

MAJOR THREATS TO INFORMATION SECURITY
John Peter Jesan
Doctoral Student
Graduate School of Computer Information Sciences
Nova Southeastern University

[John Peter Jesan is a Software Engineer / Infosec Professional working in CitiStreet, a joint venture of State Street and Citigroup companies. He is also a Doctoral Student in Computer Information Systems at Nova Southeastern University, Fort Lauderdale, FL. His area of research interest is Information Security. He got certified by National Security Agency(NSA) for Information Security Management. He is currently working on HIPAA Compliance Project in CitiStreet. He is a professional member in ACM, and an associate member in Sigma Xi (An American Research Society).

Nowadays, information is one of the very important assets in almost all organizations. Once the internal networks of those organizations are connected to the Internet, it becomes a potential target for cyber attacks. In order to secure the systems and information, each company or organization should conduct a self-hacking-audit, analyze the threats and eliminate it before getting any problem. This paper explains about the main goals of information security, its major threats and some suggestions to prevent the systems from major threats.

1. INTRODUCTION

The main goals of information security are Confidentiality, Integrity and Availability. Confidentiality means the information available on a system should be safe from unauthorized people; better examples would be customer credit card information, patient medical information in hospitals or personal information of employees in an

organization. If that information is not secured, the company or the organization involved in that will eventually lose its reputation and business.

Integrity means the information available in an organization should be complete and whole. It shouldn't be altered by any unauthorized person. Intentional or unintentional attacks on the information will cause severe damage and finally the information becomes unreliable. One of the best examples would be account holders' information in a Bank. If something happens to the banking information, it is devastating and the Bank will be in danger of losing its customers and business. In fact, in such cases, it may face a lawsuit too.

Availability is as important as Confidentiality and Integrity. It means the information requested or required by the authorized users should always be available. For example, assume that a company is hit by a hurricane and it has lost its computers and data. In such situations, the affected company should be able to install new computers and recover its data from backups. Suppose, if proper backups are not available, the concerned company cannot recover the data and resume its operation.

So whenever a company or an organization develops an application, it should focus on the above goals and accordingly develop the system, test it and release it with proper documentation.

2. MAJOR SECURITY THREATS

The main categories of the threats for the information security are as follows:

1. Intrusion or Hacking
2. Viruses and Worms
3. Trojan Horse
4. Spoofing
5. Sniffing
6. Denial of Service

2.1 Hacking

It is nothing but gaining access to a computer system without the knowledge of its owner. The people who do this kind of unlawful things are called as hackers. Once they get access to targeted systems, they can alter data available on those systems or steal private information such as SSN, personal information and sometimes some sensitive information related to bank and credit card accounts. Most of the targeted systems for hackers are eCommerce websites, individual machines and sometimes bank websites that provide facility for online banking. The targeted systems for hacking are depending on the hackers and their personal types. Some people will do hacking just for fun and curiosity.

In order to do hacking, hackers has to crawl on the targeted systems and gather the information about its strength, weakness, operating systems used, unsecured folders, shared folders, configuration files etc. They will collect all these data and do analysis about how to compromise the targeted website or system. Once they find a way, they will enter through that, and try to exploit the systems. Some hackers will use Trojan horse programs to gain access to the targeted systems. Trojan horse programs are very dangerous threats for eCommerce websites and even for personal machines.

Some of the techniques or loop holes that Hackers use for hacking are as follows:

1. Poor Implementation of Shopping Carts
2. Hidden fields in the html forms
3. Client-side validation scripts
4. Direct SQL attack
5. Session Hijacking
6. Buffer Overflow Forms
7. Port Scan

In order to prevent the systems from these kinds of attacks, most of the eCommerce websites and even single users have started to use good firewall systems; whenever there is an attack, the firewall systems reports immediately and sometimes it helps to track the attack.

Hackers can always penetrate firewall systems by some sort of new ways and hence it is always better to conduct a vulnerability test before releasing systems for operation.

2.2 Viruses and Worms

Viruses and Worms are computer programs that make computer systems not to work properly. There is a subtle difference between Virus and Worm; both can replicate itself, but when traveling on the network, Virus needs a carrier file. It can't travel on its own on the network; where as Worms can travel on its own without anything. It doesn't actually need any infected file to stick in.

