John Carlo D.R. Roxas

BSIT 4-1

**Activity 3: Designing a Secure System Architecture**

**Security Objectives**

The university portal has a lot of information not only about the students who register here but also the information about the professors, so the CIA was incorporated to better protect the sensitive data here. In confidentiality, the system encrypts all data, whether stored or transmitted, so that only authorized individuals can access it. To ensure that only authorized individuals can access a specific part of the system, RBAC, or role-based access control, is used. This helps control role-based access, ensuring that students, professors, and administrators can only see or change information they are allowed to. Integrity is also incorporated into the portal to use hashing to keep data accurate and unaltered, while audit trails record any changes, making it easy to track and address unauthorized modifications. Availability is also  incorporated,  it prioritizes setting up backup systems and failover mechanisms, so even if problems occur, the portal remains accessible to users. In terms of authenticity and accountability, these are incorporated to ensure that users are verified through secure multi-factor authentication and that all actions within the system are logged, helping to prevent unauthorized access and making it easier to trace and address any suspicious activities.

**Threat Analysis**

Passive Attacks

1. Eavesdropping
   * The impact of eavesdropping on the portal is that it compromises confidentiality, exposing sensitive user data to malicious entities, which can lead to identity theft or unauthorized access to records.
2. Traffic Analysis
   * The impact of traffic analysis on the portal is that while the data remains encrypted, this attack compromises privacy, potentially allowing attackers to profile user behavior or identify vulnerabilities in the system.

Active Attacks

1. Denial of Service (DoS)
   * This disrupts availability, potentially causing delays in course registrations or access to critical academic resources, leading to frustration and operational challenges for the university.
2. Masquerade
   * It compromises authenticity and integrity, allowing an attacker to modify records, send fraudulent communications, or steal sensitive data, destroying trust in the system.

**Secure Architecture Proposal (including the diagram)**

So the firewall is placed at the perimeter of the network to control traffic and prevent unauthorized access to the portal and database, while the intrusion detection system (IDS) continuously monitors the system for suspicious activities and detects potential intrusions or attacks by analyzing network traffic. The portal itself is protected using TLS encryption for secure data transmission and multi-factor authentication (MFA) to ensure only authorized users can log in, and encryption uses AES for data at rest and TLS for data in transit to secure sensitive data both in storage and during transmission. Data integrity is maintained by using hashing algorithms to verify that stored data has not been altered and digital signatures to prove the authenticity of critical communications. And last but not least is the database server to securely store sensitive information, ensuring both privacy and integrity through encryption. This architecture forms a robust security framework, ensuring confidentiality, authenticity, and protection from unauthorized access and attacks.

Firewall

Database Server

Data Integrity (Hashing)

Authentication (MFA)

Encryption

AES, TLS()

University Portal

Intrusion Detection System

**Mitigation Strategies**

1. To prevent eavesdropping, use TLS/SSL encryption for all communications and AES-256 encryption for data at rest. To detect, use the Intrusion Detection System (IDS) to identify unusual activities, and to recover, regenerate session keys and invalidate compromised credentials to prevent further unauthorized access.
2. To prevent traffic analysis, implement traffic obfuscation techniques like VPNs or Tor and end-to-end encryption. To detect, analyze network traffic for abnormal patterns. To recover, block malicious IP addresses and investigate the source.
3. To prevent Denial of Service (DoS) attacks, implement a Web Application Firewall (WAF), rate-limiting, and traffic filtering. To detect, set up DoS detection mechanisms and IDS to monitor for abnormal traffic patterns. To recover, activate failover systems and implement DDoS protection services.
4. To prevent masquerade attacks, implement multi-factor authentication (MFA), strong password policies, and IP whitelisting. To detect, monitor login behavior and track activities with audit trails. To recover, invalidate compromised credentials and force password resets.