Interested in learning more about security?

SANS Institute InfoSec Reading Room

Overview of Security Issues Facing Computer Users

Every security safeguard a computer user takes will reduce the number of people skilled enough to break into their computer. After all, there are a finite number of people who have the skill required to break into computer systems. Some are very skilled and patient and will be very difficult to stop. And some are not so skilled and rely on tools and applications developed by other people to do their dirty work. Fortunately the first group is a lot smaller than the second group. There are obviously hundreds of different...

Overview of Security Issues Facing Computer Users

GIAC Security Essentials Certification (GSEC)
Practicum v1.4b Option 1

March 17, 2004

Written by:
Michael C. Boeckeler

Abstract
This paper is a broad overview of several issues pertaining to computer security. The first section discusses viruses, worms and other malicious programs. The next section covers wireless networks. The implications of the 2002 war drive are discussed, as well as several different ways to secure a home wireless network. A brief discussion of firewalls – both hardware and software – follows. Next, the importance of strong passwords is discussed in detail. This is followed by a section on default settings, as well as a discussion on social engineering. The next to last section is on the wide availability of computer security information and software. The paper ends with a conclusion in which I discuss the implications of the various topics covered in the paper.

Introduction
Over the past 10 years the Internet has become ubiquitous to the average person in the United States. People of all ages use it on a regular basis, and it has become one of the driving forces of the economy. From banking to shopping to communication, it has radically changed the way many people go about their daily lives. The increased availability of broadband connections will allow more people to experience all that the Internet has to offer.

Unfortunately, some people have chosen to use the Internet and World Wide Web to hurt both individuals and entire organizations. They have developed an arsenal of tools and techniques that can be used for a variety of purposes, including stealing personal information, shutting down a company's web site, or even crippling entire networks with massive denial of service attacks. Although the "good guys" try hard to keep ahead of the "bad guys", not everything can be predicted and/or prevented. Fortunately, there are certain safeguards that can be taken today which will greatly reduce the chances of becoming a victim tomorrow.

This paper covers several important issues facing computer users today, and provides some insights on how a user can better protect his or her computer. It was written so that non-technical computer users would be able to understand it. As a result, some fairly basic points are explained in detail.

Every security safeguard a computer user takes will reduce the number of people skilled enough to break into their computer. After all, there are a finite number of people who have the skill required to break into computer systems. Some are very skilled and patient and will be very difficult to stop. And some are not so skilled and rely on tools and applications developed by other people to do their dirty work. Fortunately the first group is a lot smaller than the second group. There are obviously hundreds of different things that can be done to increase a computer or network's defenses – and not all of them are difficult or expensive to do. But every worthwhile security measure that is put into place reduces the number of people who are capable of breaking into that system. In addition to discussing viruses and wireless networks, this paper discusses some other

things which are often forgotten about, such as the importance of strong passwords, the dangers of social engineering, and the need to change default settings.

Statistics from the FBI, CERT

The CERT Coordination Center (CERT/CC), which is operated by Carnegie Mellon University, is an organization that specializes in computer security issues. CERT/CC publishes various statistics pertaining to computer security on its web site. As you can see by looking at Table 1, the number of computer security incidents has risen sharply over the past several years. The total number of vulnerabilities reported has decreased slightly from 2002 to 2003, but is still significantly higher than what was reported 3 or 4 years ago.

Table 1: CERT/CC Statistics 1999-2003[1]

Year	Incidents Reported to CERT/CC	Vulnerabilities Reported to CERT/CC
1999	9,859	417
2000	21,756	1,090
2001	52,658	2,437
2002	82,094	4,129
2003	137,529	3,794

While CERT/CC's published statistics aren't very detailed, those from the FBI/CSI survey are. For the past 8 years, the San Francisco FBI office and the Computer Security institute (CSI) have conducted a survey of organizations computer security problems. The 2003 survey had 530 respondents from a wide variety of organizations – from small companies with less than 100 employees, to large ones with over 10,000. The respondents came from all types of organizations as well, and included government, education, medical and financial organizations, among others.

Some highlights from the 2003 FBI/CSI survey[2]:

- Viruses were the #1 type of attack/misuse among respondents (82% of respondents reported this)
- Insider abuse of net access was the #2 type of attack/misuse (80%)
- Denial of Service attacks were reported by 42% of respondents
- Theft of proprietary information was reported by 21% of participants
- The costliest form of attack was theft of proprietary info, with a total of $70 million lost by those who reported it
- Denial of Service attacks were second most costly - $65 million
- Viruses cost these organizations ~$27 million
- Overall, the number of attacks have remained almost constant over the past 2 years
- Finally, almost all of the respondents use firewalls and antivirus software, and many use additional security methods and devices

These surveys agree that the danger of computer attacks has not decreased over the past year. In addition, despite widespread antivirus software use, viruses continue to be a big problem for organizations. Finally, the FBI/CSI survey showed that sometimes the best security fails to stop a determined attacker.

Discussion on Worms and Viruses

It seems like every few days there is news of a new computer virus or worm on the loose. In fact, some reports claim that there are "15 new viruses discovered each day".[3] Although there are literally thousands of known computer viruses in the world today, most are variations of other viruses. This is fortunate because it makes it easier for antivirus software companies to quickly respond to new viruses. Just like real life viruses vary in severity, so do computer viruses. Some viruses are merely a nuisance – they may flash a message on the screen on a certain date (such as the virus creator's birthday). Some are more dangerous. For example, some viruses may cause a random spontaneous reboot of your computer, causing you to lose any unsaved data. And some viruses have severe consequences. For example, some viruses may format your hard drive when activated.

Some especially insidious viruses and worms are able to disable antivirus software on a system. This is incredibly frustrating for the victim. After all, they are most likely aware that they have been infected by something, but when they try to run their antivirus program, they find that it doesn't work, it crashes, or that it has even been uninstalled! Attempting to reinstall the antivirus program often proves to be a waste of time because the virus/worm interferes with the installation process! Some of these viruses are even able to interfere when a user attempts to visit an antivirus vendor's website! Some examples of these worms and viruses include Fizzer (and its many variants), Klez (with variants) and Bug Bear (and its variants). Fortunately there are ways to eradicate these types of infections – antivirus software companies usually post instructions on how to eradicate these viruses from a system, but they are often complicated and beyond the skill level of many users. I suspect that many users eventually end up performing a complete operating system reinstall when faced with these types of infections.

Modern network aware viruses and worms are different altogether. Instead of adversely affecting a single computer, these new viruses are capable of spreading around the world in short periods of time. For example, many of these new viruses are able to email themselves to every entry in an infected computer's address book. When the unsuspecting recipient opens the infected email from someone he or she knows (after all, they were in their address book), they become infected, and the process repeats itself. During such outbreaks, people will often receive dozens of such emails – it is a viscous circle because the same people you have in your address book often have you in theirs! It is

easy to see how thousands and thousands of computers can become infected in a very short period of time. These mass infections often result in extreme network congestion, and can cause email boxes to fill to capacity. Multiply this by the thousands of infected users and servers can crash, technical support personnel become overwhelmed, and whole networks can become unusable. Modern network viruses like this one can also be used to conduct massive denial of service attacks.

With so many possible ways to become infected, all users should get into the habit of using an up to date antivirus application. Many of the available packages are easy to use and work relatively invisibly in the background. Although many ISP's conduct virus scans of messages traversing their email servers, it is a good idea to enable scanning of both inbound and outbound email messages. Users should regularly check with their antivirus vendor's website for virus definition updates.

On the other hand, users must recognize that having up to date antivirus protection isn't a magic bullet against infections. Consequently, users must be vigilant, particularly with regards to email attachments and files downloaded from the Internet. Even if an email with attachment has come from someone you know, there is no guarantee that it is safe – after all it could be the result of a friend being infected by a worm or virus, and you really have no way of knowing whether or not your friends use antivirus programs on their computers. So if you don't have automatic email scanning, manually scan attachments. As for downloading files, always be careful and scan files before you open or execute them. Beware of zip files, and make sure your antivirus program is scanning the contents of zip and other compressed files.

Viruses

A computer virus is a computer program that is loaded into a computer without the owner's knowledge.[4] While most viruses are designed to do some sort of harm to a computer user – whether that harm is causing a user grief, wasting their time, or destroying irreplaceable data – viruses can be benign.

In order to be considered a virus, the program must meet two criteria. First, the program must be able to self-replicate. Second, the program must be able to activate itself.[5] In addition, viruses spread by infecting files.

Five different types of Viruses

According to Symantec Corporation, which publishes several popular antivirus applications, there are five different types of computer viruses: boot sector, master boot record, file infector, macro and multi-partite.[6] While each of these five types of computer viruses infect different types of files, they all share the two main characteristics of viruses - the ability to self-replicate, and the ability to self-activate.

Boot Sector/Master Boot Record Viruses
Back when MS-DOS was the prevalent operating system for PC's, boot sector viruses were common. This is a virus that resides in the boot sector of a floppy or hard disk, and is activated every time a computer boots from an infected disk. From there the virus remains in memory until an uninfected floppy disk is inserted into the floppy drive. As long as the floppy disk is not write-protected, the virus will infect the floppy disk the next time the disk is accessed.

Master Boot Record viruses are very similar to Boot Sector viruses. The main difference between the two has to do with where the actual site of infection occurs. Master Boot Record viruses infect the MBR, while Boot Sector viruses infect the Boot Sector.

These types of viruses were commonly seen in computer labs at schools and universities. This was due to the fact that floppy disks were the portable storage medium of choice. All it took was one PC infected with a boot sector virus to infect every non write protected floppy disk inserted into it.

File Infector Viruses
File infector viruses infect executable program files.[7] On MSDOS and Windows based PC's, these are files ending with .com or .exe. Every time an infected file is executed, the virus is loaded into memory, and will infect any other executable programs that are later run.

Because of the danger of file infector viruses, you should always beware of unknown computer programs, whether they came as an email attachment, or were downloaded from the web. Never run an unknown executable program without first scanning it with an antivirus program. Even if you know the person who sent the program to you, you should scan it first – once again, you have no way of really knowing where the file originally came from, or whether the sender is using antivirus software on his computer.

File infector, boot sector and master boot record viruses are all platform dependent. This means that a file infector virus written for MSDOS based computers will not run on an Apple Macintosh computer.

Macro Viruses
Macro Viruses are one of the most common types of virus on the loose today. In fact, macro virus infections have cost more money and taken more time to repair than any other virus type.[8] One of the most famous (and virulent) computer viruses was a macro virus. "The Melissa virus first appeared on Friday, March 26, 1999, and spread all over the world faster than any virus seen before."[9] Melissa was a Microsoft Word macro virus.

A Macro Virus is a virus that has been created using a scripting or macro language. Many major applications, such as the applications included with

Microsoft Office, include macro and scripting languages. These are powerful tools that can be used to speed up repetitive, tedious tasks, or even create entirely new applications. In the case of the Microsoft Office applications, Microsoft has included the Visual Basic programming language. This is a subset of the same Visual Basic that is part of Microsoft's Visual Studio suite of programming languages. In the hands of a talented programmer, Visual Basic can be used to create entirely new applications. Unfortunately, it didn't take long for virus writers to realize the opportunity Visual Basic gave them – which was a powerful programming language designed to access previously unreachable parts of Microsoft Office applications. Macro viruses usually infect data files – either user created documents, or document templates.

The first macro virus to appear was called the "Concept" virus[10], and it affected Microsoft Word files. It operated by tampering with the default document template, and made it almost impossible for a user to save his or her documents. By inserting itself into the default template, it ensured that every new document created would be infected. Fortunately for Word users, Concept was mostly a nuisance. Unfortunately, its name had a double meaning – it served as proof of concept that viruses could be written using an applications macro language – and other similar viruses quickly appeared.[11]

Macro viruses differ from other computer viruses by being able to "spread across platforms."[12] For example, a Microsoft Word macro virus can just as easily infect a Windows based PC as it can infect an Apple Macintosh computer, as long as both computers have Microsoft Word installed.

Another interesting and dangerous characteristic of some macro viruses is that it is sometimes possible to infect a computer even if the user does not open the infected file. I am referring to the "preview pane" feature of Microsoft Outlook and Outlook Express email clients. This feature allows a user to read their email messages without actually opening each individual email message. Macro virus writers somehow discovered a vulnerability which existed in Outlook and Outlook Express that allowed them to infect a computer as soon as the user previewed an infected email message. The "Klez" virus was the first virus seen that was able to infect computers in this manner.[13] Fortunately, both Outlook and Outlook Express allow users to disable the preview pane, which was one of the recommended precautions for this type of virus. It is important to note that disabling the preview pane alone will not make a computer immune to the Klez or other similar viruses – infection will still occur if the user opens the infected message and/or attachment.

Multi-Partite Viruses

Multi-partite viruses are difficult to repair. They are a combination of a boot sector virus and a file infector virus. The reason why they are hard to repair is because there are two distinct areas infected. It is possible to remove the boot

sector portion of the virus, only to have the file infector portion re-infect the boot sector, and vice versa.

Worms

Worms are another type of malicious computer program. While it is debatable whether or not computer worms are a type of virus, or if they are something different[14], they do meet the two criteria for being a virus – they are able to both self-replicate, and self-activate. On the other hand, worms do not attach themselves to files like viruses do. So whether worms are viruses, or simply virus-like, really doesn't matter. What does matter is that worms are an insidious creation whose sole purpose is to cause problems for computer users.

Trojan Horses

The third type of malicious computer program/entity is the Trojan Horse. A Trojan Horse is a harmful computer program that has been hidden inside of something benign, such as an email attachment or even an innocent looking program.[15] Once a Trojan Horse has made it onto a computer, it sits there until the user opens the email attachment or program that is infected with the Trojan. Consequently, Trojans fail to meet the criteria of a virus of self activation.

So what kind of programs can a Trojan contain? Some Trojan Horses contain spyware, which is software that keeps track of World Wide Web usage statistics, and periodically transmits them back to the creator. Others display a fake login screen, and whenever a user enters their usernames and passwords, they are recorded, and ultimately sent to the hacker who created the Trojan. In addition, Trojan Horse's can be used as a way to spread viruses and worms.

Some of the most serious Trojan Horses are ones that install remote access programs on the computers of unsuspecting victims.[16] Back Orifice is this type of Trojan. Once the Back Orifice Trojan has been run on a computer, it installs a program that allows remote users to access that computer. Similar in function to legitimate remote access utilities such as Symantec pcAnywhere,[17] Back Orifice gives the remote user the ability to do almost anything they want to the infected computer. They can copy files, delete files, uninstall applications, format disks and even send documents to a printer. All of this can be done without alerting the victim. The potential damage caused by one of these Trojans is staggering.

As with file infector viruses, one of the best ways to protect against Trojan Horses is to beware of unknown executable files. Email attachments and programs downloaded from the net fall into this category. Even if you know the person who sent you the email attachment, always scan executables before running them. Be especially careful of files obtained from file sharing services such as WinMX and Gnutella.

Every file has an extension based on file type. For example, JPG picture files have a ".jpg" extension, and Word documents have a ".doc" extension.

Executable files have ".exe", ".com", ".bat" and ".vbs" extensions. One of the ways that some Trojans sneak onto a system is by using an incorrect file extension.[18] By default, Windows hides extensions. A Trojan Horse may be named "picture.jpg.exe". Since Windows hides the extension, the user will see the files as "picture.jpg", think it is an ordinary JPG picture file, and not hesitate to click on it. After all, it isn't a ".com" or ".exe" file. End result – the user was tricked into clicking on the Trojan, and whatever nasty, malicious program it contained was successfully run. Obviously, to prevent this, the user should change the Windows setting to "display all file extensions".

Antivirus Programs

Antivirus programs typically work in two different ways. First, they contain a database of signatures for all known viruses and worms. The software searches a computer for the presence of these signatures. Because new viruses and worms are found almost every day, these databases are regularly updated by the antivirus software's developers. The second way antivirus software operates is by looking for suspicious activity – such as when a virus actually tries to infect a file. For instance, some viruses change the size of a file when they infect it – and this can be easily detected by an antivirus program. On the other hand, virus writers know that antivirus programs look for changes in file size, and have devised ways to infect a file without increasing the files overall size.

Polymorphic Viruses

Just like real viruses are able to change in order to defeat a host's immune system, some computer viruses are able to change in order to defeat antivirus software. These are called polymorphic viruses, and they are able to change signatures each time they infect a new file.[19] They were developed specifically to defeat antivirus software and frequently updated virus definition databases. Any of the five types of viruses can be written to be polymorphic.

A Denial of Service scenario

A denial of service attack (DoS) is when a computer (usually many computers) is used to transmit data to a target computer in the hopes that the target computer will be overwhelmed from all of the data coming its way. For example, somebody is mad that a software company cancelled production of a long awaited game. This person is a gifted programmer, and decides he wants to get even with this company by shutting down its networks. Obviously this person doesn't want to be caught. So he obviously won't conduct this attack from his own computers, or from where he works, because he knows the attack could be traced back to him. Anyway, he needs a lot of computers to do a good job. So this person goes online and downloads the source code to an existing, well known virus. He makes a few changes to this virus, just enough so that up to date antivirus programs won't recognize the virus. He then puts the virus in several cracked games he has uploaded to an IRC fileserver. Anyone who downloads the game and installs it will become infected by his virus. The virus will send copies of itself to email addresses in infected computers' address books. And the process

repeats itself. After 36 hours the virus is set to go off, and every infected computer will start to endlessly send different types of packets to the software company's web server. The software company's web server is unable to cope with the onslaught of packets coming at it from thousands and thousands of different machines, and is forced to shut down. This is what happens in a successful denial of service attack. Because denial of service attacks are often performed by unaware victims of a virus or worm infection, it is usually very hard to find the person who was ultimately behind the attack.

Wireless Networking

Wireless networks have become increasingly popular over the past few years. They are easy to set up, don't require long runs of cable, and offer decent performance at low prices. In the home, they are used as an easy way to connect computers in different parts of the house. In addition, home users often use wireless networks as a cheap and easy way to share a broadband DSL or cable connection among several computers. Businesses use wireless networks so employees can roam around a location with their laptops or PDAs without needing to physically plug their device into an access point. Colleges and universities often use wireless networks in this same way – they allow students to connect to the network regardless of their location. So a student can check his or her email, go to an instructor's website, or even conduct research whether they are in class, in the student union, in the library or in their dorm room. Finally, wireless networks are being used more and more in public places as a way for busy people to easily connect their laptops or PDA's to the Internet. Places like Starbucks Coffee, Borders Bookstores and airport lounges have begun to offer wireless access points in certain locations. However, while wireless networks have a number of good points, they are also notoriously difficult to secure.

A few years ago a group of computer users across the United States did a weeklong survey of wireless networks to determine if people were doing an adequate job of securing their networks.[20] Such a survey is known as a "war drive" and the participants used a variety of means to detect the networks they studied. The majority of the surveying was done by car with laptop computers and PDA's equipped with wireless Ethernet cards (802.11a and 802.11b). But they also traveled on foot to get to areas not accessible by car. Some enterprising people even conducted their survey by small planes at low altitudes. What they found should scare every person who uses a wireless network.

First and foremost, it was discovered that a very low percentage of wireless networks even utilize the most basic security measures. A large percentage of wireless networks not only broadcasted SSID's (Service Set Identifier, used by different wireless networks to differentiate from one another), but had also not even bothered to change SSID's from their default values! Based on the fact that they detected SSID's with values indicating they came from high cost wireless

equipment, the war drivers concluded that even government and businesses were failing to put even basic security into place.

The war drive also discovered some surprising information regarding the range of wireless networks – from the air, access points could be detected at altitudes up to 2500 feet! So even though your 802.11b network appears to have range problems in your 2 story house, you must never forget that there is a good chance your network can be detected at surprisingly long distances. This obviously affects most users of wireless networks. In fact, unless you live on a deserted island many miles from the nearest human, you must be aware of the dangers of wireless networking. Businesses have to be aware that if they choose to use wireless networks, they open themselves to the possibility of somebody – a competitor, former employee, hacker etc – being able to drive up and park in the parking lot, turn on a laptop with wireless card – and either eavesdrop with a packet sniffer or actually connect to the network. Home users must also be careful. Even if you live in a rural area, you are at risk of somebody being able to eavesdrop or hack you. Your $100 Linksys or Netgear 802.11b router is sending out your data much farther than you realize. And if you live in an area with other houses in close proximity, or in an apartment, you absolutely must take precautions when using a wireless network. The risk and consequences of someone obtaining your personal or financial information is too great these days At the very least, securing your wireless network will prevent somebody from leaching onto your network for free

There are two fundamental methods of securing a wireless network. The first is to prevent unwanted devices from connecting to a network, and there are a number of ways to accomplish this. The second main method is to ensure that an eavesdropper is unable to obtain any meaningful data from your network. This is accomplished by encrypting the data that is broadcast. WEP – Wired Equivalent Privacy[21] – is used for this purpose.

As mentioned, there are several ways to prevent unwanted users from connecting to a wireless network. One of the first things a wireless network operator should do is disable the automatic SSID broadcasts by their wireless equipment. SSID refers to the Service Set Identifier, and it is used by wireless network equipment to differentiate between one wireless network and another.[22] Wireless access points such as wireless routers broadcast SSID's – but most can be optionally configured to not broadcast an SSID. A wireless access point that broadcasts an SSID is like somebody lighting a match in a dark room – it immediately advertises its existence. Therefore it is smart to disable SSID broadcasting. It is important to note that SSID's are still used even when the access point is no longer blindly broadcasting its SSID to the whole world. Regardless, if a device wants to connect to a wireless network, its SSID must match that of the access point.

Along with disabling SSID broadcasts, the default SSID value should be changed to something unique! Most computer equipment is configured at the factory with certain default settings. For example, it is common knowledge that many home wireless routers have a default SSID value of "Wireless". This must be changed to something unique. Otherwise turning off SSID broadcasts won't make much of a difference because any intruder who is aware that the network exists could do a trial and error and set a clients SSID to common defaults until a connection is made.

The last method of controlling who connects to a wireless network is restricting MAC addresses. A Media Access Control address (MAC) is a hardware address that uniquely identifies each node of a network.[23] So each device attached to a wireless network will have a MAC address. Many wireless routers can be configured to allow connections only with devices with specific MAC addresses. MAC addresses are supposed to be unique – so allowing only known MAC addresses should, in theory, prevent clients with unknown MAC addresses from using your network. In a home environment this is easy to do, because there aren't many MAC addresses to keep track of. But it could become more difficult if new users are added regularly, like in a busy office environment. It should be noted, however, that although MAC addresses are unique, a skilled attacker can spoof a network – even though he or she does not have a device with the proper MAC address.[24] On the other hand, every additional step that is taken to protect a computer reduces the number of people that have the skill level needed to break into it. Therefore, MAC address restrictions should be used, if possible.

WEP (Wired Equivalent Privacy) is used to encrypt the data transmitted between wireless devices. Unfortunately, using WEP can adversely affect a networks performance, especially as the degree of encryption is increased. Administrators must weigh the benefits of the added security with the decrease in throughput and find a level that is acceptable. It should also be noted that the effectiveness of WEP has been called into question, even at its highest levels of encryption.[25]

In any event, a combination of these methods should be used to secure a wireless network. Whether or not WEP should be used is beyond the scope of this paper. However, at the very least, SSID broadcasts should be disabled, default settings should be changed, and MAC addresses should be restricted to known devices.

Firewalls – hardware and software

A firewall is a device that sits between a computer or network and the outside Internet. It is designed to be the main defensive barrier against intruders. Traditionally, firewalls were a hardware device, but today there are both hardware and software firewalls.

Hardware firewalls are basically a chokepoint. All network traffic must pass through it before it can enter your network. Most firewalls operate by a set of

rules. These rules must be set up by the administrators of the network, and tell the firewall what to do under different conditions. There are different types of hardware firewalls, varying in sophistication. Organizations that use hardware firewalls often also use an application called an Intrusion Detection System (IDS). Intrusion Detection Systems often run on a separate computer that is receiving everything that passes through the firewall. They are designed to spot suspicious activity, and alert the network administrators when necessary. In addition, they can help an organization learn lessons from an incident and better prepare for the next one.[26]

Software firewalls, like ZoneAlarm and BlackIce, run on Windows based personal computers. They actually include a lot of IDS functionality. Once installed, these programs monitor both what is coming into the computer, as well as what is leaving it. So they are able to detect all sorts of external activities directed towards your computer – from port scans to a flood attack. Also, since they monitor traffic from your PC to the outside network, they can alert you to the presence of unknown malicious software, such as a virus or worm that is using your computer to conduct a DoS attack. These firewalls keep close track of which programs are allowed to access the Internet, and which aren't, but configuration is usually straightforward.

Installing and running a personal software firewall such as ZoneAlarm for the first time can be an eye opening and frightening experience. Chances are, the user will be amazed at the number of a "hits" reported by the firewall. Some of these hits are going to be false positives – packets being sent to and from the computer for legitimate reasons – but eventually the firewall will probably detect numerous attempts by outsiders to gain information about the system. Often these are port scans conducted by somebody who is interested in learning the details of the system. This can be a prelude to a more serious intrusion. Besides monitoring everything that goes in and out of a system, programs like ZoneAlarm are also able to effectively hide computers on which they are installed from the outside Internet. A hacker can't break into a computer they don't know exists. As a result, when someone does try to conduct a port scan on a computer (really the IP address) running a program like ZoneAlarm, they will learn nothing from it.

Passwords

Passwords are the most prevalent method of authenticating a user. In essence, they are the computer world's version of the key. Anybody who regularly uses computers and accesses the Internet must frequently enter passwords. Unfortunately, passwords are not perfect – they can be cracked by several different methods, and they do not provide proof of identification of the user.

So what can you do to protect yourself from having a malicious outsider go through your email, read everything on your computer, or even use your computer as a way to trigger a denial of service attack?

In my opinion, the single easiest and least expensive measure an individual or even an organization can take to protect their computers and information is to practice smart password usage. There are several facets to smart password practices, each of which is no less important than the next.

A password is effective only as long as nobody else is able to figure it out. Therefore you must always be cognizant of the passwords you select for yourself. Never choose a password which will be easy for somebody to guess. Never use your name, your child's name, a pets name or a variation of any of the aforementioned as a password. When I say variation, I mean do not take a word with significance for you, like your last name, and make predictable changes to it in an attempt to make a password that is easy to remember. For instance, if your last name is "SMITH", don't use "HTIMS" (SMITH backwards) as your password.

Never use anything else that has significance for you as a password. For example, never use your social security number, or birth date, or phone number, or bank account number for a password. There are two reasons why this is important. First and foremost, those are obvious passwords. A skilled and determined hacker will try to learn as much about you as possible, solely to be able to make educated guesses about your passwords. The second reason is just as important, however. You don't want somebody to stumble across your social security number, or credit card number while they are trying to find your passwords. For instance, if I was trying to determine the password to your email account, and somehow determined that it was a 9 digit number, the first thing I would think was that it was your social security number.

But most of all, absolutely never use any word that appears in a dictionary. There are several widely available programs that are able to crack passwords found in dictionaries. These programs – such as L0phtCrack for Windows based PC's – can quickly crack certain passwords. Due to the existence and availability of these types of programs, it would be foolish to not follow strong password practices. Bottom line – you must behave with the knowledge that malicious people will be using programs like L0phtCrack.

Brute Force

When talking about cracking a password, or cracking encryption, you may hear the term "BRUTE FORCE". A brute force attack is an attack that uses the raw power of a computer to crack encryption or a password. So for example, if a password can be up to 5 digits long, and can only use digits 0 – 9, a brute force attacker would use a computer program to try EVERY possible password until it finds the correct one. So it will first try "0". Then it will try "1". Then "2". Eventually it will try "01". "02". '03" ..."99" …"001" ..."0001" ..."00001" ..."10000" ..."10001" etc etc all the way up to "99999". Obviously this will ultimately be successful, but it could take quite a bit of time. In the case of a brute force attack against an encrypted message, depending on the speed of the computer, and the type (and degree) of encryption used, it could take weeks, months even

years to complete! In addition, many computer systems and applications have safeguards built into them that prevents a brute force attack from occurring against passwords. After the first 2 or 3 unsuccessful attempts, the computer will not allow further attempts for a given period of time.

So what can be done to make it more difficult for someone to crack your password using a brute force attack? The most obvious way to make brute force attacks more difficult is to use as many characters as are allowed when choosing a password. It will be significantly more difficult to break a 9 digit password than one with 4 digits.

Moore's Law says that computers approximately double in power every two years. In addition, operating systems such as Linux have made distributed computing inexpensive and easy. These two facts have major implications for brute force attacks – passwords that were uncrackable a few years ago via a brute force attack might now be able to be cracked in short periods of time.

Rules for creating Strong Passwords

Computer users should choose their passwords carefully. The goal is to choose a password that will minimize the chance that somebody will be able to figure it out using the methods discussed earlier. Therefore, a strong password is a password that:

1) Does not contain any words found in a dictionary
2) Does not contain any words that are of significance to the user
3) Does not contain any numbers that are of significance to the user
4) Is not a variation of 1,2 or 3

In addition, if the password is case sensitive, it is beneficial to use both upper and lower case letters.

Here are some examples of strong passwords:
FG78LpQww22
A565NQ23asdE
86YuImB3821

L0phtCrack

As previously mentioned, L0phtCrack (aka LC4) is a password cracking program for Windows based computers. It is not strictly dictionary based. First, it checks users information stored on the computer. Presumably that means it tries any names or company names it finds. Next, it uses a dictionary. Third, it checks for variations of dictionary words. Finally, if the previous 3 methods have failed to determine the password, it will perform a brute force attack.

LC4 has many impressive capabilities. It is able to crack encrypted passwords, and can even capture encrypted passwords from network traffic. It can also

break a tough cracking job up into several different pieces. Each piece can then be cracked on a separate computer, thus tremendously speeding up the cracking process. It comes with two dictionaries – one with 25,000 words, and the other with 250,000 words, but more can be added.

As a test I ran some passwords through LC4 to test its effectiveness. The table below shows the results.

Table 2: L0phtCrack test performed on AMD Athlon XP 2800+ PC

Password	Time to crack
Mississippi	17 seconds
MiSSiSsiPpi	18 seconds
cowboy	4 seconds
cowb45oy	After 12 hours I cancelled attempt

As you can see, common words make terrible passwords and varying the case makes no difference whatsoever. Changing "cowboy" to "cowb45oy" does make it a much stronger password. However, since L0phtCrack progresses from *user information* to *dictionary* to *variations of dictionary* to *brute force*, and the goal is to make our passwords as difficult as possible to crack, it makes no sense to use even a variation of a dictionary word (like "cowb45oy"). Clearly, it will take L0phtCrack much longer to crack a password such as "FG78LpQww22" than "cowb45oy".

No Passwords on Post-It-Notes

Another key to keeping your passwords secret is being careful where you store them. Unless you are alone at home, and the only person who has any type of access to your computer, it is not a good idea to keep your passwords on a post-it-note on the side of your monitor. While this is important for everyone, it is especially crucial for people who use computers at work. Why bother having passwords in the first place if you are going to have them displayed for anyone nearby to see? You may think that although you have your passwords written on a piece of paper that is underneath your monitor, they are essentially safe because your co-workers will notice if someone is snooping around your cube or office. However, don't ever forget that a determined person will use a variety of techniques to gain whatever information he needs – from technical methods like using a packet sniffer to learn passwords – to non technical methods like snooping around your workplace during lunch hour.

Future of Passwords

As previously mentioned, passwords are the computer world's version of a key. But they do have shortcomings – most importantly, a determined hacker can use several different methods to determine a user's password. Also, passwords do not provide proof of the user's identity – i.e. a person other than me can use my passwords to get into my things. Due to these problems, several alternatives to passwords have been developed, and are already being used in situations that

require the most stringent security. These alternatives include biometric devices such as fingerprint scanners and retina scanners. Biometric devices use unique biological attributes such as voice, fingerprints and retinal image to provide authentication of users.[27] A fingerprint scanner can not be spoofed with a brute force attack, and a retina scanner isn't vulnerable to a dictionary attack. In addition, fingerprint and retina scanners provide proof that a person is who they claim to be. Expect more newly developed authentication methods to appear in the future.

Default Settings

Earlier in the section about wireless networks I mentioned that the war drive survey found that a large percentage of wireless networks were configured with their default settings. This is the result of sloppiness. Fortunately, changing default settings (along with using strong passwords) is one of the easiest and least expensive ways to improve security, particularly at a business.

I have a Netgear MR814 wireless router. Its configuration program is accessed by pointing a web browser to 192.168.0.1 and entering the correct username and password. The address cannot be changed, and neither can the username – which is "admin". But what can be changed is the password and SSID. It is no secret that the default password for these routers is "password" and that the default SSID is "Wireless". In fact, either of these bits of information can be found at Netgear's website. And why should Netgear try to keep it secret? It is assumed that the user will be diligent and immediately change these settings to something unique to them. But in reality default settings are often ignored, even in enterprise settings where professionals oversee the equipment. Whether it's the result of laziness, or carelessness, or even ignorance doesn't really matter. What does matter is that the first thing a semi-intelligent intruder will do, when faced with a password or username or setting such as an SSID, is try the defaults. Besides being able to find the values for default settings at the manufacturer's websites, there are also entire web sites that have long lists of default settings for common equipment.

So in both home and business environments default settings should be changed to something unique. A good approach for choosing values for settings would be to follow the rules used to choose good passwords. In other words, use a random combination of letters and numbers. Absolutely never use a word that can be found in a dictionary. Finally, never use a word or number that has any significance to you, such as a phone number or birthday.

Social Engineering

This leads me to the next section, which I will briefly discuss – social engineering. Social engineering is when a person uses a variety of non-technical methods to get what they are after. This could include pretending to be a janitor, sweet talking a secretary, impersonating people on the telephone, or even using a variety of techniques to elicit as much information as possible during what

appears to be an innocuous conversation. Social engineering is a legitimate strategy for serious hackers, and some of the most infamous and successful hackers have been very skilled at it.

You must always beware of somebody trying to contact you out of the blue asking for personal information. By now, almost everyone who has an email account has probably received one of those sob story emails from the purported exiled king of some African country, claiming to have $100 million on deposit in a Swiss bank, and asking for your help in withdrawing it. All the exiled king needs is your name, social security number, and the number for your bank account - so he knows where to deposit your share of the money! I have probably received 30 emails similar to this over the past year (an example I recently received is in Appendix A), and I can't help but wonder if anyone has ever been stupid enough to fall for it. But I also suspect that people do fall for these and more sophisticated ploys all the time – otherwise why do these people continue to send letter like this out?

Other commonly seen fraudulent email messages are supposedly from banks or credit card companies. They explain that there has been some sort of problem with your credit card and ask for your account number to verify something, or to solve the problem. Often these emails have a link that can be clicked, bringing the victim to an exact replica of the credit card company's website.

Recently three blind Israeli brothers were implicated in a variety of crimes involving computer and telephone hacking. Although the brothers were gifted technically (able to program in a variety of languages; able to build "black boxes" that could spoof telephone systems etc), some of their most successful schemes were accomplished by their brazen social engineering skills.[28] Over the past several years, the brothers were able to run circles around Israel's largest telephone company, Bezeq International, and the people it sent to try to stop the brothers.

> "The Badirs pulled off Mamet-worthy phone cons, employing cell phones, Braille-display computers, ace code-writing skills, and an uncanny ability to impersonate anyone from corporate suits to sex-starved females. On the phone, the brothers morph into verbal 007s, intimidating men, seducing women, and wheedling classified information from steely-voiced security personnel. The phone phreakers' term for this is social engineering: using a combination of brains and guile to obtain codes for trespassing into systems to rejigger them via strings of touch-tone code. Combine this talent with supersensitive hearing - the brothers can dissect an international connection the way wine expert Robert Parker pulls notes from a glass of Bordeaux - and you have what BernieS, a legendary phreaker and contributor to the hacking journal 2600, calls "a formidable skill set."[29]

At one point the chief investigator for Bezeq ordered all phone lines used by the brothers to be shut off. A short time later the people at Bezeq received a second phone call from someone who they swore on their lives was the investigator, only this time ordering those same phone lines to be turned back on. Social engineering exemplified.

Security through availability?

The computer industry has used an interesting approach for keeping network security personnel up to date with the latest news of what hackers are using to break into computer systems. Instead of keeping news of security flaws secret, they are made public as soon as they are discovered. It doesn't matter if the person who discovered the new exploit is a hacker or a security specialist – as soon as something is discovered it is publicized. So if it is found that a few hackers have discovered a new weakness in Windows 2000, it is publicized for everybody to know. Similarly, if a security specialist stumbles upon a new way to exploit Windows, this too is made public. The idea is to get word out of new techniques, weaknesses and tools to as many security specialists as possible. It doesn't matter if this also alerts hackers who were not previously aware of the new exploits.

Table 3: Some examples of widely available security software

Name	Purpose	URL
Back Orifice 2000	Remote Access Trojan Horse	http://www.bo2k.com
Ethereal	Packet Sniffer	http://www.ethereal.com
L0phtcrack	Cracks Windows passwords	http://www.atstake.com/
Nessus	Security scanner	http://www.nessus.org
Nmap	Port Scanner	http://www.insecure.org/nmap
Smurf	Denial of Service Attack	http://www.packetstormsecurity.com
Snort	Intrusion Detection System	http://www.snort.org

You may wonder why a discovery made by a security specialist would be made public. Basically, it is because security people know that there are talented hackers out there, and they know that if one person (the security specialist) was able to discover something new, then it is possible and probable that others (i.e. hackers) will eventually discover the same thing.

This has led to the creation of a number of websites which are frequented by both hackers and security specialists. Some examples include ***WWW.ANTIONLINE.COM***, ***WWW.PHRACK.ORG*** and ***WWW.ROOTKIT.COM***. These sites contain large amounts of detailed security information and software.

For example, ***WWW.ANTIONLINE.COM*** is a website that is designed to teach its readers computer and network security methods and practices. It has numerous forums and articles and appears to be well run. ***WWW.PHRACK.ORG*** contains hundreds of detailed articles on a variety of subjects, including "How to jam a GPS device", "Traffic Lights", "Cisco IOS exploits" and "A stealthy Windows keylogger" to name a few.

WWW.ROOTKIT.COM is a site devoted to helping people obtain root privilege on a variety of operating systems. Multi-user operating systems such as UNIX, Linux and Windows NT/2000/XP, can assign different levels of privileges to different users. This is one way to protect a computer that is used by multiple users. Ordinary users don't need to be able to change important settings. They don't need to be able to uninstall applications intended to be used by many different people. They don't need to be able to change another user's password, for example. And they don't need to be able to read another user's email messages or documents. On the other hand, somebody has to be able to make these types of powerful changes if necessary. So computers that are used by multiple users, and use one of the aforementioned multi-user operating systems will often have one or more users with Administrator (also known as "root" privileges in Unix/Linux operating systems) privileges. Administrator accounts can do anything they want. No files are hidden from them on the system. They can format hard disk drives. They can reset other users' passwords. They can make serious changes to the operating system.

Ordinary users are usually assigned to a group of users with lesser rights. Usually a regular, ordinary user will be able to use some or all of the applications installed on the system, but will not be allowed to make changes to the applications or uninstall them. They will be able to read their own email and access files in their own workspace, but not the files of other users. Finally, they won't be allowed to do anything that could ultimately result in a permanent change to the overall system.

Anyway, when someone is trying to break into a computer system, one of the first things they will want to do is obtain "root" privileges. Then they will be able to change users' passwords, create new accounts, read other peoples emails – and even format hard disks and cover their tracks by erasing various logs. ***WWW.ROOTKIT.COM*** has instructions and scripts that can be downloaded to help someone obtain root on a particular operating system.

There are even books available at ordinary bookstores which teach their readers how to "hack" into a Windows or Linux computer. Many of these books include

CD-ROM's filled with shareware security applications. These are the same programs used by hackers to wreak havoc on their victims. These books are intended to familiarize computer security personnel with common methods used by hackers, but of course they can be picked up and used by anybody, including people with bad intentions.

This proliferation of software and information has had several consequences.

First and foremost, this has made it extremely easy for novice hackers to get their start. Whether they are bored teenagers looking for free games, pornography, or somebody who has more nefarious motives doesn't really matter. What does matter is that the tools needed to do some real damage are available for anybody to download. For example, scripts such as those designed to obtain root privileges allow unskilled people to do some serious things they wouldn't ordinarily be able to do. In addition, the availability of information benefits the experienced hacker by helping them keep up to date with what security professionals are looking for.

On the other hand, it has also helped individuals and organizations improve the level of security for their networks and computers. What better way to test a network's security defenses than using the exact same software as a hacker would? Whenever you make a major network change and want to check the security implications you can download the latest software and try the most up to date methods and see how your security holds up. In addition, whenever new exploits or weaknesses are discovered, security professionals can quickly check to see if their networks need work. So you can look at the widespread availability of information and software in two ways – while it does help the hacker, it also helps security personnel. The bottom line is the security world feels the benefits of widely available tools and information outweighs the risks it has created.

Conclusion

In conclusion, this paper was designed to provide an introduction to several important issues facing computer users today. Not everybody who uses the Internet has a technical background. Many are uncomfortable with performing what I would consider to be basic activities. Yet due primarily to the ease of use of recent mainstream software, as well as the proliferation of broadband connections, increasing numbers of these non-technical people are successfully using the Internet on a regular basis. I suspect that many of them diligently update their antivirus definitions, and periodically visit the Windows Update website, which are good things to get into the habit of doing. But they are not nearly enough. This is also just a suspicion of mine, but I suspect that many of these aforementioned people probably consider themselves relatively secure because they have done these things. On the other hand, I also think that things are probably changing for the better. The national media regularly reports on the latest viruses and denial of service attacks etc, and ISP's also try to alert their users to the perils of modern day computing. But they also leave the average

person unaware of many of these important issues. You never hear on CNN that the average $50 wireless router can be detected thousands of feet into the air. You never hear the importance of practicing a smart password policy. These are important things that really aren't all that complicated or difficult to do.

While it is easy to understand how the individual user with no formal computer training can be ignorant of security practices, it never ceases to amaze me when I read about business or government run networks that use default settings. These are easy things to do. I know that in the real world many network administrators are expected to shoehorn security duties into their already busy schedules, and that things like this are often overlooked. Hopefully this too will improve with the added recognition of the importance of good security. At any rate, it costs a company next to nothing to change default settings, and while that isn't enough to derail a skilled adversary, it does make it harder for the potential intruder. Same goes for enforcing a password policy for employees. How hard is it to make it a rule that passwords are no longer allowed to be written on Post-It-Notes attached to the side of a monitor? While enforcing the policy may prove easier said than done, it would also serve to educate the employees on the dangers of both inadequate passwords and unsafe password practices.

In this day and age, the consequences of ignoring security are just too great. For all people who use the Internet, the risk of somebody gaining access to personal or financial information is enormous. Yes damage can be undone, but at what price? It is now estimated that it takes the average victim of identity theft in excess of 600 hours to undo the damage done.[30] Some take longer. Some people end up having all of their money stolen from their bank accounts; others face possible bankruptcy when a hacker steals their Quicken file with all of their credit card numbers and goes on a spending spree. And what happens when the person who has stolen your money or credit card numbers is in another country and able to avoid law enforcement?

But it should also never be forgotten that bad things can still happen even though a person or business has utilized all possible security safeguards. It is very difficult to stop a skilled and determined person from breaking into a computer they have targeted. Fortunately some of the troublemakers are of questionable skill – i.e. script kiddies. But not all are. Some are highly skilled and patient people who are willing to do whatever it takes to reach their objectives. The Badir brothers in Israel are an excellent example. Everybody knew what they were up to – yet the brothers were able to largely go uncaught. Another example is the hacker who Clifford Stoll relentlessly chased through the early Internet (discussed in his book "The Cuckoo's Egg"). In that case, a foreign agent attempting to hack into U.S. government, military and research computers was noticed by Berkeley astronomer/computer administrator Clifford Stoll. Both the hacker, who was caught over a year later, and Cliff, who was instrumental in catching him, demonstrated great skill and patience. It took an almost obsessive

effort by Stoll to keep up with and eventually gain the upper hand on his adversary.

As I have learned more and more about computer security, I keep coming back to the idea that every security measure taken helps to reduce the number of people who are skilled enough to break into that system. What does this mean? First of all, I recognize that there are highly skilled people with bad intentions who are capable of defeating strong security – Group A. They are patient and determined and can come up with novel ways to defeat entrenched security. These people are difficult to stop. On the other hand, there is also another group of potential hackers out there – Group B. These people have significantly less skills than the first group. They use all of the standard programs and scripts and methods to break into systems. The tools that they use have probably been developed by others. So-called script kiddies fall into this group. Fortunately, I suspect that Group A is significantly smaller than Group B.

The way I look at it, every worthwhile security measure that is taken makes it a little more difficult to break into a system. In the case of a wireless LAN, just disabling the broadcast of the SSID isn't going to stop anyone who is halfway skilled or determined. Neither will enabling MAC address filtering or changing the default SSID to something unique. But if you do all three, you might make breaking into your network just difficult enough to deter the average member of Group B.

Appendix A – Sample social engineering email message

FROM MRS. ANGELA JOHNSON

FROM:JOHANNESBURG,SOUTH AFRICA.

E-mail: angelajohnson_ff@yahoo.co.in

ATTN:DIRECTOR/CEO,

You might be surprise to receive this letter from me since you don't know me personally. I am MRS. ANGELA JOHNSON the wife of late MR MICHAEL JOHNSON who was murdered by the Zimbabwe war veterans and irate black people. I got your contact e-mail address through South Africa chamber of commerce and industry. After due consideration of your profile,hence I decided to write to you. I write to solicit for your special assistance to my family shattered by a tyrannical Government led by a dictator and his (ZANU-PF) ruling party. President Robert Mugabe.
Because of land and farm land crisis in Zimbabwe the Government Secretly sponsored the war veterans and some irate party members to disposed the land being occupied by the white farmers. This action has led to killing of some members of opposition party including my husband who did not support this ill-fated action.
But before the death of my husband, he anticipated some dangers and so he smuggled out the sum of US$14.6 million dollars (Fourhteen point six million united state dollars) to South Africa and deposited it in a Security Company with the intention of using it for the purchase of farm machinery and chemicals for agricultural purpose in South Africa and establishment of a new farm in Swaziland.
This money was deposited in a box as a germ stone to avoid much demurrage in the Security Company. On the 29 august 2001 the warveterans and some spotters of (ZANU-PF) ruling party trooped into our compoud and axed my husband to death and my second son of 22yrs. Since then they have been terrorizing my son Antony but he managed to escape to neighbouring country South Africa as a political asylum seeker (refugee).
His position in South Africa dose not permit him to open an account or to oparate any business. That is why I want this fund to be transferred in your account so that you will assist him to invest the money in your country. I must let you know that this transaction is 100% risk free. If you accept to assist us, all I want from you is to arrange and come down to Johannesburg South Africa so that you can help him to open a non-resident bank account in your name which will aid us in transferring the money into your nominating account overseas. I have two option for you, firstly, you can choose to have certain percentage of the money for nominating your account in this transaction or we can go into pertnership with you for the proper profitabel investment of the money in your country whichever the option you want feel free to notify with him. He will then furnish you with every

detail you needed to know. We have also mapped out 5% of the total sum for any expenses that might be incurred during the time of this transction.
If you do not prefer a partnership, we are willing to give you 25% of the money while remaining 70% will remain for my family, if you are really capable and willing to assist us please contact him immediately in South Africa with this e-mail that I used to sent this mail to you.
Finally please treat this mater as urgent as possible, I'm in dire him to leave that country soonest. Thanks for you're mutual co-operation. I expecting your soonest and urgent response. And you can please contact my son ANTONY with this number .(+27-83-2382247)

Best Regards,

(MRS ANGELA JOHNSON)

References

"2003 CSI/FBI Computer Crime and Security Survey." Computer Security Institute. Feb. 2004. <http://www.gocsi.com/forms/fbi/pdf.jhtml>.

Brewin, Bob. "War flying: Wireless LAN sniffing goes airborne." Computerworld. Jan. 2004. <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,73901,00.html>.

Brewin, Bob. "Worldwide 'war drive' exposes insecure wireless LANs." Computerworld. Jan. 2004. <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,74103,00.html>.

Carr, Jim. "Biometric Devices: The Next Wave." Network Magazine. March 2004. <http://www.networkmagazine.com/article/NMG20011003S0009>.

"CERT/CC Statistics 1988 – 2003." CERT Coordination Center. Feb. 2004. <http://www.cert.org/stats/cert_stats.html>.

"Cisco Comments on Recent WLAN Security Paper from University of Maryland." Cisco. March 2004. <http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm>.

Cuadra, Fernando De La. "How an antivirus program works." Help Net Security. March 2004. <http://www.net-security.org/article.php?id=485>.

"Dealing with the Klez Virus." SCSB.ORG. Feb. 2004. <http://www.scsb.org/klezinfo.htm>.

eTrust Threat Information Center. Feb. 2004. <http://www3.ca.com/virusinfo/glossary.aspx#W>.

"Facts and Statistics." Identity Theft Resource Center. Feb. 2004. <http://www.idtheftcenter.org/facts.shtml>.

"Global Melissa Virus Information Center." F-Secure. Feb. 2004. <http://www.f-secure.com/melissa/>.

"Glossary." Symantec Security Response. Feb. 2004. <http://securityresponse.symantec.com/avcenter/refa.html>.

Johnston, Gretel. "The golden age of hacking rolls on." Computerworld. Jan. 2004. <http://www.computerworld.com/securitytopics/security/story/0,10801,75381,00.html>.

Kaplan, Michael. "Three Blind Phreaks." Wired Magazine Feb. 2004. <http://www.wired.com/wired/archive/12.02/phreaks_pr.html>.

Kaspersky, Eugene "Macro Virus Epidemics." Viruslist.COM. Jan 2004. <http://www.viruslist.com/eng/viruslistbooks.html?id=15>.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. 3rd ed. New York: Osborne/ McGraw-Hill, 2001.

"Microsoft Knowledge Base Article – 163932 – Frequently Asked Questions about Word Macro Viruses." Microsoft. Feb. 2004. <http://support.microsoft.com/default.aspx?scid=kb;en-us;163932>.

Morris, Chris. "Intrusion Detection FAQ – What do you do after you deploy the IDS?" SANS. Jan. 3, 2001. Feb. 2004. <http://www.sans.org/resources/idfaq/deploy.php>.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey. Inside Network Perimeter Security. Indianapolis: New Riders Publishing, 2003.

"Norton Antivirus Knowledge Base: What is the difference between viruses, worms and trojans?" Symantec. Feb. 2004. <http://www.symantec.com>. Path: Support; Security Response

Pfleeger, Charles P. Security In Computing. 2nd ed. Upper Saddle River, New Jersey: Prentice Hall, 1997.

Schneier, Bruce. Applied Cryptography. 2nd ed. New York: John Wiley & Sons, 1996.

Stoll, Clifford. "Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage." Pocket Books: 2000.

Tanenbaum, Andrew S. Computer Networks. 3rd ed. Upper Saddle River, New Jersey: Prentice Hall, 1996.

"The ABG's of Wireless LAN – Technology Overview." Feb. 2004. Netgear. <http://www.netgear.com/pdf_docs/ABGs_of_Wireless_2.03_web.pdf>.

"The History of Computer Viruses – A Timeline." EXN.CA – Discovery Channel Canada Online. Feb. 2004. <http://www.exn.ca/nerds/20000504-55.cfm>.

"Trojan Horse Attacks." IRCHelp. Feb. 2004. <http//www.irchelp.org/irchelp/security/trojan.html>.

"Trojan Horses: Back Orifice and Netbus." Digifriends. Feb. 2004. <www.digifriends.com/highlights/trojan_horses.shtml>.

Vaughan-Nichols, Steven J. "Making the Most from WEP." Wi-Fi Planet. Feb. 2004. <http://www.wi-fiplanet.com/tutorials/article.php/2106281>.

Wang, Wallace. Steal This Computer Book 3. San Francisco: No Starch Press, 2003.

"What are Polymorphic Viruses?" Internet Guide. Feb. 2004. <http://www.internet-guide.co.uk/polymorphic-viruses.html>.

Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/M/MAC_address.html>.

Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/S/SSID.html>.

Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/v/virus.html>.

Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/W/WEP.html>.

End Notes

[1] "CERT/CC Statistics 1988 – 2003." CERT Coordination Center. Feb. 2004. <http://www.cert.org/stats/cert_stats.html>.

[2] "2003 CSI/FBI Computer Crime and Security Survey." Computer Security Institute. Feb. 2004. <http://www.gocsi.com/forms/fbi/pdf.jhtml>.

[3] Cuadra, Fernando De La. "How an antivirus program works." Help Net Security. March 2004. <http://www.net-security.org/article.php?id=485>.

[4] Webopedia. Jan. 2004. < http://www.webopedia.com/TERM/v/virus.html>.

[5] "Norton Antivirus Knowledge Base: What is the difference between viruses, worms and trojans?" Symantec. Feb. 2004. <http://www.symantec.com>. Path: Support; Security Response

[6] "Norton Antivirus Knowledge Base: What is the difference between viruses, worms and trojans?"

[7] "Norton Antivirus Knowledge Base: What is the difference between viruses, worms and trojans?"

[8] "Norton Antivirus Knowledge Base: What is the difference between viruses, worms and trojans?"

[9] "Global Melissa Virus Information Center." F-Secure. Feb. 2004. <http://www.f-secure.com/melissa/>.

[10] Kaspersky, Eugene "Macro Virus Epidemics." Viruslist.COM. Jan 2004. < http://www.viruslist.com/eng/viruslistbooks.html?id=15>.

[11] "The History of Computer Viruses – A Timeline." EXN.CA – Discovery Channel Canada Online. Feb. 2004. <http://www.exn.ca/nerds/20000504-55.cfm>.

[12] "Microsoft Knowledge Base Article – 163932 – Frequently Asked Questions about Word Macro Viruses." Microsoft. Feb. 2004. <http://support.microsoft.com/default.aspx?scid=kb;en-us;163932>.

[13] Wang, Wallace. Steal This Computer Book 3. San Francisco: No Starch Press, 2003. p.74

[14] eTrust Threat Information Center. Feb. 2004. <http://www3.ca.com/virusinfo/glossary.aspx#W>.

[15] "Glossary." Symantec Security Response. Feb. 2004. <http://securityresponse.symantec.com/avcenter/refa.html>.

[16] Wang, p.93

[17] Wang, p94

[18] "Trojan Horse Attacks." IRCHelp. Feb. 2004. <http//www.irchelp.org/irchelp/security/trojan.html>.

[19] "What are Polymorphic Viruses?" Internet Guide. Feb. 2004. <http://www.internet-guide.co.uk/polymorphic-viruses.html>.

[20] Brewin, Bob. "Worldwide 'war drive' exposes insecure wireless LANs." Computerworld. Jan. 2004. <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,74103,00.html>.

[21] Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/W/WEP.html>.

[22] Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/S/SSID.html>.

[23] Webopedia. Jan. 2004. <http://www.webopedia.com/TERM/M/MAC_address.html>.

[24] "Cisco Comments on Recent WLAN Security Paper from University of Maryland." Cisco. March 2004. <http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm>.

[25] Vaughan-Nichols, Steven J. "Making the Most from WEP." Wi-Fi Planet. Feb. 2004. <http://www.wi-fiplanet.com/tutorials/article.php/2106281>.

[26] Morris, Chris. "Intrusion Detection FAQ – What do you do after you deploy the IDS?" SANS. Jan. 3, 2001. Feb. 2004. <http://www.sans.org/resources/idfaq/deploy.php>.

[27] Carr, Jim. "Biometric Devices: The Next Wave." Network Magazine. March 2004. <http://www.networkmagazine.com/article/NMG20011003S0009>.

[28] Kaplan, Michael. "Three Blind Phreaks." Wired Magazine Feb. 2004. <http://www.wired.com/wired/archive/12.02/phreaks_pr.html>.

[29] Kaplan

[30] "Facts and Statistics." Identity Theft Resource Center. Feb. 2004. <http://www.idtheftcenter.org/facts.shtml>.

Last Updated: August 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced