, it is not accessible from the Internet.

Technology will never replace common sense so use your judgment when opening file attachments from people you don't know or from messages that look suspicious.

Information security, much like physical security, goes beyond the installation of a personal firewall or anti-virus scanner. It is about understanding risk. Hiring a bodyguard might protect you against a mugging but has no effect against getting hit by a bus while

you are crossing a street. Using a strong password for your Yahoo account is useful but not if your laptop is plugged in a library or Internet cafe. It is sent in plaintext and available to anyone with a freely available sniffer program.

Our approach calls for:
1.implementing some initial safety measures
2.consolidation our personal data
3.base lining our system and
4.automating repetitive tasks as much as possible.
What will do this for you? It will mitigate some of the biggest risks associated with your privacy. It buys you security but also backup, archival and the convenience of having your data available when you need it.

An important benefit from this process is the education about the elements of security. This comes from the questions that arise during the implementation of the security measures above. The investment of time spent provides benefits that far outweigh the costs. You don't have to do everything yourself if you are not comfortable doing so. You can always contact a friend or family member or a computer guru from your area to help implement these suggestions.

The real world

Provided below is a personal example how information security has been included in my daily computing based on the principle of least effort but still satisfying my high level of paranoia. It should be noted technology changes very rapidly and this information is current as of February 2003.

My home network consists of three desktop computers, one server and one laptop. The operating systems I use are : Mandrake Linux 9.0, Windows 2000, OpenBSD 3.2, Windows NT 4, and RedHat Linux 8 . All are installed with their native or default file system: Linux uses ext2, Windows uses NTFS and OpenBSD uses FFS.
When I leave my apartment I leave the server turned on so I can use to synchronize my data from the Internet. I sometimes use it for application development purposes because the compilation times are significantly faster than my laptop computer.

The physical layout is illustrated below in Illustration 1. Internet connectivity is provided by a cable modem and a home office firewall appliance provides basic filtering, Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services.

The firewall is currently setup to allow all outgoing traffic and only uninitiated incoming traffic to port 22 on the server. I need to allow some incoming traffic to be able to connect to the server from the Internet.

My communication needs are met by ssh, or secure shell, provided by OpenSSH.

Ssh is comprised of a server and a client component and it enables secure communication between two computers. Mark Sowerby has written a great paper [9] with the details on the setup up and installation of OpenSSH. My Unix computers have both OpenSSH client and server pre-installed. On Microsoft Windows, OpenSSH can be installed with Cygwin. Cygwin is a UNIX environment for Windows and it comes includes many useful utilities besides OpenSSH.

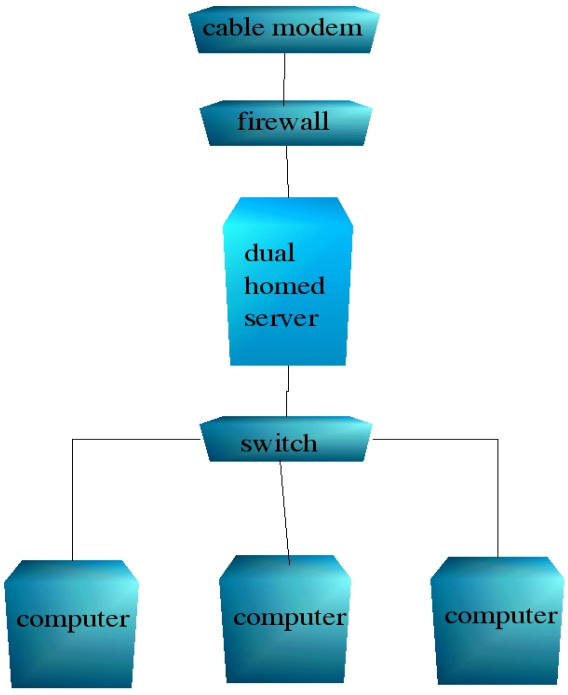

Illustration 1 : home network physical layout

My server and my laptop have the OpenSSH server component (sshd) to allow other computers to connect to them. The desktop computers only have the client (ssh) component.

