COMPUTER SECURITY- A REVIEW

Divya[1], Gaurav Sachdeva[2]

[1] Faculty, Computer science Department, DPMI, New Delhi, India
[2] Faculty, Civil Department, DPMI, New Delhi, India

ABSTRACT

Computers are used widely in companies, organizations and homes etc. we save important and confidential data in it, because of it security of computer is required. Computer security is the protection of computer parts and information from theft and destruction. This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure. We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer. Computer Security is the field which tries to keep computers safe and secure. Computer security is a field of engineering concerned with the development and deployment of measures to ensure the protection of computer systems from hostile acts or influences. Security means allowing things you do want, while stopping things you don't want from happening. There are many computer risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. In this paper introduction of computer security, its theft and protection methods are discussed. It presents some of the material that is the basis of security in computer systems.

Keyword: *Worms, malware, virus, antivirus, types of threats, IDS, firewall.*

1. INTRODUCTION

Now day’s people heavily depended on computers for managing information in systems. . It is used in almost every field such as medical, research, education, communication, media etc. In organizations information system is maintained through computerization and networking. We put confidential and private data in computers. Because of it security of computer is important.

Computer security is major issue these days. Security means preventing your data from malwares or intrusions from being modified or destroyed. Security risk is also an event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. Most people think about computer security in a corporate or business context. Companies often store a lot of very sensitive information electronically, including trade secrets, customer lists and extensive corporate documents, both finished and those in progress. Home computer users, but it is no less essential. As we do online transactions we also need secure medium.

Computer Security is concerned with four main areas:

1. Confidentiality: - Only authorized users can access the data resources and information.
2. Integrity: - Only authorized users should be able to modify the data when needed.
3. Availability: - Data should be available to users when needed.
4. Authentication: - are you really communicating with whom you think you are communicating with

We can classify the security attacks into two types as mentioned below:

Direct: This is any direct attack on your specific systems, whether from outside hackers or from disgruntled insiders.

Indirect: This is a general random attack, most common computer viruses, computer worms or computer Trojan horses.
Computer security involves implementing measures to secure a single computer. When securing a single computer, you are concerned with protecting the resources stored on that computer and protecting that computer from threats. Network security involves protecting all the resources on a network from threats.

2. COMPUTER CRIMES

2.1 Hardware theft-The act of stealing computer equipments or parts. Theft consists of people opening up the systems and taking parts out of them.

2.2 Software theft-

It refers to the unauthorized duplication or use of software. Software theft may be carried out by individuals, groups or, in some cases, organizations who then distribute the unauthorized software copies to users.

The different types of software theft are as follows:
Type 1: This involves the physical stealing of a media that includes the software or the hardware.

Type 2: This takes place when the service of a programmer is unexpectedly terminated by a company. The programs written by company programmers are exclusive to the companies they work for, but a few dishonest programmers deliberately wipe out or disable the programs written by them using the company infrastructure.

Type 3: This happens if the software is compromised by the software vendors. This is the most prevalent type of software theft. It is also referred to as software piracy. It triggers unauthorized replication of copyrighted software.

Type 4: This takes place when users make use of unauthorized activation codes or registration numbers. Many are using key generators (commonly known as keygens) to create and input serial keys at the time of registration. Keygens are sometimes helpful for generating activation codes as well. This helps users install the compromised software without legally acquiring it.

2.3 Unauthorized access:

Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access it is considered unauthorized access. Unauthorized access could also occur if a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access and possibly see an unauthorized access message.

2.4 Malware (virus, worms, Trojan horse):

Malicious software or malware is software designed to damage a system or the data it contains, or to prevent the system from being used in its normal manner. Viruses, Trojan horses, and worms are the main types of malicious software.

2.4.1 VIRUS (Vital Information Resources Under Seize).

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. Virus is a program designed to harm or cause harm on an infected computer. Its spreads through e-mail attachments, portable devices, websites containing malicious scripts and file downloads. A virus program contains instruction to initiate some sort of “event” that affects the infected computer.

Different types of computer viruses and what they do.

- **Macro Viruses:** These viruses infect the files created using some applications or programs that contain macros such as doc, pps, xls and mdb. They automatically infect the files with macros and also templates and documents that are contained in the file.

- **Direct Action Viruses:** These viruses mainly replicate or take action once they are executed. When a certain condition is met, the viruses will act by infecting the files in the directory or the folder specified in the AUTOEXEC.BAT.

- **Web Scripting Virus:** Most web pages include some complex codes in order to create an interactive and interesting content. Such a code is often exploited to cause certain undesirable actions.

- **Multipartite Virus:** These type of viruses spread in many different ways. Their actions vary depending on the OS installed and presence of certain files. They tend to hide in the computer’s memory but do not infect the hard disk

- **Polymorphic Virus:** They encode or encrypt themselves in a different way every time they infect your computer.

How do viruses spread-

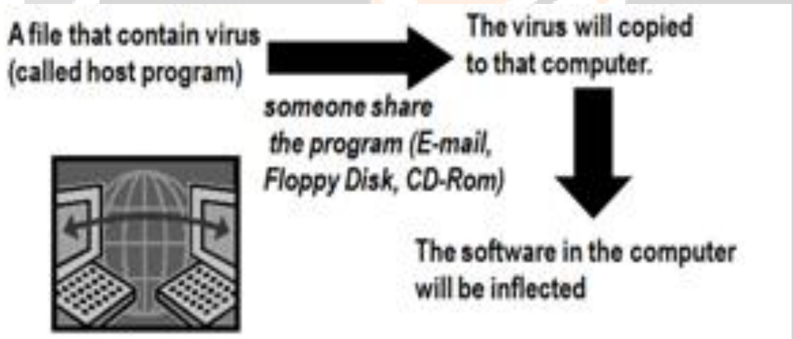

Fig -1: The process of how virus spread

2.4.2 Worm

A worm has similar characteristics of a virus. Worms are also self-replicating, but self-replication of a worm is in a different way. Worms are standalone and when it is infected on a computer, it searches for other computers connected through a local area network (LAN) or Internet connection. When a worm finds another computer, it replicates itself to the new computer and continues to search for other computers on the network to replicate. Due to the nature of replication through the network, a worm normally consumes much system resources including network bandwidth, causing network servers to stop responding.

Different types of Computer Worms are:

• **Email Worms:** Email Worms spread through infected email messages as an attachment or a link of an infected website.
• **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

• **Internet Worms:** Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.
• **IRC Worms:** IRC Worms spread through IRC chat channels, sending infected files or links to infected websites.
• **File-sharing Networks Worms:** File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

2.4.3 Trojan horse

Trojan horse is a program that conceals its purpose — it claims to do one thing but really does another. The term, Trojan horse, is usually used to refer to a non-replicating malicious program which is the main characteristic that distinguishes it from a virus. A Trojan horse program has the appearance of heaving a useful and desired function. While it may advertise its activity after launching, this information is not apparent to the user beforehand. Secretly the program performs other, undesired functions. A Trojan horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. Trojan horse programs are named for the famous wooden horse used by the Greeks to sneak soldiers into the ancient city of Troy.

Types of Trojan horse-

1. The Remote Administration Trojan horse Virus: This type of Trojan horse virus gives hacker behind the malware the possibility to gain control over the infected system. Often the remote administration Trojan horse virus functions without being identified. It can help the hacker to perform different functions including altering the registry, uploading or downloading of files, interrupting different types of communications between the infected computer and other machines.

2. The File Serving Trojan horse Virus: Trojan horse viruses from this category are able to create a file server on the infected machine. Usually this server is configured as an FTP server and with its help the intruder will be able to control network connections, upload and download various files. These Trojan horse viruses are rather small in size, sometimes not more than 10Kb, which makes it difficult to detect them. They are often attached to emails or hidden in other files that users may download from the Internet. Regularly these Trojan viruses spread with the help of funny forwarded messages that a user receives from friends. Trojan horse viruses may also be hidden in small downloadable games.

3. Distributed Denial of Service Attack Trojan horse Virus: A lot of computers can be tricked intro installing the Distributed Denial of Service Trojan so that the hacker can gain control over one, several or all computers through a client that is connected with a master server. Using the primary computer within one huge zombie network of machines, hackers are able to sent attacks at particular targets, including companies and websites. They simply flood the target server with traffic, thus making it impossible for simple users to access certain websites or systems. Often these attacks are used to stop the activity of famous brands that could handle different financial demands.

4. Keylogging Trojan horse Virus: These Trojan horse viruses make use of spyware with the goal of recording every step of user's activity on the computer. They are called keylogging because they transmit to the hacker via email the information about logged and recorded keystrokes. Hackers use this type of malware for their financial benefit (through card fraud or identity theft). Some individuals or companies can offer a great reward for valuable information.

5. The Password Stealing Trojan horse Virus: The name speaks for itself - Trojans from this category are used to steal passwords. The Trojan transmits information about passwords to the hacker through email. Just like keylogging

Trojans, this malware is used mainly for hacker's financial benefit (a lot of people use passwords to access their bank accounts or credit cards).

6. The System Killing Trojan horse Virus: These Trojans are meant to destroy everything in the system starting with drive Z and ending with drive A. One of the recent Trojan horse viruses of this type is called Trojan.Killfiles.904. The reasons for creating such Trojans are unknown but the results could be catastrophic.

