UNIT V
SYSTEM LEVEL SECURITY
Worms,viruses

Cryptography and Network security,Fifth Edition

by William Stallings

Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

Cyber Threat: List of Latest Computer Viruses 2020

https://blogs.innovanathinklabs.com/cyber-threat-latest-computer-viruses/

Cyborg Ransomware

CryptoMix Clop Ransomware

GoBrut

Jokeroo

Trojan Glupteba

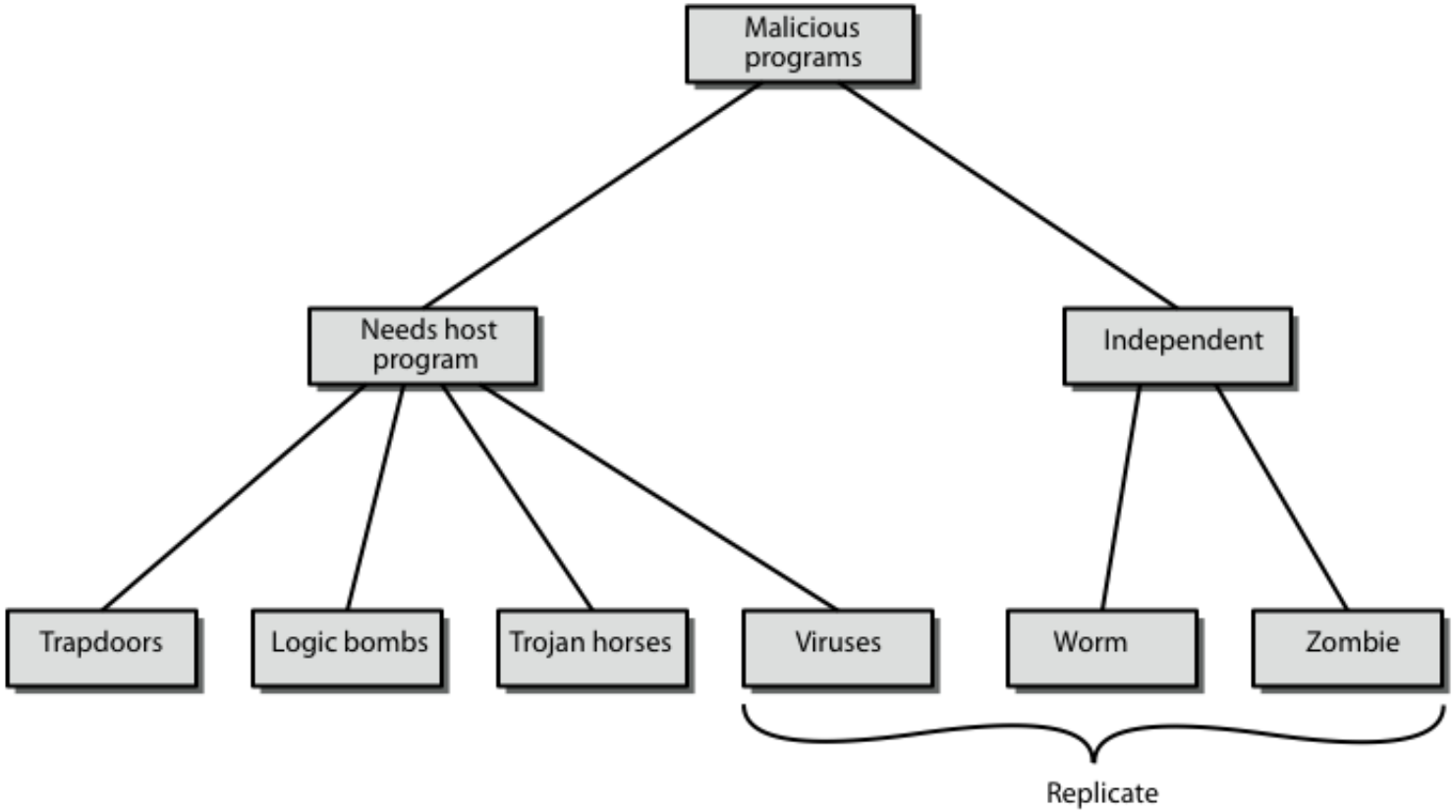
UHBVN Ransomware Attack

WannaCry

Mirai Botnet Malware Attack

BSNL Malware Attack

Malicious Software



Backdoor or Trapdoor

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks, halt machine, etc

Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data

Mobile Code

- program/script/macro that runs unchanged
  - on heterogeneous collection of platforms
  - on large homogeneous collection (Windows)
- transmitted from remote system to local system & then executed on local system
- often to inject virus, worm, or Trojan horse
- or to perform own exploits
  - unauthorized data access, root compromise

Multiple-Threat Malware

- malware may operate in multiple ways
- **multipartite** virus infects in multiple ways
  - eg. multiple file types
- **blended** attack uses multiple methods of infection or transmission
  - to maximize speed of contagion and severity
  - may include multiple types of malware
  - eg. Nimda has worm, virus, mobile code
  - can also use IM(instant messaging) & P2P(peer-to-peer file sharing)
  - Some writers characterize a blended attack as a package that includes multiple types of malware

Viruses

Viruses

- piece of software that infects programs
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run
  - Once a virus is executing, it can perform any function, such as erasing files and programs
- specific to operating system and hardware
  - taking advantage of their details and weaknesses
- a typical virus goes through phases of:
  - dormant
  - propagation
  - triggering
  - execution

Virus Structure

- A computer virus has three parts :
  - infection mechanism(infection vector) - enables replication
  - trigger - event that makes payload activate
  - payload - what it does, malicious or benign
- prepended / postpended / embedded
- when infected program invoked, executes virus code then original program code
- can block initial infection (difficult)
- or propagation (with access controls)

Virus Structure

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

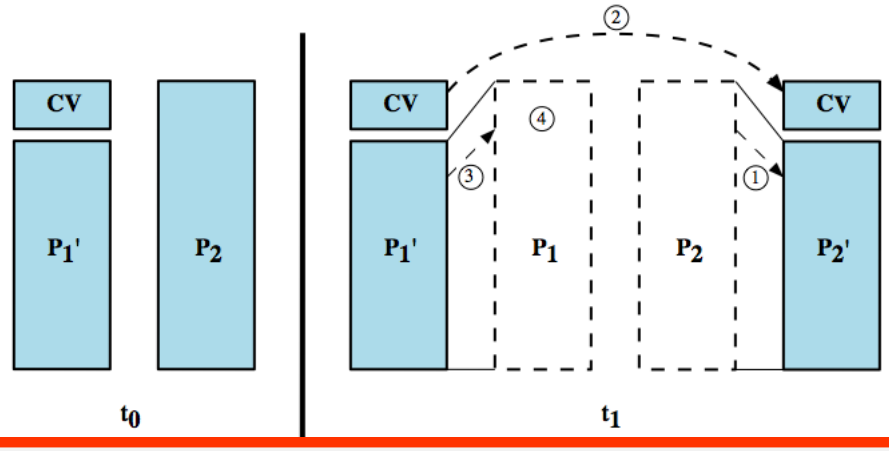
Compression Virus

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)     compress file;
        (2)     prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)     uncompress rest-of-file;
        (4)     run uncompressed file;}
        }
```



Worms,viruses

Cryptography and Network security,

Fifth Edition

by William Stallings

Course outcome:

Identify an appropriate security system to provide system level security.

Learning Outcome:

Explain the vulnerabilities and the measures to protect the system against the attacks.

Specific Outcome:

Examine malicious software (malware), especially viruses and worms, which exploit vulnerabilities in computing systems

Virus Classification

- boot sector
- file infector
- macro virus
- encrypted virus
- stealth virus
- polymorphic virus
- metamorphic virus

- Boot sector infector:Infects a master boot record or boot record.

- File infector: Infects files that operating system or shell consider to be executable.

- Macro virus: Infects files with macro code that is interpreted by an application.

- Encrypted virus: the virus creates a random encryption key,encrypt the virus When an infected program is invoked, the virus uses the stored random key to decrypt the virus.

• Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software.

•Polymorphic virus: A virus that mutates with every infection, making detection by the "signature"of the virus impossible.

• Metamorphic virus: As with a polymorphic virus ,a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. They may change their behavior as well as their appearance.

Macro Virus

- became very common in mid-1990s since
  - platform independent
  - infect documents
  - easily spread
- Virtually all of the macro viruses infect Microsoft Word documents
  - Macro viruses infect documents, not executable portions of code
  - A macro is an executable program embedded in a word processing document or other type of file
- Macro viruses are easily spread. A very common method is by electronic mail.
- more recent releases include protection
- recognized by many anti-virus programs

E-Mail Viruses

- more recent development
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list and does local damage
- then saw versions triggered reading email
- hence much faster propagation

Virus Countermeasures

- prevention - ideal solution but difficult
- realistically need:
  - detection
  - identification
  - removal
- if detect but can't identify or remove, must discard and replace infected program

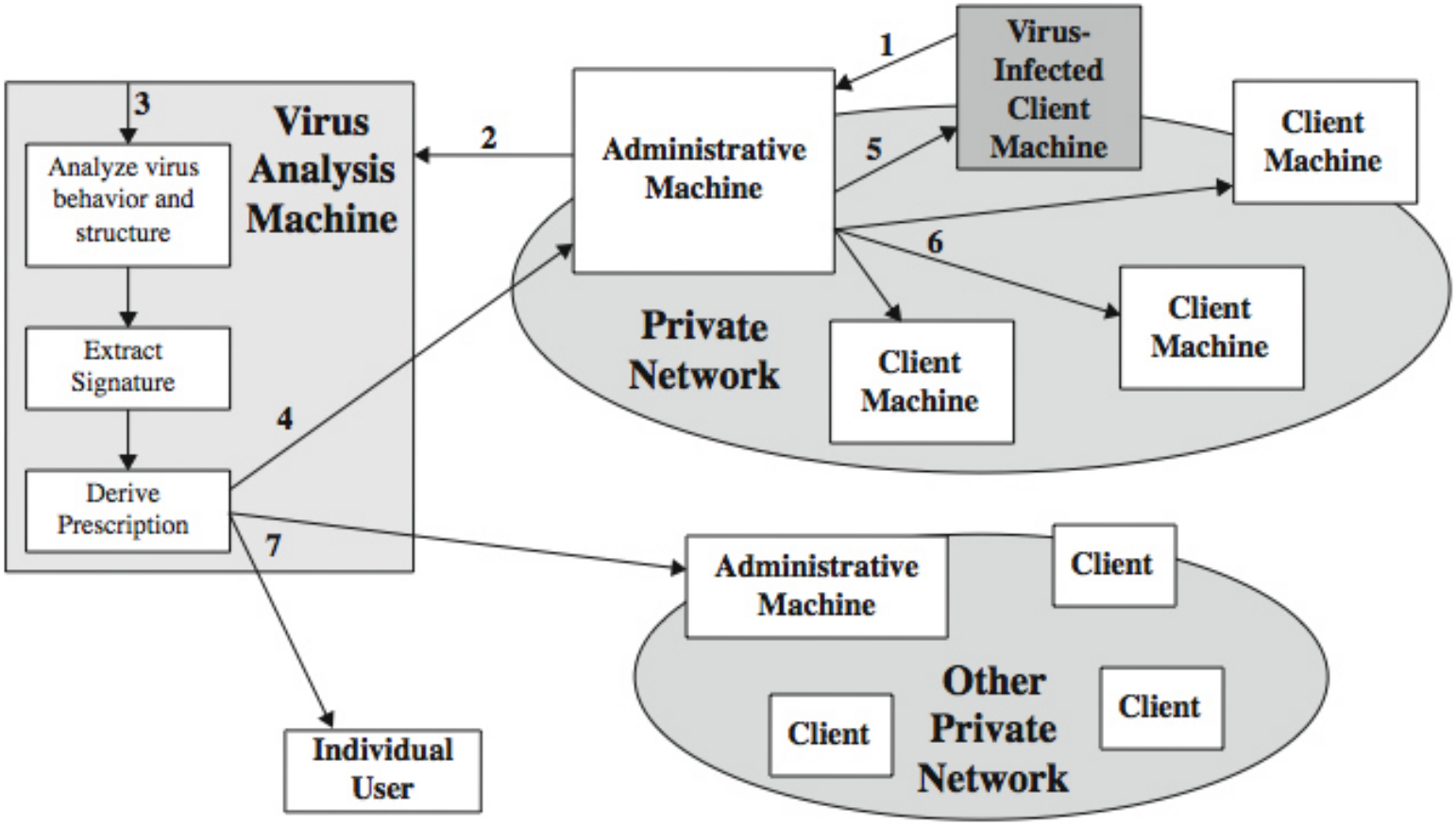
Anti-Virus Evolution

- virus & antivirus tech have both evolved
- early viruses simple code, easily removed
- as become more complex, so must the countermeasures
- generations
  - first - signature scanners
  - second - heuristics
  - third - identify actions
  - fourth - combination packages

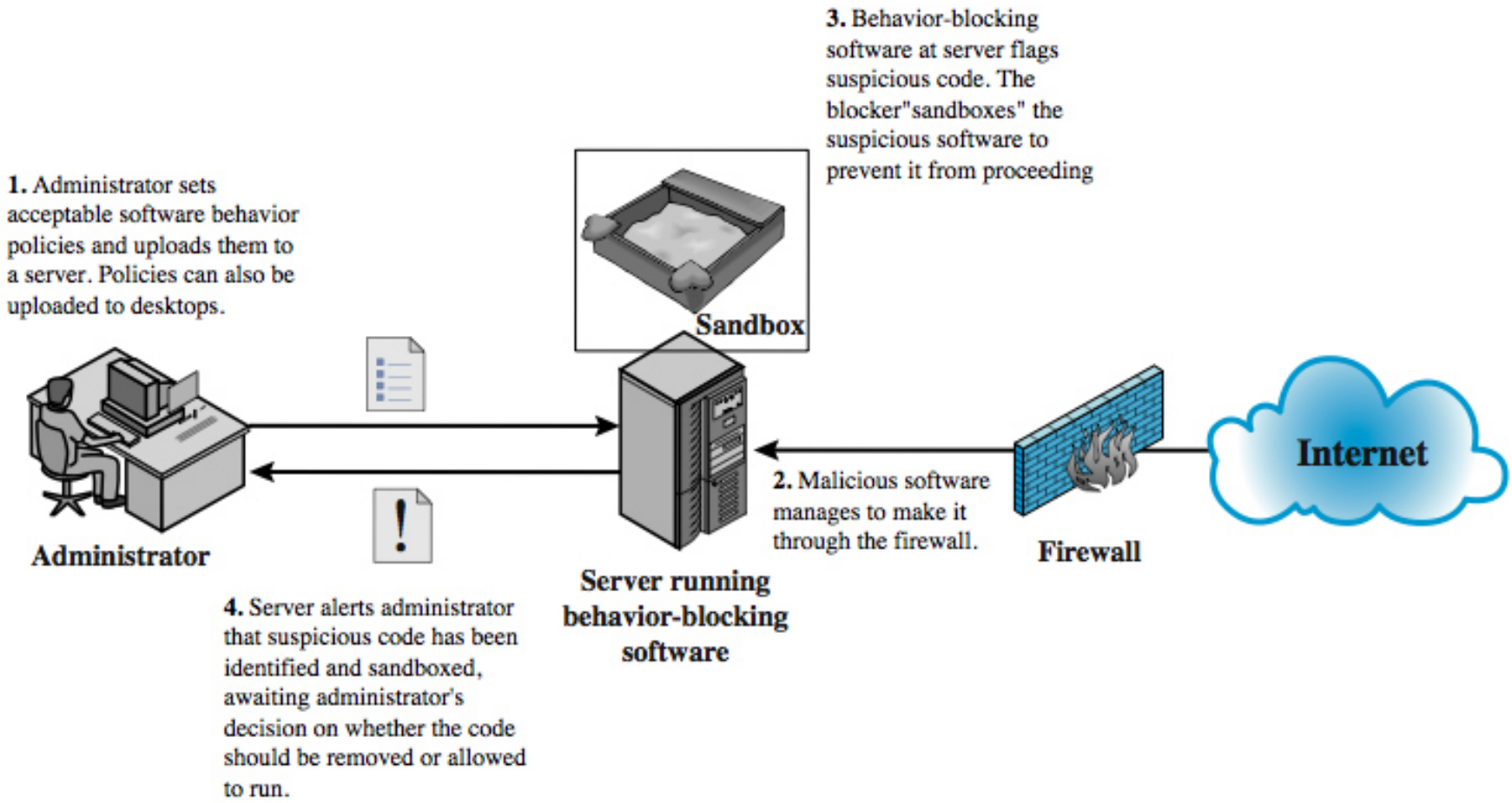
Generic Decryption

- runs executable files through GD scanner:
  - CPU emulator to interpret instructions
  - virus scanner to check known virus signatures
  - emulation control module to manage process
- lets virus decrypt itself in interpreter
- periodically scan for virus signatures
- issue is long to interpret and scan
  - tradeoff chance of detection vs time delay

Digital Immune System



Behavior-Blocking Software



THANK YOU

UNIT V

SYSTEM LEVEL SECURITY

Intrusion Detection

Cryptography and Network security,Fifth Edition by William Stallings

Course outcome:

Identify an appropriate security system to provide system level security.

Learning Outcome:

Explain the measures to protect the system against the attacks.

Specific Outcome:

Identify the classes of intruders and Intruder detection mechanism

Intruders

- significant issue for networked systems is hostile or unwanted access
- either via network or local
- can identify classes of intruders:
  - masquerader
  - misfeasor
  - clandestine user
- varying levels of competence

Intruders

- can identify classes of intruders:
  - **Masquerader** – Individual not authorized to access but penetrates a systems access to exploit legitimate user's account.(outsider)
  - **Misfeasor –** A legitimate user who access data, programs or resources for which access is unauthorised.(insider)
  - **Clandestine user –** An individual who seizes supervisory control of the system & uses this control to evade auditing & access control.

Intruders

- clearly a growing publicized problem
  - from “Wily Hacker” in 1986/87 https://en.wikipedia.org/wiki/Clifford_Stoll
- may seem benign, but still cost resources
- may use compromised system to launch other attacks
- awareness of intruders has led to the development of CERTs(Computer emergency response team)

Massive attack on public sites

- Two levels of Hackers

  Sophisticated Users- through knowledge of the technology

  Foot Soldiers – use cracking programs

- In addition to running password cracking programs , intruders attempted to modify the login software to capture the password of users logging on to the system.

Intruder Behavior Patterns: Some Examples of Intruder Patterns of Behavior

(a) Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

Scanning www.zooreach.org (162.144.6.10) [1000 ports]

Discovered open port 21/tcp on 162.144.6.10

Discovered open port 53/tcp on 162.144.6.10

Discovered open port 443/tcp on 162.144.6.10

Discovered open port 587/tcp on 162.144.6.10

Discovered open port 995/tcp on 162.144.6.10

Discovered open port 143/tcp on 162.144.6.10

Discovered open port 993/tcp on 162.144.6.10

Discovered open port 22/tcp on 162.144.6.10

Discovered open port 110/tcp on 162.144.6.10

Discovered open port 80/tcp on 162.144.6.10

Discovered open port 3306/tcp on 162.144.6.10

Discovered open port 2222/tcp on 162.144.6.10

Discovered open port 26/tcp on 162.144.6.10

(b) Criminal Enterprise

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

(c) Internal Threat

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

THANK YOU

UNIT V

SYSTEM LEVEL SECURITY

Intrusion Detection

Cryptography and Network security,Fifth Edition by William Stallings

Course outcome:

Identify an appropriate security system to provide system level security.

Learning Outcome:

Explain the measures to protect the system against the attacks.

Specific Outcome:

Identify the classes of intruders and Intruder detection mechanism

Intrusion Techniques

- aim to gain access and/or increase privileges on a system
- basic attack methodology
  - target acquisition and information gathering
  - initial access
  - privilege escalation
  - covering tracks
- key goal often is to acquire passwords
- so then exercise access rights of owner

Intrusion Techniques

- Objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.
- Intruder attempts to acquire information that should have been protected – Password.
- Password file can be protected by two ways:
- **One-way function:** The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password & compares it with the stored value.

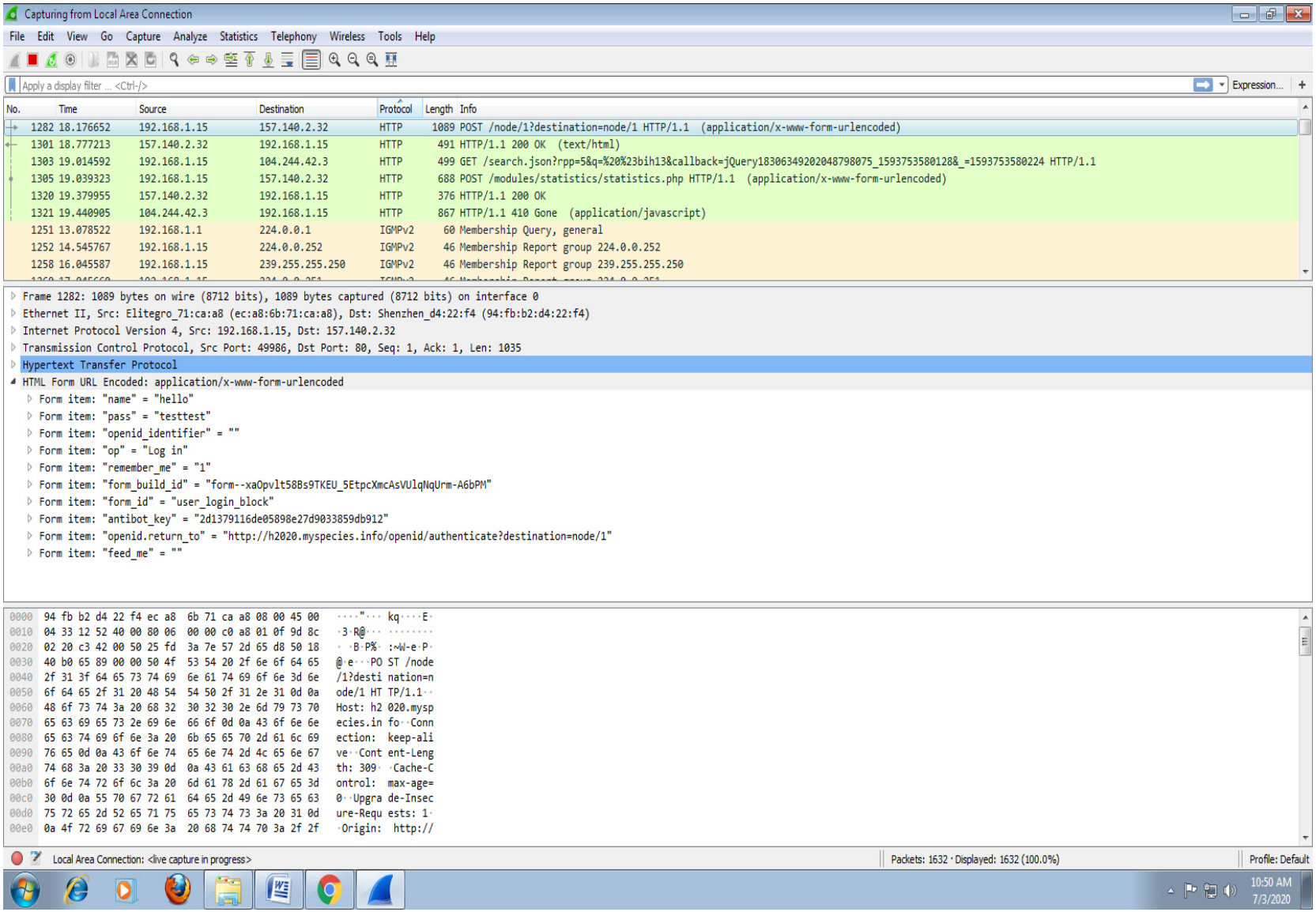
- In practice, the system usually performs a one-way transformation in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.
- **Access control:** Access to the password file is limited to one or a very few accounts.

Password Guessing

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests)
  - exhaustively searching all possible passwords
- check by login or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

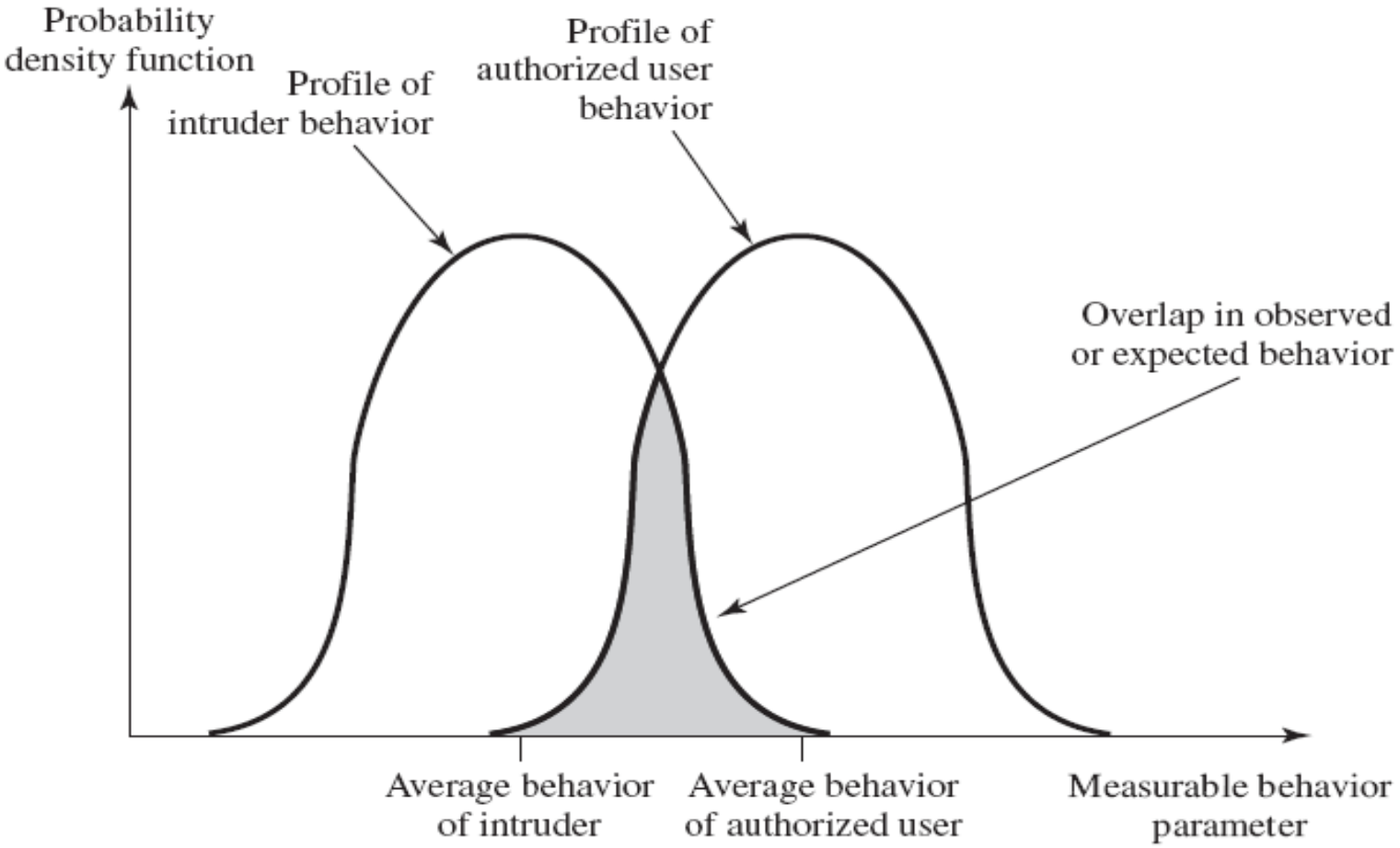
Password Capture

- another attack involves **password capture**
  - watching over shoulder as password is entered
  - using a trojan horse program to collect
  - monitoring an insecure network login
    - eg. telnet, FTP, web, email
  - extracting recorded info after successful login (web history/cache, last number dialed etc)
- using valid login/password can impersonate user
- users need to be educated to use suitable precautions/countermeasures


Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1282 18.176652 192.168.1.15 157.140.2.32 HTTP 1089 POST /node/1?destination=node/1 HTTP/1.1 (application/x-www-form-urlencoded)
1301 18.777213 157.140.2.32 192.168.1.15 HTTP 491 HTTP/1.1 200 OK (text/html)
1303 19.014592 192.168.1.15 104.244.42.3 HTTP 499 GET /search.json?rpp=5&q=%20%23bih13&callback=jQuery18306349202048798075_1593753580128&_=1593753580224 HTTP/1.1
1305 19.039323 192.168.1.15 157.140.2.32 HTTP 688 POST /modules/statistics/statistics.php HTTP/1.1 (application/x-www-form-urlencoded)
1320 19.379955 157.140.2.32 192.168.1.15 HTTP 376 HTTP/1.1 200 OK
1321 19.440905 104.244.42.3 192.168.1.15 HTTP 867 HTTP/1.1 410 Gone (application/javascript)
1251 13.078522 192.168.1.1 224.0.0.1 IGMPv2 60 Membership Query, general
1252 14.545767 192.168.1.15 224.0.0.252 IGMPv2 46 Membership Report group 224.0.0.252
1258 16.045587 192.168.1.15 239.255.255.250 IGMPv2 46 Membership Report group 239.255.255.250
Frame 1282: 1089 bytes on wire (8712 bits), 1089 bytes captured (8712 bits) on interface 0
Ethernet II, Src: Elitegro_71:ca:a8 (ec:a8:6b:71:ca:a8), Dst: Shenzhen_d4:22:f4 (94:fb:b2:d4:22:f4)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 157.140.2.32
Transmission Control Protocol, Src Port: 49986, Dst Port: 80, Seq: 1, Ack: 1, Len: 1035
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "name" = "hello"
Form item: "pass" = "testtest"
Form item: "openid_identifier" = ""
Form item: "op" = "Log in"
Form item: "remember_me" = "1"
Form item: "form_build_id" = "form--xaOpvlt58Bs9TKEU_5EtpcXmcAsVUlqNqUrm-A6bPM"
Form item: "form_id" = "user_login_block"
Form item: "antibot_key" = "2d1379116de05898e27d9033859db912"
Form item: "openid.return_to" = "http://h2020.myspecies.info/openid/authenticate?destination=node/1"
Form item: "feed_me" = ""
0000 94 fb b2 d4 22 f4 ec a8 6b 71 ca a8 08 00 45 00 ····"··· kq····E·
0010 04 33 12 52 40 00 80 06 00 00 c0 a8 01 0f 9d 8c ·3·R@··· ········
0020 02 20 c3 42 00 50 25 fd 3a 7e 57 2d 65 d8 50 18 · ·B·P%· :~W-e·P·
0030 40 b0 65 89 00 00 50 4f 53 54 20 2f 6e 6f 64 65 @·e···PO ST /node
0040 2f 31 3f 64 65 73 74 69 6e 61 74 69 6f 6e 3d 6e /1?desti nation=n
0050 6f 64 65 2f 31 20 48 54 54 50 2f 31 2e 31 0d 0a ode/1 HT TP/1.1··
0060 48 6f 73 74 3a 20 68 32 30 32 30 2e 6d 79 73 70 Host: h2 020.mysp
0070 65 63 69 65 73 2e 69 6e 66 6f 0d 0a 43 6f 6e 6e ecies.in fo··Conn
0080 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0090 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ve··Cont ent-Leng
00a0 74 68 3a 20 33 30 39 0d 0a 43 61 63 68 65 2d 43 th: 309· ·Cache-C
00b0 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d ontrol: max-age=
00c0 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 0··Upgra de-Insec
00d0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ure-Requ ests: 1·
00e0 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f ·Origin: http://
Local Area Connection: <live capture in progress>
Packets: 1632 · Displayed: 1632 (100.0%)
Profile: Default
10:50 AM
7/3/2020

Intrusion Detection

- inevitably the best intrusion prevention system will fail.
- A systems second line of defense is intrusion detection. considerations are
  - block if detected quickly
  - Can serve as deterrent
  - collect information to improve security
- Intrusion detection is based on the assumption that the behaviour of the intruder differs from that of a legitimate user.



Profiles of Behavior of Intruders and Authorized Users

THANK YOU

UNIT V

SYSTEM LEVEL SECURITY

Intrusion Detection

Cryptography and Network security,Fifth Edition by William Stallings

Approaches to Intrusion Detection

- In Anderson's study, it was postulated that one could, with reasonable confidence, distinguish between a masquerader and a legitimate user.

- statistical anomaly detection
- rule-based detection

Statistical anomaly detection

- **Involves the collection of data relating to the**

  behavior of legitimate users over a period of time.

a. Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

b. Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

Rule-based detection

- Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a. **Anomaly detection**: Rules are developed to detect deviation from previous usage patterns.

b. **Penetration identification**: An expert system approach that searches for suspicious behavior.

Audit Records

- fundamental tool for intrusion detection
- **Native audit records**
  - part of all common multi-user O/S
  - Adv: No additional collection s/w is required.
  - Dis:may not have information wanted in desired form.
- **Detection-specific audit records**
  - created specifically to collect wanted information
  - at cost of additional overhead on system running two accounting packages.

Detection-specific audit records

Each audit record contains the following fields:

- Subject – Initiator of action
- Action – login,read,write
- Object –Response of actions
- Exception-Condition
- Resource-Usage
- Time-Stamp

Statistical Anomaly Detection

- Falls into two categories
  - Threshold Detection
  - Profile based systems

Threshold detection

- Crude and ineffective detector of even moderately sophisticated attacks.
- Both the threshold and the time interval must be determined.
- Because of the variability across users ,Likely to generate a lot of false positives or a lot of false negatives.

Profile-based intrusion detection

- analyze records to get metrics over time
  - counter, gauge, interval timer, resource utilization
- use various tests on these to determine if current behavior is acceptable
  - mean & standard deviation, multivariate, markov process, time series, operational
- key advantage is no prior knowledge used

DR MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY

THANK YOU

NIA EDUCATIONAL INSTITUTIONS | Enlightening Minds

UNIT V

SYSTEM LEVEL SECURITY

Intrusion Detection

Cryptography and Network security,Fifth Edition by William Stallings

Rule-Based Intrusion Detection

- observe events on system & apply rules to decide if activity is suspicious or not.
- rule-based anomaly detection
  - analyze historical audit records to identify usage patterns & auto-generate rules for them
  - then observe current behavior & match against rules to see if conforms
  - like statistical anomaly detection,rule based intrusion detection does not require prior knowledge of security vulnerabilities.

Rule-Based Intrusion Detection

- rule-based penetration identification
  - uses expert systems technology
  - with rules identifying known penetration, weakness patterns, or suspicious behavior
  - compare audit records or states against rules
  - rules usually machine & O/S specific
  - The rules are generated by “experts”, from interviews of system administrators and security analysts
  - quality depends on how well this is done

Base-Rate Fallacy

- Intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable rate.
- practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
  - if too few intrusions detected -> false security
  - if too many false alarms -> ignore / waste time
- this is very hard to do
- existing systems seem not to have a good record

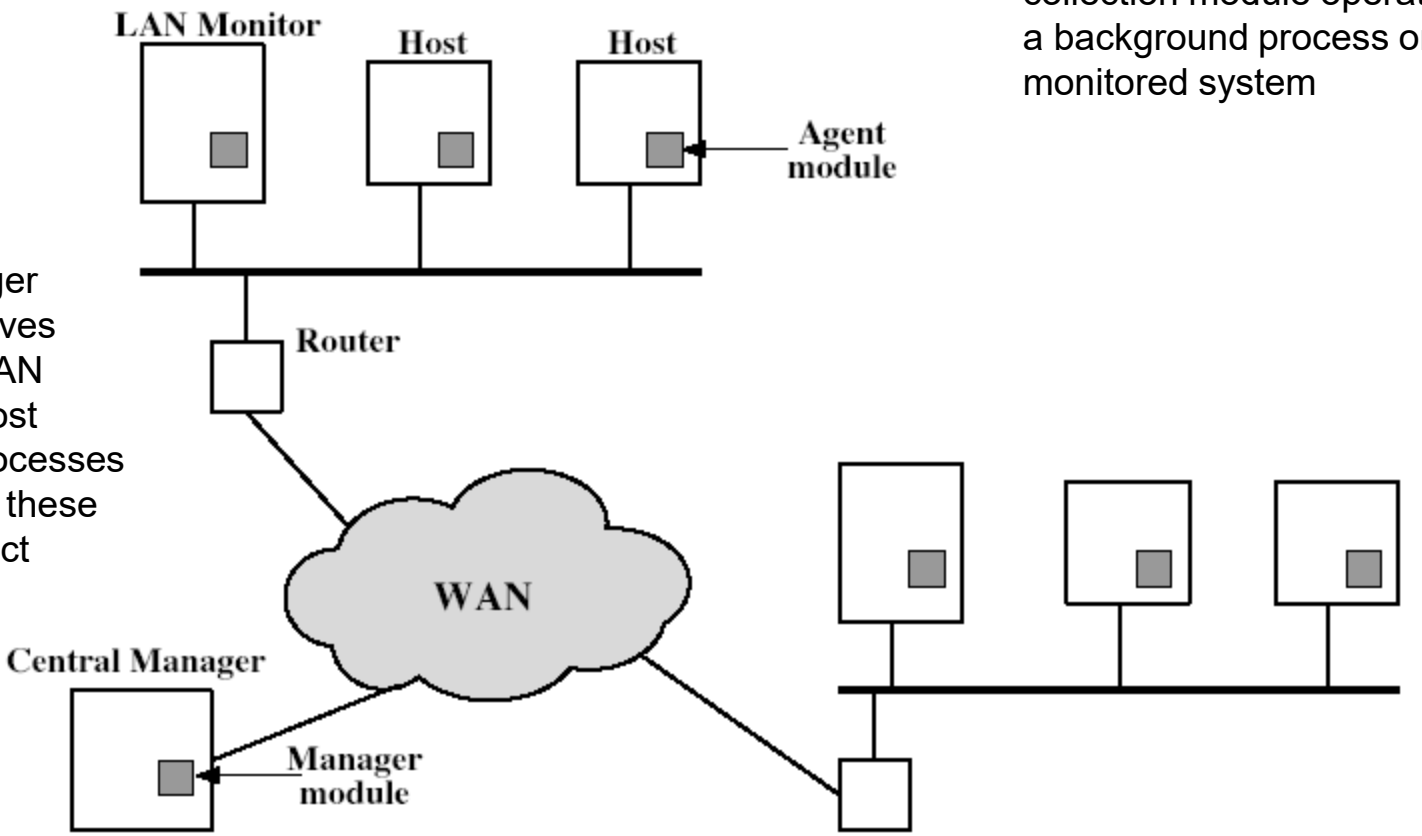
Distributed Intrusion Detection

- traditional focus is on single systems
- but typically have networked systems
- more effective defense has these working together to detect intrusions
- issues
  - dealing with varying audit record formats
  - integrity & confidentiality of networked data
  - Either a centralized or decentralized architecture can be used.

Distributed Intrusion Detection - Architecture

LAN monitor agent module: like a host agent module except it analyzes LAN traffic

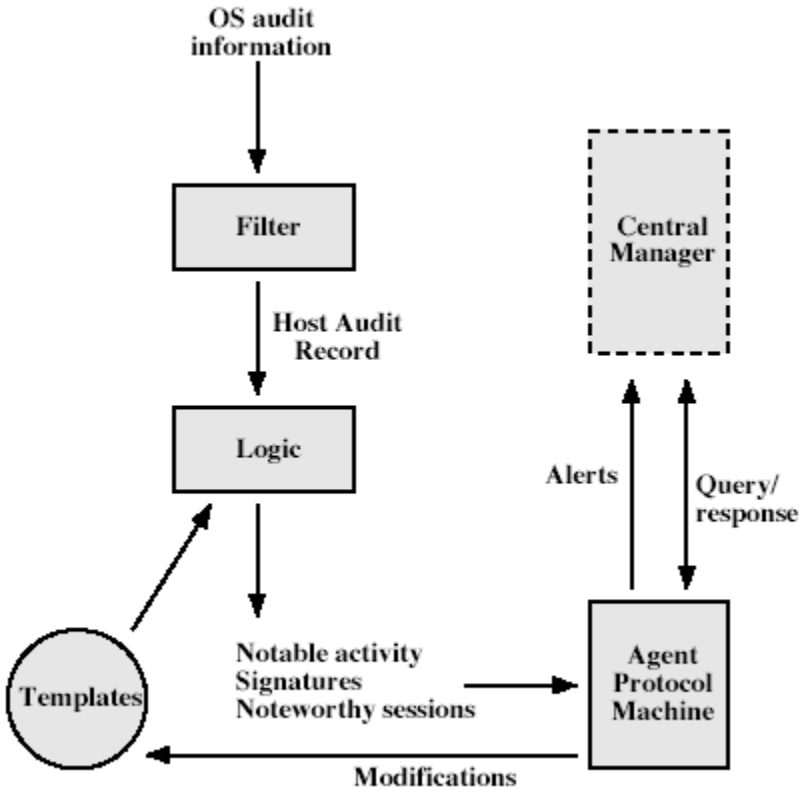
Host agent module: audit collection module operating as a background process on a monitored system



Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion

- **Host agent module:** An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security related events on the host and transmit these to the central manager.
- **LAN monitor agent module:** Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- **Central manager module:** Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

Distributed Intrusion Detection – Agent Implementation



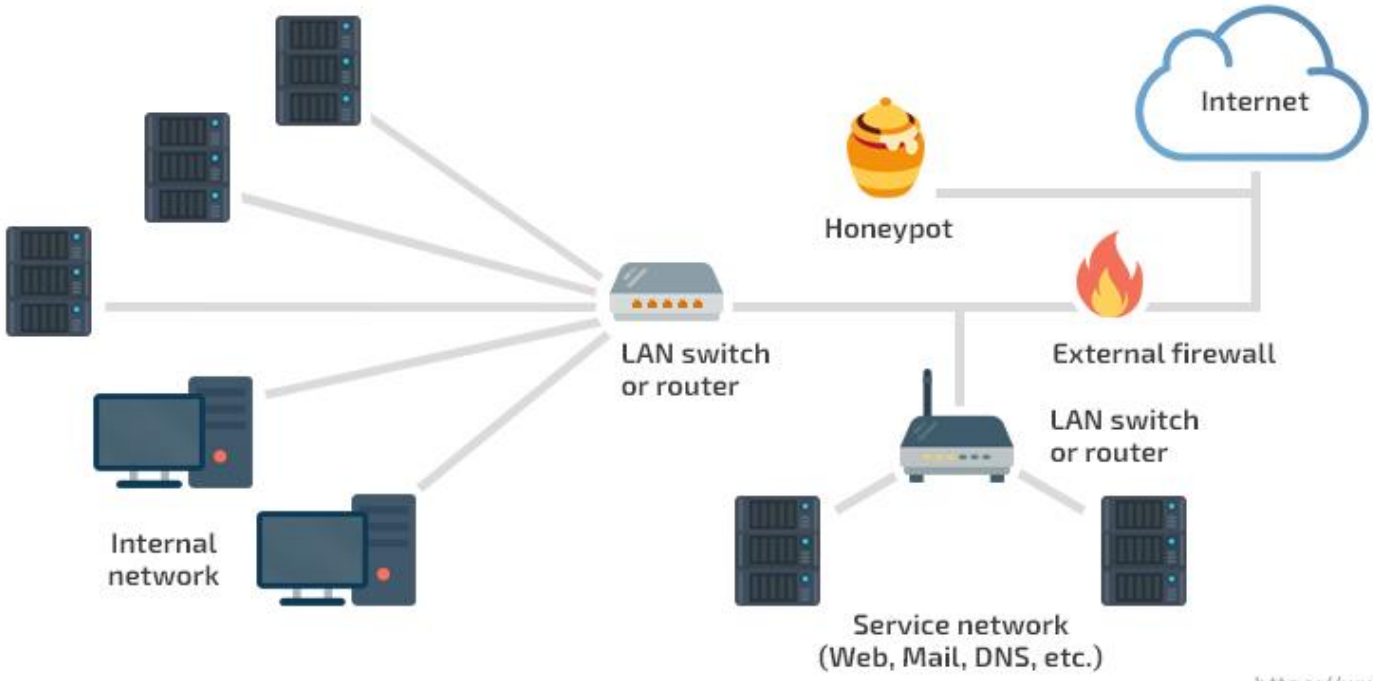
- The agent captures each audit record produced by the native audit collection system.
- A filter is applied that retains only those records that are of security interest.
- These records are reformatted into a standardized format referred to as the host audit record (HAR).
- A template-driven logic module analyzes the records for suspicious activity.
- When suspicious activity is detected, an alert is sent to the central manager.

- The LAN monitor agent audits host-host connections, services used, and volume of traffic.
- It searches for significant events, such as sudden changes in network load, the use of security-related services, and network activities such as *rlogin*.

Honeypots

- decoy systems to lure attackers away from critical systems.
  - Divert the attacker from accessing critical systems
  - to collect information of their activities
  - to encourage attacker to stay on system so administrator can respond
- are filled with fabricated information
- instrumented to collect detailed information on attackers activities.

HONEYPOT DEPLOYMENT



DR MAHALINGAM MCET COLLEGE OF ENGINEERING AND TECHNOLOGY

THANK YOU

Firewalls

Cryptography and Network security,Fifth Edition

by William Stallings

Course outcome:

Identify an appropriate security system to provide system level security.

Learning Outcome:

Explain the measures to protect the system against the attacks.

Specific Outcome:

Explain the effective means of firewall protecting the system

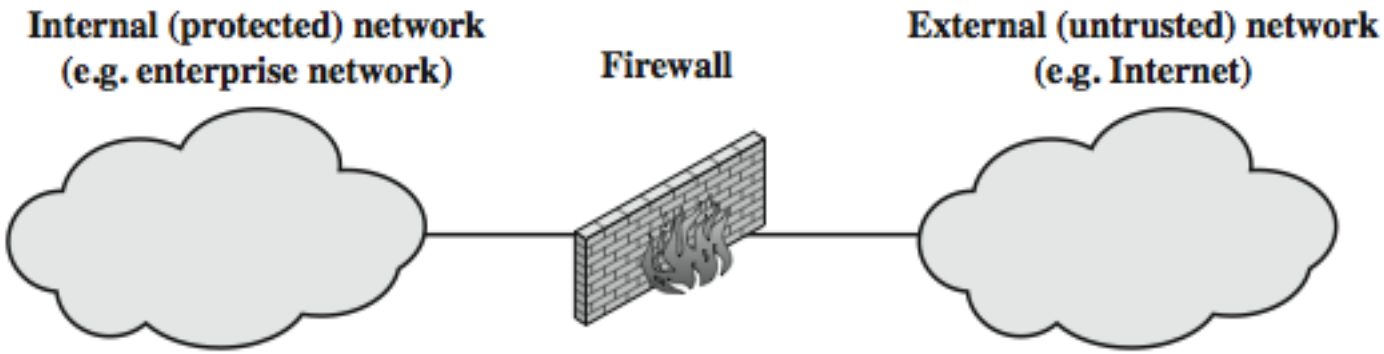
Introduction

- seen evolution of information systems
- now everyone want to be on the Internet
- and to interconnect networks
- has persistent security concerns
  - can't easily secure every system in org
- typically use a **Firewall**
- to provide **perimeter defence**
- as part of comprehensive security strategy

What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- provide NAT & usage monitoring
- implement VPNs using IPSec
- must be immune to penetration

What is a Firewall?



Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against access via WLAN
  - if improperly secured against external use
- cannot protect against malware imported via laptop, PDA, storage infected outside

types of firewalls

Have three common types of firewalls:

- Packet filters
- Application-level gateways
- Circuit-level gateways.

Firewalls – Packet Filters

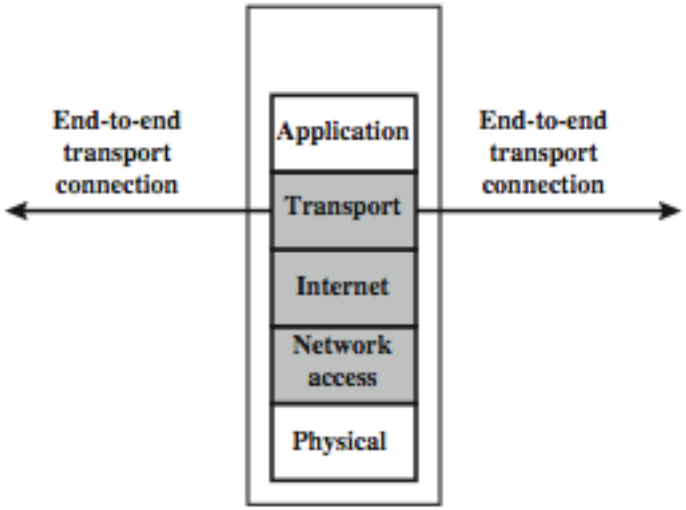
- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet to forward or discard the packet
- simplest, fastest firewall component
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules(src & dest IP addresses, ports, transport protocol & interface)
- hence restrict access to services (ports)

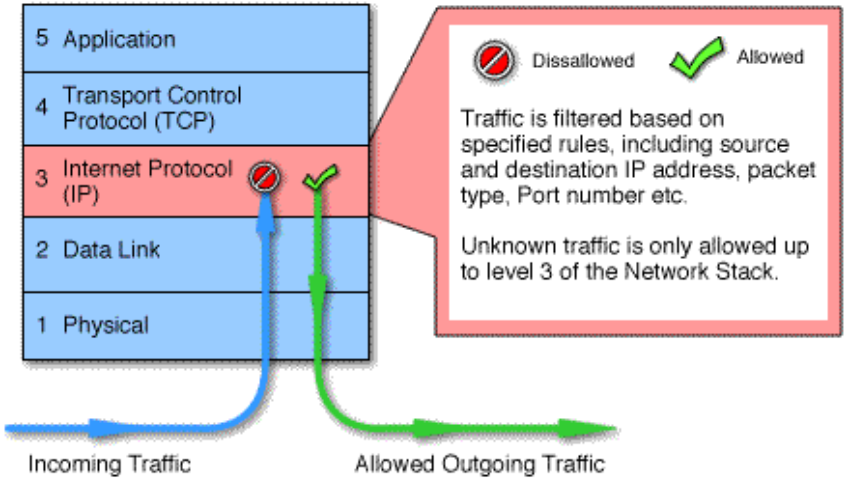
- Some advantages are simplicity, transparency & speed.
- If there is no match to any rule, then one of two default policies are applied:

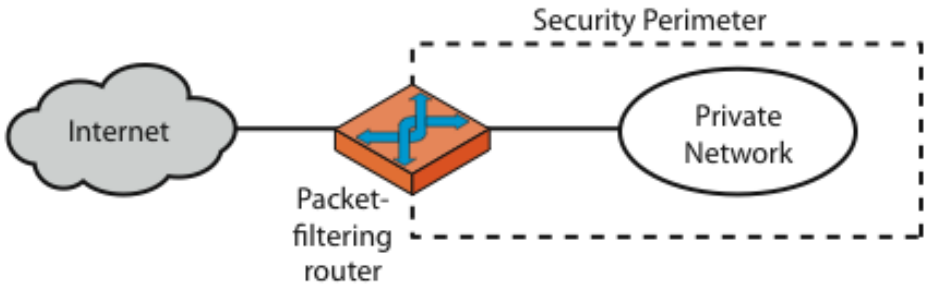
  ❖• that which is not expressly permitted is prohibited (default action is discard packet), conservative policy

  ❖• that which is not expressly prohibited is permitted (default action is forward packet), permissive policy
- Firewall policies allow you to block or allow certain types of network traffic not specified in a policy exception.

Firewalls – Packet Filters







(a) Packet-filtering router

Firewalls – Packet Filters

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Attacks on Packet Filters

- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- source routing attacks
  - attacker sets a route other than default
  - block source routed packets
- tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check

- **Stateless firewalls(Traditional** Packet Filters) are some of the oldest firewalls on the market and have been around for almost as long as the web itself. The purpose of stateless firewalls is to protect computers and networks

Firewalls – Stateful Packet Filters

- traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- stateful packet filters address this need
- they examine each IP packet in context
  - keep track of client-server sessions
  - check each packet validly belongs to one
- hence are better able to detect bogus packets out of context
- may even inspect limited application data

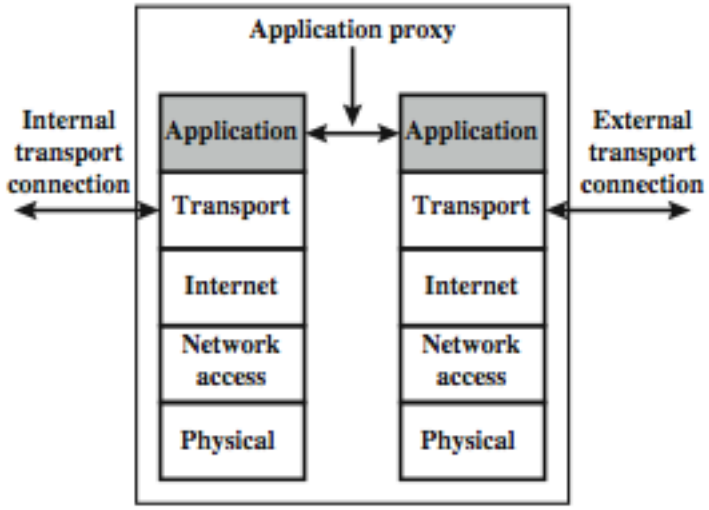
- A stateful packet inspection firewall records information about TCP connections.
- Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking.
- Some even inspect limited amounts of application data for some well-known protocols like FTP, IM and SIPS commands, in order to identify and track related connections.

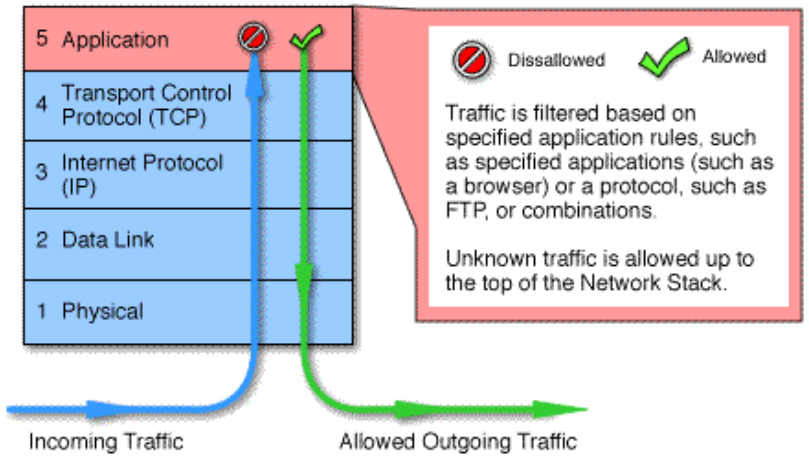
Firewalls - Application Level Gateway (or Proxy)

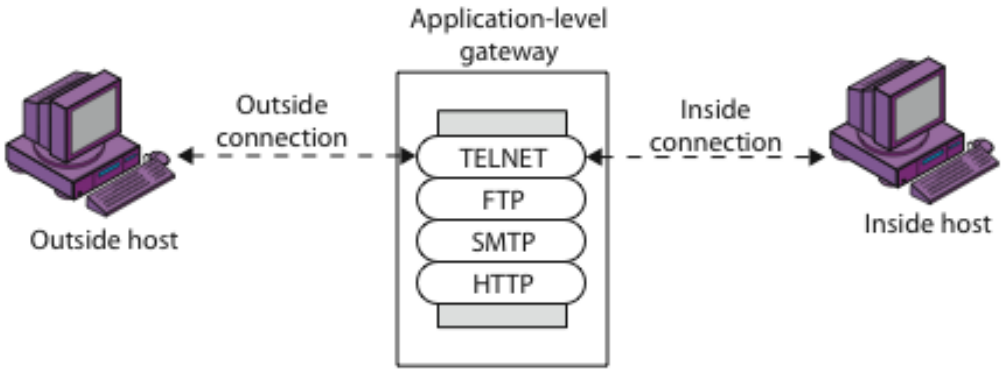
- have application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
  - can log / audit traffic at application level
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

Firewalls - Application Level Gateway (or Proxy)







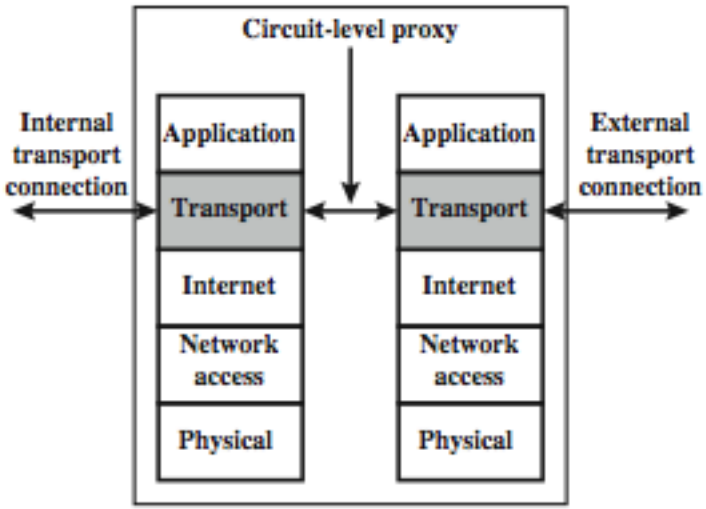
(b) Application-level gateway

Firewalls - Circuit Level Gateway

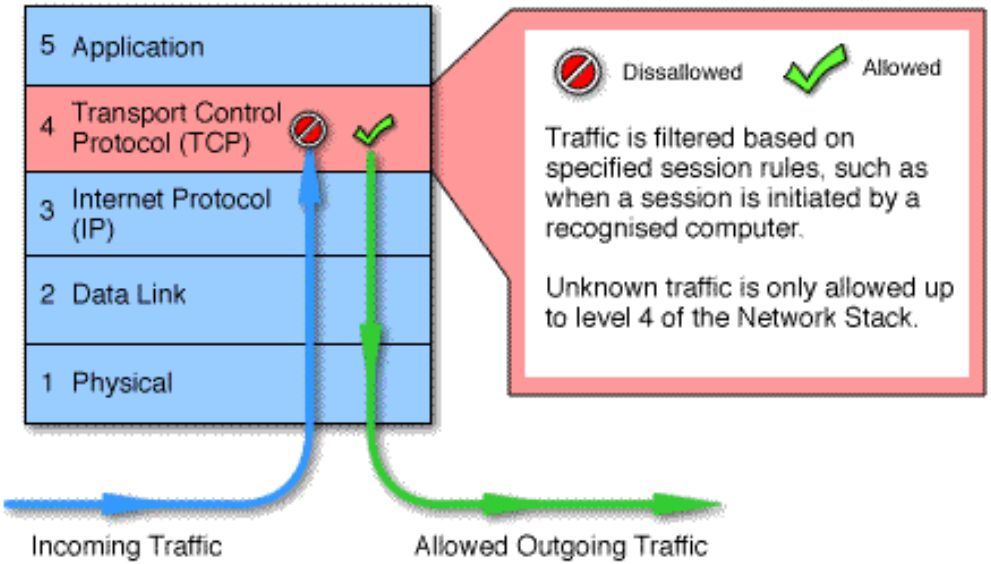
- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- SOCKS is commonly used

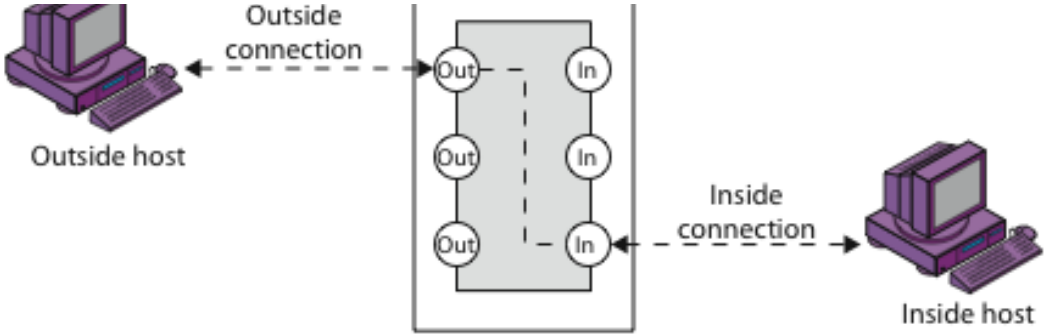
(**SOCKS**, which stands for Socket Secure, is a network protocol that facilitates communication with servers through a firewall by routing network traffic to the actual server on behalf of a client)

Firewalls - Circuit Level Gateway



(e) Circuit-level proxy firewall





(c) Circuit-level gateway

Bastion Host

- highly secure host system
- runs circuit / application level gateways
- or provides externally accessible services
- potentially exposed to "hostile" elements
- hence is secured to withstand this
  - hardened O/S, essential services, extra auth
  - proxies small, secure, independent, non-privileged
- may support 2 or more net connections
- may be trusted to enforce policy of trusted separation between these net connections

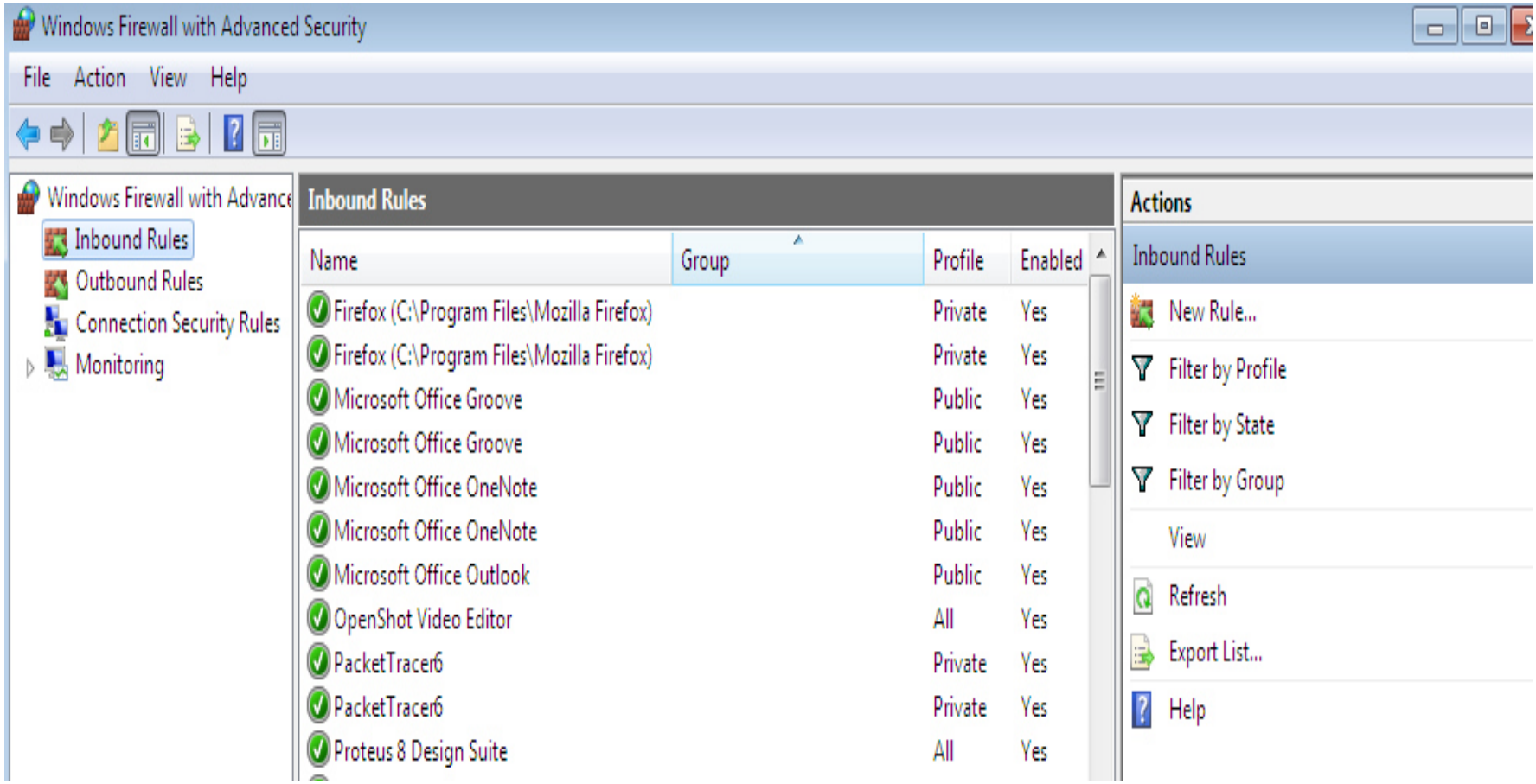
Host-Based Firewalls

- s/w module used to secure individual host
  - available in many operating systems
  - or can be provided as an add-on package
- often used on servers
- advantages:
  - can tailor filtering rules to host environment
  - protection is provided independent of topology
  - provides an additional layer of protection

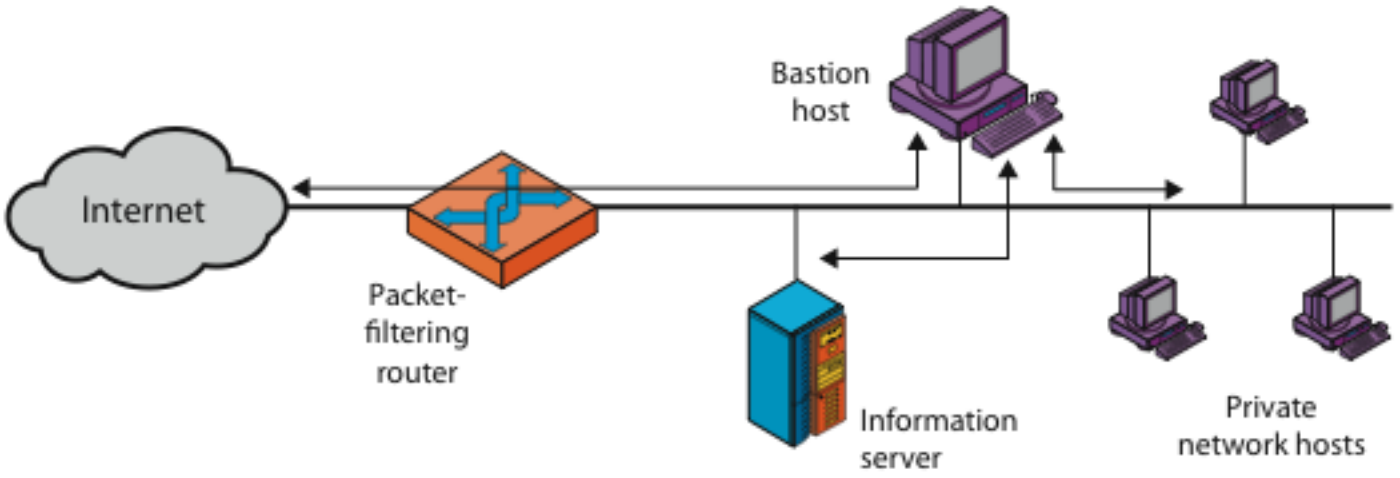
Personal Firewalls

- controls traffic between PC/workstation and Internet or enterprise network
- a software module on personal computer
- or in home/office DSL/cable/ISP router
- typically much less complex than other firewall types
- primary role to deny unauthorized remote access to the computer
- and monitor outgoing activity for malware

Personal Firewalls

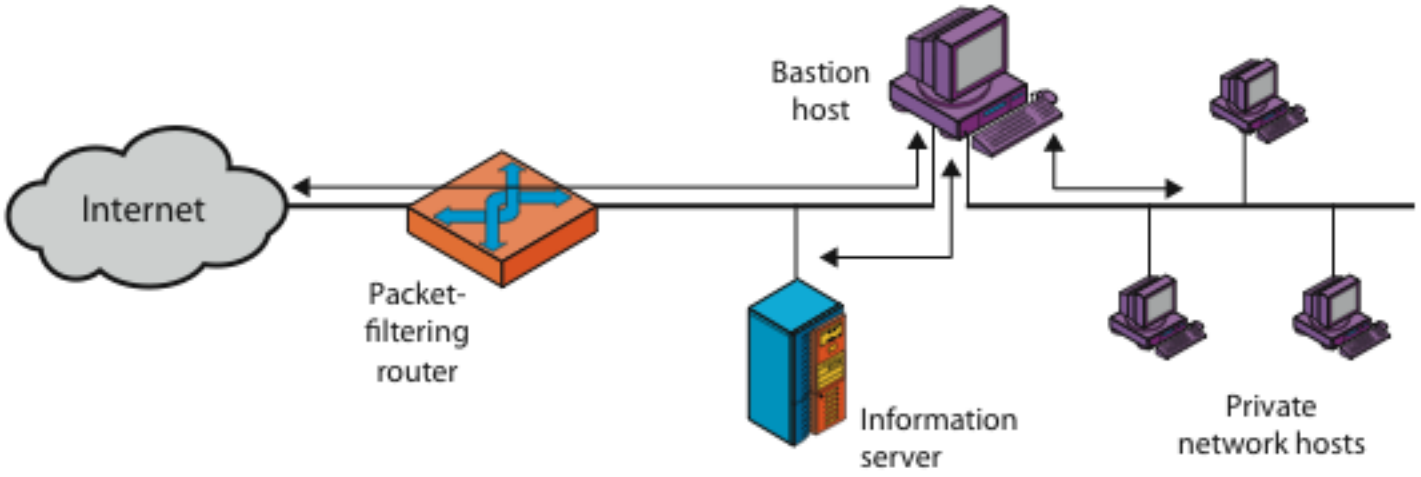


Firewall Configurations



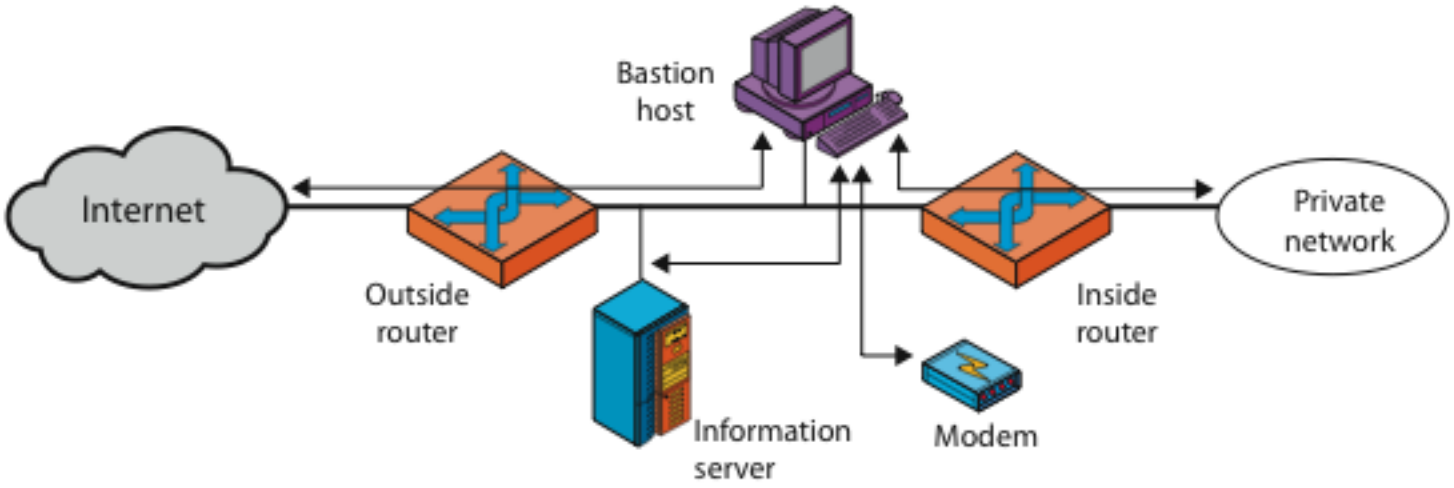
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations



(b) Screened host firewall system (dual-homed bastion host)

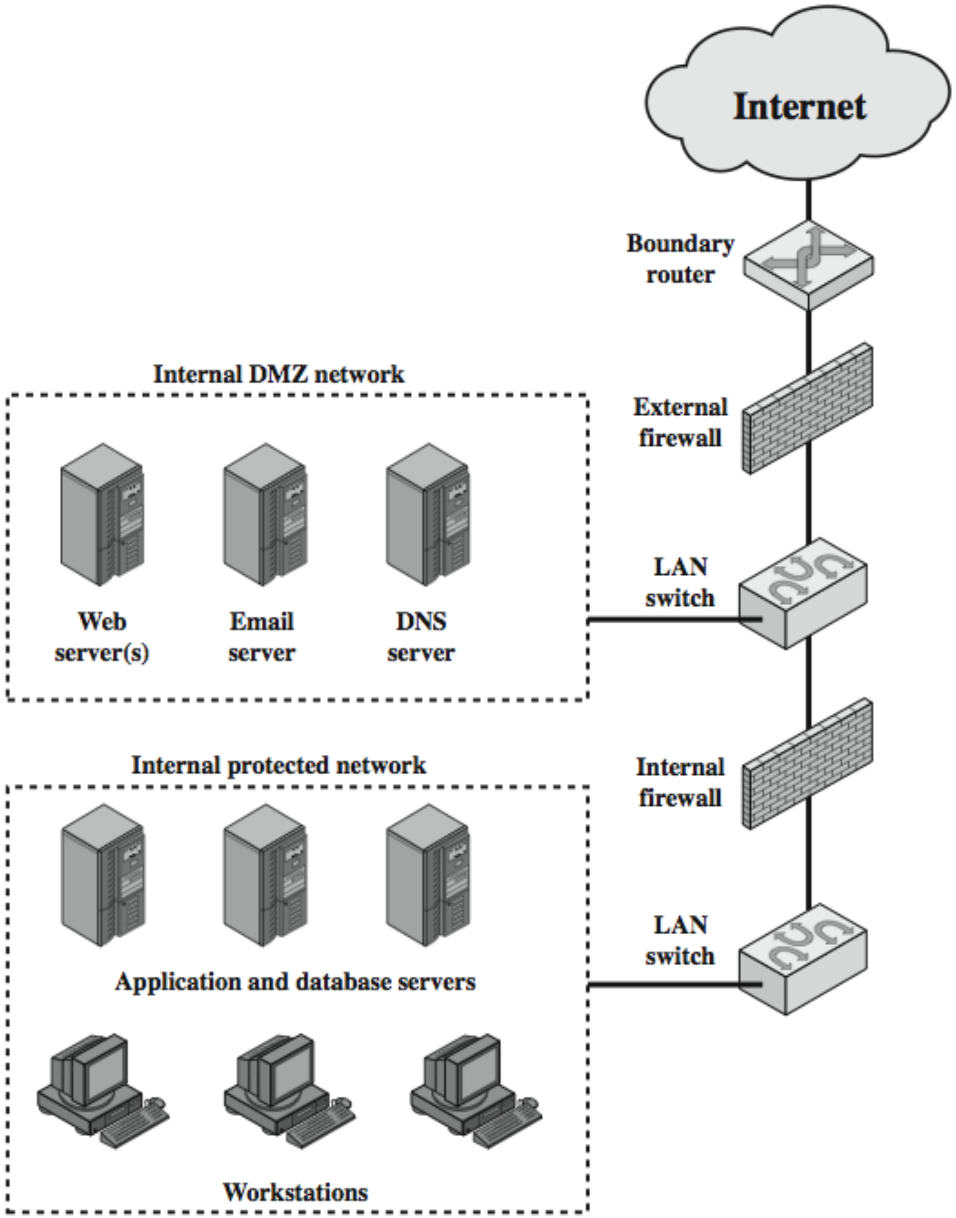
Firewall Configurations



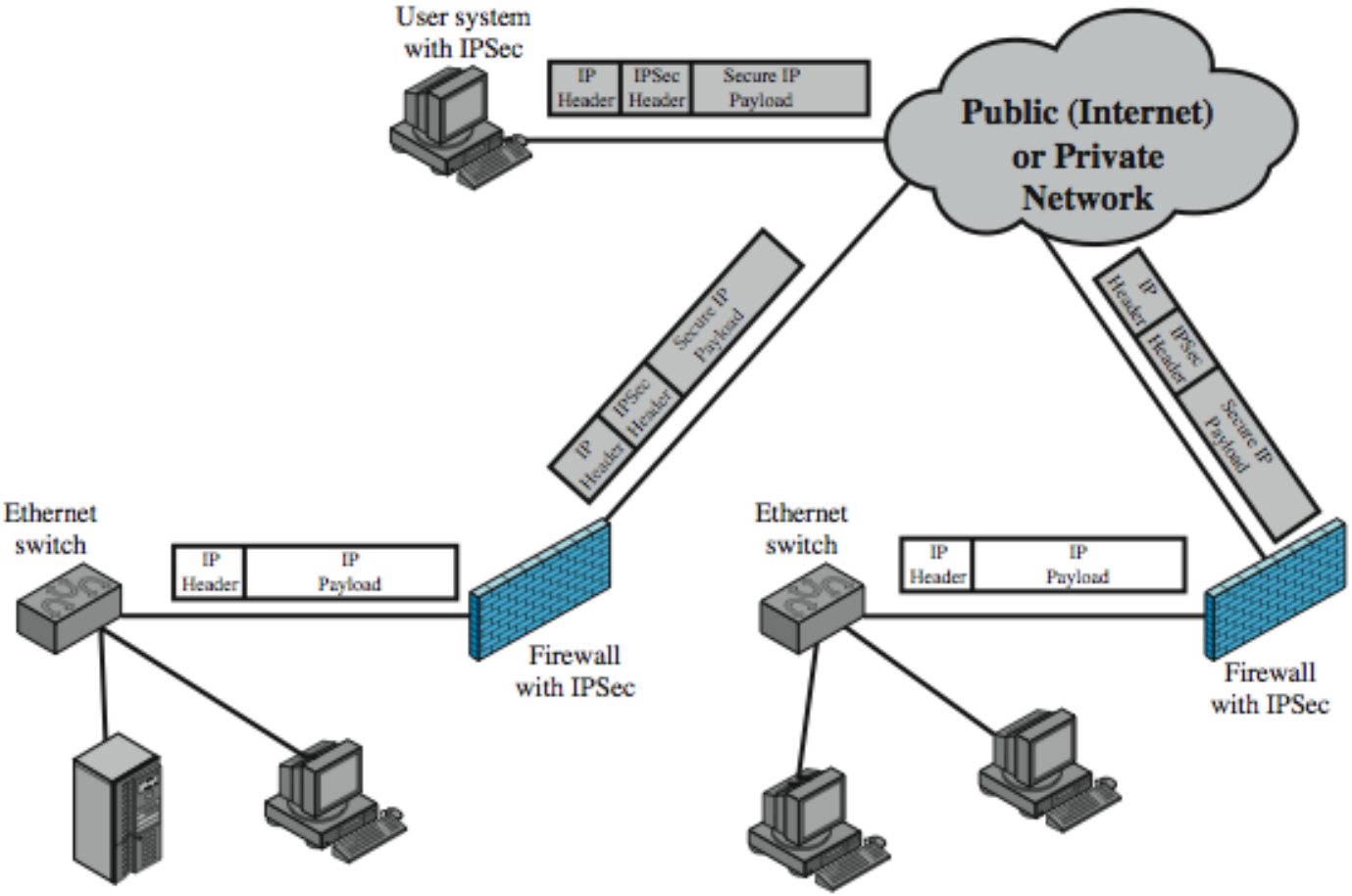
(c) Screened-subnet firewall system

DMZ Networks

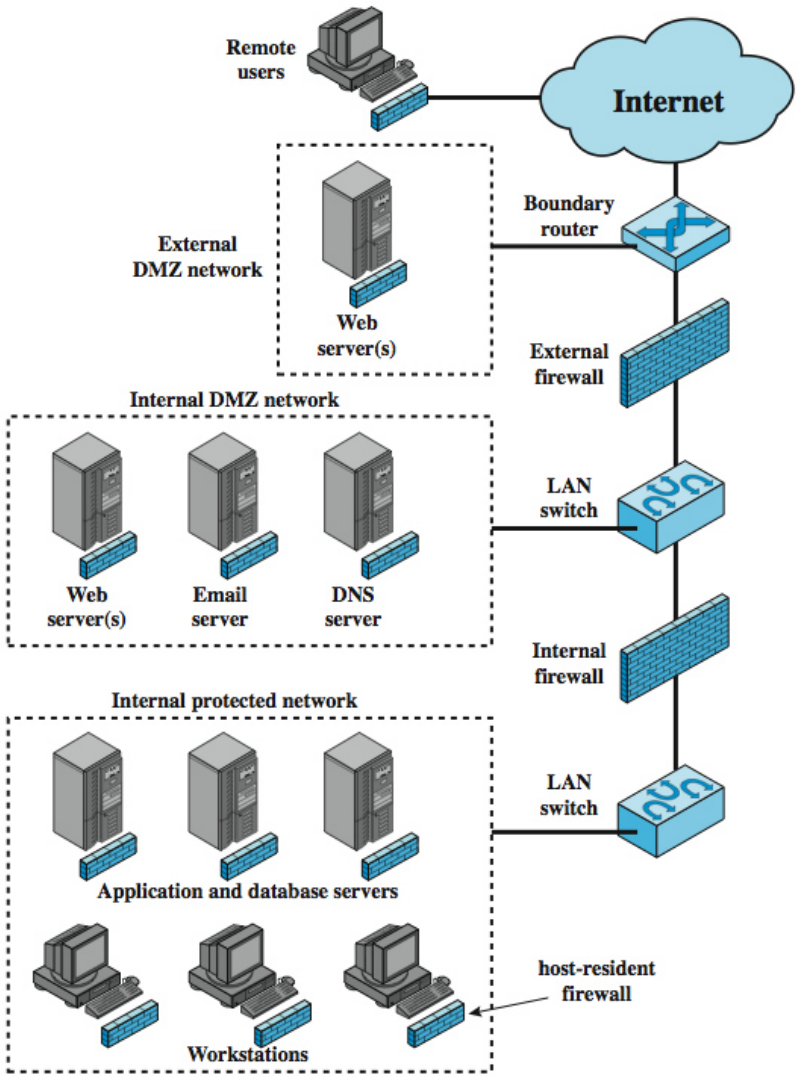
demilitarized zone



Virtual Private Networks



Distributed Firewalls



Summary of Firewall Locations and Topologies

- host-resident firewall
- screening router
- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed firewall configuration

DR MAHALINGAM
MCET
COLLEGE OF ENGINEERING AND TECHNOLOGY
Enlightening Technical Minds

THANK YOU

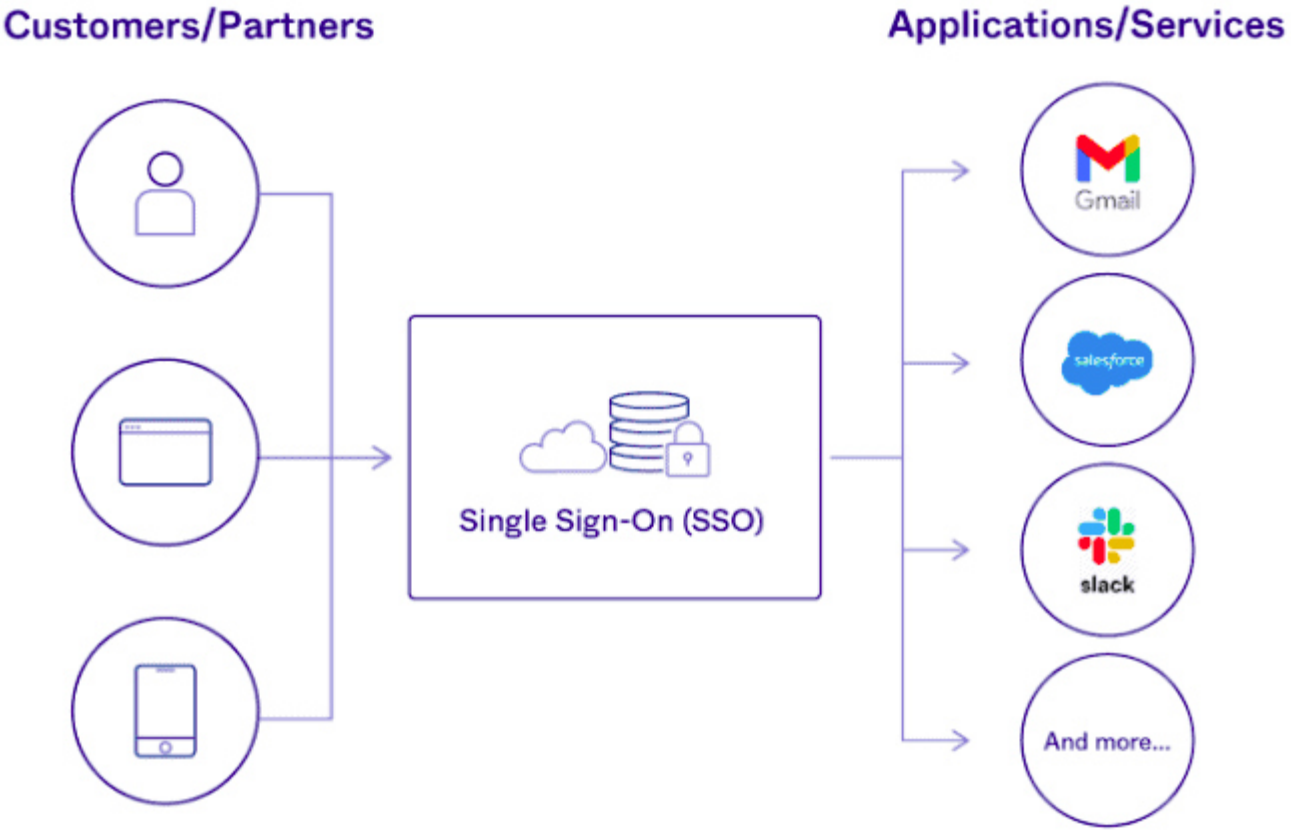
SINGLE SIGN ON (SSO)

Presented by

Abdul Rahman . M
Pranoove . K
Aditya Sagar . P
Suhita . S
Pavithra . M
Sureka . N

What is Single Sign On (SSO)?

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

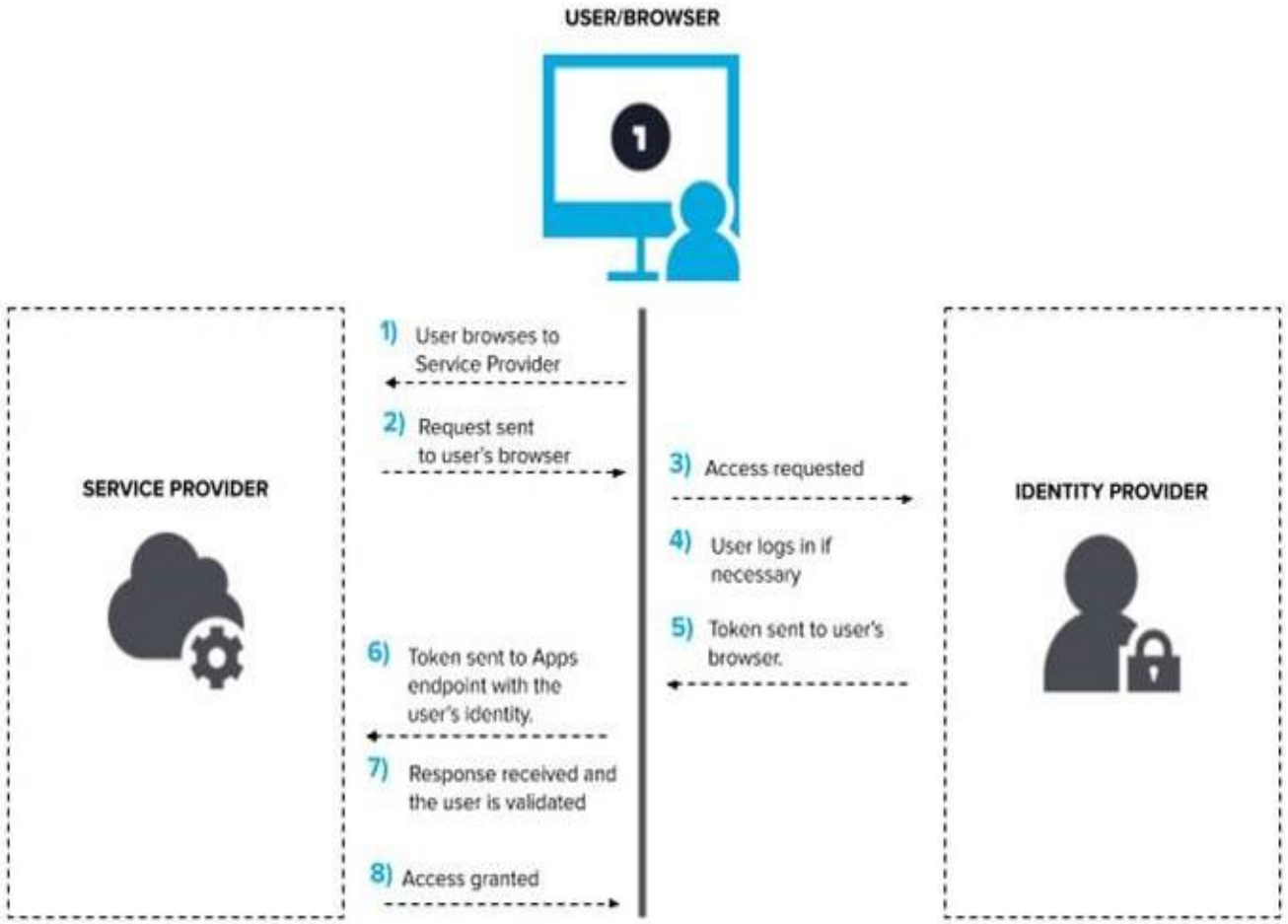

Customers/Partners
Applications/Services
Single Sign-On (SSO)
Gmail
salesforce
slack
And more...

How does an SSO works?

- SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider, like OneLogin.
- This trust relationship is often based upon a certificate that is exchanged between the identity provider and the service provider.
- This certificate can be used to sign identity information that is being sent from the identity provider to the service provider so that the service provider knows it is coming from a trusted source

How does an SSO works?

- In SSO, this identity data takes the form of tokens which contain identifying bits of information about the user like a user's email address or a username.
- Whenever a user signs in to an SSO service, the service creates an authentication token that remembers that the user is verified.
- Any app the user accesses will check with the SSO service. The SSO service passes the user's authentication token to the app and the user is allowed in.
- If, however, the user has not yet signed in, they will be prompted to do so through the SSO service.


USER/BROWSER
1
SERVICE PROVIDER
IDENTITY PROVIDER
1) User browses to Service Provider
2) Request sent to user's browser
3) Access requested
4) User logs in if necessary
5) Token sent to user's browser.
6) Token sent to Apps endpoint with the user's identity.
7) Response received and the user is validated
8) Access granted

Authentication Tokens

- The ability to pass an authentication token to external apps and services is crucial in the SSO process. This is what enables identity verification to take place separately from other cloud services, making SSO possible.
- Authentication tokens have their own communication standards to ensure that they are correct and legitimate.
- The main authentication token standard is called SAML (Security Assertion Markup Language). Similar to how webpages are written in HTML (Hypertext Markup Language), authentication tokens are written in SAML.

Is SSO secure?

- The answer to this question is “It depends.”
- Due to how single sign-on works, the token cannot be protected with the HttpOnly cookie flag and thus can be stolen by an attacker if there is a vulnerability on the logged-out website, in order to do Session Hijacking.
- Another security issue is that if the session used for SSO is stolen (which can be protected with the HttpOnly cookie flag unlike the SSO token), the attacker can access all the websites that are using the SSO system.

SSO Configurations

Some common types of SSO configurations are:

- Kerberos based
- Security Assertion Markup Language (SAML) based
- Smart card based

Emerging configuration :

- Mobile devices as access credentials

SSO Configurations

1. Kerberos based SSO

In a Kerberos-based setup, once user credentials are provided, a ticket-granting ticket (TGT) is issued. The TGT fetches service tickets for other applications the user wants to access, without asking the user to reenter credentials.

SSO Configurations

2. Security Assertion Markup Language (SAML) based SSO

SAML is an Extensible Markup Language standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML based SSO services involve communications among the user, an identity provider that maintains a user directory and a service provider.

SSO Configurations

3. Smart card based SSO

Smart card-based SSO asks an end user to use a card holding the sign-in credentials for the first login. Once the card is used, the user does not have to reenter usernames or passwords. SSO smart cards store either certificates or passwords

SSO Configurations

Using Mobile devices as access credentials

A newer variation of single-sign-on authentication has been developed using mobile devices as access credentials. Users' mobile devices can be used to automatically log them onto multiple systems, such as building-access-control systems and computer systems, through the use of authentication methods which include OpenID Connect and SAML, in conjunction with an X.509 ITU T cryptography certificate used to identify the mobile device to an access server.

Social SSO

- Google, LinkedIn, Apple, Twitter and Facebook offer popular SSO services that enable end users to log in to third-party applications with their social media authentication credentials.
- Although social single sign-on is a convenience to users, it can present security risks because it creates a single point of failure that can be exploited by attackers.
- Many security professionals recommend end users refrain from using social SSO services because, once attackers gain control of a user's SSO credentials, they can access all other applications that use the same credentials.

SSO Vendors

Multiple vendors offer SSO products, services and features. SSO vendors include the following:

- **Rippling** enables users to sign in to cloud applications from multiple devices.
- **Avatier Identity Anywhere** is SSO for Docker container-based platforms.
- **OneLogin by One Identity** is a cloud-based identity and access management platform that supports SSO.
- **Okta** is a tool with SSO functionality. Okta also supports 2FA and is primarily used by enterprises.

Advantages of SSO

- Users need to remember and manage fewer passwords and usernames for each application.
- The process of signing on and using applications is streamlined -- no need to reenter passwords.
- The chances of phishing are lessened.
- IT_help desks are likely to see fewer complaints or trouble about passwords.
- It provides simpler administration and better administrative control.
- Eliminating multiple passwords also reduces a common source of security breaches -- users writing down their passwords

Disadvantages of SSO

- It does not address certain levels of security each application sign-on may need.
- If availability is lost, users are locked out of all systems connected to SSO.
- If unauthorized users gain access, they could access more than one application.
- It increases the negative impact in case the credentials are available to other people and misused.
- single sign-on requires an increased focus on the protection of the user credentials, and should ideally be combined with strong authentication methods like smart cards and one-time password tokens


Thank
you

DDOS ATTACK

PRESENTATION BY

K.NITHIN(19BEC009)

G.ROHITH(19BEC019)

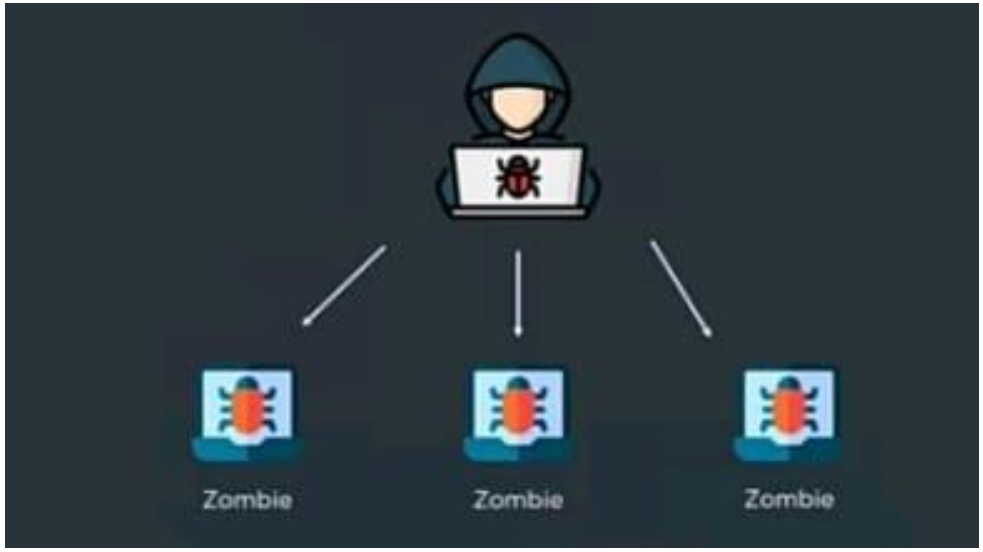
R.MANUNEETHI(19BEC025)

L.DHINA (19BEC027)

S.SATHISH KUMAR(19BEC045)

WHAT IS A DDOS ATTACK?

- Distributed Denial of Service (DDoS) Attacks
- Sending multiple requests from to a web-resource or machine
- Saturates the server capability of managing requests
- Attack is mostly carried out using a botnet of multiple devices.



DDOS ATTACKS : Analysis

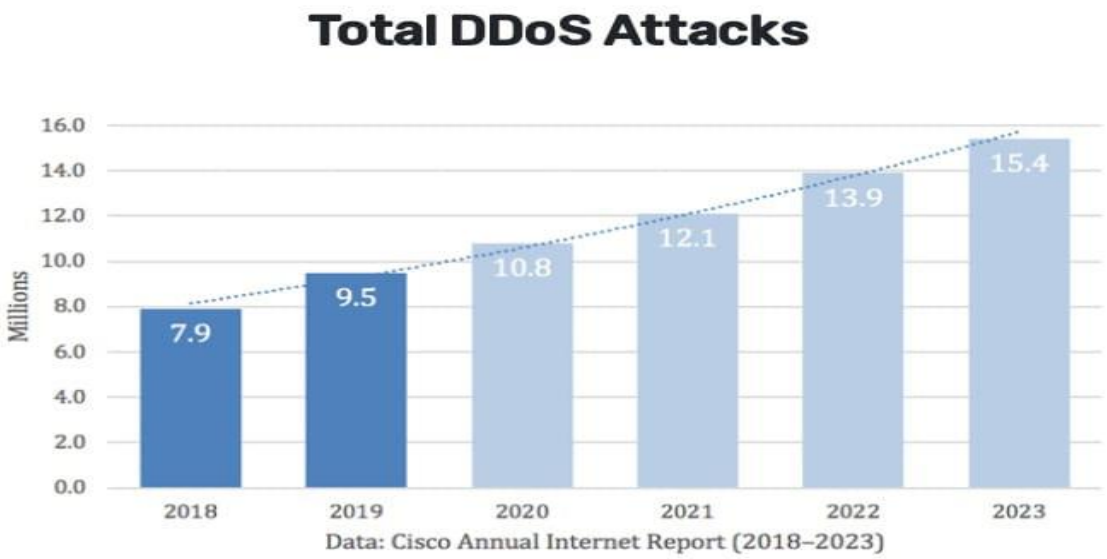


Figure 1. Cisco's analysis of DDoS total attack history and predictions.

FAMOUS DDOS ATTACKS

THE AWS DDOS ATTACK IN 2020

Amazon Web Services, the 800-pound gorilla of everything cloud computing, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.

THE GITHUB ATTACK IN 2018

On Feb. 28, 2018, GitHub, a platform for software developers, was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes. According to GitHub, the traffic was traced back to “over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints.”

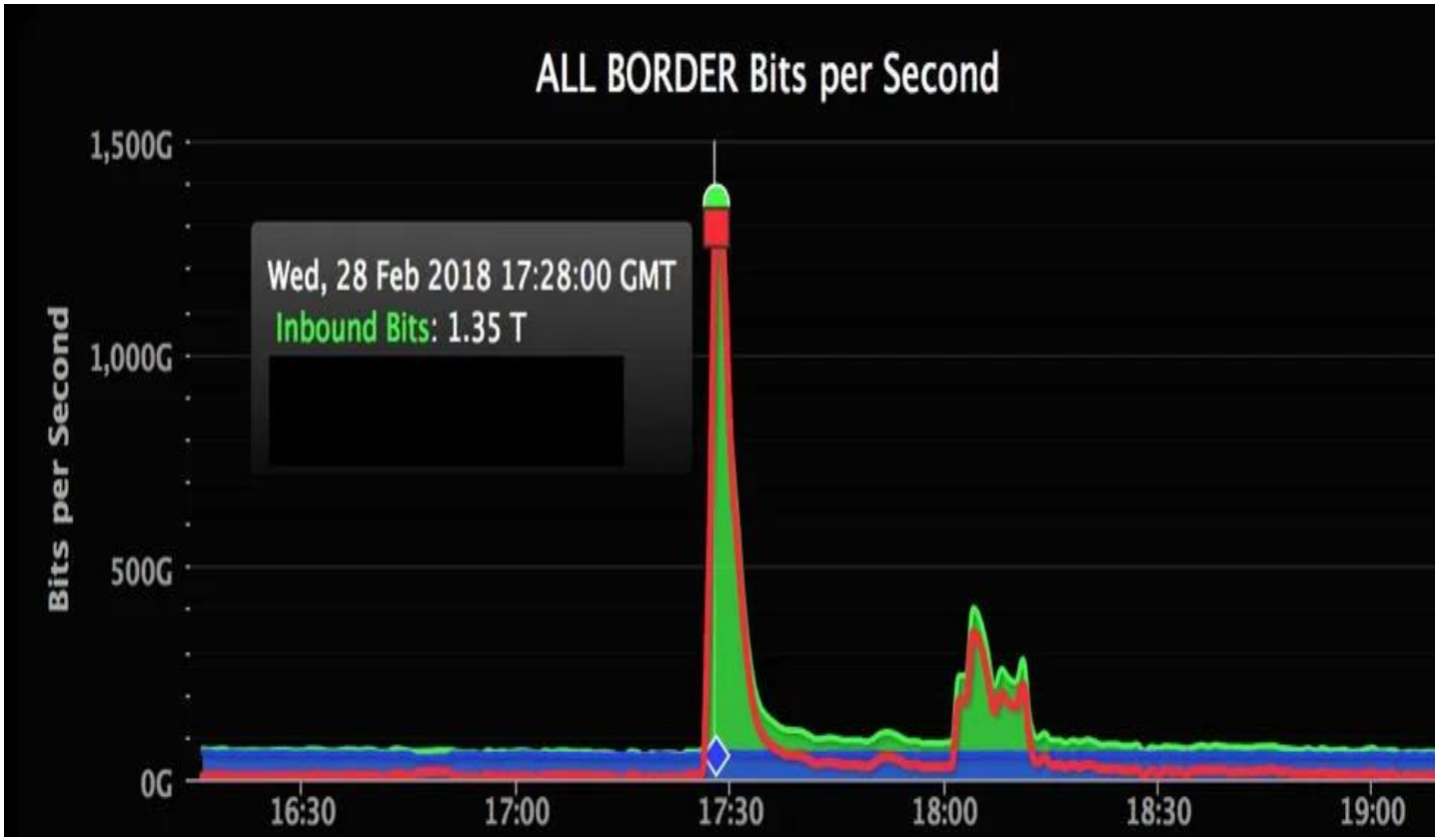
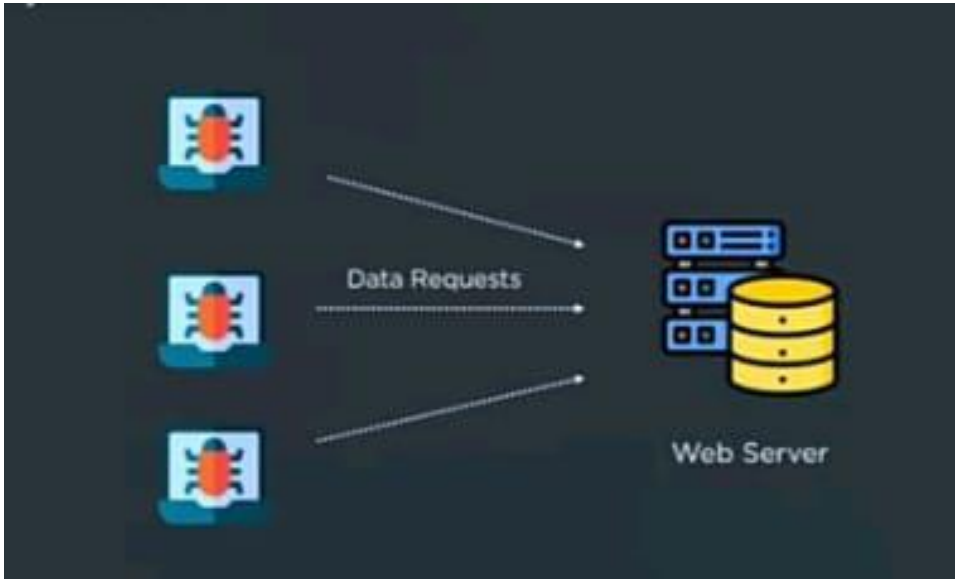


Chart of the February 2018 DDOS attack on Github .

How Does DDOS Attack Work?

A hacker must create a network of zombie bots, that can be used to attack the targeted victim when called upon, using malware infusion.

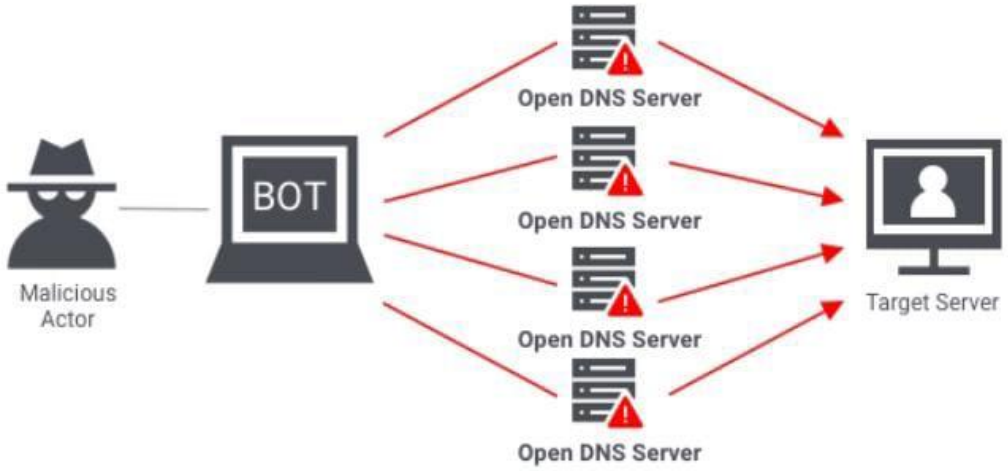


- These bots then flood the target with continuous requests that cause the server system to crash.
- The cyber attacker takes control of the devices after infecting them with malware.
- Once such a botnet has been created, specific instructions are sent remotely to each bot to carry out an attack.
- If the target is a network or web server, each bot sends requests to the server's IP address.
- Since each bot is a legitimate device on the internet, the traffic from the bot looks normal and therefore hard to separate from legitimate traffic to the server.

TYPES OF DDOS ATTACK

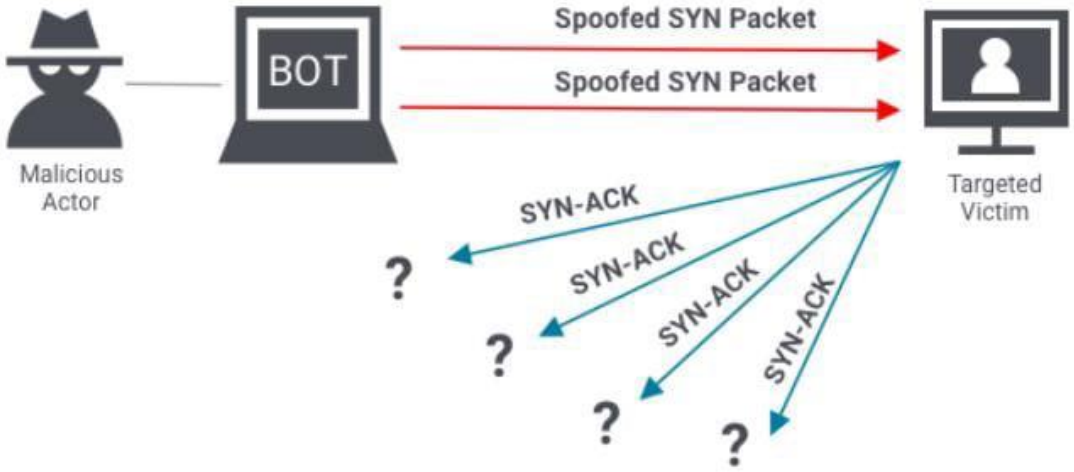
VOLUMETRIC/NETWORK BASED ATTACK

These attacks focus on consuming all the bandwidth allocated to a server. A huge volume of requests are sent to the server which warrant a reply from the server and block all the bandwidth for regular users. Examples - UDP floods, ICMP echo requests.



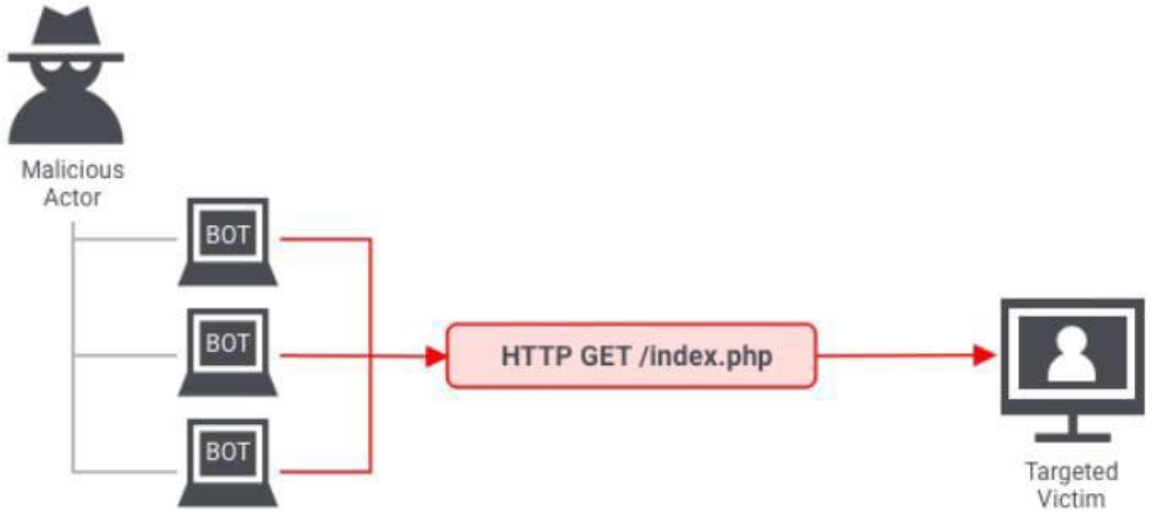
Protocol Based Attack

These consume the actual resources of a target by exhausting the firewalls and load balancers kept in place. Layers three and four of the OSI model are compromised. Example - SYN Flooding, Ping of Death.



Application Based Attack

Sophisticated attacks that crash the entire server by targeting application and OS level vulnerabilities. It can stop specific applications from delivering necessary information. Example - HTTP Flooding, BGP Hijacking



AIM OF DDOS ATTACK

- Competitive advantage of against rival business.
- Ransom demands for releasing data.
- Activist behaviour for protests and upstaging.
- The primary goal of a DoS attack is not to steal information but to slow or take down a web site.
- Most frequently, DoS attacks are carried out for profit. There are several ways to make money by staging a DoS attack.
- For instance, competitors of Amazon might find it beneficial if Amazon's service were slow or offline.

PREVENTION OF DDOS ATTACK

- Employ load balancers and firewalls.
- Detect an attack early and mitigate the damage beyond that point.
- Switch to cloud service providers like AWS and Azure
- Allocate more bandwidth to prevent clooging of data.
- Using Content delivery networks (CDNs)that have redundant servers.

VIDEO DEMONSTRATION

THANK YOU

IP SPOOFING ATTACK!

PRESENTED BY,

AKSHAYA ,KIRUTHIKA P,SIVANI ,SHANMUGA LAKSHMI,DIVIYYA SHREE I

What is spoofing?

TYPES OF IP SPOOFING

- DDOS ATTACKS
- BOTNET ATTACKS
- MAN IN THE MIDDLE ATTACKS

PREVENTION MEASURES

- Packet Filtering
- Authentication via Public Key Infrastructure
- Network Monitoring and Firewalls
- Security Training

THANK YOU!