A Review on Safety Issues of Internet Security

Dr Jammi Ashok
School of Electrical and Computer Engineering
Hawassa University, Hawassa, Ethiopia

Dr J. Vijipriya
School of Informatics
Hawassa University,Hawassa, Ethiopia

Abstract - This paper describes a review on safety issues of cyber security. Now a days, internet security is a flattering issue. Many broadcasting organizations and government officials vigorous it just as grave a threat as fanatic attacks, nuclear explosion and worldwide warming. With countless saleable, government and private schemes connected to the Internet, the concern appears acceptable. In the period of e-commerce, this review on internet security/cyber security gives a basic knowledge of security threats and an overview of how to protect the network.

Keywords: Threat, virus, worms, adware, spyware

I. INTRODUCTION

Though the vast majority of Internet users are honest and benign, there are a few who, motivated by greed or maliciousness, attempt to directly or indirectly harm the computer network. They can destroy operating system, damage data, steal information, overwhelm Web sites and clog e-mail servers. Even if the network isn't connected to the Internet or other networks, it's still vulnerable to attacks transported by diskettes or CDs, or from individuals with access to the network. Virus or worm outbreaks large enough to make the news happen nearly every week and many, many more go unreported. Corporate firewalls routinely log thousands of probes by hackers' everyday.

II. THREATS TO THE NETWORK

2.1VIRUSES

A Virus is a piece of software code or program that is written specifically to infect a computer. The effects of a virus can range from humorous text being displayed on the monitor to the destruction of all the files. The ability to infect varies from virus to virus, as does the damage they can cause. There are more than 70,000 known computer viruses with new ones being identified every day.

In the old days before the Internet a virus was only able to spread itself via floppy disk. The preferred method at present is e-mail. The virus is sent as an attachment to an email and its payload is delivered when the unsuspecting victim opens the attachment. Often the sender will put a message designed in such a way that anybody will be tempted to open it. The most famous virus through email was the "I Love You" virus which caused worldwide chaos. As soon as the attachment is opened it scans the Address Book of the recipient and e-mails itself to every address present there. The e- mail then looked as though the recipient had sent it.

Viruses are roughly categorized into subgroups such as common file- infecting viruses, worms, Trojan houses, macro viruses, and others. There is also an entire family of related hoaxes that may be damaging but aren't actually viruses. These hoaxes usually arrive in the form of an e- mail that gives a warning against a nonexistent virus or attempts to convince the user to do something that will ultimately damage the user's computer.

2.1.1 FILE- INFECTING VIRUSES

File- infecting viruses are the most common ones in the virus family. They infect executable files by adding their own code to that of the original file. As soon as user runs the infected file, the virus attaches itself to other executable files on user's hard disk. When user transfers infected files to another computer, the virus goes along for the ride and finds more files to infect.

2.1.2 WORMS

Worms are self-replicating viruses. Unlike an ordinary virus, which depends on the transfer of a host file in order to replicate, a worm is an independent entity that usually spreads itself without needing a computer user to transfer a file. Many of the newer computer viruses that make the news are worms.

Worms tend to spread very rapidly and can cause a lot of damage- In September 2003, the Swen worm infected 1.5million computers and clogged e-mail boxes around the world with fake Microsoft patches, causing massive inconvenience even for uninfected users.

2.1.3 TROJAN HORSES

A Trojan Horse(or Trojan only) does not replicate itself and is technically not a virus. A Trojan horse is a software program, often a game or utility that seems to do one thing but has incorporated within itself another, secret function that will cause damage, pass on information about the user's computer, or enable its sender to hack user's computer.

Some Trojan horses are used to spy on user's activities and steal information. However, the hackers that use Trojan horses to get to user's PC are usually not at all interested in user's data. What they are after is a PC with an "always up" broadband connection to the Internet. When they find a vulnerable PC, they use it to distribute pornography or spam e-mail or launch a Distributed Denial of Service (DDoS) attack in which they use remote PCs to attack a Web site or e-mail server. The reason they use user's PC as a host for these activities is because, to the recipient, it looks like the unwanted traffic coming from user's machine. This hides the culprits from ISPs and law enforcement agencies, making them nearly impossible to trace the origin.

2.1.4 MACRO VIRUSES

Macro viruses are written in the internal macro language provided with many applications. Many programs enable user to extend the macro language provided with an application with more complex programming languages, so that user can set up very complex routines as macros. It is very easy to write viruses or modify existing viruses within this format. Because macro viruses are so easy to write and modify, new ones pop up all the time especially within Microsoft Word and Microsoft Excel files- with thousands of variants identified. They spread easily because they travel in documents, which are often shared unlike executable files- and also because many of them, in worm-like fashion, e-mail themselves to everyone they find in the user address book. Additionally, because macro viruses spread within an application, they may spread between operating systems, for instance from a PC to a MAC!! Macro viruses activate when an infected document is opened, the degree of damage varies depending on the particular virus.

