Consumer Oriented Security Information:

Common threats on the Internet and how to avoid them

By Dave Cadrette

November 10, 2003

GIAC Security Essentials Certification
Practical Assignment Version 1.4b

Abstract

As more and more people connect to the Internet, ill intentioned people see new and undereducated users as ripe for the picking, and unfortunately, that does seem to be the case. It is crucial that even experienced users alert themselves to the dangers lurking as they connect to the World Wide Web. Information security threats come in many forms, and in a variety of camouflage.

This discussion will touch on many of the perils that users may encounter, and the techniques and technology they can use to protect themselves and their data. Strategies regarding operating system updates, anti-virus software, and personal firewalls are discussed. Spyware is another ubiquitous presence on the Internet that contains hidden and potentially dangerous technology. Fortunately, for consumers, there are cryptographic technologies to help keep “secure” transactions truly secure, and by following some simple safe computing practices, users can significantly reduce the risk they face when connecting to the Internet.

Introduction

As more and more people begin to use personal computers at home, and increasingly use the Internet for conducting various business, from banking to shopping, chatting and emails, it seems there is a frightening array of threats, that in this writer's opinion, are understated, and at least from the mainstream media perspective, misdirected – resulting in an under-educated user base and an ever-expanding list of potential exploits for the multitude of devious and malicious people to take advantage of. Fortunately for us, there is also a wide array of devices and technologies to help protect the consumer. While the Internet is ripe for nefarious activity, it is also far from the only risk facing the average consumer. Things like identity theft often begin in unassuming ways – the Internet has only made it easier to take advantage of any ill-gotten information.

Information security threats come in many forms, such as viruses and worms, but can take the form of an email masquerading as legitimate, referring the user to malformed or phony web pages (referred to as "phishing"), and so on.

For the purposes of this discussion, the focus will be on Microsoft Windows, due to the prevalence and large-scale deployment on the average home users' computer. Microsoft is estimated to have anywhere from a 90% to 95% market share for all desktop computers, with some estimating an even more dominating number of over 97%[1]. According to the Computer Industry Almanac, in 2002, there was an estimated 663 million computers in use worldwide. [2] In the United States alone, the number of computers connected to the Internet is in the neighborhood of 160 million.[3] Considering that the vast majority of computers are Microsoft-based, the security shortcomings inherent in Windows are an easy target for hackers and the like.

Based on the speed with which the recent "MS Blaster" worm spread, it is also exceedingly obvious that most users do not recognize the likelihood that a much more malicious worm using the same or similar vulnerabilities and techniques could cause significant damage to any given computer. It also brings to light the complacency of many computer users to assume that they are safe from infections. More importantly, and probably the most significant ally to the hacker is the fact that most users do not have the technical savvy to actually keep their systems protected. Even users proficient in the use of email, word processors, and other typical consumer uses are more often than not relatively inexperienced in matters of system and data security. The potential for a computer worm or virus to cause widespread damage will never really be preventable, precisely for those reasons.

[1] OneStat.com, Microsoft's Windows dominates the OS market on the web
[2] The Computer Industry Almanac, Worldwide Cumulative PC Sales Exceed 1 billion
[3] The Computer Industry Almanac, USA tops 160M Internet Users

Another, less obvious threat, is the proliferation of so-called “spy-ware” and other mechanisms designed to track and catalog online behavior. The possibilities for misuse of personal identification may seem remote or sometimes far-fetched, but I am consistently amazed by the amount of information the average consumer is willing to release to companies that make no bones about their intention to use, share, and sell personal information to anyone willing to pay for it. There are also other unsavory items like keystroke loggers available in hardware and software versions that can compromise a system.

There is a long list of products available to consumers, many of which work as advertised, but others that fail to live up to the high expectations set by the marketing departments. Anti-virus software, personal firewalls, spyware detectors, and so on, can all provide varying levels of protection from disreputable individuals or websites. Technology to protect sensitive data is also evolving, including new encryption standards, smart cards, and even automated updates from Microsoft designed to keep your computer patched and protected from the latest and greatest vulnerabilities. In addition, laws and regulations are constantly evolving, as the federal and state governments try to assist. As part of any overall security strategy, however, consumers must protect their data from as many angles as possible, and cannot rely on new laws to save them from attack. After all, there is no question that whether malicious behavior is explicitly outlined by some well-intentioned legislation or not, the hacker by design is skirting the law when stealing information.