Symptoms of a computer affected by virus, worm or Trojan horse-

- Screen displays unusual message or image
- Available memory is less than expected
- Files become corrupted
- Unknown programs or files mysteriously appear
- Music or unusual sound plays randomly
- Existing programs and files disappear
- Programs or files do not work properly
- System properties change

Some famous malwares:

- **1949 – 1966 – Self-Reproducing Automata:** Self-replicating programs were established in 1949, to produce a large number of viruses, John von Neumann, whose known to be the “Father of Cybernetics”, wrote an article on the “Theory of Self-Reproducing Automata” that was published in 1966.
- **1959 – Core Wars:** A computer game was programmed in Bell Laboratory by Victor Vysottsky, H. Douglas McIlroy and Robert P Morris. They named it Core Wars. In this game, infectious programs named organisms competed with the processing time of PC.
- **1971 – The Creeper:** Bob Thomas developed an experimental self-replicating program. It accessed through ARPANET (The Advanced Research Projects Agency Network) and copied to remote host systems with TENEX operating system. A message displayed that “I’m the creeper, catch me if you can!” Another program named Reaper was created to delete the existing harmful program the Creaper.
- **1974 – 1975 – ANIMAL:** John Walker developed a program called ANIMAL for the UNIVAC 1108. This was said to be a non-malicious Trojan that is known to spread through shared tapes.
- **1983 –** This was the year when the term “Virus” was coined by Frederick Cohen for the computer programs that are infectious as it has the tendency to replicate.
- **1986 – Brain:** This is a virus also known as the “Brain boot sector”, that is compatible with IBM PC was programmed and developed by two Pakistani programmers Basit Farooq Alvi, and his brother, Amjad Farooq Alvi.
- **1987- Lehigh:** This virus was programmed to infect command.com files from Yale University.
- ➢ **Cascade:** This virus is a self-encrypted file virus which was the outcome of IBM’s own antivirus product.
- ➢ **Jerusalem Virus:** This type of virus was first detected in the city of Jerusalem. This was developed to destroy all files in infected computers on the thirteenth day that falls on a Friday.
- **1990 –** Symantec launched one of the first antivirus programs called the Norton Antivirus, to fight against the infectious viruses. The first family of polymorphic virus called the Chameleon was developed by Ralf Burger.
- **1995 – Concept:** This virus name Concept was created to spread and attack Microsoft Word documents.
- **1999 – Happy99:** This type of worm was developed to attach itself to emails with a message Happy New Year. Outlook Express and Internet Explorer on Windows 95 and 98 were affected.
- **2000 – ILOVEYOU:** The virus is capable of deleting files in JPEGs, MP2, or MP3 formats.
- **2002 – LFM-926:** This virus was developed to infect Shockware Flash files.
- ➢ **Beast or RAT:** This is backdoor Trojan horse and is capable of infecting all versions of Windows OS.
- **2004 – MyDoom:** This infectious worm also called the Novang. This was developed to share files and permits hackers to access to infected computers. It is known as the fastest mailer worm.
- **2007 – Storm Worm:** This was a fast spreading email spamming threat against Microsoft systems that compromised millions of systems.

- **Zeus:** This is a type of Trojan that infects used capture login credentials from banking web sites and commits financial fraud.
- **2008 – Koobface:** This virus was developed and created to target Facebook and MySpace users.
- **2010 – Kenzero:** This is a virus that spreads online between sites through browsing history.
- **2013 – Cryptolocker:** This is trojan horse encrypts the files infected machine and demands a ransom to unlock the files.
- **2014 – Backoff:** Malware designed to compromise Point-of-Sale (POS) systems to steal credit card data.

2.5 Information theft

Information theft is more serious problem then hardware or software theft. There have been a growing number of cases of information theft over the past few years. While more and more electronic security measures have been going up to protect people's possessions and information, these new technologies have bugs and design flaws that are opening up whole new worlds for the technologically advanced criminal. Information theft occurs when someone steals personal or confidential information some criminals use the Internet or other computer networks to break into a particular computer system in order to access forbidden information. Eg. Password capturing, ATM spoofing, credit card number theft etc. Hackers are threat to sensitive corporate and government data because they pride themselves on getting around security measures.

3. PREVENTION

1. Encryption is one way to protect sensitive data. Sender will convert data to codes which are unreadable and the receiver must get the password and key in order to convert the codes back to meaningful data.
2. Turn on firewall. A firewall is a system designed to prevent unauthorized access to or from a private network.
3. Run up to date security software.
4. Block spyware attacks.
5. Backups are the way of securing data.
6. Installing IDS. Intrusion detection system is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways.

4. CONCLUSIONS

Computer is used in almost every field now days. Risks of computer security are also high as we save confidential information in it. Internet activity is the primary highway for these transactions. Many computer users do not realize that simply accessing the web could be making their computers more vulnerable. Data present in a computer can also be misused by unauthorized intrusions. An intruder can modify and change the program source codes and can also use your pictures or email accounts to create derogatory content such as pornographic images, fake misleading and offensive social accounts.

5. REFERENCES

[1] Robert Bakker, Edwin Keijsers, and Hans van der Beak “Alternative Concepts and Technologies for Beneficial Utilization of Rice Straw” Wageningen UR Food & Biobased Research ,Number Food & Biobased Research number 1176 ,ISBN-number 978-90-8585-755-6,December 31st, 2009

[2] Kkhkj Dittrich, D., Bailey, M., Dietrich, “Towards community standards for ethical behavior in computer security research. Tech.” Rep. 2009-1, Stevens Institute of Technology (April 2009)

[3]. Goodrich and Tamassia, Introduction to Computer Security (2010, Addison-Wesley)

[4]. www.wisegeek.com

[5] www.armor2net.com

[6] www.google.com