2.1.5 BOOT SECTOR VIRUSES

Boot sector viruses infect the boot sector on a floppy disk or the Master Boot Record (MBR) on a hard disk by overwriting the original boot code with its own code. A virus that infects these sectors is especially dangerous because every time user starts up his computer, it's loaded into memory from where it can spread to other parts of the hard disk or to another disk. Boot sector viruses frequently cause a complete system failure in which user's PC can't start up or find its hard drive.

2.2 INVASIVE SOFTWARE

Adware, Spyware, Scumware, Drug Dealer ware and Theftware are all kinds of software that arrive on user's computer without user permission or sometimes with user permission and polluting user's screen with ads, popups, sending information about user to the Internet, and generally making a nuisance of themselves by slowing down user's system or even causing system crashes, Some of these nasty soft wares are actually more like a stealth viruses or Trojan horses, loading itself without user's permission, hiding out in user's system, and resisting removal.

2.2.1 ADWARE

Adware is commonly acquired when user downloads from the Internet, Freeware or Shareware(software available for free or for a small fee). In the usual scenario, user decides to download a program- often a game or useful utility- that's available free on the Internet. When user downloads the software, user has to click through a page of unintelligible legal stuff that includes things like copyright and, in the very fine print, permission to install Adware along with the software. When user clicks okay to download the software, soon user may start noticing that there are more popup windows than usual.

2.2.2 SPYWARE

Spyware sneaks into user's computer without asking for user permission. Some Spyware even does a "drive- by download" and installs itself when user visits a Web page- sometimes as a mere cookie and sometimes even as a complete application.

Spyware often hides itself to that it's difficult to find and eradicate from user hard disk. Some Spyware will resist from being removed and even take parts of the operating system when attempt is made to eradicate it. While user is browsing the Web, Spyware is more likely engaged in antisocial behavior such as sending personal information to a third party, resetting the home page or altering system files. One of the dangers of Spyware is key logging, which enables it to record anything user types, including user's passwords, e-mail messages, real- time chats and credit card numbers. Some Spyware can even spy on user by using user's own Webcam!

2.3 SPAM

Spam is unsolicited junk e-mail which can take the form of chain mail, mass e-mailing and advertisements, threatening or abusive e-mail etc. Generally it is something that one does not want to receive and costs money to download and then delete.

Spammers get hold of user's e-mail address from a variety of sources. User may have filled the information in a form on a website or subscribed to a newsletter. User may have posted a message to a newsgroup or another user. ISP may have a directory of all its users- the equivalent of a phone book for the internet. The spammer may simply buy a list of e-mail addresses from a website that holds user information in its database. They also use tools called ”harvesters” which scan the Internet and newsgroups and collect e-mail addresses.

2.3.1 ADVERTISING SPAM

Most spam is advertising and most of what spam advertises is deceptive or fraudulent. Popular advertisements include get-rich-quick business opportunities, won0 lottery- jackpot announcements, work- at-home schemes, miracle cures, dubious investments, illegal cable descrambler kits, credit and credit repair offers, vacation prize scams etc. Spammers send advertising through e-mail because it's cheap .(almost free)

2.3.2 DANGEROUS SPAM

Some spam will bite by carrying viruses or by trying to lure the user into providing credit card numbers. Some dangerous "spam" e-mail comes, not from spammers, but from worms, that generate infected e-mail from the computers of unsuspecting hosts.

Recently, many people got e-mails that appeared to be from eBay or Pay Pal telling them that they needed to update their accounts. The e-mails looked real, complete with the appropriate logos, and provided a link to what looked like legitimate eBay or Pay Pal Web pages. Unsuspecting users who filled in the requested information found their credit card numbers and sometimes their very identities stolen. Con men and thieves have entered the high-tech age and are using Internet spam as a cheap way to run their con games.

2.4 HACKERS

At the beginning of the computer age, the word "hack-er" referred to a person who was very good with computers. Today, the same word usually refers to a person who maliciously breaks into networks, breaks the security on application software or creates viruses.

The hackers we hear the most are the system crackers who hack into individual computers or into networks. They've broken into networks at banks, universities and military bases. Corporate networks are common victims – most have been hit by hackers at least once.

Hackers change Web sites, access unauthorized services, alter and remove files, and steal information. Hackers can and do cause very serious damage to systems and have even been known to erase evidence of their activities by altering logs, leaving network administrators unaware they've been hacked.

2.5 COOKIES

Cookies are small text files that are created when user visits a web site. The web site uses the cookie to remember who the user is and what he has visited or purchased from their site, The cookie is placed on the hard disk and can be retrieved by the web site the next time the user visits. Cookies can be very useful and will prevent the user to type the same information every time. User can personalize a web page and it will look the same when visited again.

Cookies may also be used by the other web sites to gather information about the user without his knowledge. A security hole has been discovered in Internet Explorer Ver. 4&5 that allows web sites to read cookies set by other web sites. Now, it has been fixed in version 5.5.

III. BUILDING EFFECTIVE NETWORK SECURITY

3.1 MAKE A PLAN

For effective network security, one needs to execute a plan. How much network security is required, depends on size of the network is, how much it interacts with the internet, and what is the tolerance for risk.

Generally, the larger the network, the more formalized the plan should be. For a small network with a dialup connection, the entire plan can be to keep the virus software updated and not to open any suspicious e-mails. A large enterprise network may require a complex, well-choreographed, thoroughly documented plan implemented after a formal risk assessment and analysis of the network. **A typical Security plan should include**:

3.1.1 EDUCATION

The first line of defense against security threats from the Internet is education and common sense. Keep update about the latest hoaxes and viruses. There are many well- known web sites that specialize in tracking these things.

3.1.2 BE SUSPICIOUS

Be suspicious- a suspicious mind is definitely an advantage on the Internet. Learn to be on the lookout for anything that doesn't look "right"

3.1.3 AVOIDING SPAMS

There are several ways of avoiding Spam. The first is to use common sense- share e-mail address with those persons from whom e-mail is expected. If a web site asks for one's e-mail address, read their privacy policy which should clearly state that they will not pass on the details to any third party and they will not send unsolicited e-mails.

If it is necessary to give e-mail address then get a web based e-mail account just for that purpose. Some ISP"s also allow to have several e-mail addresses for one user. Set up one for this purpose and if , in any case, it starts to receive large amounts of Spam then close it and use another account. If e-mail address is posted in a newsgroup or similar then disguise it so that a harvesting program will not be able to use it.

Do not reply to Spam- this will only confirm to the spammer that it is a valid e-mail address and ultimately this will appear on many more lists.

3.1.4 USE CAUTION WHEN OPENING E-MAIL

Most viruses arrive in e-mail travel as attachments and infect the computer. The most infamous of these is the Bubble Boy virus, which carries the subject line “BubbleBoy is back!”If email is opened or even previewed, it will forward itself to everyone in the computer outlook address book.

3.1.5 USE CAUTION WHEN OPENING E-MAIL ATTACHMENTS

The most common way to acquire a virus is in an e-mail attachment. Ideally, an antivirus program should be installed. However, a virus filter isn’t completely foolproof as new viruses are created every day. As a rule, don’t open any suspicious attachments. It may consider suspicious if it’s from some unknown person. If it’s an unexpected attachment from someone known, check with that person before opening it.

If the attachment is a document created in a program that supports macros; upon opening the document, usually a dialog window asks the permission to start the macro. Choose “no” to prevent possible macro viruses from spreading to the computer.

3.1.6 BE CAREFUL WHEN DOWNLOADING SOFTWARE

The best way to download software is to first do an Internet search on it to see what kind of a reputation the software has. Carefully read any licensing agreements before clicking on the “ agree” button and consider using software that guard against unwanted Adware.Then download the software and scan it with antivirus software before installing it onto the hard disk.

3.2 ACCESS POLICIES

Although this article focuses on network threats that come from outside, be aware that security breaches happen “at home,” too. Anyone with network access can steal or damage data or networking devices. No amount of firewall protection is going to save a server if someone steals it. Take time to look at who has access to what, keep essential network devices under lock and key, and implement a password access policy to sensitive data. Good encryption techniques should be used especially on Wi- Fi network.

3.3 SOFT WARES THAT PROTECT THE NETWORK

3.3.1 ANTIVIRUS SOFTWARE

A crucial component of the security plan is virus software. There is no such thing as ideal antivirus software, and different products have different strengths and weaknesses. Antifirus software should be installed at the gateway – where the network meets the Internet, at the server level, and at the desktop. The software at the gateway screens out most infections before they get into the network, Regular scans of hard disks on servers and desktop PCs should pick up the rest, Software on desktop PCs should also be set to scan portable media in order to nab viruses that arrive, not through the network, but on diskettes and CDs.

3.3.2 KEEP UPDATED

To stay effective, antivirus software needs to be constantly updated with the signatures of recently discovered viruses. In fact, all the antivirus softwares enable the user to be automatically updated over the Internet.

3.3.3 PATCH HOLES

Modern software is very complex, making it difficult to be thoroughly tested for security holes. Often these holes are discovered after software has been out for a while. At this point, the vendor normally releases a software patch, usually available on its Web site, Many computer break-ins can be prevented simply by keeping on software patches up- to –date. Regularly schedule a check of software patches issued by the software vendors and use them where needed.

Remember, do NOT install software patches that arrive unsolicited through e- mail. They may be worms.

3.3.4 DON’T USE FILE-SHARING PROGRAMS

File-sharing programs such as Kazaa and Grokster are major culprits when it comes to dumping Adware and Spyware on the computer. They usually inform in disclosure box that they are supported by – and will install- Adware. Read this box carefully before clicking on the "agree" button- One may be agreeing to as many as ten different Adware programs.

Some even install Spyware without any information. This Adware may be very difficult or impossible to remove from the system. If in any case, one removes the Adware, The file-sharing program may not work without the Adware.

SOME MISCELLANEOUS SECURITY PRECAUTIONS

- Give only minimum required information when registering for a new software or buy something online.
- Turn off computers when they are not in use –PCs can't be hacked when they're off.
- Some e-mail programs have multiple security holes making them easily infected. Don't just use the e-mail reader that came with the operating system-shop around for the most seure program user may find that fulfills the needs.
- Disinfect PCs with antivirus software before connecting them to the network.
- Scan all removable media.

3.4 FIREWALLS

A firewall controls traffic between a private network and the Internet in order to intercept outsiders trying to break into the private network. Firewalls protect Computer/ Computer networks from intentional hostile intrusion that can ,compromise confidentiality, cause data loss or denial of service.

3.4.1 HOW FIREWALLS WORK

The firewall blocks unwanted traffic while letting through the legitimate traffic. It makes decisions that allow or deny access to services.

A firewall enforces the access control policy, but it's up to user to decide what access control policy is. He may block whole ranges of ports- everything that is not required to open. Firewalls generally come preconfigured to deny all access to all ports. It's then up to the user to instruct the firewall to allow network traffic through to specific ports on specific PCs in the network.

When a request for a service is made, the firewall inspects the request to make sure the type of request matches an available port. Only traffic for advertised services is allowed through the firewall- all other traffic is dropped.

The firewall hides computers from the Internet altogether if they don't provide services to Internet users. For instance, if only connection to the Internet is for e-mail, the firewall can be set to only let e-mail traffic through to the appropriate server, shielding the rest of the network from the outside,

3.4.2 KEEPING TRACK OF THE FIREWALL

A firewall is valuable for its logging and auditing functions, providing summaries about what type and volume of traffic passed through it, and also the kinds of break-ins were attempted. The logs will show where hackers are trying to break in. User should examine logs on a regular basis- preferably once a week- and adjust the firewall accordingly. Some ports are favorites with hackers (e.g. Telnet) and he may pay special attention to access these ports. User should scan regularly the network to find open ports and block any unused port if find open.

3.5 BACKUP AND RECOVERY

It's easier and less expensive to prevent problems before they happen, but even in well- defended networks, it should be assumed that eventually the unthinkable will happen – a virus will get through and spread among the PCs or a hacker will break into the system and destroy files. And remember, there are other, more mundane dangers to the network- for instance, equipment failure, flood, or theft- that can cause at least as much damage as a virus infection. With a bit of planning, user can restrict problems and restore the network quickly.

Back up files on a regular basis so if the network is invaded, it can be restored with backup copies. With regular nightly backups, the worst virus infection will never cause the loss of more than a day's data. Backup copies should always be stored on hard media in a separate location- NOT on a server connected to the network.
Have a plan to cover unexpected disaster. In case of a virus infection, one should have a clear plan for disinfecting PCs and restoring data. If anything in absolutely mission critical, one should even have a plan in place for replacing hardware that goes offline for purely mechanical reasons. Eradicating viruses and restoring lost data may. Unfortunately, be the easiest part of recovery.

IV. CONCLUSION

Every network administrator is faced with this dilemma" the Internet can be a dangerous place for the network, but the network needs to be connected to it. What one can do is reduce the risk to an acceptable level by implementing the following steps:

- Have a plan.
- Use common sense and know what to avoid.
- Keep viruses and other nasty programs at bay with the appropriate soft wares.
- Change password regularly.
- Protect Internet- connected networks with a firewall.
- Back up data on a regular schedule.

REFERENCES

[1] Cryptography and Network Security, Third Edition by William Stallings.
[2] http://www.spammotal.com/
[3] http://www.microsoft.com
[4] http://www.mcafeeasap.com
[5] http://www.cert.org
[6] http://csrc.nist.gov
.