Module 4: Network Security

- Network Security Introduction
- Firewall
- IDS
- IPSec

What is Network Security and why it is important?

- Network security is a broad term that covers a multitude of technologies, devices and processes.
- In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.
- Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect their network from the ever-growing landscape of cyber threats today.
- Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats today.
- These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations.
- For this reason, there are many network security management tools and applications in use today that address individual threats and exploits.

What is Network Security ?

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

How does Network Security Work?

- There are many layers to consider when addressing network security across an organization.
- Attacks can happen at any layer in the network security layers model, so our network security hardware, software and policies must be designed to address each area.
- Network security typically consists of three different controls: physical, technical and administrative.

Physical Network Security

- Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on.
- Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

How does Network Security Work?

Technical Network Security

- Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network.
- Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Administrative Network Security

- Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Different types of Network Security

- 1. Network Access Control
- 2. Antivirus and Antimalware Software
- 3. Firewall Protection
- 4. Virtual Private Networks

Network Access Control

- Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies
- To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices.
- Network access control (NAC) can be set at the most granular level.
- For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Antivirus and antimalware Solutions

- Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans.
- The best software not only scans files upon entry to the network but continuously scans and tracks files.

Firewall Protection

- Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network.
- Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.

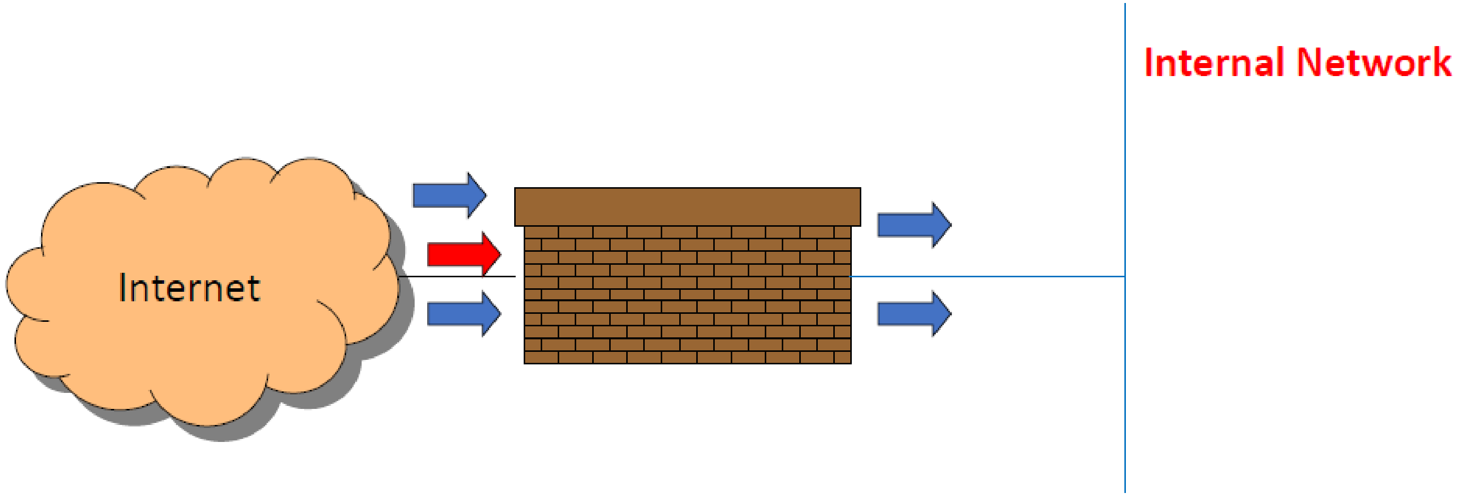
Virtual Private Network

- Virtual private networks (VPNs) create a connection to the network from another endpoint or site.
- For example, users working from home would typically connect to the organization's network over a VPN.
- Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network.

Firewall

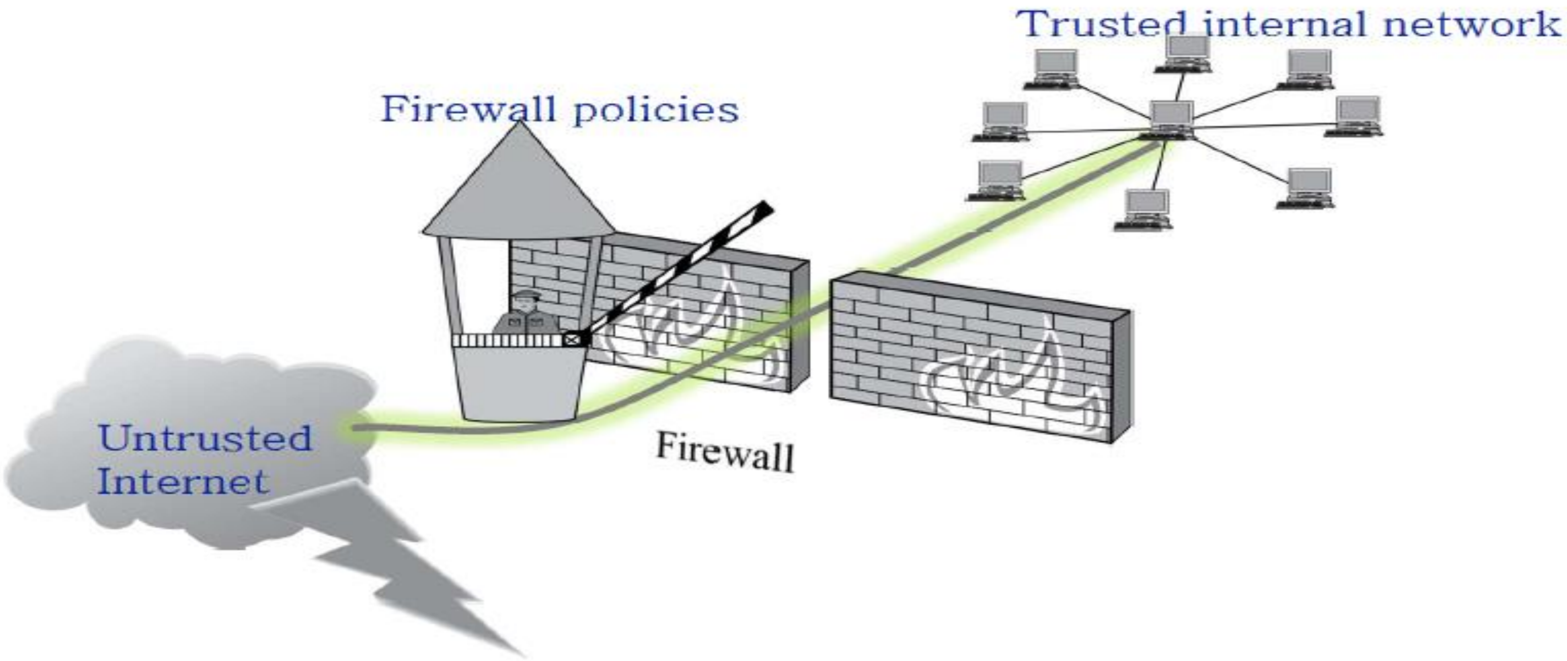
Firewall

- Interconnects two networks with differing trusts.
- Firewall inspects traffic passing through two networks
- Allows and Block traffic based on some rules
- It works like a security guard.

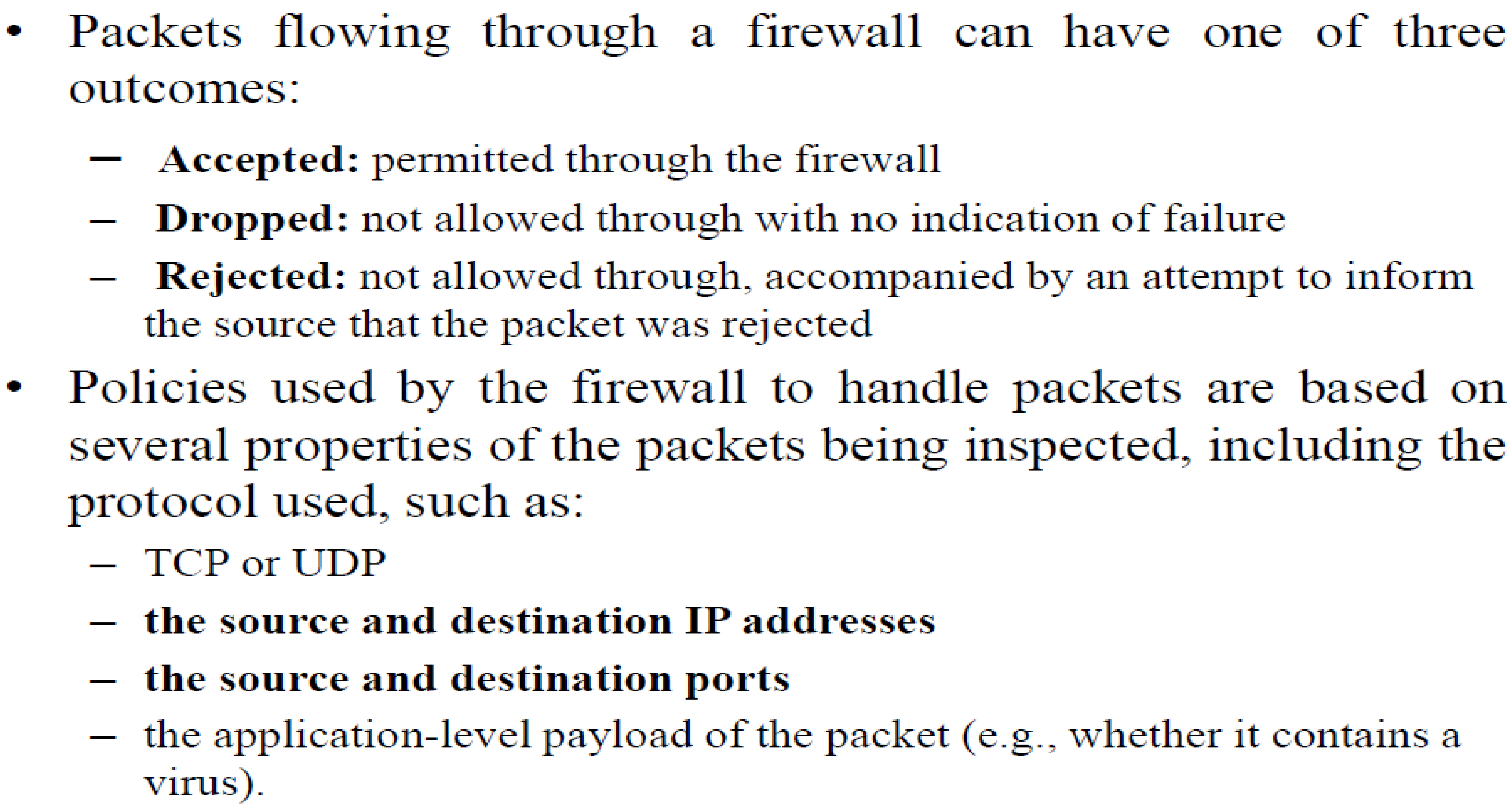


Firewall Polices

- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



Firewall Actions



- Packets flowing through a firewall can have one of three outcomes:
  - **Accepted:** permitted through the firewall
  - **Dropped:** not allowed through with no indication of failure
  - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
  - TCP or UDP
  - **the source and destination IP addresses**
  - **the source and destination ports**
  - the application-level payload of the packet (e.g., whether it contains a virus).

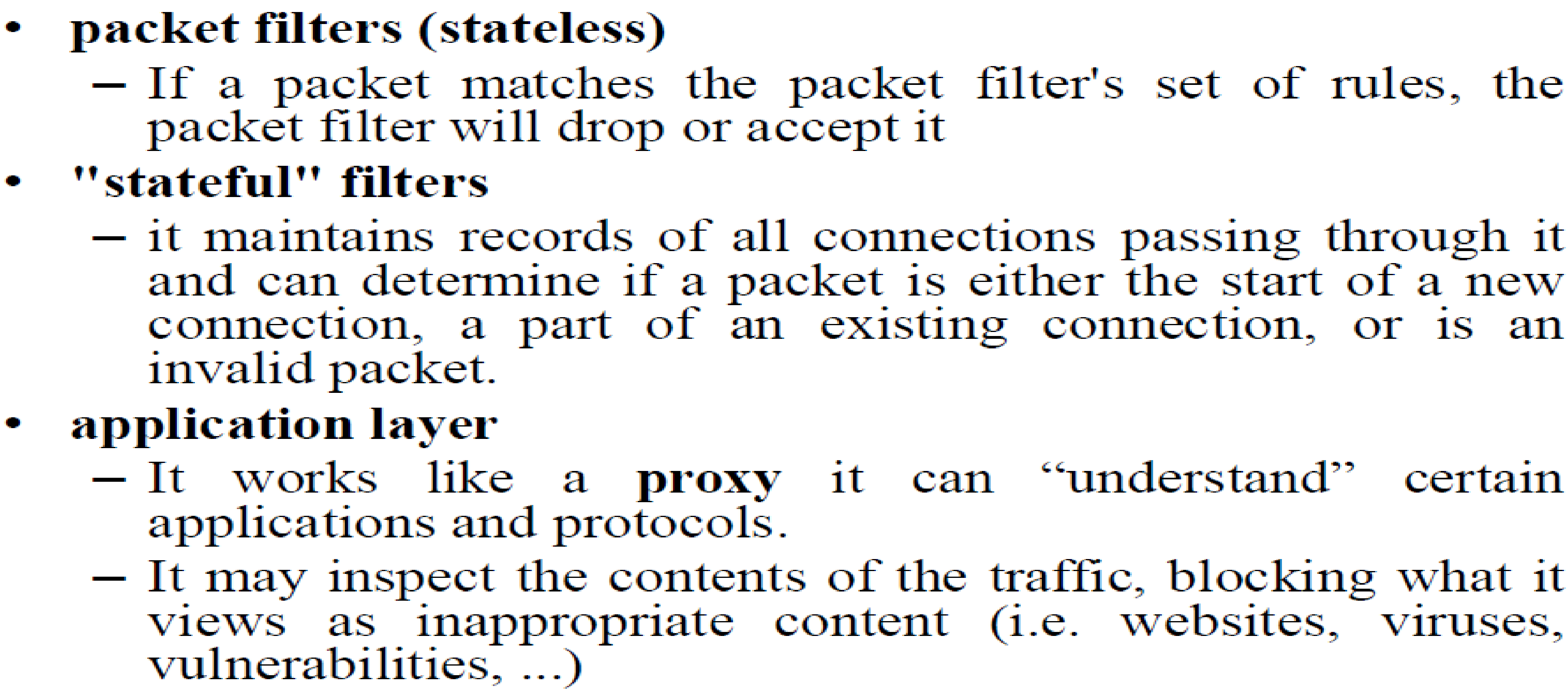
What firewalls can do and can not do?

- Firewall can not protect against insider attack.
- A firewall can take action on traffic that pass through it but it cannot do anything on traffic that does not pass through it.
- A firewall cannot protect you against complete new attacks.
- A firewall can take decision based on source IP address, destination IP address, source port number and destination port number but it can not inspect payload or data inside the packet. This may contain virus.

Blacklist and Whitelist

- Two fundamental approaches to creating firewall policies (or rulesets)
- **Blacklist** approach (default-allow)
  - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
  - Pros: flexible in ensuring that service to the internal network is not disrupted by the firewall
  - Cons: unexpected forms of malicious traffic could go through
- **Whitelist** approach (default-deny)
  - Packets are dropped or rejected unless they are specifically allowed by the firewall
  - Pros: A safer approach to defining a firewall ruleset
  - Cons: must consider all possible legitimate traffic in rulesets

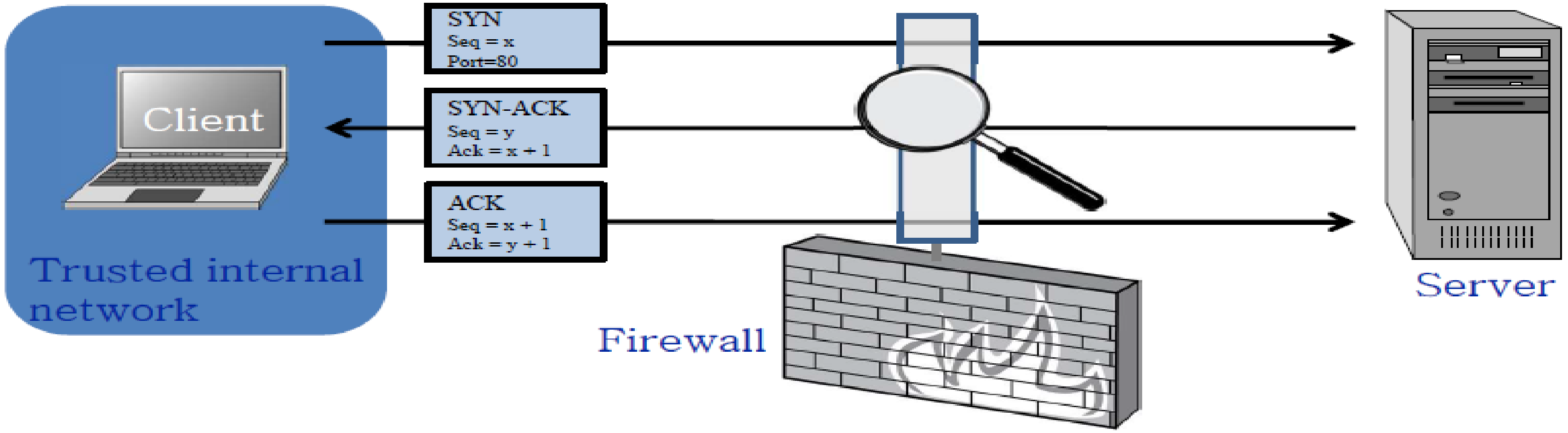
Firewall Types



- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Packet filters or Stateless Firewall

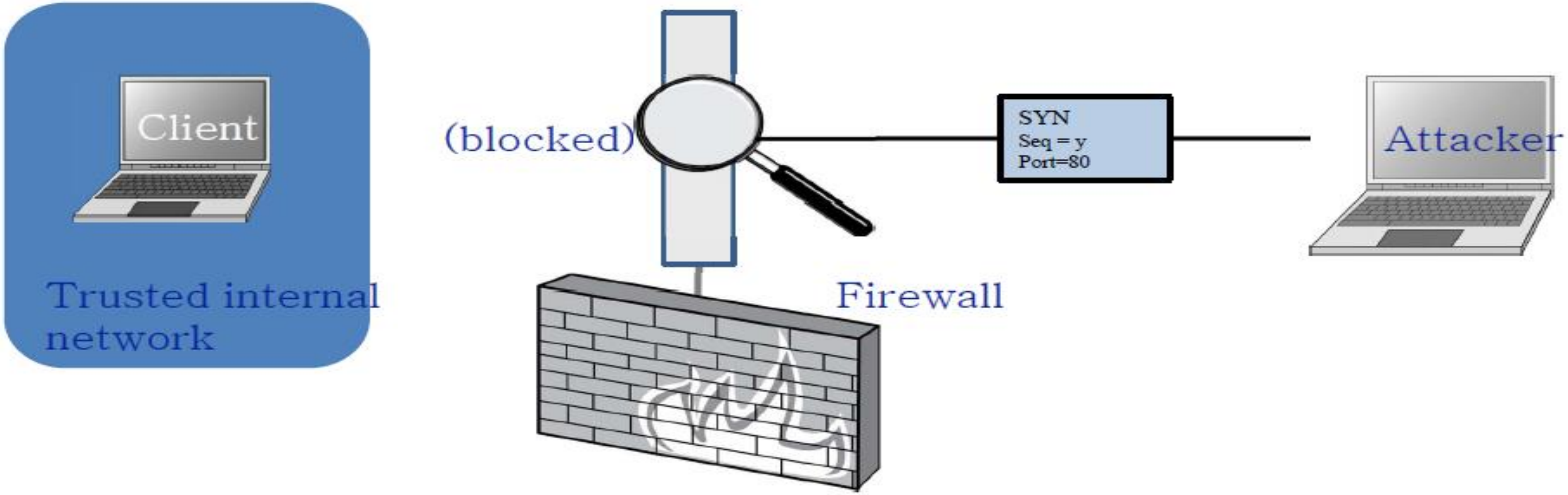
- A stateless firewall doesn’t maintain any remembered context (or “state”) with respect to the packets it is processing.
- Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

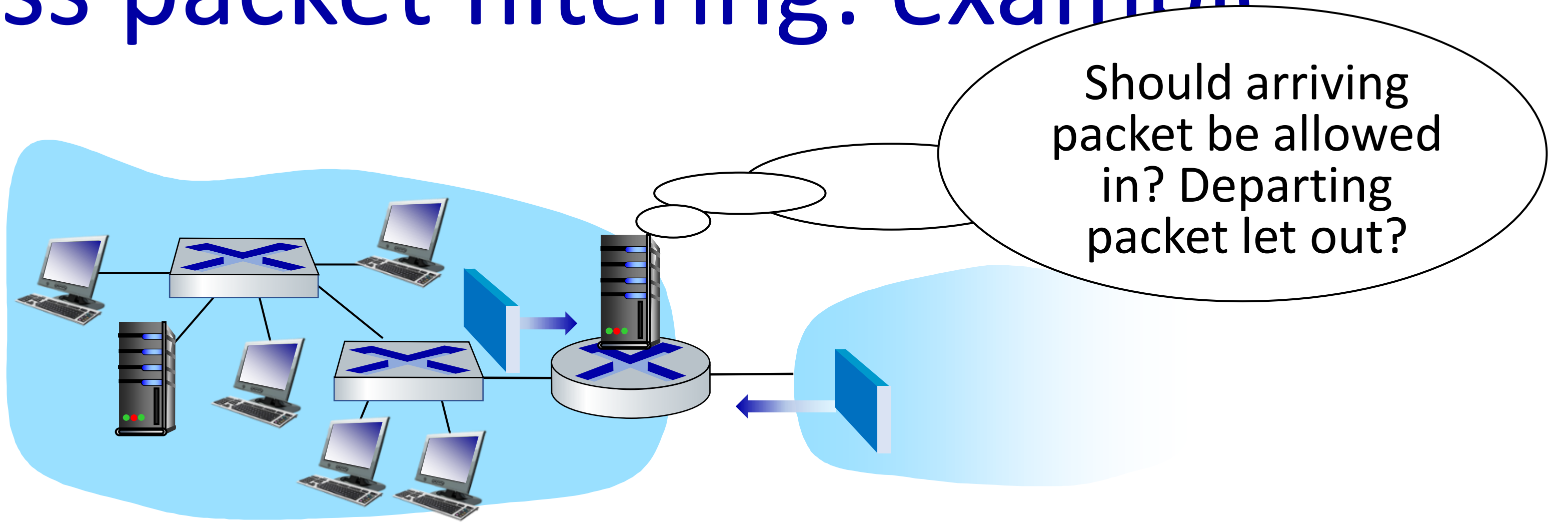
Packet filters or Stateless Firewall

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN−ACK packets, source port=80

Stateless packet filtering: example


Should arriving packet be allowed in? Departing packet let out?

- example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - result: all incoming, outgoing UDP flows and telnet connections are blocked
- example 2: block inbound TCP segments with ACK=0
  - result: prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside

Stateless packet filtering: more examples

Policy	Firewall Setting
no outside Web access	drop all outgoing packets to any IP address, port 80
no incoming TCP connections, except those for institution's public Web server only.	drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
prevent Web-radios from eating up the available bandwidth.	drop all incoming UDP packets - except DNS and router broadcasts.

Access Control Lists

ACL: Packet filters can implement rules in router with access control list (ACL)

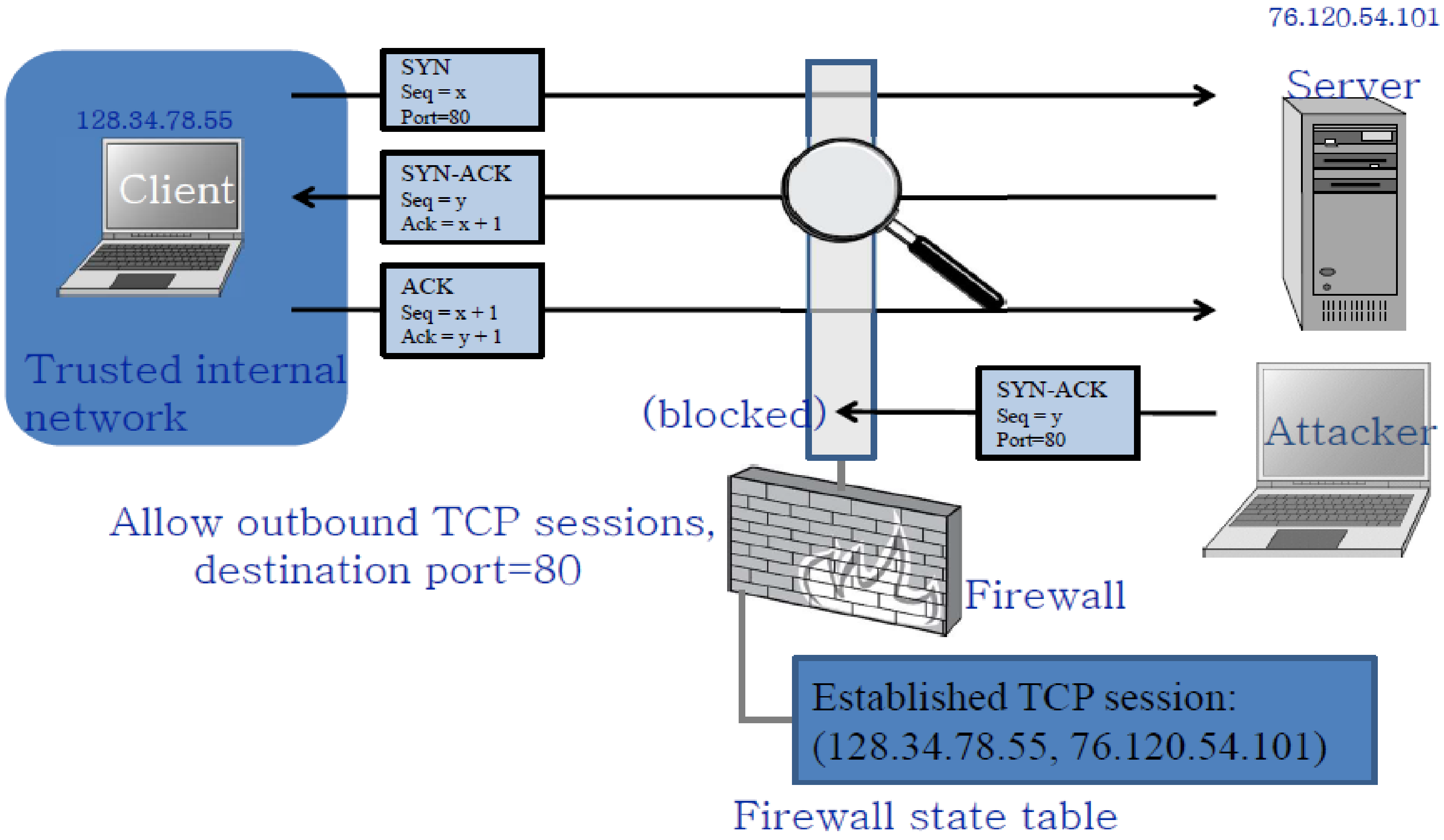
action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful Firewall

- Stateful firewalls can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Stateful Firewall

- Allow only requested TCP connections:



Stateful packet filtering

ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check connection
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	yes
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	yes
deny	all	all	all	all	all	all	

Application Firewall

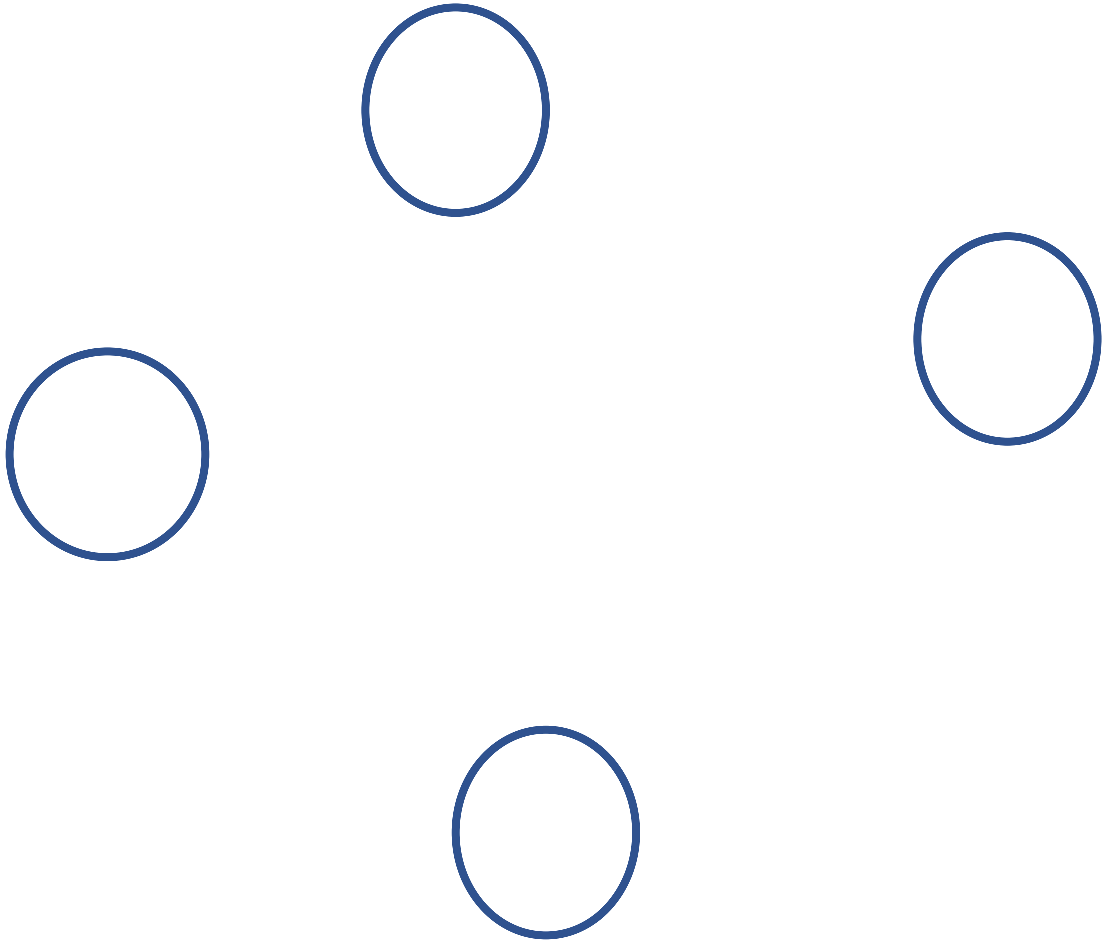
- filter packets on application data as well as on IP/TCP/UDP field

Intrusion Detection System

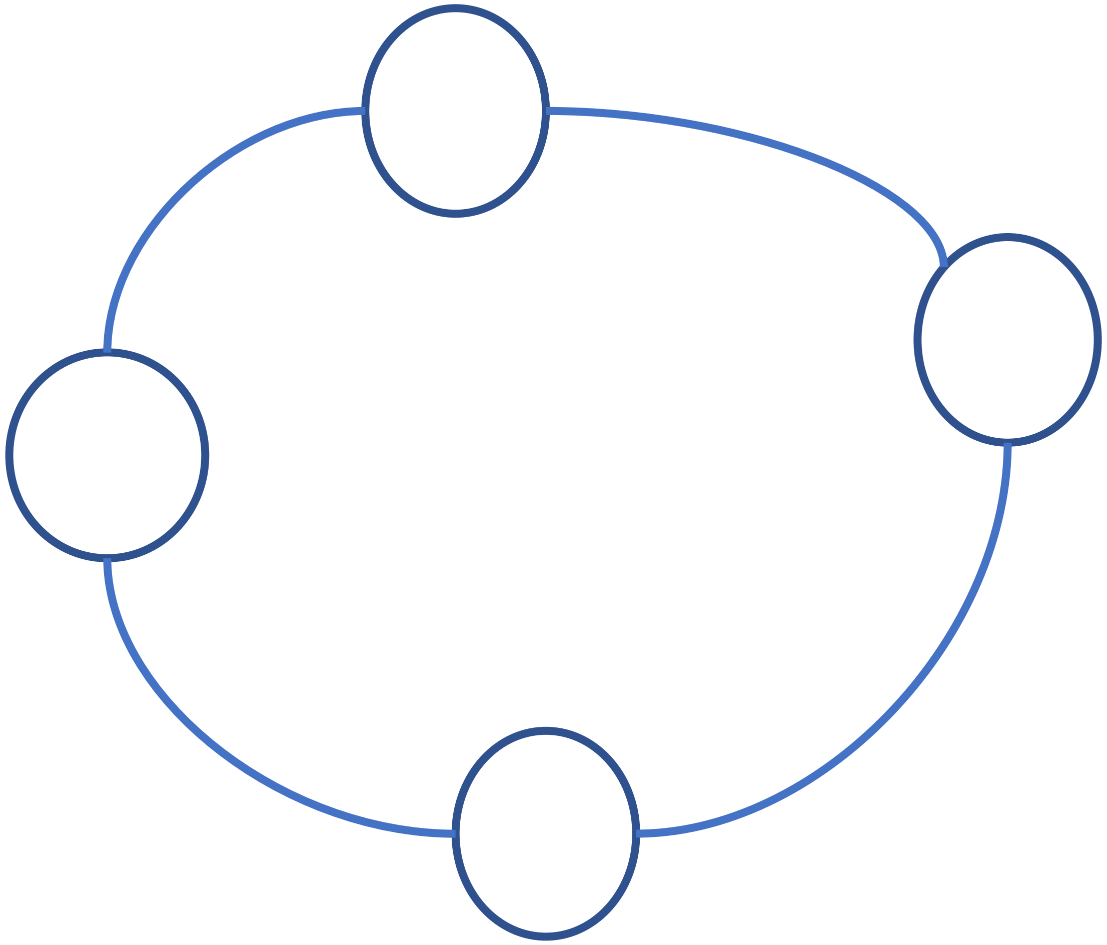
Dr. Kamalkanta Sethi
Assistant Professor

Indian Institute of Information Technology
SRICITY

Introduction to network: nodes

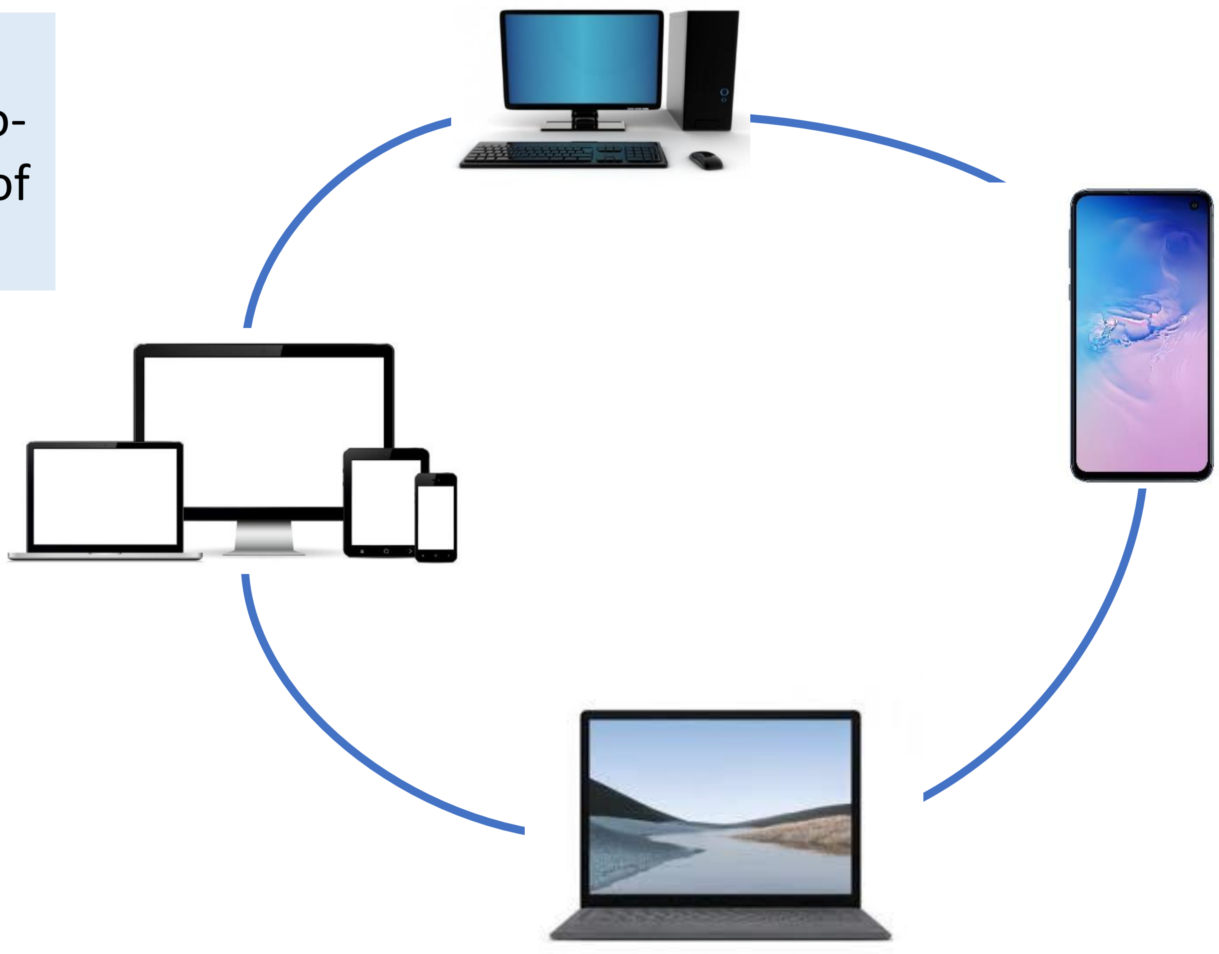


Introduction to network: nodes and vertices

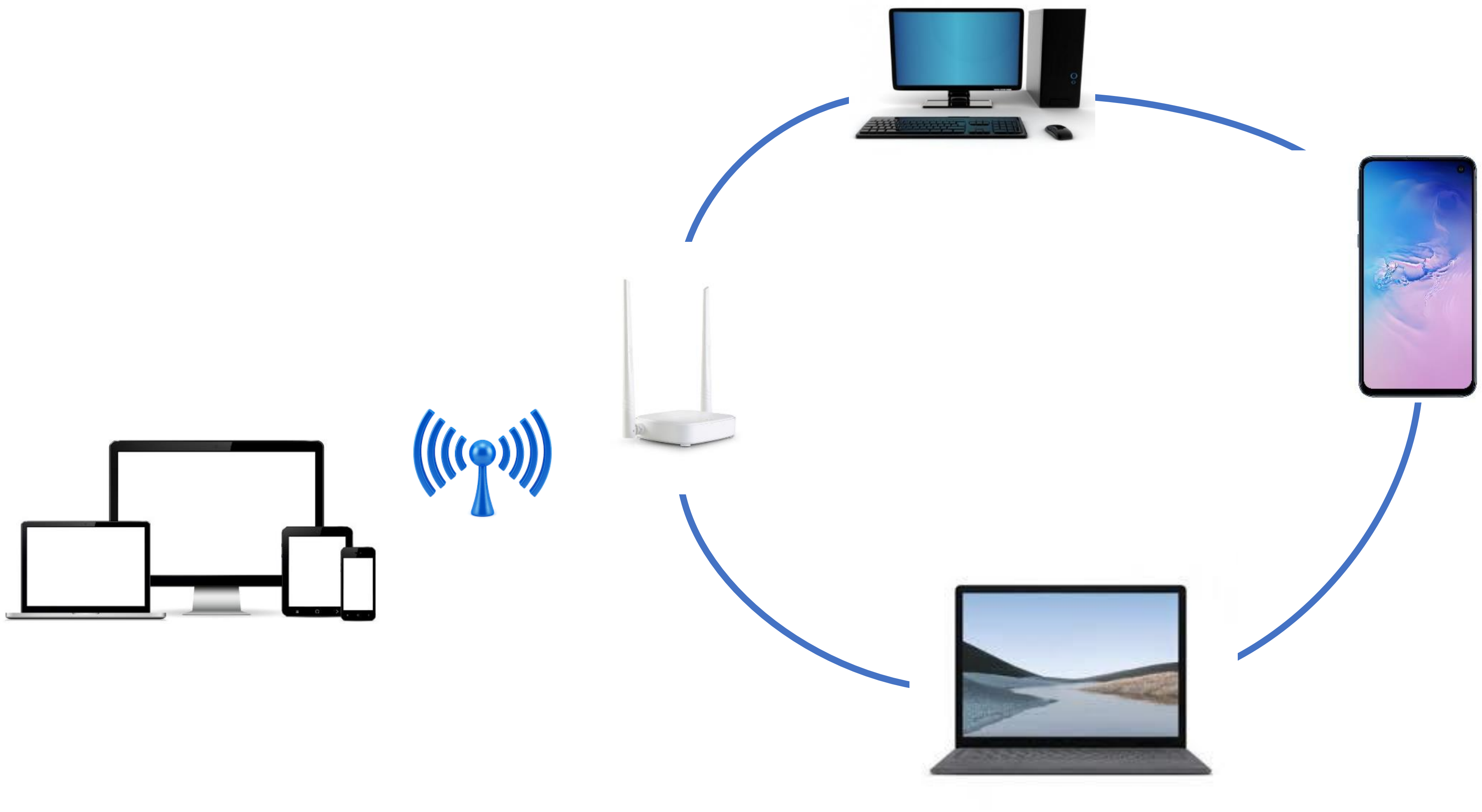


Introduction to network

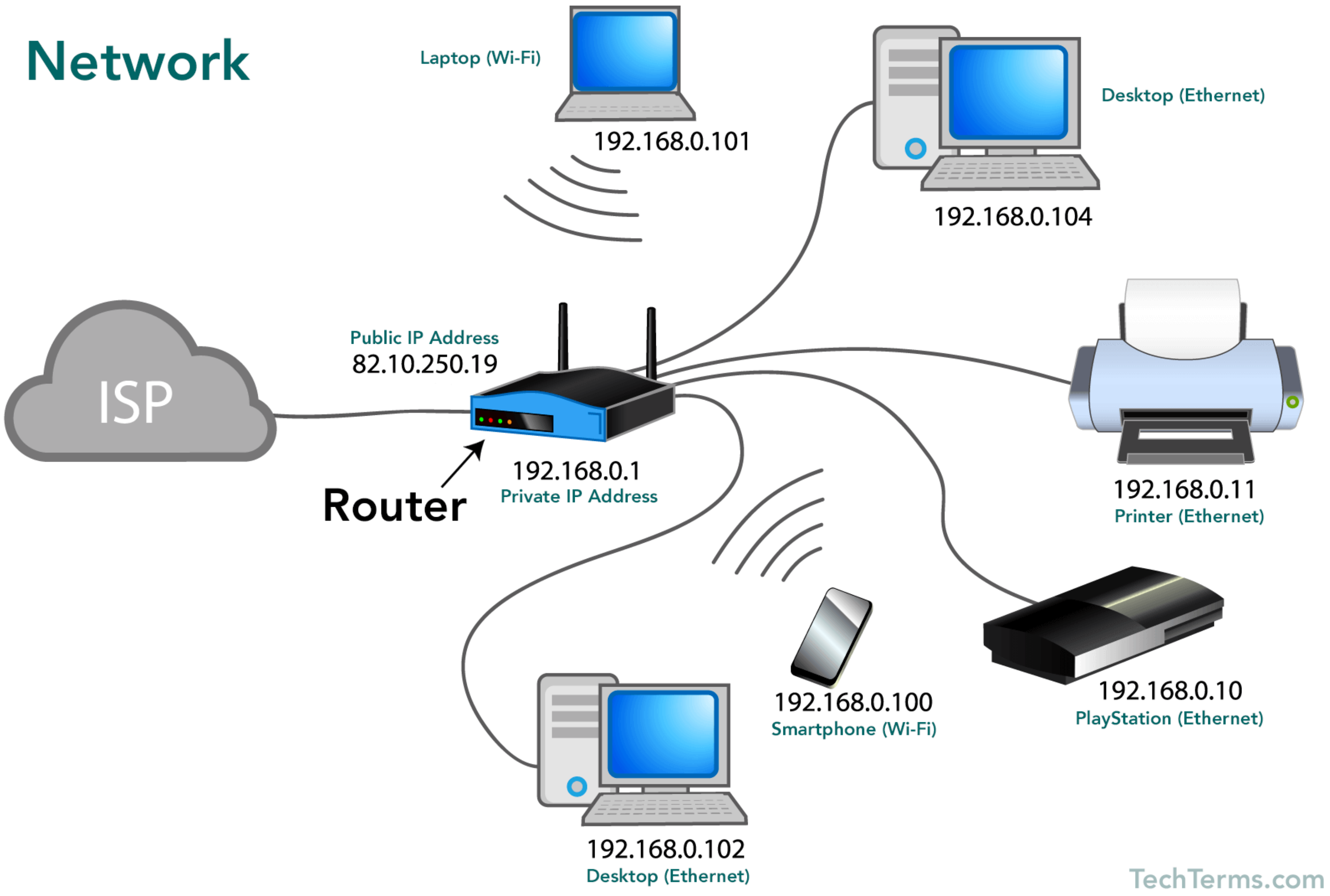
A network is a connected graph mathematically defined as a two-tuple <V,E> , where V is the set of nodes and E is the set of edges.



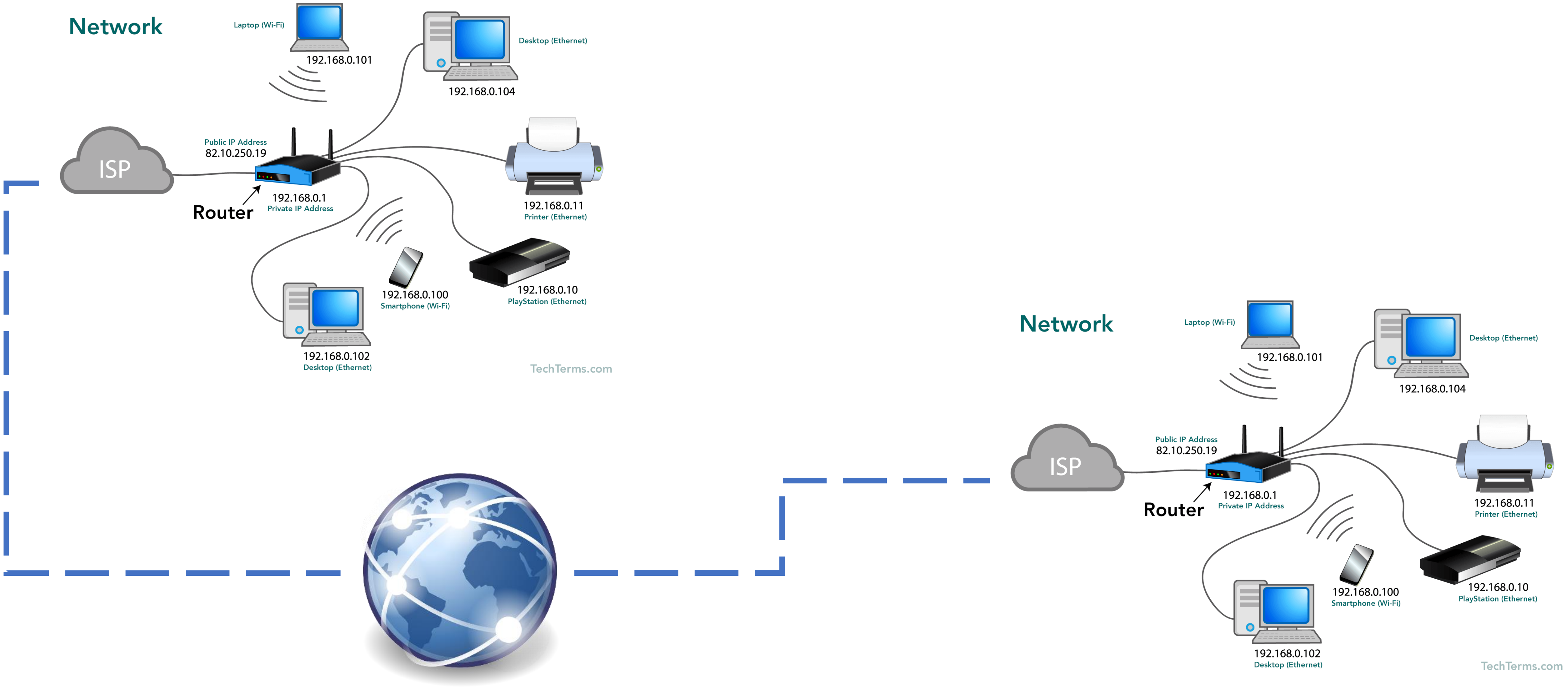
Introduction to network: wired and wireless



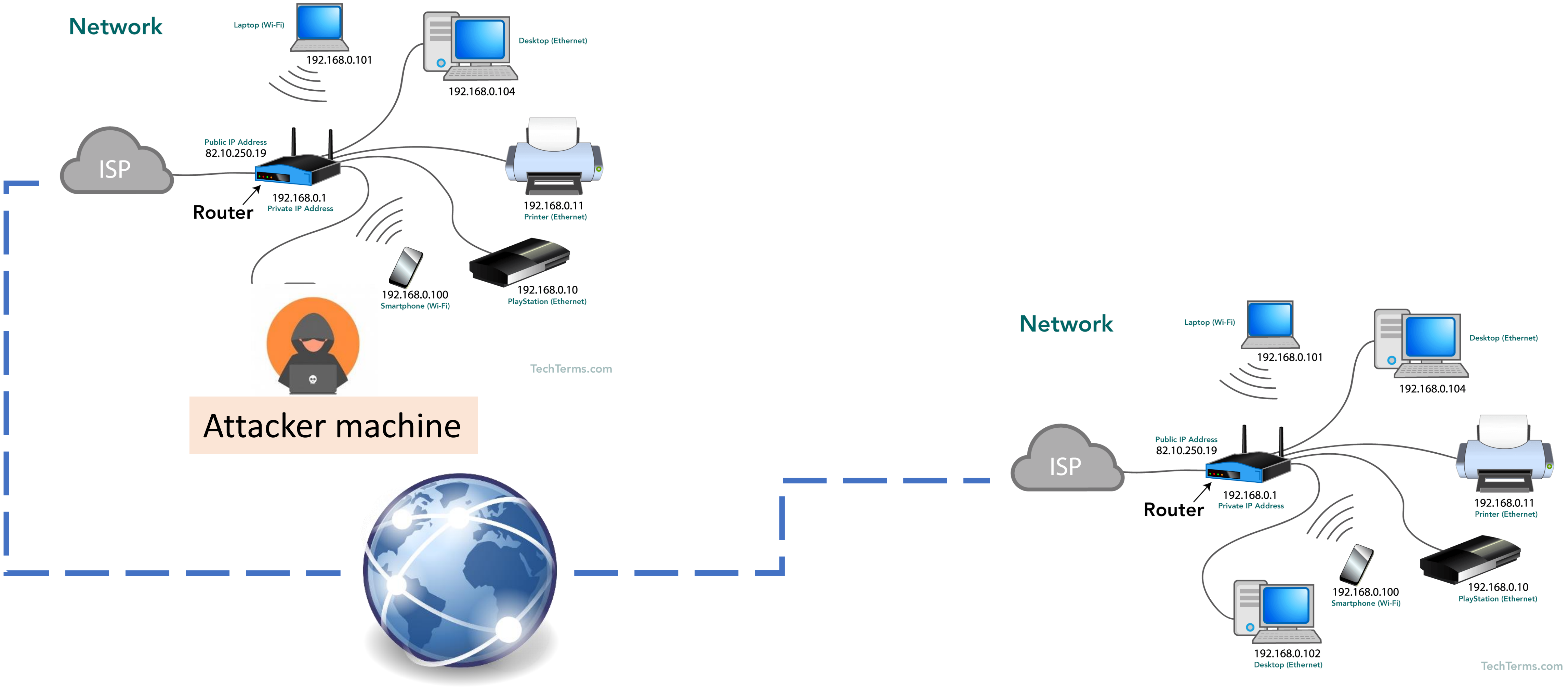
Network architecture



Internet

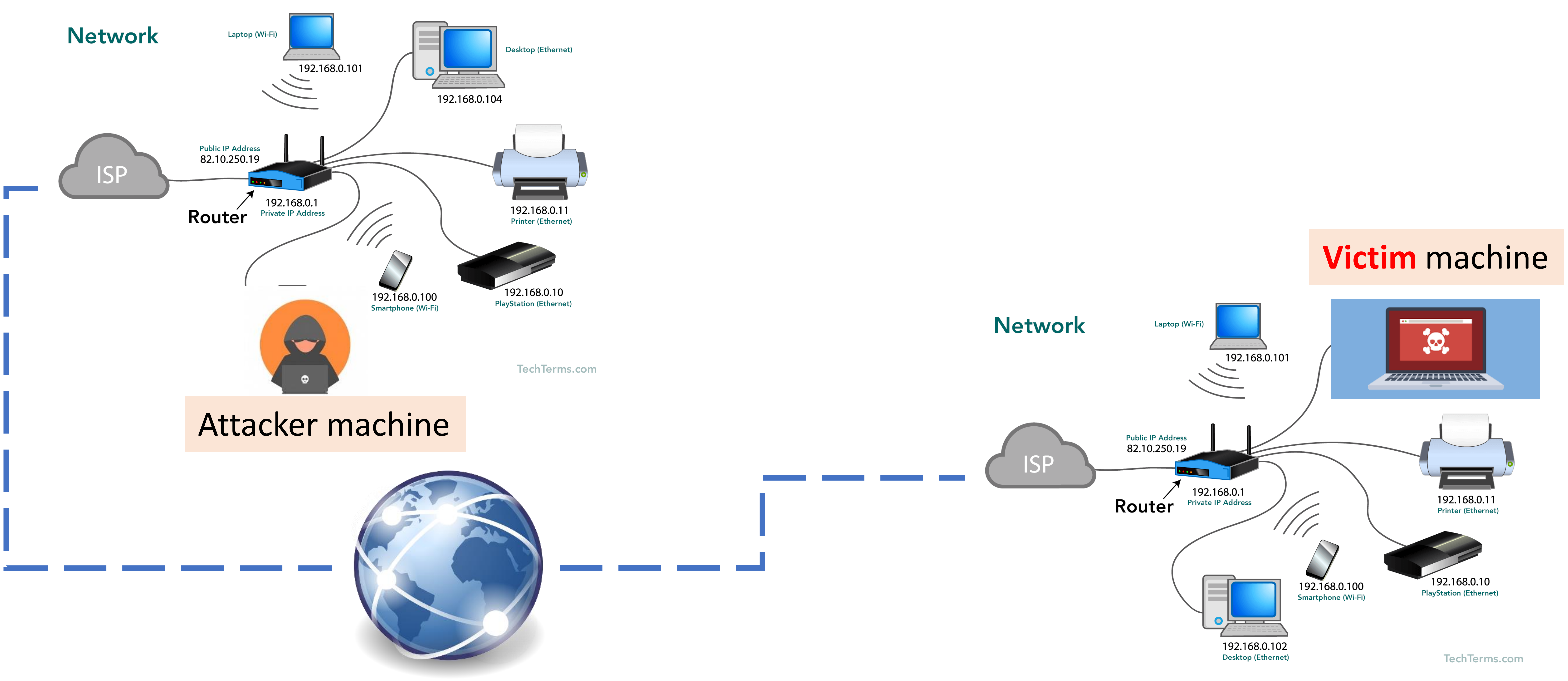

Network
Laptop (Wi-Fi)
192.168.0.101
Desktop (Ethernet)
192.168.0.104
ISP
Public IP Address
82.10.250.19
192.168.0.1
Private IP Address
Router
192.168.0.11
Printer (Ethernet)
192.168.0.100
Smartphone (Wi-Fi)
192.168.0.10
PlayStation (Ethernet)
192.168.0.102
Desktop (Ethernet)
TechTerms.com
Network
Laptop (Wi-Fi)
192.168.0.101
Desktop (Ethernet)
192.168.0.104
ISP
Public IP Address
82.10.250.19
192.168.0.1
Private IP Address
Router
192.168.0.11
Printer (Ethernet)
192.168.0.100
Smartphone (Wi-Fi)
192.168.0.10
PlayStation (Ethernet)
192.168.0.102
Desktop (Ethernet)
TechTerms.com

Malicious user



Attacker machine

Network attack



Attacker machine

Victim machine

What is Intrusion?

- ***Intrusions:*** attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network(illegal access).
- Intruders are classified into two groups.
  - External intruders do not have any authorized access to the system.
  - Internal intruders have at least some authorized access to the system. misuse their privileges or attempt to gain additional privileges for which they are not authorized.
- Although many intrusions are malicious in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.
- Based on the target, it can be network intrusions or system intrusions. Network intrusions target to attack the network where system intrusions target to attack a particular system.

Types of Intrusions

- Network Intrusions: Intrusions are initiated based on a flow of packet sent over a network.
  - Denial of Service (DoS) attack
  - Distributed Denial of Service (DDoS) attack.
  - Man-in-the-Middle attack
  - IP Spoofing
  - Port Scanning
  - Hijack attack
  - U2R attack
  - Asymmetric routing
  - SYN-Flooding
- System Intrusions: Host attacks target specific hosts or system by running malicious software to compromise the system functionalities or corrupt it. Most host attacks are categorized under the malware category. This includes worms, viruses, adwares, ransomware.

Solutions to Intrusions

- Firewall: Firewall filters network traffic between your network and outside network based on some rules configured by the administrator.
- Intrusion Detection System:
  - Filtered traffic may contain malicious data
  - It is a software that monitors the events occurring in a computer system or network and analyzing them for signs of possible *intrusions (incidents).*
- Intrusion Prevention System
  - It is a software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Intrusion Detection System(IDS)

- Intrusion detection system (IDS) monitors the network traffic and system-level applications to detect malicious activities in the network
- An IDS detects attacks as soon as possible and takes appropriate action.
- An IDS does not usually take preventive measures when an attack is detected.
- It is a reactive rather than a pro-active agent.
- It plays a role of informant rather than a police officer.
- It can deal with insider and outsider attacks.
- The most popular way to detect intrusions has been using the audit data generated by the operating system.
  - And audit trail is a record of activities on a system that are logged to a file in chronologically sorted order

IDS Requirements

- run continually with minimal human supervision
- be fault tolerant
- resist subversion
- minimal overhead on system
- scalable, to serve a large numbe of users
- Provide graceful degradation of service
- configured according to system security policies
- allow dynamic reconfiguration

IDS Architecture

- Basically, a sophisticated audit system
  - *Agent* like logger; it gathers data for analysis. It is also known as sensor.
  - *Director* like analyzer; it analyzes data obtained from the agents according to its internal rules
  - *Notifier* obtains results from director, and takes some action
    - May simply notify security officer
    - May reconfigure agents, director to alter collection, analysis methods
    - May activate response mechanism

Agents

- Obtains information and sends to director
- May put information into another form
  - Preprocessing of records to extract relevant parts
- May delete unneeded information
- Director may request agent send other information

Example

- IDS uses failed login attempts in its analysis
- Agent scans login log every 5 minutes, sends director for each new login attempt:
  - Time of failed login
  - Account name and entered password
- Director requests all records of login (failed or not) for particular user
  - Suspecting a brute-force cracking attempt

Director

- Reduces information from agents
  - Eliminates unnecessary, redundant records
- Analyzes remaining information to determine if attack under way
  - Analysis engine can use a number of techniques, discussed before, to do this
- Usually run on separate system
  - Does not impact performance of monitored systems
  - Rules, profiles not available to ordinary users

Notifier

- Accepts information from director
- Takes appropriate action
  - Notify system security officer
  - Respond to attack
- Often GUIs
  - Well-designed ones use visualization to convey information

Types of IDS

- Detection Model
    - signature detection vs. anomaly detection
- Monitoring Environment
    - Host based, vs. network based
- Operation
    - Off-line vs. real-time
- Architecture
    - Centralized vs. distributed

Types of IDS: host-based

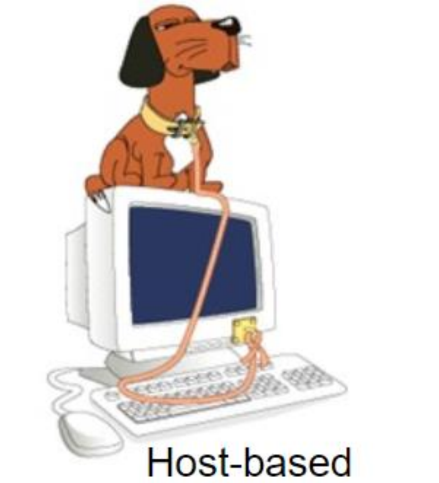
Deployed in a **single target computer**.

Monitors the **Operating System logs** and **Analyse** the **audit information** to detect trails of **intrusion**.

Audit information includes events like identification and authentication mechanism (like logins, accessed registries), file access information (like time, permissions), program executions, admin activities etc.

Deployment options:

Key servers that contain mission-critical and sensitive information.
Web servers.
FTP and DNS servers.
E-commerce database servers, etc.



Types of IDS: host-based

PROS:

- No additional hardware
- Less volume of traffic so less overhead
- Better for detecting attacks from the inside
- Near real-time detection and response
- System specific activities
- Encrypted traffic is also available for analysis
- Lower entry cost

CONS:

- **Detection is based on what any single host can record**
- **Narrow in scope (watches only specific host activities)**
- **Reduce performance of host system.**
- **Vulnerable to situation like when host operating system is compromised**
- **More expensive to implement.**
- **Deployment is challenging**
- **OS dependent**
- **Does not see packet headers.**

Types of IDS: Network-based

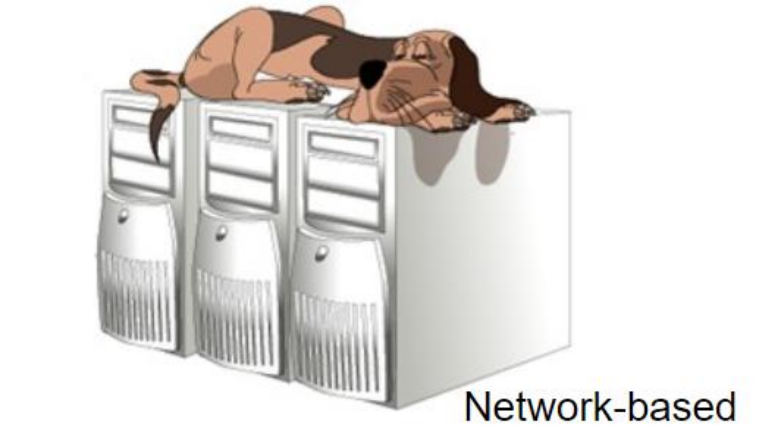
- Instead of analyzing information that originates and resides on a host, Network-based IDS analyses traffic passing through the network to detect intrusions.
- uses packet sniffing techniques to pull **packet header information** from TCP/IP packets or other protocols that are traveling along the network.
- **Packet header information** includes events like packet size (like 20KB), protocol (TCP, UDP etc.), port (like 1024), IP addresses, purpose (response or request).

Deployment options:

Outside firewall

- Just inside firewall

  -Combination of both will detect attacks getting through firewall and may help to refine firewall rule set.
- Behind remote access server
- Routers



Types of IDS: Network-based

PROS:

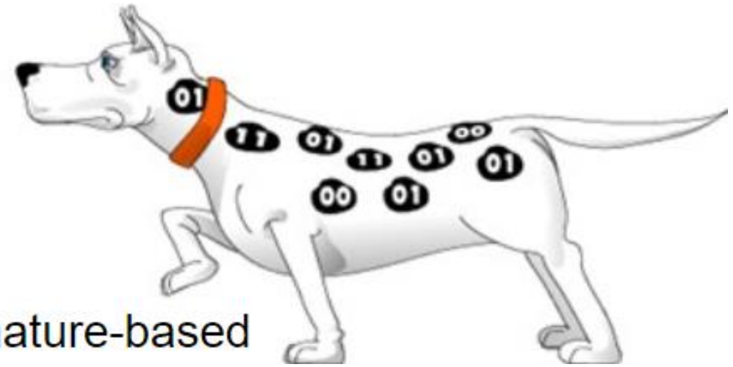
- Protect the whole network and detect network based attacks (like DOS)
- Broad in scope (watches all network activities)
- Easier setup: Easy to deploy
- Better for detecting attacks from the outside
- Less expensive to implement
- Detection is based on what can be recorded on the entire network
- Examines packet headers
- Near real-time response
- OS-independent
- Detects unsuccessful attack attempts

CONS:

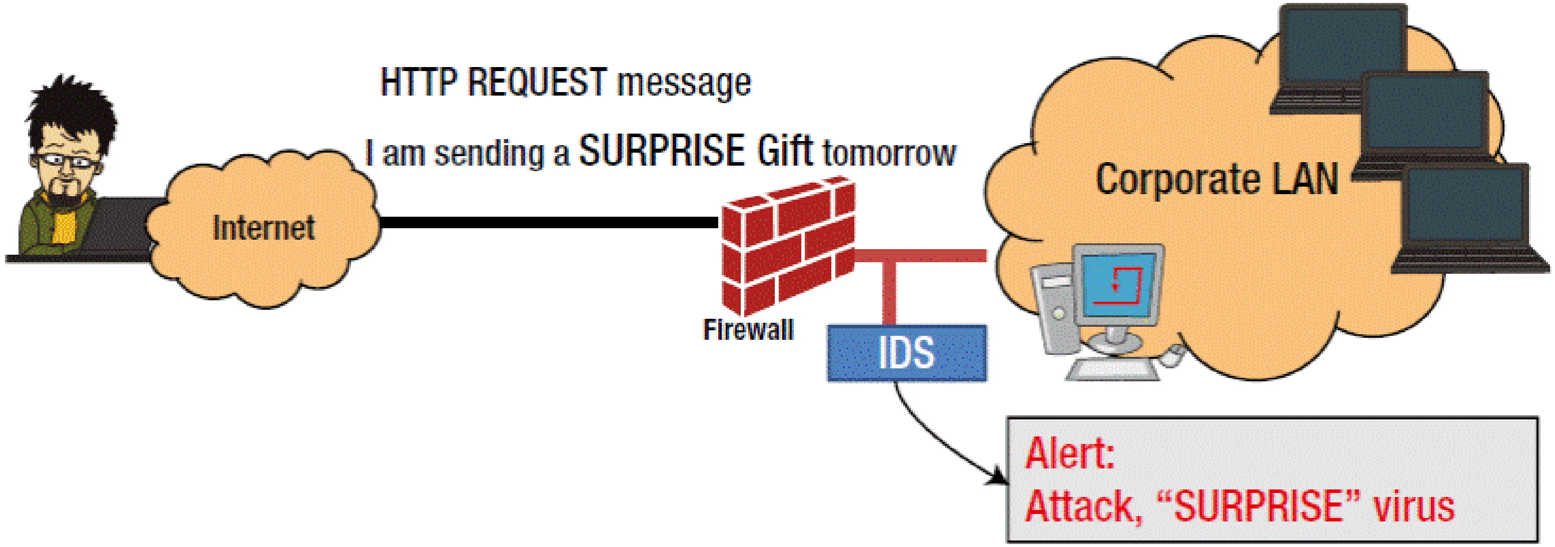
- Require all traffic information.
- Generates an enormous amount of data to be analyzed
- Cannot monitor traffic at higher network traffic rates
- Cannot deal with encrypted network traffic
- Can not detect system-specific attacks (like trojan)

Types of IDS: signature-based

Compares **signatures** against **observed events** to identify possible incidents. In case of any matching, an alert is issued.



Signature-based



Alert:
Attack, “SURPRISE” virus

Signature to Fire:

Header	Protocol	Destination Port	Signature String
IPv4	HTTP	80	SURPRISE

Source: networkingsphere.com

Types of IDS: signature-based

PROS:

- **High accuracy**
- **Low FPR (false Positive Rate),**
- **Widely available**
- **Fairly fast**
- **Easy to implement**
- **Easy to update**

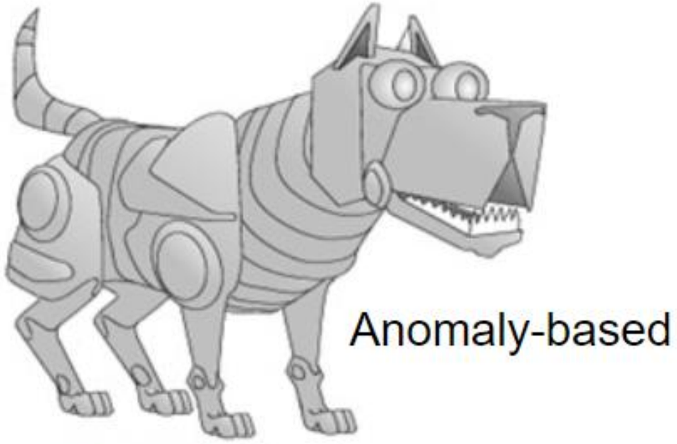
CONS:

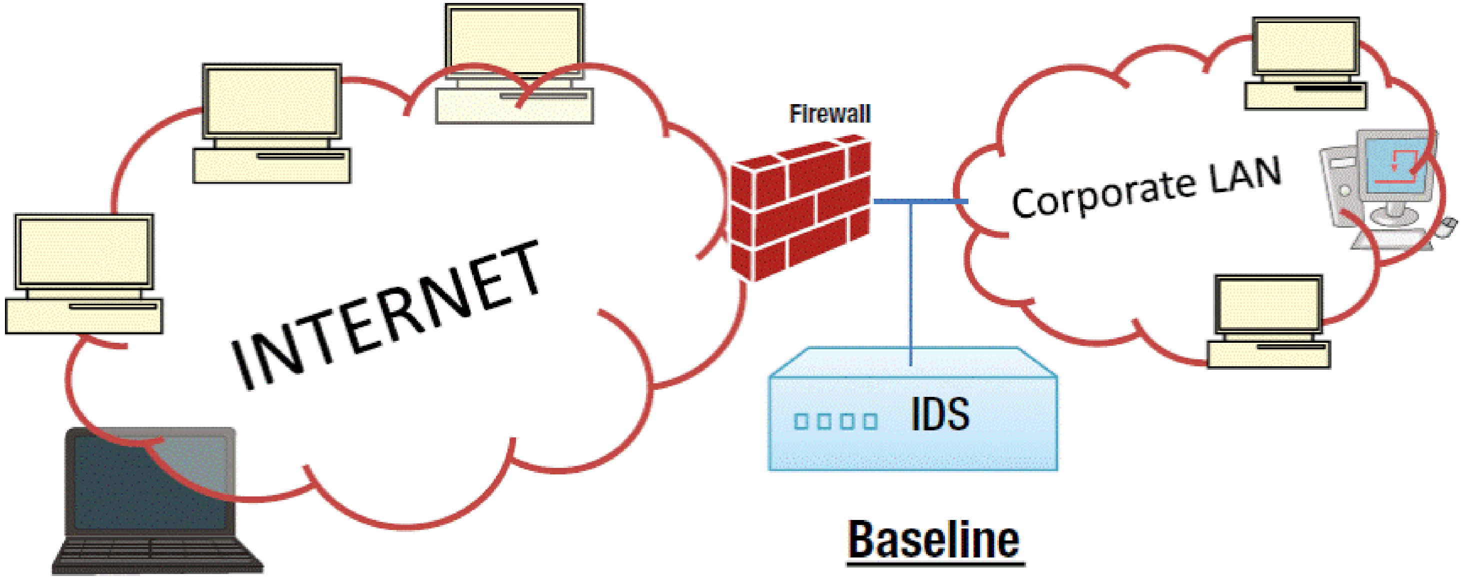
- Zero-day or unknown attack
- Cannot detect attacks for which it has no signature
- frequent update of signatures

Source: networkingsphere.com

Types of IDS: anomaly-based

Compares definitions of what is considered **normal activity** with **observed events** to identify significant deviations.





Baseline

TCP Pkts = 100/sec

UDP Pkts = 112/sec

ICMP Pkts = 43/sec

Alert !!! UDP Pkts = 425/sec !!!

Source: networkingsphere.com

Types of IDS: anomaly-based

Threshold detection

- Checks excessive event occurrences over time
- Compute statistics of certain system/network activities
- Report an alert if statistics outside range
- Example:

  For each user, store daily count of certain activities

  For example, fraction of hours spent reading email

  Maintain list of counts for several days

  Report anomaly if count is outside weighted norm

Profile based

- Characterize past behavior of users and groups
- Then, detect significant deviations
- Build it manually (this is hard)
- Analysis method (mean and standard deviation, multivariate, etc.) require machine learning and data mining techniques

Types of IDS: anomaly-based

PROS:

- Zero-day attack detection

CONS:

- High FPR (False Positive Rate)
- Greater complexity
- slower, more resource intensive

Source: networkingsphere.com

Types of IDS: specification-based

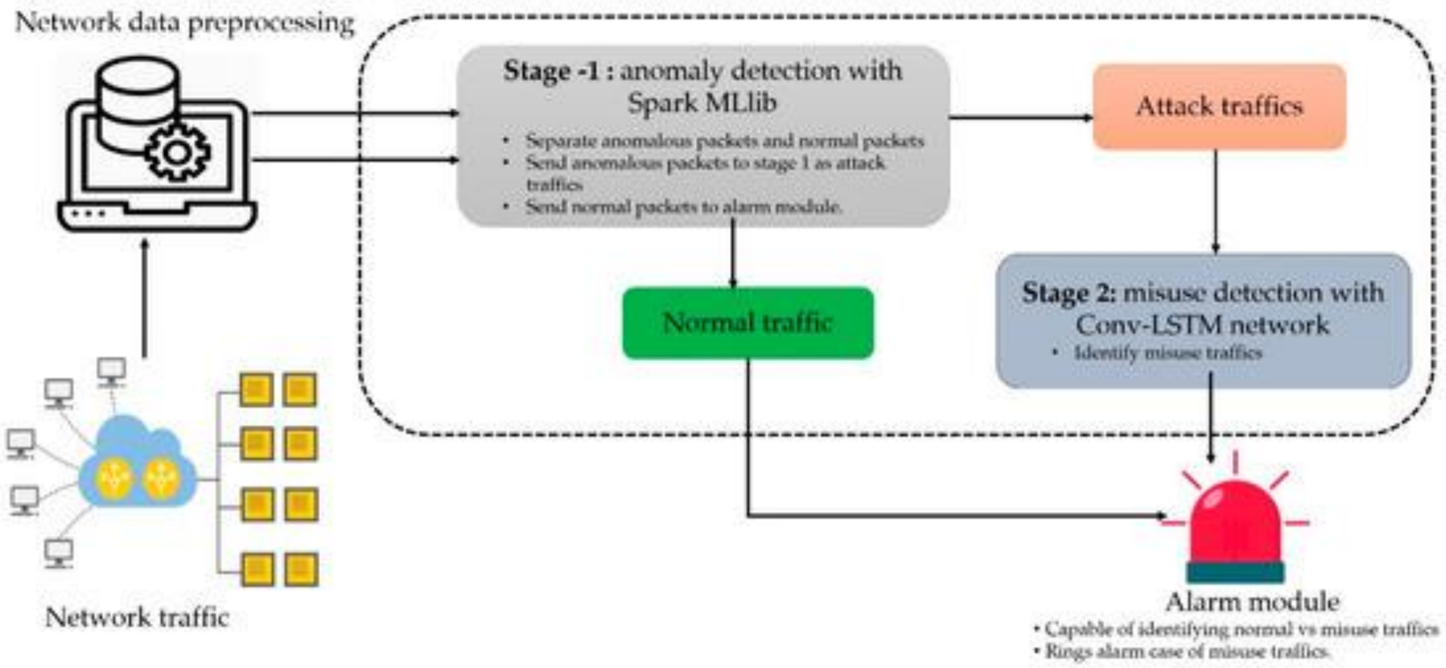
Combines the strength of both signature and anomaly based to form a **hybrid model**.

PROS:

- Able to achieve low FPR and high accuracy
- Detection of zero-day attacks

CONS:

- Implementation and deployment is very challenging
- Only theoretical results


Network data preprocessing
Stage -1 : anomaly detection with Spark MLlib
• Separate anomalous packets and normal packets
• Send anomalous packets to stage 1 as attack traffics
• Send normal packets to alarm module.
Attack traffics
Normal traffic
Stage 2: misuse detection with Conv-LSTM network
• Identify misuse traffics
Network traffic
Alarm module
• Capable of identifying normal vs misuse traffics
• Rings alarm case of misuse traffics.

"A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network"- by M.A. Khan et. Al.

IDS Types: Centralized vs. Distributed

Centralized

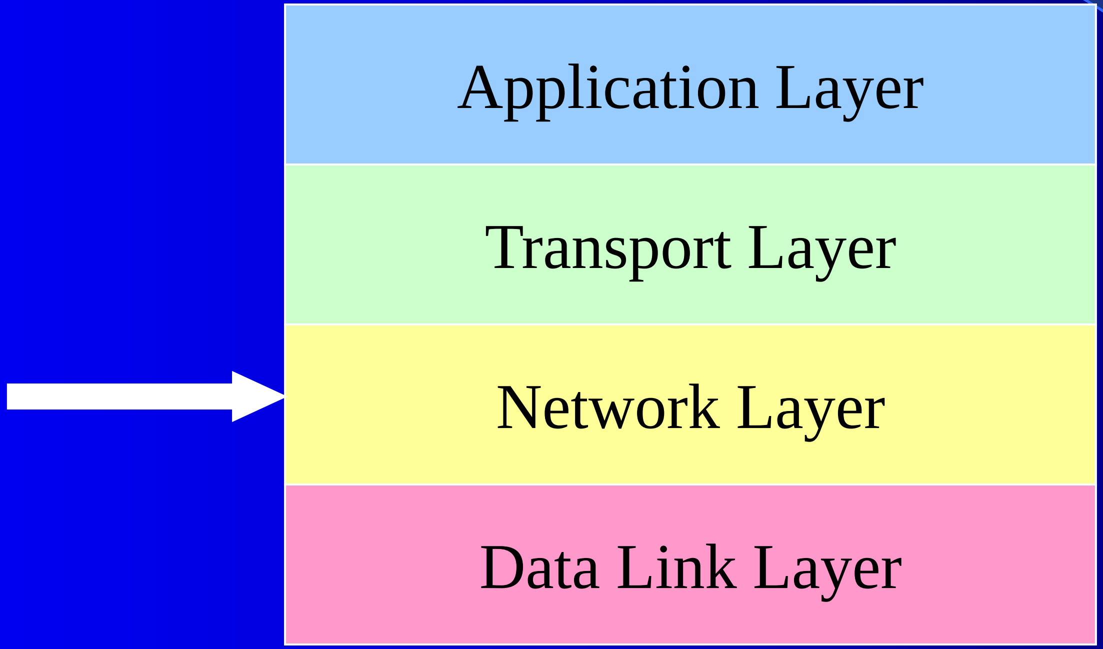
- ➢Data collected from single or multiple hosts
- ➢All data shipped to a central location for analysis

Distributed

- ➢Data collected at each host
- ➢Distributed analysis of the data

IPSec
(Internet Protocol Security)

TCP/IP Protocol Stack



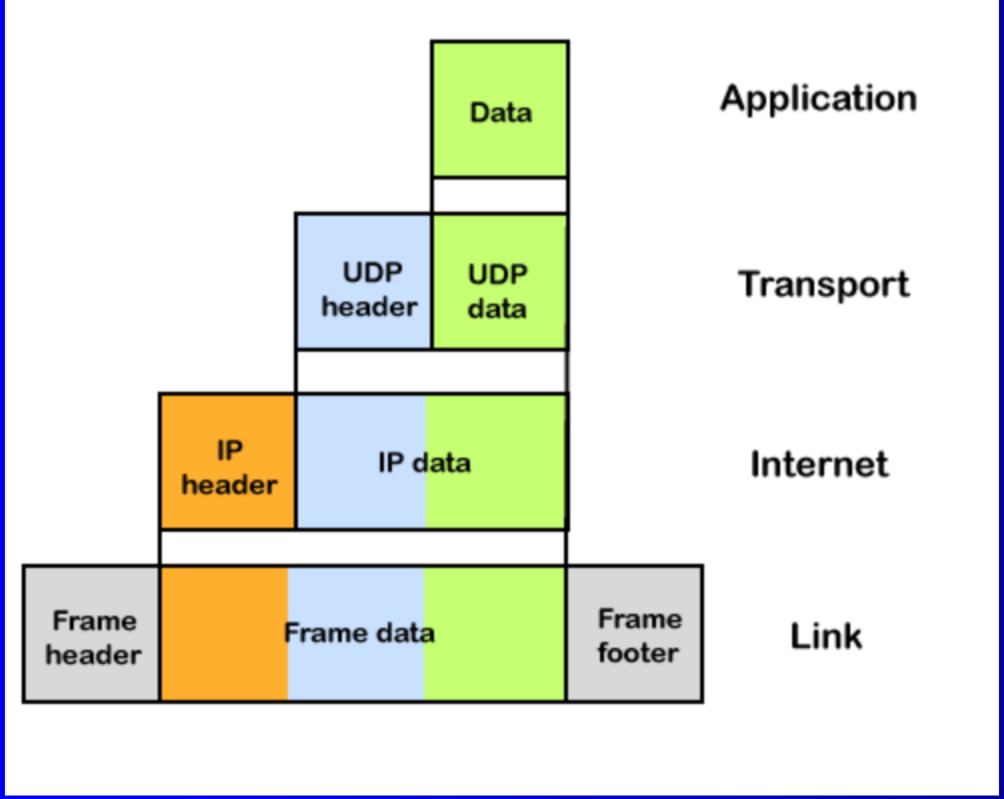
Application Layer

Transport Layer

Network Layer

Data Link Layer

Network Layer

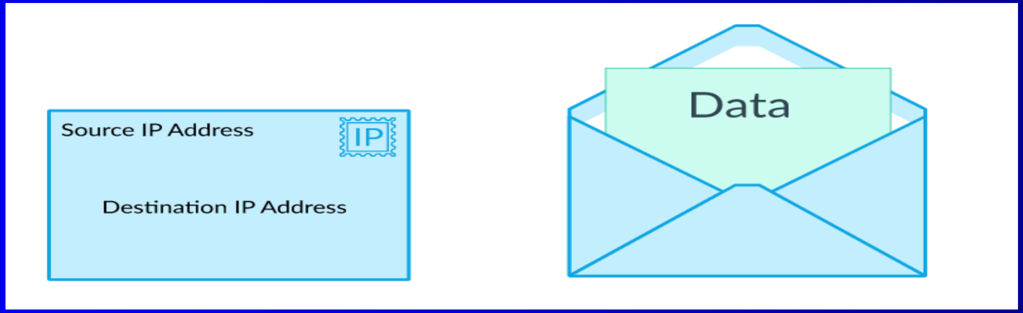


Network Layer

- Provides connectionless service
- Routing (routers): determine the path a packet has to traverse to reach its destination
- Defines addressing mechanism
  - Hosts should conform to the addressing mechanism

IP Packet

- In network layer, we use the term IP Packet
- Each IP packet contains both a header (20 or 24 bytes long) and data (variable length). The header includes the IP addresses of the source and destination, plus other fields that help to route the packet. The data is the actual content, such as a string of letters or part of a webpage.



Network Layer and Security

In most network architecture and corresponding communication protocol stack: *network layer protocol data units are transmitted in the clear*:

- Easy to inspect the data content
- Easy to forge source or destination address
- Easy to modify content
- Easy to replay data

⇓

Need network layer security protocol

IPSec

- IPSec stands for Internet Protocol Security
- IPSec provides security for IP and upper layer protocols
- IPsec protocols has two sub-protocols AH and ESP
- AH stands for Authentication Header
- ESP stands for Encapsulating Security Protocol
- Ipsec works in two modes: Tunnel mode and Transport mode

Security services by IPSec

IPSec: method of protecting IP datagrams

- Data origin authentication
- data integrity authentication
- Data content confidentiality
- Anti-replay protection

Internet Protocol Security (IPsec) is a secure network protocol that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

AH: Authentication Header

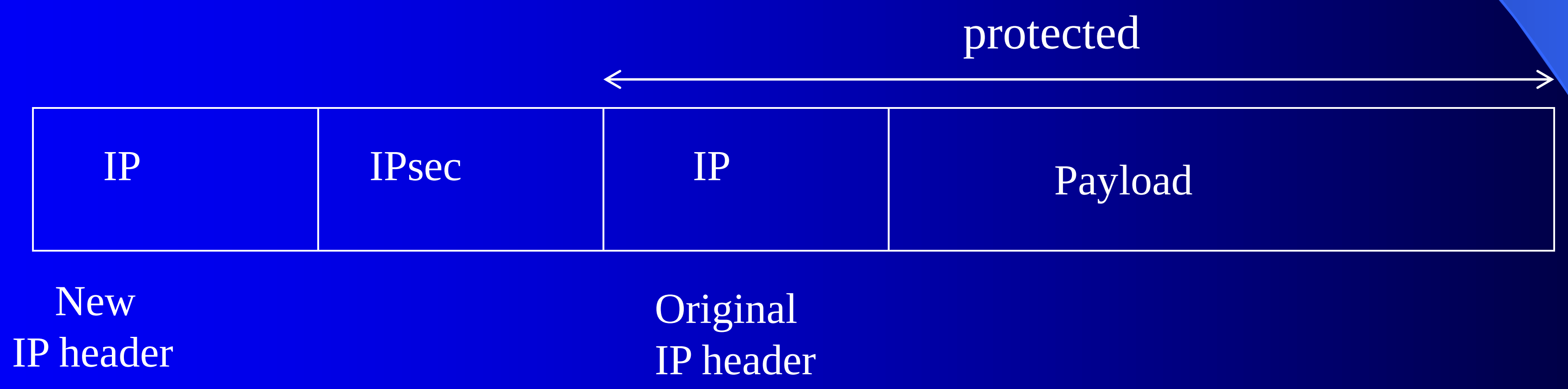
- Does NOT provide confidentiality
- Provides:
  - Data origin <u>authentication</u>
  - Connectionless data <u>integrity</u>
- May provide:
  - Non-repudiation (depends on cryptographic alg.)
  - Anti-replay protection (prevent replying of old packet)

ESP: Encapsulating Security Protocol

- Provides:
  - Confidentiality
  - Authentication (not as strong as AH: IP headers below ESP are not protected)
  - Limited traffic flow confidentiality
  - Anti-replay protection

Tunnel Mode

- Tunnel mode: Encrypts entire IP packet
  - Entire IP packet to be protected is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers



protected

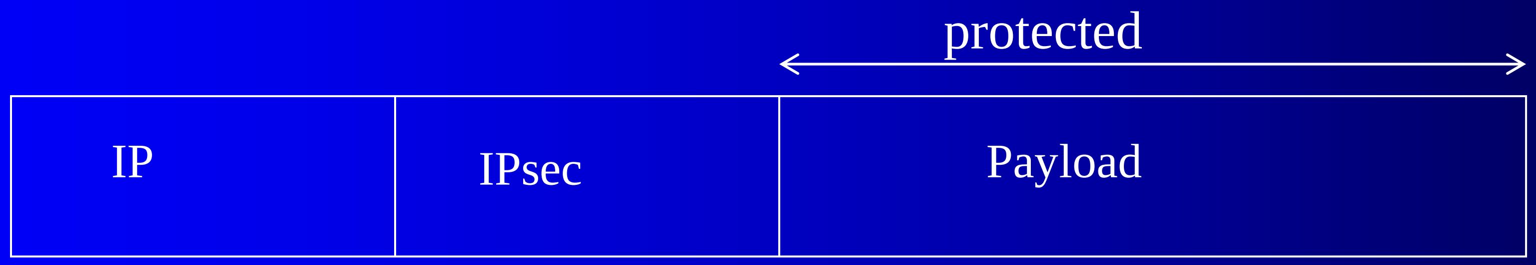
IP	IPsec	IP	Payload

New
IP header

Original
IP header

Transport Mode

- <u>Transport mode:</u> protect upper layer protocols
  - IPSec header is inserted between the IP header and payload
  - *only payload* is encrypted, authenticated



protected

IP

IPsec

Payload

Malicious Software

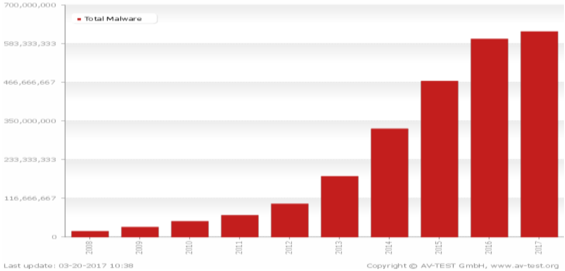
Dr. Kamalakanta Sethi

Malicious Software

- Malware is a combination of the words “Malicious” and “Software".
- Its an umbrella term to describe any software that is used to cause harm or to steal/breach data.
- Different kinds of Malware
  - Virus
  - Worms
  - Adware
  - Spyware
  - Trojan Horses etc

Malware

- **MALWARE is**
  - Malicious Software.
  - Adware, Spyware,Virus,Worm, Ransomware
- **Malware can do**
  - allow cybercriminals to get into other people’s computers without their permission
  - steal personal information
  - delete files
  - steal software serial numbers
- According to AV-Test in March 2017,the total number of malwares is increasing exponentially since 2008.
- Due to such increasing ,it is necessary to detect these files before they harm



Last update: 03-20-2017 10:38

Copyright © AV-TEST GmbH, www.av-test.org

Virus

- A virus is a program or code that can replicate itself and pass on malicious code to other nonmalicious programs by modifying them. Virus can not spread without a human action such as running the infected program.
- A good program can be modified to include a copy of the virus program, so the infected good program itself begins to act as a virus
- There are two broad categories of virus
  - A **transient virus** has a life span that depends on the life of its host; the virus runs when the program to which it is attached executes, and it terminates when the attached program ends.
  - A **resident virus** locates itself in memory; it can then remain active or be activated as a stand-alone program, even after its attached program ends.
  - (A virus which saves itself in the memory of the computer and then infects other files and programs when its originating program is no longer working. This virus can easily infect other files because it is hidden in the memory and is hard to be removed from the system.)

Computer Virus Symptoms

You may have a computer virus if you notice any of the following:

- Your computer is slow (including slow to start up and to open programmes)
- Issues shutting down or restarting
- Missing files
- Frequent system crashes and/or error messages
- Malfunctioning antivirus programmes
- Unexpected pop-ups
- Emails sent autonomously from your account.

How does a computer gets Virus

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening spam email or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements

Virus Life Cycle Phases

Dormant Phase:

The virus won’t self-replicate, nor will it delete, capture or modify data on the infected computer. The dormant phase lives up to its namesake by keeping the virus dormant and inactive.

Propagation Phase:

.During the propagation phase, viruses will create copies of their malicious code, which they’ll store on other parts of the infected computer’s disk drive.

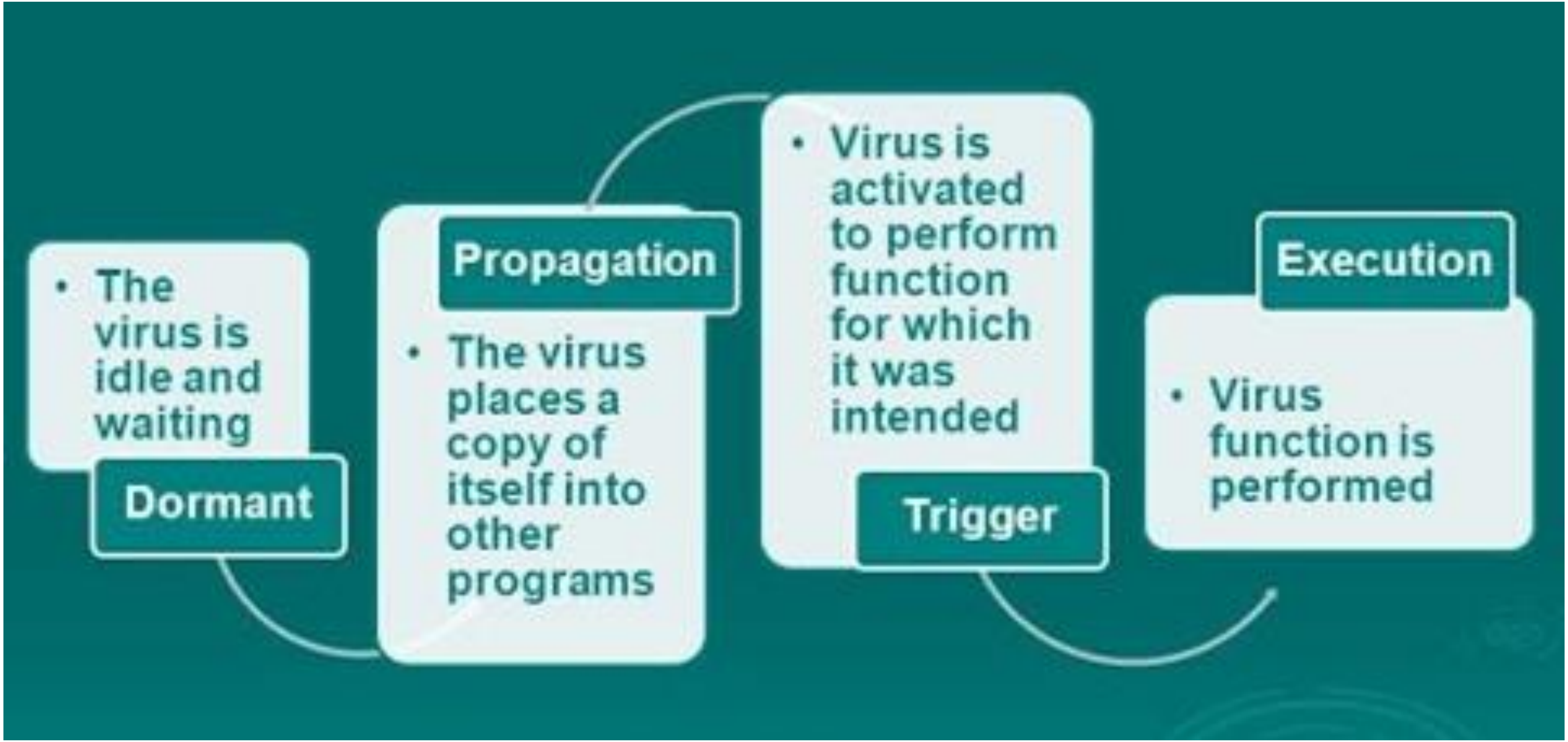
Trigger Phase:

The third phase in a virus’s infection cycle is the trigger phase. The trigger phase involves activation. Viruses aren’t considered active until they enter the trigger phase. Upon entering the trigger phase, viruses will be activated to perform their malicious activities. Once the virus has self-replicated 100 times, it will enter the trigger phase.

Execution Phase:

The fourth and final phase of a virus’s infection is the execution phase. The execution phase involves the release of a payload. Viruses have a payload. The payload is the malicious code that’s designed to harm or otherwise negatively affect the targeted computer. Some payloads can delete data. Others can cause unwanted pop-ups or advertisements.

Virus Life Cycle



Dormant

- The virus is idle and waiting

Propagation

- The virus places a copy of itself into other programs

Trigger

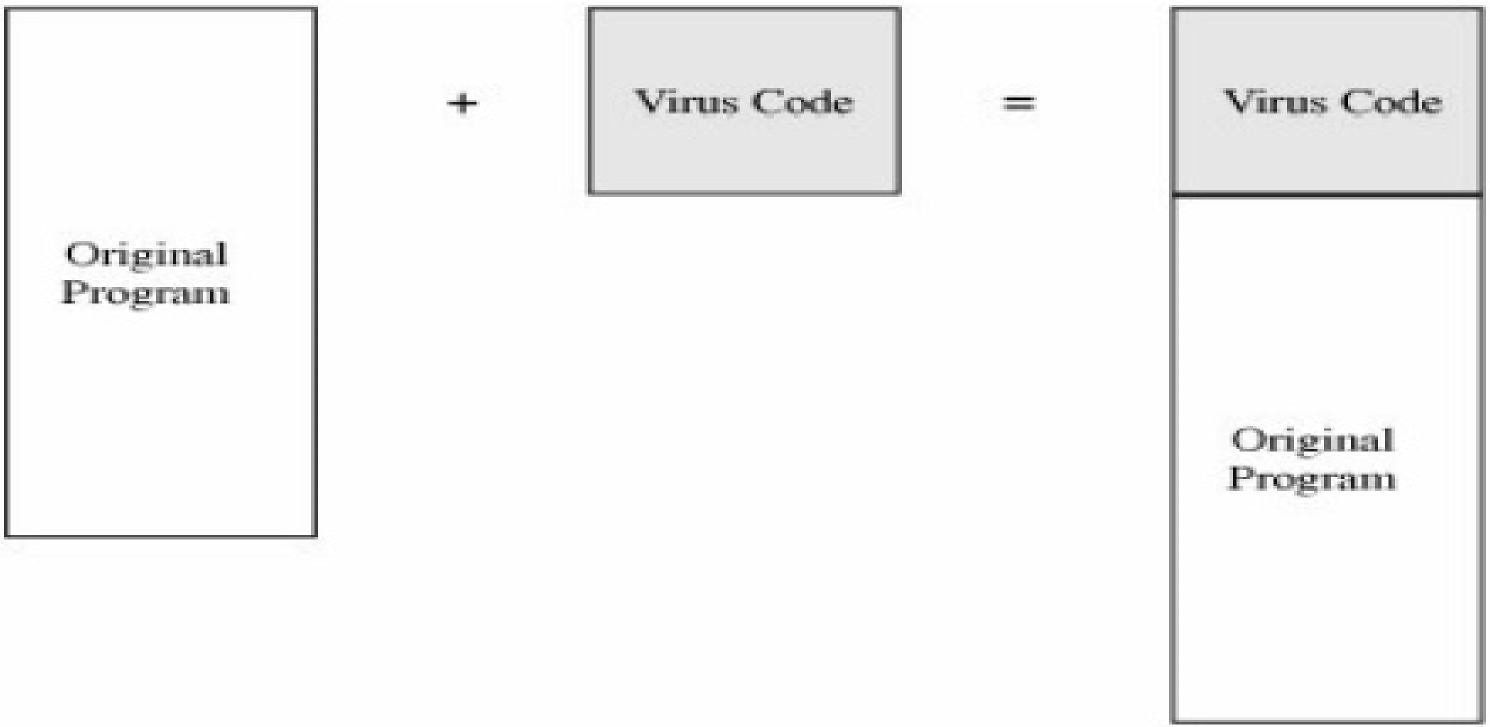
- Virus is activated to perform function for which it was intended

Execution

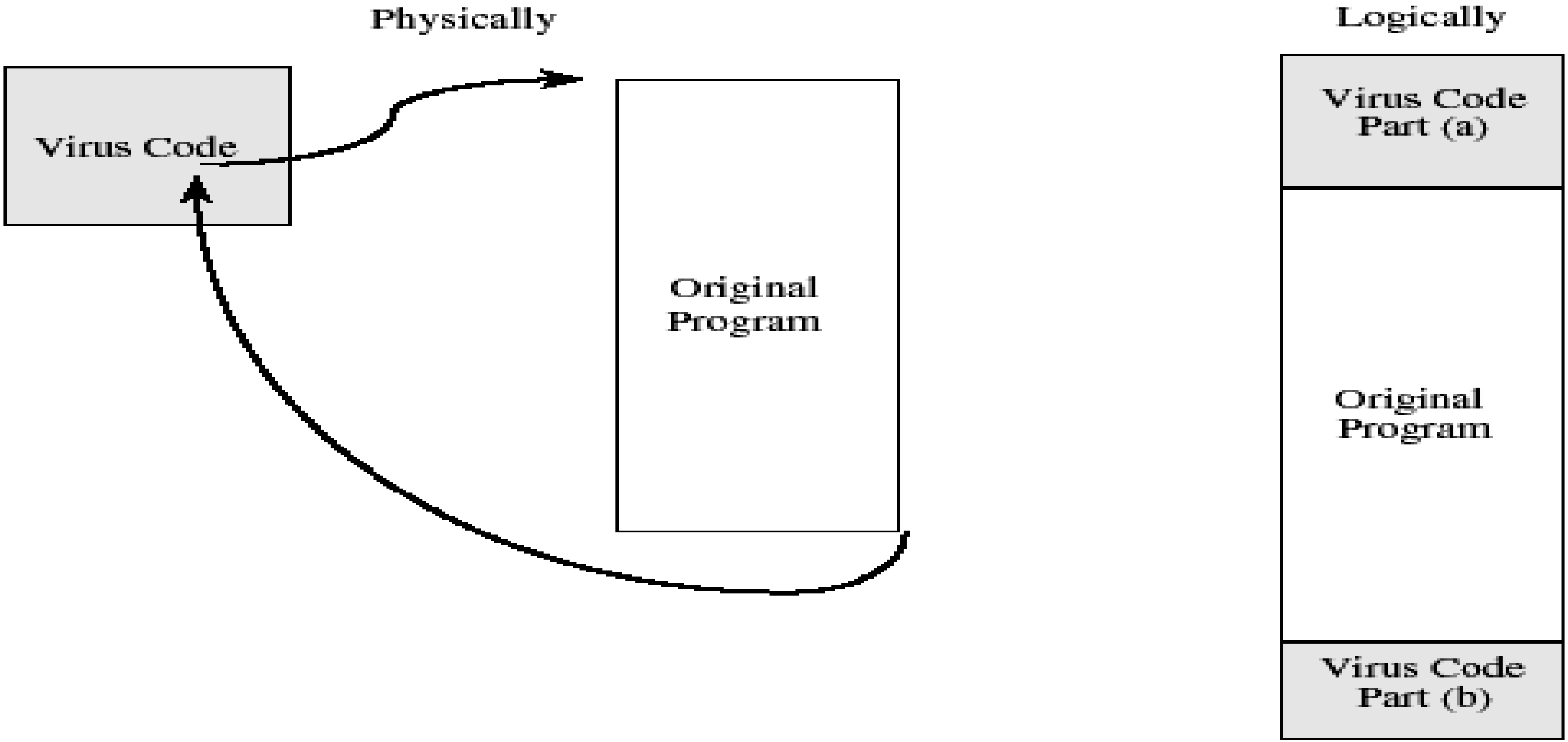
- Virus function is performed

Attached Virus

Figure 3-4. Virus Appended to a Program.

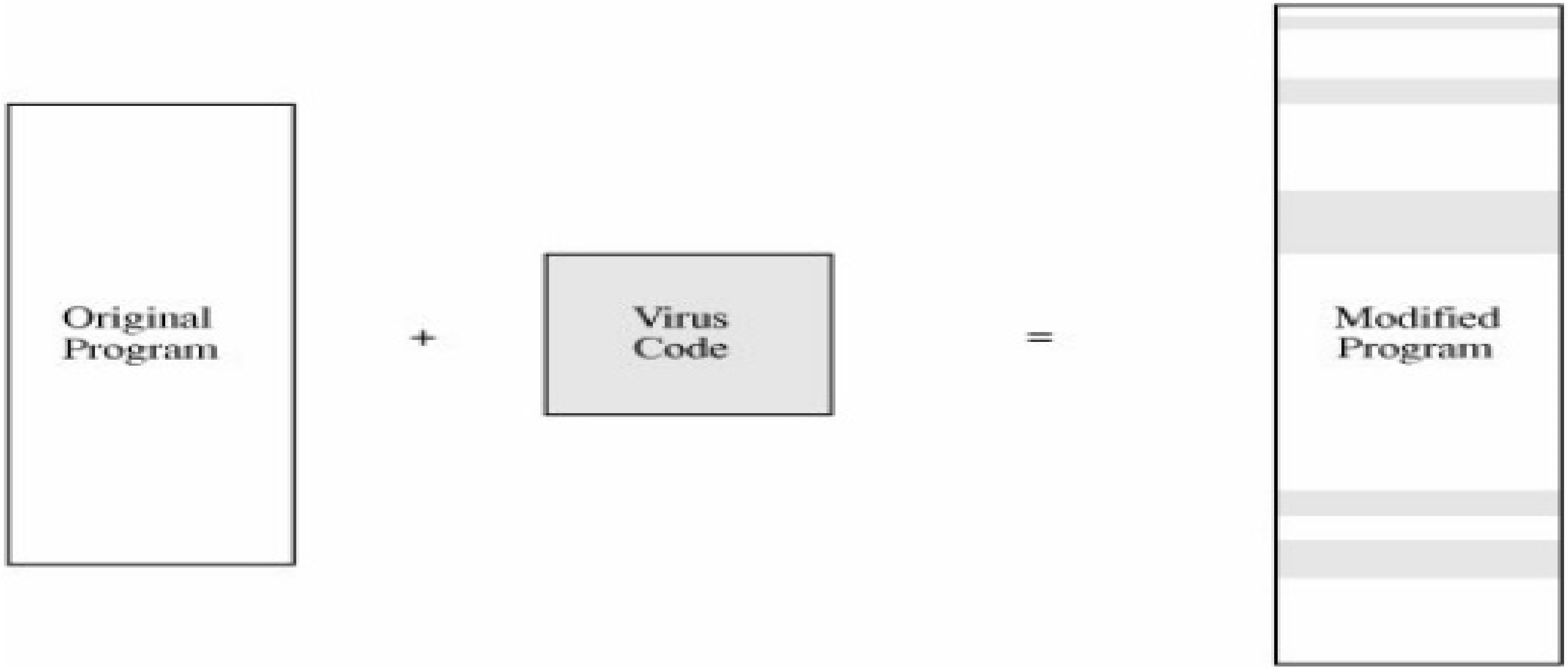


Virus surrounding a Program



Integrated Virus

Figure 3-6. Virus Integrated into a Program.



Worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers (law of exponential growth).
- The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devasting effect. One example would be for a worm to send a copy of itself to everyone listed in your email-addrss book. Then worm replicates and sends itself out to everyone listed in each of the receivers address book and manipast contiues on down the line.
- Due to copying nature of worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwith) causing web servers, network servers, and individual computers to stop responding.
- Worms spread computer to computer, but unlike a virus it has capability to travel without any human action.

Trojan Horse

- A Trojan horse at the first glance looks like a useful or genuine software but will actually do damage once installed or run on your computer.
- One of the critical characteristics of a Trojan is that it cannot replicate itself like virus (also can not reproduce by infecting other files) and worms, and a user has to install it themselves.
- Once installed, Trojan Horse software can steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.
- Trojans also known create a backdoors on your computer that gives malicious users to access to your system possibly allowing confidential or personal information to be compromised.
- Some Trojan horses are designed to be more annoying (like changing your desktop, adding silly active desktop icons, cause pop-up windows) or they can cause serious damage by deleting files or destroying information on your system.

.

Virus vs Worm

- Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage (such as deleting files from the computer system).
- Virus has self replicating power and can't be controlled by remote.

- A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks. In other words worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.
- Worms has self-replicating power and can be controlled the remote.

Virus vs Worm vs Trojan Horse

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software.	Worms replicate itself to cause slow down the computer system	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.

Spyware

- This type of malicious software, spies on you, tracks your internet activities. It helps the hacker in gathering information about the victim’s system, without the consent of the victim. This spyware’s presence is typically hidden from the host and it is very difficult to detect.
- For example, some spywares like keyloggers save your keystrokes to a text file. When you type in the address of something like a banking website and then type in your username and password, the keylogger captures that information and sends it back home.

Adware

- Adware is a form of malware that hides on your device and designed to throw advertisements up on your screen, most often within a web browser.
- Adware is known as as advertising-supported software.
- It shows advertisements for the purpose of generating revenue for its author.
- Adware is programmed to examine which Internet sites, the user visits frequently and to present and feature related advertisements.
- Not all adware has malicious intent, but it becomes a problem anyway because it harms computer performance and can be annoying.

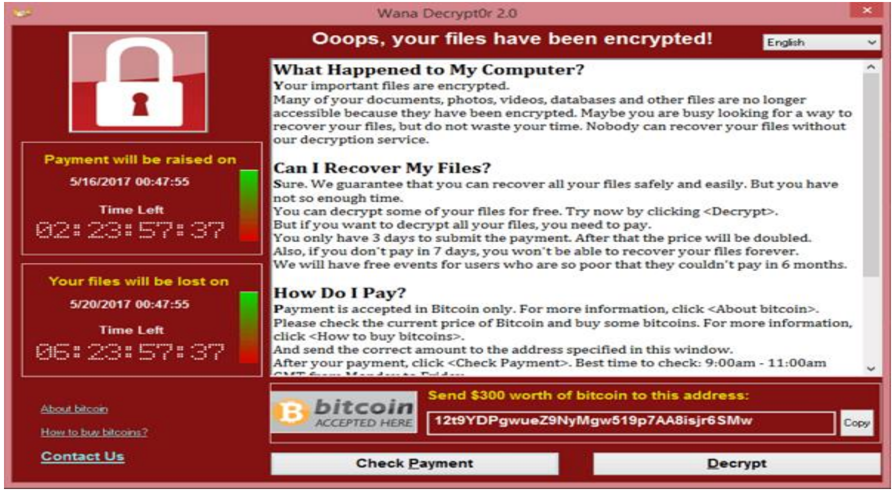
Ransomware

- Ransomware is a particularly nasty type of malware that doesn’t destroy your data but locks it behind strong encryption. Following this, the creators of the malware demand a ransom from you in order to get your data back.

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

Wannacry Attack

- The WannaCry ransomware attack was a worldwide cyberattack in May 2017 which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry

- The WannaCry attack (in 2017) targetted computers running Windows by encrypting data and demanding ransom
  - “Ransomware” attack
  - NHS and FedEx servers were affected
- WannaCry propagates using a buffer overflow vulnerability in the SMB (Sever Message Block) protocol
- Once the ransomware infects a system, it tries to contact an obscure server and proceeds to encrypt the system if the server was not reachable
- Once it infects a system, it searches for other systems on the network and spreads using the SMB protocol

Incident Response

Event Vs Response

It is important to know the difference between a security event and a security incident. A security event is an occurrence in the network that might lead to a security breach. If a security event is confirmed to have resulted in a breach, the event is termed a security incident. A security incident results in risk or damage to the resources and assets of an enterprise. Based on the breach detected, sufficient action has to be taken to limit the damage and prevent the incident from getting worse.

Event

- Security events are the first step towards identifying a threat or a complete attack. An enterprise might run into thousands of security events per day. However, not all security events indicate a cyberattack. Some of the most common sources of security events that should be analyzed in a network are explained below.
- Security events related to Firewall
  - Spike in incoming or outgoing traffic:
  - Configuration changes to firewall policies:
  - Modification to firewall settings:
- Security events to Critical Servers (file servers, web servers, and domain controllers)
  - User logins.
  - User permission changes to access the servers.
  - Changes to system settings.
  - Changes to security configurations.

Security Incident

A security incident is a security event that damages network resources or data as part of an attack or security threat. An incident doesn’t always cause direct damage, but it still puts the enterprise's security at risk. For example, a user clicking on a link in a spam email is a security incident. This incident doesn't directly cause any damage, but it could install malware that causes a ransomware attack.

Some of the security incidents that you should be monitoring in your network include:

- Traffic from known malicious IP addresses:
- Suspicious malware installations on endpoints:
- Unauthorized changes to configurations of critical devices:
- Malware infection through removable media:
- Data manipulation in databases:

Incident Response

- Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”).

  The goals of an incident response plan are to:

  - Restore operations
  - Minimize losses
  - Fix vulnerabilities quickly and thoroughly
  - Strengthen security to avoid future incidents

Need for Incident Response

- Supports responding to incidents **systematically.**
- **Minimize** loss or theft of information and disruption of services.
- Ability to use information gained during incident handling to better prepare for handling future incidents
- Helps with dealing properly with legal issues that may arise during incidents.

WHO HANDLES INCIDENT RESPONSES?

- Typically, incident response is conducted by an organization’s computer incident response team (CIRT), also known as a **cyber incident response team**.
- CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments.
- As Gartner describes, a CIRT is a group that is “responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks.”

Six steps of incidence response

- The SANS (SysAdmin, Audit, Network and Security) Institute provides six steps for effective incident response
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lesson Learned

Preparation

- It is very important phase in incident response life cycle.
- The Preparation phase covers the work an organization does to get ready for incident response. It means how much they are capable of responding to an incident (identifying different malwares, what is the impact on system, which tools to stop them)
- In this phase we have to develop policies and procedure to follow in the event of a cyber breach. We have to also establish the right tools and resources.
- In this phase of incident response planning, you have to ensure that all employees have a certain degree of awareness about cyber security and a basic level of incident response training in dealing with a cyber crisis. Everyone also has to be aware of their roles and responsibilities in case of a cyber event.
- This phase deals with documentation to record actions taken for later review.

Identification

- This phase in incident response planning, as the name suggests, is about identifying if any of your systems have been compromised means you have to identify if security incident happened or not (identify the nature of attack and its impact on system). In this phase we can use different tools such as Firewall, IDS to identify security incidents.
- In case a breach (or security incident) is indeed discovered, you should focus on answering questions such as:
  - Who discovered the breach?
  - What is the extent of the breach?
  - Is it affecting operations?
  - What could be the source of the compromise etc.

It is also important to document everything in this phase.

Containment

- After the incident has been identified, the next phase is containment. This phase of incident response phase involves everything you can do to mitigate damage once you’re already affected by a security incident (or cyber attack).
- In this phase, you need to consider what can be done to minimize the damage and prevent the damage further.
- ✓ To prevent the damage, we should follow containment strategies that may be short-term and long-term. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.

- Examples of some strategies that followed in this phase:
  - Updating the software (i.e., patching)
  - Enabling two-factor authentications for your applications
  - Maintain strong passwords
  - Migrating or moving unaffected resources to new systems
  - Upgrading older, legacy systems
  - Installing additional network protection

Eradication

- Eradication phase targets the root cause of the breach (so that we can take preventive measures. Eradication procedures will vary based on the attack.
- For example, if the authentication was the weakness, a company may consider using 2FA or even 3FA. Or, if it was an OS vulnerability, it should use a patch (mitigate all the vulnerabilities found in OS) . The key is to fix the problem in such a way that it will not be a recurring issue.
- ✓ During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.

Recovery

- ➢ In this phase the administrator restore the affected systems or devices (i.e., the systems/devices that are compromised) to normal operations, confirm that the systems are functioning normally after the security incident.
- ➢ It also determine how long those affected systems will be monitored (monitor abnormal behavior using some testing and monitoring tools) at a higher level than usual. We should be sure the affected systems are no longer vulnerable to attacks.
- ✓ Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).

Lesson Learned

- Learning and improving after an incident is one of the most important parts of incident response and the most often ignored. In this phase the incident and incident response efforts are analyzed. The goals here are to limit the chances of the incident happening again and to identify ways of improving future incident response activity.
- During this stage, the incident response team and partners meet to determine how to improve future efforts. This can involve evaluating current policies and procedures, as well specific decisions the team taken during the incident. Final analysis should be condensed into a report and used for future training.
- This phase is important and critical in incident response.

Lesson Learned: Post-incident Activity

- ✓ Exactly what happened, and at what times?
- ✓ How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- ✓ What information was needed sooner?
- ✓ What would the staff and management do differently the next time a similar incident occurs?
- ✓ How could information sharing with other organizations have been improved?
- ✓ What corrective actions can prevent similar incidents in the future?
- ✓ What precursors or indicators should be watched for in the future to detect similar incidents?
- ✓ What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Incident Response Team Services

1. **Intrusion Detection**
2. **Advisory Distribution** : A team may issue advisories within the organization regarding new vulnerabilities and threats.
3. **Education and Awareness :** Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team.
4. **Information Sharing**

Contd…

- ➢ Incident Documentation
- ✓ The current status of the incident
- ✓ A summary of the incident
- ✓ Indicators related to the incident
- ✓ Other incidents related to this incident
- ✓ Actions taken by all incident handlers on this incident
- ✓ Chain of custody, if applicable
- ✓ Impact assessments related to the incident
- ✓ Contact information for other involved parties (e.g., system owners, system administrators)
- ✓ A list of evidence gathered during the incident investigation
- ✓ Comments from incident handlers
- ✓ Next steps to be taken (e.g., rebuild the host, upgrade an application).