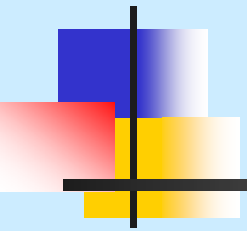
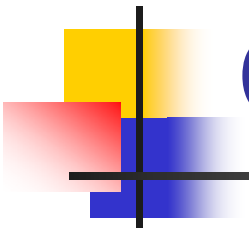


Chapter 2: Attackers and Their Attacks

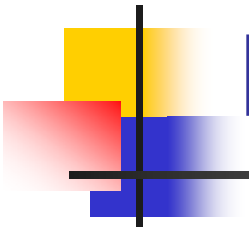


OBJECTIVES

- Develop attacker profiles
- Describe basic attacks
- Describe identity attacks
- Identify denial of service attacks
- Define malicious code (malware)

Developing Attacker Profiles

- Six categories:
  - Hackers
  - Crackers
  - Script kiddies
  - Spies
  - Employees
  - Cyberterrorists

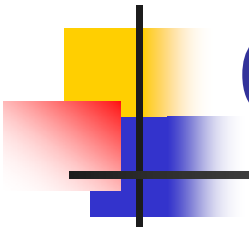


Hackers

- “An individual who breaks into computers”
- Person who uses advanced computer skills to attack computers, but not with a malicious intent
- Use their skills to expose security flaws

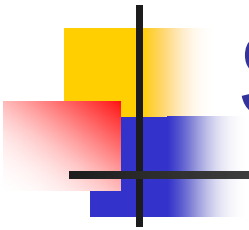
Hacker profile

- Male
- Age between 16 and 35
- Loner
- Intelligent
- Technically proficient



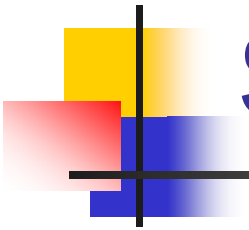
Crackers

- Person who violates system security with malicious intent
- Have advanced knowledge of computers and networks and the skills to exploit them
- Destroy data, deny legitimate users of service, or otherwise cause serious problems on computers and networks



Script Kiddies

- Break into computers to create damage
- Are unskilled users
- Download automated hacking software from Web sites and use it to break into computers
- Tend to be young computer users with almost unlimited amounts of leisure time, which they can use to attack systems



Spies

- Person hired to break into a computer and steal information
- Do not randomly search for unsecured computers to attack
- Hired to attack a specific computer that contains sensitive information

Employees

- One of the largest information security threats to business
- Employees break into their company's computer for these reasons:
  - To show the company a weakness in their security
  - To say, "I'm smarter than all of you"
  - For money
  - A dissatisfied employee wanting to get back at the company.

Cyberterrorists

- Experts fear terrorists will attack the network and computer infrastructure to cause panic
- Cyberterrorists' motivation may be defined as ideology, or attacking for the sake of their principles or beliefs
- One of the targets highest on the list of cyberterrorists is the Internet itself

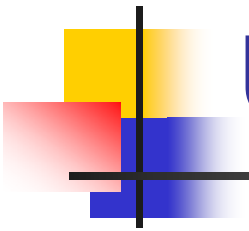
Cyberterrorists (cont.)

- Three goals of a cyberattack:
  - Deface electronic information to spread disinformation and propaganda
  - Deny service to legitimate computer users
  - Commit unauthorized intrusions into systems and networks that result in critical infrastructure outages and corruption of vital data

Developing Attacker Profiles Summary

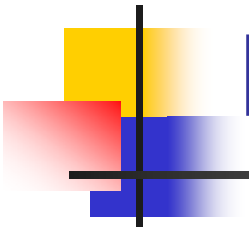
Table 1 Attacker profiles

Attacker	Skill Level	Motivation
Hacker	High	Improve security
Cracker	High	Harm systems
Script kiddie	Low	Gain recognition
Spy	High	Earn money
Employee	Varies	Varies
Cyberterrorist	High	Support ideology



Understanding Basic Attacks

- Today, the global computing infrastructure is most likely target of attacks
- Attackers are becoming more sophisticated, moving away from searching for bugs in specific software applications toward probing the underlying software and hardware infrastructure itself



Main Goals of Attacks

Regardless of how they occur , attacks try to accomplish one or more of the following goals:

- In an *access attack*, someone who should not be able to, wants to access your resources
- During a *modification or repudiation attack*, someone wants to modify information in your system
- A *denial-of-service (DoS) attack* tries to disrupt your network and services.

General Categories of Attacks

Category	Attack on:
Interruption	availability
Interception	confidentiality
Modification	Integrity
Fabrication	authenticity

Classification of Attacks

- Passive :
  - Eavesdropping on, or monitoring of transmission
  - Release of message content (disclosure) ..hence use encryption to mask the message content.
  - Traffic analysis....the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messaging being exchanged. This could be very useful

Classification of Attacks (cont.)

- Active :
  - Masquerade : an entity pretends to be a different entity
  - Replay : The passive capture of data and its subsequent retransmission to produce unauthorized effects
  - Modification of messages :some portions of a legitimate message are modified
  - Denial of service : prevents or inhibits the normal use of communications facilities.

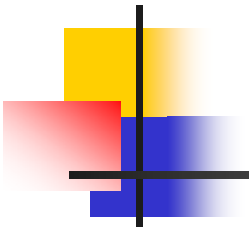
Types of Access Attacks

- Piggybacking and shoulder surfing.
- Dumpster diving : is a common physical access method
- Eavesdropping : is the process of listening in on or overhearing parts of conversations. It also includes attackers listening in on your network traffic.

Types of Access Attacks (cont.)

- Snooping : occurs when someone looks thru your files...either paper or electronic
- Interception : can be active or passive. Active might include putting a computer between sender and receiver to capture information as it is sent. Passive interception involves someone who routinely monitors network traffic.

  e.g. Government agencies routinely run intercept missions to gather intelligence .The FBI has several products that they install on ISPs to gather and process e-mail looking for keywords. These become the basis of an investigation.



Sniffing Threats

- In a network there may be several intermediate nodes (bridges, routers, gateways). Each of these reads incoming traffic and decides where to forward it to.
- Many of these nodes include S/W components. This creates an opportunity to run rogue *sniffer S/W* that reads incoming traffic and forwards sensitive information to the attacker.
- Similarly, information gleaned from network management protocols that collect diagnostics about the load and availability of nodes can be regarded to be sensitive.

Spoofing Threats

- Other threats in networks, comes from forged source address (spoofing),
- from entities denying their involvement in a transaction they had participated in,
- or from traffic flow analysis , where an attacker gains information just from the fact that two entities are exchanging messages.

Recognizing Modification and Repudiation Attacks

- Modification attacks involve the deletion, insertion, or alteration of information in an unauthorized manner that is intended to appear genuine to the user.
- These attacks can be very hard to detect.
- Website defacements are a common form.

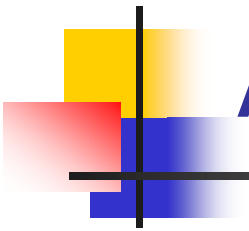
Recognizing Repudiation Attacks

- Repudiation attacks make data or information appear to be invalid or misleading.
- e.g. someone might access your e-mail server and send inflammatory information to others under the guise of one of your top managers !!!
- These attacks are fairly easy to accomplish because e-mail systems don’t check outbound mail for validity.
- Repudiation attacks, like modification attacks, usually begin as access attacks.

Denial of Service (DoS) Attacks

- DoS attacks prevent access to resources by users authorized to use those resources.
- DoS attacks are not only on the Internet, Physical DoS attacks do exist and can be as devastating than cyber DoS attacks. (a pair of wire cutters!!)
- DoS attacks on the Internet, where they have hit large companies such as Amazon, Microsoft, and AT&T.
- Most DoS attacks occur from a single system mostly from spoofed (fake) addresses, and a specific server or organization is the target.
- In a DoS attack the servers are so busy responding to false requests that they don't have time to service legitimate requests.
- The same result can occur if the attack consumes all the available bandwidth.

Identifying Denial of Service Attacks



- Denial of service (DoS) attack attempts to make a server or other network device unavailable by flooding it with requests
- After a short time, the server runs out of resources and can no longer function
- Known as a SYN attack because it exploits the SYN/ACK “handshake”

Identifying Denial of Service Attacks (cont.)

- Another DoS attack tricks computers into responding to a false request
- An attacker can send a request to all computers on the network making it appear a server is asking for a response. E.g. A PING using the ICMP protocol
- Each computer then responds to the server, overwhelming it, and causing the server to crash or be unavailable to legitimate users

Identifying Denial of Service Attacks (cont.)

- Distributed denial-of-service (DDoS) attack:
  - Instead of using one computer, a DDoS may use hundreds or thousands of computers
  - DDoS works in stages

Identifying Denial of Service Attacks (cont.)

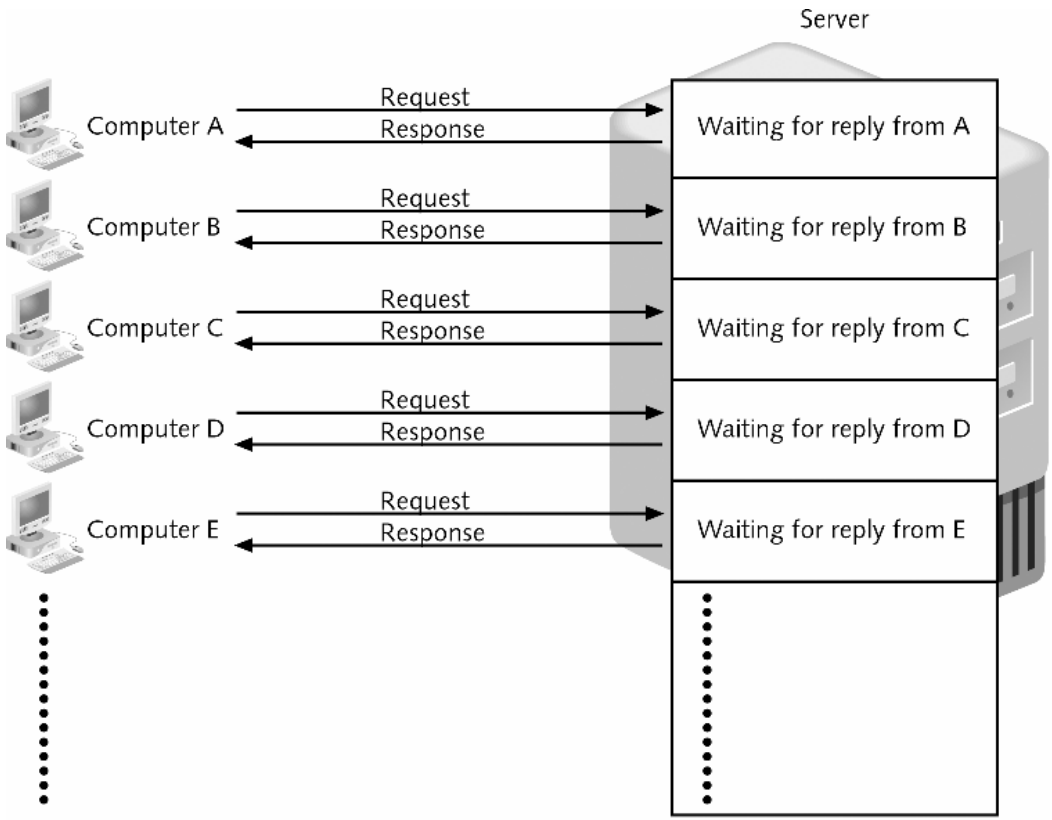
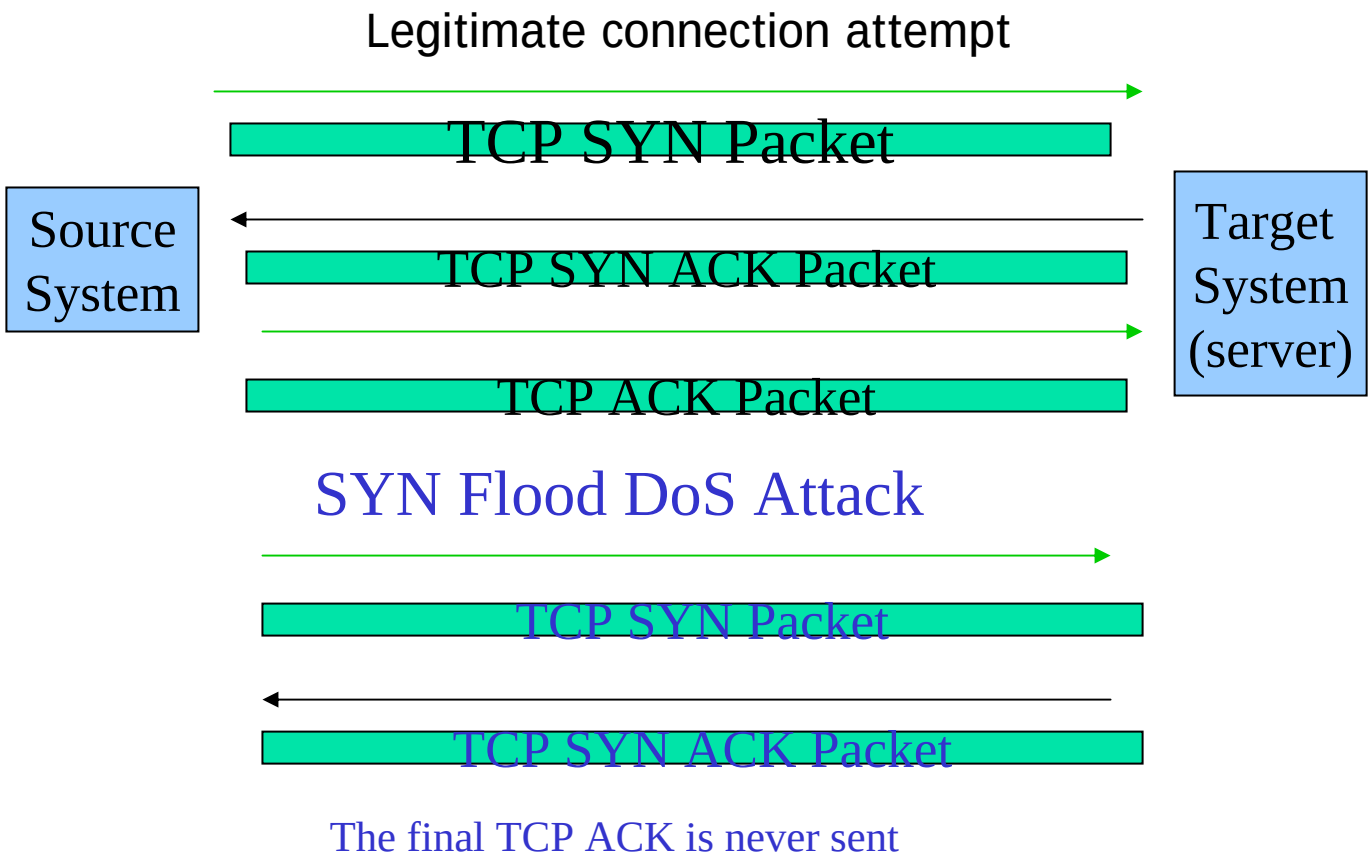


Figure 1 Server waiting for response

Single Source DoS Attacks

- The most widely known DoS attack is called SYN flood.
- In this attack, the source system sends a large number of TCP SYN packets to the target system. (The SYN packets are used to begin a new TCP connection).
- The target's pending connection buffer fills up and it can no longer respond to new connection requests.
- If the SYN flood comes from a legitimate IP address, it is relatively easy to identify the source and stop the attack. But if the source is a non-routable address like 192.168.x.x it becomes much more difficult. (impossible)
- The easiest solution is to put a timer on all pending connections and have them expire after a time. (!!!)
- Several network devices have the capability to identify SYN floods and block them.

SYN Flood DoS Attack

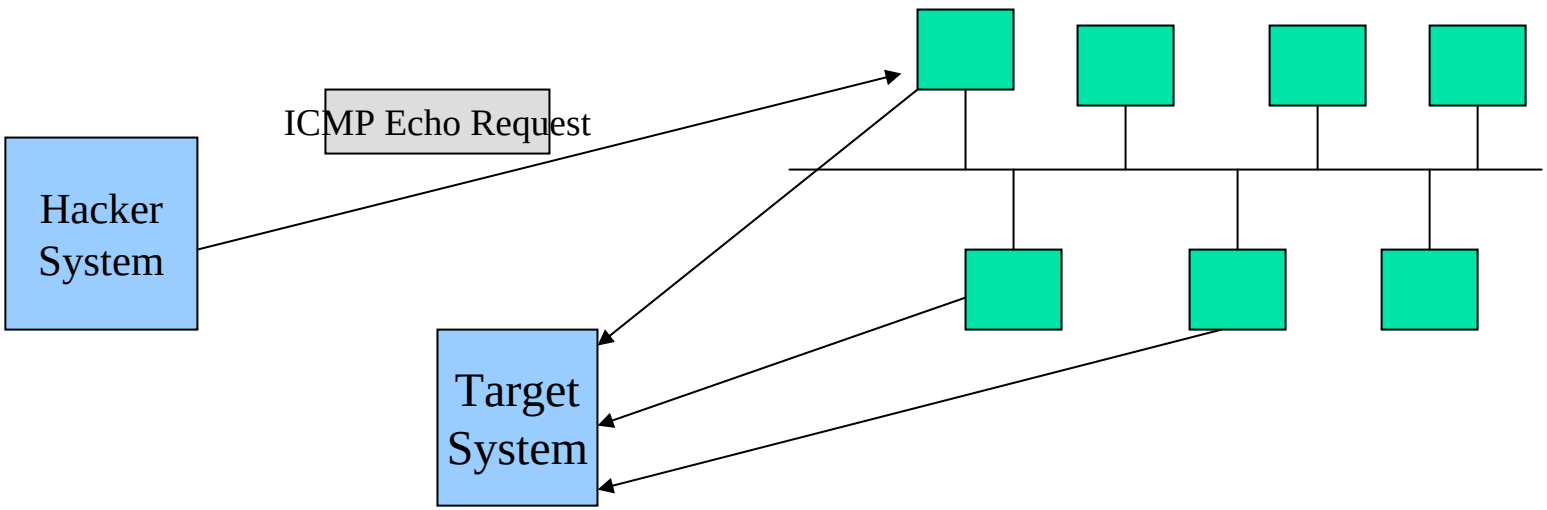


Another Common Type of DoS Attack

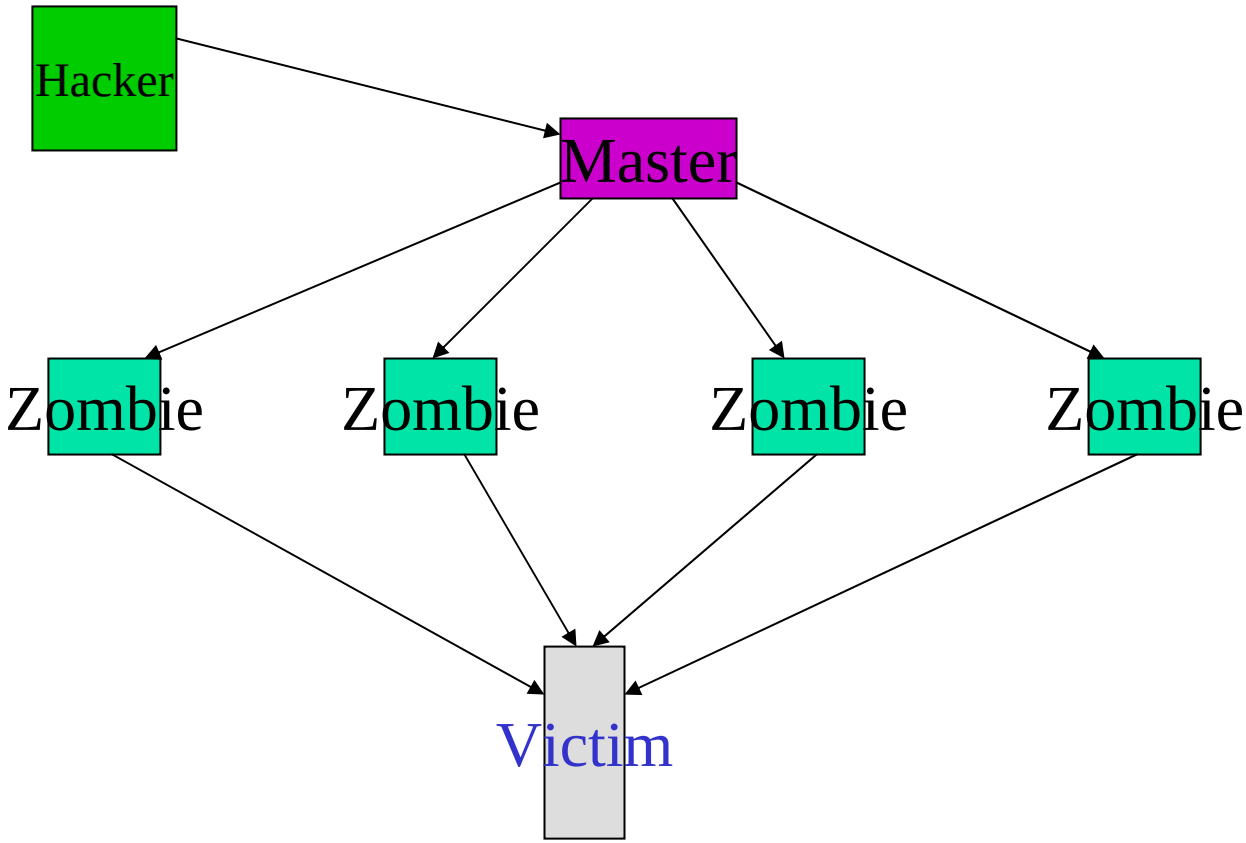
- Ping of Death
- This crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
- Normally a Ping packet does not contain any data. The Ping of Death packet contained a large amount of data.
- When this data is read by the target system, the system would crash due to buffer overflow in the protocol stack.
- This problem was quickly patched after it was identified and few systems are vulnerable today.
- Unfortunately, new DoS attacks against applications and operating systems are identified on a regular basis.

Distributed DoS (DDoS)

- Smurf Attack：This can be as simple as a hacker sending a ping packet to the broadcast address of a large network while spoofing the source address to direct all the responses at a target.



Distributed DoS Attacks



Programming Flaw

- This includes such things as leaving a back door in a program for later access to the system.
- E.g. a tool to be used while debugging the program.
- Hackers have identified most of the known back doors and, in turn, programmers have fixed them.
- Some of these backdoors still exist because the software in question has not been updated on systems where it is running.
- The boom in Web site programming has created a new category of unwise programming. In online shopping, information on what you are buying is kept in the URL string itself.(item number, quantity ,price). This information is used by the Web site to determine how much to charge your credit card. Many of those sites do not verify the information when the item is ordered.

Buffer Overflow BO

- BO is one type of programming flaw exploited by hackers
- BOs are harder to find than bad passwords or configuration mistakes.
- BOs are especially nasty because they tend to allow hackers to run any command they wish on the target system
- Most BO scripts allow hackers to create another means of accessing the target system
- BOs are not restricted to accessing remote systems. There are several BOs that allow users on a system to upgrade their access level.
- Buffer overflow attack examples

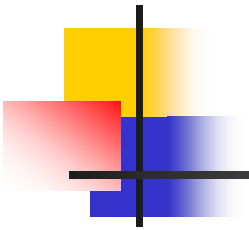
  E.g. Code Red, Slapper, Slammer

What is Buffer Overflow ?

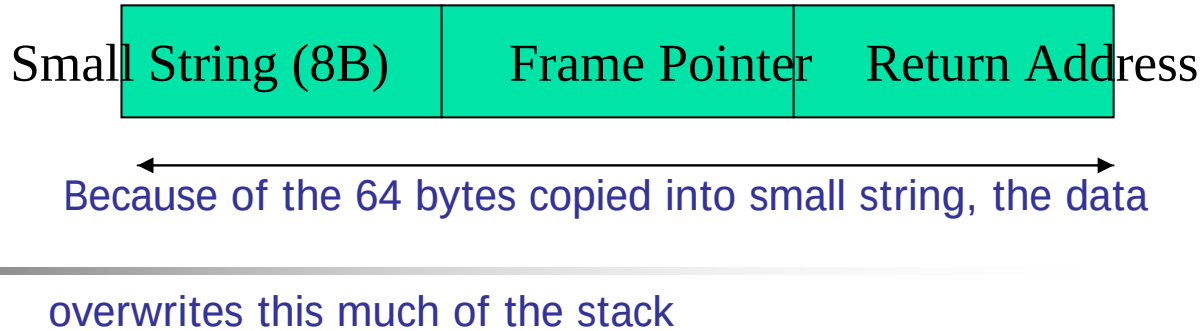
- Simply BO is an attempt to stuff too much information into a space in a computer's memory.
- For instance, if I create a variable that is 8 bytes long and I try to stuff 9 bytes into it....the 9^{th} byte is placed immediately following the 8^{th} byte.
- If I stuff a lot of extra data into that variable, eventually I will run into the Stack , and in particular, the return address of the function to be executed next.
- The stack controls switching between programs and also stores the local variables to a function.

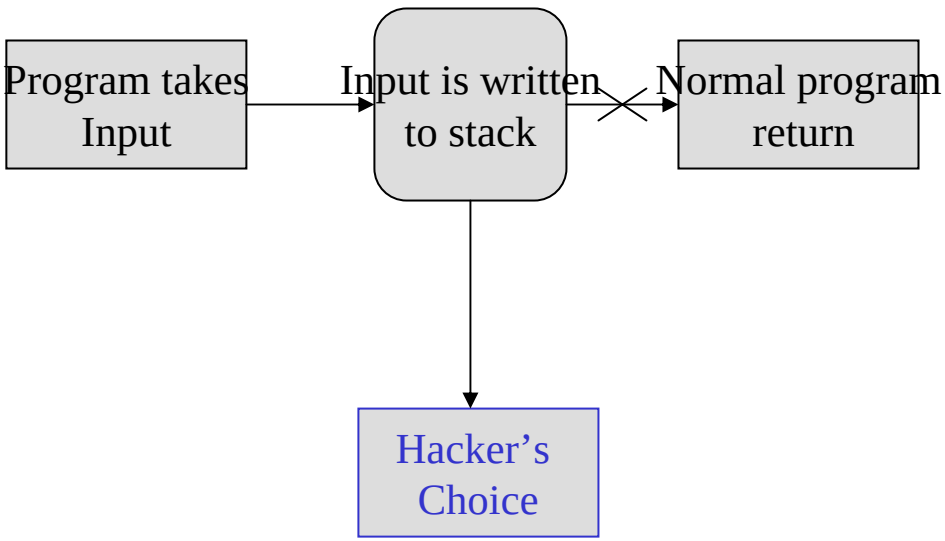
What is Buffer Overflow ?(cont.)

- In some cases, when a BO is exploited, the hacker places instructions in a local variable that is then stored on the stack.
- The information placed in the local variable is large enough to place an instruction on the stack and overwrite the return address to point to this instruction.
- These instructions may cause another application to start, or change a configuration file to allow hacker access.



How Buffer Overflow Works





- If an appropriate string were provided, the return address could be pointed at a command to perform.
- Why do BOs exist?

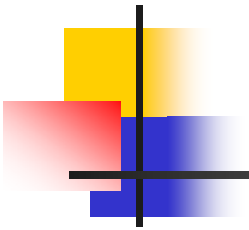
The flaw in an application that copies user data into another variable without checking the amount of data copied.

Note: many of the string copying fns in C do not perform size checking.

There are some automated scripts that can be used to examine code before it is compiled to identify BOs.

Sniffing Switched Networks

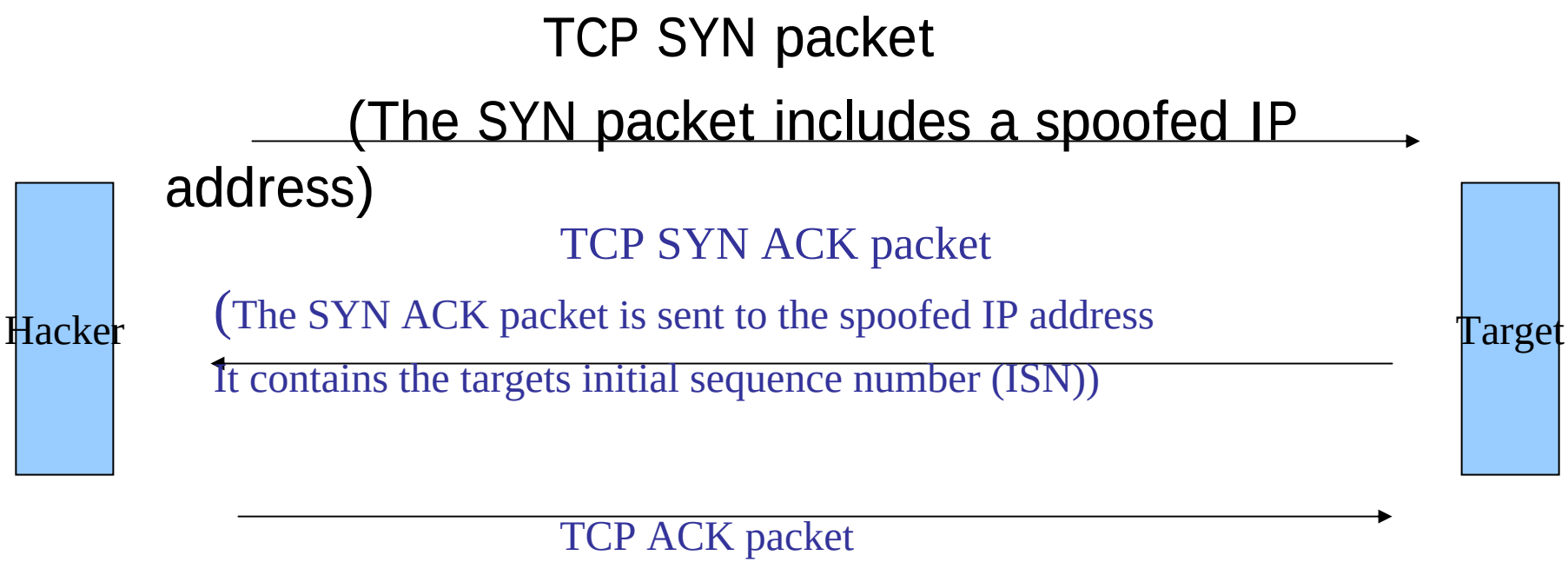
- Sniffers have been used by hackers/crackers to gather passwords and other information from networks by placing a NIC into promiscuous mode on shared media networks (using hubs).
- For a switched network, the hacker must do one of two things :
  - Convince the switch that the traffic of interest should be directed to the sniffer (redirecting traffic)
  - Cause the switch to send all traffic to all ports. This can occur if the memory is full. The attacker must be directly attached to the switch in question.



IP Spoofing

- There is no validation of the IP address in a packet, therefore a hacker could modify the source address of the packet and make the packet appear to come from anywhere !

Details of IP Spoofing



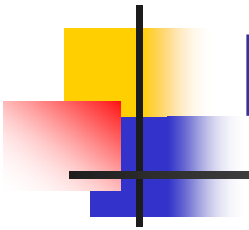
The hacker must craft the final ACK packet to acknowledge the target's ISN in the SYN ACK packet to complete the connection)

Redirecting Traffic

- ARP Spoofing : the sniffer responds to the ARP request before the real system and provide its own MAC address. The sending system will then send all its traffic to the sniffer.
- In order for ARP spoofing to be effective, the sniffer must have the capability to forward all traffic on to the correct destination, otherwise instead of sniffing the sniffer will cause a DoS on the network.
- Another form of ARP spoofing is for the hacker to change the ARP address table so that packets are redirected to his computer instead of to a valid computer (p.45)
- ARP spoofing only works on the local network.

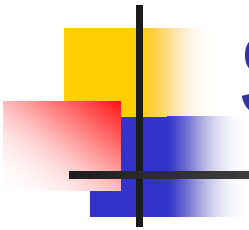
MAC Duplicating

- To convince the switch to send traffic to the sniffer, the sniffer duplicates the MAC address of the target system.
- Utilities are available to change the MAC address on Windows systems.
- For ARP spoofing to work, the sniffer must be on the same local subnet as either the sender or duplicate system.



DNS Spoofing

- To fool the sending system into sending traffic to the sniffer using the sniffer's correct MAC address.
- The sniffer sends replies to DNS requests to the sending system. The replies provide the sniffer's IP address as the address of whatever system is being requested.
- The sender can now ARP the sniffer's IP address.
- This will cause the sending system to send all traffiv to the sniffer.
- The sniffer must then forward all traffic to the real destination.
- For DNS spoofing to be possible, the sniffer must be in the network path from the sending system to the DNS server if not on the local subnet with the sending system.

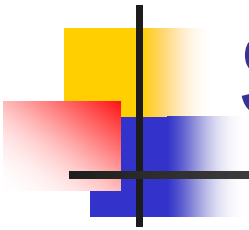


Social Engineering

- The best computer security practices are easily subverted by bad human practices
  - E.g. giving passwords out over the phone to anyone who asks
- Social engineering attacks tend to be cheap, easy, effective
- Easiest way to attack a computer system requires almost no technical ability and is usually highly successful
- Social engineering relies on tricking and deceiving someone to access a system
- Social engineering is not limited to telephone calls or dated credentials

Social Engineering (cont.)

- Dumpster diving: digging through trash receptacles to find computer manuals, printouts, or password lists that have been thrown away
- Phishing: sending people electronic requests for information that appear to come from a valid source

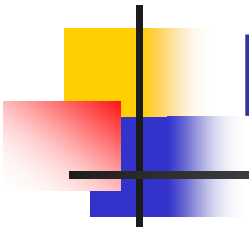


Social Engineering (cont.)

- Phishing
  - Attackers send plausible email requesting you to visit a web site
  - To “update” your information
  - Typically a bank, popular web site, etc.
  - The attacker controls the site and uses it to obtain your credit card, SSN, etc.
  - Likelihood of success based on attacker’s ability to convince the victim that he’s real and that the victim had better go to the site or suffer dire consequences

Social Engineering (continued)

- Develop strong instructions or company policies regarding:
  - When passwords are given out
  - Who can enter the premises
  - What to do when asked questions by another employee that may reveal protected information
- Educate all employees about the policies and ensure that these policies are followed

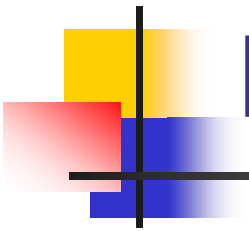


Password Guessing

- Password: secret combination of letters and numbers that validates or authenticates a user
- Passwords are used with usernames to log on to a system using a dialog box
- Attackers attempt to exploit weak passwords by password guessing

Password Guessing (cont.)

Figure 2 Username and password



Password Guessing (cont.)

- Characteristics of weak passwords:
  - Using a short password (XYZ)
  - Using a common word (blue)
  - Using personal information (name of a pet)
  - Using same password for all accounts
  - Writing the password down and leaving it under the mouse pad or keyboard
  - Not changing passwords unless forced to do so

Password Guessing (cont.)

- Brute force: attacker attempts to create every possible password combination by changing one character at a time, using each newly generated password to access the system
- Dictionary attack: takes each word from a dictionary and encodes it (hashing) in the same way the computer encodes a user's password

Password Guessing (cont.)

- Software exploitation: takes advantage of any weakness in software to bypass security requiring a password
  - Buffer overflow: occurs when a computer program attempts to stuff more data into a temporary storage area than it can hold

Password Guessing (cont.)

- Policies to minimize password-guessing attacks:
  - Passwords must have at least eight characters
  - Passwords must contain a combination of letters, numbers, and special characters
  - Passwords should expire at least every 30 days
  - Passwords cannot be reused for 12 months
  - The same password should not be duplicated and used on two or more systems

Are there Good Alternatives to Passwords?

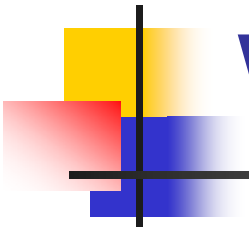
- Smart Cards
- Biometrics

In both cases an organization that deploys them will incur extra costs.

Also, they are not appropriate for every situation : e.g. an online retailer trying to use biometrics to authenticate customers!!!

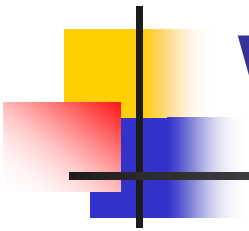
Passwords are likely to be with us for the foreseeable future.

The best defense against weak passwords is good security awareness training for employees.



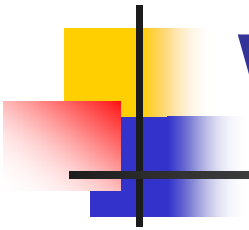
Weak Keys

- Cryptography:
  - Science of transforming information so it is secure while being transmitted or stored
  - Does not attempt to hide existence of data; “scrambles” data so it cannot be viewed by unauthorized users



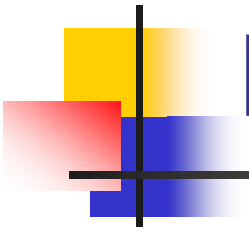
Weak Keys (cont.)

- Encryption: changing the original text to a secret message using cryptography
- Success of cryptography depends on the process used to encrypt and decrypt messages
- Process is based on algorithms



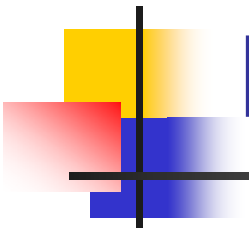
Weak Keys (cont.)

- Algorithm is given a key that it uses to encrypt the message
- Any mathematical key that creates a detectable pattern or structure (weak keys) provides an attacker with valuable information to break the encryption



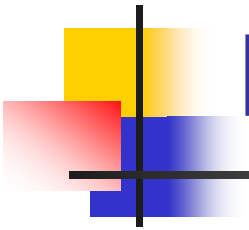
Mathematical Attacks

- Cryptanalysis: process of attempting to break an encrypted message
- Mathematical attack: analyzes characters in an encrypted text to discover the keys and decrypt the data



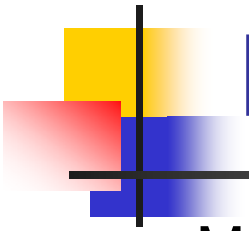
Birthday Attacks

- Birthday paradox:
  - When you meet someone for the first time, you have a 1 in 365 chance (0.027%) that he has the same birthday as you
  - If you meet 60 people, the probability leaps to over 99% that you will share the same birthday with one of these people
- Birthday attack: attack on a cryptographical system that exploits the mathematics underlying the birthday paradox



Examining Identity Attacks

- Category of attacks in which the attacker attempts to assume the identity of a valid user

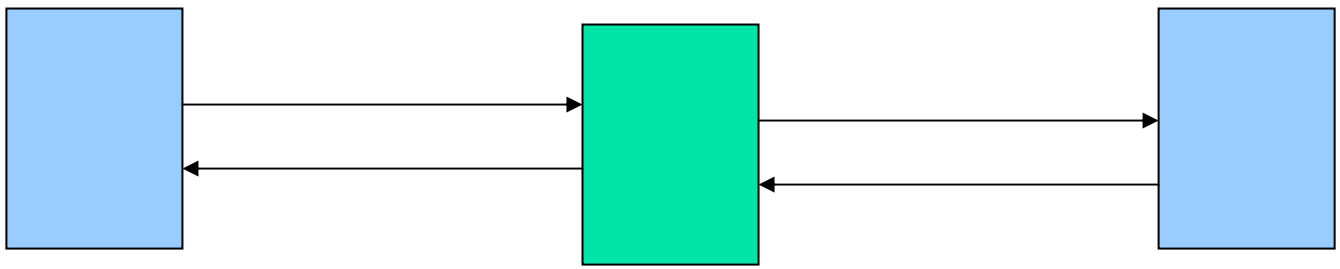


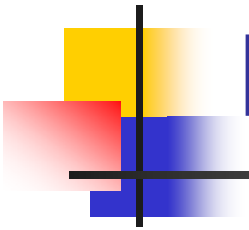
Man-in-the-Middle Attacks

- Make it seem that two computers are communicating with each other, when actually they are sending and receiving data with a computer between them
- Can be active or passive:
  - Passive attack: attacker captures sensitive data being transmitted and sends it to the original recipient without his presence being detected
  - Active attack: contents of the message are intercepted and altered before being sent on

Man-in-the-Middle Attacks

Computer A	Man-in-the-middle	Computer B
Computer A thinks	Intercepts the	Computer B thinks
It is talking to B	conversation	It is talking to A





Replay Attacks

- Similar to an active man-in-the-middle attack
- Whereas an active man-in-the-middle attack changes the contents of a message before sending it on, a replay attack only captures the message and then sends it again later
- Takes advantage of communications between a network device and a file server

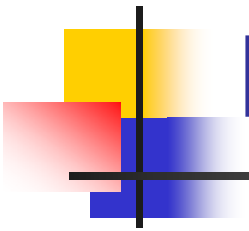
TCP/IP Hijacking

- With wired networks, TCP/IP hijacking uses spoofing, which is the act of pretending to be the legitimate owner
- One particular type of spoofing is Address Resolution Protocol (ARP) spoofing
- In ARP spoofing, each computer using TCP/IP must have a unique IP address

TCP/IP Hijacking (cont.)

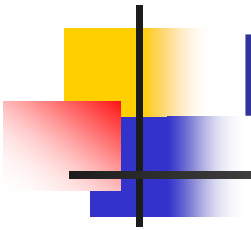
- Certain types of local area networks (LANs), such as Ethernet, must also have another address, called the media access control (MAC) address, to move information around the network
- Computers on a network keep a table that links an IP address with the corresponding address
- In ARP spoofing, a hacker changes the table so packets are redirected to his computer

Understanding Software Exploitation



- Database Exploitation…if a client session can be spoofed, the attacker can formulate queries against the database that disclose information
- Application Exploitation...The macro virus is an example
- E-mail Exploitation... A popular exploitation of e-mail clients involves accessing the client address book and propagating viruses

Understanding Software Exploitation (cont)

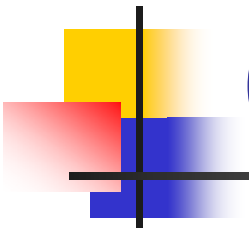


- Spyware ...differs from malware in that it works-often actively – on behalf of a third party.
- Rather than self replicating, like viruses and worms, it spreads to other machines by users who inadvertently do so, by downloading other programs, visiting infected sites, etc
- The spyware monitors user's activity and responds to them by offering unsolicited pop-up ads (adware), gathers information about them to pass on to the marketers, or intercept personal data
- Microsoft has released Microsoft AntiSpyware to combat this problem

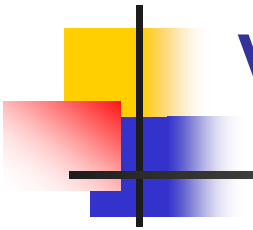
Understanding Software Exploitation (cont)

- **Rootkits** recently have become the software the latest fashion in software exploitation.
- Rootkits are programs that have the ability to hide certain things from the operating system
- With a rootkit, there may be a number of processes running on a system that do not show up in the Task Manager, or connections established or available that do not appear in a netstat display – the rootkit masks the presence of these items
- The rootkit is able to do that by manipulating function calls to the operating system and filtering out information that would normally appear
- Unfortunately, many rootkits are written to get around antivirus and anti-spyware programs that are not kept up to date
- There are rootkit analyzers.....Spybot , Spyware Doctor

Understanding Malicious Code (Malware)



- Consists of computer programs designed to break into computers or to create havoc on computers
- Most common types:
  - Viruses
  - Worms
  - Logic bombs
  - Trojan horses
  - Back doors



Viruses

- Programs that secretly attach to another document (word document) or program and execute when that document or program is opened.
- Virus programs are not structured to exist by themselves.
- Might contain instructions that cause problems ranging from displaying an annoying message to erasing files from a hard drive or causing a computer to crash repeatedly
- Examples : Michelangelo , Melissa (a macro virus)
- Complete lists and descriptions available at
  - www.symantec.com
  - www.mcafee.com

Symptoms of Virus infection

- The programs on your system start to load more slowly
- Unusual files appear on your hard drive, or files start to disappear from your system (sometimes key files in the system are deleted which renders the system inoperable)
- Program sizes change from the installed versions

Symptoms of Virus Infection (cont.)

- Your browser, word processing application, or other S/W begins to exhibit unusual operating characteristics
- The system mysteriously shuts itself down or restarts and does a great deal of unanticipated disk activity.
- You mysteriously lose access to a disk drive or other system resources
- Your system suddenly doesn't reboot or gives unexpected error messages during startup.
- *Note : This list is by no means comprehensive*

How Viruses Work

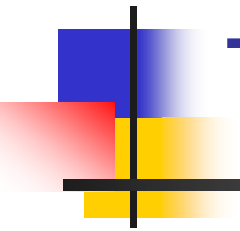
- A virus, in most cases, tries to accomplish one of two things:
  - Render your system inoperable
  - Or , spread to other systems
- Many viruses will spread to other systems, given the chance, and then render your system inoperable
- If your system is infected, the virus may try to attach itself to every file in your system and spread each time you send a file or document to others

How Viruses Work (cont.)

- Many newer viruses spread using e-mail
- The infected system includes an attachment to any email that you send to another user
- The recipient opens this file, thinking it's something you legitimately sent him
- When they open the file, the virus infects the target system.
- This virus may then attach itself to all the e-mails the newly infected system sends, which in turn infect the recipients of the e-mails

Viruses (cont.)

- Drawback of antivirus software is that it must be updated to recognize new viruses
- Updates (definition files or signature files) can be downloaded automatically from the Internet to a user's computer
- Types of viruses:
  - Transient Virus: is only active when a program it has infected is running
  - Resident Virus : establishes itself in memory when the program it has infected is running. A Resident (TSR) virus can become active even after the program it has attached to has terminated by linking itself into the execution of other programs.



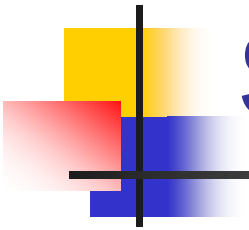
Types of Viruses

Viruses take many different forms.

The following slides briefly introduces the most common forms.

Polymorphic Virus

- Change form in order to avoid detection
- These types attack your system, display a message on your computer, and delete files on your system
- The virus will try to hide from your antivirus software
- Frequently it will encrypt parts of itself to avoid detection...when it does this it is called *mutation*
- *The mutation process makes it hard for antivirus software to detect the virus*

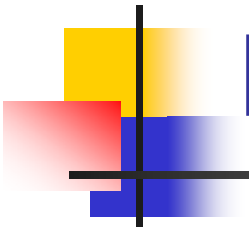


Stealth Virus

- Attempts to avoid detection by masking itself from applications
- It may attach itself to the boot sector of the hard drive
- When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection
- An infected file may report a file size different from what is actually present in order to avoid detection
- Stealth viruses may also move themselves from fileA to fileB during a virus scan for the same reasons

Retrovirus

- Attacks or bypasses the anti-virus software installed in a computer
- It can be considered an *anti-antivirus*
- Retroviruses can directly attack your antivirus software and potentially destroy the virus definition database file
- Destroying this information without your knowledge, would leave you with a false sense of security
- The virus may also directly attack an antivirus program to create bypasses for the virus

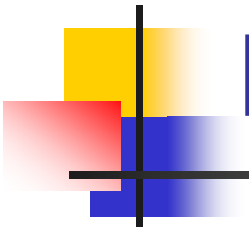


Multipartite Virus

- Attacks your system in multiple ways
- It may attempt to infect your boot sector, infect all of your executable files, and destroy your application files
- The hope here is that you won't be able to correct all the problems and will allow the infestation to continue

Armored Virus

- Is designed to make itself difficult to detect or analyze
- They cover themselves with protective code that stops debuggers or disassemblers from examining critical elements of the virus
- The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
- From the perspective of the creator, the more time it takes to deconstruct the virus, the longer it can live
- Thus, the more time it has to replicate and spread to as many machines as possible

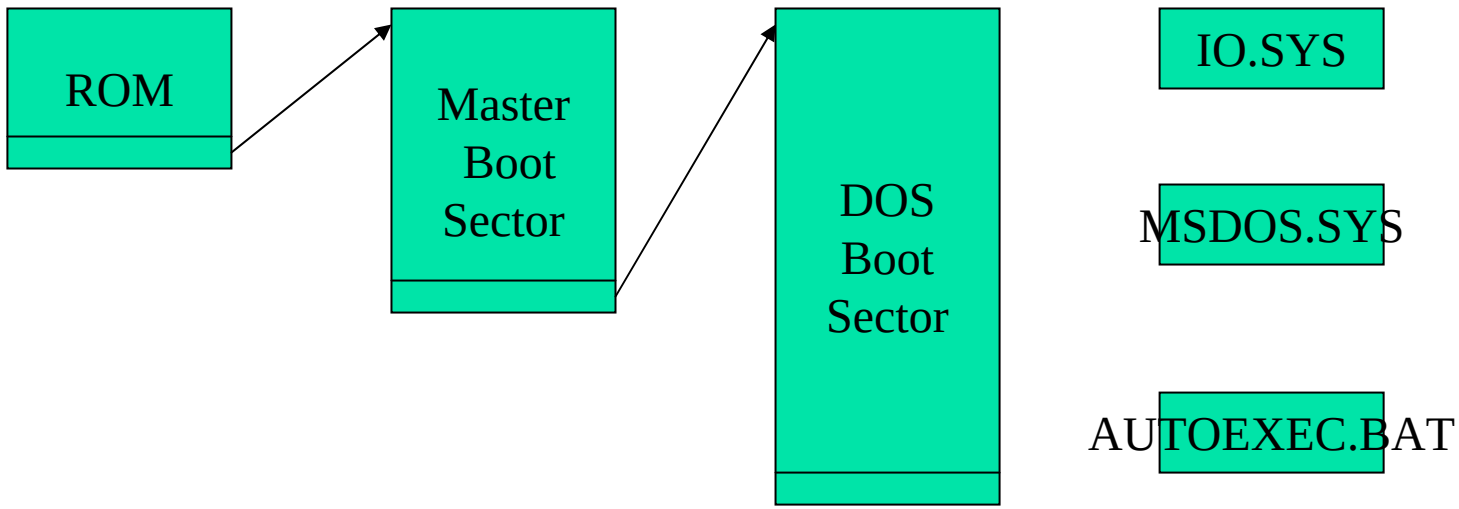


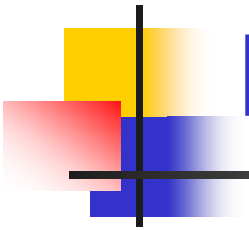
Phage Virus

- Modifies and alters other programs and databases
- The virus infects all these files
- The only way to remove this virus is to reinstall the programs that are infected
- If you miss even a single incident of this virus on the system, the process will start again and infect the system once more

PC Boot Sequence

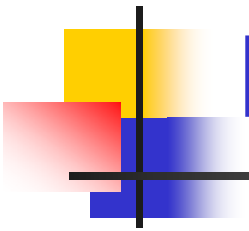
Typical Boot Sequence :





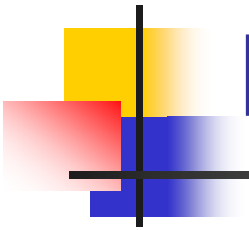
PC Boot Sequence (continued)

- The Boot Sequence :
  - ROM : initialization routine that locates the master boot sector on secondary storage.
  - MBS : In a standard location (s=0,t=1), contains some executable code and a partition table dividing the disk into partitions and indicating which partitions are bootable. The MBS also locates the DOS Boot sector DBS on secondary storage.
  - DBS : contains executable code and the FAT that records where files are stored. Clusters with physical defects are marked bad in the FAT.



PC Boot Sequence (continued)

- The boot sequence continues by:
  - Loading the IO.SYS program containing the BIOS and the SYSINIT program.
  - SYSINIT loads MSDOS.SYS
  - Control passes to DOS which runs the command interpreter COMMAND.COM consulting the AUTOEXEC.BAT file. COMMAND.COM prompts the user for input.

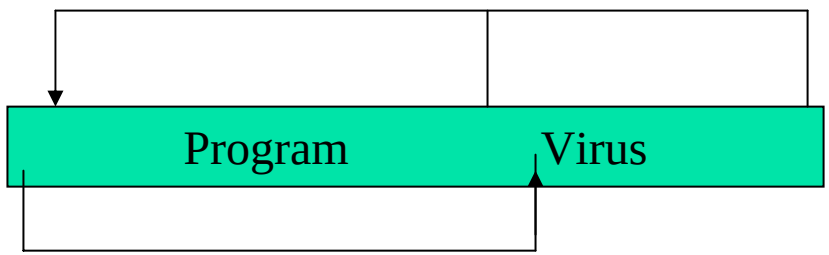


Bootstrap Virus

- A bootstrap virus resides in one of the boot sectors.
- As it becomes active before DOS is fully operational, it can only use BIOS functions and is written for a particular machine architecture.
- Other types :
  - Stored virus (New Zealand Virus)
  - Brain Virus
  - Lehigh Virus (COMMAND.COM)
- Boot viruses are written in machine language.

Parasitic Virus

- A parasitic virus is attached to an executable program i.e. a .COM or .EXE file, and infects other programs.
- Such a virus typically appends itself to the infected program and inserts a jump to the viral code at the beginning of the program.
- At the end of the virus, there is a jump back to the start of the program. E.g Vienna Virus

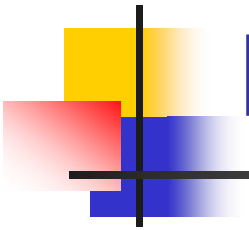


Companion Virus

- Attaches itself to legitimate programs and then creates a program with a different file extension...this file may reside in your system's temporary directory
- When a user types the name of the legitimate program, the companion virus executes instead of the real program
- This effectively hides the virus from the user
- Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that they point to the infected program
- The infected program may perform its bad deed and then start the real program

Companion Virus (cont.)

- Filenames in DOS typically have extensions .DIR, .COM , .EXE
- For convenience users do not have to specify the full filename of a program they want to execute and can omit the extension.
- If a user calls a program in this fashion, then DOS first looks for a .COM file with this name, then for a .EXE file , then for a .BAT file.
- A companion file exploits this default searchpath.
- If the original program is a .EXE file , then a .COM file with the same name and containing a virus could be created and the infected program would be executed.
- Ex. The AIDs 2 virus.



Macro Viruses

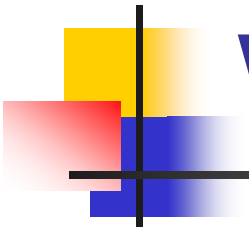
- Macro viruses are written in a HLL
- A macro virus can attach itself to a spreadsheet or a word document.
- This type of virus is particularly interesting and damaging.
  - The virus is attached to a data file : therefore it will bypass integrity protection mechanisms targeting ‘normal’ executables. (OS , programs)
  - The virus is in HLL is much more platform independent than a m/c language virus.
  - Text documents are widely exchanged by email. An excellent way for a virus to spread.
  - Macro viruses started in 1995.
  - Macro viruses are the fastest growing virus today

Present Virus Activity (CERT)

- Visit the CERT?CC Activity web page at

http ://www.us-cert.gov/current/current_activity.html

- Here you will find a detailed description of the current viruses as well as links to pages on older threats

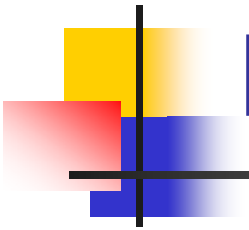


Worms

- A worm can reproduce itself, is self-contained, and doesn't need a host application to be transported
- A worm is a program that crawls from system to system without any assistance from its victims.
- A worm spreads on its own and also replicates on its own.

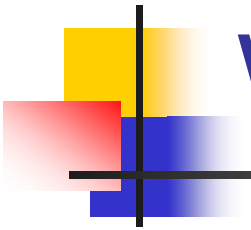
Worms (cont.)

- Although similar in nature, worms are different from viruses in two regards:
  - A virus attaches itself to a computer document, such as an e-mail message, and is spread by traveling along with the document
  - A virus needs the user to perform some type of action, such as starting a program or reading an e-mail message, to start the infection
  - The Melissa worm spread itself to more than 100,000 users in a relatively short period when it first came out. *One site received more than 32,000 copies of Melissa in a 45-minute period*



Malicious Code Attacks

- Multiple new viruses and worms appear every week.
- The Skulls.B Trojan horse contains the Cabir.B worm (spreads to cellphones via bluetooth)
- Skulls wipes out your application files
- Cabir burns your battery trying to spread.

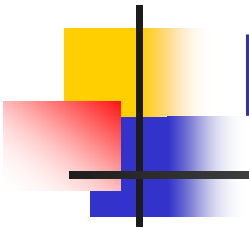


Worms (continued)

- Worms are usually distributed via e-mail attachments as separate executable programs
- In many instances, reading the e-mail message starts the worm
- If the worm does not start automatically, attackers can trick the user to start the program and launch the worm
- Famous worms : Morris , CodeRed (it used legitimate web connections to attack, firewalls did not protect the victim) .

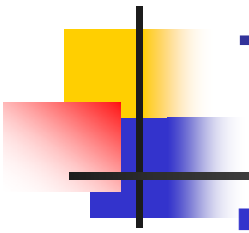
Slapper Worm (2002)

- It exploited a vulnerability in the OpenSSL module of the Apache server.
- Once into the system, the worm chose an IP address to attack.
- Slapper would then examine the target IP address to see if it had an Apache web server running on an Intel platform.
- Finally the worm checked if the target was vulnerable to attack.
- The attack was run over HTTPS on port 443. this made the attack difficult to detect since the traffic was encrypted.
- The good news: the check was made over regular HTTP on port 80 and thus was easy to detect.
- The exploit that was run on the target caused the worm to get a command shell.
- With this command shell, the worm would copy itself to the target, compile itself, and execute the new binary code.
- Slapper would then begin looking for victims and start the process all over again.
- Perhaps the most dangerous part of Slapper worm is its communication ability.



Logic Bombs

- Computer program that lies dormant until triggered by a specific event, for example:
  - A certain date being reached on the system calendar
  - A person's rank in an organization dropping below a specified level



Trojan Horses

- Just like the Greeks used a gift to hide evidence of their attack.
- Trojan horses are programs that hide their true intent and then reveal themselves when activated
- Might disguise themselves as free calendar programs or other interesting software
- Most Trojan horse programs also contain mechanisms to spread themselves to new victims.
- Common strategies:
  - Giving a malicious program the name of a file associated with a benign program
  - Combining two or more executable programs into a single filename

Trojan Horse Example

- ILOVEYOU Trojan horse was an e-mail visual basic attachment. The attachment was made to appear like a text file.
- When the user opened it , it would execute the VB code and mail itself to a large number of other people who were found in the victim's address book.
- In many organizations that program caused e-mail services to stop completely.

Trojan Horses (cont.)

- Defend against Trojan horses with the following products:
  - Antivirus tools, which are one of the best defenses against combination programs
  - Special software that alerts you to the existence of a Trojan horse program
  - Anti-Trojan horse software that disinfects a computer containing a Trojan horse