Global Information Assurance Certification Paper

Introduction to Network and Data Protection

A Security Primer for Beginners

Ron Beck

20 March 2001

Introduction

This document describes the field of network and information security from a beginner's aspect. It was written to be used as an introductory level tool to educate novice information systems users about the potential dangers of data communications. From this document, a reader will be able to understand basic terms and concepts, perform low-level risk assessments of their own information systems, and if possible, mitigate some of the risks they might encounter.

Background

In a time not so long ago, in a world technologically different than the one we live in today, there was little worry about network and data security. The Internet as we know it did not exist at the time. There was no World Wide Web or email. File swapping between users was usually accomplished through rudimentary bulletin board systems or hand-to-hand exchanges of floppy disks. Personal trust was high and security concerns were negligible. Throughout the 90's, as technology increased and costs were reduced, more people began to utilize common user communications such as the web and email. Although the sheer number of people "online" increased exponentially, personal trust and concerns for security took a backseat to speed and accessibility. It has taken global security incidents and personal losses to make some of these novice users aware of the risks involved with data communications and information transfer.

The Terms and Concepts

There are plenty of online glossaries of computer related terms available for the new user to use to better acquaint themselves with the real-world risks associated with being connected to the Internet. Below is a listing of some of the more important terms and concepts that a user must be aware of in order to protect them from threats to their data and resources. Some of these terms can be found along with numerous others at http://www.securityportal.com/research/security101/glossary.html

Back Door - A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Bug - An unwanted and unintended attribute of a program or piece of hardware, especially one that causes it to malfunction

BugTraq - A full-disclosure moderated mailing list for the discussion and announcement of computer security vulnerabilities.

CERT - Computer Emergency Response Team - Officially called the CERT Coordination Center; CERT is the Internet's official emergency team.

Compromise - An intrusion of security policy, which has the potential of disclosing private system information to an unauthorized user.

Firewall - A system or combination of systems that enforces a boundary between two or more networks, or a gateway that limits access between networks in accordance with local security policy. Can be a program that resides on a personal computer that filters all network traffic to prevent unauthorized communications and system compromise.

Hacking - Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Intrusion - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Password - A series of characters, usually without spaces, that is unique to a single username. A password is leveraged to determine the authenticity of a user

Signature Files – Files that enable anti-virus software to recognize and detect viruses and that contain instructions to clean files infected by viruses.

Trojan Horse - An apparently useful and innocent program containing additional hidden code, which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Virus - A program that "infects" other programs by modifying them to include a copy of itself. These infected programs in turn infect other programs.

Worm - An independent program that replicates from machine to machine across network connections, often clogging networks and information systems as it spreads. A worm typically spreads through Microsoft Windows email programs or through Internet Relay Chat

The Risks

A new computer out of the box should be considered insecure at the least. Most computers bought at a retail establishment are severely outdated in terms of information protection and those purchased from online or telephone retailers are only slightly better than their brick and mortar counterparts. The combination of naivety on behalf of the user and the age of the security programs installed or included with the computer can lead to problems. Below are some the security issues that a novice user MUST be aware of:

"I've got Antivirus Software. I'm OK"

The Problem

A first time computer owner usually has minimal experience with information systems. When they set up the computer their first instinct is to believe that the manufacturer has included all necessary virus protection programs. They are partially right in this assumption. The majority of manufacturers do include anti-virus programs, but for the most part, they are antiquated in terms of virus recognition.

The Example

John buys a computer from the local electronics super-store. It is an older version but is priced just right and meets the hardware specifications he believes he needs. Windows 98 is included with the computer and it has anti-virus software pre-loaded but unbeknownst to John is the fact that since his computer sat on the shelf for an extended period of time, the signature files are over a year old and in dire need of updating. The anti-virus program may notify him of this, but since he is not aware of the risks, he may cancel the update. Later on, he receives an email that contains a virus. The virus would have been identified had the signature files been updated, but alas, John thought his system was fine the way it came. Law #8 of the Ten Immutable Laws of Security: An out of date virus scanner is only marginally better than no virus scanner at all.

The Solution

When you become the owner of ANY computer regardless of age, make, networked or not, you must ensure that there is anti-virus software installed and that it is up to date. Signature files must be updated monthly at the least. It is recommended that you update them bi-monthly and always be aware of incident response updates, i.e., when a virus strikes globally, the CERT and anti-virus companies will release updated signature files as soon as possible. Make every effort to obtain these updates as well. Most anti-virus programs have features included that will handle the scheduled updates automatically, but it is up to the user to ensure that these updates occur and are successful.

Unfortunately, some of the anti-virus programs installed on older computers do not have the auto-update feature. If that is the case, then upgrade to a newer version or change vendors to one that does provide this service. Norton AntiVirus and/or McAfee Virus Scan can be purchased at their respective websites and 30-day trial versions of both can be downloaded for free at http://www.download.com.

With the frequency in which new viruses are being released and subsequently discovered, it is foolish not to be pro-active. Never open attachments and files downloaded from the Internet unless you have scanned them first with your updated anti-virus program. Also, scan floppy disks first before opening the files they contain. Taking the steps to prevent foreign data from infecting your system beforehand will save you time and lost data in the long run.

"Software – A story of trial and error"

The Problem

All computers need software in order to do anything. There are two types of software, operating system and application. Every computer, be it a PC or a Macintosh has to have an operating system such as Windows 98 in order to run. Application software such as Quicken is needed to accomplish the tasks that the operating system cannot. Both types can have "bugs" that may cause decreased system performance and/or create security issues.

The Example

Mary purchases a top of the line system from an online company with Windows Millennium Edition as the operating system. At first the computer runs great and she is happy with her purchase. Soon however, she notices that her system is running slower than it had and that some of her personal files are either missing or corrupted. One day not long after, her computer crashes and she can no longer get it to boot. She has lost all her personal information and has to reload the system from scratch.

The Solution

Out of the box software can also be a cause of security issues and system degradation. Almost every initial version of Windows has had bugs that caused system problems. Some application software such as AOL 5.0 for example, was *designed* to prevent users from utilizing their systems the way they wanted to. For the most part, when these flaws are identified, they are corrected. When a software company removes these flaws, improves features and functions, or adds components it may just be considered an upgrade or new release.

There are some bugs or flaws that can be more serious and can provide others access to a system. If someone with bad intentions discovers these flaws, they may keep this information to themselves as a method of compromising other machines. When this occurs and the software manufacturer is made aware of the bug, a patch or fix is released as a security update and is considered critical. It is imperative that a user also be made aware of these issues and takes every step possible to correct them. Unfortunately, most novice users do not even know where to look for this information and are left in the dark until their system is compromised and/or starts performing differently.

Some companies have begun taking a proactive approach to this situation. Microsoft now includes a program called Windows Update with its Windows operating system. Like the anti-virus program, it downloads and if necessary, installs software updates on a scheduled basis. It also has the capability to look for critical updates whenever a computer is connected to the Internet. It is highly beneficial to utilize this tool and keep system software current and as bug-free as possible. For the other software packages that are installed on a system, but that do not have update modules included, it is

recommended that a user frequently check to see if the vendor has released any patches or fixes.

"Network Security is for companies, not me"

The Problem

Corporate information security can be very different from personal information protection. Companies invest millions of dollars into information security every year to protect the assets and resources of their businesses. This is sometimes done behind the scenes so as to not disrupt the productivity of its employees. However, this may cause a false sense of security for some employees when they purchase their own machines for personal use.

Employees who work all day long on a computer may not be aware of the security policies and procedures implemented on their corporate network. They may not be aware that there is a firewall keeping their data safe. They might not know that the anti-virus software that runs on their desktop is configured to update itself whenever a user logs on. They may be oblivious to the file permissions that protect their information from prying eyes within the company. So when they purchase a home computer, they mistakenly may believe that it will be as secure as one at their office.

The Example

Betty has been working with computers for over three years at her job. She considers herself computer literate but not an expert and she feels comfortable enough to purchase a computer for her house. She buys a network ready mid-range system complete with Windows 2000. Since she likes the network speed at the office she also subscribes to a broadband Internet Service Provider and installs a cable modem on her system. She takes no security precautions while setting the system up and soon she is up and running on the Net. Two weeks later she notices obvious performance degradation, mysterious files on her hard drive, and that the network activity lights on her cable modem are always blinking. Later that year, she is contacted by law enforcement agents inquiring about her possible involvement in an attack on a computer system she had never heard of.