The server is dual homed and acts as an additional firewall to protect the desktop computers. Dual homed means it has two network interfaces and thus can be part of two networks. The firewall software filters network information going from one network to another. The software also allows fine-grained rules and it is currently configured to reject all uninitiated inbound traffic and allow only select outbound traffic (such as http, instant messaging and some games). My family uses one of the desktop computers and I sometimes need to change the firewall rules to accommodate their requests. It took some time to balance the right combination of firewall rules and it is a constant work in progress.

For example, I started out blocking all ICMP packets. Doing so fortifies my computer against security scanners. But this means my computer will never get 'Host Unreachable' or 'No route to host' error messages so it will just wait for a reply that will never come. It is irritating sometimes but rarely fatal. One day I wasn't able to connect to the server from an outside network. After some troubleshooting I learned it there was a problem with MTU discovery. This is technical topic but the rejected ICMP packets played an important role. I had to relax my firewall rules to allow some of this traffic to be able to communicate. Finding the right balance of security require some trial and error.

How do I deal with my personal data?

All my computers have a local copy of my data but when I'm on the road I want to be able to access my data from the Internet (for synchronization purposes). My folder structure

needs to accommodate cross platform applications as well as the various operating systems I use. Below is a snapshot of the major elements:

folder	***comment***
/archive	past work and files I do not need any current access to.
/bin	various tools that I sometimes need to run on other computers, or various device drivers for my computers so I don't have to reach for disks, my security toolkit and things of this nature. My MP3 collection is also found here.
/data	
/app_data	application data and settings such as Quicken, Opera, Internet Explorer, etc.
/win32	
/src	source code for programs I write or libraries I use
/desktop	desktop or current work folder
/personal	private data such as password list, PGP key pairs, digital certificates, etc.
/Word	document files. I use OpenOffice Writer and save files in Microsoft Word format for cross platform support
/Excel	spreadsheets. I use Kspread and save files in Excel format.
/projects	work folders, divided by project

Notice I save some application data and the synchronization allows functionality similar to Windows' roaming profiles. An example of application data is configuration settings. If I change a setting in my word processor (OpenOffice Writer), say to turn off AutoCorrection, this change will be propagated to all my computers where I use that program. In this case it is my Mandrake and Red Hat Linux and my OpenBSD computer. It is very convenient although not applicable to every application. Using many operating systems increasing the difficulty in setting up such a scheme. For example, I would like to be have all my bookmarks saved and updated automatically. But due to the large differences in how websites are coded, I have to use many browsers (Internet Explorer, Opera, Mozilla and Konqueror). Each browser has a specific bookmark management approach, usually incompatible with others. To make it all work would need to a program that would translate their formats and update each browser. Instead of writing such a program I use Yahoo Bookmarks, the lowest common denominator and a reasonable solution.

To maintain compatibility between Windows and Unix, I save my files in text format or in Microsoft formats like Excel or Word.

A program called Unison does the file synchronization. Unison is an open source and robust program and it works on all my operating systems. It uses SSH so I can secure synchronize from anywhere with an Internet connection (and with firewall rules that allows me to do that).

For simplicity I use a logical star schema where all my computers connect to the server to synchronize. Scripts are used to automate the process. In an effort to conserve bandwidth and time I have three root folders (archive, bin and data). Each has a different synchronization setting. The bulk of my documents are in data directory and this folder that is being synchronized most often, every time I log on a computer and then every five hours thereafter. The bin folder is automatically synchronized weekly and the archive folder monthly.

Password Management

I use a web based perl script (whose URL is found in Resources section) to generate passwords. Then I store them in a text file that I can easily search. I save the website/organization name, my user name and password. This file is encrypted with my master key whose pass code is not written anywhere and it is the one I must remember. Favorite or motivational quotes are used for pass codes to secret keys to make them a bit more fun.

In addition to the master key, I do not write down the PINs to my bank and credit cards and vigorously recommend that no one does either. The stakes become much higher when you have a card number, a name and a PIN written down anywhere. For convenience, I do not keep many such cards (it is better for your credit score anyway) and I use a simple algorithm based on the numbers on the card to determine the PIN. One such algorithm might be the absolute value of five minus the second digit of the number grouping, repeating the subtraction for the first four groups or quadruplets. For example if my bankcard has : 7411 8382 2910 1929, applying the above formula would yield a PIN of 9844. A math enthusiast can use a modulus function, while another might just scramble the numbers in a way that is natural to him/her; the point is not to write it down and to avoid using one's birthrate for the PIN.

How do I protect my privacy?

