

Securing Home Computers from Hijacking: Security, Threats and Preventions

Ms. Rekha Goyal, Ms. Poonam Sharma,
Lecturer Dept of Computer Science
M.M.Modi College, Patiala.

Abstract--Security in today's world is playing a major role in every field. If the user of computer system is not aware about the threats involved that can hamper it's working, then the knowledge of the user is considered to be incomplete. In this paper the first part is discussing the general security issues and the threats and the second part is specifying the ways in which user should tackle these threats and thus maintain the security of the systems. We can secure our systems by using different network techniques e.g. updated operating, encryption & decryption and firewall. In this we are discussing about defense approach model to provide security from the intruders and unauthorized person who can do harm to our computer a well information. This model has four-layer approach: Network Access, Operating System, User Application and Data.

I.SECURITY

In today's world, security is the biggest challenge faced by all organizations. The changing security threats from both inside and outside the computer network world is creating havoc on PC operations, and is also affecting profitability and user satisfaction. So all organizations must also comply with new regulations and laws created to protect consumer privacy and secure electronic information.

Forms of Security threats

WORMS AND VIRUSES

The most common security threat to computers is through worms and viruses, as they can have a devastating effect any PC through out the world. Destructive strains spread much faster and, infect an entire connection of PC's in seconds. Cleaning the infected computers takes much longer. The results of these attacks are lost orders, corrupted databases, and angry and frustrated users. As the updating is made for the latest operating system and antivirus software, new viruses can penetrate and thus break the defenses of the computer system. At the same time, users add on to it by unwittingly accessing malicious Websites, downloading untrustworthy material, or opening malicious e-mail

attachments. Although these attacks are unintentional, they too cause significant financial losses. Security systems must detect and repel worms, viruses, and spy ware at all points in the network.

II.INFORMATION THEFT

All organizations deals with information so information theft has become a big business today. The hackers break into business networks and thus steal credit cards or social security numbers for profit.

Hackers: "How they do it?"

Hacking attacks progress in a series of stages, using various tools and techniques. A hacking attack consists of the following stages:

- a. *Target Selection:* In the target selection a hacker identifies a specific computer to attack.
- b. *Target Identification:* Under this the hacker determines the characteristics of the target before actually using it.
- c. *Attack Method Selection:* In this stage the hacker selects one or more specific attack methods to use against the target.
- d. *Attack Progression:* The hacker proceeds with the actual attack or series of attacks.

The major techniques used to accomplish the phases of hacking include:

- a. Eaves dropping and snooping
- b. Denial-of-service
- c. Protocol exploitation
- d. Impersonation
- e. Man-in-the-middle
- f. Hijacking

III.EAVESDROPPING AND SNOOPING

The first and easiest thing a hacker can do to gain information about a network is simply to listen, and then ask the network computers information about themselves. In this method the hacker may not even contact the computers directly but instead communicate with other computers that provide services to that computer (DNS computers). Common hacking practices include the following activities:

- a. Password capture
- b. Traffic analysis
- c. Network address scanning
- d. Port scanning
- e. Finger, Whois, NSLookup, and DNS range grabbing
- f. SNMP data gathering

Example: Password Capture

Most of the networking protocols are too weak to encrypt passwords, thus allowing any computer on the path between the client and the server to "overhear" the username and password. An eavesdropping hacker must also have access to a computer that is situated on a network link with network traffic flowing over it. The more data that flows over the link, the more likely the hacker will capture passwords sent in the clear, i.e. in unencrypted form. The hackers can install software on those computers that will allow them to snoop as well. The hacker may be typing at a computer in New York while a compromised computer in San Francisco records everything that goes over that remote network for the hacker's later perusal. Snooping Windows passwords over the Internet is surprisingly easy. Microsoft has built in a password Challenge/Response authentication mechanism into Internet Explorer.

IV.DENIAL OF SERVICE

The next easiest attack on the network is to disable some aspect of it or even bring the entire network down. There are a number of methods a hacker can use to disable a computer or a service provided by a computer. Most of these methods affect computers using TCP/IP, because TCP/IP is the most widely used inter network protocol and because the most pressing hacker threat is from the Internet. Methods hackers can use to disable computers or computer services include these:

- a. Ping of Death (malformed ICMP packets)
- b. SYN (Synchronize Connection Establishments) Attacks and ICMP (Internet Control Message Protocol) flooding.

