# Module 5

Tools and Methods used in Cybercrime

# Introduction

- Attackers are systematic in launching their attacks
- Stages of attack are:
  - Initial uncovering
  - Network probe
  - Crossing the line towards electronic crime
  - Capturing the network
  - Grab the data
  - Covering tracks

- **Initial uncovering**
  - the attacker gathers information, as much as possible
  - The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute
  - the attacker uncovers as much information as possible on the company's internal network
- **Network probe**
  - the attacker uses more invasive techniques to scan the information.
  - Ping sweep, port scanning

- **Crossing the line toward electronic crime (E-crime):**
  - exploiting possible holes on the target system
  - programming errors can be used by attackers to compromise a system' Once the attackers are able to access a user account without many privileges,
  - they will attempt further exploits to get an administrator or "root" access
- **Capturing the network**
  - attacker attempts to "own" the network
  - remove any evidence of the attack.

- **Grab the data:**
  - steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites
  - Leads to potentially expensive and embarrassing situation for an individual and/or for an organization.
- **Covering tracks**
  - activities undertaken by the attacker to extend misuse of the system without being detected
  - attacker can remain undetected for long periods or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action

- Tools used to cover tracks
  - http://www.ibt.ku.dk/jesper/ELSave/
  - http://ntsecurity.nu/toolbox/winzapper/
  - http://www.evidenceeliminator.com/
  - http://www.traceless.com/computer-forensics/
  - http://www.acesoft.net/

# Proxy Servers and Anonymizers

- computer on a network which acts as an intermediary for connections with other computers on that network.
- The attacker first connects to a proxy server and establishes a connection with the target system
- A client connects to the proxy server and requests some services
- The proxy server evaluates the request and provides the resource by establishing the connection
- Using a proxy server can allow an attacker to hide ID

- Purpose of proxy server:
  - Keep the systems behind the curtain
  - Speed up access to a resource
  - Specialized proxy servers are used to filter unwanted content
  - Proxy server can be used as IP address multiplexer
- List of websites where free proxy servers can be found:
  - http://www.proxy4free.com
  - http://www.publicproxyservers.com
  - http://www.proxz.com
  - http://www.anonymitychecker.com
  - http://www.surf24h.com

- *An anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- used to make Web surfing anonymous by utilizing a that acts as a proxy server for the web client
- List of websites where information about anonymizers can be found:
  - http://www.anonymizer.com
  - http://www.browzar.com
  - http://www.anonymize.net
  - http://www.anonymouse.ws
  - http://www.anonymousindex.com

# Phishing

- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- Stealing of personal and financial data
- Infect the system with viruses
- Messages look authentic and attempt to get users to reveal their personal information

# How Phishing Works?

- Planning
- Setup
- Attack
- Collection
- Identity theft and fraud

# Password Cracking

- Need for password cracking
  - 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.

- Steps followed for password cracking are:
  - 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.

- attacker can also create a script file - considered as manual cracking, is time-consuming and not usually effective
- One way function is applied to the password - in combination with other data, and the resulting value is stored – authentication
- most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools

# Password cracking tools

- www.defaultpassword.com
- http://www.oxid.it/cain.html
- http://www.openwall.com/john
- http://freeworld.thc.org/thc-hydra
- http://www.aircrack-ng.org
- http://www.solarwinds.com
- http://project-rainbowcrack.com
- http://www.hoobie.net/brutus

# Password cracking attacks

- Online attacks
- Offline attacks
- Non-electronic attacks

# Online Attacks

- An attacker can create a script file
  - Ex: man-in-the middle (MITM) attack
- active eavesdropping
- attacker establishes a connection between a victim and the server to which a victim is connected
- used to obtain the passwords for E-Mail accounts on public websites

# Offline Attacks

- attacks are performed from a location other than the target
- require physical access to the computer and copying the password file from the system onto removable media
- Types of offline attack are:
  - Dictionary attack
  - Hybrid attack
  - Brute force attack

# Strong, Weak and Random Passwords

- A weak password is one, which could be easily guessed, short, common and a system default password
- A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it.
- Random password - random strings of characters
- Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols

- General guidelines applicable to the password policies:
  - Passwords and user logon identities (IDs) should be unique to each authorized user.
  - Passwords should consist of a minimum of eight alphanumeric characters
  - should be computer-controlled lists of prescribed password rules and periodic testing
  - Passwords should be kept private
  - Passwords shall be changed every 30/45 days or less
  - User accounts should be frozen after five failed logon attempts
  - Sessions should be suspended after 15 minutes
  - Successful logons should display the date and time of the last logon and logoff
  - Logon IDs and passwords should be suspended after a specified period of non-use
  - For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session

- Password guidelines to avoid being victim of E-Mail accounts hacked/attacked by the attackers:
  - Passwords used for business E-Mail accounts, personal E-Mail accounts should be kept separate.
  - Passwords should be of minimum eight alphanumeric characters
  - Passwords should be changed every 30/45 days
  - Passwords should not be shared with relatives and/or friends
  - Password used previously should not be used while renewing the password
  - Passwords should not be stored under mobile phones/PDAs
  - 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
  - In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately

# Keyloggers and Spywares

- Keystroke logging is the practice of noting the keys struck on a keyboard
- software keylogger, hardware keylogger, antikeylogger

# Software Keyloggers

- Software keyloggers are software programs installed on the computer systems
- located between the OS and the keyboard hardware, and every keystroke is recorded
- installed on a computer system by Trojans or viruses without the knowledge of the user
- A keylogger usually consists of two files that get installed in the same directory:
  - dynamic link library (DLL) file
  - EXEcutable (EXE) file
- EXEcutable (EXE) file that installs the DLL fi le and DLL file records the keystrokes

# Software keyloggers

- http://www.soft-central.net
- http://www.spytech-web.com
- http://www.relytec.com
- http://www.stealthkeylogger.org
- http://kgb-spy-software.en.softonic.com
- http://www.cyberspysoftware.com
- http://www.mykeylogger.com

# Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- connected to the PC and/or to the keyboard
- save every keystroke into
- a file or in the memory of the hardware device
- Installed in ATM machines

# Antikeylogger

- Tool that can detect the keylogger installed on the computer system and remove it
- Advantages of antikeyloggers are:
  - Firewalls cannot detect the installations of keyloggers on the systems
  - This software does not require regular updates of signature bases
  - Prevents Internet banking frauds
  - It prevents ID theft
  - It secures E-Mail and instant messaging/chatting

# Spywares

- type of malware - that is installed on computers - collects information about users without their knowledge
- secretly installed on the user's personal computer
- Spyware programs collect personal information about the victim
- 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
- Anti-Spyware softwares are used to overcome the emergence of Spywares

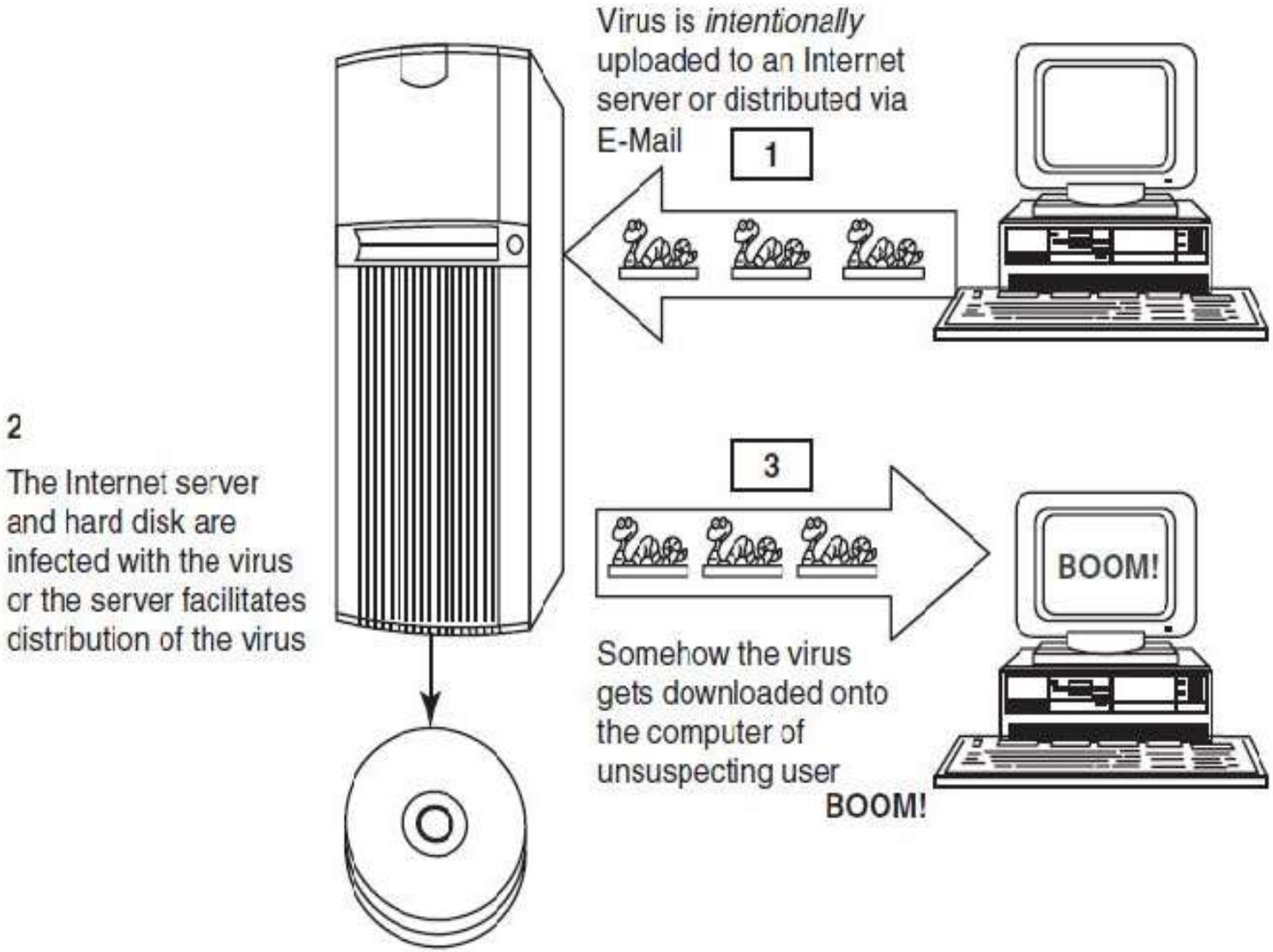
# Spywares

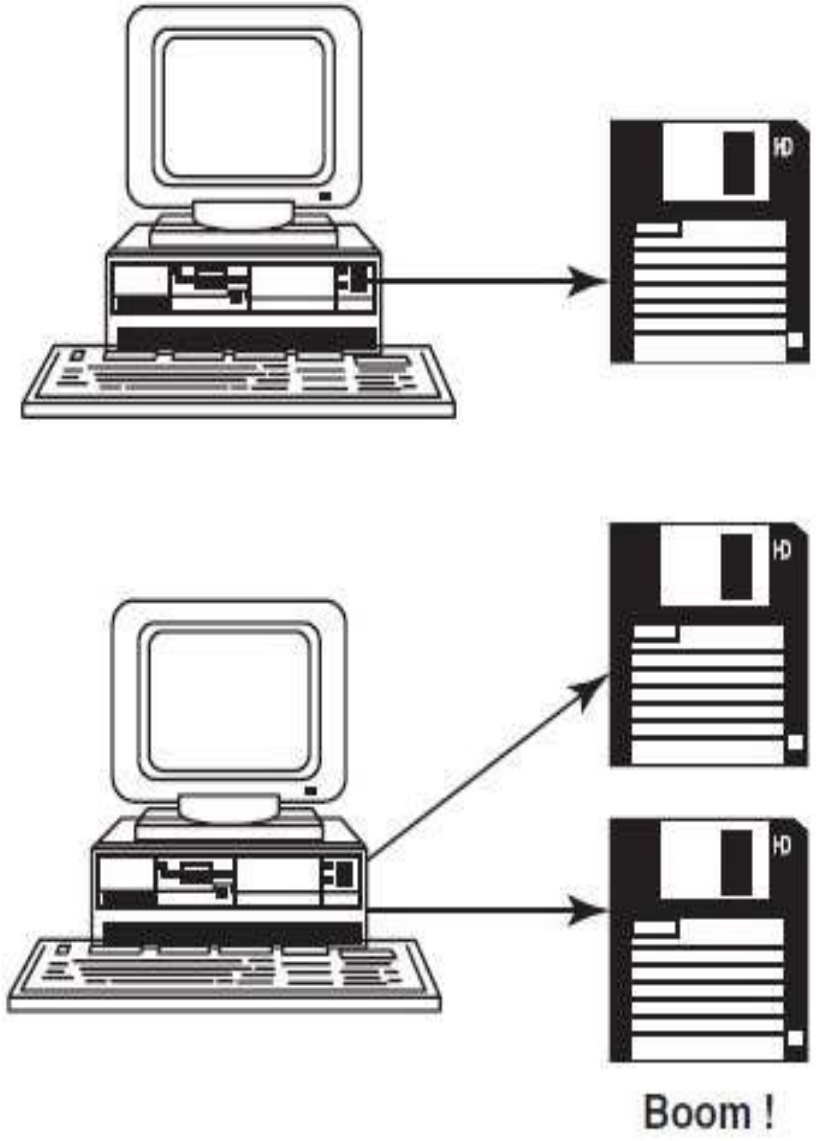
- 007 Spy
- Spector Pro
- eBlaster
- Remotespy
- Stealth Recorder Pro
- Stealth Website Logger
- Flexispy

# Virus and Worms

- Computer virus is a program that can “infect” legitimate programs by modifying them
- Viruses contain malicious instructions that may cause damage or annoyance
- Viruses can often spread without any readily visible symptoms
- A virus can start on event-driven effects, time-driven effects or can occur at random
- Computer virus has the ability to copy itself and infect the system

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


Virus is *intentionally* uploaded to an Internet server or distributed via E-Mail
1
2
The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus
3
Somehow the virus gets downloaded onto the computer of unsuspecting user
BOOM!
BOOM!




1

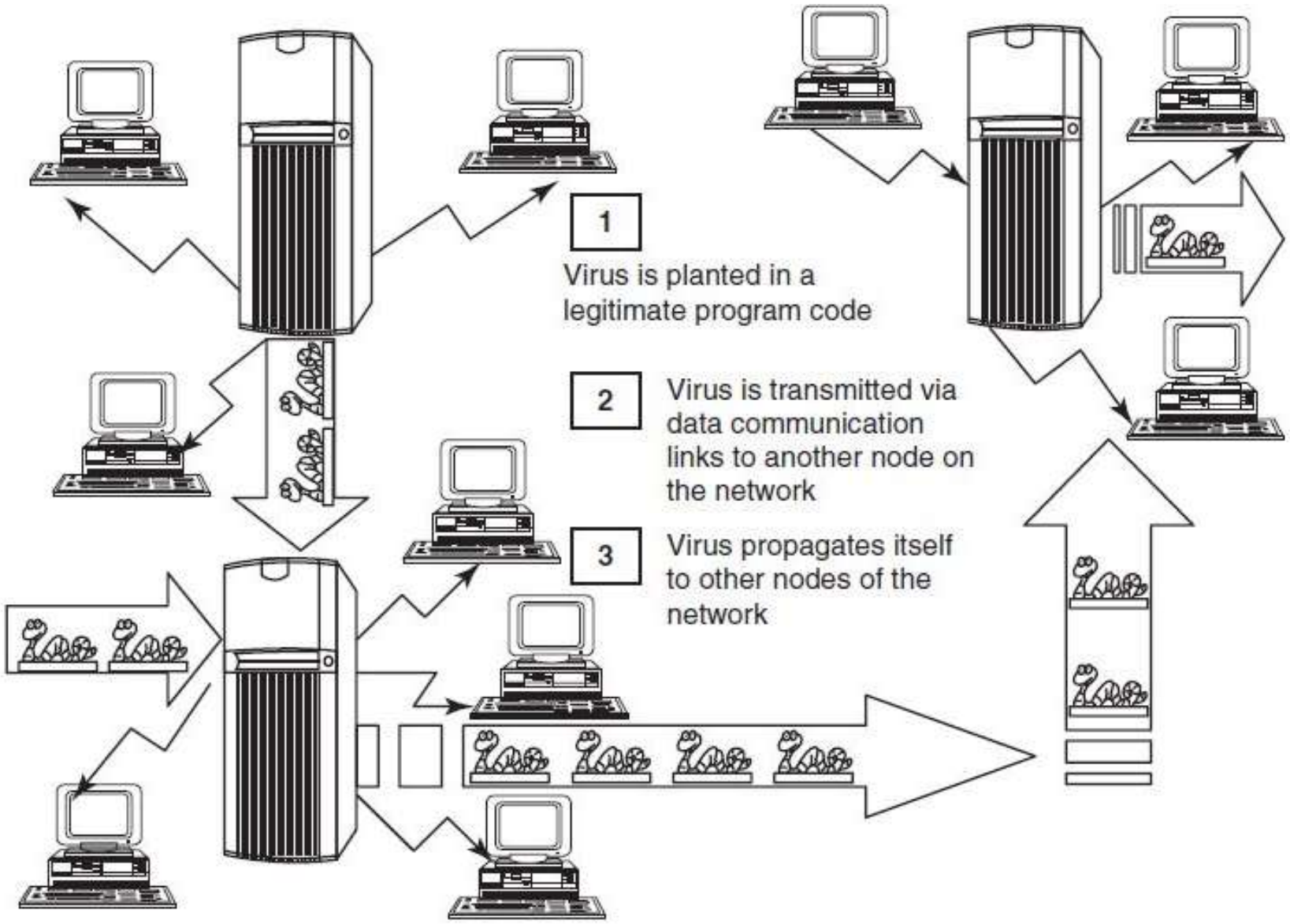
Virus-infected diskette is loaded to a micro-computer system and the hard disk is infected

2

A clean diskette is loaded into an Infected micro-computer system

3

When removed, this (previously clean) diskette is also now infected with the virus


1
Virus is planted in a legitimate program code
2
Virus is transmitted via data communication links to another node on the network
3
Virus propagates itself to other nodes of the network

- true virus can only spread from one system to another
- Viruses can increase their chances of spreading to other systems
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities
- Trojan is a code/program that appears to be harmless but hides malicious functions

# Virus v/s worm

| *Sr. No.* | *Facet* | *Virus* | *Worm* |
|---|---|---|---|
| 1 | Different types | Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus | E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms |
| 2 | Spread mode | Needs a host program to spread | Self, without user intervention |
| 3 | What is it? | A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus | A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention |
| 4 | Inception | The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it. | The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted |
| 5 | Prevalence | Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005) | Prevalence for virus is very high as against moderate prevalence for a worm. |

# Types of Viruses

- Boot sector viruses
- Program viruses
- Multipartite viruses
- Stealth viruses
- Polymorphic viruses
- Macroviruses
- Active X and Java Control

- Virus attack specific file types (or files).
- A virus manipulates a program to execute tasks unintentionally.
- An infected program produces more viruses.
- An infected program may run without error for a long time.
- Viruses can modify themselves and may possibly escape detection this way.

# Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside harmless program or data.
- get control and cause harm - ruining the file allocation table on the hard disk
- Can be widely redistributed as part of a computer virus
- Trojans can be induced into the system through web browser, via E-Mail or software downloaded from the Internet, through a USB flash drive or other portable media.
- Trojans appear benign and harmless - perform malicious functions to harm the computer system

# Treats posed by Trojan Horses

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

# Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms – hides from user.
- Very similar to a virus, difficult to detect
- dangerous parasite – allows a malicious person to perform any possible action on a compromised system
- backdoors are autonomic malicious programs
- Programmers
- sometimes leave such backdoors in their software for diagnostics and troubleshooting purpose

- Functions of backdoor are:
  - It allows an attacker to create, delete, rename, copy or edit any file, execute various commands
  - It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer
  - It steals sensitive personal information, valuable documents, passwords, login names, ID details
  - It records keystrokes that a user types on a computer's keyboard and captures screenshots
  - It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server
  - It infects files, corrupts installed applications and damages the entire system
  - It distributes infected files to remote computers with certain security vulnerabilities
  - It installs hidden FTP server that can be used by malicious persons for various illegal purposes
  - It degrades Internet connection speed and overall system performance, decreases system security and causes software instability
  - It provides no uninstall feature, and hides processes, files and other objects to complicate its removal

# Examples of backdoor trojans

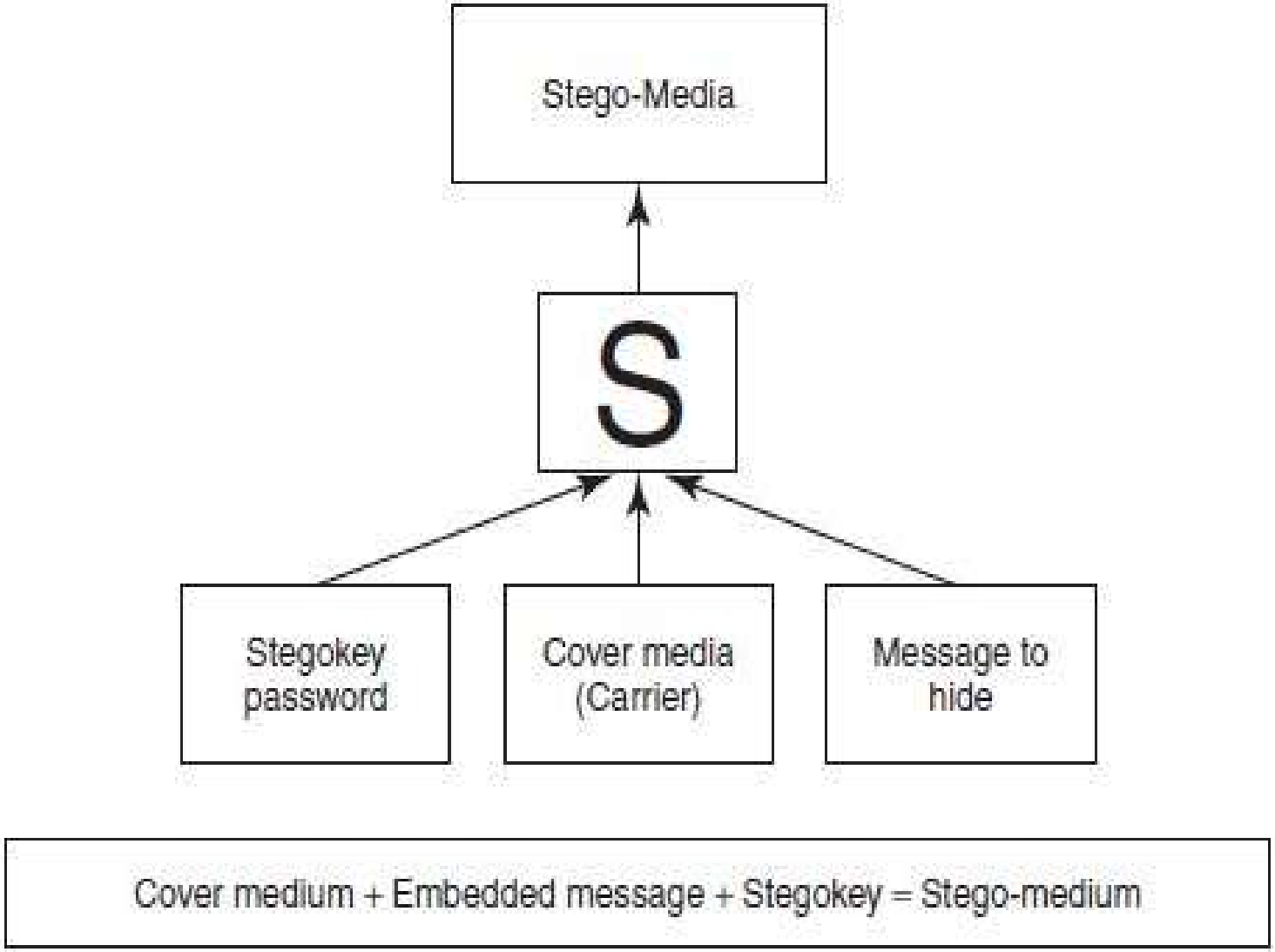
- Back Orifice
- Bifrost
- SAP backdoors
- Onapsis Bizploit

# How to Protect from Trojan Horses and Backdoors

- Stay away from suspect websites/weblinks
- Surf on the Web cautiously
- Install antivirus/Trojan remover software

# Steganography

- It is a method that attempts to hide the existence of a message or communication
- the art and science of hiding information
- Also called as data hiding, information hiding and digital watermarking
- aids confidentiality and integrity of the data
- *Digital watermarking is the process of* irreversibly embedding information into a digital signal – audio, video or pictures


Stego-Media
S
Stegokey password
Cover media (Carrier)
Message to hide
Cover medium + Embedded message + Stegokey = Stego-medium

# Steganography tools

- DiSi-Steganograph
- Invisible Folders
- Invisible Secrets
- Stealth Files
- Hermetic Stego
- DriveCrypt Plus (DCPP)
- MSU StegoVideo
- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography

# DoS and DDoS Attacks

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

# DoS Attacks

- Here the attacker floods the bandwidth of the victim's network - depriving him of the services he is entitled to access or provide
- The main objective is to prevent the Internet site or service from functioning efficiently or temporarily or indefinitely.
- Target of DoS attacks are: banks, credit card payment gateways, mobile phone networks root name servers
- Use of Buffer overflow technique - *Spoofing.*
- creation of IP packets with a forged (spoofed) source IP address – so as to conceal the ID of the sender or impersonating another computing system

- The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- The victim machine keeps waiting for response from the attacker’s machine for each request
- This consumes the bandwidth of the network which then fails to serve the valid requests and ultimately breaks down

- Symptoms of DoS attack are:
  - Unusually slow network performance
  - unavailability of a particular website
  - inability to access any website
  - dramatic increase in the number of Spam E-Mails received
- Effects of DoS attack:
  - 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

- Bandwidth attacks
  - Loading any website takes certain time. “loading” consumes some amount of memory
- Logic attacks
  - These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack
- Protocol attacks
  - 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
- Unintentional DoS attack
  - This is a scenario where a website ends up denied

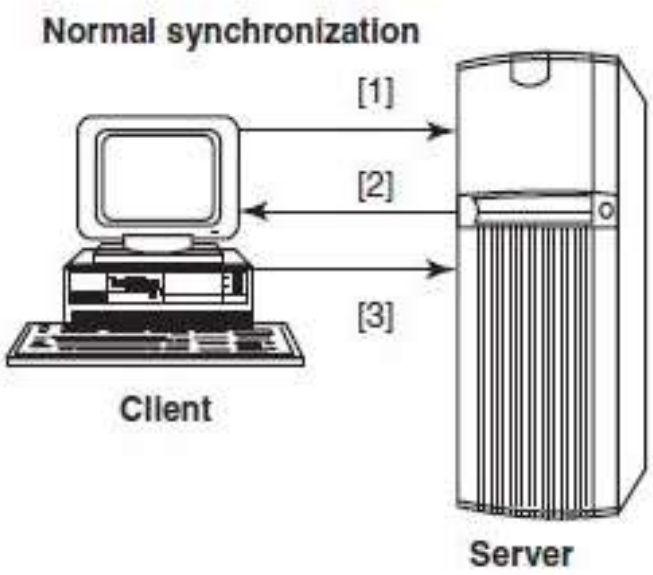
# Types or Levels of DoS Attacks

- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- Nuke

- Flood attack
  - earliest form of DoS attack
  - ping flood
  - Attacker sends a number of ping packets – more traffic
- Ping of death attack
  - sends oversized Internet Control Message Protocol (ICMP) packets
  - The maximum packet size allowed is of 65,536 octets
  - May result in crash, freeze or reboot, resulting in DoS

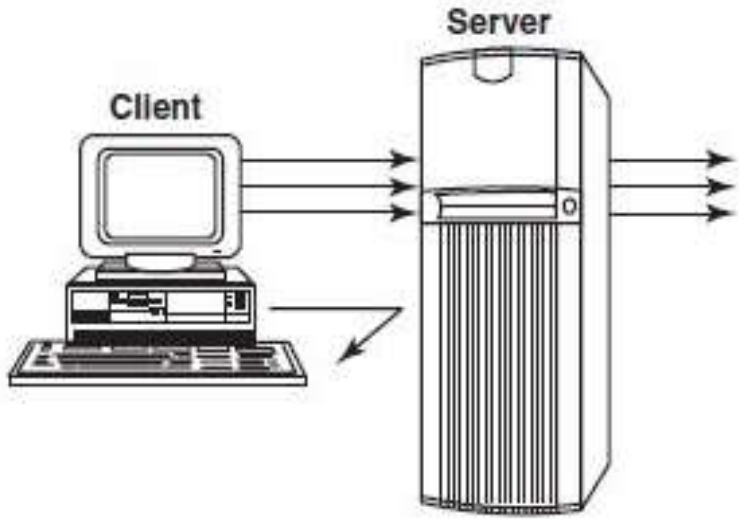
- SYN attack
  - *TCP SYN Flooding*
  - An attacker initiates a TCP connection to the server with an SYN
  - The server replies with an SYN-ACK
  - Th e client then does not send back an ACK, causing the server to allocate memory for the pending connection and wait
- Teardrop attack
  - fragmented packets are forged to overlap each other when the receiving host tries to reassemble them
  - Use of IP's packet fragmentation algorithm
  - This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code.

- Smurf attack
  - Generates significant computer network traffic on a victim network
  - spoofed broadcast ping messages - ICMP echo request (ping)
  - magnified DoS attack of ping replies thereby flooding the victim
- Nuke
  - Attack based on fragmented or invalid ICMP packets sent to the target
  - Use of ping utility to send the corrupt data
  - Slows down the affected computer




**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

# Tools Used to Launch DoS Attack

- Jolt2
- Nemesy
- Targa
- Crazy Pinger
- SomeTrouble

# DDoS Attacks

- an attacker may use your computer to attack another computer
- security vulnerabilities or weaknesses - an attacker can take control of the computer
- attack is “distributed” - attacker is using multiple computers
- A DDoS attack is a distributed DoS - large number of zombie systems are synchronized to attack a particular system
- zombie systems – secondary victims, main target is – primary victim

# Tools used to launch DDoS attack

- Trinoo
- Tribe Flood Network (TFN)
- Stacheldraht
- Mstream
- Shaft
- MyDoom

# How to Protect from DoS/DDoS Attacks

- Implement router filters.
- If such filters are available, install patches to guard against TCP SYN flooding.
- Disable any unused or inessential network service.
- Enable quota systems on OS if they are available.
- Observe system's performance and establish baselines for ordinary activity.
- Routinely examine physical security with regard to your current needs.
- Use Tripwire or a similar tool to detect changes in configuration information or other files
- Invest in and maintain "hot spares" – machines that can be placed into service quickly if a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies
- Establish and maintain appropriate password policies

# Tools for detecting DoS/DDoS attacks

- Zombie Zapper
- Remote Intrusion Detector (RID)
- Security Auditor's Research Assistant (SARA)
- Find_DDoS
- DDoSPing

# SQL Injection

- SQL injection is a code injection technique - exploits a security vulnerability - database layer of an application
- SQL insertion attacks
- SQL servers - common database servers to store confidential data
- Malicious Code is inserted into a web form - to make a system execute a command shell
- The attacker determines whether a database and the tables residing into it are vulnerable, before launching
- an attack.

# Steps for SQL Injection Attack

- The attacker looks for the webpages that allow submitting data
- The attacker checks the source code of the HTML, and look for “FORM” tag in the HTML code
- The attacker inputs a single quote under the text box provided on the webpage to accept the username and password
- The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database

- Blind SQL Injection
  - web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker
  - This type of attack can become time-intensive
  - There are tools that can automate these attacks once the location of the vulnerability and the target information have been established

- SQL injection can result in:
  - Obtain some basic information if the purpose of the attack is reconnaissance
  - May gain access to the database by obtaining username and their password
  - Add new data to the database
  - Modify data currently in the database
- Tools used:
  - AppDetectivePro
  - DbProtect
  - Database Scanner
  - SQLPoke
  - NGSSQLCrack
  - Microsoft SQL Server Fingerprint (MSSQLFP) Tool

# How to Prevent SQL Injection Attacks

- Input validation
- Modify error reports
- Other preventions

# Input validation

- Replace all single quotes (escape quotes) to two single quotes
- Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously.
- Numeric values should be checked while accepting a query string value
- Keep all text boxes and form fields as short as possible

# Modify error reports

- errors should not be displayed to outside users
- developer should handle or configure the error reports

# Other preventions

- The default system accounts for SQL server 2000 should never be used
- Isolate database server and web server
- unused triggers, stored procedures, user-defined functions – should be moved to isolated servers.

# Buffer Overflow

- Buffer overflow is the anomaly where the process stores data in a buffer outside the memory
- Triggered by inputs that are designed to execute code or alter the way the program operates – leading to many software vulnerabilities
- C and C++ - no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array
- Ex:

```
int main () {
  int buffer[10];
  buffer[20] = 10;
  }
```

# Types of Buffer Overflow

- Stack-Based Buffer Overflow
  - occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer
- NOPs – No Operation
  - Also called as NOOP - no operation performed
  - Is used to not to change the state of status flags or memory locations in the code.

- Characteristics of stack based programming:
  - “Stack” is a memory space in which automatic variables are allocated
  - Function parameters are allocated on the stack and are not automatically initialized by the system
  - Once a function has completed its cycle, the reference to the variable in the stack is removed
- Exploiting the stack based buffer overflow to manipulate the program can be done by overwriting:
  - A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
  - The return address in a stack frame
  - A function pointer, or exception handler, which is subsequently executed

# NOPs

- Use of NOP opcode - which allows code to execute when the exact value of the instruction pointer is indeterminate
- Technique used for exploiting a stack buffer overflow
- The attacker would find the right memory address
- Large sections of stack are corrupted with NOOP machine instruction – at the end an instruction is placed perform a relative jump to the top of the buffer where the shellcode is located.
- Attackers would look into patterns of NOOP machine instructions in order to detect a shellcode in use

# Heap Buffer Overflow

- Heap buffer overflow occurs in the heap data area
- the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain.
- Characteristic features are:
  - “Heap” is a “free store” that is a memory space, where dynamic objects are allocated
  - The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions
  - Dynamically created variables re created on the heap before the execution program is initialized to zeros

# How to Minimize Buffer Overflow

- Assessment of secure code manually
- Disable stack execution
- Compiler tools
- Dynamic run-time checks
- Tools used:
  - StackGuard
  - ProPolice
  - LibSafe

# Phishing

- “Phishing” is the use of social engineering tactics to trick users into revealing confidential information.
- It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- It is an act of sending an E-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for ID theft.
- It is a scam to steal valuable information such as credit card and social security numbers (SSN), user IDs and passwords – brand spoofing

# Methods of Phishing

- Dragnet
  - use of spammed E-Mails
  - Dragnet phishers do not identify specific prospective victims in advance
- Rod-and-reel
  - phishers identify specific prospective victims in advance
- Lobsterpot
  - focuses upon use of spoofed websites
- Gillnet
  - relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites

# Phishing Techniques

- URL (weblink) manipulation
- Filter evasion
- Website forgery
- Flash Phishing
- Social Phishing
- Phone Phishing

# Spear Phishing

- “Spear Phishing” is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering