Dr. MAHALINGAM COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds Estd. 1998
An Autonomous Institution (Since 2011)
Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY
Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade 'A++'
Accredited by NBA - Tier1 (Mech, Auto, Civil, EEE, ECE, E&I and CSE)
Udumalai Road, Pollachi - 642 003 Tel: 04259-236030/40/50 Fax: 04259-236070 www.mcet.in

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO1: Explain about Proxy servers and anonymizes

SO1:Discuss about Proxy servers and anonymizes, Phishing and Password cracking

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Proxy Server

- Proxy server is a computer on a network which act as an intermediary for connections with other computers on that network.
- It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
- Proxies were invented to add structure and encapsulation to distributed systems.
- Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.

Proxy server has the following purposes:

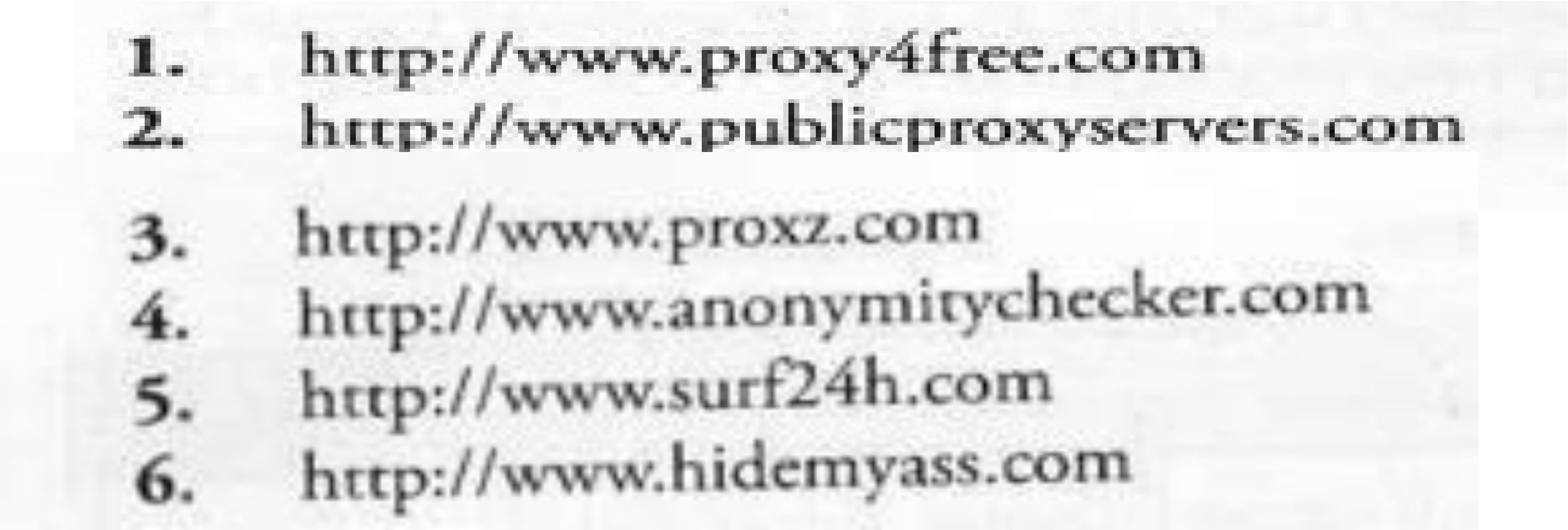
1. Keep the systems behind the curtain
2. Speed up access to access to a resources. It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.

A proxy server may reside on the user’s local computer, or at various points between the user’s computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
- A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching**.**

Advantages of Proxy server

- Cache memory can serve all users.
- If one or more websites are requested frequently, may be by different users , it is likely to be in the proxy's cache memory, which will improve user response time.
- There are special servers available known as cache servers.
- Listed below few websites where free proxy servers were found:



1. http://www.proxy4free.com
2. http://www.publicproxyservers.com
3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.com
6. http://www.hidemyass.com

Anonymizer

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user’s behalf, protecting personal information by hiding the client computer’s identifying information.

Main reasons for using anonymizers

There are many reasons for using anonymizers.

- Anonymizers help minimize risk.
- They can be used to prevent identity theft, or to protect search histories from public disclosure.
- Some countries apply heavy censorship on the internet. Anonymizers can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself.
- Furthermore, as information itself about Anonymizer websites are banned in these countries, users are wary that they may be falling into a government-set trap.
- Anonymizers are also used by people who wish to receive objective information with the growing target marketing on the internet and targeted information.

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.

It accesses the Internet on the user’s behalf, protecting personal information by hiding the client computer’s identifying information

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO1: Explain about Proxy servers and anonymizes

SO1:Discuss about Proxy servers and anonymizes, Phishing and Password cracking

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Phishers frequently use emotions like fear, curiosity, urgency, and greed to force recipients to open attachments or click on links.
- Phishing attacks are designed to appear to come from legitimate (legal) companies and individuals.

How phishing works?

Phishing works in the following ways:

1. Planning

- Criminals, usually called as phishers, decide the target and determine how to get E-mail address of that target or customers of that business.
- Phishers often use mass mailing and address collection techniques as spammers.

2. Setup

- Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target.
- Most often this involves E-Mail addresses and a webpage.

3. Attack

This is the step people are most familiar with the phisher sends a phony message that appears to be from a reputable source.

4. Collection

Phishers record the information of victims entering into webpages or pop-up windows.

5. Identify theft and fraud

Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Password Cracking

- Password cracking is a process of recovering passwords from data that have been stored by a computer system.
- Usually, an attacker follows a common approach - repeatedly making guesses for the password.
- The purpose of password cracking is as follows:
  - ➢ To recover a forgotten password.
  - ➢ As a preventive measure by system administrators to check for easily crackable passwords.
  - ➢ To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following seeps:

- Find a valid user account such as an Administrator or Guest
- create a list of possible passwords;
- rank the passwords from high to low probability
- key-in each password
- try again until a successful password is found.

Example

Password may be Name, date of birth, vehicle number, etc.

Password cracking Attacks

Password cracking attacks can be classified under three categories as follows:

- Online attacks
- offline attacks
- non-electronic attacks

Online Attacks

- An attacker can create a script file that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- 'The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."
- It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.
- When a victim client connects co the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server .
- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites char would like co gain the access to banking websites.

Offline Attacks

- Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.
- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media

Weak Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes.

Passwords that can be easily guessed by acquaintances of the netizens (such as dace of birth, pet's name and spouses' name) are considered to be very weak.

Here are some of the examples of "weak passwords":

- User name
- aaaa-repeated letter
- Pet name
- 1234
- Date of birth, etc

Strong password

- A strong password is long enough, random or otherwise difficult to guess - producible only by the user who chooses it.
- The length of time deemed to be too long will vary ,with the attacker and the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker.
- A student's password might nor be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it.
- Here are some examples of strong passwords:
  - Convert_£100 co Euros!: Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
  - 382465304H: it is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.
  - 4pRte!ai@3: It is not a dictionary word: however it has cases of alpha along with numeric and punctuation characters.

Random Password

- Random Password are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.
- The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack.
- the users are required to choose new passwords regularly, usually after 30 or 45 days.
- The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (10s) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.

5. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.

6. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.

7. Successful logons should display the date and time of the last logon and logoff

8. Logon IDs and passwords should be suspended after a specified period of non-use.

9. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session for the failed user.

Netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.

6. Passwords of personal E-Mail accounts (Yahoo/Hocmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public lnternet facilities such as cybercafes/hotels/libraries.

7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber attacks.

8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks

9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks

10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO1: Explain about Proxy servers and anonymizes

SO2: Explain about Key loggers and spywares

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Key loggers

- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims IT savvy behavior.
- It can be classified as

1. Software keylogger and
2. Hardware keylogger.

Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.

Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.

Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily.

A keylogger usually consists of two files that get installed in the same direccory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes

Hardware Keyloggers

- To install these keyloggers, physical access to the computer system is required.
- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PlNs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence

Antikeylogger

- Antikeylogger is a tool that can detect the keyloggcr installed on the computer system and also can remove the tool.
- Advantages of using antikeylogger are as follows:
  1. Firewalls cannot detect the installations of keyloggers on the systems; hence, anrikeyloggers can detect installations of keylogger.
  2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
  3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
  4. It prevents ID theft
  5. It secures E-Mail and instant messaging/chatting.

Spywares

- Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.
- The presence of Spyware is typically hidden from the user, it is secretly installed on the user's personal computer.
- Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.
- It is clearly understood from the term Spyware that it secretly monitors the user.
- The features and functions of such Spywarcs are beyond simple monitoring.
- Spywarc programs collect personal information about the victim, such as the lnternet surfing habits/patterns and websites visited.

Spywares

- The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system.
- Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the lnternet speed connection with Internet Service Provider (ISP).
- To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares are available in the market.
- lnstallation of anti-spyware software has become a common element nowadays from computer security practices perspective.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO1: Explain about Proxy servers and anonymizes

SO3:Describe about virus and worms.

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Virus

- Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer.
- Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern.
- Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random.

