LNMIIT
The LNM Institute of Information Technology

Network Attacks and Security

Classroom Code:o7l60yk

LNMIIT
The LNM Institute of Information Technology

Outline

- Network Transmission/ Communication Media (Weakness)
- Threats to Network Communications
- Interception: Eavesdropping and Wiretapping
- Modification, Fabrication: Data Corruption
- Interruption: Loss of service
- Port Scanning
- Network Attack Defenses

Communication Medium

LNMIIT
The LNM Institute of Information Technology

Medium	Strengths	Weaknesses
Wire	• Widely Used • Lost cost buy, install maintain	• Susceptible to Emanation • Susceptible to physical wiretapping
Optical Fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong Signal not seriously affected by weather	• Exposed to interception along the path of transmission • Requires Line of Sight • Signals must be repeated
Wireless (Radio/ WiFi)	• Widely Available • Built into many computers	• Signal Degrades over distance • Signal interceptable around transmitter
Satellite	• Strong, Fast Signal	• Delay due to distance signal travels up and down • Signal Exposed over wide area at receiving end.

Potential Threats in Networks

- *interception*, or unauthorized viewing
- *modification*, or unauthorized change
- *fabrication*, or unauthorized creation
- *interruption*, or preventing authorized access

CIA Triad

- **Confidentiality, integrity and availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization.
- Confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people get it.

CIA Triad

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle . Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

CIA Triad

- Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts.
- It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important.

Interception

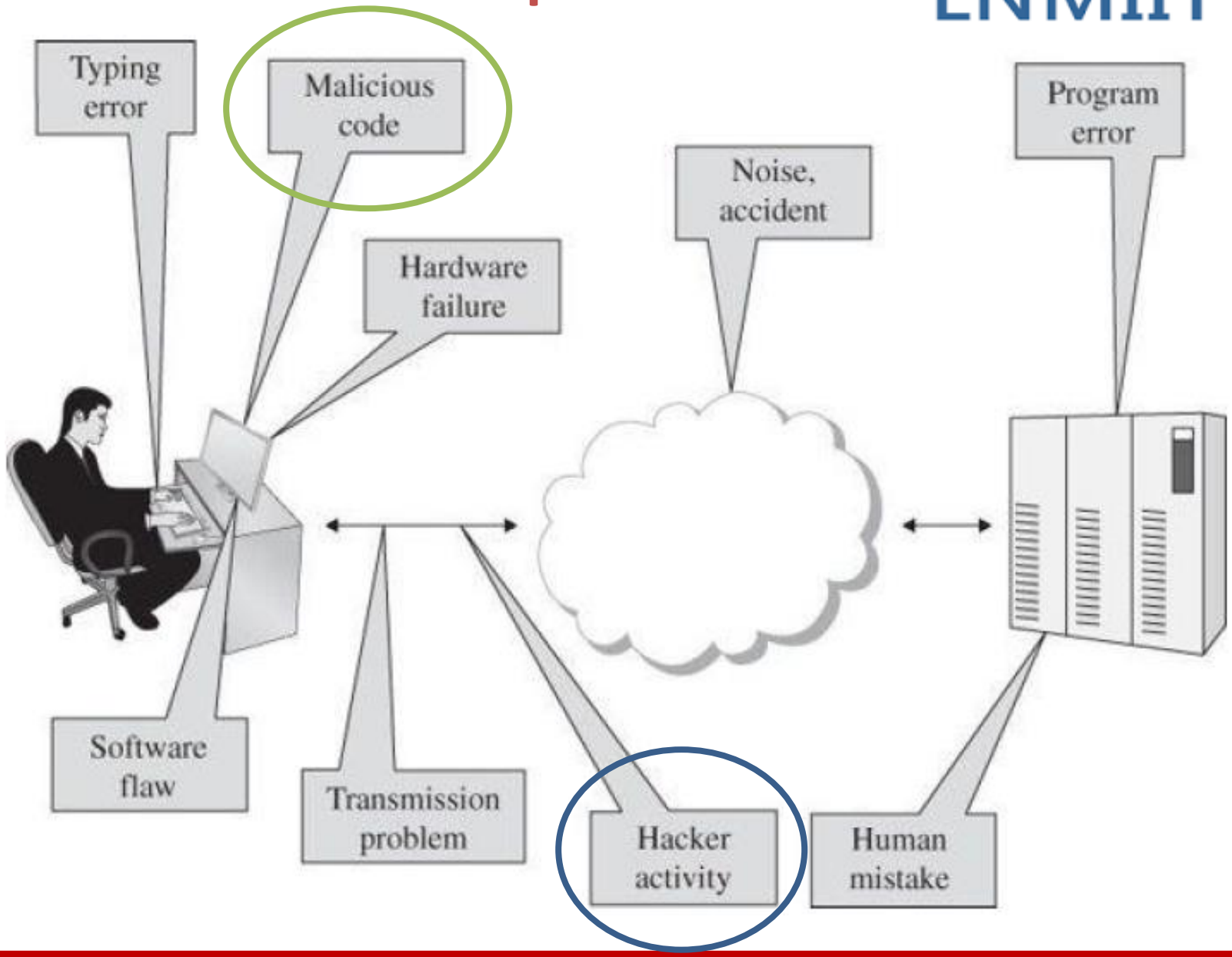
- **Wiretapping**: It is the data interception often covert and unauthorized. This name wiretap refers to the original mechanism, which was a device that was attached to a wire to split off a second pathway that data would follow in addition to the primary path. The way to tap depends on medium of Communication.
- **Eavesdropping**: Network eavesdropping is a network layer attack that focuses on capturing small *packets* from the network transmitted by other computers and reading the data content in search of any type of information.

Data Corruption

- The threat here is that a communication will be changed during transmission. Sometimes the act involves **modifying data en route**, other times it may be **crafting new content** or **repeating an existing communication**. These three attacks are called **modification**, **insertion**, and **replay**, respectively.
- Such attacks can be malicious or not, induced or from natural causes.

Data Corruption Sources

LNMIIT



LNMIIT
The LNM Institute of Information Technology

Modification Failure/ Attacks

- **Sequencing**
- **Substitution**
- **Insertion**
- **Replay**

LNMIIT
The LNM Institute of Information Technology

Interruption: Loss of service

- **Routing**
- **Excessive Demand**
- **Component Failure**

LNMIIT
The LNM Institute of Information Technology

Port Scanning

- Scanning is an inspection activity, and as such it causes no harm itself. However, scanning is often used as a first step in an attack, a probe, to determine what further attacks might succeed.
- An easy way to gather network information is to use a **port scanner**, a program that, for a particular Internet (IP) address, reports which ports respond to queries and which of several known vulnerabilities seem to be present.

LNMIIT
The LNM Institute of Information Technology

Port Scanner

- Port scanning tells an attacker three things: which standard ports or services are running and responding on the target system, what operating system is installed on the target system, and what applications and versions of applications are present. This information is readily available for the asking from a networked system.
- It can be obtained quietly, anonymously, without identification or authentication, drawing little or no attention to the scan.

Port Scanner: Single Host

LNMIIT

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port       State     Service Reason      Product  Version  Extra info
21   tcp   open      ftp     syn-ack     ProFTPD  1.3.1
22   tcp   filtered  ssh     no-response
25   tcp   filtered  smtp    no-response
80   tcp   open      http    syn-ack     Apache   2.2.3    (CentOS)
106  tcp   open      pop3pw  syn-ack     poppassd
110  tcp   open      pop3    syn-ack     Courier pop3d
111  tcp   filtered  rpcbind no-response
113  tcp   filtered  auth    no-response
143  tcp   open      imap    syn-ack     Courier Imapd      rel'd 2004
443  tcp   open      http    syn-ack     Apache  2.2.3      (CentOS)
465  tcp   open      unknown syn-ack
646  tcp   filtered  ldp     no-response
993  tcp   open      imap    syn-ack     Courier Imapd      rel'd 2004
995  tcp   open              syn-ack
2049 tcp   filtered  nfs     no-response
3306 tcp   open      mysql   syn-ack     MySQL   5.0.45
8443 tcp   open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

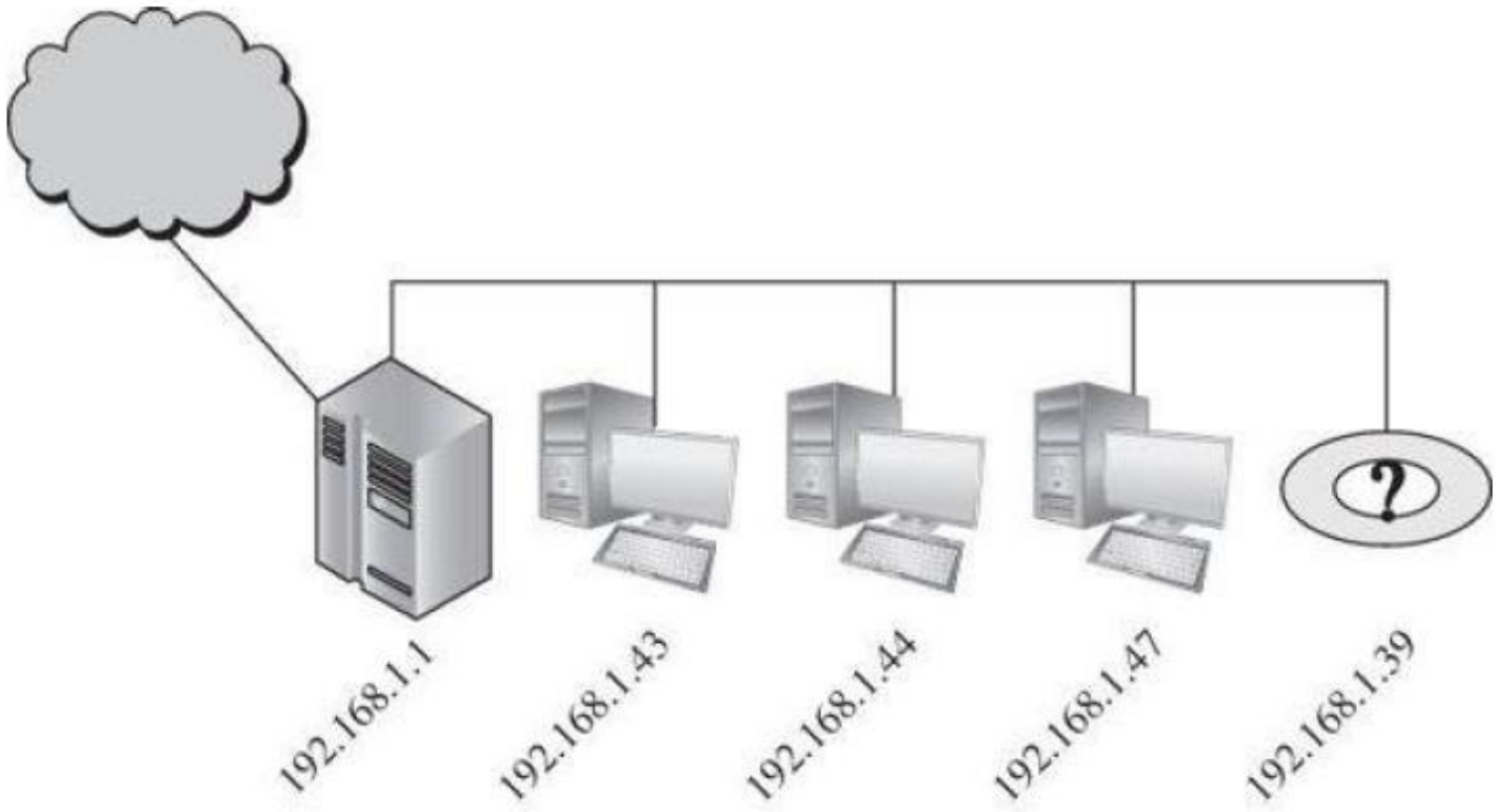
Port Scanner: Small Network

LNMIIT

```
Starting Nmap 5.21 (http://nmap.org) at 2015-00-00 12:32
Eastern Daylight Time


Nmap scan report for router (192.168.1.1)
Host is up (0.00s latency).
MAC Address: 00:11:22:33:44:55 (Brand 1}


Nmap scan report for computer (192.168.1.39)
Host is up (0.78s latency).
MAC Address: 00:22:33:44:55:66 (Brand 2)


Nmap scan report computer (192.168.1.43)
Host is up (0.010s latency).
MAC Address: 00:11:33:55:77:99 (Brand 3)


Nmap scan report for unknown device 192.168.1.44
Host is up (0.010s latency).
MAC Address: 00:12:34:56:78:9A (Brand 4)


Nmap scan report for computer (192.168.1.47)
Host is up.
```

Port Scanner: Small Network

LNMIIT
The LNM Institute of Information Technology



The Latency time for all devices is almost similar they may be in same network segment. So one can draw the connectivity diagram.

LNMIIT
The LNM Institute of Information Technology

Dangerous Port Scanning

The two examples shown exposes the following:

- how many hosts there are
- what their IP addresses are
- what their physical (MAC) addresses are
- what brand each is
- what operating system each runs, and what version
- what ports respond to service requests
- what service applications respond, and what program and version they are running
- how long responses took (which reveals speed of various network connections and thus may indicate the design of the network)

LNMIIT
The LNM Institute of Information Technology

Port Scanning

- Nmap even has an option by which it automatically generates a specified number of random IP addresses and then scans those addresses. This point is especially significant for computer security. For example: 100.200.*.*

LNMIIT
The LNM Institute of Information Technology

Network Attack Defences

- **Encryption**
- **Firewall**
- **Intrusion Detection/ Protection System**
- **Security Information and Event Management**

Encryption/ Cryptography

Symmetric Encryption (secret key): use the same key for both encryption and decryption.

- so $P = D(K,E(K,P))$ meaning that the same key, K, is used both to encrypt a message and later to decrypt it.

Asymmetric Encryption(public key): use different keys for encryption and decryption. Here encryption and decryption keys come in pairs.

- A decryption key, K_D, inverts the encryption of key K_E, so that $P = D(K_D, E(K_E,P))$.

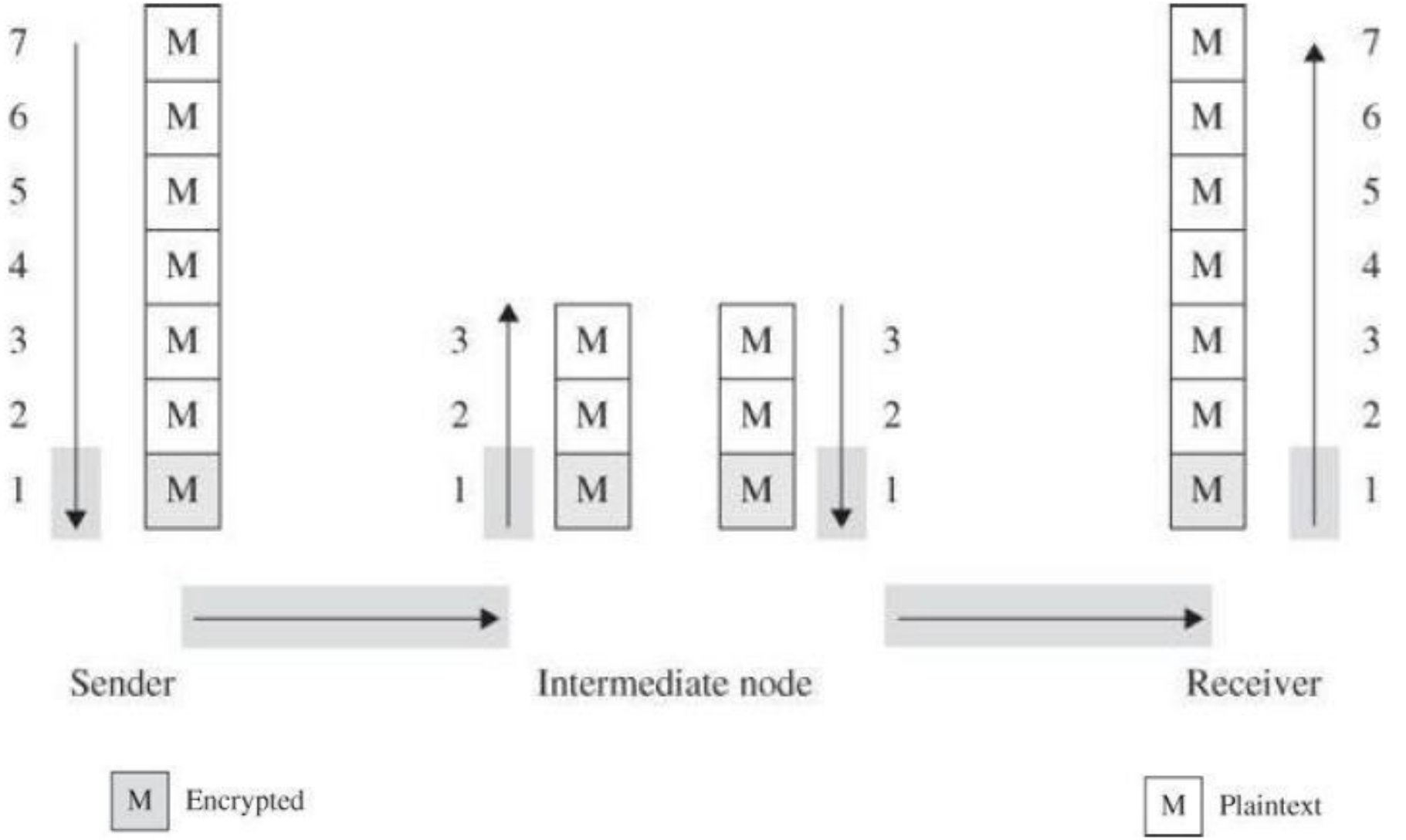
Network Encryption

Encryption can be applied either between two hosts (called link encryption) or between two applications (called end-to-end encryption).

Link Encryption

- The data are encrypted just before the system places them on the physical communications link. In this case, encryption occurs at layer 1 or 2 in the OSI model.
- Similarly, decryption occurs just as the communication arrives at and enters the receiving computer.
- **Link encryption covers a communication from one node to the next on the path to the destination.**

Link Encryption



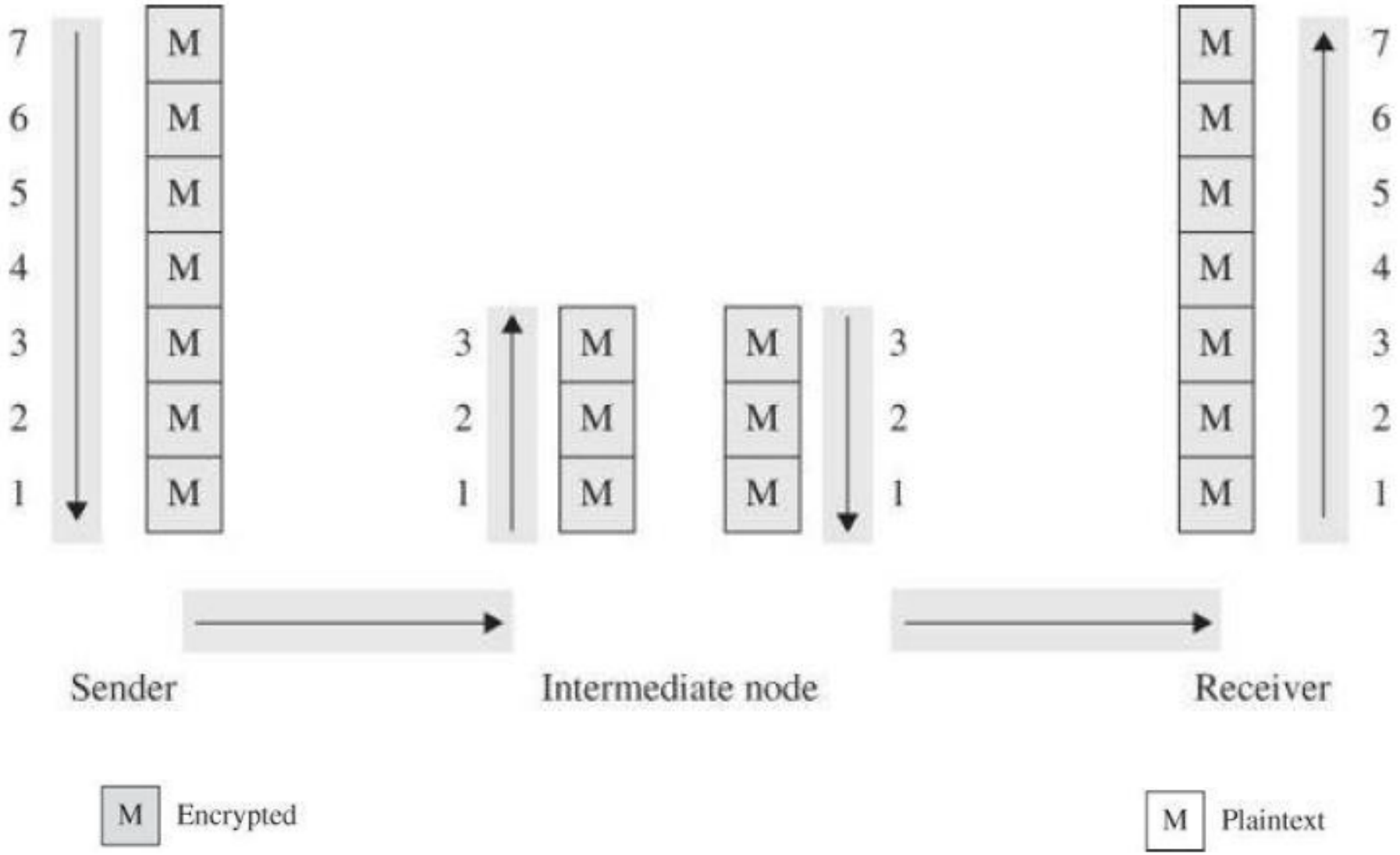
LNMIIT
The LNM Institute of Information Technology

End-to-End Encryption

- **End-to-end encryption** provides security from one end of a transmission to the other. The encryption can be applied between the user and the host by a hardware device. Alternatively, the encryption can be done by software running on the host computer.
- In either case, the encryption/decryption is performed at the highest levels, usually by an **application** at OSI level 7.
- **End-to-end encryption covers a communication from origin to destination.**

End-to End Encryption

LNMIIT



Link vs. End-to-End Encryption

LNMIIT

Link Encryption	End-to-End Encryption
Security within Hosts	
Data Partially exposed in sending host	Data protected in sending host
Data Partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of User	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrator selects encryption	User select algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation
All or no data encrypted	User can selectively encrypt data items
Implementation Consideration	
Requires one key per pair of hosts	Requires one key per pair of users
Provide node authentication	Provide user authentication

Encryption

- **Browser Encryption**
  - **SSH Encryption**
  - **SSL and TLS Encryption**
  - **Cipher Suites**
  - **HTTP with SSL → HTTPS**
    - **SSL Session**
- **Onion Routing**
- **VPN**

SSL Session

- To use SSL, the client requests an SSL session.
- The server responds with its public key certificate so that the client can determine the authenticity of the server.
- The client returns a symmetric session key encrypted under the server's public key.
- Both the server and client compute the session key, and then they switch to encrypted communication, using the shared session key.

Onion Routing

- **If someone monitoring traffic between points A and B would know the volume of traffic communicated.**
- To overcome it, a model is developed that uses a collection of forwarding hosts, each of whom knows only from where a communication was received and to where to send it next.
- Thus, to send untraceable data from A to B, A picks some number of forwarding hosts, call them X, Y, and Z.
- A begins by encrypting the communication under B's public key. A then appends a header from Z to B, and encrypts the result under Z's public key.
- A then puts a header on that from Y to Z and encrypts that under Y's public key. A then puts a header on that communication from X to Y and encrypts that under X's public key.
- Finally, A puts on a header to send the package to X.

Onion Routing

- Upon receiving the package, X decrypts it and finds instructions to forward the inner package to Y.
- Y then decrypts it and finds instructions to forward the inner package to Z.
- Z then decrypts it and finds instructions to forward the inner package to B.
- The package is deconstructed like peeling the layers from an onion, which is why this technique is called onion routing.

Firewall

- A **firewall** is a device that filters all traffic between a protected or “inside” network and a less trustworthy or “outside” network.
- Usually a firewall runs on a dedicated device; because it is a single point through which traffic is channeled, performance is important, which means that only firewall functions should run on the firewall machine.

Firewall

- Generally, a firewall is a computer with memory, storage devices, interface cards for network access, and other devices.
- It runs an operating system and executes application programs.
- Often the hardware, operating system, and applications are sold as a package, so **the firewall application (a program) is sometimes also called a firewall.**

Purpose of Firewalls

Firewalls enforce predetermined rules governing what traffic can flow.

- The purpose of a firewall is to keep attackers outside a protected environment.
- To accomplish it, firewalls implement a security policy that is specifically designed to address what bad things might happen.
- For example, the policy might be to prevent any access from outside (while still allowing traffic to pass from the inside to the outside).
- The policy might permit accesses only from certain places, from certain users, or for certain activities.

LNMIIT
The LNM Institute of Information Technology

Firewall Design

- Firewalls are simple devices that rigorously and effectively control the flow of data to and from a network.
- Two qualities lead to that effectiveness: a well-understood traffic flow **policy** and a **trust**worthy design and implementation.

Firewall Policy

LNMIIT
The LNM Institute of Information Technology

- A firewall implements a **security policy**, that is, a set of rules that determine what traffic can or cannot pass through the firewall.

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Trustworthy Design

- A firewall is positioned as the single physical connection between a protected (internal) network and an uncontrolled (external) one. This will ensures the firewall will be always invoked.
- A firewall is typically well isolated, making it highly immune to modification. Usually a firewall is implemented on a separate computer, with direct connections only to the outside and inside networks.

LNMIIT
The LNM Institute of Information Technology

Type of Firewall

- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways (or proxies)
- Circuit-level gateways
- Guards
- Personal firewalls

LNMIIT
The LNM Institute of Information Technology

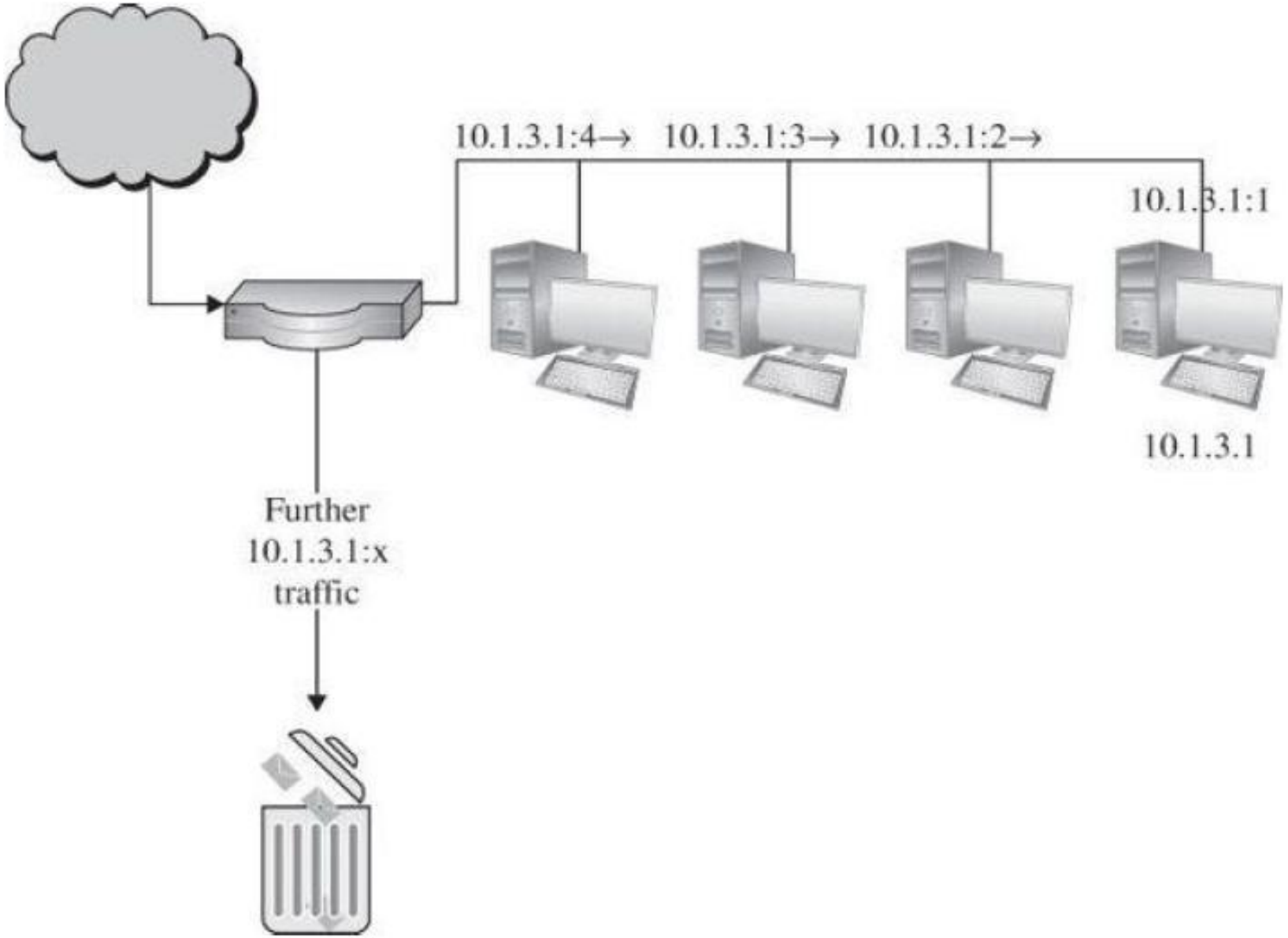
Packet Filtering Gateway

- A **packet filtering gateway** or **screening router** is the simplest type of firewall.
- It controls access on the basis of packet address (source or destination) or specific transport protocol type (such as HTTP web traffic) by examining the control information of each single packet.
- A firewall can screen traffic before it gets to the protected network.
- So, if the port scan originated from address 100.200.3.4, you might configure the packet filtering gateway firewall to discard all packets from that address.
- Packet filters do not “see inside” a packet.

Stateful Inspection Firewall

- Filtering firewalls work on packets one at a time, accepting or rejecting each packet and moving on to the next.
- They have no concept of “state” or “context” from one packet to the next.
- A **stateful inspection firewall** maintains state information from one packet to another in the input stream.

Stateful Inspection Firewall



Application-level Gateways (Proxy)

- Packet filters look only at the headers of packets, not at the data inside the packets.
- Therefore, a packet filter would pass anything to port 25, assuming its screening rules allow inbound connections to that port.
- Applications (such as the email delivery agent) often act on behalf of all users, so they require privileges of all users (for example, to store incoming mail messages so that inside users can read them). A flawed application, running with all-users privileges, can cause much damage.

LNMIIT
The LNM Institute of Information Technology

Application Proxy Gateway

- An **application proxy gateway** is a firewall that simulates the (proper) effects of an application at level 7 so that the application receives only requests to act properly.
- A proxy gateway is a two-headed device: From inside, the gateway appears to be the outside (destination) connection, while to outsiders the proxy host responds just as the insider would.
- In fact, it behaves like a man in the middle (**Safe**).

LNMIIT
The LNM Institute of Information Technology

Application Proxy Gateway

- Capabilities
  - Permit only read access to outsiders
  - Permit filtered read access to outsiders
  - Creates access log of insiders
  - Perform replacement in the output to outsides like returning count instead of names or identification
  - Encrypt the emails/ data going outside for companies with multiple location
  - .. .. … etc.

LNMIIT
The LNM Institute of Information Technology

Circuit-level Gateway

- A **circuit-level gateway** is a firewall that essentially allows one network to be an extension of another. It operates at OSI level 5, the session level, and it functions as a virtual gateway between two/ more networks. It supports encrypted communication among them.
- Circuit-level gateway enables to implement a virtual private network where Users are unaware of the cryptography and management is assured of the confidentiality protection.

Guard

- A **guard** is a sophisticated firewall.
- **A guard can implement any programmable set of conditions, even if the program conditions become highly sophisticated.**
- The degree of control a guard can provide is limited only by what is computable.

Personal Firewall

- A personal firewall is a program that runs on a single host to monitor and control traffic to that host. It can only work in conjunction with support from the operating system.

- Windows Firewall

LNMIIT
The LNM Institute of Information Technology

Can and Can't of Firewalls

- Firewalls can protect an environment only if the firewalls control the entire perimeter. That is, firewalls are effective only if no unmediated connections breach the perimeter.
- If even one inside host connects to an outside address, by a wireless connection for example, the entire inside net is vulnerable through the unprotected host.

LNMIIT
The LNM Institute of Information Technology

Can and Can't of Firewalls

- Firewalls can protect an environment only if the firewalls control the entire perimeter. That is, firewalls are effective only if no unmediated connections breach the perimeter.
- If even one inside host connects to an outside address, by a wireless connection for example, the entire inside net is vulnerable through the unprotected host.

Can and Can't of Firewalls

- Firewalls do not protect data outside the perimeter; data that have properly passed (outbound) through the firewall are just as exposed as if there were no firewall.

Can and Can't of Firewalls

- Firewalls are the most visible part of an installation to the outside, so they are the most attractive target for attack. For this reason, several different layers of protection, called defense in depth, are better than relying on the strength of just a single firewall.

LNMIIT
The LNM Institute of Information Technology

Can and Can't of Firewalls

- Firewalls must be correctly configured, that configuration must be updated as the internal and external environment changes, and firewall activity reports must be reviewed periodically for evidence of attempted or successful intrusion.

Can and Can't of Firewalls

- Firewalls exercise only minor control over the content admitted to the inside, meaning that inaccurate data or malicious code must be controlled by other means inside the perimeter.

Intrusion Detection and Prevention Systems

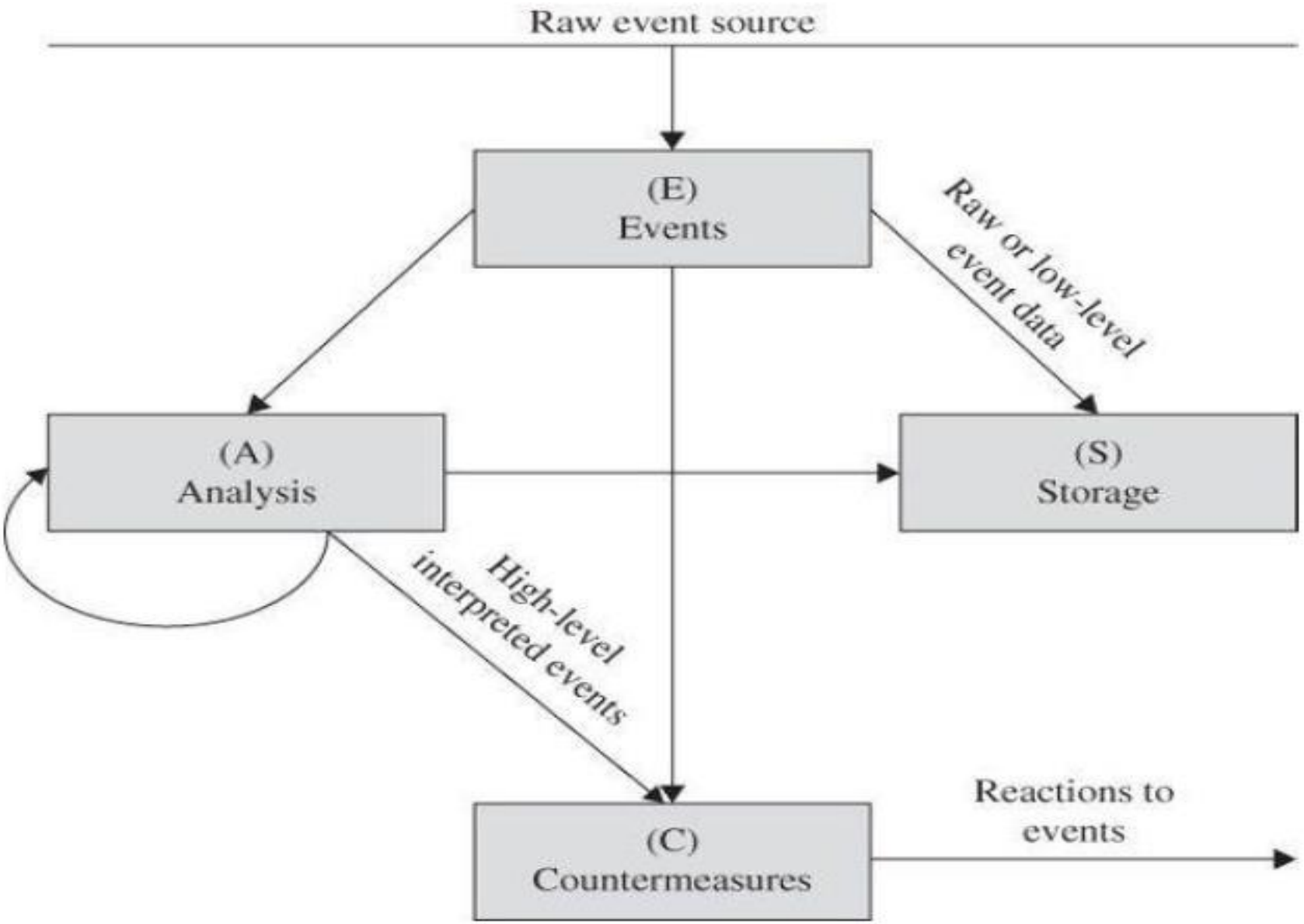
- It is possible that sometime the preventive technologies including Access Control, Encryption and Firewall may be failed to stop a malicious activity.
- Intrusion detection systems complement these preventive controls as the next line of defense.

Intrusion Detection Systems

- An intrusion detection system (IDS) is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events.
- The components in the figure are the four basic elements of an intrusion detection system, based on the Common Intrusion Detection Framework.
- An IDS receives raw inputs from sensors. It saves those inputs, analyzes them, and takes some controlling action.

Intrusion Detection Systems

LNMIIT



LNMIIT
The LNM Institute of Information Technology

Functions of IDS

Ideally, IDSs should perform a variety of functions:

- monitoring users and system activity
- auditing system configuration for vulnerabilities and misconfigurations
- assessing the integrity of critical system and data files
- recognizing known attack patterns in system activity
- identifying abnormal activity through statistical analysis
- managing audit trails and highlighting user violation of policy or normal activity
- correcting system configuration errors
- installing and operating traps to record information about intruders

Types of IDSs

- **Signature-based** intrusion detection systems perform simple pattern-matching and report situations that match a pattern (signature) corresponding to a known attack type.
- **Heuristic** intrusion detection systems, also known as **anomaly based**, build a model of acceptable behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable so that the heuristic IDS will now treat that previously unclassified behavior as acceptable.

Types of IDSs

- Heuristic intrusion detection systems are said to learn what constitute anomalies or improper behavior.
- This learning occurs as an **artificial intelligence** component of the tool, the **inference engine**, identifies pieces of attacks and rates the degree to which these pieces are associated with malicious behavior.

LNMIIT
The LNM Institute of Information Technology

Types of IDSs

- Intrusion detection devices can be network based or host based.
- A **network-based** IDS is a stand-alone device attached to the network to monitor traffic throughout that network.
- A **host-based** IDS runs on a single workstation or client or host, to protect that one host.

LNMIIT
The LNM Institute of Information Technology

Types of IDSs

- **Front End Versus Internal IDSs**
- **Code Modification Checkers**
- **Vulnerability Scanners**

LNMIIT
The LNM Institute of Information Technology

Intrusion Prevention System

- **Intrusion prevention systems extend IDS technology with built-in protective response.**

Stealth Mode in IDSs

- An IDS is a network device (or, in the case of a host-based IDS, a program running on a network device).
- Any network device is potentially vulnerable to network attacks (like denial of service attack).

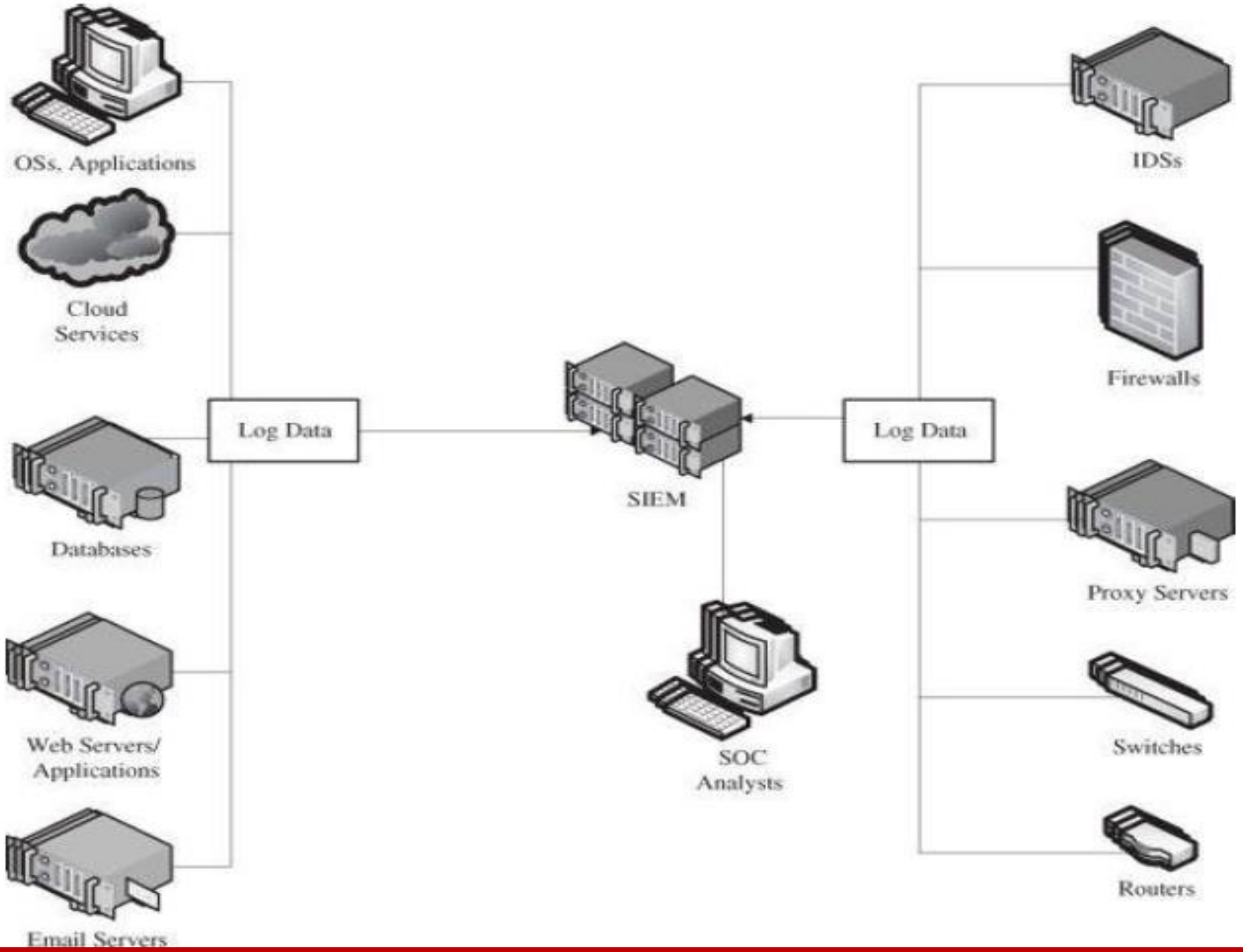
LNMIIT
The LNM Institute of Information Technology

How?? Stealth Mode

- IDSs run in **stealth mode** by using two network interfaces: one for the network (or network segment) it is monitoring and the other to generate alerts and perhaps perform other administrative needs.
- The IDS uses the monitored interface as input only; it never sends packets out through that interface.
- Often, the interface is configured so that the device has no published address through the monitored interface; that is, no router can route anything directly to that address because the router does not know such a device exists.
- **It is the perfect passive wiretap.**
- If the IDS needs to generate an alert, it uses only the alarm interface on a completely separate control network.

Security Information and Event Management (SIEM)

- Very Large organizations with multiple locations (100s or 1000s) creates a **Security Operations Center** (**SOC**).
- SOC is a team of security personnel dedicated to monitoring a network for security incidents and investigating and remediating those incidents.
- SIEMs are software systems that collect security-relevant data from a variety of hardware and software products in order to create a unified security dashboard


OSs, Applications
Cloud Services
Databases
Web Servers/ Applications
Email Servers
Log Data
SIEM
SOC Analysts
Log Data
IDSs
Firewalls
Proxy Servers
Switches
Routers

SIEM Challenges

- Cost
- Data Portability (when one need to change SIEM product)
- Log Source Compatibility
- Deployment Complexity
- Customization
- Full Time Maintenance Activity
- User Training

LNMIIT
The LNM Institute of Information Technology

Thank you, for your time and attention!




The LNMIIT: Where young dreams take shape .....