Co-funded by the European Union

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber Security 4 ALL(CS4ALL)

Co-funded by
the European Union

Chapter 2: Network Security Architectures

Index

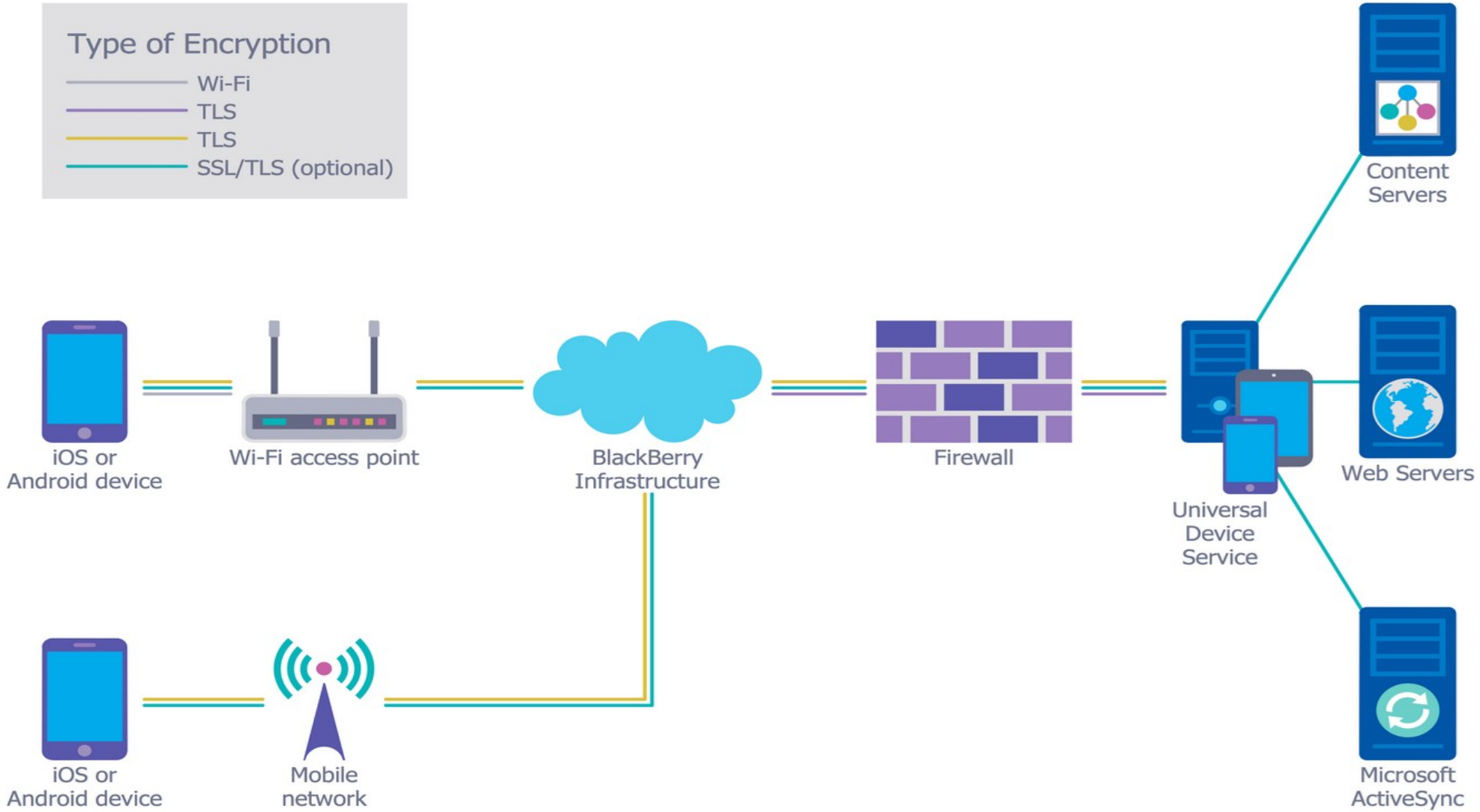
2.1 Firewall Architectures
2.2 Management by Exception
2.3 System Auditing
2.4 Basics of Intrusion Detection
2.5 Signature Versus Behavioural Detection
2.6 IDS Versus IPS
2.7 Design of SIEM
2.8 Design of a SOC

Co-funded by
the European Union

Introduction to Network Security Architecture

- Refers to the framework of policies, hardware, software, and processes used to protect a network from unauthorized access, attacks, and other cyber threats
- Provides a basis for an organization's cyber defenses and helps to protect all of the company's IT assets
- A strategy that provides formal processes to design robust and secure networks

Co-funded by the European Union



Co-funded by the European Union

Key Components

1. **Perimeter Security**:
   - Firewalls (Packet-filtering, Stateful, NGFW)
   - Intrusion Detection/Prevention Systems (IDS/IPS)
   - Demilitarized Zone (DMZ)
2. **Network Segmentation**:
   - VLANs
   - Zero Trust Segmentation
3. **Access Control**:
   - Role-Based Access Control (RBAC)
   - Multi-Factor Authentication (MFA)
4. **Data Encryption**:
   - TLS, IPsec for data in transit
   - Encryption for data at rest
5. **Endpoint Security**:
   - Antivirus, EDR, Mobile Device Management (MDM)
6. **Cloud Security**:
   - Securing cloud environments through encryption and access control

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Modern Approaches

1. **Zero Trust Architecture**:
   - Assumes no entity is trusted by default; verifies every access request.
2. **Software-Defined Networking (SDN)**:
   - Centralized network control for dynamic security policies.
3. **AI and Machine Learning**:
   - Enhances threat detection and automated responses.

Co-funded by the European Union

Challenges

- Complexity with hybrid networks
- Advanced threats (e.g., APTs, ransomware)
- Regulatory compliance (e.g., GDPR, HIPAA)

Co-funded by
the European Union

2.1 Firewall Architectures

- The design and structure of firewalls used to control and monitor network traffic.
- act as gatekeepers, deciding what traffic can enter or leave a network based on predefined security rules.
- are used depending on the security requirements, network size, and complexity.

Co-funded by the European Union

2.1.1 Packet-Filtering Firewall

- Inspects each packet header and filters traffic based on source/destination IP address, port, and protocol.
- **Advantages**:
  - Fast and simple to implement.
  - Low resource consumption.
- **Limitations**:
  - Cannot inspect the content of the packet.
  - Vulnerable to IP spoofing.

Co-funded by the European Union

2.1.2 Stateful Inspection Firewall

- Tracks the state of active connections and makes filtering decisions based on the connection's context.
- **Advantages**:
  - More secure than packet filtering.
  - Monitors entire session, not just individual packets.
- **Limitations**:
  - Higher resource consumption.
  - Complex to configure.

Co-funded by the European Union

2.1.3 Proxy-Based Firewall

- Acts as an intermediary between internal and external networks. All traffic passes through the proxy, which inspects and filters it.
- **Advantages**:
  - Deep packet inspection and content filtering.
  - Masks internal IP addresses, adding an extra layer of security.
- **Limitations**:
  - Slower performance due to traffic processing.
  - Requires more resources.

Co-funded by
the European Union

2.1.4 Next-Generation Firewall (NGFW)

- Integrates traditional firewall capabilities with advanced features like deep packet inspection, intrusion prevention, and application awareness.
- **Advantages**:
  - Detects and blocks advanced threats.
  - Can identify and control applications, users, and content.
- **Limitations**:
  - High cost.
  - Complex to configure and manage.

Co-funded by the European Union

2.1.5 Unified Threat Management (UTM) Firewall

- Combines multiple security functions (firewall, IDS/IPS, antivirus, VPN, etc.) into one solution.
- **Advantages**:
  - Simplifies security management.
  - Cost-effective for small to medium-sized businesses.
- **Limitations**:
  - Limited scalability.
  - Performance can degrade with multiple security features enabled.

Co-funded by the European Union

2.1.6 Cloud-Based Firewalls (Firewall as a Service - FWaaS)

- Firewall services delivered from the cloud to protect on-premises, remote, and cloud-based systems.
- **Advantages**:
  - Scalable and flexible.
  - Centralized management across hybrid environments.
- **Limitations**:
  - Dependent on internet connectivity.
  - Latency issues in some cases.

Co-funded by the European Union

2.1.7 Demilitarized Zone (DMZ) Firewall Architecture

- Uses multiple firewalls to create a **DMZ**, a buffer zone between the internal network and the external internet. Public services (e.g., web servers) are placed in the DMZ, limiting exposure of internal resources.
- **Advantages**:
  - Protects sensitive internal networks from external threats.
  - Allows secure public-facing services.
- **Limitations**:
  - More complex to configure and maintain.

Co-funded by the European Union

2.2 Management by Exception (MBE)

- Refers to the practice of monitoring network systems and focusing managerial efforts only on abnormal events or deviations from normal behavior.
- Rather than constantly reviewing all network activities, security managers intervene only when the system detects potential security incidents, threats, or breaches that deviate from pre-defined thresholds or normal baselines.

Key Aspects of MBE in Network Security:

1. Defining Normal Behavior
2. Automated Monitoring Systems
3. Exception-Based Alerts
4. Predefined Security Policies and Rules

Co-funded by the European Union

Example Scenarios of MBE

1. Anomalous Traffic Patterns
2. Failed Login Attempts
3. Unauthorized Access

Co-funded by
the European Union

Advantages

1. Efficient Resource Allocation
2. Improved Incident Response
3. Reduced False Positives
4. Scalability

Co-funded by
the European Union

Challenges

1. Threshold Definition
2. Reactive Nature
3. Complexity of Attack Vectors
4. Dependency on Automation

Co-funded by
the European Union

Tools for MBE

1. Intrusion Detection/Prevention Systems (IDS/IPS)
2. Security Information and Event Management (SIEM)
3. Firewall Logs
4. Endpoint Detection and Response (EDR)

Co-funded by the European Union

2.3 System Auditing in Network Security Architecture

- Refers to the process of reviewing, monitoring, and evaluating network systems and their activities to ensure security, compliance, and performance.
- Involves tracking the operations of network devices, users, applications, and other assets to detect vulnerabilities, misconfigurations, and security breaches.
- Effective auditing plays a critical role in maintaining the integrity, confidentiality, and availability of network resources.

Key Components of System Auditing in Network Security

1. Audit Logs
2. udit Trails
3. User Activity Monitoring
4. Configuration Auditing
5. Access Control Auditing
6. Compliance Auditing

Co-funded by the European Union

Benefits

1. Security Breach Detection
2. Accountability and Transparency
3. Forensic Analysis
4. Compliance and Risk Management
5. Performance Monitoring:

Co-funded by
the European Union

Challenges

1. Log Volume and Storage
2. Real-Time Analysis
3. Log Integrity
4. False Positives

Co-funded by
the European Union

Tools and Technologies for System Auditing

1. Security Information and Event Management (SIEM)
2. Intrusion Detection and Prevention Systems (IDS/IPS)
3. Log Management Solutions
4. Configuration Management Tools
5. Network Access Control (NAC) Solutions

Co-funded by the European Union

Best Practices

1. Establish Clear Audit Policies
2. Centralized Log Management
3. Regular Log Review and Analysis
4. Ensure Log Integrity
5. Retention Policies
6. Automate Where Possible

Co-funded by
the European Union

2.4 Basics of Intrusion Detection

- A critical component of **network security architecture** that focuses on identifying unauthorized access, suspicious activities, or malicious behavior within a network.
- Used to monitor and analyze network traffic or system activities for signs of potential attacks, breaches, or policy violations.
- Essential for protecting network assets, ensuring the integrity of systems, and preventing data loss or damage.

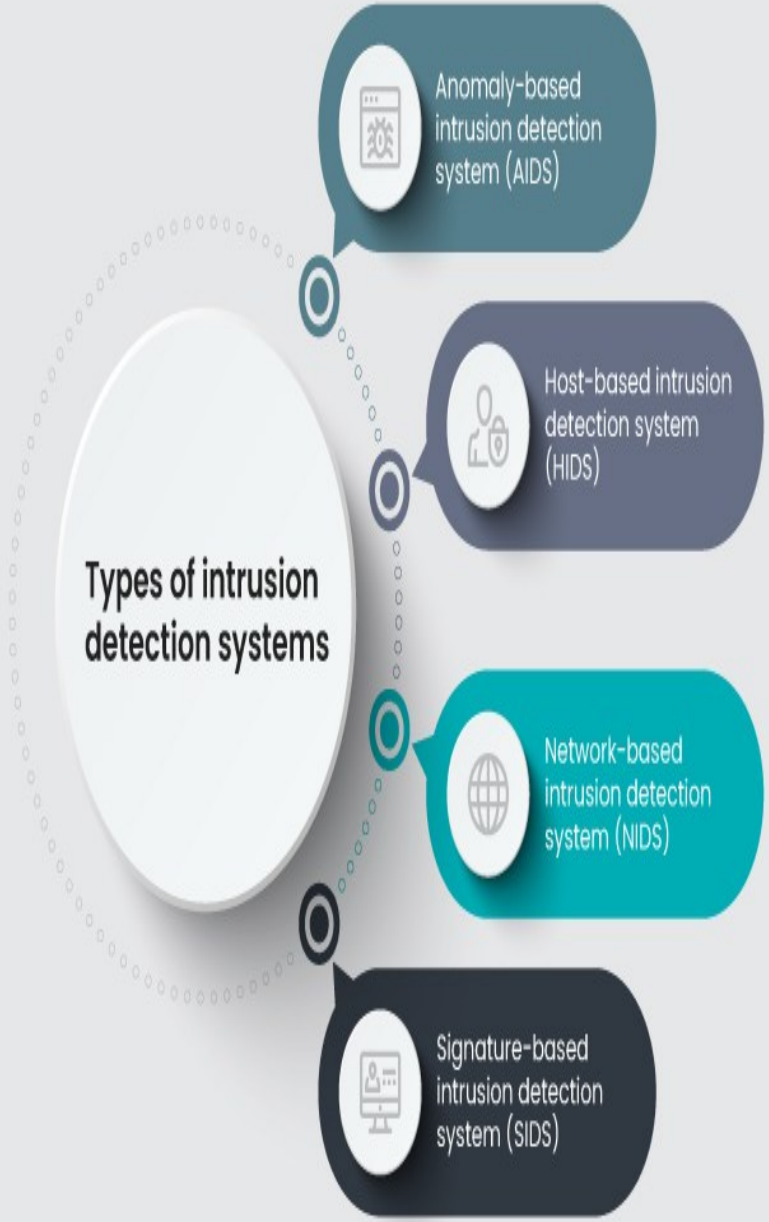
Key Concepts of Intrusion Detection

1. **Intrusion**:
   - Any unauthorized or malicious attempt to access, manipulate, or compromise the confidentiality, integrity, or availability of network systems or data.
   - can be external (from outside attackers) or internal (from authorized users misusing their access).
2. **Intrusion Detection System (IDS)**:
   - **A** tool or software that monitors network or system activities for suspicious patterns that may indicate a security incident.
   - Acts as an early warning system, alerting administrators when potential threats are detected, enabling quick responses to prevent or mitigate damage.

Co-funded by the European Union

Types of Intrusion Detection Systems (IDS)

1. **Network-Based IDS (NIDS)**:
   - NIDS monitors traffic flowing across the network, examining packet data to detect suspicious patterns or known attack signatures.
2. **Host-Based IDS (HIDS)**:
   - HIDS runs on individual hosts or endpoints, monitoring system activity, file changes, and log entries to detect abnormal behavior or malware infections.



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Detection Techniques in IDS

1. **Signature-Based Detection**:
   - Detects intrusions by comparing network traffic or system activities to a database of known attack patterns or signatures (e.g., specific byte sequences or known malware).
2. **Anomaly-Based Detection**:
   - Builds a baseline of normal network or system behavior, then detects deviations from this baseline that may indicate malicious activity.
3. **Hybrid Detection**:
   - : Combines both **signature-based** and **anomaly-based** detection methods to take advantage of the strengths of both approaches.

Co-funded by the European Union

Key Benefits of Intrusion Detection

1. Early Threat Detection
2. Improved Incident Response
3. Enhanced Network Visibility
4. Compliance and Reporting
5. Defense Against a Wide Range of Attacks

Co-funded by
the European Union

Challenges in Intrusion Detection

1. False Positives
2. False Negatives
3. Resource-Intensive
4. Tuning and Maintenance

Co-funded by
the European Union

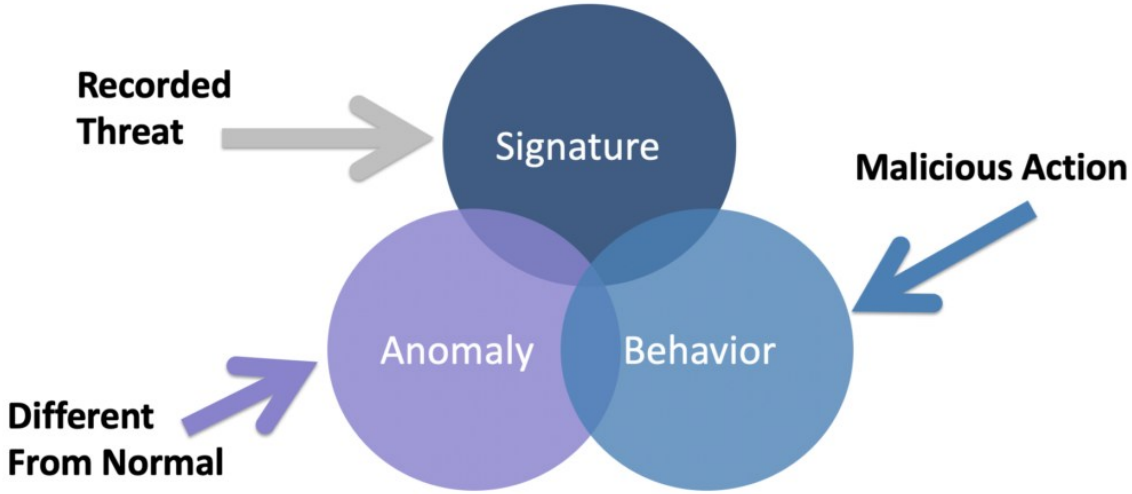
Best Practices for Implementing Intrusion Detection

1. Deploy IDS at Critical Network Points
2. Regularly Update Signatures
3. Baseline Network Behavior
4. Integrate with Other Security Tools
5. Conduct Regular Audits and Reviews

Co-funded by the European Union

2.5 Signature Versus Behavioural Detection

- When it comes to cyber threat detection, there are generally two main approaches:
- signature-based detection and behavior-based detection



Co-funded by the European Union

Signature-based detection

- used in Intrusion Prevention Systems (IPS) to identify known threats based on unique patterns called signatures
- software catches threats by their known ‘signature’ of malicious code
- Like the ‘fingerprints’ of a virus
- Makes it accurate in identifying known threats, as it is able to match the threat with its known code
- slight change in the code of a virus, it changes signature completely

Co-funded by the European Union

Behavior-based detection

- technique that analyzes the actions or behavior of files or network traffic to detect malware
- rely on heuristic rules or machine learning algorithms that can identify suspicious or malicious activities
- can detect new or unknown malware that has no signature, as well as malware that tries to hide or disguise its signature

Co-funded by
the European Union

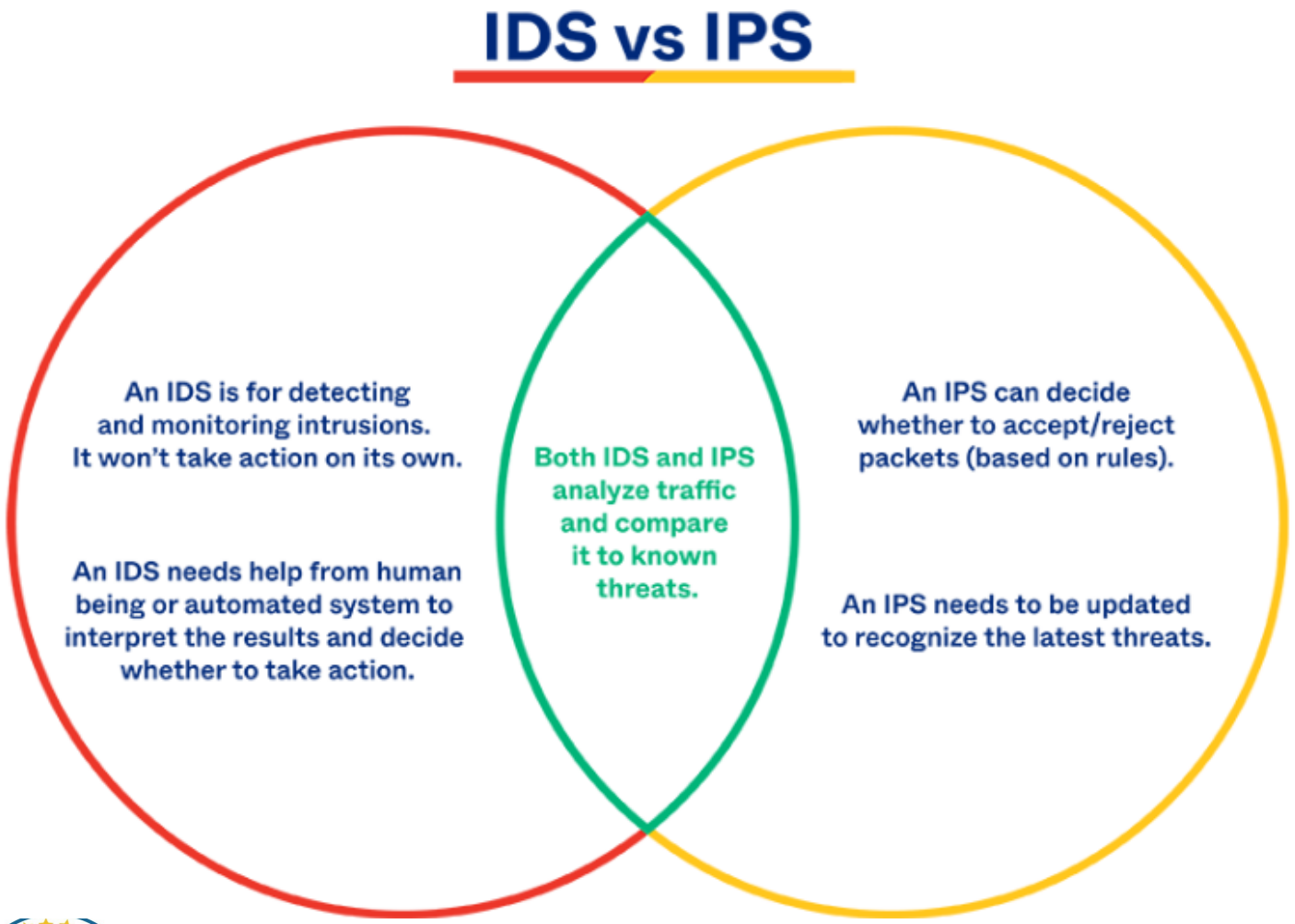
Pros and Cons

- Signature-based detection is fast, accurate, and easy to implement for known malware
- ineffective for new or unknown malware, or malware that alters its signature.

- Behavior-based detection is effective for new or unknown malware, or malware that hides its signature
- prone to false positives, evasion, and resource consumption.

Co-funded by the European Union

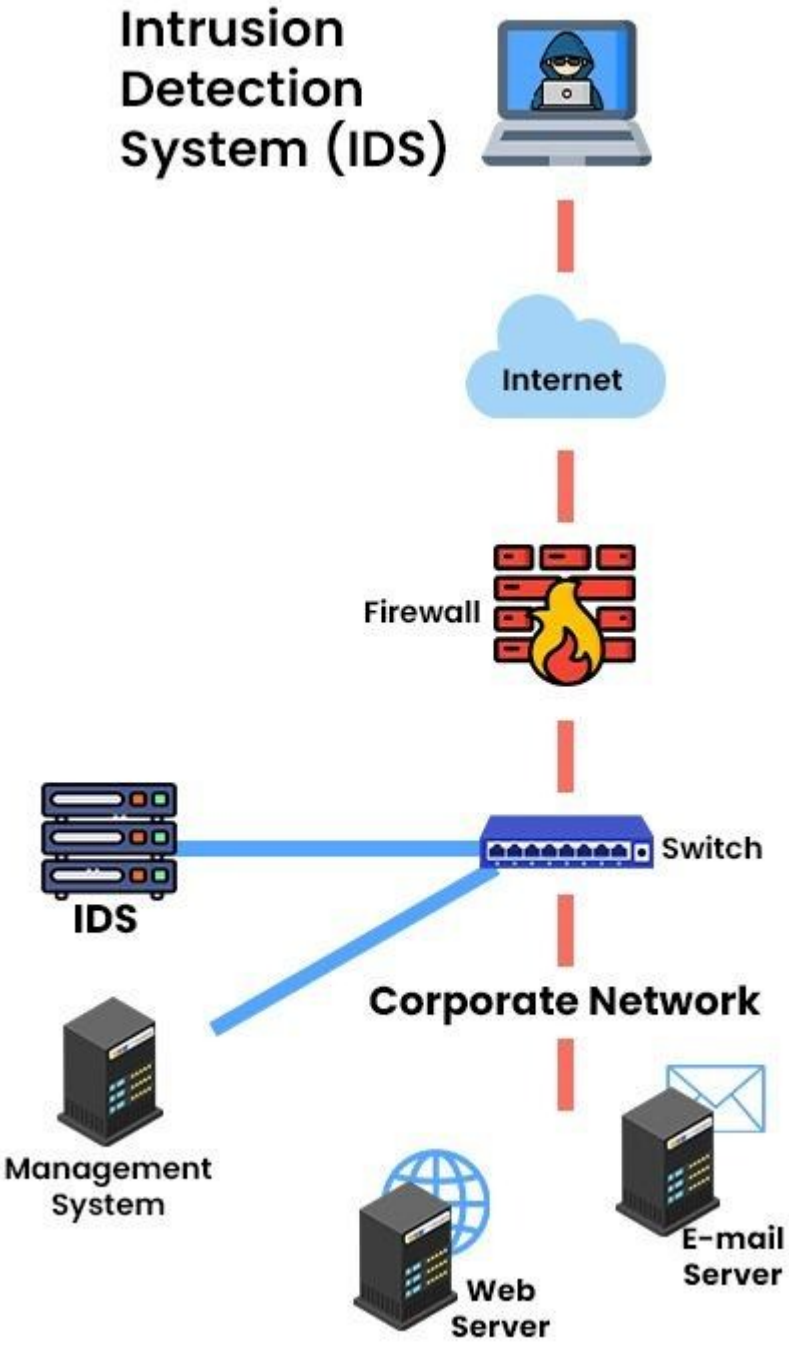
2.6 IDS Versus IPS



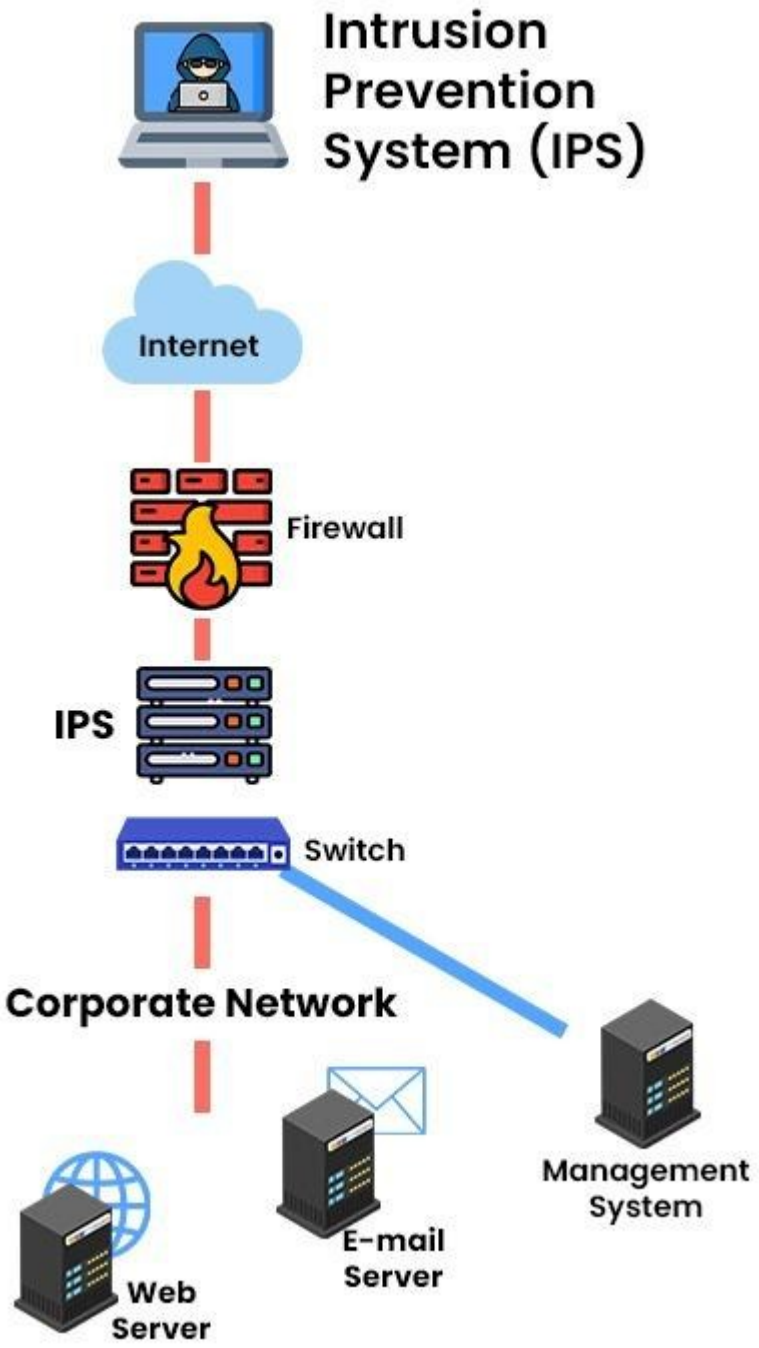
Co-funded by the European Union

Factors	Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
Function	IDS only alerts the network administrator when it detects an intrusion.	IPS actively blocks or drops the malicious packets before they reach the target.
Placement	IDS is usually placed outside the network perimeter, such as behind a firewall or a router.	IPS is usually placed inside the network perimeter, such as between a firewall and a switch.
System Type	Passive as it only monitors and then notifies the administrator.	Active as it monitor as well automatically defends the network.
Anomaly Response	Sends a notification to the user or log	Drops or modifies malicious packets
Performance	Low impact on the network speed as it only detects the intrusion.	High impact on network speed as it has to analyze and modify or block traffic in real time.

Co-funded by the European Union



Co-funded by the European Union



Co-funded by the European Union

2.7 Design of SIEM

- SIEM combines two functions:
- security information management and
- security event management

1. provides real-time security monitoring
2. allowing teams to track and analyze events
3. maintain security data logs for auditing and compliance purposes

- makes behavioral anomalies visible to security teams, enhancing the monitoring process with AI to automate incident detection and response processes.

Co-funded by the European Union

SIEM PROCESS FLOW

SIEM Operational Process Flow

Co-funded by the European Union

How Does SIEM Work?

- Data collection
- Data storage
- Policies and rules
- Data consolidation and correlation

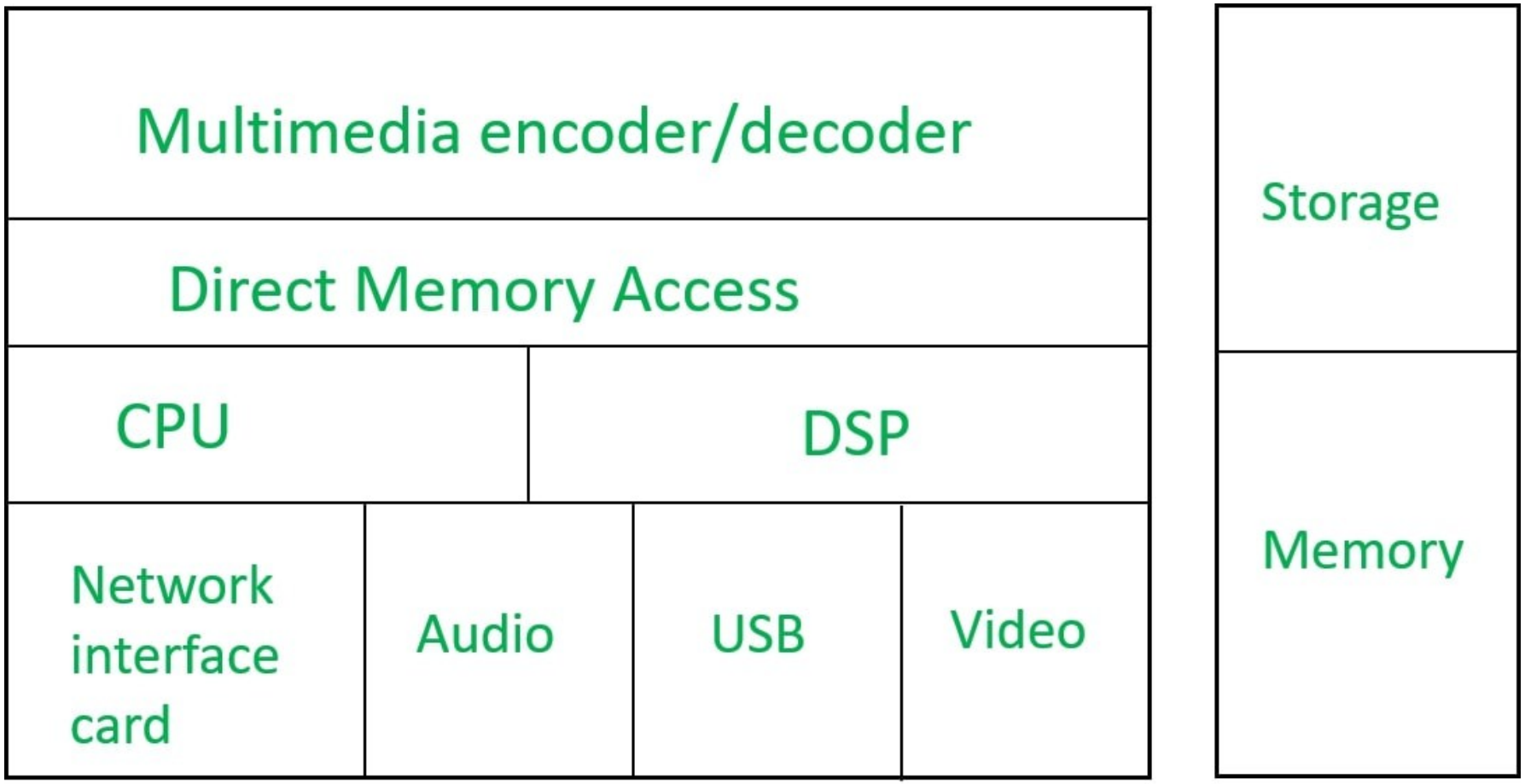
Co-funded by
the European Union

2.8 Design of a SOC

- System On Chip
- a small integrated chip that contains all the required components and circuits of a particular system

Co-funded by
the European Union

Architecture of SoC



Co-funded by the European Union

Advantages of SoC

- small in size and includes many features and functions.
- consumes low power.
- flexible in terms of size, and power factor.
- built on a single chip.
- cost-effective.
- produced in a large quantity.

Co-funded by the European Union

Disadvantages of SoC

- Time-consuming designing process.
- takes six to twelve months.
- If any component of the SoC is not functioning properly then it cannot be replaced in that case an entire SoC has to be replaced.
- Visibility is limited.

Co-funded by
the European Union

Uses of SoC

- Used in smartphones, smartwatches, tablets, and computers.
- Internet of Things applications such as home automation.
- Embedded systems applications especially where the microcontroller is used.

Co-funded by the European Union

Learning Outcome

After successful completion of this course, students would be able to:

1. understand the key concepts of signature-based detection
2. Enhance the knowledge of Security information and event management tools have provided a definitive security infrastructure to defend organizations and their networks.
3. Learn the concepts of SoCs help simplify circuit board design, resulting in improved power and speed without compromising system functionality
4. Understand various Firewall Architectures and their roles in securing network boundaries.
5. Differentiate between Signature-Based and Behavioral Detection techniques in Intrusion Detection Systems (IDS).
6. Design the structure and key components of a Security Information and Event Management (SIEM) system and a Security Operations Center (SOC) for comprehensive threat management.

Question no 1

Which type of firewall inspects traffic at the application layer and can filter based on specific protocols like HTTP and FTP?

A. Packet-filtering firewall

B. Stateful firewall

C. Next-Generation Firewall (NGFW)

D. Proxy firewall

Co-funded by the European Union

Question no 2

What is the primary purpose of Management by Exception in network security?

A. **Monitoring all network traffic in detail**

B. **Automating the response to all detected threats**

C. **Focusing on abnormal or critical security events**

D. **Blocking all unauthorized network access**

Co-funded by the European Union

Question no 3

System auditing in network security primarily helps to:

A. **Block unauthorized users**

B. **Track and analyze network activities for compliance and threat detection**

C. **Encrypt data on the network**

D. **Design firewall rules for traffic filtering**

Co-funded by the European Union

Question no 4

Which type of detection method in IDS relies on identifying known attack patterns?

A. **Signature-based detection**
B. **Anomaly-based detection**
C. **Heuristic-based detection**
D. **Behavioral-based detection**

Co-funded by the European Union

Question no 5

How does an Intrusion Detection System (IDS) differ from an Intrusion Prevention System (IPS)?

A. **IDS actively blocks malicious traffic, while IPS only monitors**

B. **IDS only detects and alerts, while IPS can block suspicious traffic**

C. **IDS operates at the network layer, while IPS operates at the application layer**

D. **IDS is used for encryption, while IPS is used for decryption**

Co-funded by the European Union

Question no 6

System on chip means:

A. **It consists of both analog and digital IC**
B. **Only analog IC**
C. **Only digital IC**
D. **None of the mentioned**

Co-funded by
the European Union

Question no 07

What are the major components of the intrusion detection system?

A. Analysis Engine
B. Event provider
C. Alert Database
D. All of the mentioned

Co-funded by the European Union

Question no 08

What role does the term "packet filtering" play in the operation of an IPS?

A. **Improving website aesthetics**
B. **Enhancing server performance**
C. **Analyzing and selectively blocking or allowing network packets**
D. **Granting unrestricted access to all user**

Co-funded by the European Union

Question no 09

How does an IPS handle encrypted traffic to detect and prevent malicious activities?

A. **Improving website aesthetics**
B. **Enhancing server performance**
C. **By decrypting and inspecting encrypted traffic before making decisions**
D. **Granting unrestricted access to all users**

Co-funded by the European Union

Question no 10

What is the primary role of an Intrusion Detection System (IDS) in web security?

A. Enhancing website aesthetics
B. Actively blocking malicious traffic
C. Monitoring and detecting potential security incidents
D. Granting unrestricted access to all users

Co-funded by the European Union

Answers

1. **A.** Next-Generation Firewall (NGFW)
2. **C.** Focusing on abnormal or critical security events
3. **B.** Track and analyze network activities for compliance and threat detection
4. **A.** Signature-based detection
5. **B.** IDS only detects and alerts, while IPS can block suspicious traffic
6. **A.** It consists of both analog and digital IC
7. **D.** All of the mentioned
8. **C.** Analyzing and selectively blocking or allowing network packets
9. **C.** By decrypting and inspecting encrypted traffic before making decisions
10. **C.** Monitoring and detecting potential security incidents

Co-funded by the European Union

REFERENCES

- Stallings, W. (2020). Network Security Essentials: Applications and Standards. Pearson.

https://elhacker.info/manuales/Redes/3._Network-security-essentials-4th-edition-william-stallings.pdf

Co-funded by the European Union

Reference Book

- "Building Internet Firewalls" by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, 2nd Edition

Co-funded by
the European Union