I give out personal information judiciously. I read privacy policies for websites I frequent and ask for them if they are not readily listed. Merchants are usually required by the credit card companies to have privacy policies. I've found a few and notified them as well as the credit card company (email askvisa@visa.com).

Web Surfing

Spy ware is a direct attack on privacy and I mitigate it by running using Linux and using the Opera browser. On Windows I use Opera as well or Internet Explorer with the High Security setting.

Opera lets me run multiple windows within the browser and it disables pop-up windows with one key (F12). Thus it eliminates the need to run an additional program to control unwanted browser pop-up windows.

I also use a fast public proxy at home for my desktop computers and on my laptop I use anonymizer.com (paid subscription) for complete privacy if I am at work or at a client and would like to check my email.

The proxy server protects my anonymity from the web sites I visit. On the laptop I would like to protect anonymity from the local network as well and anonymizer.com provides a fast and reliable server as well as more sophisticated functions like URL encoding.

Email

I use discrete email addresses for various functions:

- private account to communicate to friends and family only
- public account to email mailing lists, newsgroups, forums
- critical, account for receiving system alerts of all kinds
- spam, account I give out publicly at a industry conferences and the like

These days a lot of websites ask for personal information and email addresses. For trivial purposes (like downloading a white paper or an evaluation program) I sometimes provide fake information (Jonathan Doeh, 789 Main Street, etc.) However, I keep using the same fictitious information for consistency. For email I use a temporary address graciously provided at no cost by spamhole.com. A lot of sites send an email confirmation upon registering and the spamhole address will forward to your real address for a configurable amount of time (I usually pick one hour).

PGP is used for encryption and secure communication. On my Linux machines GnuPG was already installed and integrated into my mail program, kmail. Encryption/decryption can be done automatically or with a touch of a button.

I encrypt my email when sending sensitive information, a rare occurrence in my case. However, every time I post to a public forum or mailing list, I sign my message. It is simply too easy to send spam, trojans or worse, offensive messages seemingly from you and your email address to a public forum. It has happened many times to others.

To include the obvious, I do not run any program that is sent by email, regardless if it's sent by Bill Gates or my mother.

Operating Systems (OS) Configuration

Once my systems are secured I take a baseline so I can automate the process of auditing and intrusion detection.

How do I know if I can trust the information my system is giving me? I use a file integrity checker on every computer: tripwire for Unix and GFI Languard for Windows. Both are great programs that are available at no cost. These programs detect is critical files and programs have been altered. They do so by taking a snapshot of the file's properties and

contents and then it compares against the snapshot. They run periodically (every 5 hours) and send an email if any files have been indeed altered. Tripwire uses an SMTP daemon (like postfix or sendmail) to send email while GFI Languard includes an SMTP server in the program.

How do I know if any attempts have been made to attack my computer? I employ log analysis (automated of course). On my Unix machines I run swatch, a tool that monitors system log entries and provides alerts if it finds items it deems suspicious. It is configured to look for specific anomalies and to send me an email alert upon a match. In general, logs still require periodic human examination. My swatch is configured to be highly sensitive so I receive alerts once in a while that prompt me to examine the logs.

On Windows systems I use scripting to achieve this automation. A program called dumpel can copy the system log to a text file. Then I use perl to parse the file, that is, to look for suspicious patterns. Perl is installed with Cygwin. On Windows systems I do not run an SMTP server so in case there is something suspicious, the results are written to a text file that is being watched by GFI Languard (the file integrity checker). When this results file changes, GFI Languard will send me an email alert.

Setting up all these scripts took a little patience and skill but luckily Steve Elky has done an exceptional job at documenting this topic and providing example scripts. The paper, hosted at SANS, is oriented at the corporate setting but it can be easily adapted to individual use.

On the server I initially used PortSentry, a program that monitors the servers' ports in order to detect if someone is scanning them. Scanning ports is typically the reconnaissance prior to an attack. PortSentry will log the action and take evasive measures by dropping any responses by the system to the attacker's IP address. It is effective although I do not use because outside scans are blocked by the firewall appliance. I also run port scanners against the server myself to verify its security and PortSentry had to be manually stopped to in order to do so. The cost to convenience was large while additional security benefits were small.