Ping of Death

A specially constructed ICMP packet that violates the construction rules can cause the recipient computer to crash if that computer's networking software does not check for invalid ICMP packets.

SYN Attacks and ICMP Flooding

Hackers disable the networking capability of computers is by overloading the network protocol software of the target computer with connection attempts or information requests. Attacker can send one SYN packet after another to a target computer, and that target computer will then be unable to process other connection attempts from legitimate users because all of its available time and memory will be spent processing SYN requests. A similar network protocol attack is ICMP flooding, in which the hacker sends a constant stream of ICMP echo requests to the target computer. The target computer then spends most of its time responding to the echo requests instead of processing legitimate network traffic. Firewall and operating system software can be used to update to prevent these attacks.

V.PROTOCOL EXPLOITATION

Protocol Exploitation is currently the most popular form of hacking on the Internet. Protocol exploitation is an attack based on exploiting a bug in a public service in order to gain more access than would normally be allowed. One way to do so is by means of Buffer overruns method, which is an artifact of the way the modern compilers of certain programming languages create programs

VI. IMPERSONATION

- . The goal of a hacker is to penetrate your network security and get the information or resources on the computers in your network. These attacks are used when a specific target is the goal.

VII.MAN-IN-THE-MIDDLE

A special case of the impersonation attack is the man-in-the-middle attack, where the hacker operates between two computers on your network, or between a client computer on the Internet or other WAN network and your server computer in your secure LAN. When the client computer opens a connection to the server computer, the hacker's computer intercepts it. The hacker computer opens a connection on behalf of the client computer to the server computer. Ideally, the client will think he is communicating with the server, the server will think it is communicating with the client, and the hacker computer in the middle will be able to observe and alter all of the communications between them.

IX.HIJACKING

One last hacker trick is the hijacking of an already established and authenticated networking connection. This can occur at two layers of the networking protocol at the TCP connection layer and at the SMB or NFS Session layer.

Home computers are not very secure and are easy to break-in. Intruders attack home computers through high-speed Internet connections, dial-in connections.

How attackers do it?

- a. Through E-Mail
- b. Through Un-trusted Websites
- c. Through Internet Shares

Attackers send mail with a virus. Virus activates when we read that email, creating an opening that intruders use to enter or access the computer. When they are on the computers, they install new programs that let them continue to use the computer. These are known as “backdoors”. They steal the information saved by the user on his computer. Intruders want the information stored by the users, which is personal such as credit card numbers, PINs, Passwords etc. The intruders also use the resources of the systems for their own purpose.

Vulnerabilities in Home Computers

There are following types by which the Security of Home Computers can be breached:

- a. *Intrusion*
- b. The intruders always look for way to break into computers connected to internet. They try to breach the computer security defense.

a. *Malicious Code*

- c. Malicious code is unwanted and destructive software such as Viruses, Worms and Trojans.
- d. *Virus*: A virus is malicious code that infects itself to other objects or program.
- e. *Worm*: A worm is malicious code that replicates by making copies of itself on the same computer. Worms don't infect other program files on a computer.
- f. *Trojan*: A Trojan horse is a program that perform malicious action when activated such
- g. as destroying files.

A. *Key Loggers*

- h. Key loggers are software applications that capture the key logging events and can mail to remote intruder via email. These are invisible and undetectable to users.

B. *Bots*

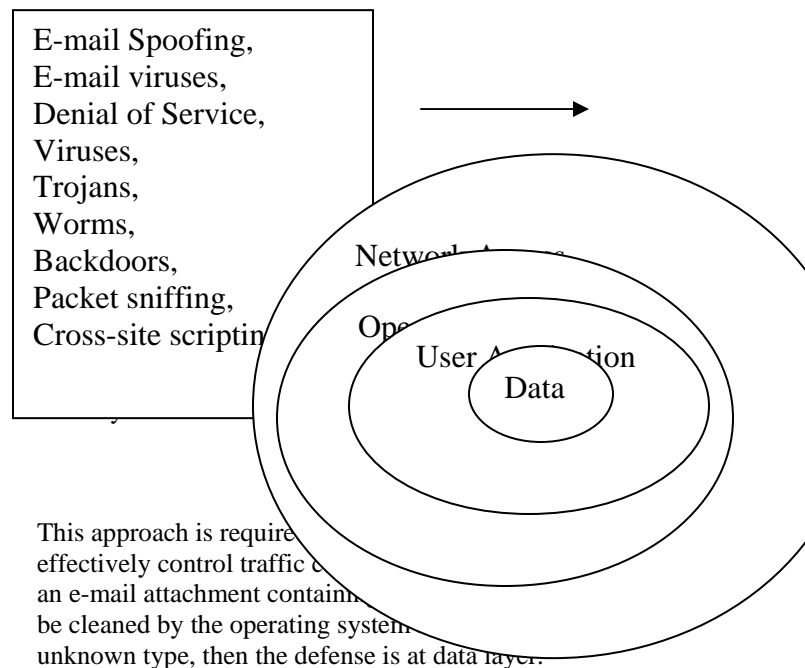
- i. Bot is derived from the word “Robot”, which means “worker”. Bots are used on the internet. Google bot is search bot that visits through the web pages on the net to collect information.

Indication of Infection

- a. Poor system performance
- b. Abnormal system behavior e.g. system restarts or hangs frequently
- c. Unknown services are running
- d. Crashing of applications
- e. Change in file extensions or contents
- f. Hard Disk is busy

The Defense Approach for the Home Computers

The defended area is the user's data in the Home Computer security. In Home Computer security the defense in depth has four layers: Network Access, Operating System, User Application and Data.



This approach is required to effectively control traffic and an e-mail attachment containing a virus can be cleaned by the operating system. If an unknown type, then the defense is at data layer.

Defensive Measures at various layers:

Network Access Layer

The defensive measures that are taken are:

- a. Use a Firewall
- b. Disconnect from the Internet when not using it

Use of Firewall

A firewall places a barrier between the computer and hackers. The firewall provides security against a variety of computer worms that are transmitted over the network. Firewall takes one of two forms:

- a. Personal Firewall- Specialized software on the individual computer e.g. ZoneAlarm, Windows Internet Connection Firewall (ICE) etc.
- b. Hardware Firewall- A separate device e.g. Linksys EtherFast Cable/DSL Router

Personal Firewall

A personal Firewall is software that provides defense mechanism for the computer. The firewall acts as a guard for the connected computer that checks everybody entering or going out of the home. Microsoft Corporation provides Internet Connection Firewall for Windows XP SP2 users only.

Configuring Internet Connection Firewall

Windows XP with SP2 includes a built-in firewall. By default it is disabled, To enable this do the following steps:

- a. Go to Start menu\Control Panel\Network and Internet Connections\Network Connections\Under Dial-Up or LAN, click the icon to select the connection that user wants to help protect.
- b. In the task Pane on the left, under Network Tasks, click the Change Settings of this Connection.
- c. On the Advanced tab, under Internet Connection Firewall, check the box next to this computer from the Internet.

Disconnect from the Internet when not using it

The users who are using dial-up access to the internet disconnect when they are not using the connection. Home users with “Always On” broadband access services such as cable modems leave their computer permanently connected to the internet. A permanent connection allows them to access their files over the internet

Defensive Measures at Operating System layer

The defensive measures at this layer are:

- a. Keep up-to-date security patches and update release for Operating System
- b. Make a boot/ERD disk and keep it current
- c. Install and keep updated Antivirus software
- d. Install and keep updated Antispyware software

Keep up-to-date security patches and update releases for Operating System

Operating System performs basic tasks such as recognizing input from the keyboard, sending output to the monitor, keeping track of files and folders on the disk and controlling peripheral devices. Various Operating Systems such as Windows (9x, NT Workstation, 2000 Professional, XP Home Edition & Professional Edition) and Linux etc. used. Every application has the feature to update automatically through Internet.

Using “Window Update”

Microsoft Web site provides updates for windows operating system software and hardware. Updates address protect against security threats. The patches, hot fixes and services packs are free of cost

Automatic Updates

Windows automatically updates user’s computer. Windows recognizes when the user is online and uses the Internet connection to search for downloads from the Windows Update Web site.

Using MBSA

MBSA is Microsoft Baseline Security Analyzer version 2.0 gives the ability to assess the administrative vulnerabilities. MBSA scans the computer and generates the report about the security checks.

✓ *Make a Boot/ERD disk and keep it current*

A boot disk allows the user to boot from a diskette instead of hard drive. Windows use the emergency repair procedure to fix problems. The backup utility in windows is used to create an ERD.

✓ *Install and Keep up-to-date Antivirus Software*

Anti Virus software searches for specific patterns that matches a signature. Anti-virus program protect the files automatically. Anti-virus provides regular update for these virus signatures. The anti-virus software includes automatic updating of virus definition files, scanning and cleaning of email messages, script blocking and real time anti-virus protection.

✓ *Install and Keep up-to-date AntiSpyware Software (Microsoft AntiSpyware) Beta: AntiSpyware software helps to protect users from spyware and other unwanted software*

Defensive Measures at User Application Layer

The defensive measures at this layer are:

- ✓ Don’t install programs from unknown origin
- ✓ Precautions with E-mail
- ✓ Chat clients
- ✓ Securing Web browser

✓ *Don’t install programs from unknown origin*

Installing programs from unknown origin can give chances of malicious code. Programs to be installed should have authorized by the company. User should not use Pirated software, because pirate software can install backdoors.

✓ *Precautions with Email*

Most of e-mails are unsolicited and unfamiliar address. E-mail “spoofing” is when an email message appears to have originated from one source when it was sent from another

source. Email spoofing is an attempt to trick the user into making a damaging statement. Spam is flooding the Internet with many copies of the same message. Most spam is commercial advertising. If user responds they sell their address to every other spammer. When user receives an e-mail asking him to visit his bank's web site, it signifies the beginning of a phishing fraud. It would ask him to provide confidential banking information.

✓ *Chat Clients*

Internet chat applications such as instant messaging applications and Internet Relay Chat (IRC) networks provide a way for bi-directional transmission between computers. Many chat clients allow for the exchange of executable code that presents risks to email clients.

✓ *Securing Web Browser*

Web browsers are capable of parsing active code in many forms, including Java Script, ActiveX and Java code. These are automatically downloaded and executed by the web browser. Malicious individuals take advantage of this. IE uses a Zone Security model that permitted to perform certain actions.

Defensive Measures at Data Layer

The defensive measures that are taken at this layer are:

- ✓ User must backup his important files
- ✓ Use Encryption to ensure confidentiality of sensitive data
- ✓ File Checksum
- ✓ Password Policy
- ✓ Login Settings
- ✓ Audit Policy Settings
- ✓ Event Viewer

✓ *User must backup his important files*

Backing up data is a task user should perform regardless of whether his system is secured or not. User can backup data to an external hard drive, a personal tape drive, Zip or CD-burner. "Backup" is an in-built program that comes with windows operating system. It is located at start>programs>Accessories>system tools.

✓ *User Encryption to ensure confidentiality of sensitive data*

User can use the encrypting file system to encrypt important data files. Whenever an intruder tries to access encrypted files then with the help this system this person is prevented from doing this so. This is done by giving and access denied message. If due to some of reasons the files encryption certificate an associated private key is lost, then the data recovery can be done with the help of person known as recovery agent.

✓ *File Checksum*

File Checksum is a utility that computers MD5 or SHA1 cryptographic hash for files. It can compare hash values to make sure that the files have not been changed.

✓ *Password Policy*

Password should be complex and change regularly. Password Policy setting controls the complexity of the password.

✓ *Login Settings*

Windows NT, 2000 and XP come with many users and groups that include Administrator, Backup Operator, Guest, Power User and many more. The purpose of these groups is to enhance the abilities of a user. All unnecessary users must be disabled.

✓ *Audit Policy Settings*

User can set the Audit Policy setting to determine the security events to report the user. The user can choose to monitor changes to use of a sensitive file, user accounts and passwords, changes to security policies and use of privileges.

✓ *Event Viewer*

A component a user can use to view and manage event logs, gather information about hardware and software problems and monitor security events. It maintains logs of three kinds: application, system and security.

