Christopher Spadavecchia
CPE 592
Final Project
Question 2

Securing Stevens, One Document at a Time

In this paper, I propose a secure, role-based document server design using File Transfer Protocol (FTP) and HyperText Transfer Protocol (HTTP) tailored for the Stevens Institute of Technology. This system will ensure access control, confidentiality, and integrity of documents shared between teachers and students. Given the constraints and goals, especially limiting access within the Stevens network or over a Virtual Private Network (VPN), this design prioritizes internal network isolation, secure authentication, and controlled collaboration. The proposed system is a web-based document server accessible over HTTP(S) with optional FTP support for legacy compatibility. It will be deployed on a private subnet of the Stevens Network and accessible externally only through a secured VPN connection.

Teachers can upload and share documents with specific groups of students using a user management panel. Access control lists (ACLs) map documents to specific user roles, ensuring that only authorized individuals can view or edit content. Each user logs in using institutional credentials through Lightweight Directory Access Protocol (LDAP) or Active Directory. LDAP is an open, vendor-neutral protocol that enables applications to query and manage directory information services, such as user identities and access privileges, across a network. Active Directory, developed by Microsoft, extends LDAP functionality by incorporating additional services like Kerberos authentication and Group Policy, which allow centralized management of users, devices, and permissions in a secure domain environment. A version control system, such as a Git backend or document diffing tool, will track student edits. These edits will be stored as pending changes until a teacher reviews, approves, rejects, or merges them into the live version. Audit trails will log all modifications for accountability. Teachers will also have dynamic permission control through the web interface, enabling them to revoke access when needed. Access tokens and session cookies will be invalidated immediately upon revocation to ensure that unauthorized access is prevented.

The server will reside behind a university firewall, configured to allow access only from whitelisted internal IP ranges. All Domain Name System (DNS) and Internal Protocol (IP) routing will restrict public access, thereby enforcing internal network isolation. For remote access, Stevens' VPN service will be used. Only users connected via the official VPN will be able to resolve or reach the internal server's IP address. Integration with the VPN login will map authenticated users to document access roles. In addition to VPN use, a reverse proxy can be deployed to perform URL-based routing and Transport Layer Security (TLS) termination, further protecting internal resources from external probing or misconfiguration.

The system will face several security challenges. Unauthorized access by a student to documents not intended for their group will be mitigated through Role-Based Access Control (RBAC) and ACLs, combined with LDAP authentication and optional two-factor authentication. Man-in-the-middle (MitM) attacks, where attackers might intercept credentials or content, will be prevented by enforcing HTTPS with TLS 1.3 encryption and prohibiting plain FTP. Data tampering or malicious modifications will be countered by implementing cryptographic hashing such as SHA-256 and storing checksums of original versions. A cryptographic hash function like SHA-256 takes an input (e.g., a document) and produces a fixed-size string of characters, which serves as a unique fingerprint of the data. Even the slightest change in the input results in a completely different hash value, making it easy to detect tampering. By storing the original hash value (checksum) alongside each file version, the server can continuously verify the integrity of the document by recalculating its hash and comparing it to the stored value. If the values differ, it indicates that the file has been altered, either accidentally or maliciously. Signed commits will ensure changes are verified. Denial of Service (DoS) attacks that might overload the server will be mitigated by rate limiting, the use of fail2ban, and load balancers. Rate limiting controls the number of requests a user or IP address can make in a given timeframe, thereby reducing the impact of automated or excessive access attempts. Fail2ban monitors log files for repeated failed login attempts or suspicious activity and blocks the offending IP addresses temporarily or permanently, helping to deter brute-force attacks. Load balancers distribute incoming network traffic across multiple servers to ensure no single server bears the full burden, which enhances performance and availability while providing resilience against traffic spikes typically seen during DoS attempts. Insider threats, such as misuse of access rights, will be addressed by maintaining detailed access logs and deploying behavior-based anomaly detection. To avoid accidental external exposure, strict firewall rules, subnet isolation, the absence of public DNS entries, and periodic vulnerability scans will be enforced.

In wireless environments, as demonstrated in analyses of the 802.11 Wired Equivalent Privacy (WEP) protocol, even seemingly encrypted transmissions can be vulnerable to interception and manipulation. Researchers found that weak key management and reuse of initialization vectors (IVs) allowed attackers to perform keystream reuse attacks and decrypt messages without needing to brute-force encryption keys. These keystream reuse attacks are possible because WEP uses a 24-bit IV field that can easily repeat, especially under high traffic conditions, allowing attackers to analyze multiple packets encrypted with the same keystream. If the attacker knows the plaintext of one message, they can XOR it with the ciphertext to recover the keystream and use it to decrypt other messages encrypted with the same IV. Furthermore, the WEP protocol uses a linear checksum for integrity, which can be manipulated to modify messages without detection. Attackers can even inject or replay packets by exploiting the fact that WEP access points do not enforce IV uniqueness. These flaws highlight the need for strong key handling and authentication methods, reinforcing why the proposed document server should avoid using legacy wireless authentication mechanisms and should isolate document access to VPN-authenticated sessions. Moreover, by enforcing proper session expiration and not relying on static shared keys, the system prevents repeated misuse and spoofing, problems that plagued earlier wireless standards.

Intrusion detection is another layer of defense that enhances survivability. As shown in wireless ad-hoc networks, where there is no fixed infrastructure and every node must serve as both host and router, traditional intrusion detection systems (IDS) fail due to the lack of centralized audit points. In such cases, anomaly detection and localized IDS agents that cooperatively detect threats based on statistical patterns were proven effective. Although the Stevens network is not ad-hoc, similar principles apply. The document server should log access activity and monitor usage patterns, flagging anomalies such as unusual access times or excessive document downloads. Incorporating a lightweight host-based IDS on the server and integrating alerts with the campus-wide SIEM (Security Information and Event Management) system would provide early warning and response capabilities. A SIEM aggregates and correlates security event data from sources like firewalls, IDS logs, and authentication servers in order to detect patterns indicative of malicious activity. Through real-time monitoring, automated alerting, and centralized visibility, it enables rapid response from security teams. For this document server, SIEM integration ensures that suspicious activity, such as unauthorized access attempts or irregular file behavior, can be identified and addressed quickly.

Authentication and access control are fundamental to network security, restricting access and privileges using secure identity verification systems. Encryption using HTTPS ensures confidentiality and protects against data manipulation. Ensuring system integrity through detection and proactive recovery measures addresses potential compromises. Hash functions are critical for document integrity and verification of content edits. The limitations of poorly designed encryption protocols like WEP reinforce the importance of robust cryptographic implementations. Finally, using a VPN tunnel ensures secure, encrypted remote access limited to authorized users within the Stevens Network.

The proposed document server leverages secure authentication, role-based controls, and document versioning to meet Stevens' internal collaboration needs. It limits access to the Stevens Network or its VPN, provides a clear workflow for change approval, and enforces robust protections against common security threats. Properly implemented, this system will support flexible, secure educational collaboration while upholding core principles of network and information security.

Citations

Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, ACM, 2001.

Hubaux, Jean-Pierre, Levente Buttyán, and Srdan Čapkun. "The Quest for Security in Mobile Ad Hoc Networks." Proceedings of the 1st ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2001), ACM, 2001.

Zhang, Yongguang, and Wenke Lee. "Intrusion Detection in Wireless Ad-Hoc Networks." Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000), ACM, 2000.