Viruses and Worms are really annoying problem for all systems. The ultimate aim of these Viruses and Worms are making a good working system to malfunction and sometimes worms can sniff in and steal private information to send it to its creator. As per Trendmicro, so far 60,000 viruses have been identified and 400 new viruses are getting created every month. Earlier days, Viruses were spreading through floppy diskettes. Nowadays, it spreads through Internet, which is a broad gateway for these malicious programs. It can spread quickly and affect all systems in an organization within a minute and can create millions of dollar loss for the organization in a minute.

Viruses can be classified into different categories as given below depending on the way it affects the systems.

- *Polymorphic Virus* : It changes its signature with every infection
- *Stealth Virus*: This virus has to change something to infect the system. After changing something, it has to gain control over some system functions to hide itself and the infected files. In order to do this, it has to reside in memory.
- *Tunneling Virus*: These types of viruses will tunnel under anti-virus softwares and try to escape from the eyes of anti-virus softwares.
- *Virus Droppers*: This type is actually a program that creates virus and affect the computer systems using its virus. It itself is not a virus. It is a creator of virus. Because it is not a virus, it is difficult to detect it through

anti-virus softwares.

- *Cavity Virus*: This virus will actually maintain the size of the infected files not to be identified by the anti-virus softwares.

The better way to avoid viruses is installing anti-virus softwares on all systems. Some new viruses may even try to bypass antivirus softwares; so, it is very important to keep virus-signature-database up to date. In addition to anti-virus software, users should be very careful while downloading files from internet or mails, because that may contain some malicious virus. If the files or mails are not from trusted source, it is better to delete it right away without opening it.

2.3 Trojan Horse

Trojan Horse programs are initially used for system administration purposes. System administrators used these programs to control their work-stations remotely. These programs are having two components; one runs as a server and another one runs as a client. The server part is installed on the work stations and the client is installed on the administrators' machines. Though it has a good purpose, its power can be used for bad purposes too. Hackers can use these programs to get control on their target machines and watch all the activities. This is very dangerous than Virus and DoS for the eCommerce businesses. The threatening issues with Trojan Horses are as follows:

1. It allows for data integrity attack.
2. It allows gaining control over the target machine and to steal private information available on the target system. This way it affects privacy policy.
3. It can store key strokes and make it viewable for hackers. As a result, hackers can easily get the victim's login-ids and passwords. This way, it affects confidentiality.
4. Hackers can see screen shots of targeted machines using Trojan horses. Sometimes, if websites are not secured properly, some third party companies can collect consumer information and pass it to some

other businesses. It is a serious threat to customer privacy.

5. It can be installed very easily on the target machines simply by sending it as an email attachment.

Basically, Trojan Horse programs affect the very basic principles of information security.

2.4 Spoofing

The exact meaning of spoofing is deceiving others. It is actually fooling other computer users to think that the source of their information is coming from a legitimate user. There are several methods of spoofing. Some of them are as follows:

1. IP Spoofing
2. DNS Spoofing
3. ARP(Address Resolution Protocol) Spoofing

2.4.1 IP Spoofing: It changes the source-address of an IP packet to show that it is from a legitimate source, but really it might be coming from a hacker. Thus, the hacker attacks the system and at the same time hides his IP address from the eyes of firewalls. The targeted systems for IP Spoofing are UNIX systems and RPC services. Basically, the services that require IP authentication are the main targets for IP Spoofing. This can be easily found and filtered by modern firewall systems with proper configuration.

2.4.2 DNS Spoofing: This will direct the users to incorrect location. In other words, directing the users to a different website and collecting personal information through web forms illegally. DNS Spoofing is actually very dangerous threat, because DNS is the one that manages domain names and creates equivalent IP addresses. Suppose, if the domain name is www.dell.com <<http://www.dell.com/>> and DNS calculates an IP address that is related to a hacker's site, the users will be directed to the hacker's website. If the hacker maintains his website similar to dell, then the users may think that

the hacker's website is the real dell- website and may provide all bank or credit card information when trying to purchase something. Now, the hacker can get that information easily without any difficulties.

2.4.3 ARP Spoofing: Another name of for ARP Spoofing is ARP Poisoning. ARP is actually maintaining a table of MAC addresses of all computers connected in a network. Any information that comes to ARP is delivered to respective computer based on the mappings available on the ARP's tables. Suppose, if ARP couldn't find MAC address for a message, it broadcasts a message to all systems to get a reply from the exact destination-machine with its MAC address; when it gets the destination-machine's MAC address, it updates it on MAC table. This is the stage where ARP spoofing can happen.

ARP Spoofing actually happens when a hacker (hacker's machine) sends a reply to the ARP's broadcasted message saying that the hacker's machine is the legitimate one. Then, ARP gets hacker's MAC address and add it to its table. As a result, hacker will gain a legitimate connection to the network illegally. Once hacker is connected to the network, he can do all sorts of things.

2.5 Sniffing

It means seeing all packets passed through wires or sometimes through air for wireless networks. Initially, this technique was being used for fixing network problems. Because it can watch network packets, it is now being used by hackers for scanning login_ids and passwords over the wires. TCPDUmp and Snoop are better examples for sniffing tools. The main targeted systems for sniffing attacks are UNIX based systems. The better way to avoid sniffing attack is encryption. If sensitive information is encrypted before sending to wires, hackers can't really understand what it is. They need the key to decrypt the information. This way, the information sent over network could always be safe with encryption.

2.6 Denial of Service (DoS)

This DoS attack is not really used for stealing the information. The main aim of this attack is to bring down the targeted network and make it to deny the service for

legitimate users. In order to do DoS attacks, people do not need to be an expert. They can do this attack with simple ping command. Normally, when experienced hackers attack a site with DoS, they won't do the attack directly from their machine. They will install a small program called zombies on some computers those are in intermediate level in the networks; whenever they want to attack, they will run those programs remotely and will make the intermediate computers to launch the attacks simultaneously.

If the intermediate computers are more than 1000, the targeted servers will definitely go down because of the overload. Finally, the legitimate users may not be able to get proper service from those affected servers. The remedy would be restarting the servers, but by that time, the owner would have lost valuable time, business and money. The examples for DoS tools are FloodNet, TFN2K and Trinoo etc. Better firewall system could trace this and block it right away before it touches the servers.

3.0 SUGGESTIONS TO OVERCOME THESE PROBLEMS

There are no 100% solutions for these security problems and threats, but some of the following suggestions could control these issues to some extent.

1. Increase the awareness of the above issues among all computer users and instruct them with some kinds of do's and don'ts.
2. Use SSL connection for all transactions related to money and private information.
3. Use symmetric key based encryption and decryption for all transactions, because PKI Cryptography may not work for session based transactions.
4. Install Anti-Virus softwares on the systems and keep database of viral signatures up to date. Nowadays, lots of companies are providing Virus scanning and cleaning

softwares for an affordable cost. Some better examples are McAfee, Norton Antivirus and trendmicro etc.

5. Install good firewall system to prevent attacks from DoS and Trojan Horses and be up to date on the latest patches of firewalls.

6. If there is any change in the behavior of the systems, inspect the firewall settings immediately and fix it right away when there is any problem on the settings. McAfee firewall has all these kinds of features.

7. Look for the latest advisories on the new viruses, worms and Trojan horses etc. If there is anything needs to be installed, better do it immediately.

8. Most of the websites are not caring about the customer's privacy. They should follow the directions given by FTC (Federal Trade Commission) and protect customer privacy. If they don't do so, anybody can sue those companies.

9. Look for updates or new patches for the operating systems. Nowadays, Microsoft is providing free update (Service pack-2) on Windows XP that contains virus protection software, firewall and security center. It is better to get that installed on all windows systems.

10. Train system administrators and developers to handle these vulnerabilities properly and it is better to employ a cyber security professional who is an expert in securing systems.

11. Above all, the vendors of operating systems should provide patches for security mechanisms; because, they are the creators of the operating systems; they know their system better than anybody else. It is easy for them to give effective systems to handle the web threats.

4.0 References:

McClure, S., & Shah, Saumil & Shah, Shreeraj (2003). Web Hacking : Attacks and Defense. Boston: Pearson Education, Inc

Jacobs, J., & Clemmer, L., & Dalton, M., & Rogers, R., & Posluns, J (2003). SSCP: Systems Security Certification Practitioner: Rockland: Syngress Publishing, Inc.

Bishop, M., (2003). Computer Security Art and Science: Boston: Pearson Education, Inc

Virus Tutorial. Retrieved on Sep 29, 2004 from <http://www.cknow.com/vtutor/index.htm>

Virus Primer. Retrieved on Sep 29, 2004 from <http://www.trendmicro.com/en/security/general/virus/overview.htm>

Brookins, Nick (2004). Security for all. Retrieved on Sep 29, 2004 from <http://www.computeruser.com/articles/2308,5,88,1,0801,04.html>