Angel Ordonez Retamar

CPE 592-WS1 Final Project

*I pledge my honor that I have abided by the Stevens Honor System*

# Document Server for Stevens Network

The objective of this project is to design a secure document server for the Stevens Network that will facilitate document sharing between teachers and students while maintaining strict access control, data integrity, and secure communication. The importance of secure document sharing cannot be overstated, especially in educational settings where sensitive information such as grades, assignments, and research papers are involved. Unauthorized access to such data can lead to breaches of confidentiality, data manipulation, or even loss of critical academic information. The project will address security challenges associated with document sharing, including unauthorized access, tampering, and network vulnerabilities. The proposed system will allow teachers to securely share documents with students and grant, or revoke permissions as needed. Students will be able to edit documents, but changes will only become visible after the teacher’s approval. The system also will ensure that shared documents remain accessible only within the Stevens Network or a secure VPN connection. The system's ability to enforce access control and maintain data integrity is crucial in upholding the institution's data security standards.

The design of this document server will use the following course topics: cryptography and encryption algorithms for secure data storage and sharing, wireless networking protocols to restrict access to the Stevens Network, digital watermarking techniques to maintain data integrity and authenticity, and security challenges related to network access and data sharing. The project will address the implementation of each feature, the associated security challenges, and the proposed mitigation strategies.

To secure document sharing and group access, the system will employ encryption techniques to protect files during storage and transmission. Teachers, acting as administrators, will be able to upload documents to the server, specifying the group of students who can access them. The server will use symmetric key encryption, such as AES, to encrypt documents before storing them. This choice is driven by AES's efficiency, high-speed encryption capabilities, and widespread acceptance as a secure standard. Additionally, AES's ability to handle large volumes of data without significant performance degradation makes it suitable for an academic environment where documents can range from simple text files to multimedia content. Group keys will be generated and securely distributed using asymmetric cryptography, such as RSA, to the authorized users. RSA is chosen for its robust public-key encryption properties, which are essential for securely transmitting keys over potentially insecure networks. Security challenges include ensuring that only authorized users receive the decryption key without interception and preventing unauthorized access if the keys are leaked. Mitigation strategies include using secure key distribution protocols that utilize RSA to transmit the AES key and implement role-based access control (RBAC) to manage permissions efficiently. RBAC not only simplifies the management of user rights but also ensures that only designated users have access based on their roles, reducing the risk of data exposure.

To ensure controlled editing and teacher approval, students will be able to submit edits but the changes will be stored temporarily as encrypted draft versions. The system will generate a digital signature for each draft using a secure hashing algorithm, such as

SHA-256. The teacher must approve the edited draft for it to be merged into the official document. Security challenges include ensuring that draft versions are not altered without authorization and verifying that approved versions remain unchanged. Mitigation strategies include using digital signatures to authenticate the source and integrity of each version and storing version histories with hash-based checksums to detect unauthorized changes.

To control permissions, teachers will be able to revoke access to shared documents at any time. When a revocation occurs, the document is re-encrypted with a new key, and previous keys will be invalidated. Active sessions that still hold old keys will immediately be terminated. The server will periodically check for key validity to enforce revocations in real-time. Security challenges include ensuring that revocations instantly take effect even if users are currently accessing the document and avoiding prolonged access after revocation. Mitigation strategies include implementing short-lived session keys that require frequent re-authentication and monitoring active sessions and enforce logouts upon key invalidation.

To restrict access to the Stevens Network, the document server will only be accessible within the university's local network or via VPN. The VPN gateway will enforce multi-factor authentication to strengthen security. All data transmitted over VPN will be encrypted using secure protocols such as OpenVPN or IPSec. Security challenges include an attacker obtaining VPN credentials and attackers mimicking internal IP addresses to gain access. Mitigation strategies include using MFA to add an additional layer of security for VPN access and implementing IPsec-based authentication to verify client legitimacy.

Overall threats and vulnerabilities include data theft through unauthorized access, data integrity issues from unapproved edits, and potential for man-in-the-middle attacks on VPN connections. Overall mitigation techniques would include protecting data at rest and in transit using encryption such as AES and RSA, ensuring data integrity and non-repudiation of edits, and VPN authentication, IP filtering, and MFA. Tools and technologies that would be implemented include Python's PyCryptodome for encryption and hashing, FTP for file transfers within the local network, HTTP over SSL/TLS for secure web access, and OpenVPN for secure remote access.

In conclusion, the proposed secure document server design addresses the challenges of secure document sharing, controlled editing, permission management, and restricted network access within the Stevens Network. By employing robust encryption techniques, secure network protocols, and careful access management, the system ensures data confidentiality and availability. This project highlights the importance of integrating cryptography and secure networking practices into practical applications. Implementing these measures effectively mitigate potential security threats and follows best practices in network security and data management.