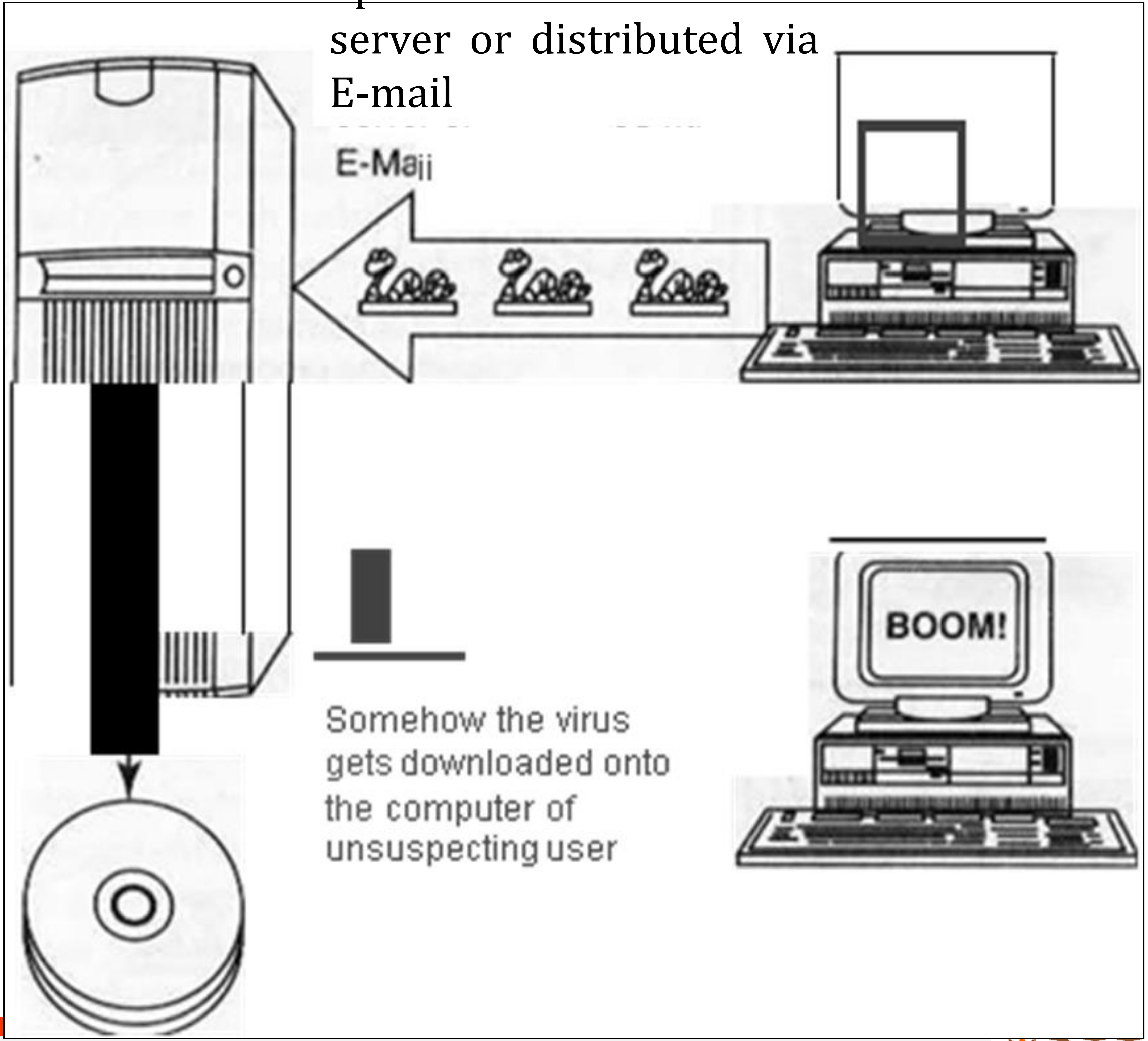
Virus

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus.
2. delete files inside the system into which viruses enter
3. scramble data on a hard disk
4. cause erratic screen behavior
5. halt the system (PC)
6. just replicate themselves to propagate further harm.

Virus spreads through the Internet.

Viruses are intentionally uploaded to an Internet server or distributed via E-mail



Somehow the virus gets downloaded onto the computer of unsuspecting user

The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus

Virus

- Computer virus has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another {in some form of executable code) when its host is taken to the target computer.
- For instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives.
- Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.

Types of Viruses

1. Boot sector viruses: It infects the storage media on which OS is stored (e.g., floppy disk and hard drives) and which is used to start the computer system.

- The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors.
- The first sector is called the BOOT and it carries the master boot record (MBR). MBR's function is to read and load OS, that is, it enables computer system to start through OS.
- Hence, if a virus attacks an MBR or infects the boot record of a disk, such floppy disk infects victim's hard drive when he/she reboots the system while the infected disk is in the drive.
- Once the victim's hard drive is infected all the floppy diskettes that are being used in the system will be infected. Boot sector viruses often spread to other systems when shared infected disks and pirated sofrware(s) are used.

Types of Virus

2. Program viruses:

- These viruses become active when the program file is executed.
- Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.

3. Maltipartite viruses:

- It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
- When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.

Types of Virus(contd)

4. Stealth viruses:

- It camouflages and/or masks itself and so detecting this type of virus is very difficult.
- It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system.
- It alters its file size and conceals itself in the computer memory to remain in the system undetected.
- The first computer virus, named as Brain, was a stealth virus. A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.

Types of Virus(contd)

5. Polymorphic viruses:

- It acts like a "chameleon" that changes its virus signature every time it spreads through the system. Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
- Polymorphic generators are the routines that can be linked with the existing viruses. These generators are not viruses but the purpose of these generators is to hide actual viruses under the cloak of polymorphism.
- The first all-purpose polymorphic generator was the mutation engine (MrE) published in 1991.
- Other known polymorphic generators are Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'n'Roses Polymorphic Engine (GPE) and Dark Slayer Confusion Engine (DSCE).

Types of Virus(contd)

6. Macroviruses: Many applicacions, such as Microsoft Word and Microsoft Excel, support MACROs. These macros are programmed as a macro embedded in a document.

- Once a macrovirus gets onto a victim's computer then every document he/she produces will become infected.
- This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.

7. Active X and Java Control: All the web browsers have settings about Active X and Java Controls.

Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work - such as enabling or disabling pop-ups, downloading files and sound, which invites the threats for die computer system being targeted by unwanted software(s) floating in cyberspace.

worms

- A computer worm is a self-replicating malwarc computer program.
- It uses a computer network to send copies of itself to other nodes (computers to the network) and it may do so without any user intervention.
- This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program.
- Worms almost always cause at lease some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Worms(contd)

Almost every day new viruses/worms are created and they become new created to netizens.

1. A virus attacks specific file types (or files).

2. A virus manipulates a program to execute tasks unintentionally.

3. An infected program produces more viruses.

4. An infected program may run without error for a long time.

5. Viruses can modify themselves and may possibly escape detection this way.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO1: Explain about Proxy servers and anonymizes

SO4:To learn about Trojan Horses and Backdoors.

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Trojan Horses

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.
- For example, ruining the file allocation table on the hard disk. A Trojan Horse may get widely redistributed as part of a computer virus.
- Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet.

Trojan Horses(contd)

- It is also possible to inadvertently transfer malware through a USB Rash drive or other portable media.
- It is possible that one could be forced to reformat USB Rash drive or other portable device to eliminate infection and avoid transferring it to other machines.
- Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
- Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

- Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false website's, display porno site , play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

Backdoor

- A backdoor is means access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves as part of an exploit.
- In some cases a worm is designed to take advantage of a backdoor created by an earlier attack.

Backdoor(contd)

- A backdoor works in background and hides from the user. It is very similar to a virus and therefore, is quite difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system.
- Most backdoors are autonomic malicious programs that must be somehow installed to a computer.
- Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host.
- Programmers sometimes backdoors in their software for diagnostics and troubleshooting purposes.
- Attackers often discover these undocumented features and use them to intrude into the system.

Functions of Backdoors

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands, change any system settings alter the windows registry, run, control and terminate applications, install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and attacks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined ITP server or transfers it through a background Internet connection to a remote host.

Functions of Backdoors

6. It infects files, corrupts installed applications and damages the entire system.

7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.

8. It installs hidden TTP server that can be used by malicious persons for various illegal purposes.

9. It degrades internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.

10. It provides no uninstall feature and hides processes, files and other objects to complicate its removal as much as possible.

Examples of backdoor

Back Orifice: It enables a user to control a computer running the Microsoft Windows OS from a remote location.

Bifrost: It can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.

SAP backdoors: Backdoors can present into SAP User Master that supports an authentication mechanism when a user connects to access SAP and ASAP Program Modules which support SAP Business Objects.

Onapsis Bizploit: It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploration phases of specialized ERP penetration tests.

How to Protect from Trojan Horses and Backdoors

Stay away from suspect websites/weblfoks: Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things.

Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats.

Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO2:Summarize about Attacks

SO1: Describe about steganography.

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

Steganography

- Steganography is a Greek word that means sheltered writing.'' lt is a method that attempts to hide the existence of a message or communication.
- The word "steganography" comes from the two Greek words: steganos meaning "covered'' and graphein meaning “to write" that means "concealed writing.
- This idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes.
- The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messenger's head and then tattooing a secret message on it, letting his hair grow back and then shaving it again after he arrived at the receiving party to reveal the message.

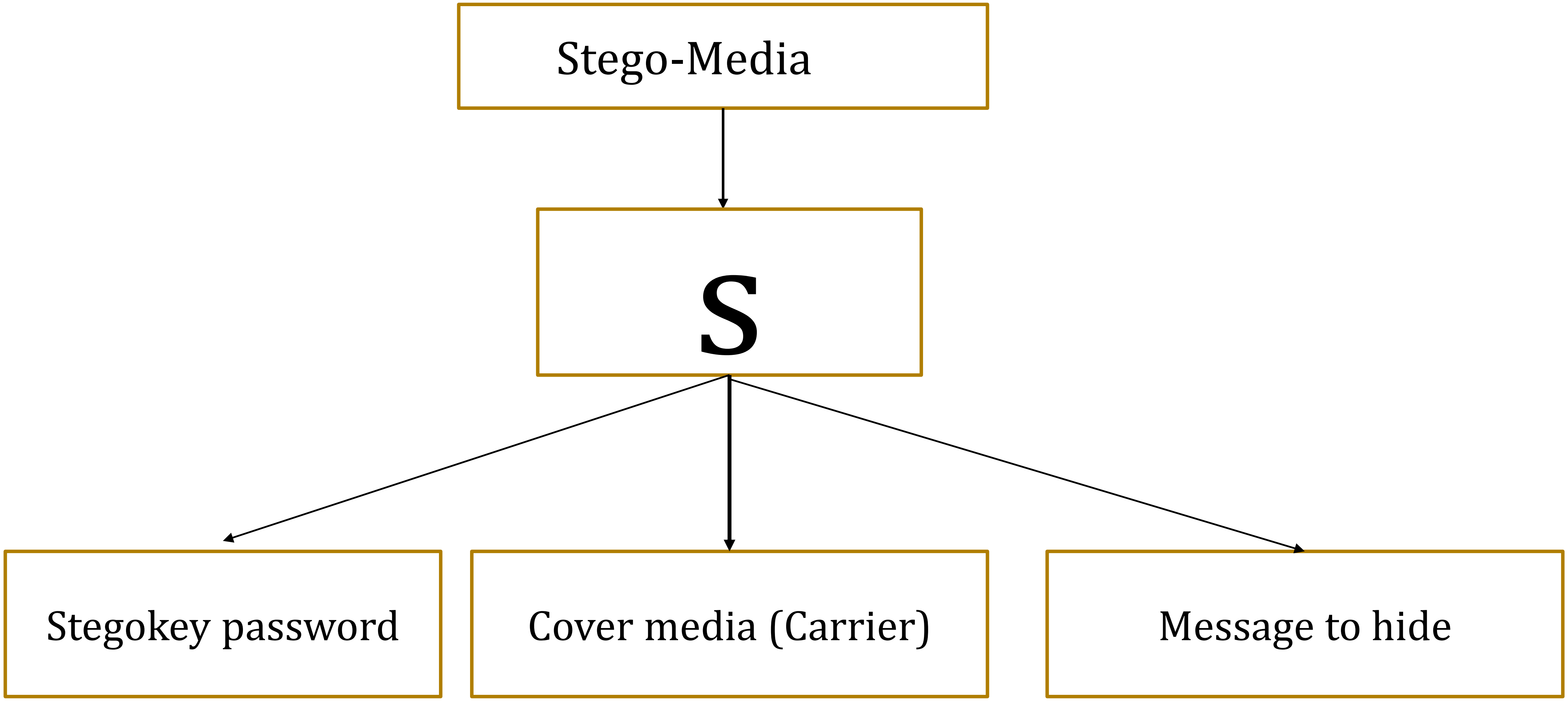
Steganography

- steganography, the art and science of hiding information so that it does not even appear to exist.
- The different names for steganography are data hiding, information hiding and digital watermarking.
- For example, in a digit.al image the least significant bit of each word can be used to comprise a message without causing any significant change in the image.
- Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data. Digital watermarking is the process of possibly irreversibly embedding information into a digital signal.
- The signal may be audio, pictures or video. If the signal is copied then the information is also carried in the copy.

Steganography(contd)

- The term "cover" or "cover mediun" is used to describe the original, innocent message, data, audio, still, video and so on. It is the medium that hides the secret message.
- It must have parts that can be altered or used without damaging or noticeably changing the cover media.
- If the cover media are digital, these alterable parts are called "redundant bits”.
- These bits or a subset can be replaced with the message that is intended to be hidden.
- steganography in digital media is very similar to "digital water marking.“
- In other words, when steganography is used to place a hidden "trademark" in images, music and software. The result is a technique referred to as "watermarking" .

How steganography works.



Stego-Media

S

Stegokey password

Cover media (Carrier)

Message to hide

Cover medium + Embedded message + Stegokey = Stego-medium

Steganalysis

- Steganalysis *is* the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them and if possible recover it.
- Automated tools are used to detect such steganographed data/information hidden in the image and audio and video files

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO2:Summarize about Attacks

SO2:Explain about DoS/DDoS attacks.

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

DoS and DDoS attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., informarion systems) unavailable to its intended users.

DoS Attacks

- In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- Although the means to carry our, motives for and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely.
- The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers

The United States Computer Emergency Response Team defines symptoms of DoS attack to include:

1. Unusually slow network performance (opening files or accessing websites)

2. unavailability of a particular website

3. inability to access any website

4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

A DoS artack may do the following:

- Flood a network with traffic, thereby preventing legitimate network traffic.
- Disrupt connections between two systems, thereby preventing access to a service.
- Prevent a particular individual from accessing a service.
- Disrupt service to a specific system or person.

Classification of DoS Attacks

1. Bandwidth attacks

Loading any website takes certain time. Loading means complete webpage appearing on the screen and system is awaiting user's input. This "loading" consumes some amount of memory.

Every site is given with a particular amount of bandwidth for its hosting, for example, 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site.

The attacker does the same - he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth. Thus, the site becomes out of service.

Classification of DoS Attacks

2. Logic attacks: These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.

3. Protocol attacks: Protocols are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.

Types or Levels of DoS Attacks

1. Flood attack:

- This is the earliest form of DoS attack and is also known as ping flood.
- It is based on an attacker simply sending the victim overwhelming number of ping packers, usually by using the "ping" command, which result into more traffic than the victim can handle.
- This requires the attacker to have a faster network connection than the victim.
- It is very simple to launch, but to prevent it completely is the most difficult.

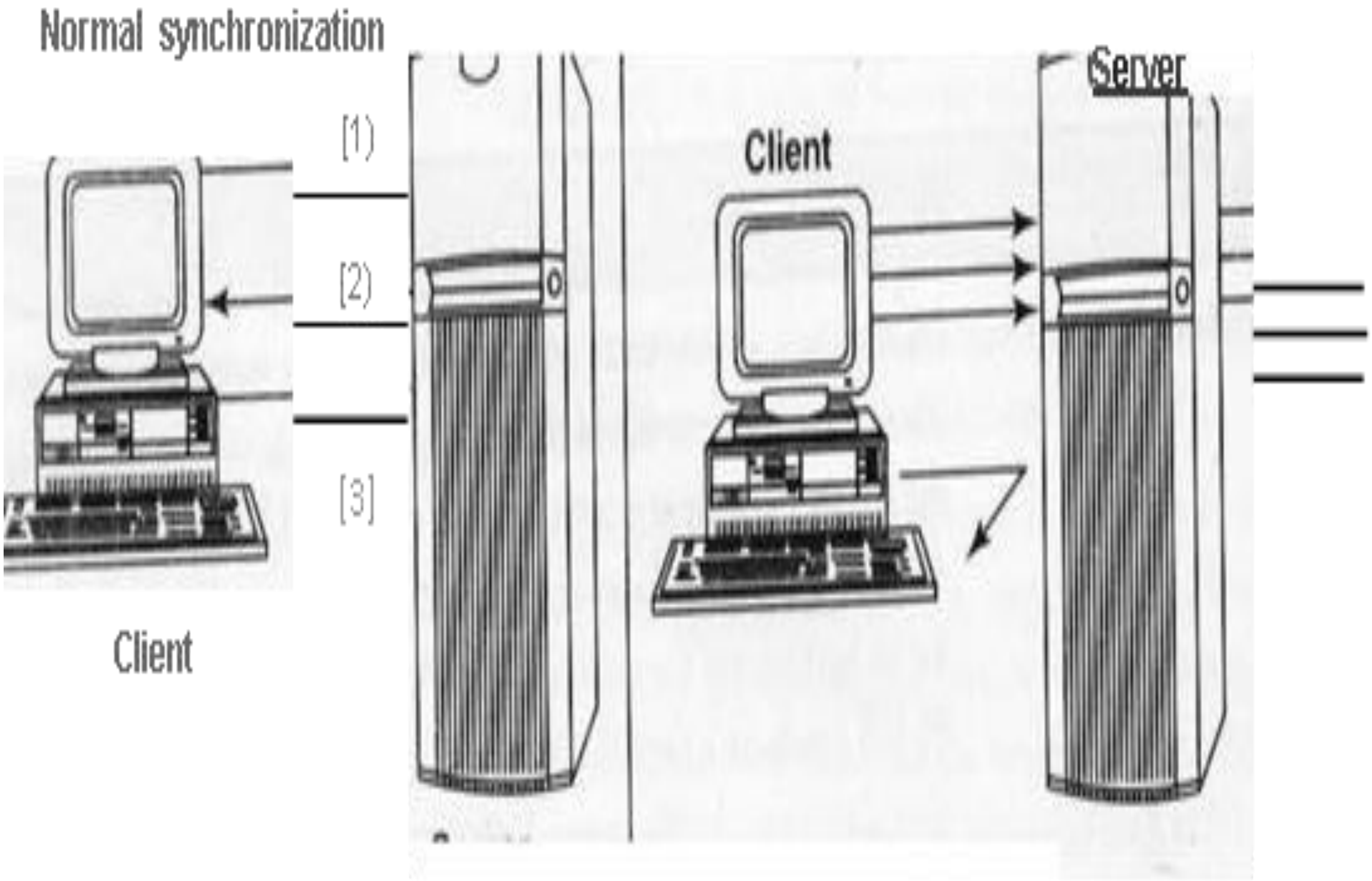
Types or Levels of DoS Attacks(contd)

2. Ping of death attack:

- The ping of death attack sends oversized internet Control Message Prorocol.
- (lCMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages to the victim.
- The maximum packet size allowed is of 65,536 octets. Some systems, upon receiving the oversized packer, will crash, Freeze or reboot, resulting in DoS.

3.SYN attack:

- It is also termed as TCP SYN Flooding. In the Transmission Control Prococol (TCP), handshaking of network connections is done with SYN and ACK messages.
- An attacker initiates a TCP connection to d1c server with an SYN The server replies with an SYN-ACK.
- The client then does not send back an ACK, causing the server to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.


Normal synchronization
[1)
[2)
[3]
Client
Client
Server

3-way Handshake

- Client sends synchronize (syn) pkt to web server
- Server sends synchronize acknowledgment (syn-ack)
- Client replies with an acknowledgment pkt, the connect is established

Chaotic Handshake

- Client sends multiple synchronize (syn) pkts to web server - all with bad addresses.
- Server sends synchronize acknowledgments to in-correct addresses leaving half open connections and flooded queue.
- Legitimate user is denied access because queue is full and additional connections cannot be accepted.

Types or Levels of DoS Attacks(contd)

4. Teardrop attack:

- The teardrop attack is an attack where fragmented packers are forged co overlap each other when the receiving host tries to reassemble them.
- IP’s packer fragmentation algorithm is used to send corrupted packers to confuse the victim and may hang the system.
- This attack can crash various 0S’s due to a bug in their TCP/JP fragmentation reassembly code.
- Windows 3. 1x, Windows 95 and Windows NT OS’s as well as versions of Linux are vulnerable to chis attack.

Types or Levels of DoS Attacks(contd)

4. Smurf attack: :

- It is a way of generating significant computer network traffic on a victim network.
- This is a type of DoS attack that floods a target system via spoofed broadcast ping messages.
- This attack consists of a host sending an ICMP echo request (ping) to a network broadcast address (e.g., network addresses with the host portion of the address having all 1’s).
- Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic.
- On a multi-access broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim.
- Internet relay that (IRC) servers are the primary victim of smurf attacks on the Internet.

Tools Used to Launch DoS Attack

Jolt2: A major vulnerability has been discovered in Windows' networking code. The vulnerability allow remote attackers to cause a DoS attack against Windows-based machines - the attack came the target machine to consume I00% of the CPU time on processing of illegal packets.

Nemesy: This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.

Targa: It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successfully.

Crazy Pinger: This tool could send large packets of ICMP to remote target network.

Some Trouble: It is a remote flooder and bomber. It is developed in Delphi.

DDoS Attack

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the Do$ attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called "secondary victims" and the main target is called "primary victim."
-

How to Protect from DoS/DDoS Attacks

1. Implement router filters. This will lessen your exposure to certain DoS accacks.

2. If such filters are available for your system, install patches to guard against TCP SYN flooding.

3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.

4. Enable quota systems on your OS if they are available.

5. Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.

How to Protect from DoS/DDoS Attacks(contd)

7. Use Tripwire or a similar tool to detect changes in configuration information or other files

8. Invest in and maintain "hot spares" - machines that can be placed into service quickly if a similar machine is disabled.

9. Invest in redundant and fault-tolerant network configurations.

10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You

19ITOC1004 – Cyber Law and Information Security

Unit III – Tools and Methods Used in Cybercrime

CO3: Analyze the cybercrime using tools and methods

LO2:Summarize about Attacks

SO3: Discuss about attacks on wireless networks.

Prepared by

G. Keerthika

AP/IT

Unit III – Tools and Methods Used in Cybercrime

- Introduction - Proxy servers and anonymizes - Phishing, Password cracking - Key loggers and spywares, virus and worms - Trojan Horses and Backdoors – Steganography - DoS and DDoS attacks - Attacks on Wireless Networks.

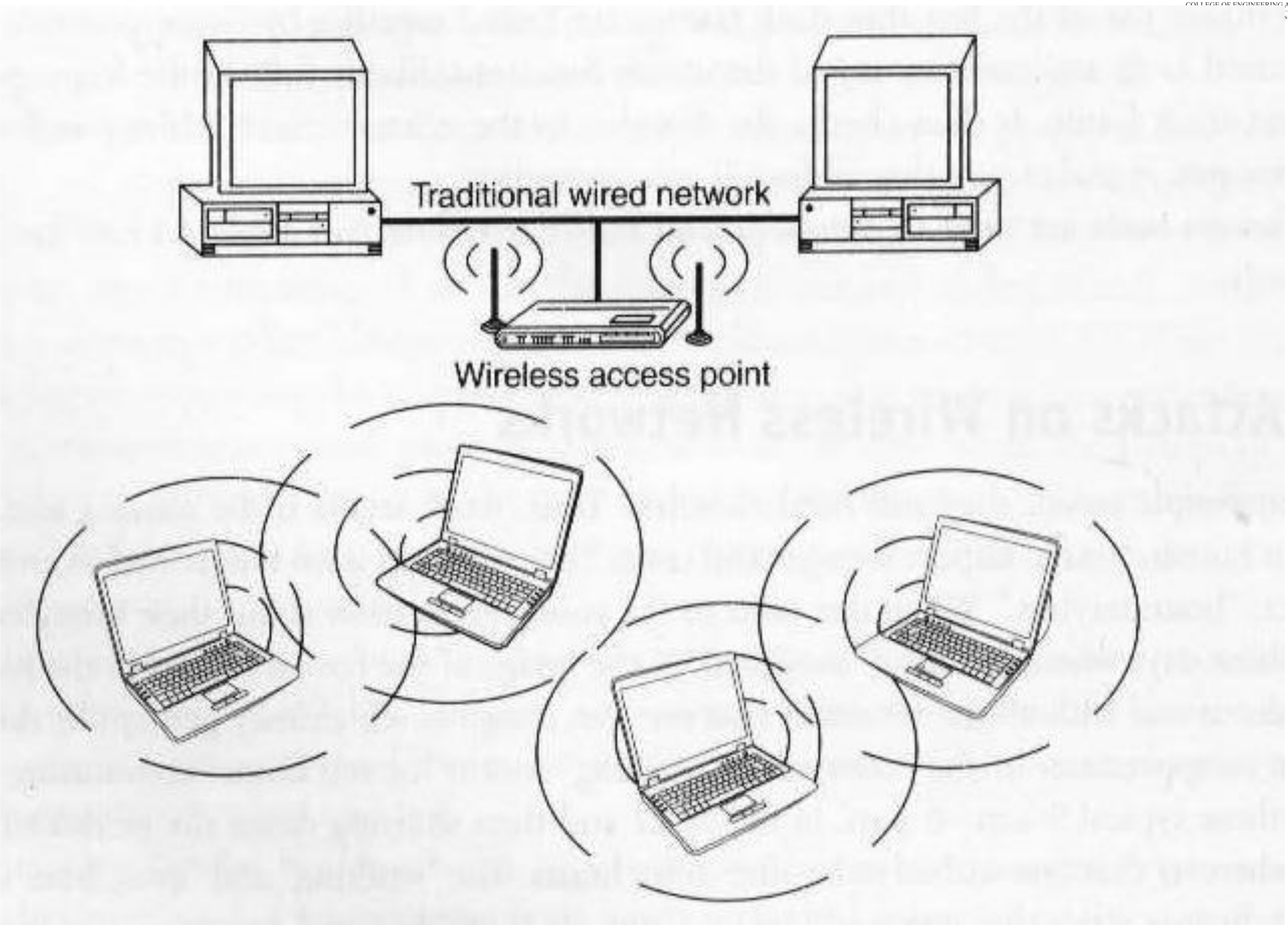
Attacks on Wireless Networks

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, cele-cottagers and in some cases, branch workers.

2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).

3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.

4. **Road warrior:** This is the ultimate mobile user and spends little time in the office, however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels. This type includes the sales and field forces.


Traditional wired network
Wireless access point

Wireless Technology

1. 802.11 networking standards: Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.

- 802. 11: It is applicable to WLANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

- 802.11a: It provides 54 Mbps transmission in the 5 GHz band and uses orthogonal frequency division multiplexing (OPDM) which is more efficient coding technique compared with FHSS and DSSS.

Wireless Technology

- 802.11b: It provides 11 Mbps transmission in the 2.4 GHz band and uses complementary code keying (CCK) modulation to improve speeds.
- 802.11g: It provide 54 Mbps transmission in the 2.4 GH band and the same OFDM coding as 802.11a, hence it is a lot faster than 802.11a and 802.11 b.
- 802.11n: It is the newest standard available widely and uses multiple-input multiple-output (MIMO) that enabled to improve the speed and range significantly.

Wireless Technology(contd)

2. Access points: It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals.

Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.

3. Wi-Fi hotspots: A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants.

- **Free Wi-Fi hotspots:** Wireless Internet service is offered in public areas, free of cost and that to without any authentication.
- **Commercial hotpots:** The users are redirected to authentication and online payment to avail the wireless Internet service in public areas.

Wireless Technology(contd)

4. Service set identifier (SSID): It is the name of 802.11 i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other.

- While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN.
- It is always advised to turn OFF the broadcast of the SSID, which results in the detected network displaying as an unnamed network and the user would need to manually enter the correct SSID to connect to the network.
- Hence, it is also advised to set the SSID manually rather than leaving it blank. Moreover, it is important to note chat turning off the broadcast of the SSJD discourages casual wireless snooping, however, it does not stop an attacker trying to attack the network.

Wireless Technology(contd)

5. Wired equivalence privacy (WEP): Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997.

- It is always termed as deprecated security algorithm for LEEE 802. I Ii WLANs. SSID along with WEP delivers fair amount of secured wireless network.

6. Wi-Fi protected access (WPA and WPA2): During 2001, serious weakness in WEP was identified that resulted WEP cracking software(s) being made available to enable cybercriminals to intrude into WLANs.

- WPA was introduced as an interim standard co replace WEP to improve upon the security features of WEP.
- WPA2 is the approved Wi-Fi alliance interoperable implementation of 802.11i. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.

Wireless Technology(contd)

7. Media access control (MAC): It is a unique identifier of each node of the network and it is assigned by the manufacturer of a network interface card (NlC) scored in its hardware.

- MAC address filtering allows only the devices with specific MAC addresses to access the network.
- The router should be configured stating which addresses are allowed. Although this method appears to be very secure, the attacker can spoof a MAC address.
- That is, copy the known MAC address to entire network that the device he/she is using belongs to the network,.
- At the same time it is important to note that, in case you purchase a new device or if any visitors would like to connect to the network, you will need to add the MAC addresses of these new devices to the list of approved addresses.

Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access *is* termed as **wireless cracking.**

1. **Sniffing:** It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network.
    - 'lhe attacker usually installs the sniffers remotely on the victims system and conducts activities such as
        - Passive scanning of wireless network
        - detection of SSID
        - collecting the MAC address, collecting the frames to crack WEP

-

Traditional Techniques of Attacks on Wireless Networks(contd)

2. Spoofing: The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage.

The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network.

It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one. . This convenient feature is always exploited by the attacker.

- **MAC address Spoofing:** It is a technique of changing an assigned media access control (MAC) address of a networked device to a different one.

This allows the attacker to bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.

IP Spoofing: It is a process of creating IP packers with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

Traditional Techniques of Attacks on Wireless Networks (contd)

Frame Spoofing: The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications.

Frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detected unless the address is entirely faked/bogus.

Traditional Techniques of Attacks on Wireless Networks (contd)

4. Man-in-the-middle attack (MITM): It refers to the scenario wherein an attacker on host A inserts A between all communications - between hosts X and Y without knowledge of X and Y.

All messages sent by X do reach Y but through A and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.

5. Encryption cracking: It is always advised that the first step to protect wireless networks is to use WPA encryption.

The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field.

Hence, the second step is to use a long and highly randomized encryption key, this is very important. It is a little pain to remember long random encryption, however, at the same time these keys are much harder to crack.

How to Secure the Wireless Networks

1. Change the default settings of all the equipment's/components of wireless network (e.g., [P address/ user IDs/administrator passwords. ere.).

2. Enable WPA/WEP encryption.

3. Change the default SSID.

4. Enable MAC address filtering.

5. Disable remote login.

6. Disable SSID broadcast.

7. Disable the features that are not used in the AP (e.g., printing/music support).

8. Avoid providing the network a name which can be easily identified

9. Connect only to secured wireless network {i.e., do not auto connect to open Wi-Fi hotspots).

10. Upgrade router's firmware periodically.

How to Secure the Wireless Networks(contd)

11. Assign static IP addresses to devices.

12. Enable firewalls on each computer and the router.

13. Position the router or AP safely.

14. Turn off the network during extended periods when not in use.

15. Periodic and regular monitor wireless network security.

References

Text Book(s): T1. Nina Godbole, Sunit Belapure, ―Cyber security: Understanding Cybercrime, Computer Forensics and Legal perspectives‖, Wiley India Pvt.Ltd, 2019.

Reference Book(s):

R1. Aparna Viswanatha , ―Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes‖, LexisNexis Publishers, 2012.

R2. Rodney D. Ryder, " Guide to Cyber Laws", Second Edition, Wadhwa and Company, 2007.

Web References:

1. http://www.cyberlawsindia.net/internet-crime.html

2. http://www.computerforensicsworld.com

Thank You