Unit 6

Logic Based System

Topics

- Malicious logic
- Vulnerability analysis
- Auditing
- Intrusion detection
- Applications: Network security, operating system security, user security, program security
- Special Topics: Data privacy, introduction to digital forensics, enterprise security specification.

Malicious logic

- *Malicious logic* is a set of instructions that cause a site's security policy to be violated.

Forms of Malicious Logic

- Trojan Horses
- Computer Viruses
  - Boot Sector Infectors
  - Executable Infectors
  - Multipartite Viruses
  - TSR Viruses
  - Stealth Viruses
  - Encrypted Viruses
  - Polymorphic Viruses
  - Macro Viruses
- Computer Worms
- Other Forms of Malicious Logic
  - Rabbits and Bacteria
  - Logic Bombs

Trojan Horses

- *Trojan horse* is a program with an overt (documented or known) effect and a *covert* (undocumented or unexpected) effect.

- A *propagating Trojan horse* (also called a *replicating Trojan horse*) is a Trojan horse that creates a copy of itself.

- EXAMPLE: The following UNIX script is named *ls* and is placed in a directory.
  - cp /bin/sh /tmp/.xxsh
  - chmod u+s,o+x /tmp/.xxsh
  - rm ./ls
  - ls $*
- It creates a copy of the UNIX shell that is setuid to the user executing this program This program is deleted, and then the correct *ls* command is executed. On most systems, it is against policy to trick someone into creating a shell that is setuid to themselves. If someone is tricked into executing this script, a violation of the (implicit) security policy occurs. This script is an example of malicious logic.

EXAMPLE

The NetBus program allows an attacker to control a Windows NT workstation remotely. The attacker can intercept keystrokes or mouse motions, upload and download files, and act as a system administrator would act.

In order for this program to work, the victim Windows NT system must have a server with which the NetBus program can communicate. This requires someone on the victim's system to load and execute a small program that runs the server.

This small program was placed in several small game programs as well as in some other "fun" programs, which could be distributed to Web sites where unsuspecting users would be likely to download them.

Computer Viruses

- *computer virus* is a program that inserts itself into one or more files and then performs some (possibly null) action.
- This type of Trojan horse propagates itself only as specific programs When the Trojan horse can propagate freely and insert a copy of itself into another file, it becomes a computer virus.
- The first phase, in which the virus inserts itself into a file, is called the *insertion phase*. The second phase, in which it performs some action, is called the *execution phase*. The NEXT pseudocode fragment shows how a simple computer virus works.

Example :As this code indicates, the insertion phase must be present but need not always be executed. It would check for an uninfected boot file (the *spread-condition* mentioned in the pseudocode) and, if one was found, would infect that file (the *set of target files*). Then it would increment a counter and test to see if the counter was at 4. If so, it would erase the disk. These operations were the *action(s)*.

```
beginvirus:
    if spread-condition then begin
        for some set of target files do begin
            if target is not infected then begin
               determine where to place virus instructions
               copy instructions from beginvirus to endvirus
                  into target
               alter target to execute added instructions
            end;
        end;
    end;
    perform some action(s)
    goto beginning of infected program
endvirus:
```

Boot Sector Infectors

- The *boot sector* is the part of a disk used to bootstrap the system or mount a disk.
- Code in that sector is executed when the system “sees” the disk for the first time. When the system boots, or the disk is mounted, any virus in that sector is executed.
- A *boot sector infector* is a virus that inserts itself into the boot sector of a disk.
- Eg - The Brain virus for the IBM PC is a boot sector infector. When the system boots from an infected disk, the virus is in the boot sector and is loaded. It moves the disk interrupt vector (location 13H or 19) to an alternative interrupt vector (location 6DH or 109) and sets the disk interrupt vector location to invoke the Brain virus now in memory. It then loads the original boot sector and continues the boot.

Example

- The Brain (or Pakistani) virus, written for IBM PCs, is thought to have been created in early 1986 but was first reported in the United States in October 1987. It alters the boot sectors of floppy disks, possibly corrupting files in the process. It also spreads to any uninfected floppy disks inserted into the system. Since then, numerous variations of this virus have been reported.

Executable Infectors

- An *executable infector* is a virus that infects executable programs.
- The PC variety of executable infectors are called COM or EXE viruses because they infect programs with those extensions. Figure 19–1 illustrates how infection can occur. The virus can prepend itself to the executable (as shown in the figure) or append itself.

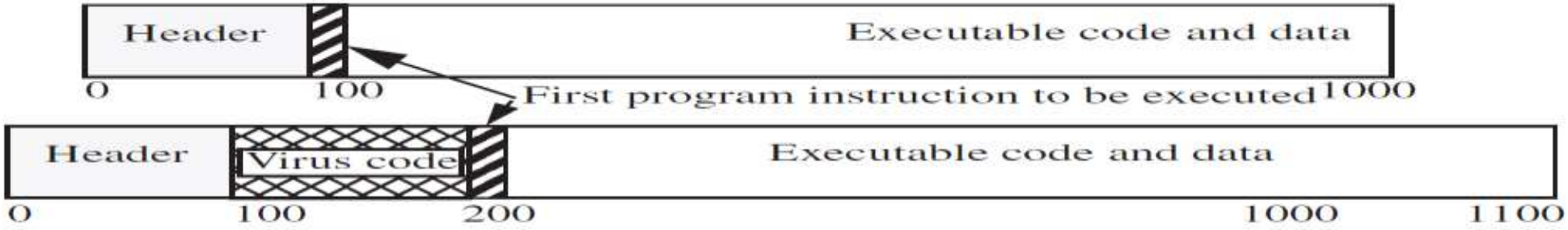


Figure 19–1 How an executable infector works. It inserts itself into the program so that the virus code will be executed before the application code. In this example, the virus is 100 words long and prepends itself to the executable code.

Multipartite Viruses

- *multipartite virus* is one that can infect either boot sectors or applications.
- Such a virus typically has two parts, one for each type. When it infects an executable, it acts as an executable infector; when it infects a boot sector, it works as a boot sector infector.

TSR Viruses

- A *terminate and stay resident* (TSR) virus is one that stays active (resident) in memory after the application (or bootstrapping, or disk mounting) has terminated.
- TSR viruses can be boot sector infectors or executable infectors. Eg – Brain Virus

Stealth Viruses

- *Stealth* viruses are viruses that conceal the infection of files.
- Example - The Stealth virus (also called the IDF virus or the 4096 virus) is an executable infector. It modifies the DOS service interrupt handler (rather than the interrupt vector; this way, checking the values in the interrupt vector will not reveal the presence of the virus).

Polymorphic Viruses

- *A polymorphic* virus is a virus that changes its form each time it inserts itself into another program.

- **Macro Viruses**
- A *macro* virus is a virus composed of a sequence of instructions that is interpreted, rather than executed directly.
- For example, a spreadsheet virus executes when the spreadsheet interprets these instructions. If the macro language allows the macro to access files or other systems, the virus can access them, too.

Computer Worms

- A computer virus infects other programs. A variant of the virus is a program that spreads from computer to computer, spawning copies of itself on each one.
- A *computer worm* is a program that copies itself from one computer to another.

Other forms of malicious Logic

- **Rabbits and Bacteria**
- Some malicious logic multiplies so rapidly that resources become exhausted. This creates a denial of service attack.
- A *bacterium* or a *rabbit* is a program that absorbs all of some class of resource.
- **Logic Bombs**
- A *logic bomb* is a program that performs an action that violates the security policy when some external event occurs

EFFECT OF COMPUTER VIRUS

- It can slow down your computer.
- It might corrupt your system files.
- It might make some programs faulty or corrupt.
- It might damage your boot sector creating problems when you boot into the windows.
- it might steal important information from your computer and send to some other person.
- It might change the power ratings of your computer and could blast the system.

Vulnerability analysis

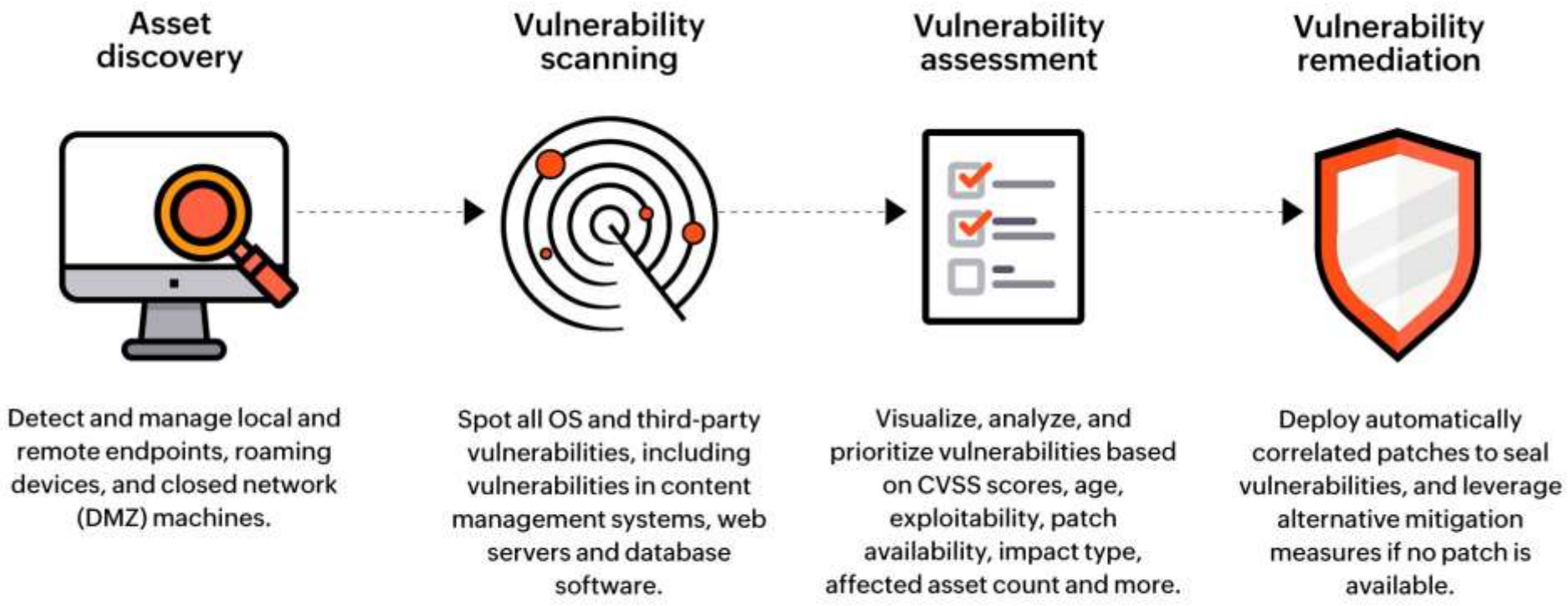
Vulnerability analysis

- A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system.
- A vulnerability analysis is a review that focuses on security-relevant issues that either moderately or severely impact the security of the product or system.

Steps to conducting a proper vulnerability assessment

- Identify where your most sensitive data is stored.
- Uncover hidden sources of data.
- Identify which servers run mission-critical applications.
- Identify which systems and networks to access.
- Review all ports and processes and check for misconfiguration.

Steps to vulnerability analysis



Auditing

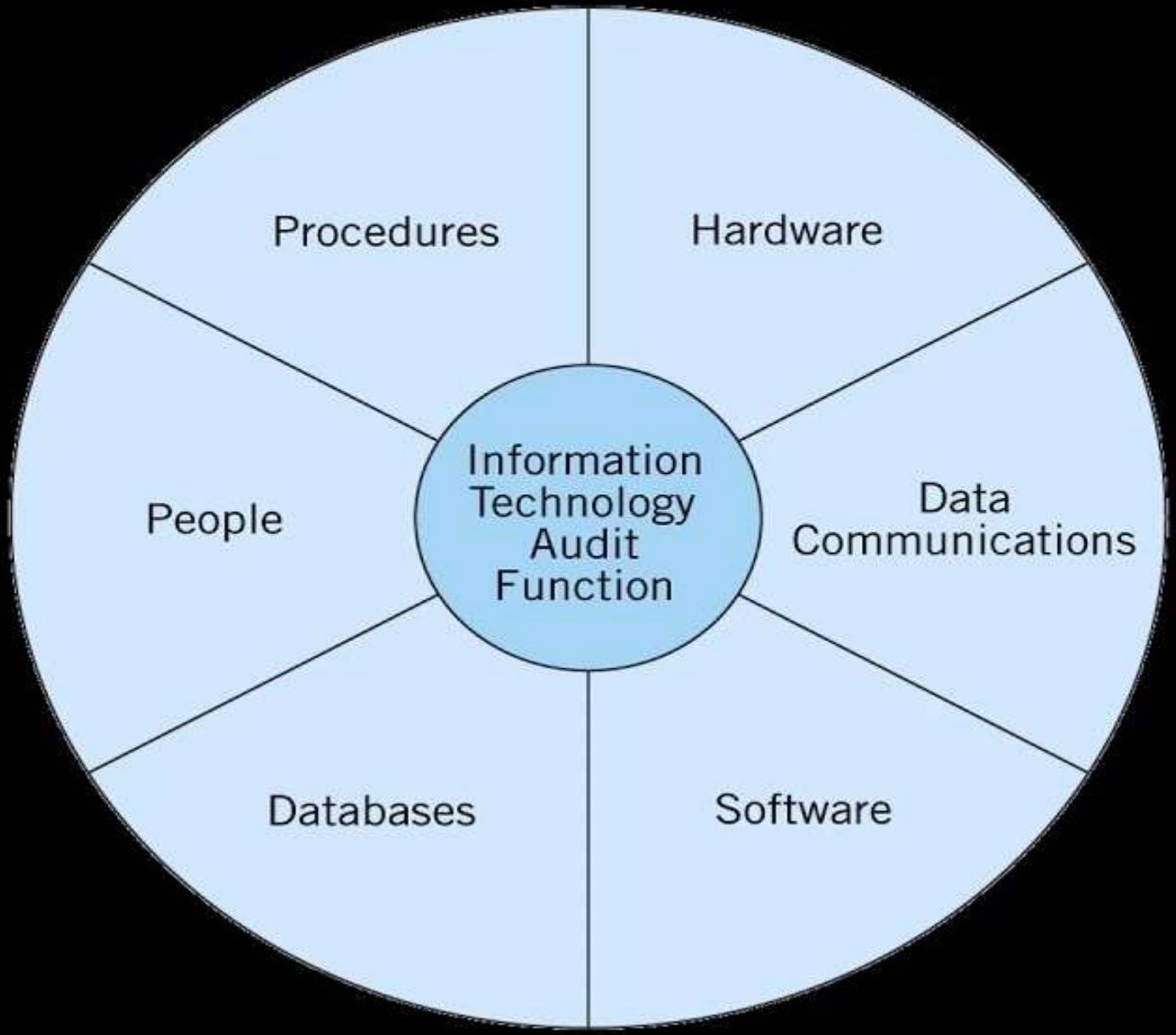
- An information technology audit, or information systems audit, is an examination of the management controls within an Information technology infrastructure and business applications.


First-Party Audits
Internal Audits
AUDIT LEVELS
Third-Party Audits
Independent Examination
Second-Party Audits
Customer Audits

IT Audit strategies

- Review IT organizational structure.
- Review IT policies and procedures.
- Review IT standards.
- Review IT documentation.
- Review the organization's BIA.
- Interview the appropriate personnel.
- Observe the processes and employee performance.

The Components of an IT Audit

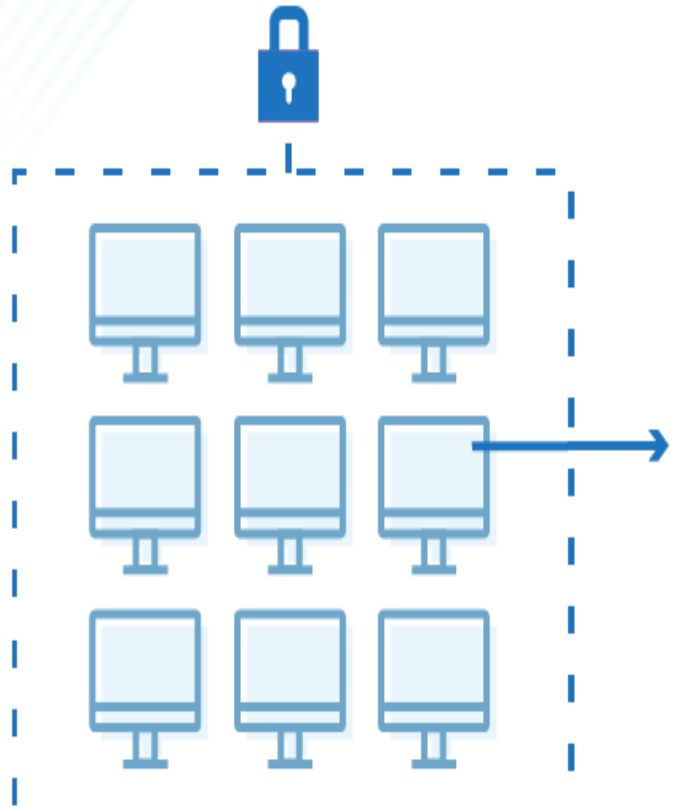


Intrusion Detection System

- An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.
- Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

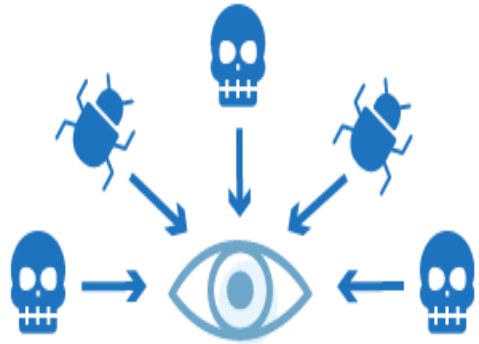
- Intrusion detection systems primarily use two key intrusion detection methods: **signature-based intrusion detection and anomaly-based intrusion detection**
- A NIDS system operates at the network level and monitors traffic from all devices going in and out of the network.
- NIDS performs analysis on the traffic looking for patterns and abnormal behaviours upon which a warning is sent.

What Does an Intrusion Detection System Do?

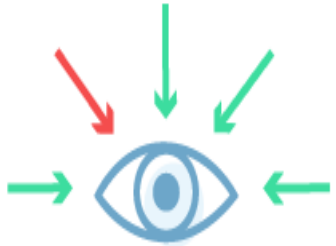


Network Intrusion Detection

Host Intrusion Detection

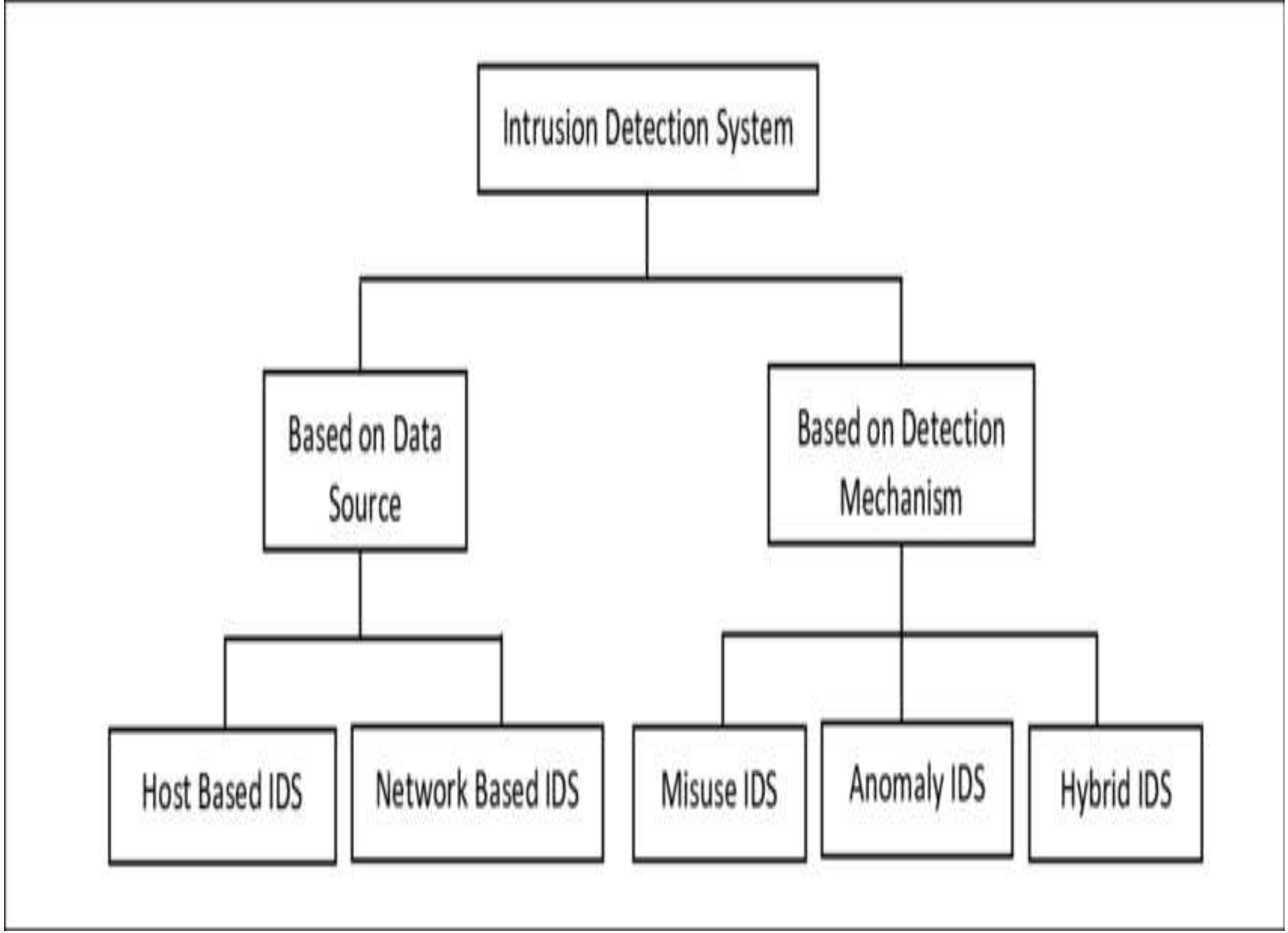


Signature-based Detection



Anomaly-Based Detection

What Does an Intrusion Prevention System Do?


Intrusion Detection System
Based on Data Source
Based on Detection Mechanism
Host Based IDS
Network Based IDS
Misuse IDS
Anomaly IDS
Hybrid IDS

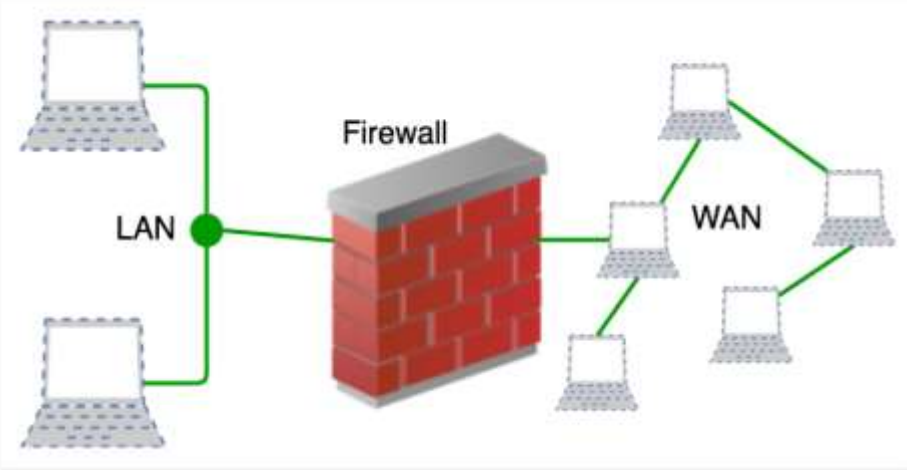
Network security

- 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.

Types of Network Security Protections

- Firewall.
- Network Segmentation.
- Remote Access VPN.
- Email Security.
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems (IPS)
- Sandboxing.

Firewall



- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
- a defined set of security rules it accepts, rejects or drops that specific traffic.
- **Accept :** allow the traffic
  Reject : block the traffic but reply with an “unreachable error”
  Drop : block the traffic with no reply

Network Segmentation

- Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.
- Example : Imagine a large bank with several branch offices. The bank's security policy restricts branch employees from accessing its financial reporting system. Network segmentation can enforce the security policy by preventing all branch traffic from reaching the financial system. And by reducing overall network traffic, the financial system will work better for the financial analysts who use it.

Remote Access VPN

- In a Remote-access VPNs, individual hosts or clients, such as telecommuters, mobile users, and extranet consumers, are able to access a company network securely over the Internet. Each host typically has VPN client software loaded or uses a web-based client.
- VPNs can be characterized as host-to-network

Email Security

- Email security refers to various cybersecurity measures to secure the access and content of an email account or service.
- Email security is important because malicious email is a popular medium for spreading ransomware, spyware, worms, different types of malware, social engineering attacks like phishing or spear phishing emails and other cyber threats.

Data loss prevention

- Data loss prevention (DLP) software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage). The terms "data loss" and "data leak" are related and are often used interchangeably
- Prevention by :
  - Database Hardening. One of the best ways to prevent data loss is to secure a database by hardening it as much as possible.
  - Manage Database Access Tightly. ...
  - Secure Authentication. ...
  - Secure Communication. ...

IPS

- An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats.
- Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.
- The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks.
- IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

Operating system security


1. Minimum Installation
2. Secure Profile for Installation
3. Enable OS Security During Inst.
4. Complete Post Installation Security Checklist
5. Check & Fix Missing Updates
6. Test Security before Next Steps
Secure Installation of Operating System

Operating system security

- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions

Protected Objects

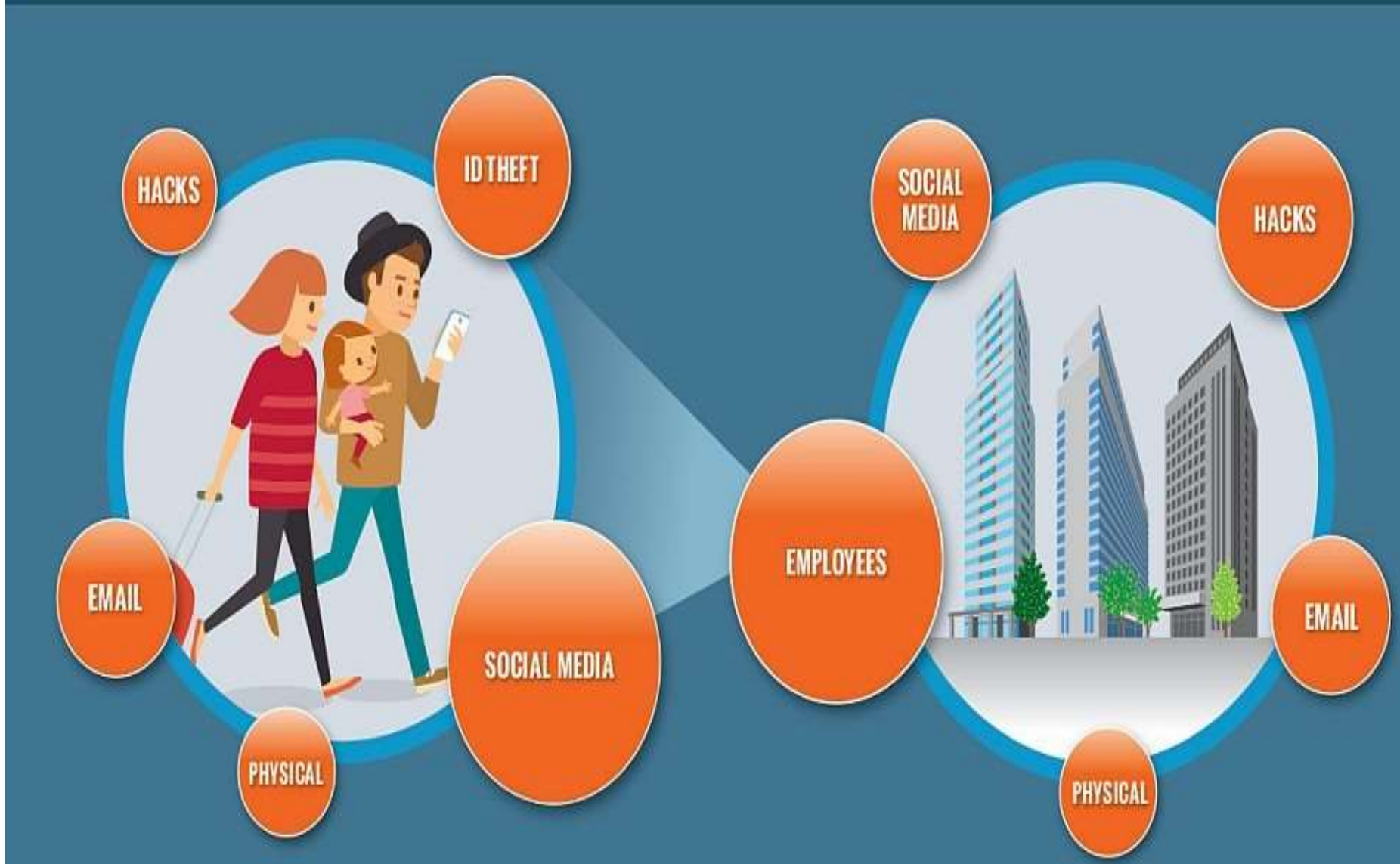
- Hardware, software and data.
- Memory.
- Sharable I/O devices.
- Serially reusable I/O devices.
- Sharable programs and sub-procedures.
- Sharable data.

As it assumed responsibility for controlled sharing, the operating system had to protect these objects.

User Security

- User security awareness training helps every employee in your organization recognize, avoid, and report potential threats that can compromise critical data and systems, including phishing, malware, ransomware, and spyware.

The Human Factor - **Social Engineering Risk Points**



Securing user account

- Use a long/secure password.
- Do not reuse or share passwords.
- Use Two-Factor Authentication (2FA) .
- Use a password management application.
- Check web site security.

Program Security

- A security program is the **entirety of an organization's security policies, procedures, tools and controls.**
- Protection from an unauthorized access to the system.
- Strict allocation of user roles and their access to certain data.
- Protection of the stored and processed data from damage and loss


Awareness & Training
Risk Assessment
Managed Services
Security Program
Policies & Procedures
Design & Implementation
Business Case

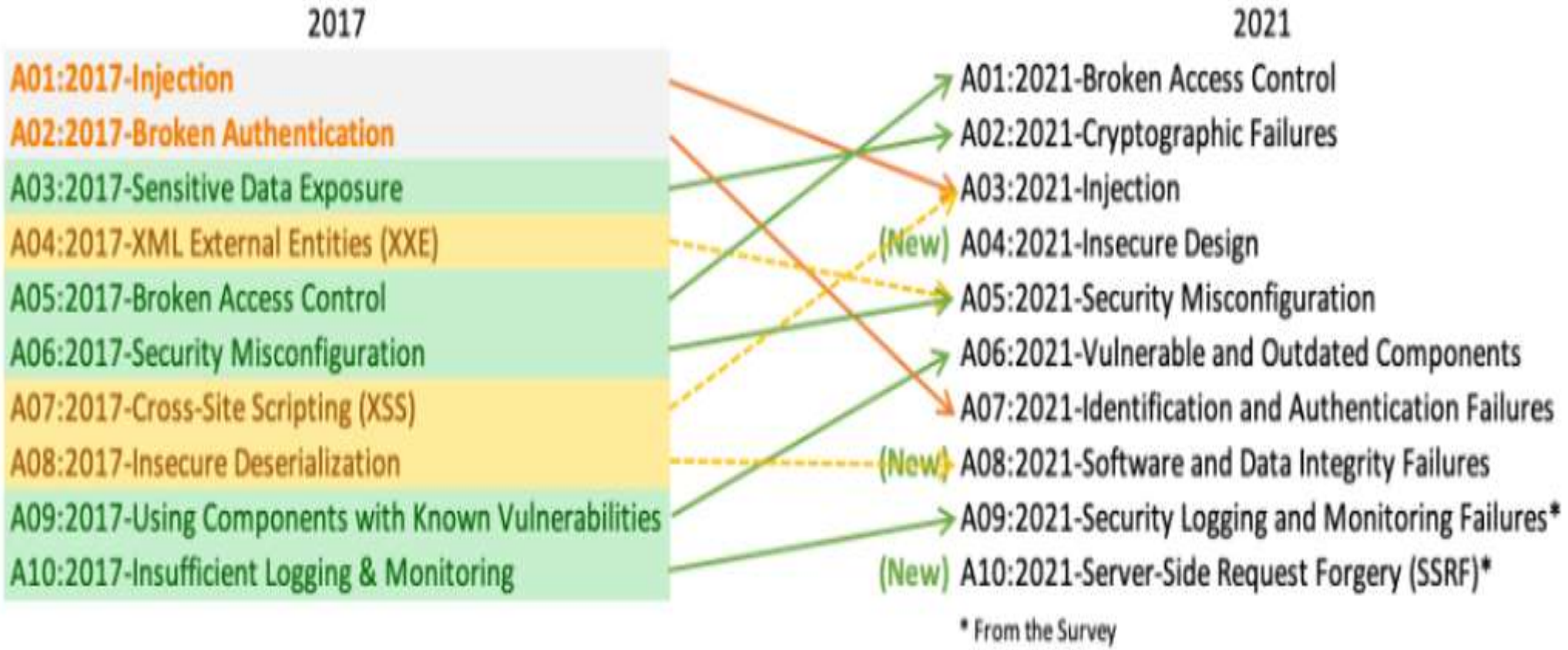
Application Security

- Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
- Examples of application security features.
  - Authentication,
  - authorization,
  - encryption,
  - logging,
  - application security testing

- Application Security Tools are designed to protect software applications from external threats throughout the entire application lifecycle.
- The purpose of this class of tools is to protect the many different kinds of application against data theft or other nefarious intent.

- **Building secure applications: Top 10 application security best...**
- Follow the OWASP top ten.
- Get an application security audit.
- Implement proper logging.
- Use real-time security monitoring and protection.
- Encrypt everything.
- Harden everything. (hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one.)
- Keep your servers up to date.
- Keep your software up to date

OWASP stands for Open Web Application Security Project.




Application Security
Application
Internet
Application Security
Application Server

Digital Privacy

- Digital privacy (also internet or online privacy) means the protection of any data a user creates or transmits while navigating the web via a mobile or desktop.

- The concept of digital privacy can best be described as the protection of the information of private citizens who use digital mediums.
- Information such as the date and time of his searches, what browser he used to access websites and even how long he viewed websites can be retained on a search engine's servers

Digital Forensics

Global Digital Forensics Market Size and Forecast 2015-2024

What is Forensics ?

- **Collection and analysis of evidence.**
- **Using scientific test or techniques.**
- **To establish facts against crime.**
- **For presenting in a legal proceeding.**
- **Therefore Forensic science is a scientific method of gathering and examining information about the past which is then used in court of law.**

Digital Forensics

- Digital Forensics deals with the **process of finding evidence related to a digital crime.**
- It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.
- It provides the forensic team with the best techniques and tools to **solve complicated digital-related cases**.

- Digital Forensics Specialists are generally consulted to investigate **cyber-crimes, crimes that involve a security breach in a system or network.**
- When a cyber-crime occurs, digital forensics specialists can assist in various ways.

Investigation Carried by:

- Law Enforcement officials.
- Investigation Departments.
- Civil Litigations.
- Insurance Companies.
- Private Corporations.
- Individual/Private Citizens.

Use-Cases of Digital Forensics

- Banking credit/debit card related crimes.
- Data Recovery.
- Financial Fraud Investigation.
- Damage control in the wake of cybercrime.
- Post Attack Identification.
- Log Analysis.
- Cyber Crime Investigation.
- Malware Analysis and so on….

Branches of Digital Forensics:

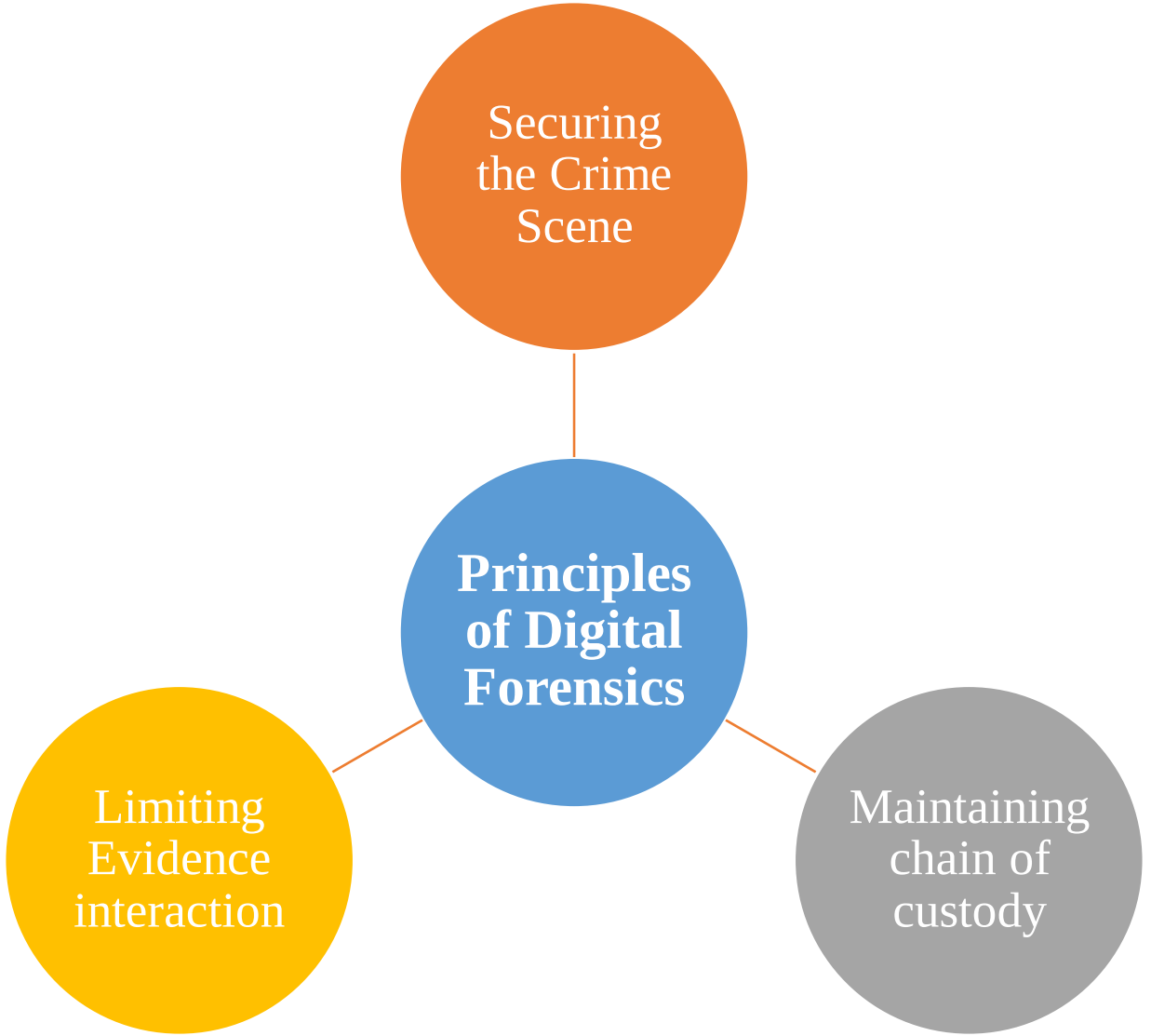
- Network Forensics.
- Email Forensics
- Web Forensics.
- Software Forensics.
- Memory Forensics.
- System Forensics.
- Cloud Forensics.
- Mobile Device Forensics
- Blockchain Forensics and so on..

Goals of a Digital Forensics Examiner

- **As a digital forensics investigator, you should have a goal for investigation.**

1. **What is the crime and Evidence?**
2. **Where it can be found?**
3. **When was the crime committed ?**
4. **Who is the culprit of the crime?**
5. **How was the crime committed?**

Principles of Digital Forensics



Digital Forensics Scientific Process

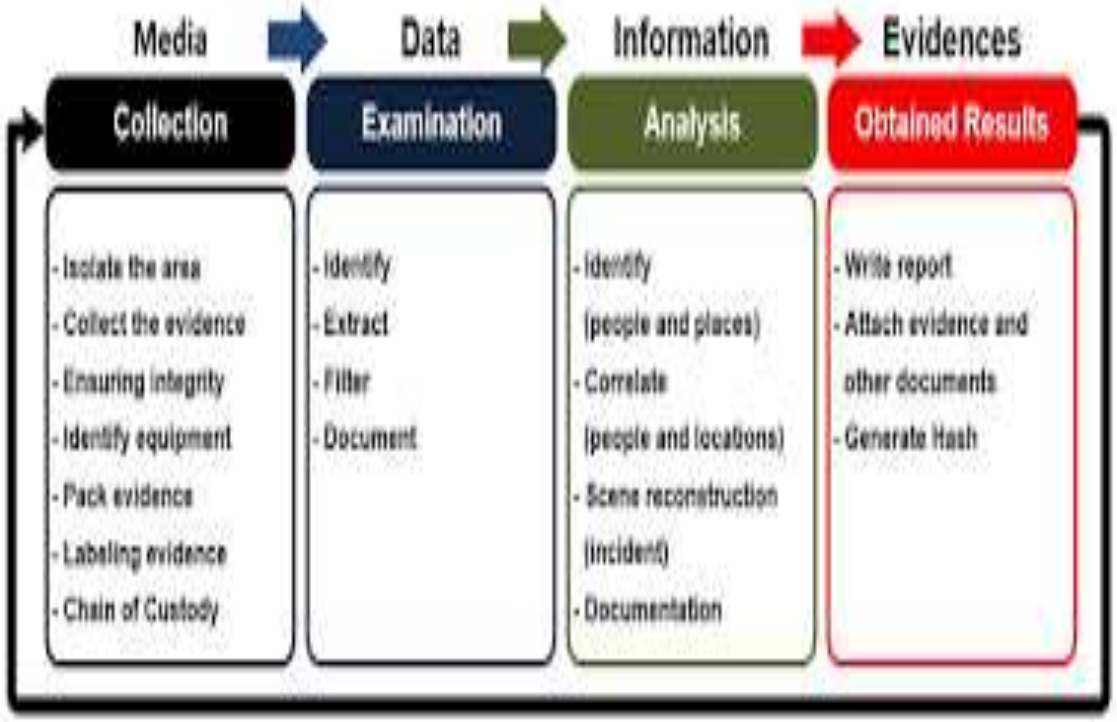
Digital Forensics Scientific Process:

A. Evidence Identification and collection.

B. Preservation.

C. Examination and Analysis.

D. Reporting.

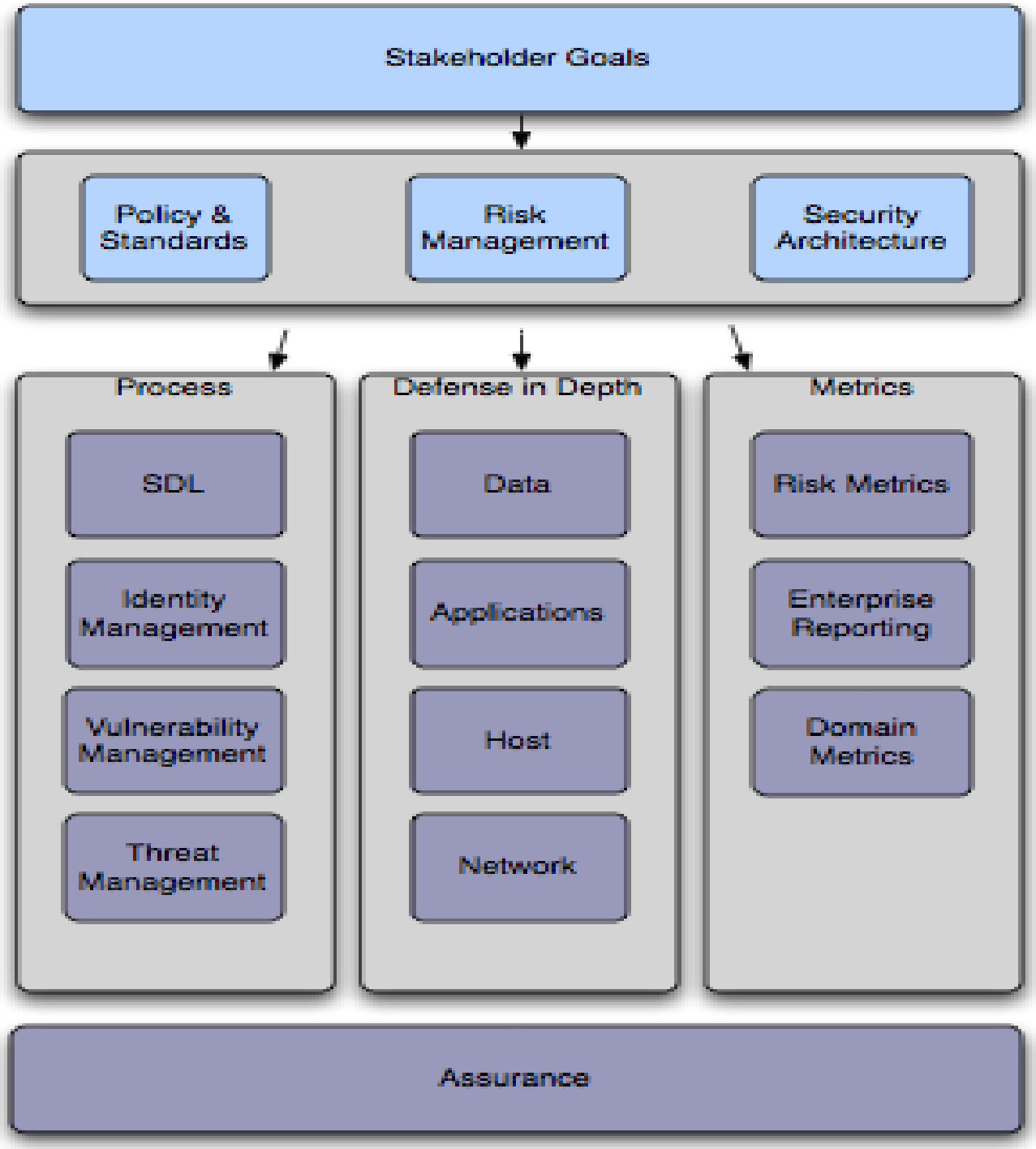


Enterprise security specification

- Enterprise security specification is a specification aimed at fomenting a minimum standard of security for enterprise applications.
- Updated Security Applications (firewalls, proxies, antivirus software, etc.) Network Architecture Design (and review) Endpoint Controls & Analysis

Major Types of Enterprise CyberSecurity Tools

- Network Firewall.
- Application Firewall.
- Anti-Virus Software (AV) .
- Network Proxy.
- Endpoint Detection and Response (EDR) .
- Vulnerability Patching.
- Intrusion Detection and Protection Systems (IDS/IPS) .
- Role-Based Access Control (RBAC)


Stakeholder Goals
Policy & Standards
Risk Management
Security Architecture
Process
SDL
Identity Management
Vulnerability Management
Threat Management
Defense in Depth
Data
Applications
Host
Network
Metrics
Risk Metrics
Enterprise Reporting
Domain Metrics
Assurance