Another approach in limiting port scanning is personal firewalls. For convenience I use the default firewall of my Unix systems (shorewall on Linux, pf on OpenBSD). On Windows I use ZoneAlarm. All firewalls are set to reject all connections to ports not explicitly specified as well as limit certain types of ICMP packets. My firewall logs are automatically submitted to dshield.org periodically to help with worldwide attack correlation. On Windows systems I enable TCP/IP filtering for an additional layer of protection should ZoneAlarm be compromised or misconfigured.

There are additional intrusion detection measures one can take, however keeping risk and convenience in mind, I stop with the measures described above. On Windows systems, some intrusion detection functions are integrated into software firewalls (such as Privatefirewall from privacyware.com).

Every time I log into a computer a script is executed that will attempt to:
1)synchronize my files with the server
2)verify key processes are running (like intrusion detection, log analysis, etc)
3)verify the last time I logged into the computer matches its records (a text file)
4)update the file to include this login time and date.

I use a text file to keep track of my login behavior because it is an additional security measure and it works across multiple operating systems. Operating systems also keep track of this information but there are automated tools to alter this information to hide the tracks of an attacker. If my system is compromised, nothing stops the attacker from modifying my text file as well. However it is an additional step that the attacker might or might not take.

Usually once a month, I run some security programs on my computers to verify their state. These are port scanners, vulnerability scanners and rootkit detectors. At the moment it is a manual processes that takes me about 25 minutes. I am planning to automate them to have each computer scan each other periodically and parse the results against a known baseline.

General

Whenever I'm home and go to sleep, I turn all my computers off and turn off the cable modem as well by using a central power console; keeping in compliance with the aforementioned security tenet to run only what's absolutely necessary.

I rarely have a need to install computer programs from the internet and when I do I verify their authenticity. In Unix I can do this with *rpm –checksig* or comparing md5 fingerprints..

I regularly donate to organizations like EFF and ACLU, which keep me privy of important updates and fight to protect the privacy of the individual.

Summary

Once past the initial cost of installation and setup, the time spent on maintaining your systems shouldn't be a significant. You should receive alerts for anomalies and most daily tasks should be automated. My personal setup is not meant to be followed blindly; it is simply a manifestation of the general guidelines and something that works well for me. It is not hacker proof, nothing is, but it significantly raises the skill level and time required to compromise your system(s).

Network Associates and Symantec sell all in one security products, and with annual subscriptions your time investment is greatly reduced for this area.

The primary goals of information security are confidentiality, integrity and availability. That is, information should be available only to the right people, should be modified only by authorized people and be accessible. The most effective method to achieve these goals is a vigilant and informed population.

Some guiding principles of security are:
1)defense in depth (use many layers of security measures)
2)less is more (use only programs or functionality you truly need)
3)simplicity beats complexity (the simpler the system, the easier it is to understand it and secure it).

Applying these principles along with definition of risk to your daily computing (and other activities) will significantly increase your privacy. From the examples given above, it is feasible to achieve an adequate level of security with minimum hassle and maximum functionality.

List of References:

1. National Highway Traffic Safety Administration. “Traffic Safety Facts 2001”. December 2002. URL: http://www-nrd.nhtsa.dot.gov/pdf/nrd-30/NCSA/TSFAnn/TSF2001.pdf

2. Gibson, David. “ Security In-Depth for Home-based Networks with an “Always-on” Internet Connection” November 20, 2002. URL: http://www.giac.org/practical/David_Gibson_GSEC.doc

3. Porter, Brian. “Security and Privacy at home”. November 5, 2002. URL: http://www.giac.org/practical/Brian_Porter_GSEC.doc

4. Blauvel, Brad. “HOWTO: Logon Scripts as Anti-Virus Tools”. October 2, 2002. URL: http://www.giac.org/practical/Brad_Blauvelt_GSEC.doc

5. Luhn, Robert and Spanbauer, Scott. “Protect your PC” . PC World Magazine. July 2002. URL: http://www.pcworld.com/reviews/article/0,aid,97430,00.asp

6. Carnegie Mellon, Software Engineering Institute, CERT Coordination Center: “Home Network Security” December 5, 2001. URL:http://www.cert.org/tech_tips/home_networks.html

7. Miller, Michael. Absolute PC Security and Privacy. Sybex, August 2002.

8. Gralla, Preston and Schaeffer, Jody. Complete Idiot's Guide to Internet Privacy and Security. Alpha Books, January 2002

