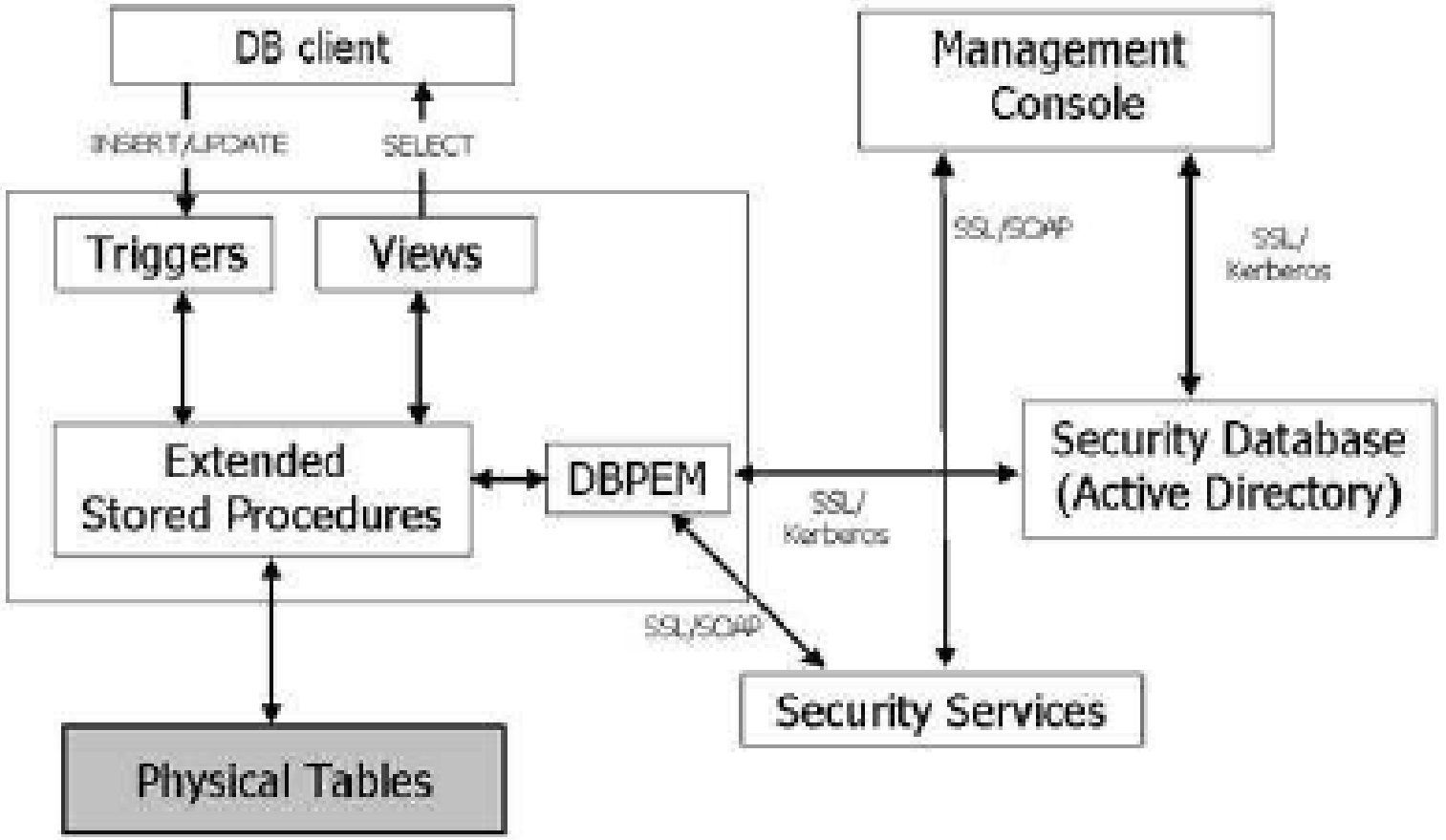
Chapter 1. SECURITY OVERVIEW

- Security Definition: Security is an intensive field that protects information, data, and resources from unauthorized access, unauthorized alteration, and destruction.
- Objectives of Information Security
  - Protect the integrity, availability, and confidentiality of information.
  - Ensure properly controlled and authorized access to information.
  - Prevent and respond to threats and security risks.



Architecture of a database security system

- The Important Role of Security
  - Security is a sinking factor in today's digital environment, especially as information becomes a critical resource.
  - The positive impact of security on organizational trust, reputation, and customer relationships.
- The Link Between Security and Risk Management: Security and risk management are deeply linked; Security helps mitigate risks and protect the organization from negative consequences.

- Scope of Information Security: Security is not only about technology, but it also requires attention to culture, processes, and people.
- The Necessity of Security in Modern Society: In today's digital age, security is an important key to maintaining safety and protecting privacy.
- Current and Future Challenges: Recognize current challenges as threat intensification and emphasize the need for innovation to deal with them.

- Information and Data
  - A description of the importance of information and data to the organization's operations.
  - Distinguish between public and sensitive information.
- Information system
  - Clearly state the role of the information system in the day-to-day operation of the organization.
  - Basic characteristics of systems, including networks, servers, and connected devices.

- Software and Applications: Emphasize the importance of protecting software and applications from unauthorized use or hacking.
- Process and Services: Identify critical processes and services that the organization must protect, and emphasize the alignment between security and day-to-day operations.
- Personnel: Clearly state the important role of personnel and the importance of educating and training them in information security.

- Privacy and Legal Compliance: Describe your organization's obligations and responsibilities regarding privacy and legal compliance.
- Resilience and Redundancy: Clearly state the need for a disaster recovery plan and contingency measures to mitigate the impact of a security incident.

- Security vulnerability definition: Describe the concept of a security vulnerability and how it can be interpreted as a weakness in the system.
- Classification of security vulnerabilities: List and describe common types of security vulnerabilities, including software, hardware, and people vulnerabilities.
- Relationship to Threats and Risks: Reconcile security vulnerabilities with threats and risks to understand why they need to be addressed.

- Practical Examples of Security Vulnerabilities: Provide specific examples of information security incidents that have occurred due to security vulnerabilities.
- Impact of Security Vulnerabilities: Assess the negative impact of a security vulnerability, including financial and reputational damage to the organization.
- Causes of security vulnerabilities: Analyze the main causes leading to the occurrence of security vulnerabilities, including human and technical factors.

- Security Testing and Vulnerability Detection: Presents the process of security testing and how to detect security vulnerabilities before they can be exploited.
- Prevention and Coping Strategies: Clearly state the strategy the organization needs to implement to prevent and respond to security vulnerabilities.

- Unauthorized Access Control: Describes how hackers can control or gain unauthorized access to systems or data.
- Network attacks: List and describe cyber attack methods such as sniffing, spoofing, and phishing.
- Phishing and Social Engineering: Explain how hackers use email, phone, or social media phishing techniques to deceive users.

- DoS (Denial of Service) Attack: Describes how hackers send large amounts of traffic to overload the system, making the service unavailable.
- Ransomware Attack: Demonstrates how ransomware encrypts data and demands a ransom to recover it.
- SQL Injection and Cross-Site Scripting (XSS) Attacks: Describes how hackers can enter malicious SQL commands or scripts into websites and applications to obtain information or perform unauthorized actions.

- Zero-Day Attacks: An introduction to undisclosed security vulnerabilities and how hackers can take advantage of them before taking precautions.
- Insider Threat Attack: Describe how people in the organization could become a threat if they abuse their authority.
- IoT (Internet of Things) Attack: Link to how Internet-connected devices can become weaknesses in secure systems.

- Monitoring and Logging: Describe how the system continuously monitors and records activities to detect manifestations of an attack.
- Data Analysis and Security Reporting: An introduction to using data analysis tools and techniques to identify suspicious patterns.
- Intrusion Detection System (IDS): Describe how the alert system can recognize unusual activities and alert immediately.
- Network Intrusion Detection System (NIDS): Presentation of how network alert systems monitor network traffic to detect attack activities.

1.5. Measures to detect attacked systems

- Host-based Intrusion Detection System - HIDS: Describes how the host alert system monitors activities on each device to detect intrusions.
- Security Information and Event Management - SIEM): An introduction to how SIEM can combine data from multiple sources to analyze and report security events.
- Periodic security check: Describe the importance of performing periodic security checks for early detection of security issues.

1.5. Measures to detect attacked systems

- Reputation Model and Risk Classification: Clearly state the use of reputation models and risk classifications to prioritize threats.
- Behavioral analysis method: An introduction to analyzing user and system behavior to identify suspicious activity.
- Application of Artificial Intelligence and Machine Learning: Describes how artificial intelligence and machine learning can be used to improve attack detection and response.

- Research and propose security privacy Rules

- Objectives and Scope: Describe the specific objectives targeted by the privacy policy and their scope, including the type of data and the system.
- Basic Rules and Regulations: List the basic rules and principles that everyone in the organization needs to follow to ensure information security.
- Access Management: Describes how to manage access and privileges, including the process for granting and withdrawing permissions.

- Network and System Security: Specification of specific security measures deployed on networks and systems to protect against attacks.
- Password Management: Describes how to manage and protect passwords, including the process of creating, managing, and especially changing passwords periodically.
- Physical Security: Specification of physical security measures such as access control to buildings, engine rooms, and critical equipment.

- Data Backup and Restore Policy: Describes how the organization will perform data backups and recovery procedures after an incident.
- Mobile Media Policy: Regulates the use and protection of information on mobile devices such as phones and tablets.
- Security Education and Training: Describe an education and training plan to improve employee security awareness and behavior.

- Compliance and Performance Evaluation: Specify how the organization will monitor and evaluate performance for security policy compliance.
- Acknowledging and updating the Policy: Describe the process for assessing, validating, and updating security policies to ensure efficiency and relevance to a changing environment.

Enjoy the Course…!