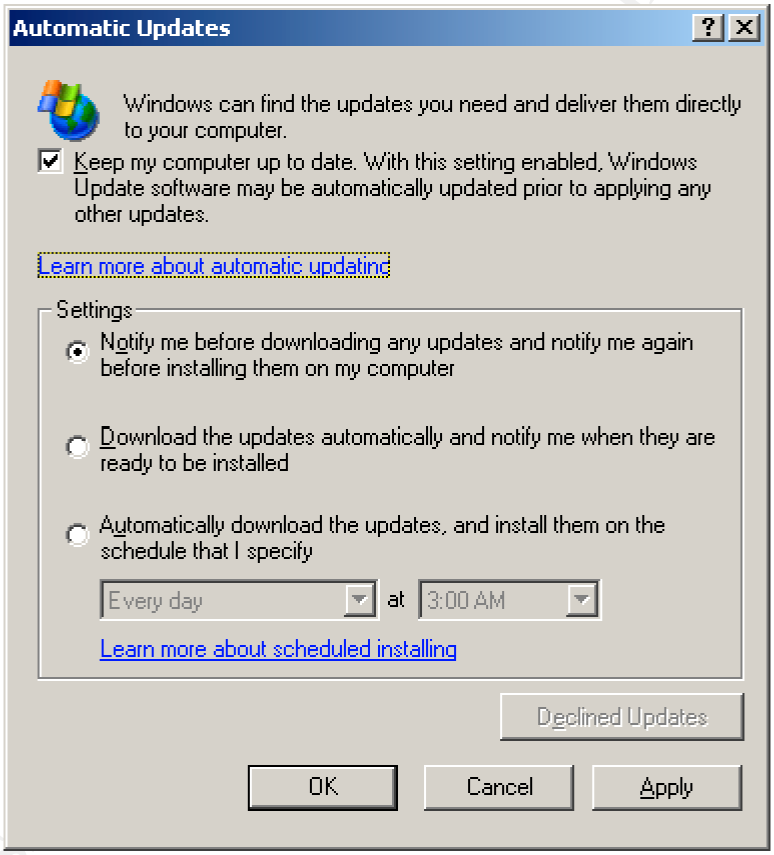
Operating System Updates

First and foremost, any defense-in-depth tactics should begin by keeping the operating system on their PC up to date with the latest security fixes from the publisher. For the corporate computer user, there will generally be some type of system administration structure in place to either assist users or provide instructions for patching systems, and many organizations have tools in place to “push” updates to desktop computers. In addition, there are often other layers of security at a corporate level to help protect desktop PC’s. Unfortunately, home users do not have the same benefit of built-in system administrators and help-desk support, so they must be conscientious and thorough when setting up and maintaining their systems.

In the case of Microsoft Windows, Microsoft has attempted to make the task of tracking the multitude of hotfixes and updates somewhat less convoluted using the web-based application Windows Update.

The Windows Update tool can be accessed from any number of locations within windows, like within the Windows Control Panel, or via shortcuts on the Start Menu, but most commonly from within Internet Explorer. In an open browser, users can click Tools=>Windows Update, which will connect to the Microsoft site http://windowsupdate.microsoft.com - from there, Microsoft uses a JavaScript applet to check your computer's operating system and patch level. Used regularly, this tool can effectively keep your computer secure, at least from operating system vulnerabilities. Microsoft Windows 2000 and Windows XP also offer completely automatic updating – there is a good level of granularity, from simply being notified that updates are available to having them automatically downloaded and installed with no intervention, and scheduling the updates for any convenient time – but no less than once a week if choosing this option. Figure 1 shows a screen shot of the Windows 2000 Automatic Updates dialog, showing some of the options available for automatic updating. Users can change these settings by accessing the "Automatic Updates" icon in Windows 2000/XP.

Figure 1



Automatic Updates

Windows can find the updates you need and deliver them directly to your computer.

☑ Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

Settings

● Notify me before downloading any updates and notify me again before installing them on my computer

○ Download the updates automatically and notify me when they are ready to be installed

○ Automatically download the updates, and install them on the schedule that I specify

Every day at 3:00 AM

Learn more about scheduled installing

Microsoft attempts to make the process of updating Windows relatively painless, but occasionally will offer updates and fixes that can cause other unrelated issues to occur. Having the computer set to have every update automatically download and install without intervention may sound appealing, but there have been cases where the "cure" was worse than the potential problem. On the other hand, for users who would otherwise be unable to discern what a truly critical or necessary patch is versus simply installing all available updates, would clearly benefit from the latter option. To take advantage of things like automatic and scheduled downloads, however, the user must be connected to the internet essentially continuously (likely through a broadband connection), which brings it's own host of issues, not the least of which is that the computer could be infected or attacked before the updates are installed, if the user has not installed a patch by the time an exploit is "in the wild".