9. Sowerby, Mark. “SSH, a practical guide to installation, configuration, and use.” October 23, 2002. URL: http://www.giac.org/practical/Mark_Sowerby_GSEC.doc

10. Security Watch. PC Magazine. URL: http://www.pcmag.com/category2/0,4148,12,00.asp

11. Smith, Randy Franklin. “Dangerous Services, Part 1”. Security Administrator. December 7, 2000. URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16301

12. Smith, Randy Franklin. “Dangerous Services, Part 2”. Security Administrator. December 21, 2000. URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16363

13. McGuire, Thomas. “Windows 2000 Services Tweak guide”. Techspot.com. March 26, 2001. URL: http://www.3dspotlight.com/tweaks/win2k_services/index.shtml

Resources

Read an overview of anti-virus scanners from alt.comp.virus newsgroup participants:
http://www.claymania.com/anti-virus.html

AVG Anti-Virus from Grisoft is a great no cost anti-virus scanner:
http://www.grisoft.com/

TrendMicro HouseCall is a web based no cost anti-virus scanner that runs within Internet Explorer: http://housecall.trendmicro.com/

Read a PC World article on how personal firewalls work:
http://www.pcworld.com/howto/article.asp?aid=17012

For software reviews that should help selecting a personal firewall, go to firewallguide.com
http://www.firewallguide.com/software.htm

ZoneAlarm is a great personal firewall and a no cost version is available.
http://zonealarm.com

Read 'Spyware: Read the End User License Agreement – Users Beware!" by Junadi Junadi for an introduction to this topic:
http://www.giac.org/practical/GSEC/Junadi_Junadi_GSEC.pdf

Go to spywareinfo.com for more resources on spyware, including online scanners
http://www.spywareinfo.com/

General privacy portal with news and resources:
http://www.privacy.org/

The Electronic Frontier Foundation (EFF) is a non-profit group working to protect an individual's digital rights: http://www.eff.org/

The American Civil Liberties Union (ACLU) is non-profit group with a more expanded scope than EFF: http://www.aclu.org/

Read a PC Magazine article comparing various broadband routers (dated February 2002)
http://www.pcmag.com/article2/0,4149,223571,00.asp

The about.com guide to using remailers to protect your anonymity when sending email
http://email.about.com/cs/remailers/

Read the anonymous remailers FAQ (frequently asked questions) :
http://www.mit.edu/activities/safe/fighting-back/anonymous-remailer-faq

Google directory of free proxy servers, to protect anonymity when web browsing.
http://directory.google.com/Top/Computers/Internet/Proxies/Free/

The Windows 2000 Professional Baseline Security Checklist is good resource for hardening the operating system:
http://www.microsoft.com/technet/security/tools/chklist/w2kprocl.asp

Use Microsoft Baseline Security Analyzer for Windows computers:
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q320454&ID=KB;EN-US;Q320454&

Read "Windows XP: Your Definitive Lockdown Guide" for tips on securing Windows XP:
http://www.windowsecurity.com/articles/Windows_XP_Your_Definitive_Lockdown_Guide.html

Counterpane log analysis list of resources and links:
http://www.counterpane.com/log-analysis.html

Read "Automated Auditing in a Windows 2000 Environment" for pointers and tips on using scripting to automate auditing:
http://www.sans.org/resources/auto_audit.php

The online password generator of personal preference:
http://geodsoft.com/cgi-bin/password.pl?back=/howto/password/password_admin.htm%23psr2

Unison replication program, an exceptional synchronization program
http://www.cis.upenn.edu/~bcpierce/unison/

See Unison user group for specific questions not addressed by the documentation
http://groups.yahoo.com/group/unison-users

Cygwin is a Unix environment for Windows and required for using Unison over ssh.
http://www.cygwin.com/

OpenSSH is a no cost implementation of the ssh protocol suite to enable secure communication：http://openssh.org/

Read a Cygwin and OpenSSH installation tutorial
http://tech.erdelynet.com/cygwin-sshd.html

GfiLanGuard System Integrity Monitor for Windows. It is a free, simple and effective program: http://www.gfi.com/lansim/

"Life Without NetBIOS" explains how to turn off NetBIOS in Windows 2000 as well as the benefits of doing so: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=21537

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive