

Introduction to Cyber Security

Module 4

Network Security

Topics

- Firewalls
- Proxies
- DMZ
- Internet security protocols and standards
- Intrusion detection and prevention

Why Network Security 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 it from the ever-growing landscape of cyber threats today.
- Today's network architecture is complex and is faced with a threat environment that is always changing and attackers that are always trying to find and exploit vulnerabilities.
- 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.

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.

Contd...

- **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.

Types of Network Security

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

Network Access Control

- 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 Software

- 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

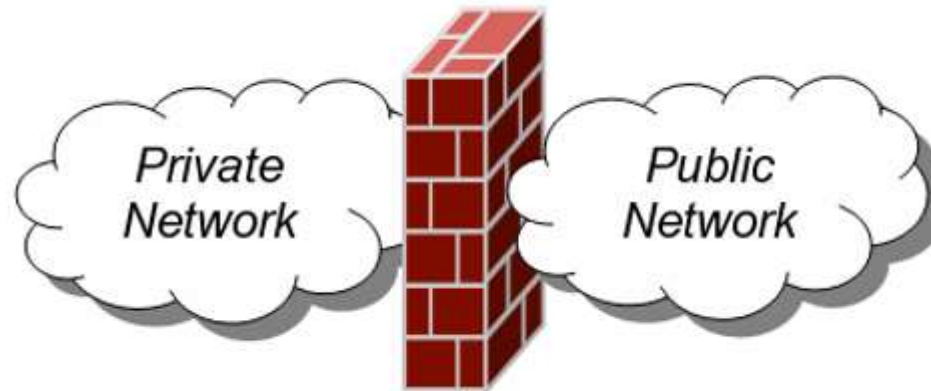
- Firewalls, as their name suggests, act as a **barrier between the untrusted external networks and your trusted internal network.**
- Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.
- For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

Virtual Private Networks

- 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.
- Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

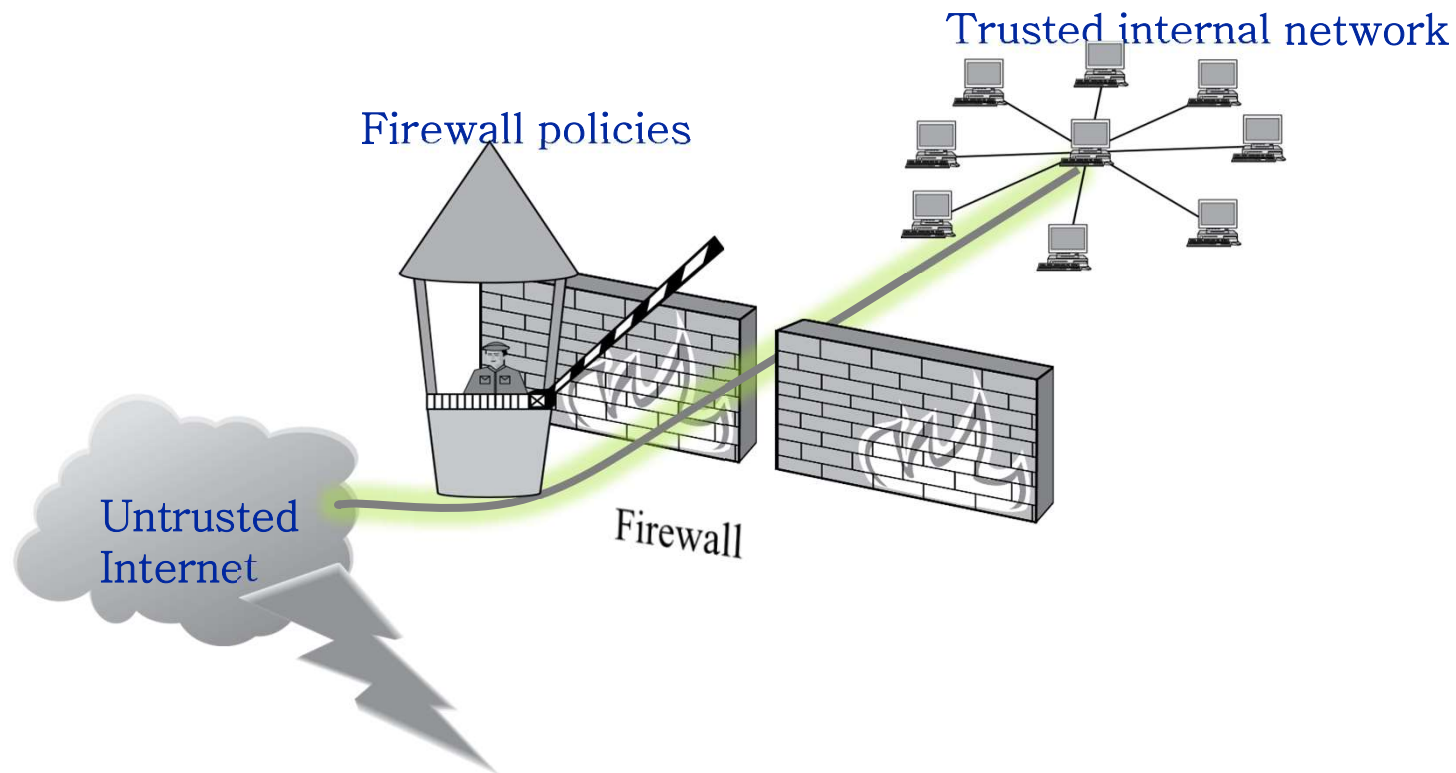
Firewall

- A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Policies

- 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**.



Policy 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).

Blacklist and Whitelist

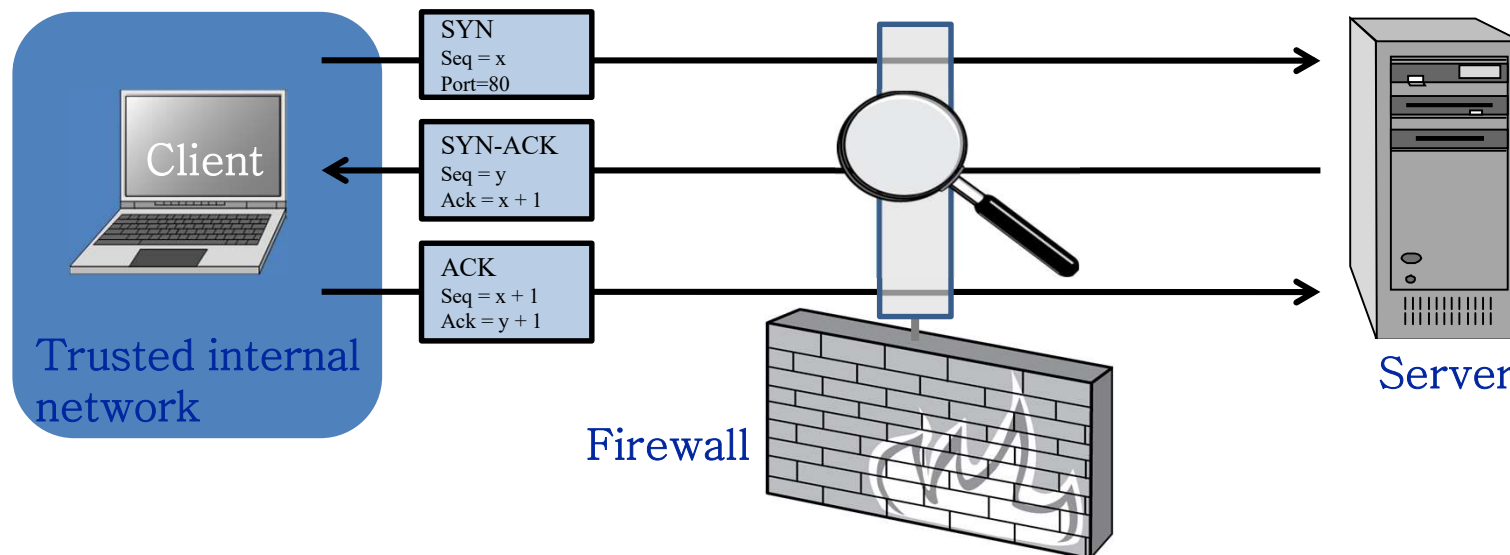
- Two fundamental approaches to creating firewall policies (or rulesets)
- **Blacklist** approach (default-allow)
 - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
 - Pros: flexible in ensuring that service to the internal network is not disrupted 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, ...)

Stateless Firewall

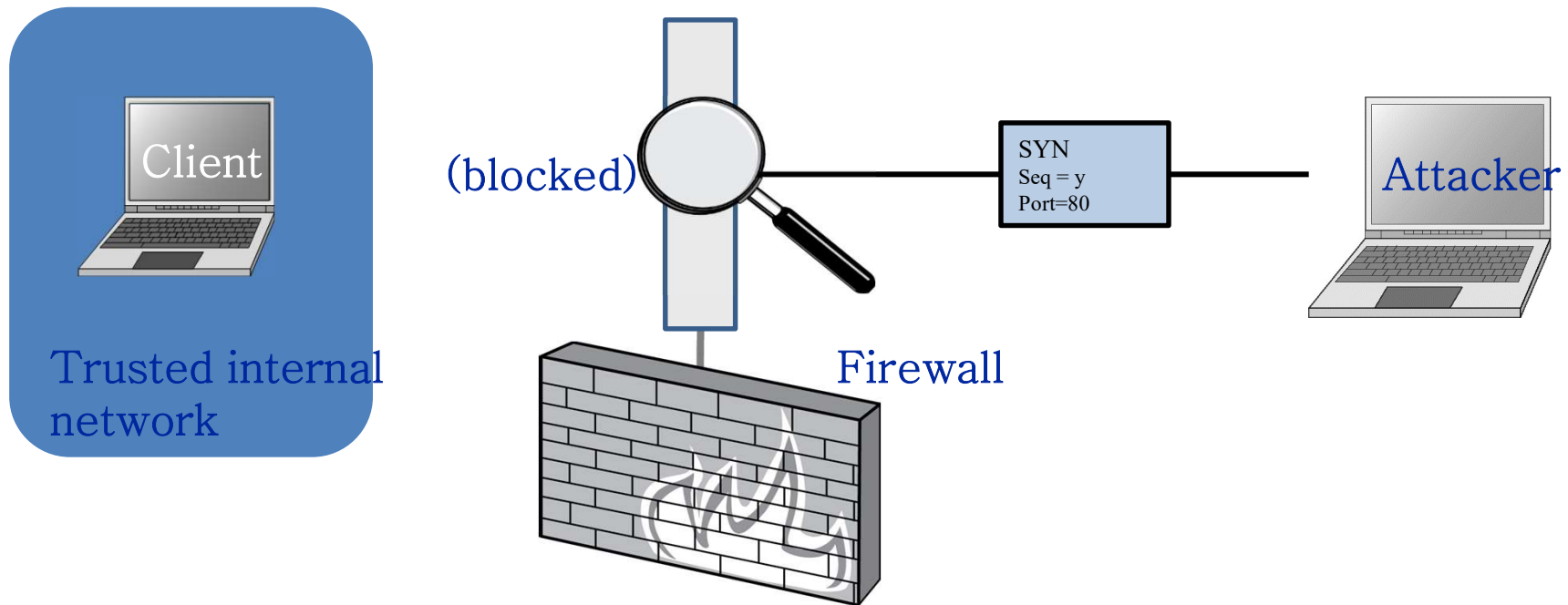
- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing.
- Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



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

Stateless Restrictions

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



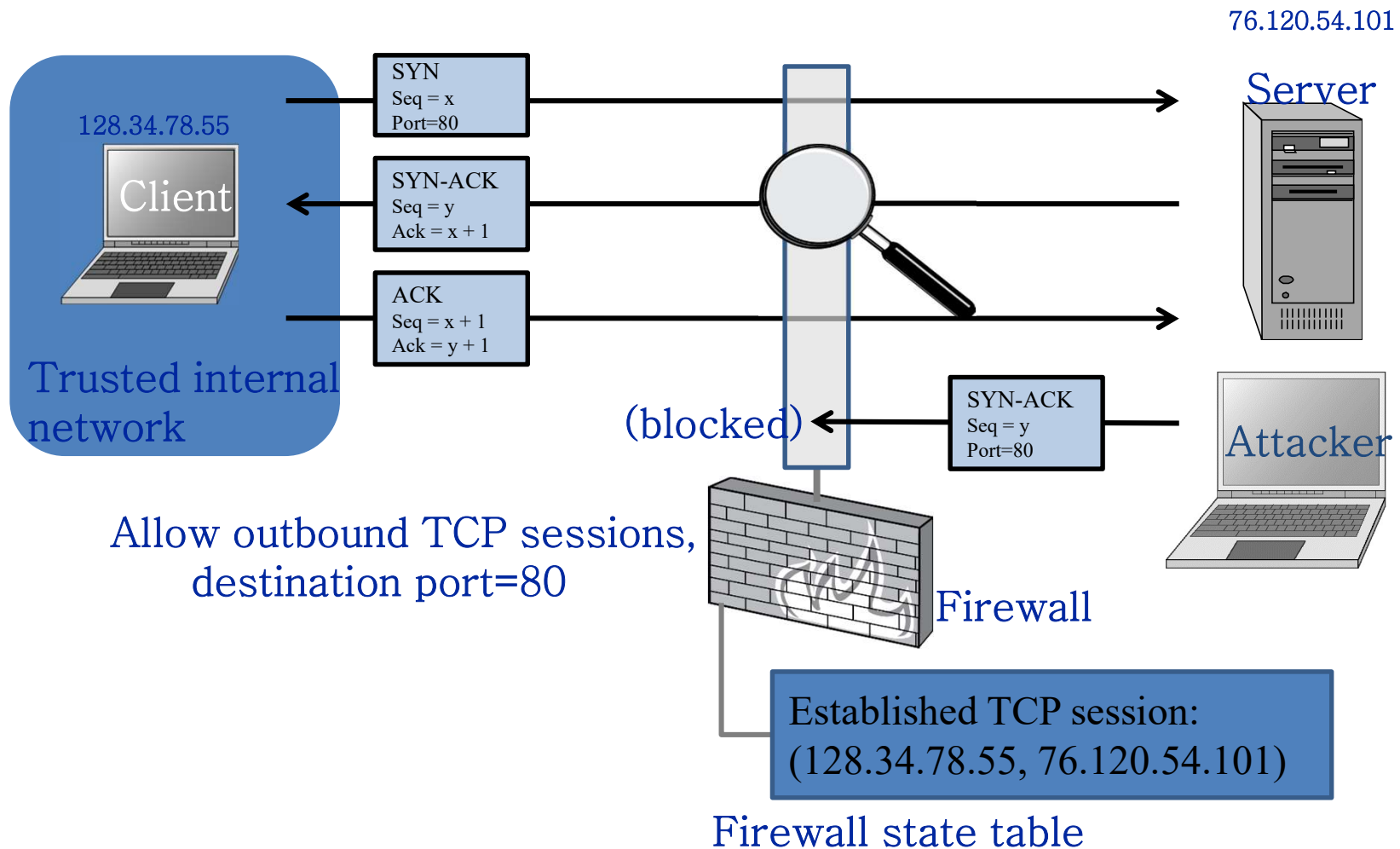
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

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.

Example

- Allow only requested TCP connections:

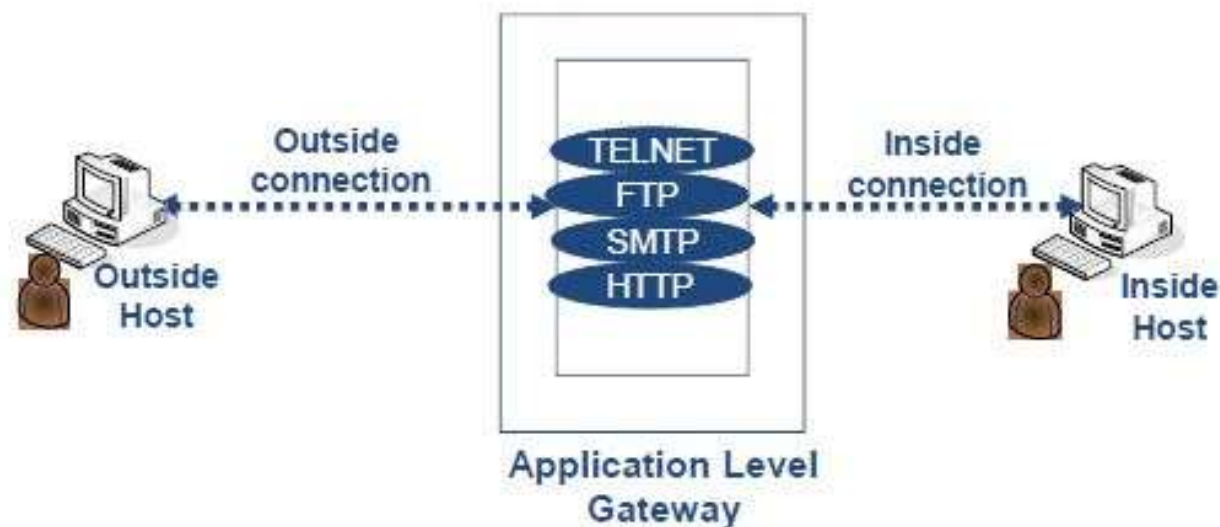


Contd...

- TCP-based connections are easy to check
 - TCP SYN packet
- UDP-based traffic is not so clear
 - There is no UDP connection set up
 - Treat a UDP session starts when a legitimate UDP packet is allowed through the firewall (such as from inside to outside)
 - Session is defined by (source IP, source port, dest IP, dest port)

Application Level Firewall

- An application firewall is a type of firewall that scans, monitors and controls network, Internet and local system access and operations to and from an application or service.
- This type of firewall makes it possible to control and manage the operations of an application or service that's external to the IT environment.

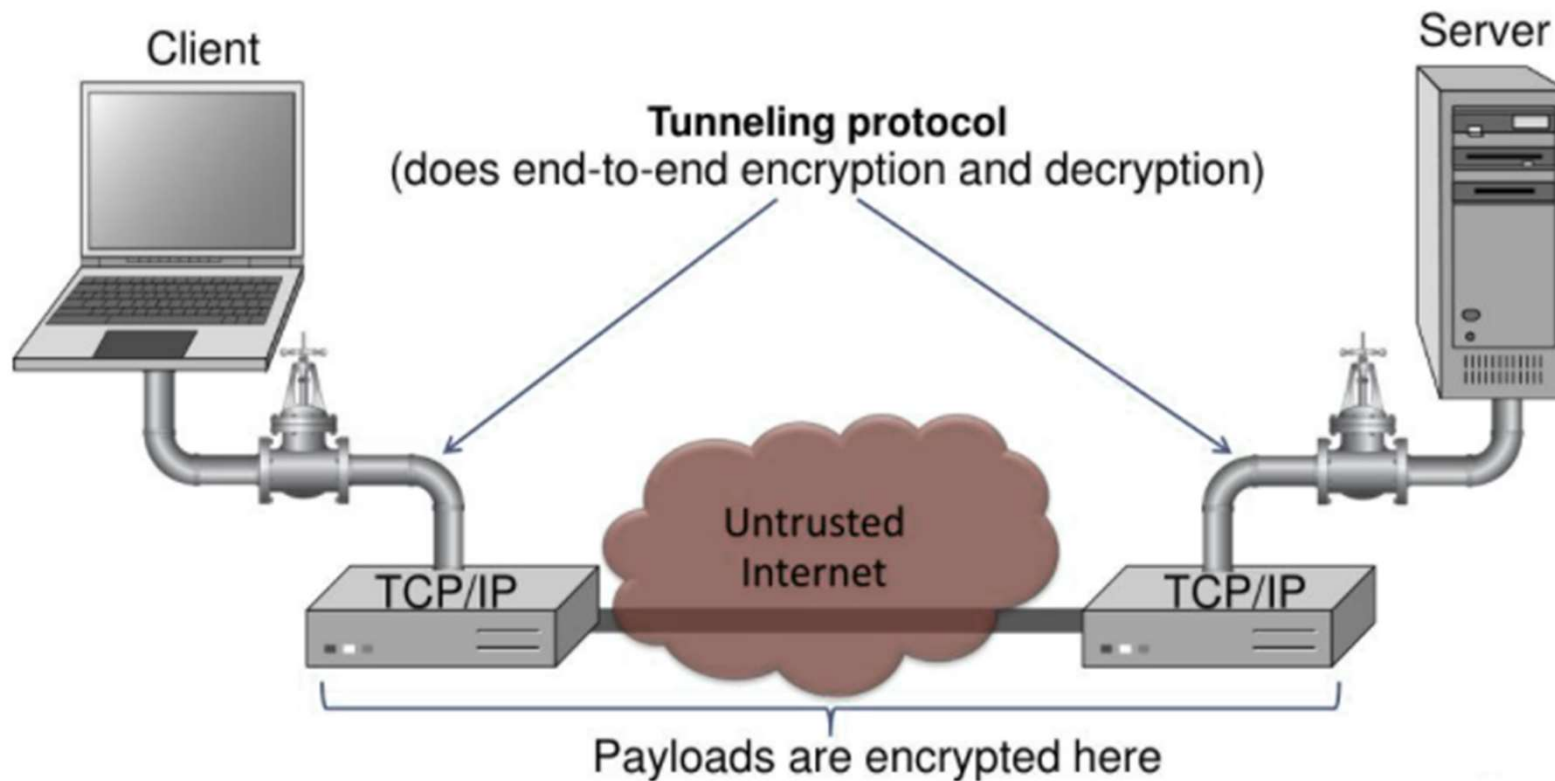


Tunnels

- The contents of TCP packets are not normally encrypted, so if someone is eavesdropping on a TCP connection, he can often see the complete contents of the payloads in this session.
- One way to prevent such eavesdropping without changing the software performing the communication is to use a **tunneling protocol**.
- In such a protocol, the communication between a client and server is automatically encrypted, so that useful eavesdropping is infeasible.

Tunneling Prevents Eavesdropping

- Packets sent over the Internet are automatically encrypted.



Intrusion Detection System

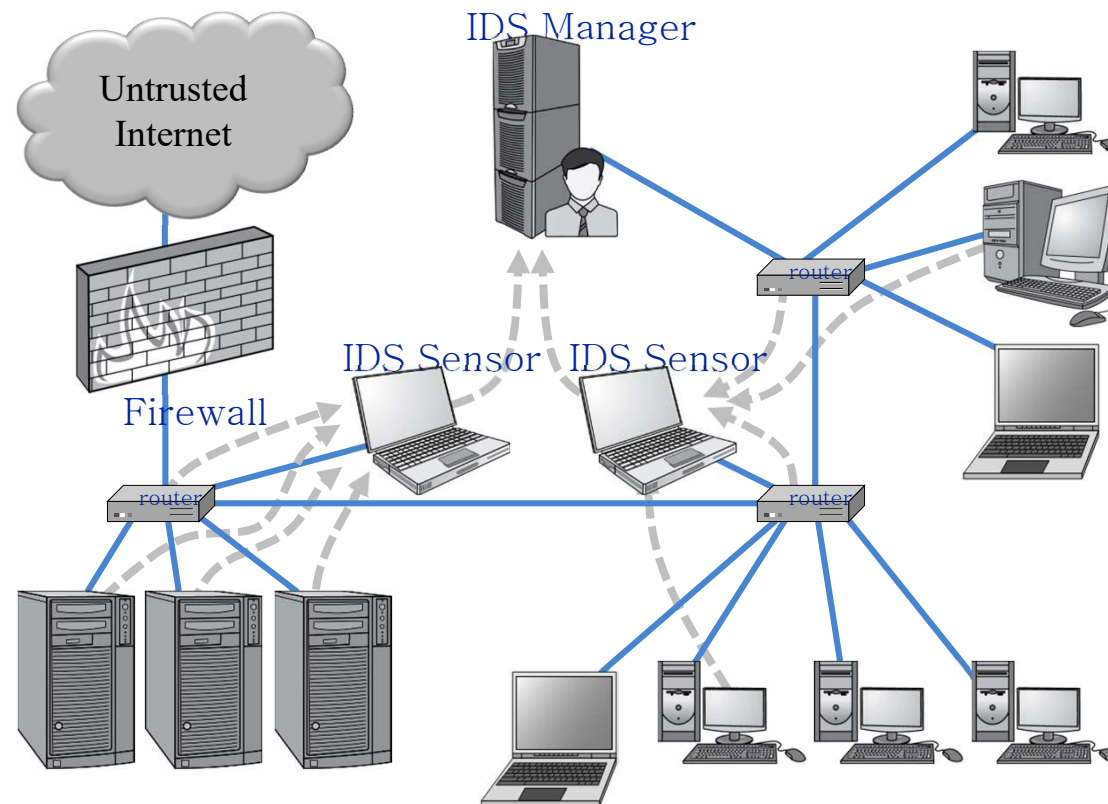
- **Intrusion**
 - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing / networking resources)
- **Intrusion detection**
 - The identification through intrusion signatures and report of intrusion activities
- **Intrusion prevention**
 - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

IDS Components

- **Sensors:** Sensors are responsible for collecting data.
- **Analyzers:** Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred.
- **User Interface:** The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a manager, director, or console component.

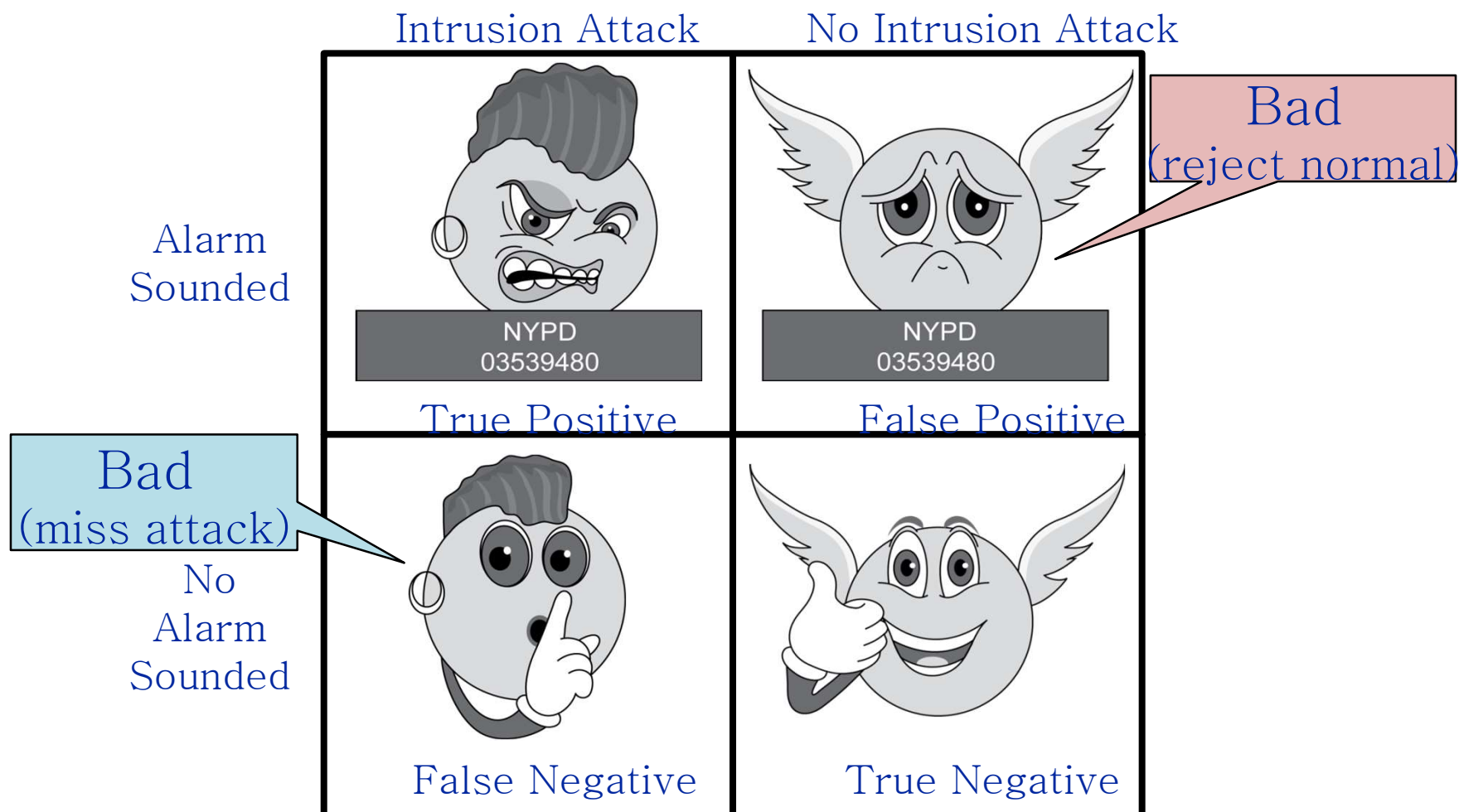
Contd...

- **IDS analyzer (manager)** compiles data from the IDS sensors to determine if an intrusion has occurred.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.



Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative).



How to calculate the accuracy of an IDS?

$$TPR = \frac{a}{a + c}$$

$$TNR = \frac{b}{b + d}$$

$$Accuracy = \frac{a + b}{a + b + c + d}$$

where,

a = attack traffic identified correctly

b = legitimate traffic identified correctly

c = attack traffic mis-classified as legitimate

d = legitimate traffic mis-classified as attack

TPR: True Positive Rate

TNR: True Negative Rate

Base-Rate Fallacy

- true-positive rate is conflict with false-negative rate.
- ✓ There is a trade-off
- If # of intrusions \ll # of all events, the effectiveness of an intrusion detection system can be reduced.
- In particular, the effectiveness of some IDSs can be misinterpreted due to a statistical error known as the base-rate fallacy.
- This type of error occurs when the probability of some conditional event is assessed without considering the “base rate” of that event.

Contd...

- Suppose an IDS has 1% chance of false positives, and 1% of false negatives. Suppose further...
 - An intrusion detection system generates 1,000,100 log entries.
 - Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Among the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative**.
- Among the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That means false alarm rate is roughly 99%!

Types of IDS

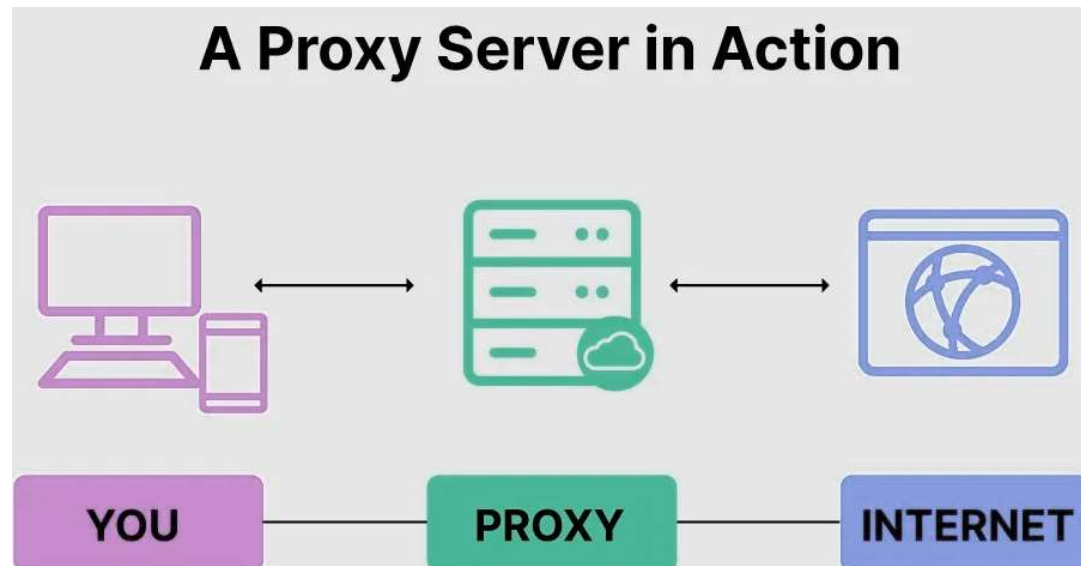
- **Host-based IDS (HIDS):** Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.
- **Network-based IDS (NIDS):** Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.
- **Distributed or hybrid IDS:** Combines information from a number of sensors, often both host and network-based, in a central analyzer that is able to better identify and respond to intrusion activity.

Analysis Approaches

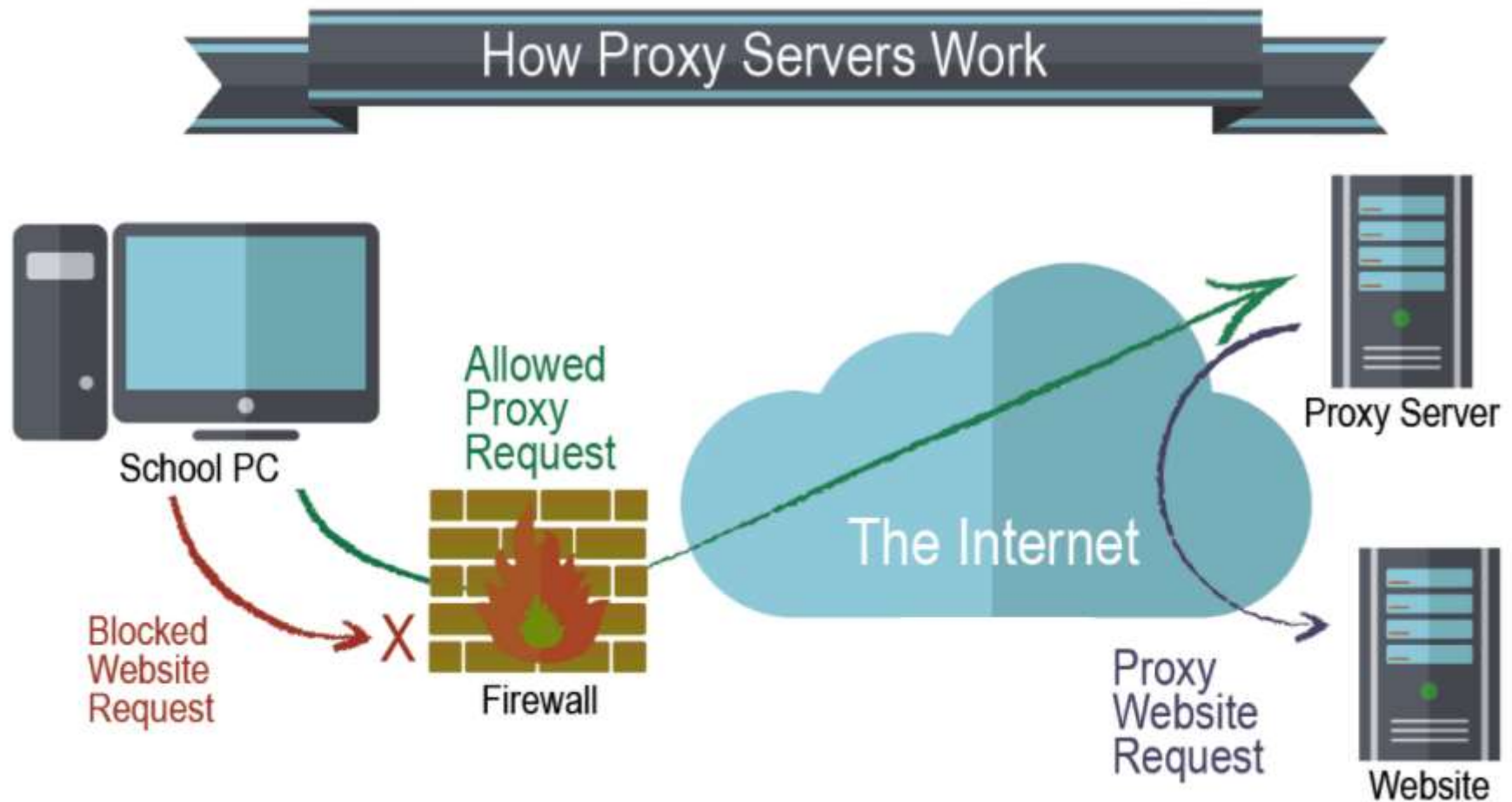
- **Rule/Signature Based Intrusion Detection**
 - Rules and signatures identify the types of actions that match certain known profiles for an intrusion attack
 - Alarm raised can indicate what attack triggers the alarm
 - **Problem: Cannot deal with unknown attacks**
- **Statistical/Anomaly Based Intrusion Detection**
 - Statistical representation (**profile**) of the typical ways that a user acts or a host is used
 - Determine when a user or host is acting in highly unusual, anomalous ways.
 - Alarm when a user or host deviates significantly from the stored profile for that person or machine
 - **Problem: High false positive rate, cannot tell which attack triggers the alarm**

Proxy Server

- A proxy server provides a gateway between users and the internet. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.
- Because a proxy server has its own IP address, it acts as a go-between for a computer and the internet. Your computer knows this address, and when you send a request on the internet, it is routed to the proxy, which then gets the response from the web server and forwards the data from the page to your computer’s browser.



Hide Your Real IP Address Behind a Proxy



Benefits of a Proxy Server

- **Enhanced security:** Can act like a firewall between your systems and the internet. Without them, hackers have easy access to your IP address, which they can use to infiltrate your computer or network.
- **Private browsing, watching, listening, and shopping:** Use different proxies to help you avoid getting inundated with unwanted ads or the collection of IP-specific data.
- **Access to location-specific content:** You can designate a proxy server with an address associated with another country. You can, in effect, make it look like you are in that country and gain full access to all the content computers in that country are allowed to interact with.
- **Prevent employees from browsing inappropriate or distracting sites:** You can use it to block access to websites that run contrary to your organization's principles. Some organizations block social media sites like Facebook.

Types of Proxy Servers

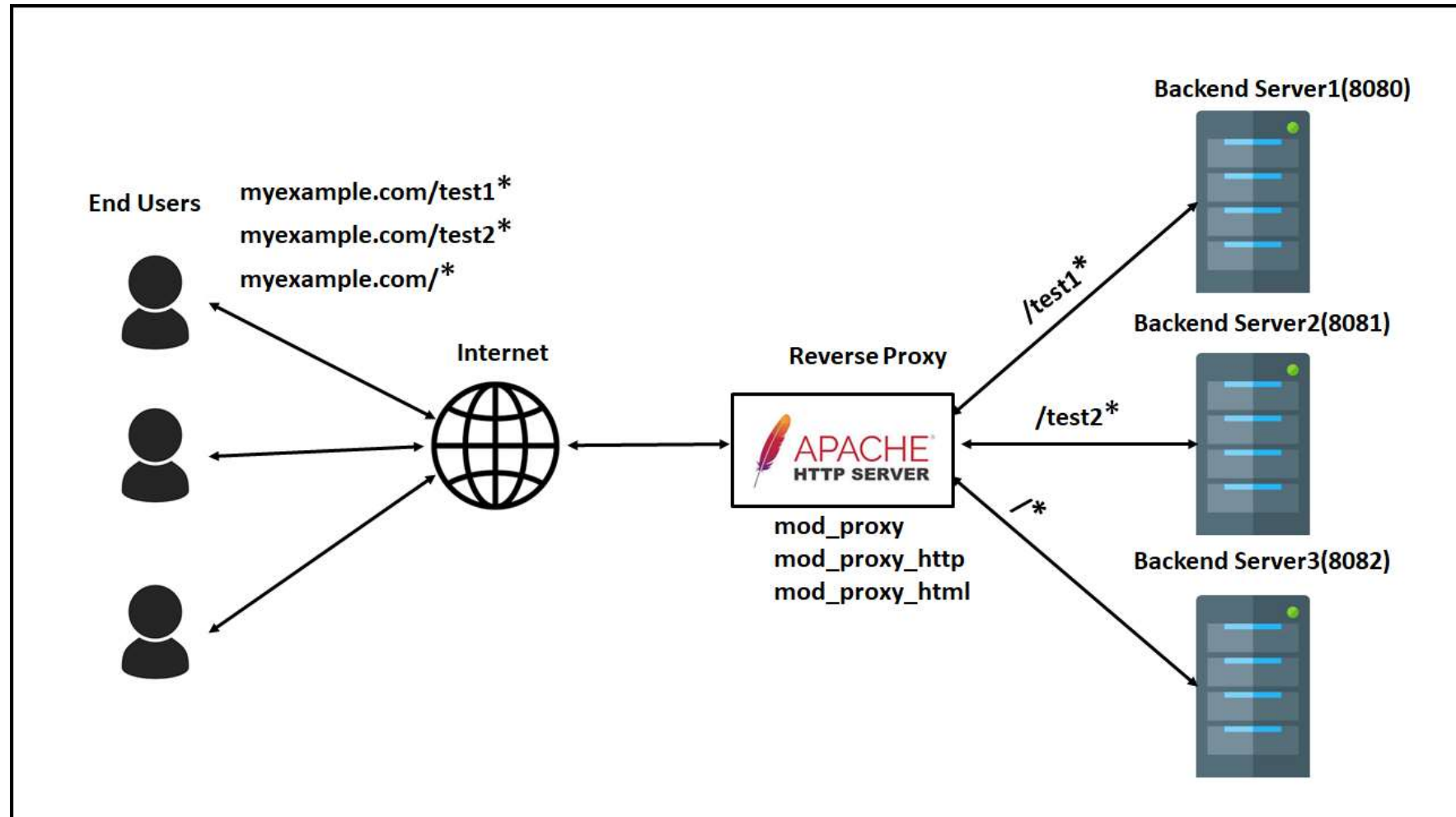
1. Forward Proxies:

- ✓ A forward proxy server sits between the client and an external network. It evaluates the outbound requests and takes action on them before relaying that request to the external resource.
- ✓ Most proxy services that we're likely to encounter are forward proxies. Virtual Private Networks and Web content filters are both examples of forward proxies.

2. Reverse Proxies:

- ✓ A reverse proxy server sits between a network and multiple other internal resources.
- ✓ A large website might have dozens of servers that collectively serve requests from a single domain.
- ✓ To accomplish that, client requests would resolve to a machine that would act as a load balancer.
- ✓ The load balancer would then proxy that traffic back to the individual servers.
- ✓ Some popular open source reverse proxies are: Varnish, Squid

Contd...



Assignment: Study other types of proxies.

Demilitarized Zone (DMZ)

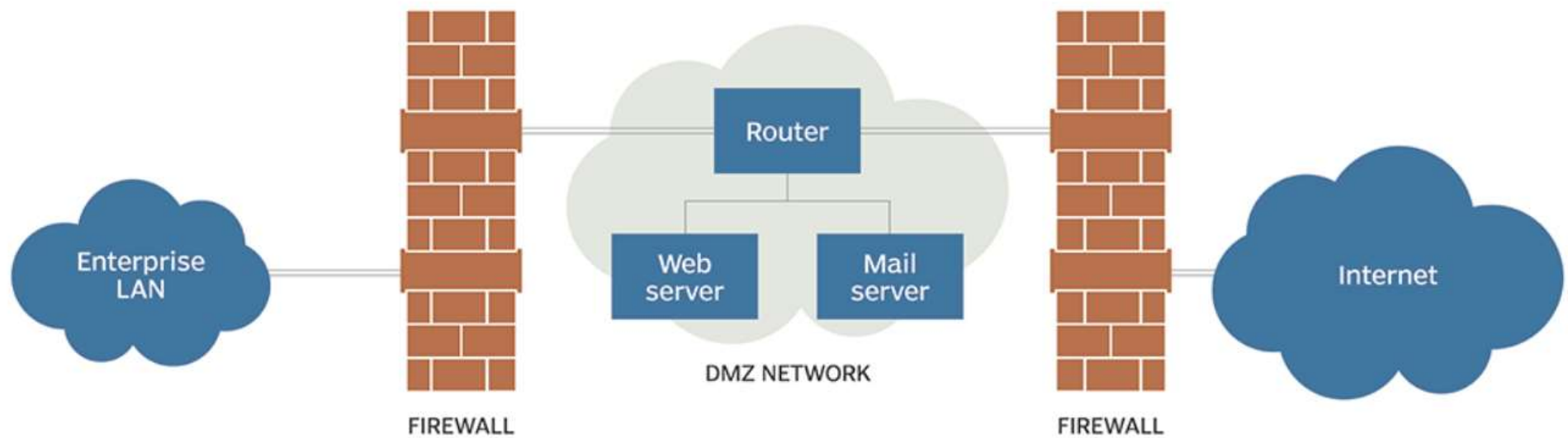
- In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet.
- DMZs are also known as perimeter networks or screened subnetworks.
- DMZs provide a level of network segmentation that helps protect internal corporate networks. These subnetworks restrict remote access to internal servers and resources, making it difficult for attackers to access the internal network. This strategy is useful for both individual use and large organizations.
- Businesses place applications and servers that are exposed to the internet in a DMZ, separating them from the internal network. The DMZ isolates these resources so, if they are compromised, the attack is unlikely to cause exposure, damage or loss.

How does DMZ Work?

- DMZs function as a buffer zone between the public internet and the private network. The DMZ subnet is deployed between two firewalls. All inbound network packets are then screened using a firewall or other security appliance before they arrive at the servers hosted in the DMZ.
- If better-prepared threat actors pass through the first firewall, they must then gain unauthorized access to the services in the DMZ before they can do any damage. Those systems are likely to be hardened against such attacks.
- Finally, assuming well-resourced threat actors take over a system hosted in the DMZ, they must still break through the internal firewall before they can reach sensitive enterprise resources.

Contd...

DMZ network architecture



Thank You !!!

Introduction to Cyber Security

Module 4

Network Security

Part B

Internet Security Protocols

After studying this topic, you should be able to:

- Provide an overview of MIME.
- Understand the functionality of S/MIME and the security threats it addresses.
- Explain the key components of SSL.
- Discuss the use of HTTPS.
- Provide an overview of IPsec.

Secure Email and S/MIME

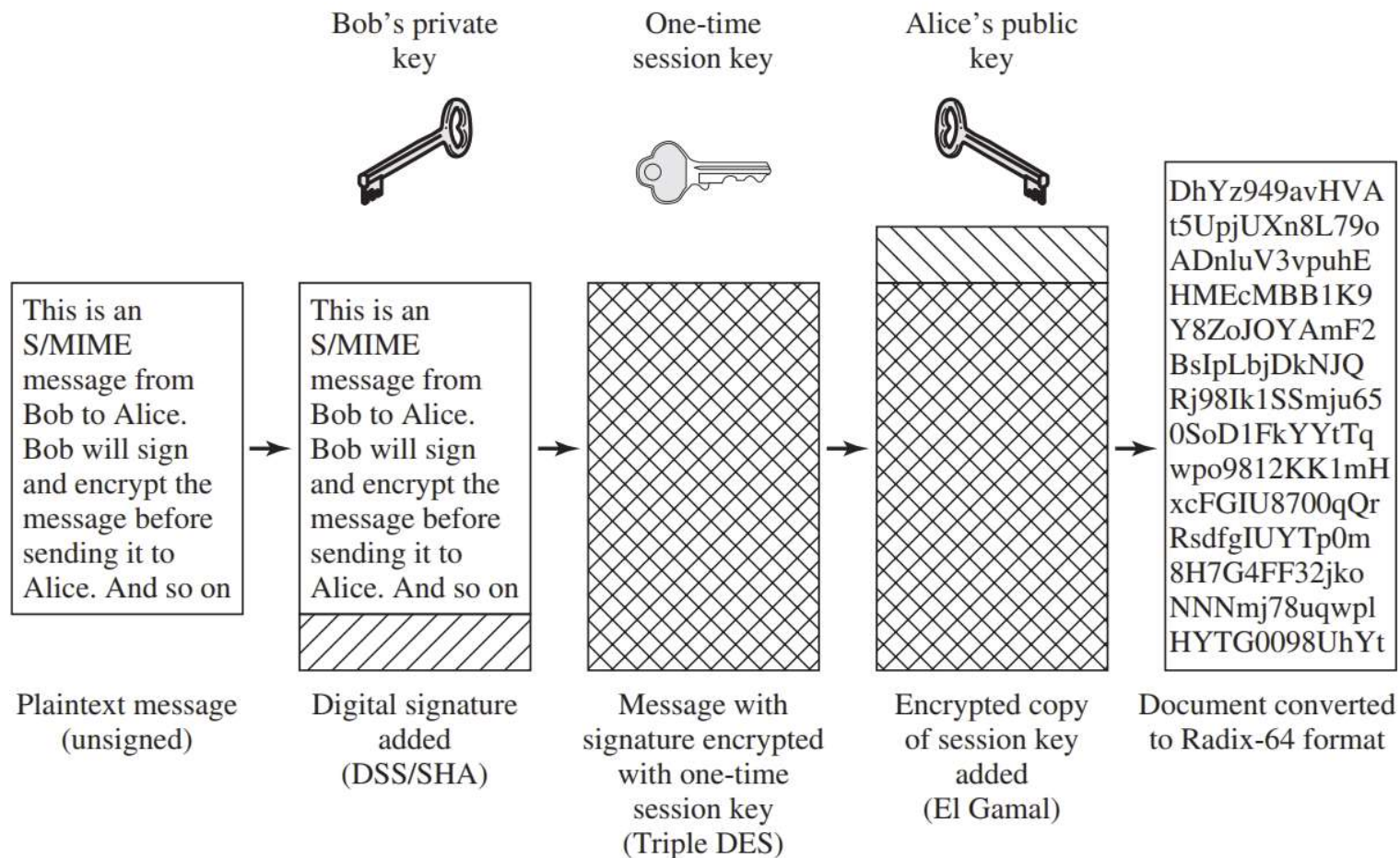
- S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.
- **MIME:**
 - ✓ MIME is an extension to the old RFC 822 specification of an Internet mail format.
 - ✓ RFC 822 defines a simple header with To, From, Subject, and other fields that can be used to route an e-mail message through the Internet and that provides basic information about the e-mail content.
 - ✓ RFC 822 assumes a simple ASCII text format for the content.

MIME

- MIME provides a number of new header fields that define information about the body of the message, including the format of the body and any encoding that is done to facilitate transfer.
- Most important, MIME defines a number of content formats, which standardize representations for the support of multimedia e-mail.
- Examples include text, image, audio, and video.

S/MIME

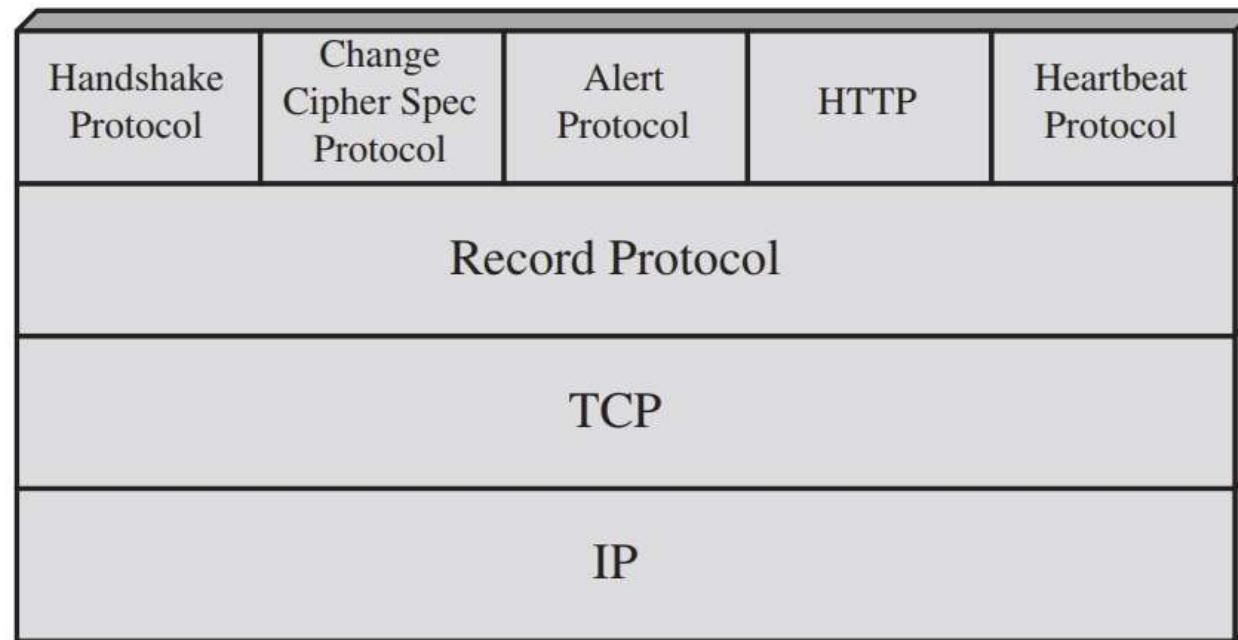
- S/MIME is defined as a set of additional MIME content types and provides the ability to sign and/or encrypt e-mail messages.



SSL and TLS

Transport Layer Security (TLS) Architecture:

- ✓ TLS is designed to make use of TCP to provide a reliable end-to-end secure service.
- ✓ TLS is not a single protocol but rather two layers of protocols



SSL/TLS Protocol Stack

HTTPS

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- The HTTPS capability is built into all modern Web browsers. Its use depends on the Web server supporting HTTPS communication.
- A normal HTTP connection uses port 80. If HTTPS is specified, port 443 is used, which invokes SSL.

Contd...

- When HTTPS is used, the following elements of the communication are encrypted:
 - ✓ URL of the requested document
 - ✓ Contents of the document
 - ✓ Contents of browser forms (filled in by browser user)
 - ✓ Cookies sent from browser to server and from server to browser
 - ✓ Contents of HTTP header

IPv4 and IPv6 Security

- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The key management facility is concerned with the secure exchange of keys.
- The current version of IPsec, known as IPsecv3, encompasses authentication and confidentiality.
- Key management is provided by the Internet Key Exchange standard, IKEv2.

Honeypots

- A further component of intrusion detection technology is the honeypot.
- Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.
- Honeypots are designed to:
 - ✓ Divert an attacker from accessing critical systems.
 - ✓ Collect information about the attacker's activity.
 - ✓ Encourage the attacker to stay on the system long enough for administrators to respond.
- These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system would not access.

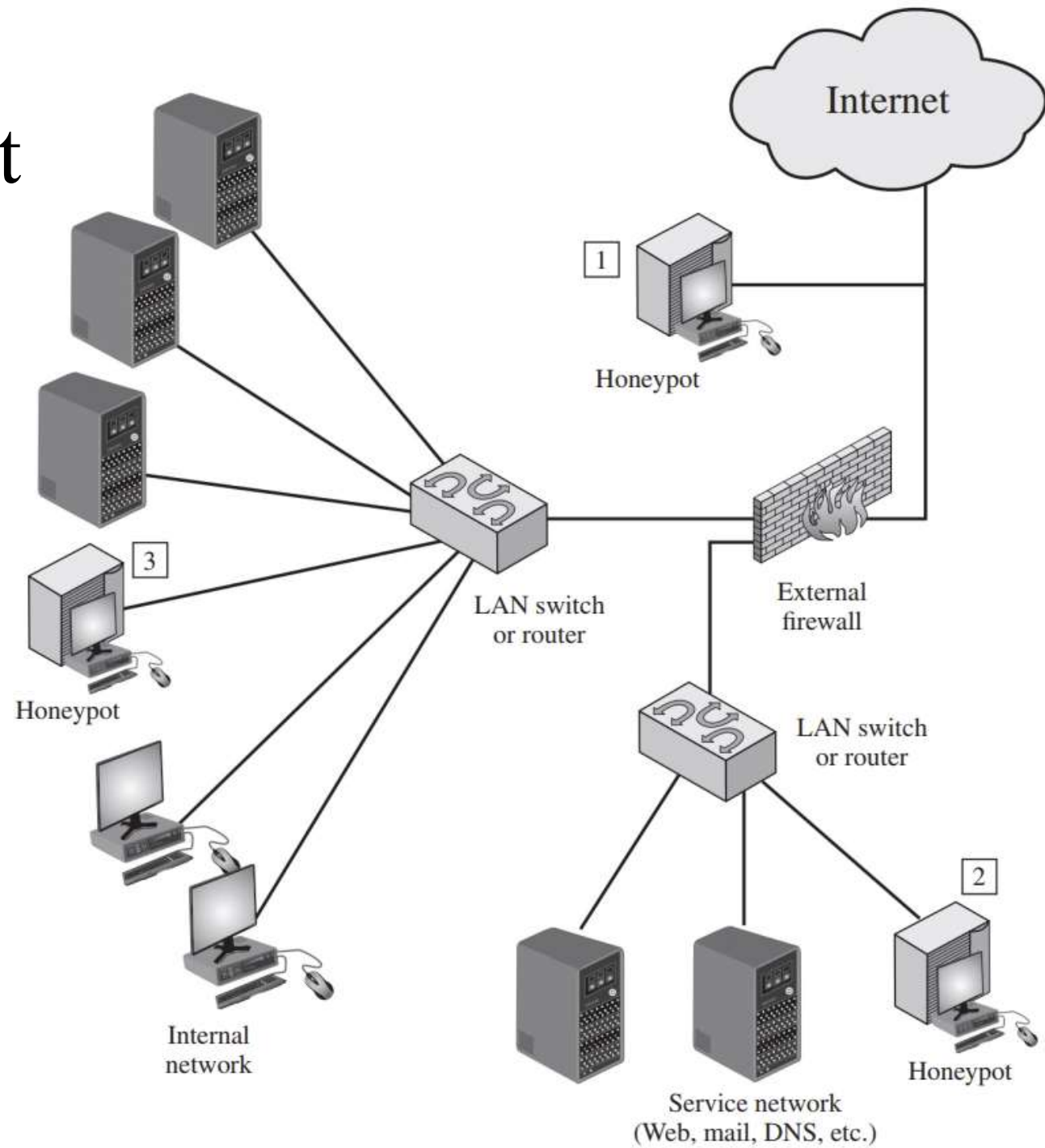
Contd...

- Thus, any access to the honeypot is suspect.
- The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.
- Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.
- The honeypot is a resource that has no production value. There is no legitimate reason for anyone outside the network to interact with a honeypot.
- Thus, any attempt to communicate with the system is most likely a probe, scan, or attack.

Contd...

- Conversely, if a honeypot initiates outbound communication, the system has probably been compromised.
- Honeypots are typically classified as being either low or high interaction.
- ✓ **Low interaction honeypot:** Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems.
- ✓ **High interaction honeypot:** Is a real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers.

Deployment Locations



System Security

Dr. Amit Praseed

The Microsoft Dialer Exploit

- Microsoft Dialer was a program for dialing a telephone
- In 1999, security analyst David Litchfield was interested in this software
 - Dialer had to accept phone numbers of different lengths, given country variations, outgoing access codes, and remote signals
 - He tried dialer.exe with a 20, 25 and 50 digit phone numbers, and the program still worked fine.
 - When he tried a 100-digit phone number, the program crashed.
 - The programmer had probably made an undocumented and untested decision that nobody would ever try to dial a 100-digit phone number
 - The dialer.exe program is treated as a program call by the operating system, so by controlling what dialer.exe overwrote, we can redirect execution to continue anywhere with any instructions we want

What will happen here...

```
#include <stdio.h>

int main()
{
    char s1[5], s2[5];

    printf("%s\n",s2);

    scanf("%s",s1);

    printf("%s\n",s2);

    return 0;
}
```

Input: abcdefgh

What will happen here...

```
#include <stdio.h>

int main()
{
    char s1[5], s2[5];

    printf("%s\n",s2);

    scanf("%s",s1);

    printf("%s\n",s2);

    return 0;
}
```

Input: abcdefgh

Output:



abcdefgh

fgh

Memory Allocation

- Memory is a limited but flexible resource; any memory location can hold any piece of code or data.
- To make managing computer memory efficient, operating systems jam one data element next to another, without regard for data type, size, content, or purpose
- Program counter indicates the next instruction - as long as program flow is sequential, hardware bumps up the value in the program counter
- Instructions such as IF, WHILE, FOR, GOTO or CALL divert the flow of execution, causing the hardware to put a new destination address into the program counter.
- Hardware simply fetches the byte (or bytes) at the address pointed to by the program counter and executes it as an instruction.
- **Instructions and data are all binary strings; only the context of use says a byte, for example, 0x41 represents the letter A, the number 65, or the instruction to move the contents of register 1 to the stack pointer**

Memory Allocation - The Security Aspect

- Hardware recognizes more than one mode of instruction - privileged instructions that can be executed only when the processor is running in a protected mode.
 - Trying to execute something that does not correspond to a valid instruction or trying to execute a privileged instruction when not in the proper mode will cause a program fault.
 - When hardware generates a program fault, it stops the current thread of execution and transfers control to code that will take recovery action
- In memory, code is indistinguishable from data. The origin of code (respected source or attacker) is also not visible.
- The attacker's trick is to cause data to spill over into executable code and then to select the data values such that they are interpreted as valid instructions to perform the attacker's goal.
- For some attackers this is a two-step goal: First cause the overflow and then experiment with the ensuing action to cause a desired, predictable result

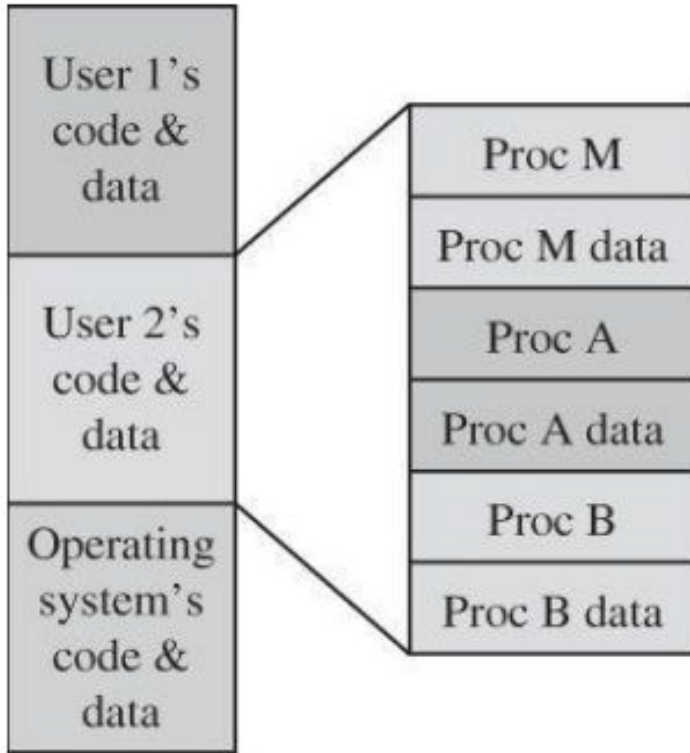
Harm from Overflows

- The attacker may replace code in the system space
 - Every program is invoked by an operating system that may run with higher privileges than those of a regular program
 - By replacing a few instructions right after returning from his or her own procedure, the attacker regains control from the operating system, possibly with raised privileges - **privilege escalation**
- The intruder may wander into an area called the stack and heap
 - By causing an overflow into the stack, the attacker can change either the old stack pointer or the return address
 - Changing the context or return address allows the attacker to redirect execution to code written by the attacker.

Implications of Overwriting Memory

- If the extra character overflows into the user's data space, it simply overwrites an existing variable value, perhaps affecting the program's result but affecting no other program or data
- If it overlaps an already executed instruction, the user should perceive no effect.
- If it overlaps an instruction that is not yet executed, the machine will try to execute an instruction with operation code corresponding to the overwritten data - if there is no instruction with operation code 0x42, the system will halt on an illegal instruction exception
- What happens if the system owns the space???

Implications of Overwriting Memory



A data overflow either falls strictly within a data space or it spills over into an adjacent code area. The data end up on top of one of

- another piece of your data
- an instruction of yours
- data or code belonging to another program
- data or code belonging to the operating system

Overflow Countermeasures

- Check lengths before writing
- Confirm that array subscripts are within limits
- Double-check boundary condition code to catch possible off-by-one errors
- Monitor input and accept only as many characters as can be handled
- Use string utilities that transfer only a bounded amount of data
- Check procedures that might overrun their space
- Limit programs' privileges, so if a piece of code is overtaken maliciously, the violator does not acquire elevated system privileges as part of the compromise.

Incomplete Mediation

- Verifying that the subject is authorized to perform the operation on an object is called mediation

`http://www.somesite.com/subpage/userinput.asp?
parm1=(808)555-1212&parm2=2015Jan17`

- The parameters parm1 and parm2 look like a telephone number and a date
- What would happen if parm2 were submitted as 1800Jan01? Or 1800Feb30? Or 2048Min32? Or 1Aardvark2Many?
- One possibility is that the system would fail catastrophically
- Another possibility is that the receiving program would continue to execute but would generate a very wrong result

Input Validation

- Client Side Validation
 - the program can restrict choices to valid ones only
 - search for and screen out errors
- However, attackers are free to modify the GET or POST parameters
- Solution: Complete Mediation
- Time-of-Check to Time-of-Use
 - modern processors and operating systems usually change the order in which instructions and procedures are executed
 - Instructions that appear to be adjacent may not actually be executed immediately after each other, either because of intentionally changed order or because of the effects of other processes in concurrent execution
 - It exploits the delay between the two actions: check and use, i.e. between the time the access was checked and the time the result of the check was used, a change occurred, invalidating the result of the check
 - The access-checking software must own the request data until the requested action is complete.
 - Another protection technique is to ensure serial integrity, that is, to allow no interruption (loss of control) during the validation

Integer Overflow

- An integer overflow is a peculiar type of overflow, in that its outcome is somewhat different from that of the other types of overflows.
- An integer overflow occurs because a storage location is of fixed, finite size and therefore can contain only integers up to a certain limit.
- The overflow depends on whether the data values are signed
- When a computation causes a value to exceed any limit, the extra data does not spill over to affect adjacent data items
- Either a hardware program exception or fault condition is signaled, which causes transfer to an error handling routine, or the excess digits on the most significant end of the data item are lost.

Race Conditions

- Situation in which program behavior depends on the order in which two procedures execute
- Suppose two processes or threads are using a common shared variable $X=5$
 - P1 is trying to do $X++$
 - P2 is trying to do $X--$
 - After both P1 and P2 execute once, what will be the output?

Race Conditions

- Situation in which program behavior depends on the order in which two procedures execute
- Suppose two processes or threads are using a common shared variable $X=5$
 - P1 is trying to do $X++$
 - P2 is trying to do $X--$
 - After both P1 and P2 execute once, what will be the output?
 - Logically, the output should be $X=5$
- However, incorrect programming practices could result in the value of X being 4, 5 or 6!!!

Race Conditions

P1

register1 = X

register1 = register1 + 1

X= register1

P2

register2 = X

register2 = register2 - 1

X= register2

Race Conditions

P1:	register1 = X	{register1 = 5}
P1:	register1 = register1 + 1	{register1 = 6}
P2:	register2 = X	{register2 = 5}
P2:	register2 = register2 - 1	{register2 = 4}
P1:	X = register1	{X = 6}
P1:	X = register2	{X = 4}

Final answer becomes X=4 (incorrect)

Starbucks Gift Card Hacked using Race Conditions

- Egor Homakov of the Sakurity security consultancy found a race condition in the section of the Starbucks website responsible for checking balances and transferring money to gift cards.
- To test if an exploit would work in the real world, the researcher bought three \$5 cards.
- After a fair amount of experimentation, he managed to transfer the \$5 balance from card A to card B twice.
- As a result, Homakov now had a total balance of \$20, a net—and fraudulent—gain of \$5.
- Starbucks later issued a statement claiming that the issue had been fixed

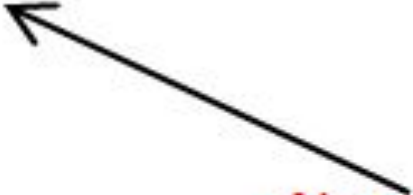
Fixing Race Conditions

- Race conditions occur when multiple processes attempt to modify the same shared data
- The solution is to make sure that only one process can access the variable at a time
- The portion of code which modifies shared variables is called critical section
- Only a single process should be able to access their critical section at a time
- This is done using the concept of semaphores or monitors
- Semaphore is an integer variable with 2 operations defined on it
 - P operation is also called wait, sleep, or down operation
 - V operation is also called signal, wake-up, or up operation.
 - Both operations are atomic and semaphore(s) is always initialized to one.

Fixing Race Conditions

```
P(Semaphore s){  
    while(S == 0); /* wait until s=0 */  
    s=s-1;  
}
```

```
V(Semaphore s){  
    s=s+1;  
}
```



Note that there is
Semicolon after while.
The code gets stuck
Here while s is 0.

Fixing Race Conditions

```
while (true) {  
    . . .  
    /* produce an item in next_produced */  
    . . .  
    wait(empty);  
    wait(mutex);  
    . . .  
    /* add next_produced to the buffer */  
    . . .  
    signal(mutex);  
    signal(full);  
}
```

Producer Code

Fixing Race Conditions

```
while (true) {  
    wait(full);  
    wait(mutex);  
    . . .  
    /* remove an item from buffer to next_consumed */  
    . . .  
    signal(mutex);  
    signal(empty);  
    . . .  
    /* consume the item in next_consumed */  
    . . .  
}
```

Consumer Code

Malicious Code

Dr. Amit Praseed

WannaCry

- The WannaCry attack 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 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
 - This acted as a killswitch to stop the spread of the ransomware
- Once it infects a system, it searches for other systems on the network and spreads using the SMB protocol

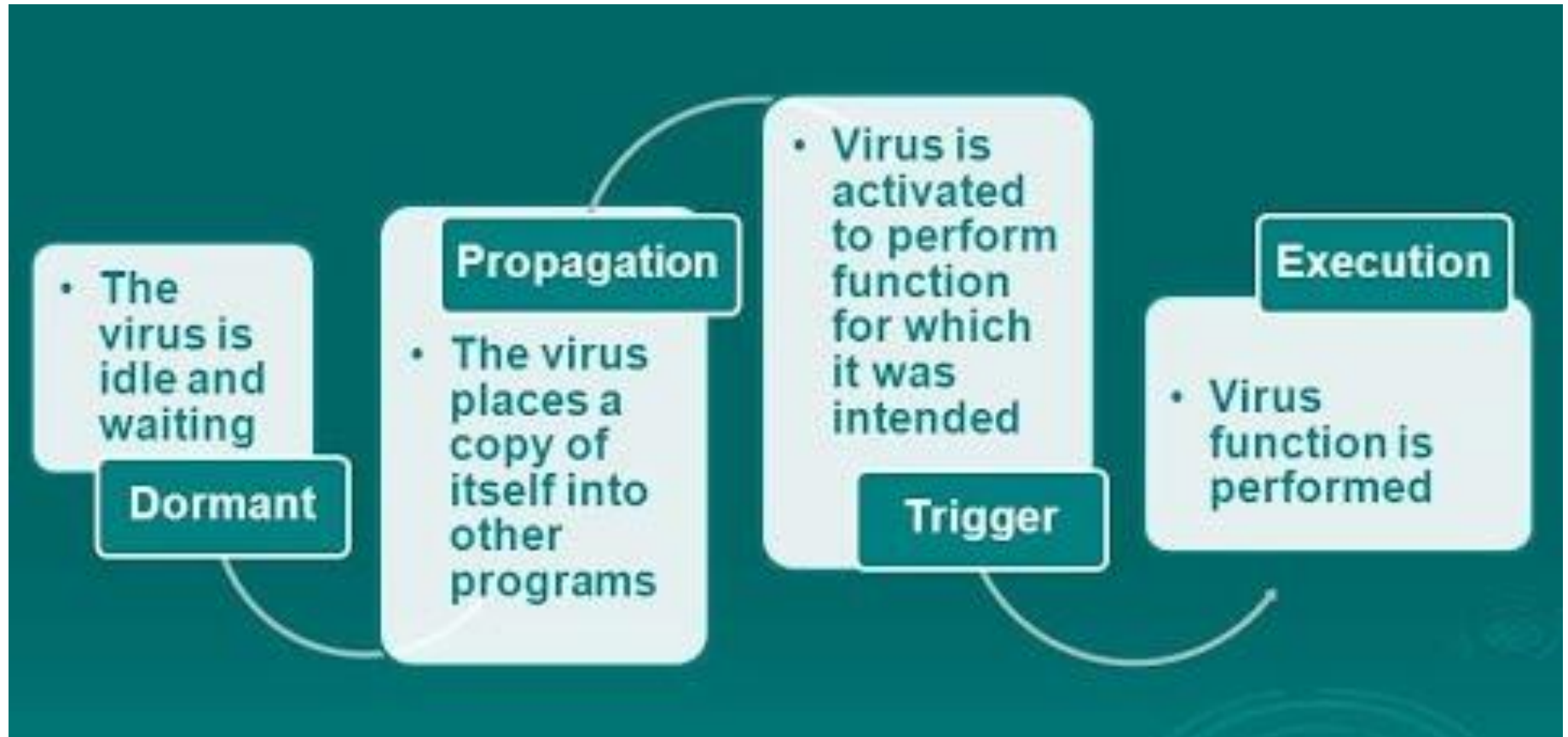
Malicious Code

- Malicious code or rogue programs or malware is the general name for programs or program parts planted by an agent with malicious intent to cause unanticipated or undesired effects
 - Distinguishes this type of code from unintentional errors, even though both kinds can certainly have similar and serious negative effects.
- Malware is an umbrella term for a wide variety of software
 - Virus
 - Worms
 - Adware
 - Spyware
 - Trojan Horses etc...

Virus

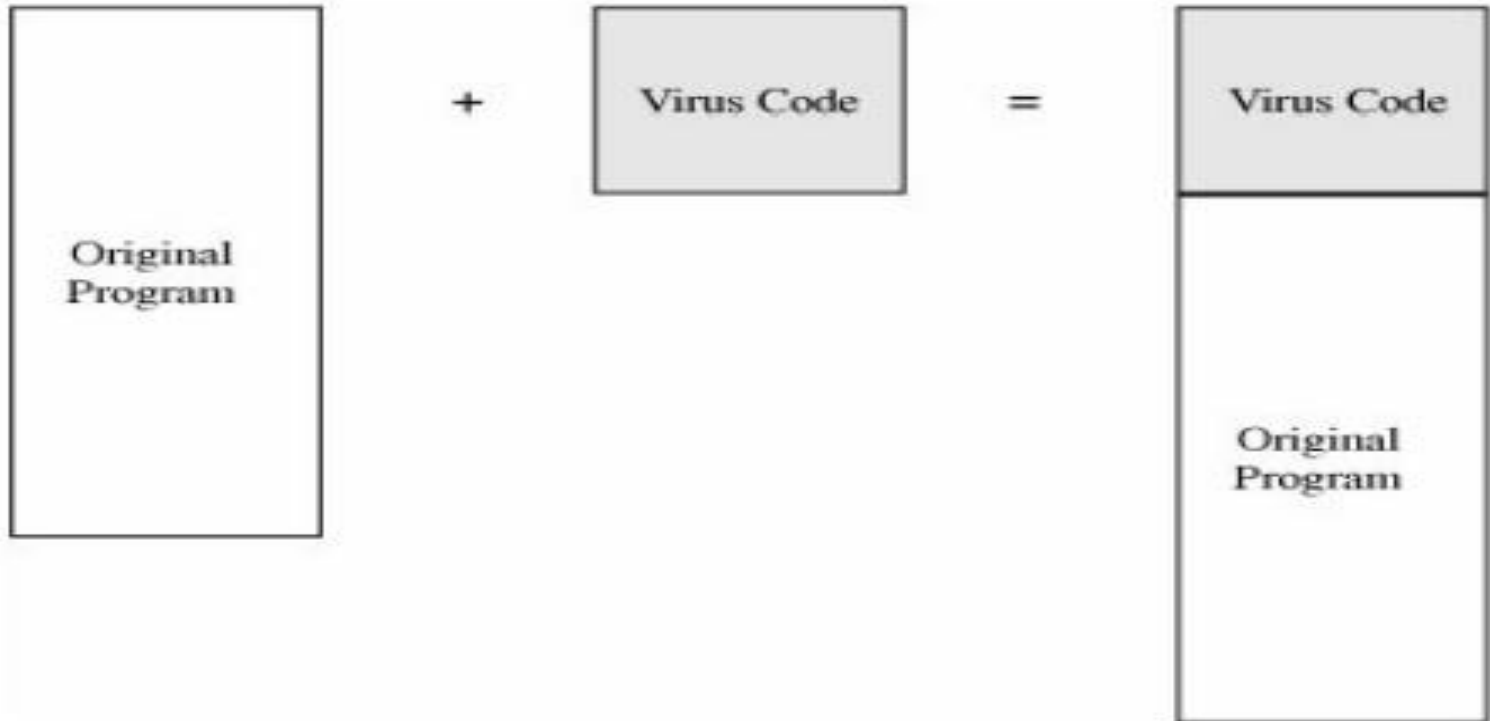
- A virus is a program that can replicate itself and pass on malicious code to other nonmalicious programs by modifying them.
- A good program can be modified to include a copy of the virus program, so the infected good program itself begins to act as a virus
- There are two broad categories of virus
 - 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.

Virus Life Cycle

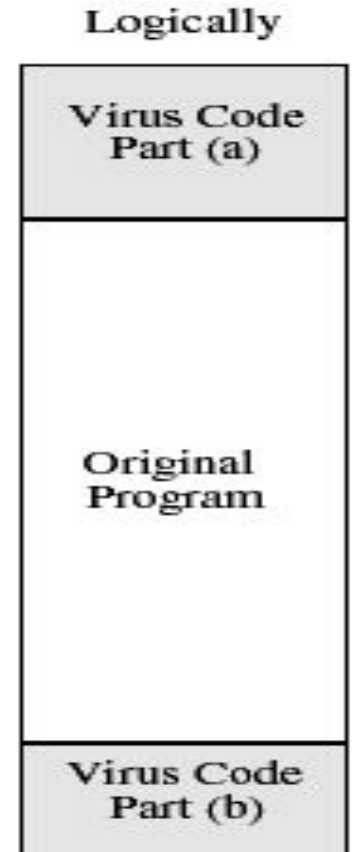
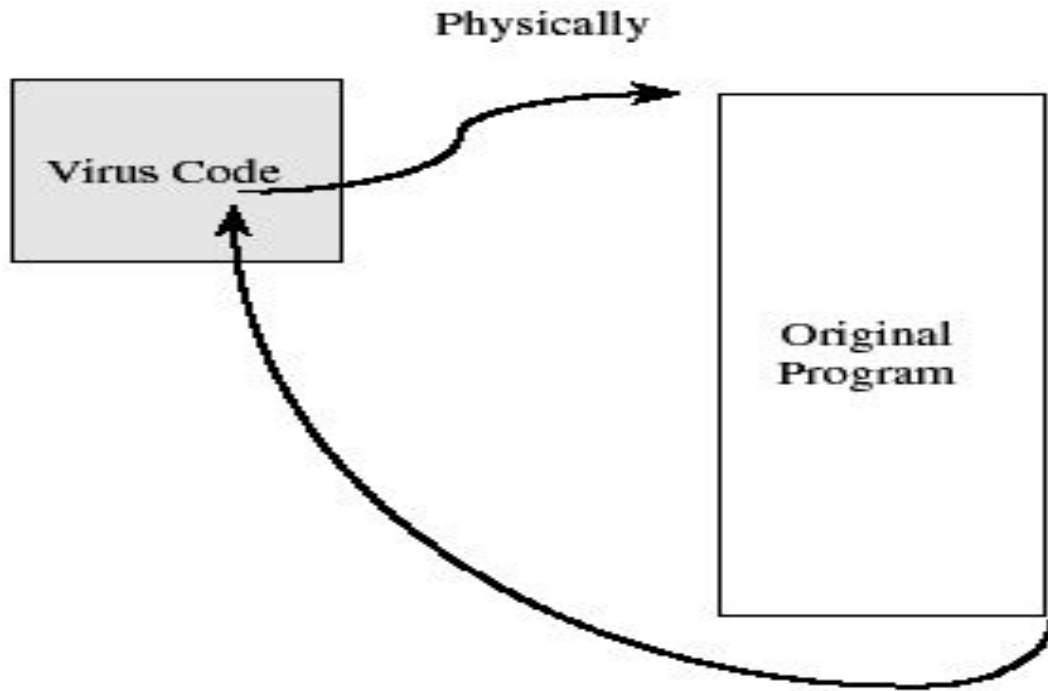


Attached Virus

Figure 3-4. Virus Appended to a Program.

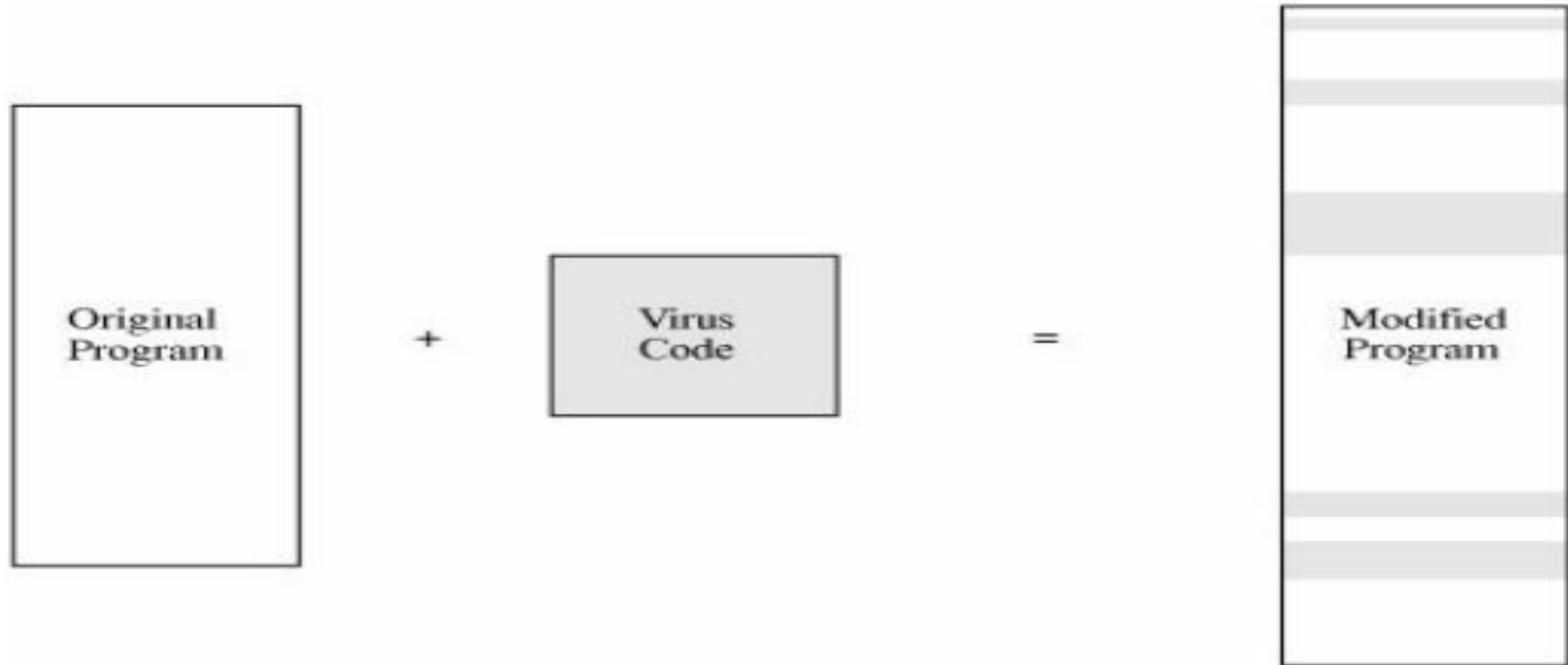


Virus surrounding a Program



Integrated Virus

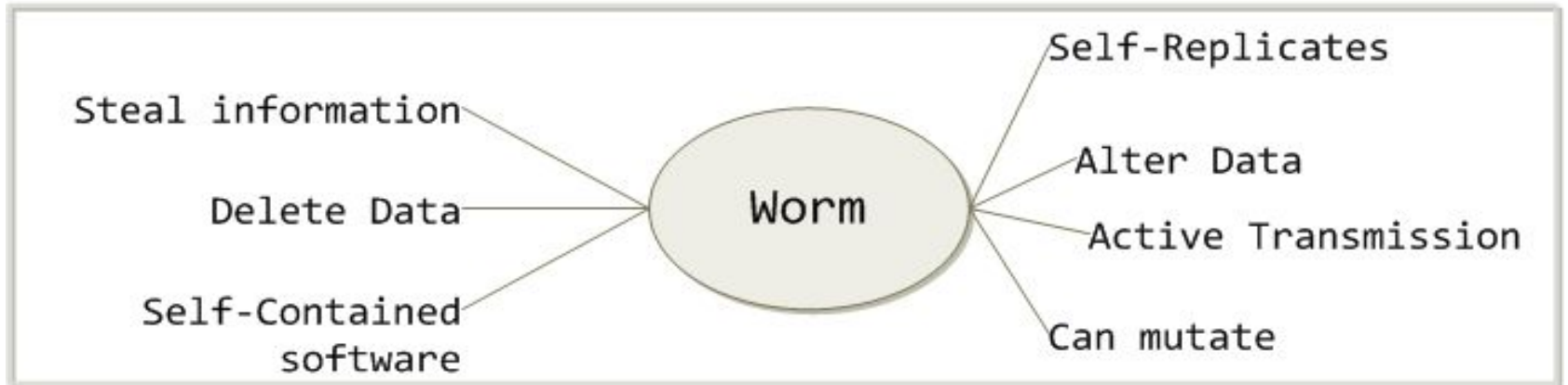
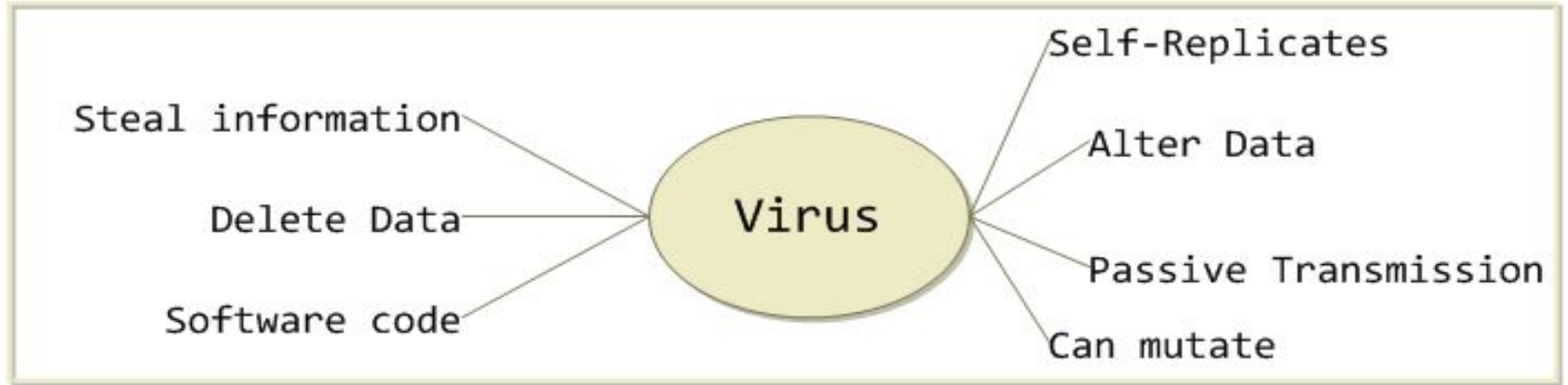
Figure 3-6. Virus Integrated into a Program.



Worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers
- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time
- Many worms are designed only to spread, and do not attempt to change the systems they pass through. However, side effects of worm infestation can be damaging by themselves
- Eg: Morris Worm spread using a buffer overflow vulnerability in the UNIX fingerd utility. Morris' coding mistake, in instructing the worm to replicate itself regardless of a computer's reported infection status, transformed the worm from a potentially harmless intellectual and computing exercise into a viral denial of service attack

Virus vs Worm



Trojan Horse

- A Trojan horse is any malware that misleads users of its true intent
- Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves
- Once installed, trojans may perform a range of malicious actions
 - Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.
 - Can be used to launch attacks discreetly
 - Since individual trojans typically use a specific set of ports for this communication, it can be relatively simple to detect them.
- Eg: Storm Worm was a trojan horse worm that spread through emails with catchy titles. The infected systems were turned into a botnet

Introduction to Cyber Security

Module 6

Incident Response

Topics

- Incident Prioritization,
- Incident Handling,
- Disaster Recovery,
- Incident Response and Handling Process,
- Incident Management

Event vs Incident ???



Event vs Incident

- An **event** is any **observable occurrence** in a system or network.
- Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- **Adverse events** are events with a **negative consequence**, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- A **computer security incident** is a violation or imminent threat of violation of computer security policies. For example:
 - ✓ *An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.*

Cyber Security Incident

There are many types of information (or IT) security incident that could be classified as a cyber security incident, ranging from serious cyber security attacks on critical national infrastructure and major organized cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction.

Topic	Basic cyber security incident	Sophisticated cyber security attack
Type of attacker	<ul style="list-style-type: none"> • Small-time criminals • Individuals or groups just 'having fun' or 'responding to a challenge' • Localised, community or individual Hacktivists • Insiders 	<ul style="list-style-type: none"> • Serious organised crime • State-sponsored attack • Extremist groups
Target of attack	<ul style="list-style-type: none"> • General public • Private sector • Non-strategic government departments 	<ul style="list-style-type: none"> • Major corporate organisations • International organisations • Governments • Critical national infrastructure • National security / defence
Purpose of attack	<ul style="list-style-type: none"> • Financial gain • Limited disruption • Publicity • Vendettas or revenge 	<ul style="list-style-type: none"> • Major financial reward • Widespread disruption • Discover national secrets • Steal intellectual property of national importance • Terrorism • Warfare
Capability of attacker	<ul style="list-style-type: none"> • Low skill • Limited resource • Publicly available attack tools • Not well organised • Local reach 	<ul style="list-style-type: none"> • Highly skilled professionals • Extremely well resourced • Bespoke tools • Highly organised • International presence
Response requirements	<ul style="list-style-type: none"> • Restore services • Special monitoring and organisation • Some industry information sharing 	<ul style="list-style-type: none"> • Tailored guidance for specialist industry and specific capabilities • Implications for government security services • CNI sector-specific industry response

Need for Incident Response

- Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur.
- One of the benefits of having an incident response capability is that it **supports responding to incidents systematically.**
- Incident response helps personnel to **minimize loss or theft of information and disruption of services** caused by incidents.
- Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data.
- An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

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”).
- Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as **collateral damage such as brand reputation, are kept at a minimum.**
- As the cyberattacks increase in scale and frequency, incident response plans become more vital to a company’s cyber defenses.

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.”

Incident Response Policy, Plan, and Procedure Creation

Policy Elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Plan Elements

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Procedure Elements

- Procedures should be based on the incident response policy and plan.
- Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team.
- SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.
- SOPs should be tested to validate their accuracy and usefulness.

SIX STEPS FOR EFFECTIVE INCIDENT RESPONSE

The **SANS** Institute provides six steps for effective incident response:

- 1. Preparation:** Developing policies and procedures to follow in the event of a cyber breach. Key to this process is effective training to respond to a breach and documentation to record actions taken for later review.
- 2. Identification:** This is the process of detecting a breach and enabling a quick, focused response.
- 3. Containment:** One of the first steps after identification is to contain the damage and prevent further penetration.

Contd...

4. **Eradication:** This stage involves neutralizing the threat and restoring internal systems to as close to their previous state as possible. This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

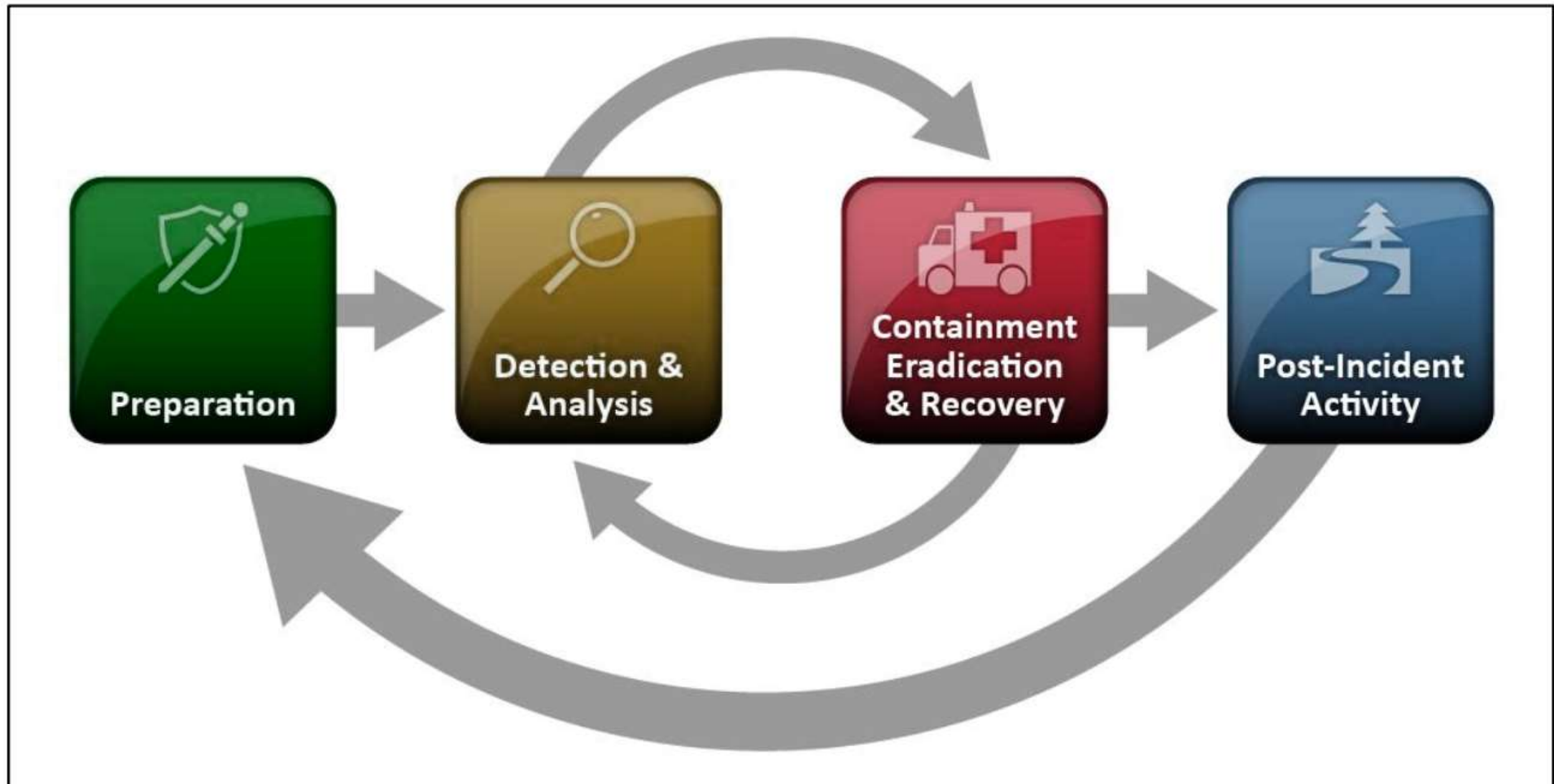
5. **Recovery:** Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition.

6. **Lessons Learned:** 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 made during the incident. Final analysis should be condensed into a report and used for future training.

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**

Incident Response Life Cycle



Preparation

1. Preparing to Handle Incidents

➤ Incident Handler Communications and Facilities:

- ✓ Contact information
- ✓ On-call information
- ✓ Incident reporting mechanisms
- ✓ Issue tracking system
- ✓ Smartphones
- ✓ Encryption software
- ✓ War room
- ✓ Secure storage facility

Contd...

➤ Incident Analysis Hardware and Software:

- ✓ Digital forensic workstations and/or backup devices
- ✓ Laptops
- ✓ Spare workstations, servers, and networking equipment, or the virtualized equivalents
- ✓ Blank removable media
- ✓ Portable printer
- ✓ Packet sniffers and protocol analyzers
- ✓ Digital forensic software
- ✓ Evidence gathering accessories

Contd...

➤ Incident Analysis Resources:

- ✓ Port lists
- ✓ Documentation
- ✓ Network diagrams and lists of critical assets
- ✓ Current baselines
- ✓ Cryptographic hashes

➤ Incident Mitigation Software:

Preparation Contd...

2. Preventing Incidents

- Risk Assessments.
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training.

Detection and Analysis

➤ Attack Vectors

- ✓ External/Removable Media
- ✓ Attrition
- ✓ Web
- ✓ Email
- ✓ Impersonation
- ✓ Improper Usage
- ✓ Loss or Theft of Equipment

Contd...

➤ Signs of an Incident

- ✓ Incidents may be detected through many different means, with varying levels of detail and fidelity.
- ✓ Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers.
- ✓ Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- ✓ The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.
- ✓ Signs of an incident fall into one of two categories: **precursors and indicators**. A *precursor* is a sign that an incident may occur in the future. An *indicator* is a sign that an incident may have occurred or may be occurring now.

Contd...

➤ Incident Analysis

- ✓ Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate.
- ✓ Profile Networks and Systems
- ✓ Understand Normal Behaviors
- ✓ Create a Log Retention Policy
- ✓ Perform Event Correlation
- ✓ Maintain and Use a Knowledge Base of Information
- ✓ Run Packet Sniffers to Collect Additional Data
- ✓ Filter the Data

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).

Contd...

➤ Incident Prioritization

Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- ✓ *Functional Impact of the Incident*
- ✓ *Information Impact of the Incident*
- ✓ *Recoverability from the Incident*

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Functional Impact Categories

Contd...

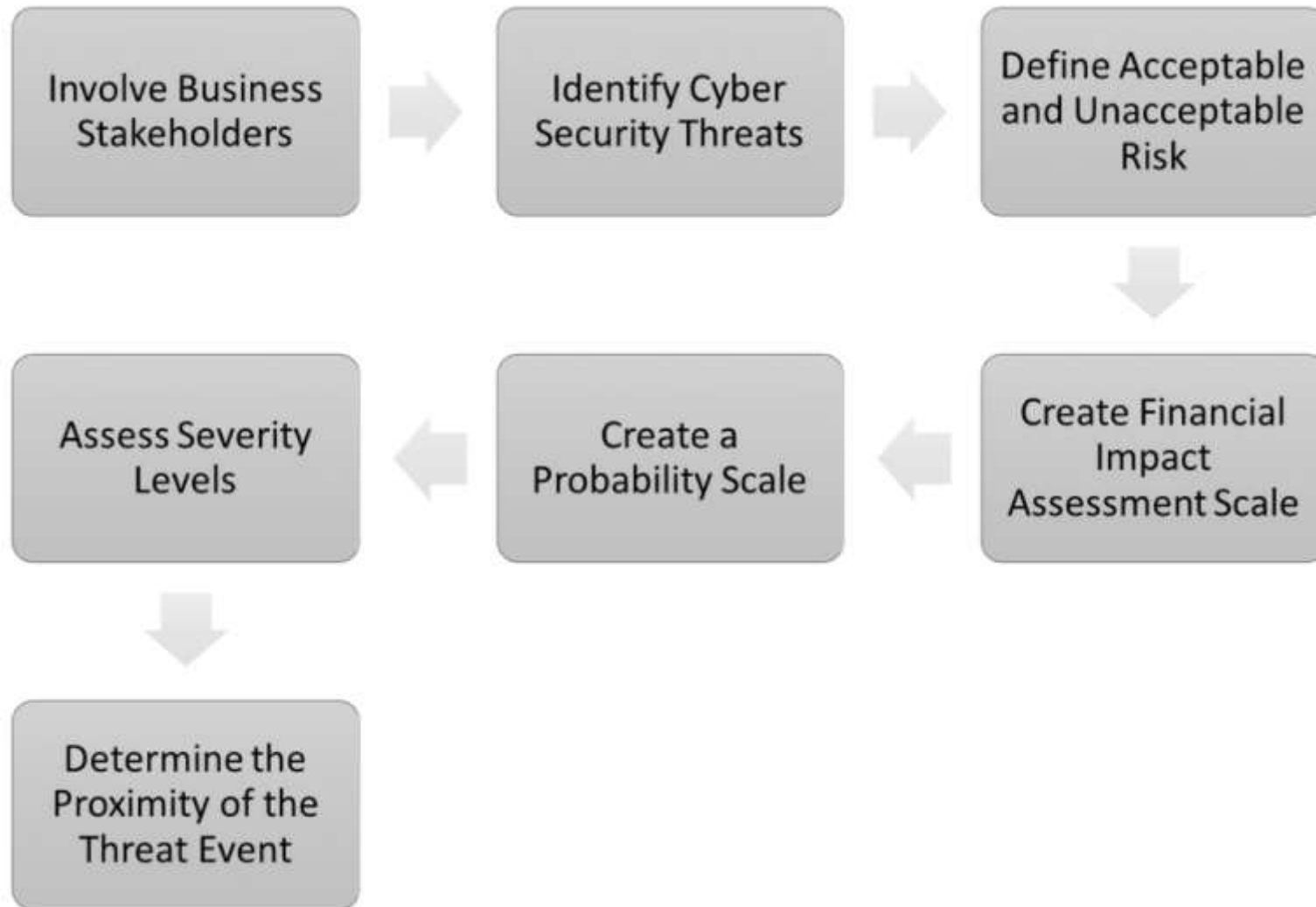
Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Information Impact Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Recoverability Effort Categories

Incident Prioritization



Contd...

➤ Incident Notification

- ✓ CIO
- ✓ Head of information security
- ✓ Local information security officer
- ✓ Other incident response teams within the organization
- ✓ External incident response teams (if appropriate)
- ✓ System owner
- ✓ Human resources (for cases involving employees, such as harassment through email)
- ✓ Public affairs (for incidents that may generate publicity)
- ✓ Legal department (for incidents with potential legal ramifications)
- ✓ US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
- ✓ Law enforcement (if appropriate)

Containment, Eradication, and Recovery

➤ Choosing a Containment Strategy

- ✓ Containment is important before an incident overwhelms resources or increases damage.
- ✓ Most incidents require containment, so that is an important consideration early in the course of handling each incident.
- ✓ Containment provides time for developing a tailored remediation strategy.
- ✓ 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.

Contd...

➤ Evidence Gathering and Handling

- ✓ Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- ✓ Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- ✓ Time and date (including time zone) of each occurrence of evidence handling
- ✓ Locations where the evidence was stored.

Contd...

➤ Identifying the Attacking Hosts

- ✓ Validating the Attacking Host's IP Address
- ✓ Researching the Attacking Host through Search Engines
- ✓ Using Incident Databases
- ✓ Monitoring Possible Attacker Communication Channels

Contd...

➤ Eradication and Recovery

- ✓ After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.
- ✓ During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.
- ✓ In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
- ✓ 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).

Post-Incident Activity

➤ Lessons Learned

- ✓ 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?
- ✓ Were any steps or actions taken that might have inhibited the recovery?
- ✓ 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?

Contd...

➤ Using Collected Incident Data

- ✓ Number of Incidents Handled
- ✓ Time Per Incident
- ✓ Objective Assessment of Each Incident
- ✓ Subjective Assessment of Each Incident

Contd...

➤ Evidence Retention

- Organizations should establish policy for how long evidence from an incident should be retained.
- Most organizations choose to retain all evidence for months or years after the incident ends.
- The following factors should be considered during the policy creation:
 - ✓ Prosecution
 - ✓ Data Retention
 - ✓ Cost

References

- [1] <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>
- [2] <https://www.forcepoint.com/cyber-edu/incident-response>
- [3] <https://digitalguardian.com/blog/what-incident-response>
- [4] https://www.drizgroup.com/driz_group_blog/7-steps-to-prioritize-cyber-security-threats-threat-remediation
- [5] <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

Thank You !!!