The issue of patching operating systems is becoming more and more of an issue, especially of late, since Microsoft has released a significant number of patches since September 2003, increasing the possibility that users may ignore new fixes, assuming new articles they read or stories they hear relate to previously installed updates. There is no simple solution to the issues with patching Windows, but end user education is key in any scheme.

Anti-Virus Protection

Another critical step in defending your system from attack is an up-to-date anti-virus program. Viruses in all their forms, from self-replicating worms, dubious executable files, Trojan Horses, macro viruses, and the latest term – "blended threats" combining one or more techniques of infection. New viruses are discovered every day – and require diligence to keep the detecting software current. According to Symantec, the anti-virus signatures they offer for their Norton Anti-Virus product detects over 65,000 different virus threats.[4] F-Prot, another anti-virus vendor, professes to detect over **99,000** different threats.[5] Using either claim as a frame of reference, it is easy to see that the variety and sheer number of viruses potentially poised to infect a computer requires some type of protection.

There are a fair number of products available that offer protection from viruses – some may require subscription fees to continue receiving updates, others do not, but all purport to protect your system against viruses, and with subtle differences, most will do an adequate job. Some of the better-known products are listed in Table 1 for your reference:

Table 1

Product	Publisher	Web Site
Norton AntiVirus 2003	Symantec	http://www.symantec.com
McAfee VirusScan 8.0	McAfee	http://www.mcafee.com
Sophos AntiVirus 3.0	Sophos	http://www.sophos.com
F-Prot AntiVirus 3.14	Frisk Software International	http://www.f-prot.com
PC-Cillin 2003	Trend Micro	http://www.trendmicro.com
F-Secure 2003	F-Secure	http://www.f-secure.com
ETrust EZ Antivirus	Computer Associates	http://www.my-etrust.com

[4] Symantec, Updated Detection List
[5] F-Prot Product Information

All of the software listed above will assist in defending your computer against known viruses, but risks still exist – it is critical to regularly update whatever software is installed to maintain protection against new and always changing viruses. In many corporate environments, virus definitions are "pushed" to the desktop computer by a central server, making it transparent to the end user. For a home user, however, some type of scheduled updating or regular manual intervention will be required. Some would argue daily updates are required, though once or twice a week should prove more than sufficient in most cases.

Many of the delivery methods for viruses capitalize on the average users' "bad" behavior or other social engineering methodologies to assist in the spread of the virus. One only needs look back to the "I Love You" virus in May 2000 to see how user behavior can impact the spread of a virus. This particular worm required the user to open an attachment in an email before it could infect a system. Even though there was widespread publicity about the threat and how it spread, it continued to wreak havoc for several days.

As is the case with operating system updates, we return to the issue of user education to protect themselves from threats. There are a lot of things a home user can do to mitigate some of the techniques virus writers use to distribute their handiwork. Most are based in common sense, but it seems that less experienced users do not always follow generally accepted "safe" practices.

Personal Firewalls

As more and more users utilize broadband Internet connections, the threat of system compromise is greatly increased, since the computer will generally be connected to an "always-on" kind of setup. In fact, in the United States alone, the number of users subscribed to either cable or DSL broadband service is approaching 20 million. [6] This is a number that can only be expected to grow – worldwide, it is estimated that cable modem subscribers will number 37 million by 2007.[7] A personal firewall is one way that a broadband user can help to diminish the ability of a hacker to break into a computer.

A firewall is either a software program or hardware device that sits logically (software) or physically (hardware) between the Internet and the computer. Firewalls are essentially traffic filters that act to prevent malicious users from using openings in the network to gain access to the PC. Various methods for accomplishing this are used, commonly packet filtering, which can classify a packet by IP address or application and allow or deny access based on a set of rules. More advanced firewalls sometimes use a method of filtering called "Stateful Inspection". This is a method of filtering that goes beyond just opening or closing a given port, or restricting by a given application (i.e. FTP). Searching for a comprehensive definition of what exactly this means resulted in several

[6] CyberAtlas, Broadband Based On Behavior
[7] CyberAtlas, Worldwide Cable Modem Subs Expected to Double By 2007

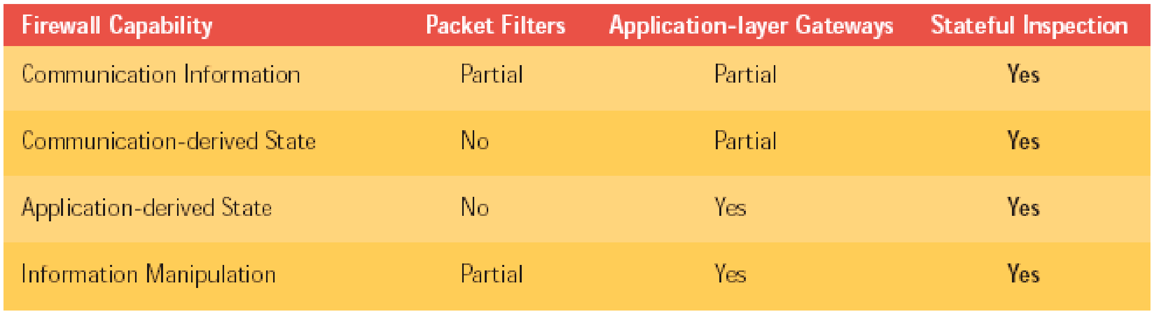
variations on what exactly this means, but it is commonly accepted that Checkpoint Software Technologies, a firewall vendor, essentially created the technology and even received a patent for it.[8]

According to Checkpoint:

> “With Stateful Inspection, packets are intercepted at the network layer for best performance (as in packet filters), but then data derived from all communication layers is accessed and analyzed for improved security (compared to layers 4-7 in application-layer gateways). Stateful Inspection then introduces a higher level of security by incorporating communication- and application-derived state and context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. It also delivers the ability to create virtual session information for tracking connectionless protocols (e.g. RPC and UDP-based applications), something no other firewall technology can accomplish.”[9]

Checkpoint also offers a comparison chart of firewall technologies for reference, reproduced in Figure 2 here, from http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf:

Figure 2



Firewall Capability	Packet Filters	Application-layer Gateways	Stateful Inspection
Communication Information	Partial	Partial	Yes
Communication-derived State	No	Partial	Yes
Application-derived State	No	Yes	Yes
Information Manipulation	Partial	Yes	Yes

Another method of filtering is by application, or as referred to in Figure 2, Application-Layer Gateways. With this method, traffic is allowed or blocked based primarily on the application in use (e.g. telnet, HTTP, etc.), not by port.

There are many different products available to the consumer, some that are free, and others costing hundreds of dollars. It is beyond the scope of this discussion to perform any comprehensive review or comparison of the multitude of products in the market. One question that can be considered is whether a dedicated hardware device or a piece of software is better suited for the home user. It can be argued that there is really no difference between hardware and software, since even a hardware device is running some type of software to process the rule sets. Since a hardware device is dedicated to a particular function, however, it can be expected that there will be performance improvements. On the negative side of the equation, though, a dedicated device will likely cost more

[8] CheckPoint Software Technologies Press Release

[9] Checkpoint Software Technologies, Stateful Inspection Technology

than a comparable software product, though this is not always the case. For the purposes of this discussion, the focus will be software, given that most average consumers would likely shy away from a dedicated device, with occasional exceptions, of course.

In strictly hardware terms, however, for the casual home user with a broadband connection, it makes sense that some type of switch or router is installed between the Internet connection and the computer itself, which will provide some firewall-type protections, including Network Address Translation (NAT). Basically, the router keeps the connection to the Internet segregated from directly connecting to the computer's network connection. The router assigns a private IP address to the internal computer(s), and the router presents a single public IP address to the internet facing connection, protecting your computer from direct port scans and other malicious activity. Most routers designed for home use have many lesser-used ports closed by default, with standard ports open (like HTTP [port 80] and FTP [port 21]).

Newer versions of Microsoft Windows also include some built in firewall capability, though it has some limitations in terms of configuration. Microsoft's version, referred to as the "Internet Connection Firewall" (ICF), is a "stateful" firewall – which means the state of communication is continuously monitored and updated, and the firewall will only allow inbound communications when the internal or private computer has initiated the connection. When lacking any other firewall, it is a reasonable protection, though it has limitations. For instance, when using the Internet Connection Sharing feature of Windows, the ICF will prevent any computer other than the computer actually running ICF from receiving any traffic – since the ICF computer does not initiate the connection. Obviously, this defeats the purpose of Internet Connection Sharing, so when setting up a home network, this is an important consideration. ICF also allows pass-through connections to authorized services that may require it, like if you are running a web server.

Most of the consumer-oriented software firewall products available have been summarized and reviewed by different publications – many products have some type of trial package for download. A quick search of the Internet listed page after page of product reviews and comparisons. One of the more easy to use and up date lists was on the PC Magazine site, "Software Firewall Product Guide", at http://www.pcmag.com/category2/0,4148,4722,00.asp

In any case, a firewall is only one part of an overall security strategy. Holes that are left open by the firewall for legitimate purposes can also be used for worms or virus exploits. This is exactly what the MS Blaster worm took advantage of, demonstrating the need for a more comprehensive approach.

The Threat of Spyware

One of the more pervasive threats to consumer information is spyware (sometimes referred to as “adware”). While usually not a direct threat to your computer system, small programs installed with or without the users’ knowledge have advanced capabilities to collect and share personal information, and track internet usage. Some of the information may be somewhat innocuous, but more disconcerting is the privacy policies (or more appropriately, the information sharing policies) of many of the ever-present and more popular downloaded or bundled software program publishers.

Some of the more invasive spyware programs may hijack system settings, connect to the Internet without your knowledge, modify browser settings, create pop-up ads even when your browser is not running, and more – some behaviors are not too distant from what virus writers try to accomplish. Some examples of the types of software that are bundled with other programs, and often installed when downloading things like free games:

• Gator	http://www.gator.com
• Bargain Buddy	http://www.exactadvertising.com
• BonziBuddy	http://www.bonzi.com

All three of these programs try to deliver targeted advertisements, which in and of itself is not necessarily a bad thing, but according to Spyware-Guide.Com (http://www.spywareguide.com/index.php), they also have the following behaviors:

- Stay resident in background
- Stealth: hides itself from user
- Makes changes to browser settings
- Connects to the Internet by itself

There is a ton of useful and informative information available from many sites on the Internet about the perils of installing these programs. Unfortunately, some programs will not work if the bundles are uninstalled. The best course of action is not to install that type of program in the first place.

Beyond programs that users may be aware of, users happening upon malicious websites or signing up for unrealistic contests could be the victim of a hijacked browser. Generally, the hijacker will change default browser settings, along with other background settings changes. For instance, responding to a pop-up ad for “Free Scratch and Win”, with a chance to win some vague prize, will result in several changes to your computer:

- It changes home page and search page settings to point to http://xzoomy.com, and complains if you try to change them back.
- Opens pop-up advertisements every few minutes.

- Downloads and installs arbitrary unsigned code as part of an update feature

In addition, the software's terms of use go into greater detail about the invasiveness of the program. Since I find the blatant misuse of users' naiveté to be especially disturbing, some of the terms are reproduced here[10]:

- I understand that by accepting these terms and conditions, this program will be installed on my computer and my web browser home and search page will be changed in order to allow me access.
- In order to use this program, I understand that I will need an Internet connection that makes contacting the FreeScratchAndWin.com server possible, and I understand that any charges incurred for connecting to the Internet are at my own expense.
- I further understand that search tool bar will be added to my web browser which will remain visible as long as the software is installed and agree that I wish to use your search engine for my web browsers default error page.
- To insure you always have the latest version and for your convenience this software will automatically update itself from time to time once installed. Also we will download other companies programs to your computer which you will have the choice to install or not install once downloaded.
- If you decide to change your homepage at a later date we will ask you each time you use our program if you would like to set your homepage to our search engine.
- I understand that, by accepting these terms and conditions, bookmarks will be added to my favorites.
- In order for us to keep this software free we will open advertisements while you surf the web.
- To prevent your browser from becoming cluttered when our toolbar is installed, any other toolbars you currently have visible will be deactivated. They can be restored manually through the Internet Explorer "View" menu.
- Once installed if you decide to change your start or search page this information will be sent back to our server. Also information in regards to your browsing will be sent to our servers, such as how long you surf for, and your surfing habits.

The plain truth, in this writers' opinion, is that the everyday user does not look twice at these terms, which fly by during the installation process with a simple click. I think if one were to be verbally asked if it was acceptable for all of this to take place on their computer, the answer would be no. Unfortunately, some of these programs can be installed with a misleading dialogue box or other hidden method, meaning the user didn't know it was installed at all. One of the more notorious stealth browser hijackers is "CoolWebSearch" (http://www.coolwebsearch.com). This product goes as far as to modify the Microsoft Windows hosts file, changing it so that MSN Search, Yahoo Search, and Google are pointed to the local host address (127.0.0.1), rendering them essentially useless, and pointing to it's own search engine instead.

Many banner ads or pop up ads presented as you surf the internet also contain "cookies", which are small text files kept on your computer, and they can be used to track various information. Cookies in general can be very useful, by saving

[10] Free Scratch and Win, Terms of Service

page preferences or information to make the Internet surfing experience more personalized. For instance, if you visit a web site that allows you to customize the information presented to you (like search preferences, page layout, etc.), that information is often kept in the form of a cookie. The next time you visit the site, it references the cookie, and displays the page based on that information. On the negative side, cookies may contain personally identifiable information, and may be used to track your surfing behavior, and so on. Cookies do not represent the same type of invasive threat that actually installing a program can be, but privacy policies of some companies call into question what happens with the data once they collect it.

Thankfully, there are a number of products available that will assist in the detection and removal of these products. Many are available for purchase, but there are many high quality programs that are free. Specifically, one of the consistently highest rated and popular programs of this nature is "Spybot Search and Destroy", whose home page is http://security.kolla.de/.

This particular program is a CNET[11] and PC Magazine[12] Editor's Choice, which only represent 2 of many other positive reviews. The program detects virtually all known adware and spyware, allowing removal, or exclusion, if you want to keep it. Downloading regular updates is a must, since the landscape is always changing. The program is easy to use and install, and provides a good deal of information about the software it finds on your computer, including links to privacy policies, publisher home pages, and so on. The best feature of all is the cost – it is free. Every home user should be conscious of what is happening on their computer, and Spybot Search and Destroy gives great insight to that end.

Technology to Protect Data

Being aware of the threats and concerns facing the average computer user is all well and good, but technology to assist consumers and protect data is also evolving. Being aware of the available technologies allows consumers to make informed choices about firms and websites they do business with, to ensure that their data is protected.

First and foremost, users should make sure that communications with websites where sensitive data is exchanged (financial information, etc.) is encrypted. You can think of encryption as a sealed envelope protecting each packet of data, except with the 128-bit scheme in use today, no one would be able to open the envelope without the proper key.

Today's cryptography methods operate with a two-way process (as does all cryptography) – essentially, the raw data (often referred to as plaintext) is

[11] Spybot CNET Product Review
[12] Spybot PC Magazine Product Review

scrambled with a mathematical algorithm. Part of the equation is a key, which when used in the encryption formula, results in encrypted data (ciphertext). In order to unscramble the data, the receiver of the data performs a similar mathematical process on the ciphertext. The important factor in this process is that the same key must be used to decrypt the data. It follows, then, that the length of the key is an important feature in the encryption process. A longer key is inherently harder to guess, given the exponential increase in possible combinations.

There are two types of cryptographic communications commonly used:

- Symmetric, or private-key cryptography, where the sender and receiver use the same key for both encryption and decryption.
- Asymmetric, or public-key cryptography, where the sender encrypts with a private key, and then the receiver decrypts the data using a mathematically related public key. This is the underlying method used in most secure Internet transactions.

When communicating securely on the Internet, many enterprises use a Public Key Infrastructure (PKI) model. With this structure, there is more than simply encryption and decryption involved. For a complete solution, digital certificates, public-key cryptography, and certificate authorities are all incorporated into a total, enterprise-wide network security architecture.[13] Digital Certificates are usually provided by a trusted third party (a certificate authority), and are supported in most modern browsers. There are a number of standards in terms of certificates, but they all work the same way. A certificate is installed on a server, which contains a private key, along with a corresponding public key. These certificates can be issued from any number of providers. On the Internet, there may be a hierarchical certificate chain, wherein one certificate testifies to the authenticity of the previous certificate. At the top level of the hierarchy is a “root” certificate, which is trusted without a certificate from any other certifying authority.[14]

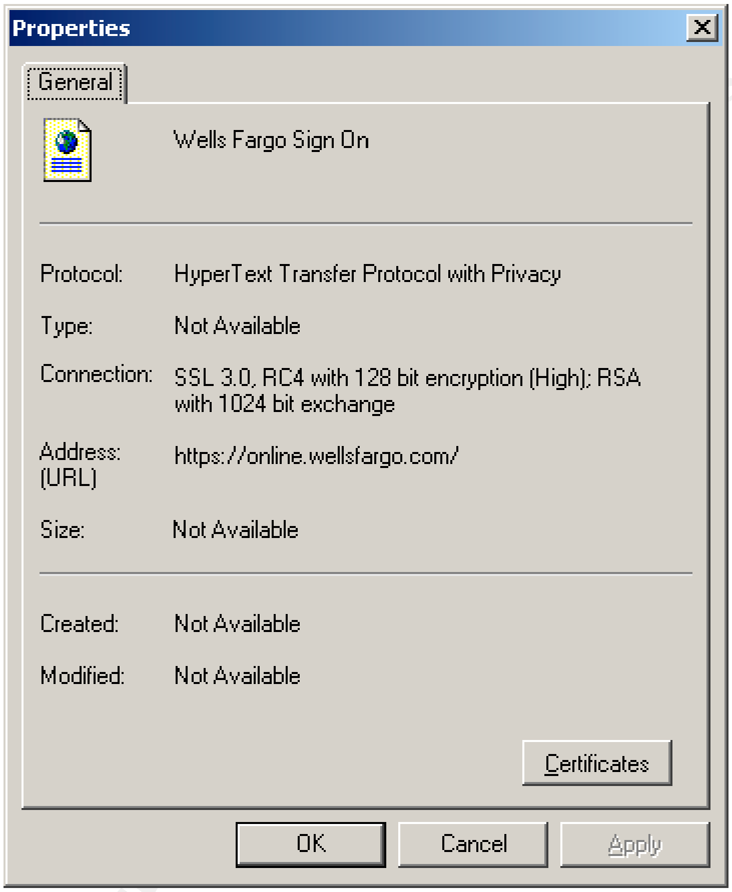
A list of trusted root certificate authorities is included with default installations of Microsoft Internet Explorer. To view the list, from Internet Explorer, click Tools=>Internet Options, the Content Tab, and then click on Certificates. Another box will open, where you can choose the Trusted Root Certification Authorities tab, and be presented with a list of the root publishers.

Using Internet explorer on a secure site, a padlock will appear in the lower right hand corner of the browser (🔒). Hovering the mouse pointer over the symbol will indicate the level of security in use (56 bit or 128 bit). Double click on the padlock, and a window will open detailing the certificate in use. Similarly, clicking

[13] Verisign, Understanding PKI
[14] RSA Security, How Are Certificates Used

File=>Properties will provide more detailed information relative to the actual algorithms in use. As shown in Figure 3, the particular connection is using “SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange”. Further explanation follows.

Figure 3



Wells Fargo Sign On

Protocol: HyperText Transfer Protocol with Privacy

Type: Not Available

Connection: SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange

Address: (URL) https://online.wellsfargo.com/

Size: Not Available

Created: Not Available

Modified: Not Available

Figure 4

SSL 3.0 = Secure Sockets Layer version 3.0, a standard for secure communications originally developed by Netscape. SSL uses cryptography for security - in the above example, it uses RC4.

RC4 = An encryption algorithm developed by RSA Security. According to RSA, this algorithm is based on a random permutation.[15] 128-bit encryption means that the key in use is one of 2^{128} different possible combinations. To give some perspective, this adds up to 3.4 x 10^{38} different permutations. If this number represented milligrams, it would represent weight equal to nearly 57 million planet Earths. Needless to say, this is very secure.

[15] RSA Security, What is RC4

Safe Computing Practices

So, we know that Internet communications can be encrypted in such a way as to make the data virtually unattainable through existing brute force methods. Clearly, hackers and identity thieves look to other avenues to gain access to data and documents.   It is increasingly important for every Internet user to educate themselves to help protect their computer - and their identity - from trouble. At the very least, following several relatively simple practices when using the Internet can significantly reduce the risk of attack or infection.

Privacy and Email

Many sites have privacy policies about how they deal with your personal information. While it is probably unrealistic to expect to read every policy from front to back – and understand it all, it is important to be aware that there are sites and gimmicks to try to encourage you to divulge personal information. Free downloads, “Sweepstakes” entries, and phony web pages trick unsuspecting users all too often into revealing extremely damaging information, notably credit card and social security numbers. Junk emails also serve as an effective conduit to obtain this information, as evidenced by the flood of Spam that affects nearly everyone with an email address.

If you must sign up for that free chance to win a million dollars, or a trip to <enter destination here>, or if you have already won a valuable prize – exercise caution! When giving out your information, do not use your primary email. It is a reasonably painless process to set up an email address using a free service such as Hotmail or Yahoo. Use this secondary account for those purposes – that way, if you begin receiving too much junk mail, you can simply stop using it – and create another account.

Always treat uninvited email with caution - above all if it includes an attachment. Never open any attachment you are not expecting or that is received from unknown people. Also, never respond to a spammer directly, since that often only validates your email address as genuine.

A more recent phenomenon is called “phishing”. A criminal sends an email purporting to represent a well-known company (e.g. Paypal, eBay, financial institutions, etc.), which when responded to, direct the user to a phony web page, disguised to look authentic. At that point, they ask for information that a reputable businesses would have no need for – like a social security number, along with credit card numbers and the like. Most sites contain detailed information about what types of email they will send and what information they will never ask you for. eBay, for example states:

> “eBay will never ask you to provide sign-in passwords, credit card numbers, or other sensitive information through email. If we request information from you, we will always direct you back to the eBay site. With very few exceptions, you can submit the requested information through your "My eBay" page.”[16]

Occasionally, some businesses may even send an official notice in response to a flood of reported spoof emails to all users. The key to avoiding these scams is to make sure that whatever site you are visiting is genuine. Rather than clicking a link in an email, visit the site through a URL you know to be legitimate.

Finally, passwords for all of your account should be kept secret. Just as you would not make copies of your car and house keys and leave them laying around for anyone to make use of them, or leave your doors unlocked for that matter, passwords must be considered with the same sense of security. Make it easy for you to remember (a childhood address, for instance), but hard for others to guess. A mixture of letters and numbers is good – but a pass phrase is better, since the length of the password will decrease the likelihood of a brute force attack being successful. Changing passwords regularly is a good habit to get into as well.

The Federal Trade Commission maintains several web pages offering tips to avoid scams, report abuse, and minimize the risk of identity theft, and many other Internet and E-Commerce topics. Visit http://www.ftc.gov/bcp/menu-internet.htm for much more useful information.

Protect the connection

There are certain measures all users should take to protect their computer from digital intrusion, whether through a worm or virus, or a disreputable user looking for exploits, beyond simply being cautious when releasing personal information.

Use of a personal firewall can be an effective safeguard against exploits and worms that take advantage of little-used ports, and from hackers scanning the Internet for similar vulnerabilities. They run the gamut from a free download to a dedicated hardware device costing a few hundred dollars. Most users would be best served by a software firewall, given the reasonable cost and added protection.

Another potential measure to take, particularly if there is an always-on broadband connection involved is the use of a router. Again, given the relatively small cost, the added protection is worth the effort.

[16] eBay Help Center, Email and Websites Impersonating eBay

Protect the Software

Since Microsoft Windows is such a prevalent piece of operating system software, any potential exploit is ripe for attack. It is essential for any consumer to maintain their operating system by regularly updating it, either on an automatic schedule, or manually. Regular installation of patches and updates costs nothing but bandwidth.

Clearly, anti-virus protection is nearly a necessity in today's environment. Virus writers are becoming more creative in their methods, and many of the rapidly spreading viruses encountered have not really been particularly damaging to the computers they infect – it is only a matter of time before an exploit is used to create serious damage to personal computers. There are a significant number of products on the market that will assist in this regard, and it is money well spent for anyone who connects to the Internet.

Conclusion

The biggest threat facing consumers today is ignorance. Failure to recognize the dishonest and seedy underbelly activity on the Internet can only lead to future difficulties. Unfortunately, much like "real" society, there are people who will not take any extra precautions, putting everyone at greater risk.

Following the guidelines discussed here, and keeping abreast of the rapidly changing landscape will help to protect your computer and your information. So, after you have your anti-virus software and personal firewall running, your operating systems updated, and avoid common browsing and email pitfalls, there are still plenty of additional things you can do to protect against threats. Steps like disabling file sharing, the Windows Scripting host, reviewing Internet Explorer security, and taking advantage of the multitude of resources available on the Internet can go a long way. Even if you do not have a comprehensive "defense-in-depth" strategy, it is critical to have an awareness of the threats out there to better prepare yourself and your systems to prevent unforeseen and potentially damaging circumstances.

List of References:

OneStat.com, *Microsoft's Windows dominates the OS market on the web*, available online at: http://www.onestat.com/html/aboutus_pressbox24.html

The Computer Industry Almanac, *Worldwide Cumulative PC Sales Exceed 1 billion*, available online at: http://www.c-i-a.com/pr0203.htm

The Computer Industry Almanac, *USA tops 160M Internet Users*, available online at: http://www.c-i-a.com/pr1202.htm

Updated Detection list information for Norton Antivirus, http://securityresponse.symantec.com/

F-Prot Product Information page, http://www.f-prot.com/currentversions.html

CyberAtlas, *Broadband Based On Behavior*, available online at: http://cyberatlas.internet.com/markets/broadband/article/0,,10099_2208421,00.html

CyberAtlas, *Worldwide Cable Modem Subs Expected to Double By 2007*, available online at: http://cyberatlas.internet.com/markets/broadband/article/0,,10099_2239451,00.html

Check Point Software Technologies, *Check Point Software Technologies Ltd. Awarded Patent For Stateful Inspection Technology,* available online at: http://www.checkpoint.com/press/1997/patent2.html

Check Point Software Technologies, *Stateful Inspection Technology*, pp 1, 3; available online at: http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf

Free Scratch and Win, Terms of Service, available online at: http://www.freescratchandwin.com/terms.html

CNET Product Review – Spybot Search and Destroy, available online at: http://www.cnet.com/software/0-806181-1204-20848563.html?tag=plug

PC Magazine Product Review – Spybot Search and Destroy available online at: http://www.pcmag.com/article2/0,4149,994109,00.asp

Verisign, *Understanding PKI*, available online at: http://verisign.netscape.com/security/pki/understanding.html

RSA Security, *How Are Certificates Used*, available online at:
http://www.rsasecurity.com/rsalabs/faq/4-1-3-11.html

RSA Security, *What is RC4*, available online at:
http://www.rsasecurity.com/rsalabs/faq/3-6-3.html

eBay Help Center, *Email and Websites Impersonating eBay*, available online at:
http://pages.ebay.com/help/confidence/isgw-account-theft-spoof.html