The Solution

Windows as a whole is extremely insecure and without taking specific steps and applying all applicable patches and updates, a user is basically hanging up a very large neon sign that says, "Hack Me!" Some default configurations of Windows allow for network access to all files and printers attached to the system. Couple these gaping security holes with software developed to exploit the Windows operating system and you come up with major data protection concerns. Amazingly, this crisis doesn't affect novice users only. Most intermediate and some expert users are not even aware of all the potential ways a hacker can access a computer running Windows. So it's easy to understand how simple it is for hackers to exploit these flaws.

By maintaining a firewall and keeping your computer secure you prevent others from causing problems through the use of your system. Many of the more publicized denial of service attacks that were launched against companies such as Yahoo and Amazon.com in early 2000 originated partially from hacked personal computers. The hackers took control of home computers in mass numbers and directed those systems to carry out the attacks on those websites. If you make sure your computer is locked up as tightly as possible you prevent damage to not only your own data but to other's as well.

The solutions to this problem are relatively easy, yet seldom enacted. First of all turn off the file and print sharing option in Windows and remove the Client for Microsoft networks if you are not connected to another computer in your home. Then invest in a personal firewall for your computer. Unlike a conventional firewall, the personal version is relatively inexpensive, designed to be operated by a home user and does not require a separate machine to run on. These devices are actually software that the user installs directly on the computer. They can be purchased online, bundled with anti-virus software, or even downloaded for free. For more information about how they work, and where to find one, and for other security guides including online testing of your system's security visit http://www.firewallguide.com.

Common Sense

Once you've accomplished the steps necessary to keep the hackers from accessing your system, you still need to use common sense in order to prevent falling victim to Law #1 of the Ten Immutable Laws of Security: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore. Don't fall prey to the Trojan horse, i.e., a file that you believe does one thing, but in reality does something completely different and usually malicious. Just like virus-laden email messages, if you don't know what a file does or whom it is from, then don't execute it. Viruses must be run by the user in order to spread copies of themselves and do their damage. Trojan horses must be run by the user in order for the hacker to gain access to your system. Once he has done that you have stumbled upon Law #2 of the Ten Immutable Laws of Security: If a bad guy can alter the operating system on your computer, it's not your computer anymore.

If you are familiar with corporate security policies then try to follow them at home. If not then follow the solutions listed in the pages above and remember to use strong passwords, avoid the darker sides of the web and the files that can be found there, and back up your data often. That last point will save you the most aggravation and time if you do have the unfortunate luck of being compromised and losing your data files.

Summary

Network and data security are concepts that may be foreign to some users of personal computers, but they shouldn't be. Situations found in real life often mimic the ones found in the cyber world. Getting a flu shot to stay healthy is similar to using anti-virus software to keep your computer up and running. Storing vital documents such as birth

certificates in a safe place to avoid loss is the same thing as backing up your computer's data to an external location. Taking your car in to get a tune up or replacing it with a newer, maybe safer model is the just like applying a patch or upgrading your software. If you lock your door to your house at night, then you should lock the "door" to your computer by implementing some form of firewall.

If you apply real world comparisons to the way you run your computer, you will see that data and network security are something that any user, novice to expert, must utilize when using their computers. Without it you are causing yourself and others potential problems down the road. Protect your computers the way you would protect yourself and your belongings and in the end, we'll all be better off for it.

Bibliography

Unknown. "Glossary – Security 101." URL: http://www.securityportal.com/research/security101/glossary.html (20 March 2001).

NTA Monitor. "Denial of Service Attacks - Yahoo/ Amazon." February 16, 2001. URL: http://www.nta-monitor.com/news/yahoo.htm (20 March 2001).

Lawler, Scott. "Are You a Good Internet Neighbor?" October 24, 2000. URL: http://www.sans.org/infosecFAQ/start/neighbor.htm (20 March 2001).

Hammon, Robert. "History of the Internet." History of the Internet, WWW, IRC, and MUDs. URL: http://www.socio.demon.co.uk/history.html (20 March 2001).

Culp, Scott. "The Ten Immutable Laws of Security." Microsoft TechNet. Oct 2000. URL: http://www.microsoft.com/technet/security/10imlaws.asp (20 March 2001).