



Different Types of Attacks

Information Security



PART - I

- Introduction
- Cryptographic Attacks
- Injection Attacks
- Privilege escalation

By Koteswar
Rao

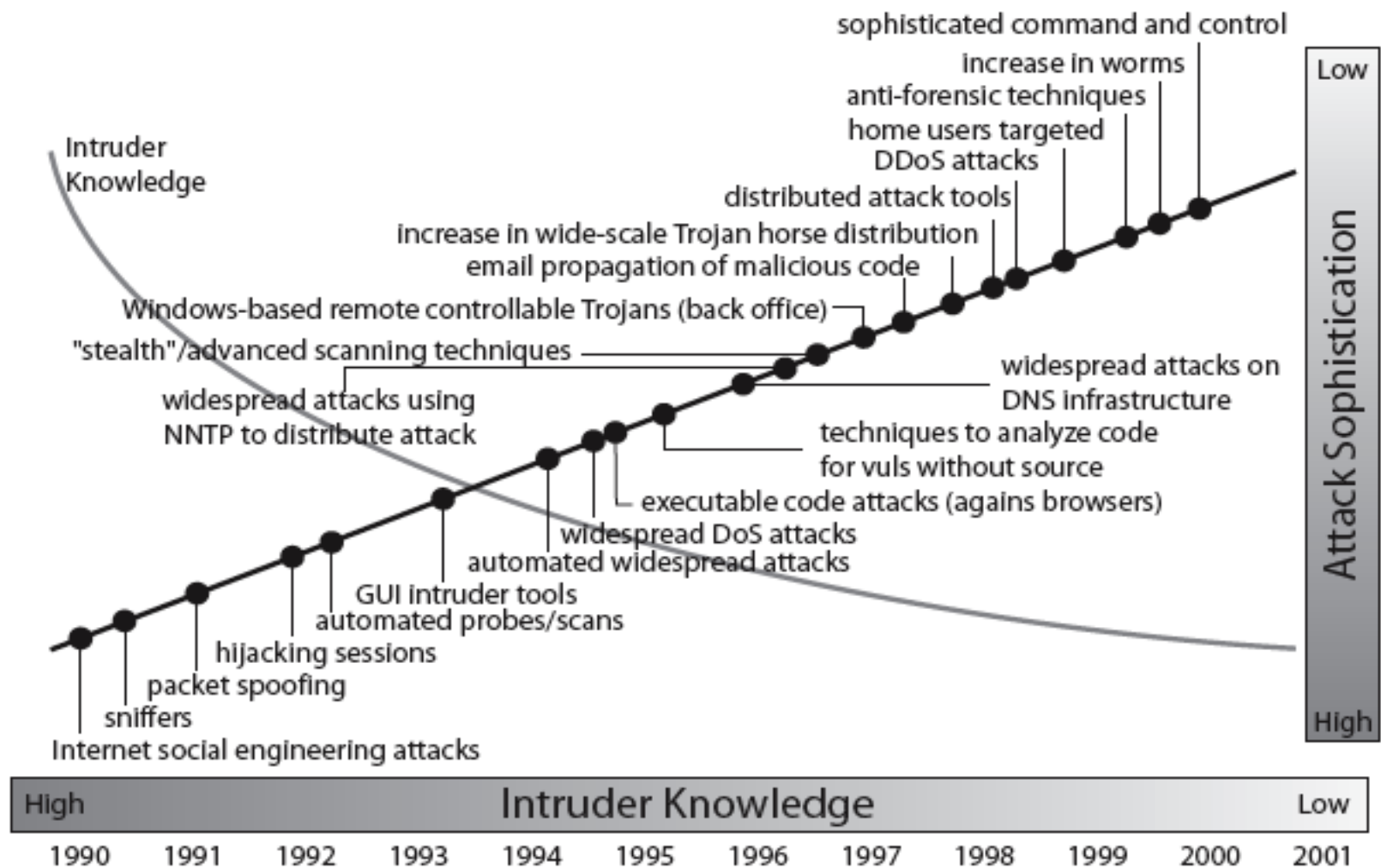
Attack

- Act or action that exploits vulnerability in controlled system.
- Vulnerability-
 - An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Types of attacks

- Cryptographic Attacks
- Injection Attacks
- Privilege escalation
- Phishing
- DoS
- Spoofing
- Malwares

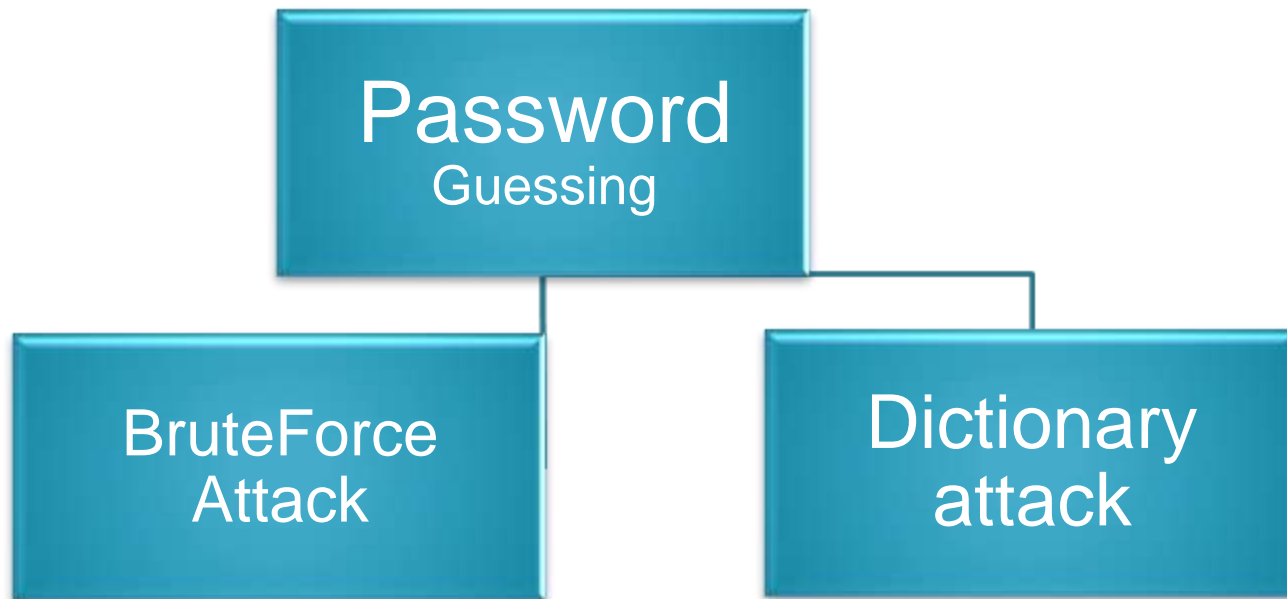
Security Trends



Source: CERT

Password guessing attack

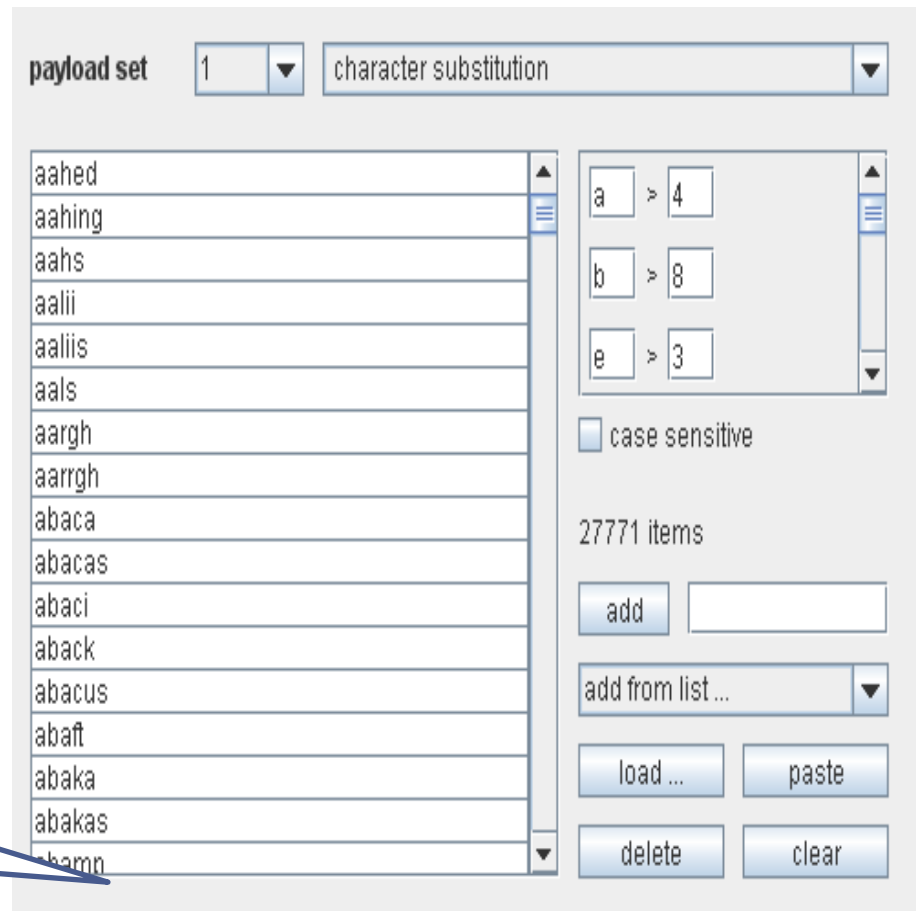
- unauthorized user repeatedly tries to log on to a computer or network by guessing usernames and passwords.



Brute force attack

- Brute force attack is a type of password guessing attack. In this type of attack, attackers systematically try every conceivable combination to find out the password of a

Password
guessing
program



Download link :

<http://portswigger.net/burp/help/intruder.html>

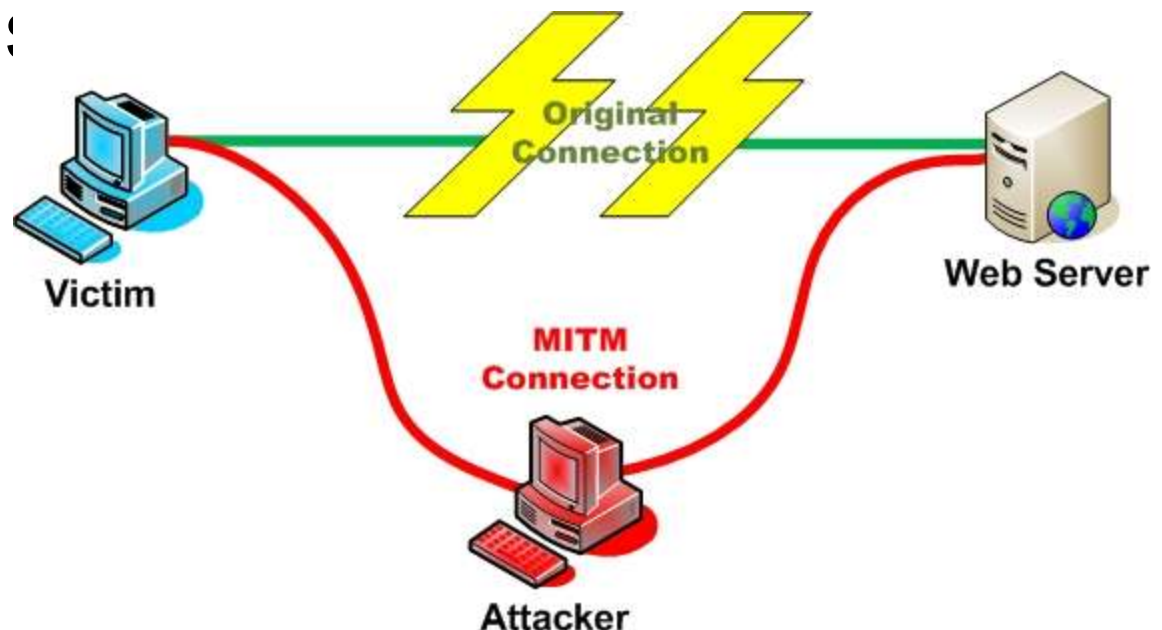
Dictionary attack

- This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks.



Man in the middle attack

- occur when an attacker successfully inserts an intermediary software or program between two communicating system:



Man in the middle attack(contd..)

- The MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based. It's possible to capture a session cookie reading the http header, but it's also possible to change an amount of money transaction inside the application context,

Man in the middle attack(contd..)

Request	Response	Trap
<pre>POST http://janaina:8180/WebGoat/attack?menu=410 HTTP/1.1 Host: janaina:8180 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4 Paros/3.2.1 2 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: en-us,en;q=0.5 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Proxy-Connection: keep-alive Referer: http://janaina:8180/WebGoat/attack?Screen=57&menu=410 Cookie: JSESSIONID=B33154E70ABA78849F1D83EC1183BB9B Authorization: Basic Z3Vlc3Q6Z3Vlc3Q= Content-Type: application/x-www-form-urlencoded Content-Length: 81 QTY1=6&QTY2=6&QTY3=6&QTY4=6&field2=4128+3214+0002+1999&field1=111&SUBMIT=Purchase</pre>		

Raw View ▼

MITM Attack tools

There are several tools to realize a MITM attack. These tools are particularly efficient in LAN network environments, because they implement extra functionalities, like the arp spoof capabilities that permit the interception of communication between hosts.

1. PacketCreator
2. Ettercap
3. Dsniff
4. Cain e Abel

Cross-Site Scripting in a Nutshell

- Consider a web site that gathers user input
- User input is displayed back to user
 - Validate address, search results, etc.
- Attacker crafts URL with a script in it and sends to victim
 - Victim clicks on link
 - Script in the URL is sent to server as user input
 - User input displayed; script "reflected" back to client
 - Script runs on client
- Which state do I live in? I am a resident of:
`<SCRIPT LANGUAGE=Javascript>alert ("You are vulnerable to cross-site scripting!");</SCRIPT>`

Cross-Site Scripting Overview

- Attacker intends to obtain sensitive data from victim user that is only accessible from within a valid session with the target site
- Attacker has analyzed the target site and identified a vulnerable CGI script (one that does not properly filter user supplied input, such as HTML `<SCRIPT>` tags)
 - The site displays back to the user something the user types in, such as a name, account number, or anything, really
- Attacker has written a specialized browser script (most likely in JavaScript) that performs an action as a victim user on the target site

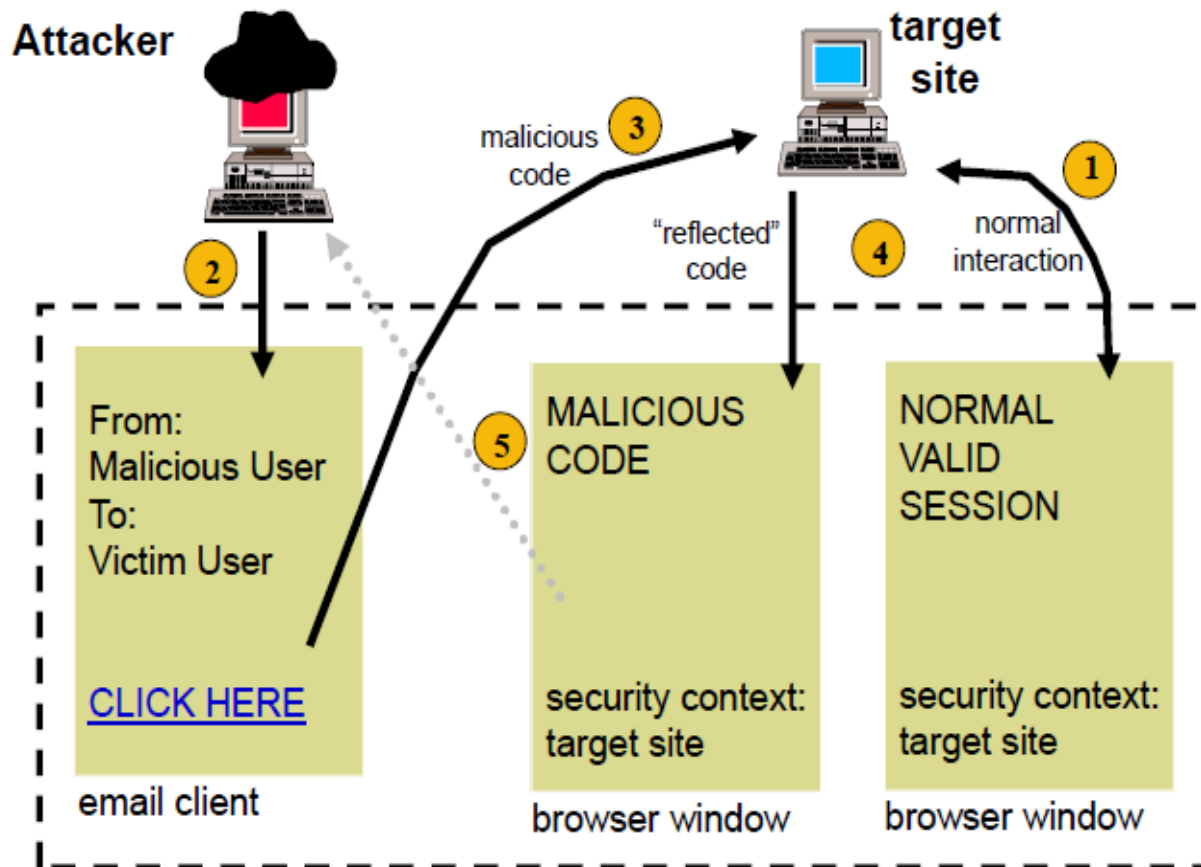
Ways of Launching Cross-Site Scripting Attacks

- Attacker's script must be sent to the victim
 - Inter-user communication within the target site (i.e., message board, etc.)
 - URL provided on a third-party web site (either clicked on by victim user or automatically loaded when visiting a malicious web site)
 - URL embedded in an email or newsgroup posting

How Cross-Site Scripting Attacks Work

- 1) Victim logs into the target site
 - Could occur through social engineering by attacker
 - Log in to your account to get this special offer!!!
- 2) Victim then clicks on a URL or visits a web site that includes the malicious code
- 3) Victim user's browser transmits malicious code to the vulnerable script on the target site as a web request
- 4) Target site reflects the malicious code back to the victim user's browser in the response to the request
- 5) Malicious code executes within victim user's browser under the security context of the target site

How It Works (continued)



When Will The Attack Be Successful?

- User must be convinced to click on a URL or visit a malicious web site

AND

- User must be currently logged into the target site and have a valid session (that has not timed out)
- Both conditions can be accomplished through social engineering via e-mail or telephone

Cross-Site Scripting Defenses

- Remove from user input all characters that are meaningful in scripting languages:
 - `=<>"'();`
 - You must do this filtering on the server side
 - You cannot do this filtering using Javascript on the client, because the attacker can get around such filtering
- More generally, on the server-side, your application must filter user input to remove:
 - Quotes of all kinds (', ", and `)
 - Semicolons (;), Asterisks (*), Percents (%), Underscores (_)
 - Other shell/scripting metacharacters (`=&|*?~<>^()[]{}$\\n\\r`)
- Your best bet – define characters that are ok (alpha and numeric), and filter everything else out

PART - II

1. Phishing
2. DoS attack
3. Spoofing

By Rohan Bharadwaj

Phishing

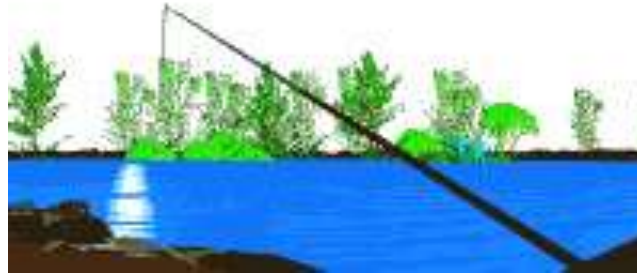
- **Phishing** is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.
- Con artists might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card company, and request that you provide personal information.

History of Phishing

- **Phreaking** + **Fishing** = **Phishing**
Phreaking = Experiment with telecommunication networks in 70's
Fishing = Use bait to lure the target
- **Phishing** in 1995
Target: AOL users
Purpose: getting account passwords for free time
Threat level: low
Techniques: Similar names (www.ao1.com for www.aol.com), social engineering
- **Phishing** in 2001
Target: Ebayers and major banks
Purpose: getting credit card numbers, account numbers
Threat level: medium
Techniques: Same in 1995, keylogger
- **Phishing** in 2007
Target: Paypal, banks, ebay
Purpose: bank accounts
Threat level: high
Techniques: browser vulnerabilities, link obfuscation



A bad day phishin', beats a good day workin'



- 2,000,000 emails are sent
- 5% get to the end user – 100,000 (APWG)
- 5% click on the phishing link – 5,000 (APWG)
- 2% enter data into the phishing site –100 (Gartner)
- \$1,200 from each person who enters data (FTC)
- Potential reward: **\$120,000**

In 2005 David Levi made over \$360,000 from 160 people using an eBay Phishing scam

Spear-**Phishing**: Improved Target Selection



- **Socially aware attacks**
 - ✓ Mine social relationships from public data
 - ✓ **Phishing** email appears to arrive from someone known to the victim
 - ✓ Use spoofed identity of trusted organization to gain trust
 - ✓ Urge victims to update or validate their account
 - ✓ Threaten to terminate the account if the victims not reply
 - ✓ Use gift or bonus as a bait
 - ✓ Security promises
- **Context-aware attacks**
 - ✓ “Your bid on eBay has won!”
 - ✓ “The books on your Amazon wish list are on sale!”




http://paypal-billing-confirm.com/webscr.php?cmd=LogIn

PayPal® [Sign Up](#) | [Log In](#) | [Help](#)

Welcome Send Money Request Money Merchant Tools Auction Tools

Member Log In

Secure Log In 

Registered users log in here. Be sure to [protect your password](#).

Email Address: [Forget your email address?](#)

Password: [Forget your password?](#)

New users [sign up here!](#) It only takes a minute.

[About](#) | [Account Types](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#) | [Jobs](#) | [Buyer Credit](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

[PayPal, an eBay company](#)

Copyright © 1999-2006 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

How To Tell If An E-mail Message is Fraudulent



- Here are a few phrases to look for if you think an e-mail message is a **phishing** scam.
- **"Verify your account."** Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail. If you receive an e-mail from anyone asking you to update your credit card information, do not respond: this is a **phishing** scam.
- **"If you don't respond within 48 hours, your account will be closed."** These messages convey a sense of urgency so that you'll respond immediately without thinking. **Phishing** e-mail might even claim that your response is required because your account might have been compromised.

How To Tell If An E-mail Message is Fraudulent (cont'd)

- **"Dear Valued Customer."** **Phishing** e-mail messages are usually sent out in bulk and often do not contain your first or last name.
- **"Click the link below to gain access to your account."** HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site.
The links that you are urged to click may contain all or part of a real company's name and are usually **"masked,"** meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site.

-

How to Tell If An E-mail Message is Fraudulent (cont'd)



- **Con artists** also use Uniform Resource Locators (**URLs**) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters.
- For example, the URL "www.microsoft.com" could appear instead as:
 - www.mi**c**osoft.com
 - www.mir**c**osoft.com
 - www.**verify**-microsoft.com



- Never respond to an email asking for personal information
- Always check the site to see if it is secure. Call the phone number if necessary
- Never click on the link on the email. Retype the address in a new window
- Keep your browser updated
- Keep antivirus definitions updated
- Use a firewall

DoS attack



- It is also known as “network saturation attack” or “bandwidth consumption attack”.
- Attackers make Denial-of-Service attacks by sending a large number of protocol packets to a network.

Consequences of DoS

- Saturate network resources.
- Disrupt connections between two computers, thereby preventing communication between services.
- Disrupt services to a specific computer.

Common DoS Attacks

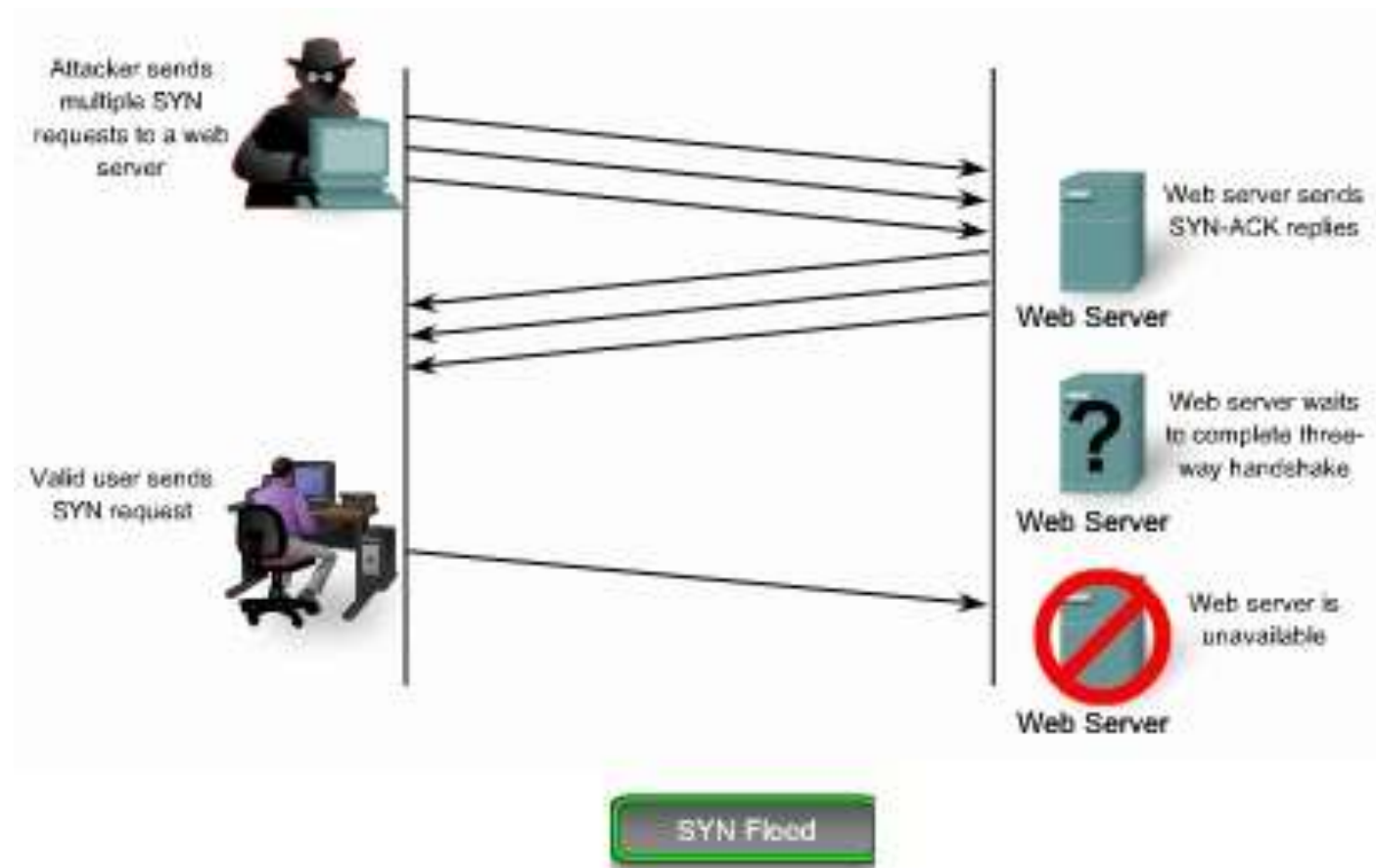
1. SYN attack
2. PING flood
3. Ping of death
4. Teardrop attack
5. Smurf attack



SYN attack/SYN flooding

- A SYN attack affects computers running on the TCP/IP protocol.
- an attacker sends multiple SYN packets to the target computer.
- For each SYN packet received, the target computer allocates resources and sends an acknowledgement (SYN-ACK) to the source IP address. Since the target computer does not receive a response from the attacking computer, it attempts to resend the SYN-ACK.
- This leaves TCP ports in a half-open state. When an attacker sends TCP SYNs repeatedly, the target computer eventually runs out of resources and is unable to handle any more connections, thereby denying services to legitimate users.




Diagram showins SYN flood
















PING flood

- It relies on the ICMP echo command, more popularly known as ping .
- In legitimate situations the ping command is used by network administrators to test connectivity between two computers.
- In the **ping flood** attack, it is used to flood large amounts of data packets to the victim's computer in an attempt to overload it.

Ping flood (contd..)

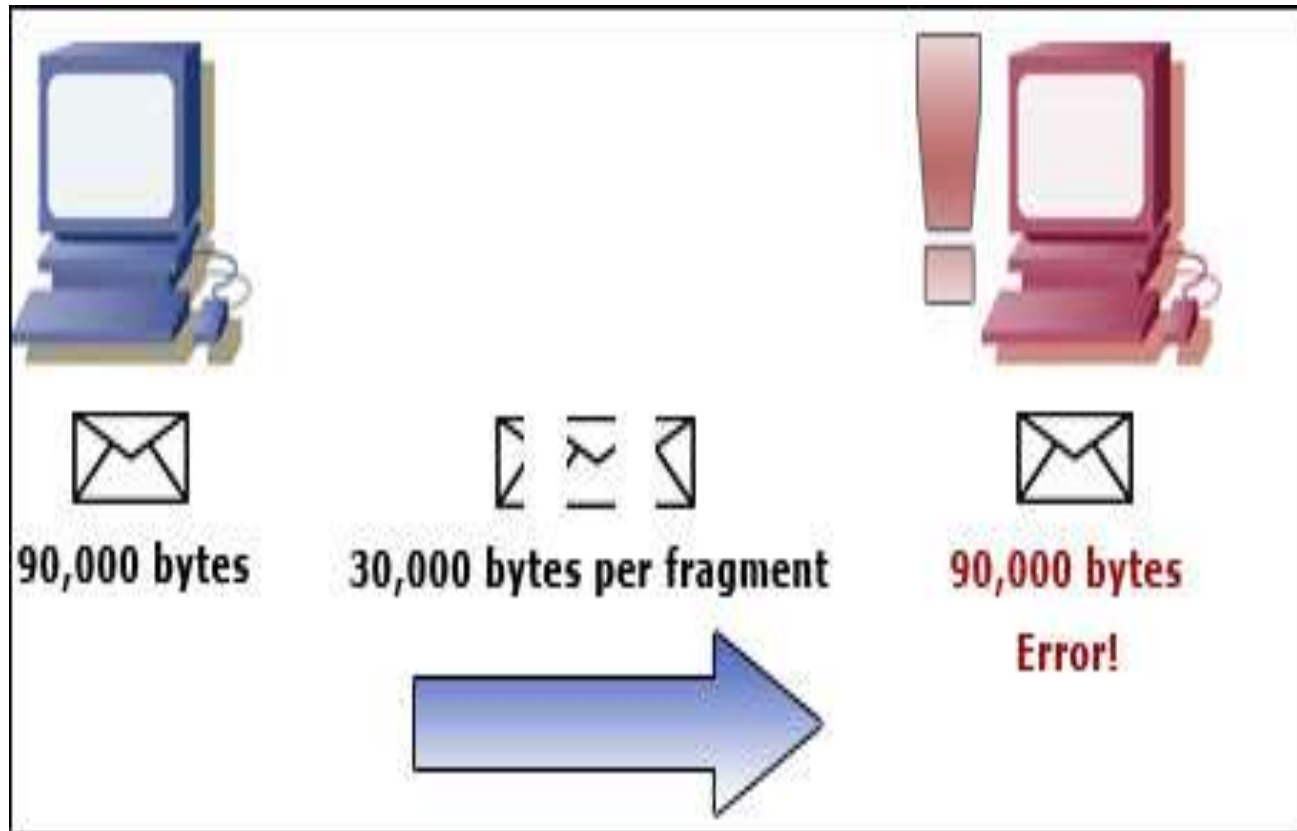
Statistics Conversations Events Logs					
<div>   ▼</div>					
Statistics Item				Statistics Data	
UDP					
[-] ICMP				Count	
ICMP_PING Windows				149	
ICMP_Ping				149	
FTP_CTRL					

<div>   ▼   </div>					
Severity	Time	Protocol	Event	Source	Destinations
	19:53:41	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:42	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:43	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:44	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:45	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:46	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147
	19:53:47	ICMP	ICMP_Ping	192.168.1.100	64.233.189.147

Ping of death

- The maximum size for a packet is 65,535 bytes. If one were to send a packet larger than that, the receiving computer would ultimately crash from confusion.
- Sending a ping of this size is against the rules of the TCP/IP protocol, but hackers can bypass this by cleverly sending the packets in fragments. When the fragments are assembled on the receiving computer, the overall packet size is too great. This will cause a buffer overflow and crash the device.

Ping of death



Software to ping attack



Download Link:-

<http://www.softpedia.com/progScreenshots/AtTacK-PiNG-Screenshot-80794.html>

Teardrop attack

- Teardrop attacks exploit the reassembly of fragmented IP packets. Fragment offset indicates the starting position of the data contained in a fragmented packet relative to the data of the original unfragmented packet.

The router checks for discrepancies in the fragment offset field.

IP Header

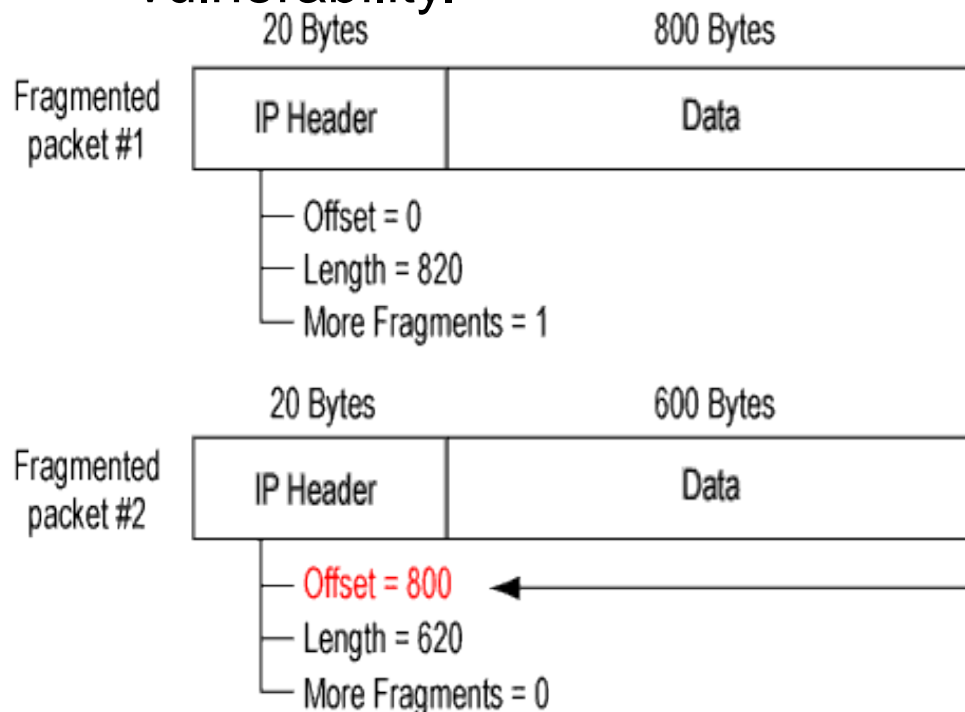
Version	Header Length	Type of service	Total Packet Length (in Bytes)			
Identification			x	D	M	Fragment Offset
Time to Live (TTL)	Protocol		Header Checksum			
Source Address						
Destination Address						
Options (if any)						
Payload						

20 Bytes

Image 33

Teardrop attack(contd..)

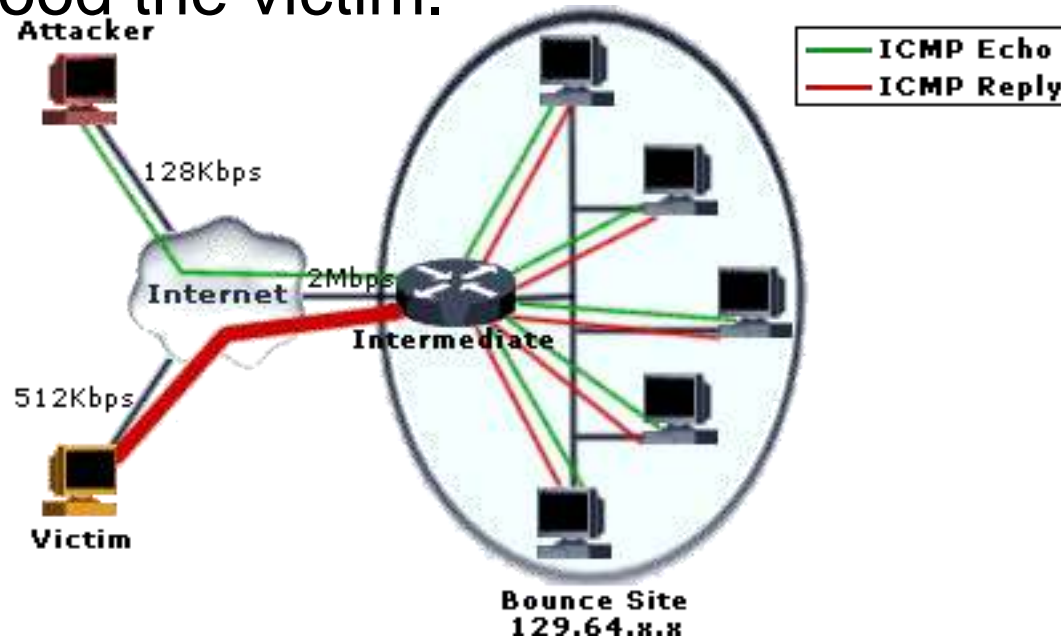
- When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash, especially if it is running an older operating system that has this vulnerability.



The second fragment purports to begin 20 bytes earlier (at 800) than the first fragment ends (at 820). The offset of fragment #2 is not in accord with the packet length of fragment #1. This discrepancy can cause some systems to crash during the reassembly attempt.

Smurf attack

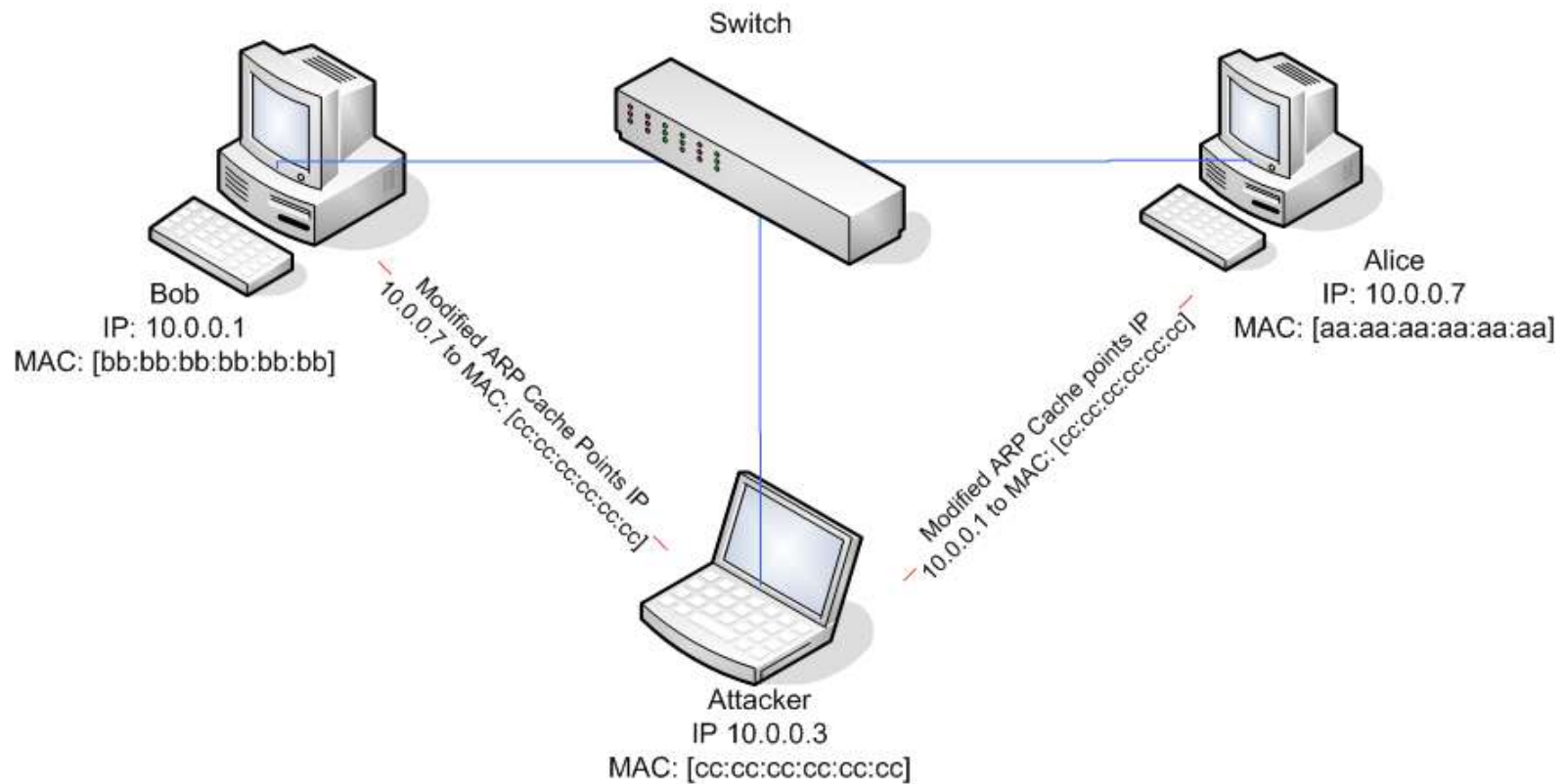
- The attacker sends a large amount of ICMP traffic to a broadcast address and uses a victim's IP address as the source IP so the replies from all the devices that respond to the broadcast address will flood the victim.



Spoofing

- Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address.
- In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity.

Spoofing(contd..)



PART -III

MALWARES

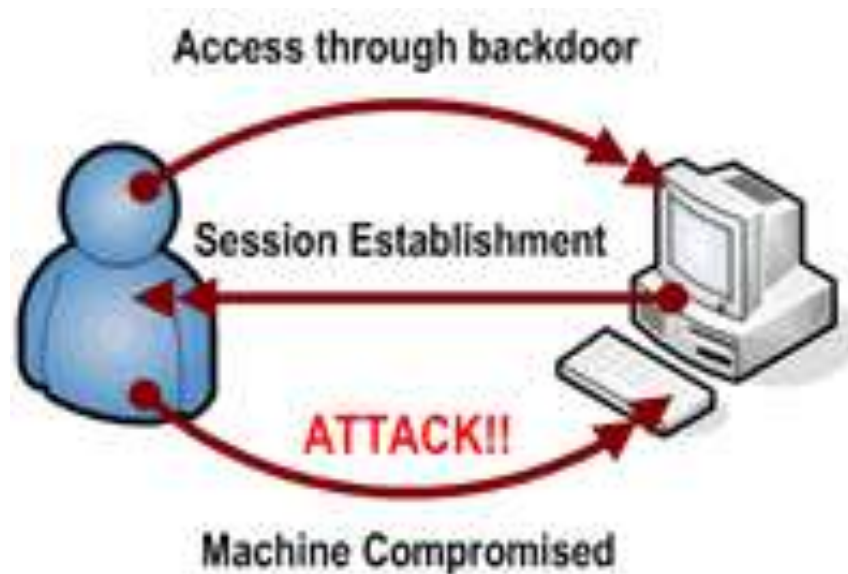


By Manohar
Mantry

Back Door

- Back door is a program or account that allows access to a system by skipping the security checks.
- Many vendors and developers implement back doors to save time and effort by skipping the security checks while troubleshooting.
- Back door is considered to be a security threat and should be kept with the highest security.
- If a back door becomes known to attackers and malicious users, they can use it to exploit the system.

Backdoor is a secret or unauthorized channel for accessing computer system. In an attack scenario, hackers install backdoors on a machine, once compromised, to access it in an easier manner at later times



Virus

- Definition
 - A virus is a small piece of software that piggybacks on real programs in order to get executed
 - Once it's running, it spreads by inserting copies of itself into other executable code or documents

Computer Virus Timeline

- **1949**

Theories for self-replicating programs are first developed.-John von Newmann.

- **1981**

Apple Viruses 1, 2, and 3 are some of the first viruses “in the world,” or in the public domain. Found on the Apple II operating system, the viruses spread through Texas A&M via pirated computer games.

- **1983**

Fred Cohen, while working on his dissertation, formally defines a computer virus as “a computer program that can affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself.”

- **1986**

Two programmers named Basit and Amjad replace the executable code in the boot sector of a floppy disk with their own code designed to infect each 360kb floppy accessed on any drive. Infected floppies had “© Brain” for a volume label.

- **1987**

The Lehigh virus, one of the first file viruses, infects command.com files.


- **1988**

One of the most common viruses, Jerusalem, is unleashed. Activated every Friday the 13th, the virus affects both .exe and .com files and deletes any programs run on that day. MacMag and the Scores virus cause the first major Macintosh outbreaks.

- ...


General virus types

- While there are thousands of variations of viruses, most fall into one of following general categories, each of which works slightly differently.
 1. Boot sector virus
 2. Macro virus
 3. Multipartite virus
 4. Polymorphic virus
 5. Stealth virus
 6. E-mail viruses



Boot Virus : Replaces or implants itself in the boot sector. This kind of virus can prevent you from being able to boot your hard disk.

Macro Virus : Written using a simple macro programming language, these viruses affect Microsoft Office applications such as Word and Excel. A document infected with a macro virus generally modifies a pre-existing, common command (such as save) to trigger to trigger its payload upon execution of that command.



Multiparatite Virus :Infects both files and boot sector--a double whammy that can reinfect your system dozen times before it's caught.

Polymorphic Virus :

Changes code whenever it passes to another machine



Stealth Virus:

Hides in presence by making an infected

file not appear infected.

E-mail Virus :

An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself dozens of people in victims e-mail address book.

Case study-Melissa Virus

- March 1999
- the Melissa virus was the fastest-spreading virus ever seen
- Someone created the virus as a Word document uploaded to an Internet newsgroup
- People who downloaded the document and opened it would trigger the virus
- The virus would then send the document in an e-mail message to the first 50 people in the person's address book

Case study-Melissa Virus

- Took advantage of the programming language built into Microsoft Word called VBA (Visual Basic for Applications)

Prevention

- Updates
- Anti-Viruses
- More secure operating systems
e.g. UNIX

Worms

- **Worm** – A worm is a computer program that has ability to copy itself from machine to machine. Worms normally move around and infect other machines through computer networks. Worms eat up storage space and slows down the computer. But worms don't alter or delete files.

Trojan horses

- A Trojan horse is simply a computer program that claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk).
- When loaded onto your machine, a Trojan horse can capture information from your system.

Trojan horses(contd..)

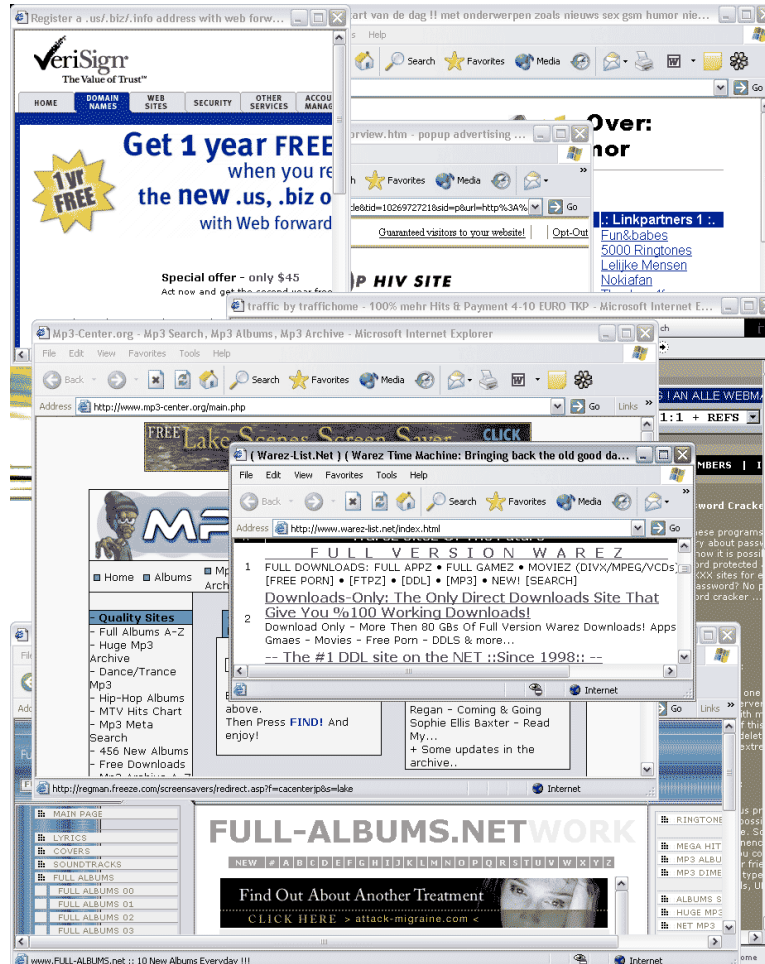
- It allows a malicious hacker to remotely control your computer.
- Trojan horse has no way to replicate automatically.

What is Spyware ?



- **Spyware** is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.

What is Adware?

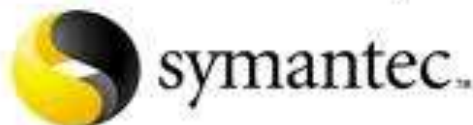


- Adware are created by advertising companies
- Comes in the form of popups, unexplained advertising programs on your computer desktop like “Casino Night”.
- Advertising companies hope to generate money from customers who receive the popups or unexplained programs on their computers.
- Also a LEGAL program!

Conclusion



- Always use Anti-virus software.
- Scan external devices when connected to computer.
- Enable firewall.
- Read carefully and then click a link.



Queries???

Silver Partner



F-Secure®



NOD32
Antivirus System



FARONICS™



Norton
AntiVirus™



ANSAP