

Chapter Three

Infrastructure security (IS)

Introduction to Infrastructure security

- Infrastructure security is a critical aspect of **safeguarding** the underlying foundation that supports an organization's IT operations.
- It encompasses the **protection** of **hardware, software, networks, data centers**, and other essential components that constitute an **organization's information technology** infrastructure.
- The primary goal of infrastructure security is **to ensure** the **confidentiality, integrity, and availability** of information and resources.

Introduction to Infrastructure security

- Infrastructure security is the practice of protecting critical systems and assets against physical and cyber threats.
- most commonly used to refer to technology assets, including:
 - Computers and endpoints/devices
 - Networking systems
 - Cloud resources — both hardware and software
- IS system is the process of protecting the data from unauthorized access disclosure, destruction or disruption.

Key components of infrastructure security include:

- 1. Physical Security:** Securing **physical access** to data centers, server rooms, and network closets to prevent unauthorized personnel from tampering with hardware.
 - **Implementing measures** such as **biometric** access controls, **surveillance** systems, and **security** personnel to monitor and control physical access.

Cont..

2. Network Security:

- Protecting the organization's network infrastructure against unauthorized access, data interception, and other malicious activities.
- Measures - Employing firewalls, intrusion detection/prevention systems, and virtual private networks (VPNs) to secure network communication.

Cont..

3. Server Security:

- Ensuring the **security of servers** by implementing access controls, regular security updates, and configuration management practices.
- Employing server hardening techniques to **eliminate unnecessary services and reduce the attack** surface.

4. Data Security:

- Implementing **encryption** mechanisms to **protect sensitive data** both in **transit** and at **rest**.
- Enforcing **data access controls** and **data loss prevention** (DLP) measures to **prevent unauthorized access** and data **leaks**.
- promote a **security-conscious culture** within the organization.

Cont..

5. Endpoint Security:

- Securing **end-user devices** such as laptops, desktops, and mobile devices to prevent malware infections and unauthorized access.
- Implementing **antivirus software**, **endpoint detection** and **response (EDR)** solutions, and mobile device management (**MDM**) tools.

6. Cloud Security:

- Ensuring the security of **cloud-based infrastructure and services** by implementing **access controls**, **encryption**, and **monitoring**.
- Following **best practices** for secure configuration and **regularly auditing** and **assessing** the security posture of cloud environments.

Cont..

7. Incident Response and Disaster Recovery:

- Developing and implementing incident response plans to effectively respond to security incidents.
- Establishing robust disaster recovery mechanisms to minimize downtime and data loss in the event of a catastrophic failure or cyberattack.

8. Security Policies and Training:

- Developing and enforcing security policies that define acceptable use, access controls, and other security guidelines.
- Providing ongoing security awareness training to employees to promote a security-conscious culture within the organization.

Cont..

- Infrastructure security is a **dynamic** field that requires **continuous monitoring**, **adaptation**, and **improvement** to address evolving **threats** and **vulnerabilities**.
- Organizations should **adopt** a holistic approach, combining technical controls, **policies**, and **user education** to create a resilient and secure infrastructure.
- **Regular** security **assessments**, **audits**, and **updates** are essential to **maintaining** the effectiveness of infrastructure security measures.

Goal of Infrastructure Security

- The **primary** goal of infrastructure security is to **protect** an organization's information technology (IT) infrastructure from a variety of **threats** and **risks**. This includes safeguarding the hardware, software, networks, data, and other critical components that make up the infrastructure.

Goal of Infrastructure Security

- Boost security measures and your overall posture.
- Protect data from being stolen or otherwise compromised, minimizing financial risk incurred with steep fines.
- Ensure compliance with evolving data privacy rules that mandate consumer information be kept safe from attack.
- Minimize the risk of damage due to user carelessness.

Cont..

- The **overarching objectives** of infrastructure security are **to ensure** the:
 - **Confidentiality of Information**
 - **Integrity of Systems and Data**
 - **Availability of Resources**
 - **Resilience Against Cyber Threats** - Establish a resilient infrastructure that can **withstand and recover** from various **cyber threats**, including malware, ransomware, DDoS attacks, and other malicious activities.
 - **Compliance with Regulations and Standards**
 - **Mitigation of Risks**
 - **Efficient Incident Response**
 - **Protection Against Unauthorized Access**
 - **Continuous Monitoring and Improvement**
 - **User Awareness and Training**

Cont...

- By achieving the above goals, organizations can create a secure and resilient IT infrastructure that not only protects sensitive information but also supports the overall business objectives without compromising the integrity, availability, and confidentiality of critical assets.
- Infrastructure security is an ongoing process that requires a proactive and adaptive approach to address emerging threats and vulnerabilities in the ever-changing landscape of cybersecurity.

Level of IS

- **Physical level:** protection in the form of locked doors, fences, backup generators, security cameras and the like.
- **Network level:** traffic encryption, whether it is on-premises or in the cloud, proper firewall management and the use of authentication and authorization systems.
- **Application level:** protection of databases against attacks such as SQL injections as well as the hardening of other applications against unauthorized use or malicious exploits.
- **Data level:** is a lowest level of IS. data encryption, backups and anonymization tactics where they are appropriate.

Host security

- A host is **any computer** including work stations, network servers, laptops, wirelessly networked devices.
- Securing host involves :-
 - ▢ Protecting the **physical** devices
 - ▢ Securing an **operating system software**
 - ▢ Using software based software application
 - ▢ Monitoring logs
- Three important elements to secure Host (network server or client)
Applications Data

Securing Devices

- Prevent unauthorized users from gaining physical access to equipment
- Aspects of securing devices
 - ▢ Physical access security
 - ▢ Host hardware security
 - ▢ Mobile device security
- Physical access security
 - ▢ Restricting access to equipment areas
 - ▢ Hardware locks
 - ▢ Standard keyed entry lock provides minimal security
 - ▢ Deadbolt locks provide additional security

Securing devices

❖ Hardware security

- Physical security protecting host system hardware
- Portable devices have steel bracket security slot
 - ▢ Cable lock inserted into slot and secured to device
 - ▢ Cable connected to lock secured to desk or immobile object
- Laptops may be placed in a safe locking cabinets
 - Can be prewired for power and network connections
 - Allow devices to charge while stored

Continue...

□ **Mobile device security**

- Many security provisions that apply to laptops apply to mobile devices
- Mobile devices' unique security features
 - **Remote wipe / sanitation**
 - Data can be remotely erased if device is stolen
 - **GPS tracking**
 - Can pinpoint location to within 100 meters
 - **Voice encryption**
 - Used to mask content of voice communication over a smartphone

Network monitoring and diagnosis tools

- Network monitoring and diagnosis tools play a crucial role in maintaining the **health, performance, and security of computer networks**.
- These tools help IT professionals **identify issues, troubleshoot problems, and optimize network performance**.
- Network monitoring - a process in which all network components

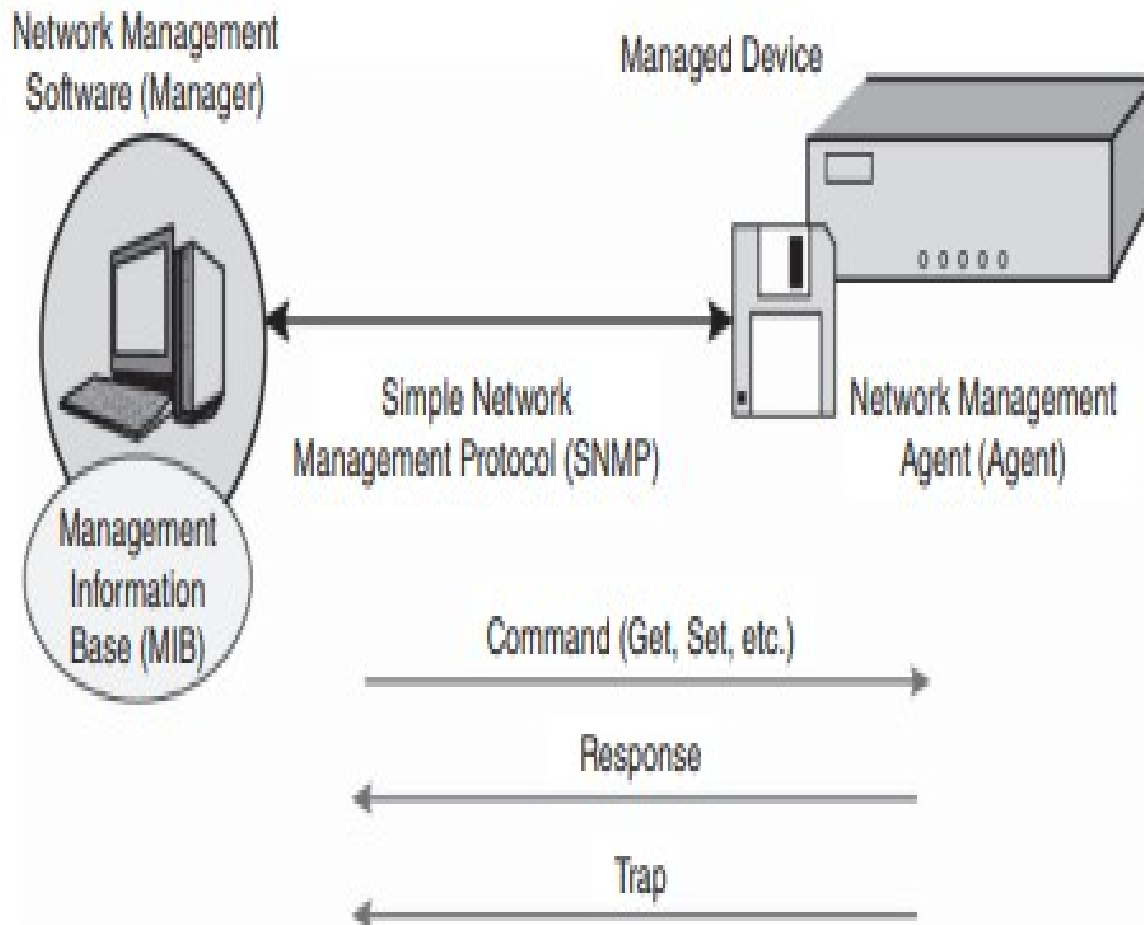
Cont...

- Fault and performance are evaluated continuously to maintain and optimize their availability.
- One important aspect of network monitoring is that find performance issues and bottlenecks proactively helps in identifying issues at the initial stage.
- Efficient proactive monitoring can prevent network downtime or failures.
- Some commonly used network monitoring and diagnosis tools

SNMP(simple network management protocol)

- It is a widely used protocol for **managing and monitoring network devices** and their functions.
- SNMP is used to monitor the **network**, **detect network faults**, and sometimes even used to configure **remote devices**.
- It is implemented on the **application layer** of the networking stack
- Component of SNMP
 - ▢ **SNMP Manager** :It is a centralized system or software used to monitor network. It is also known as Network Management Station (NMS)
 - ▢ **SNMP agent**: specialized software run by Managed devices(network device) which collect and store information about the device's status and configuration
 - ▢ **Management information bases** : consists of information on resources that are to be managed

Simple Network Management Protocol (SNMP)



Nagios core

- It is an open-source monitoring system that enables organizations to monitor the availability and performance of their entire IT infrastructure. It can monitor hosts, services, and network devices, providing alerts and reports on any issues that may arise.
- Through the user network interface, can be monitored current network status with host status totals and network service status totals broken down at the top of the page
- Track performance events through the alerts system, which send out notifications by email and SMS.

Key features

- Performance dashboard
- Alert system
- Availability reports
- Capacity planning
- Community-created plugins
- APIs

Zabbix

- Zabbix is an open-source network monitoring that combines network, server, cloud, application, service monitoring into one unified solution.
- It uses SNMP and IPMP to monitor your network.
- The Autodiscover feature automatically locates network devices and add them to be monitored
- Zabbix has a notification system
- Alerts are sent by email, SMS, messenger, jabber, or custom scripts to update you on evolving network security events.

Key features

- Auto-discovery feature
- SNMP and IPMP monitoring
- Application monitoring
- Network monitoring templates
- Automatic detection of configuration changes
- Alerts system

Icinga

- Icinga is an open-source network monitoring tool that monitors the performance of your network, cloud-service, and data center.
- The software is web-based and can be configured through the GUI or with the Domain specific language(DSL)
- Can be logged in to the GUI and use the dashboard to view an overview of performance management
- The dashboard displays whether there are any problems with the performance or availability.

Key features

- Web-based GUI
- DSL configuration available
- Dashboard
- Icinga modules/ extensions

Others

- Datadog network performance monitoring
- Paessler PRTG network monitoring
- Atera
- ManageEngine opManager and so on.

Security of different media

- Media divided into four categories
 - I. Print media: *printed materials, such as books, newspaper and magazines, that contain words and images.*
 - II. Broadcast media: *mass communication channels, such as television and radio.*
 - III. Internet media: *distributed online and can include emails and online publications*
 - IV. Out-of-home (outdoor)media: *media that reaches people when they are outside of their homes, like billboards.*

Storage media

1. Why do we store our important documents?

Ans. We store our important document to have access to these documents in future.

2. What are two types of store?

Ans. Two types of store are main store and backing store

3. Which types is used to store current data temporarily?

Ans. Main store is used to store data temporarily eg RAM

Backing storage vs main memory

- Main memory(sometimes known as internal memory or primary storage) is another name for RAM.
- Main memory is usually used to store data temporarily. In the case of RAM, it is volatile(this means that when power is swithed off all of the data in the memory disappears).
- Main memory is used to store data whiles it is being processed by the CPU. Data can be put into memory, and read back from it, very quickly.

- 
- Backing storage /secondary storage is the name for all other data storage devices in a computer: hard-drives, etc
 - Backing storage is usually non-volatile, so it is generally used to store data for a long time.

Storage media and devices

- The device that actually holds the data is known as the storage medium(media is the plural)
- The device that save data onto the storage medium, or read data from it, is knowns as the storage devices.
- Sometimes the storage medium is a fixed (permanent) part of storage device eg. The magnetic coated discs built into hard drive

Magnetic Tape



- Stores data magnetically like audio cassette
- Possesses large capacity
- Cheap storage device
- It uses serial access method to store data
- Runs at slow speed
- Used as a backup device

Magnetic disk



- The disk inside is round in shape
- It uses random access method to read or write data.
- Faster than magnetic tape
- Types
 - Floppy disk
 - Hard disk

Floppy disk

- It is small flexible disk kept in plastic cover.
- It has a low capacity
- It is faster speed than tapes
- It is portable
- It is cheap
- Used to transfer a small files from one computer to another



Hard disk

- Made up of metal disk inside sealed container
- Large capacity
- Fastest speed
- Fixed inside computer
- Used to store large amount of data and software
- Also called Winchester disk



Compact disk



- Thin metal disk in hard plastic coating
- Larger capacity than floppy disk
- Faster speed than floppy disk
- Used for software distribution
- Is called compact disk because it is very thin

Intrusion detection mechanism

- What is intrusion?
- Any set of action that attempt to compromise the confidentiality, integrity, or availability of a computer resource.
- Intrusion detection: detection of break-ins and break-in attempts via automated software systems

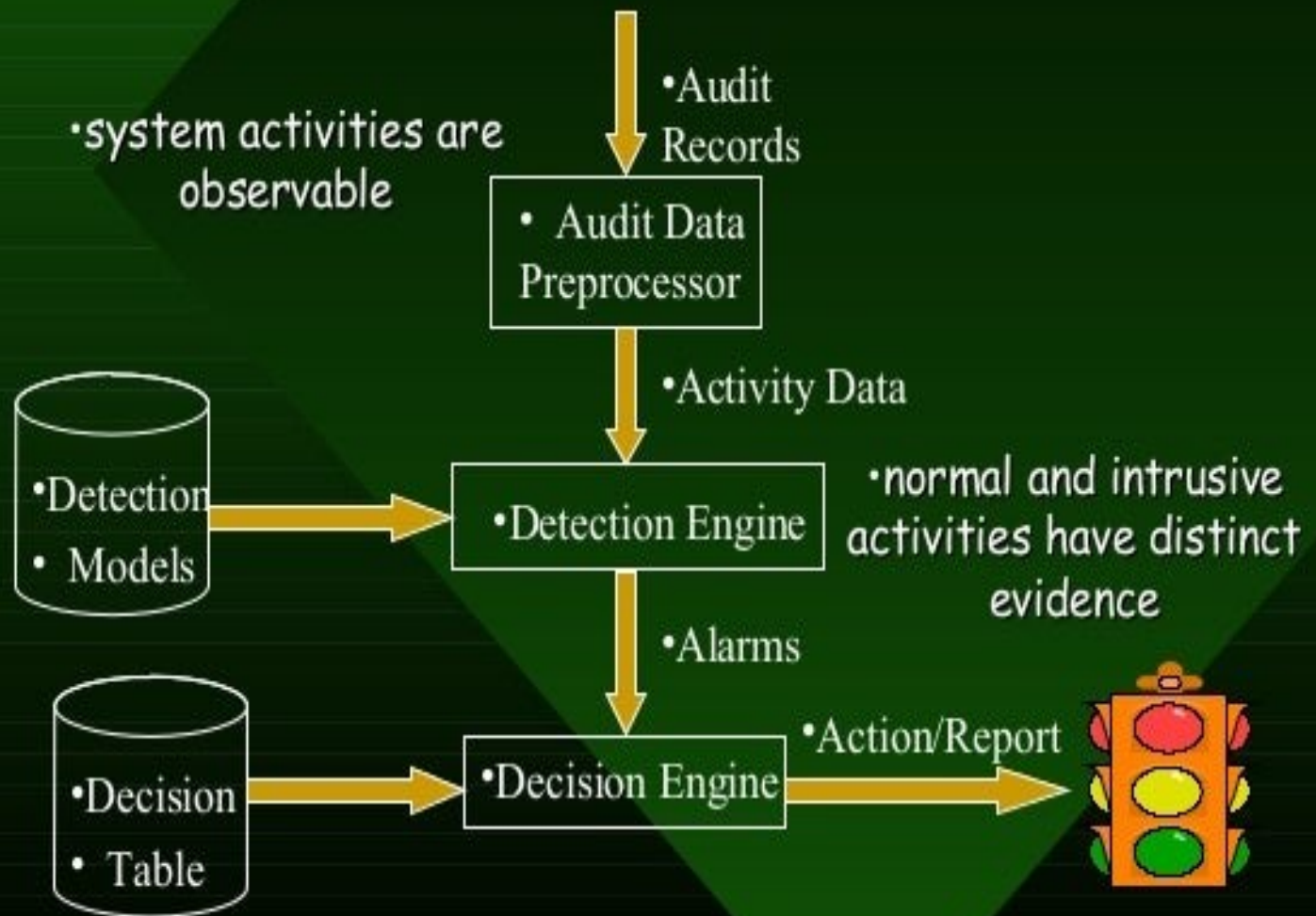
Intrusion detection system (IDS)

- Is the process of identifying and responding to malicious activities targeted at resources
- IDS is a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these thresholds are met.
- It uses a collected information and predefined knowledge-based system to reason about the possibility of an intrusion.
- It also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion etc

Function of IDS

- An IDS detect attacks as soon as possible and takes appropriate action
- An IDS does not usually take preventive measure when an attack is detected
- It is a reactive rather than a pro-active agent
- It plays a role of information rather than a police officer.
- Major components of are
 - Detection devices
 - ▢ Central processing devices(control panel)
 - ▢ Alarm/ notification devices

Components of Intrusion Detection System



Detection methods in IDS

- Based on detection approaches, it divided in to two
 1. **Signature-based detection**
 - ✓ matching signature of well-known attacks against state change in system or stream of packets through network
 - ✓ effective against known threats, it's ineffective against zero-day vulnerabilities and novel attack techniques.
 - ✓ Examples:
 - a telnet attempts with username "root" which is violation of an organization security policy
 - An email with a subject "free-picture" and an attachment "freepics.exe" characteristics of malware

2. Behavioral (Anomaly) based

- focuses on identifying deviations from established normal systems or network behavior baselines.
- Has profile to represent normal behavior of
 - ▢ Hosts, user, network connection or application
 - ▢ Developed by monitoring the characteristics of typical activities over a period of a time.
- Profiles can be for behavioural attributes like:
 - ▢ Number of email sent by a user, number of failed logins for a host, level of processor usage etc
- Anomaly-based detection methods, supported by ML, can be quite effective against zero-day attacks and emerging and new threats. However, it can throw false positives often.

Signature-based vs behavioral based IDS

Signature based IDS	Anomaly base IDs
Signature: DB of known attack patterns	Profile: model of normal behaviors
IDS reports situation that match signatures	IDS reports situation that deviate from profile
Good"low false alarm rate, instantaneous detection	Good cat detect some new attacks