IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Ekanayake Bandara
Student Reference Number:10899241

Module Code: PUSL 2025	Module Name: Security Architecture & Cryptography
Coursework Title: Design and Evaluation of a Secure System Architecture for Online Learning Management System for a University.	
Deadline Date:2024/03/04	Member of staff responsible for coursework:
Programme: BSc (Hons) Computer Security	

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.

We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.

Signed on behalf of the group:

Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***

Signed:

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state name of software……

Overall mark _____% Assessors Initials _____ Date_____

*Please delete as appropriate

Secure System Architecture for Online Learning Management System

Introduction

Universities now rely heavily on online learning management systems to provide flexible and easily accessible instruction. However, issues with data security and privacy are brought up by their broad use. A safe system architecture created especially for university LMS systems is presented in this research. My goal is to reduce security threats while maintaining the availability of educational resources. Data security, access control, authentication procedures, secure communication, attack resistance, and regulatory compliance are some of the major issues. I suggest a defence in depth strategy and carry out exhaustive tests to confirm our architecture's efficacy. Universities may improve the security of their online learning environments and safeguard sensitive data by putting these precautions into place.

Principles I use to design this secure system architecture

I create this system by applying the CIA Triad and the model I use for this system is Clark Wilson Model the reason I decide to use this model because this is the best model for the LMS system. By using this model, I can apply the CIA Triad for all of the method. But this Clark Wilson Model mainly focus on the integrity. This model addresses all the goals of the integrity.

This how we can apply the Clark Wilson model for the CIA Triad

Confidentiality

This Clarke Wilson paradigm emphasizes access control above confidentiality, ensuring that only authorized users may access certain resources inside the LMS. By limiting unwanted access to private data, this helps to preserve confidentiality inadvertently.

Integrity

By demanding well formed transactions and enforcing the separation of tasks, this paradigm strongly emphasizes data integrity. This preserves the integrity principle by guaranteeing that the data in the LMS stays reliable, accurate, and consistent.

Availability

Although this model does not prioritize availability, we may nevertheless use it in this way: by correctly putting its guiding principles like limited access and fault recovery mechanisms into practice, we can help ensure the availability of the LMS inadvertently. The system is less prone to mistakes and downtime, which improves availability, by preventing unauthorized alterations and guaranteeing the accuracy of transactions.

Security requirement and the threats in the scenario

Threats in the scenario

These are the treats mostly focused when design a security architecture for the LMS.

- Unauthorized access
- Data breaches

- Malware attacks
- Phishing attacks
- Denial of Service (DoS) attacks
- Insider threats
- Loss of data
- Regulatory non-compliance

Security requirements

- Data confidentiality
- User Authentication
- Access Control
- Availability
- Backup and Recovery

These are the security requirements I use for this system. Below I propose these requirements using the Clack Wilson model.

Security requirements using Clark Wilson model

- Data confidentiality

  Make sure that sensitive information, such student records and course materials, may only be accessed by those who are allowed. Apply access restrictions using the least privilege concept. To limit access to sensitive data based on users' roles and responsibilities, employ role based access control.

- User Authentication

  Apply strong authentication procedures to verify the identities of users when they log into the LMS. Implement authentication procedures to verify the identities of users before allowing them access to the LMS. To improve security, use multi factor authentication and other strong authentication methods.

- Access Control

  Implement fine grained access restrictions to limit users' access to particular LMS resources. To impose access controls based on user roles and permissions, use role-based access control. To stop illegal access to private information, use separation of roles.

- Availability

  Towards that aim, I make sure the LMS platform is always accessible to instructors and students. Recognize service interruptions and put recovery plans in place for them. Make use of failover and redundancy procedures to guarantee the LMS's high availability.

- Backup and Recovery

  Towards that aim, make sure the LMS platform is always accessible to instructors and students. Recognize service interruptions and put recovery plans in place for them. Make use of failover and redundancy procedures to guarantee the LMS's high availability.

Security Architecture Design

- Access control mechanisms

  Use role-based access control to enforce the principle of least privilege. Assign roles with certain rights, such as administrator, professor, and student.

  Use Access Control Lists to limit access to resources that are considered sensitive according to user roles and data classifications.

- Encryption

  Employ robust encryption techniques to safeguard data while it's in transit and at rest inside the LMS.

  Use Public Key Infrastructure to issue digital certificates and manage keys securely.

- Authentication

  To improve the security of user authentication, use multi-factor authentication. Request a combination of the user's knowledge (password), property (smart card) and identity (biometrics),

  Implement account lockout procedures to reduce the impact of brute force and password guessing attacks.

- Intrusion Detection/Prevention system

  Install network-based IDS/IPS to keep an eye on network traffic, detect unusual activity and alert or prevent any vulnerability.

  On LMS servers, implement host-based IDS/IPS to detect and handle suspicious activity or unwanted access attempts.

- Logging/Auditing Mechanisms

  Monitor all important security events such as system configuration changes, access control adjustments, and authentication attempts.

  Regularly examine audit logs for anomalies, security incidents, and regulatory compliance.

- System Integrity Controls

  To ensure the integrity of important system files and configurations, use digital signatures.

  To ensure the integrity of the system boot process and prevent damage to boot components, use safe boot procedures.

- Scalability and Maintainability

  Create a scalable security architecture by using modular and scalable components that can handle the increase in the number of users and data.

Regularly update and patch security components to fix vulnerabilities and ensure the security architecture continues to function over time.

Effectiveness of the system

Using MFA techniques significantly increases user authentication security by reducing the likelihood of unauthorized access.

Encryption methods reduce the chance of data breaches by ensuring data privacy in transit and at rest.

RBAC rules effectively manage access to sensitive data, therefore mitigating the potential impact of insider threats.

Efficiency of the system

Because of its modular architecture, it can easily expand or contract to meet evolving security needs.

The overall effectiveness of threat detection and system recovery is enhanced by both automated intrusion detection systems and redundancy measures.