Threat Modeling Report

Created on 03/01/2025 22:00:54

Threat Model Name: University Web Portal

Owner: Sayed Helmy - Eyad Mazhar

Reviewer: DR Mohamed Seif

Contributors: Mahmoud Waleed - Amr Saber

Description: The system represents a secure IT infrastructure for an organization, focusing on internal and external operations. Key components include a Web Portal for external access, a Staff Portal for internal use, a Finance DB for critical financial data, and servers for backup, monitoring, and auditing purposes. Communication relies on encrypted data flows using HTTPS, IPsec, and TLS, ensuring secure interactions between users, portals, and databases. Firewalls, both internal and external, control access and protect the system. The system supports various users, including remote staff via VPN and internal staff using secure workstations.

Assumptions: The system assumes encrypted communication for all data flows and properly configured firewalls to block unauthorized traffic. User access is secured through multi-factor authentication (MFA), and endpoint devices like staff workstations have up-to-date protection. Access controls limit movement within the system, and automated updates ensure timely patching of vulnerabilities. Backup servers are assumed to be isolated for disaster recovery, and third-party services (e.g., payment gateways) follow secure practices. External users and remote staff access the system from secure environments.

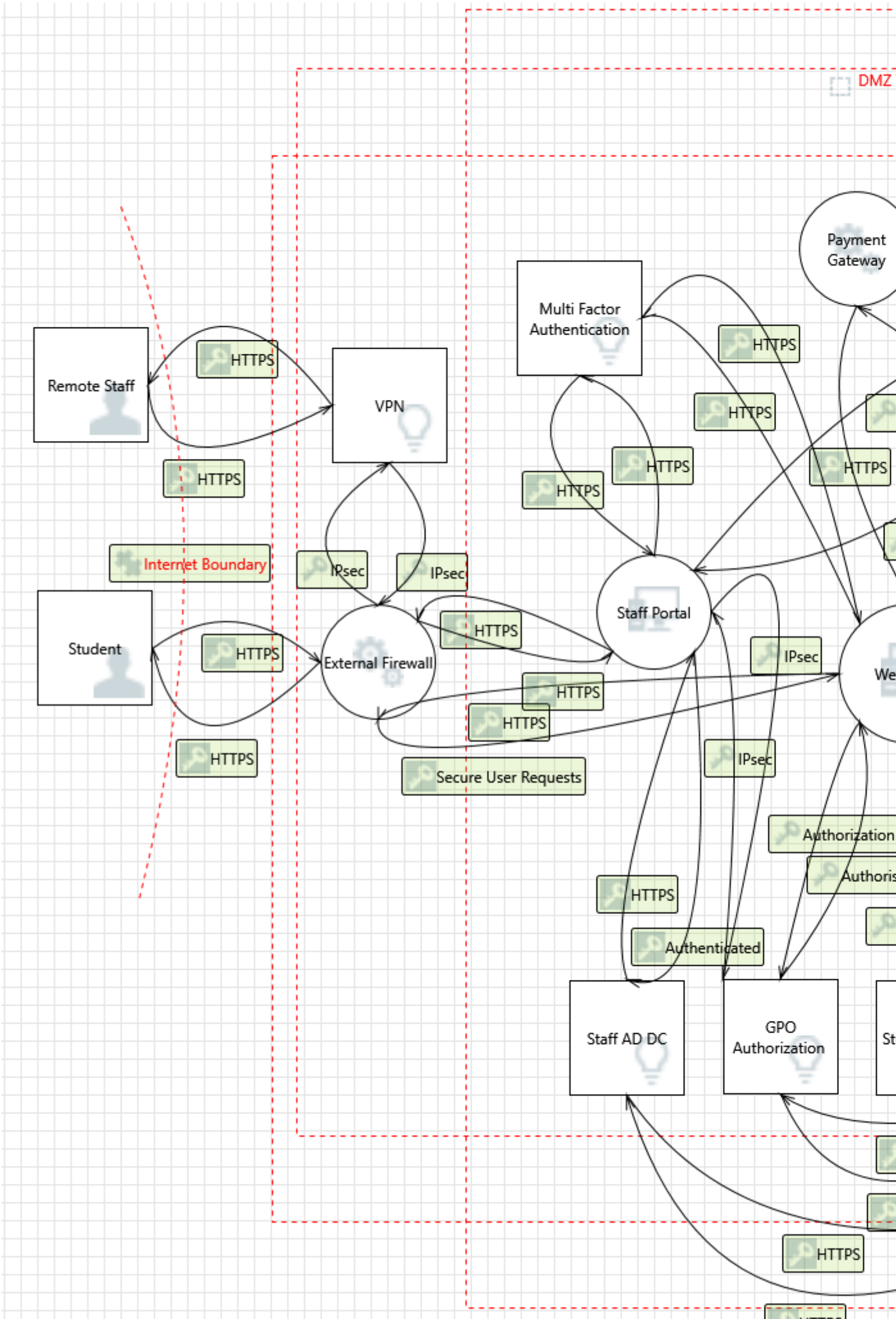
External Dependencies: The system depends on third-party services like payment gateways and potentially external storage for backups or logs. Network infrastructure, including VPNs and firewalls, must be robust and secure. It also relies on industry standards (e.g., HTTPS, IPsec) for encryption. External environments, such as those used by remote staff, must be secure to avoid threats. Additionally, the system incorporates third-party software and libraries, requiring regular updates to address vulnerabilities.

Threat Model Summary:

Not Started	22

Not Applicable	0
Needs Investigation	0
Mitigation Implemented	171
Total	193
Total Migrated	0

Diagram: University portal


DMZ
Payment Gateway
Multi Factor Authentication
Remote Staff
HTTPS
VPN
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
Internet Boundary
IPsec
IPsec
Staff Portal
Student
HTTPS
External Firewall
HTTPS
IPsec
HTTPS
HTTPS
HTTPS
IPsec
Secure User Requests
Authorization
HTTPS
Authenticated
Staff AD DC
GPO Authorization
HTTPS

University portal Diagram Summary:

Not Started	22
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	171
Total	193
Total Migrated	0

Threat(s) Not Associated With an Interaction:

1. Elevation by Changing the Execution Flow in Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Staff Portal in order to change the flow of program execution within Staff Portal to the attacker's choosing.

Justification: Use control flow integrity (CFI) to ensure execution remains within predefined paths. Validate and sanitize all user inputs to prevent code injection attacks.

2. Staff Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Workstations may be able to remotely execute code for Staff Portal.

Justification: Secure the portal by applying patches and updates to eliminate vulnerabilities. Utilize sandboxing to isolate untrusted code execution and prevent privilege escalation.

3. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Utilize distributed storage systems to ensure high availability. Implement robust monitoring systems to identify and resolve access issues promptly.

4. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Apply content delivery networks (CDNs) and alternate network paths to mitigate interruptions. Use firewalls and IPS to monitor and prevent attacks aimed at disrupting HTTPS traffic.

5. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Apply redundancy measures, such as clustering or mirroring, for critical data stores. Ensure backups are available and conduct regular restoration tests to verify data recovery capabilities.

6. Data Flow Automated OS and Security Updates Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Implement automatic retry mechanisms and failover systems to maintain update availability. Use monitoring systems to detect and block malicious attempts to disrupt data flows.

7. Data Store Denies Staff Workstations Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff Workstations claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Enable detailed logging of all write operations to capture data provenance, timestamps, and transaction metadata. Use role-based access control (RBAC) to enforce write permissions, ensuring only authorized sources can perform data operations.

8. The Staff Workstations Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Automated OS and Security Updates may be tampered with by an attacker. This may lead to corruption of Staff Workstations. Ensure the integrity of the data flow to the data store.

Justification: Employ cryptographic integrity checks, such as hashing (e.g., SHA-256), to validate data integrity. Use secure communication protocols for Automated OS and Security Updates, such as TLS, to prevent tampering during data transmission.

9. Spoofing of Destination Data Store Staff Workstations [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Staff Workstations may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Staff Workstations. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Deploy mutual TLS authentication or certificate-based identification for communication with Staff Workstations. Implement logging mechanisms to record the origin of data writes and validate the identity of the destination before processing. Use unique identifiers to ensure data integrity and prevent redirection to unauthorized targets.

10. Potential Process Crash or Stop for Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Staff Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Deploy auto-scaling solutions and resource monitoring to manage high-load scenarios. Conduct regular stress testing to identify vulnerabilities and implement recovery strategies like failover systems.

11. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Staff Workstations can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Enforce strict input sanitization and apply a CSP to block unauthorized script execution. Monitor web traffic for anomalous patterns indicative of XSS attacks.

12. Potential Data Repudiation by Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Implement logging and auditing mechanisms to document all received data with timestamps. Use cryptographic signatures to validate and ensure non-repudiation.

13. Persistent Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: The web server 'Staff Portal' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'Staff Workstations' inputs and output.

Justification: Apply RBAC and enforce least privilege principles on Staff Workstations. Encrypt sensitive data and ensure regular reviews of access permissions.

14. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: The web server 'Staff Portal' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Implement input sanitization at all entry points and apply database-level constraints to prevent the storage of malicious scripts. Use a CSP to restrict script execution.

15. Spoofing of Source Data Store Staff Workstations [State: Mitigation Implemented] [Priority: High]

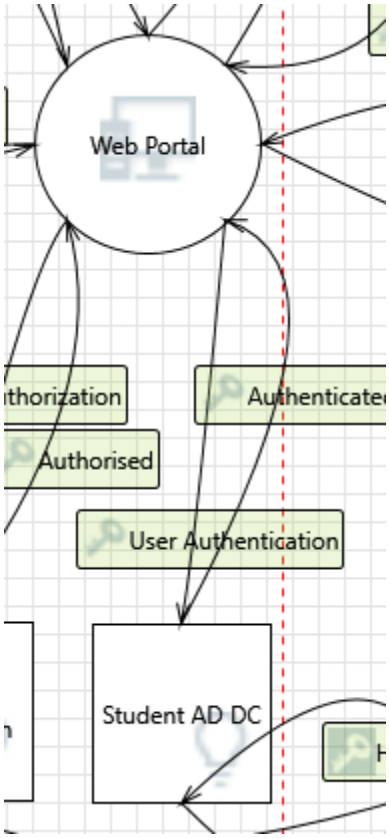
Category: Spoofing

Description: Staff Workstations may be spoofed by an attacker and this may lead to incorrect data delivered to Staff Portal. Consider using a standard authentication mechanism to identify the source data store.

Justification: Risk Explanation: Attackers may spoof staff workstations to manipulate or introduce incorrect data into the Staff Portal. This compromises the integrity and reliability of the data. Precedent: Spoofing attacks are common in environments without robust authentication mechanisms. Likelihood: High, as spoofing is relatively straightforward if authentication mechanisms are

weak. Impact: Severe, potentially leading to operational disruption and loss of

Interaction: Authenticated



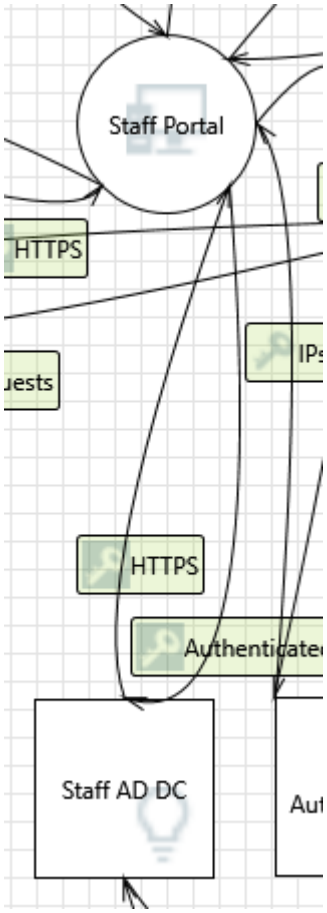
16. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of Student AD DC in order to gain additional privilege.

Justification: This threat exploits potential weaknesses in the authentication or authorization process, allowing an attacker to impersonate the Student AD DC. Such impersonation can grant unauthorized access to restricted resources or elevate privileges. Implementing robust role-based access control (RBAC), enforcing strict identity verification mechanisms like MFA, and auditing privilege escalation attempts are necessary to mitigate this risk. Logs and monitoring tools should also be employed to detect and prevent unauthorized impersonation attempts.

Interaction: Authenticated



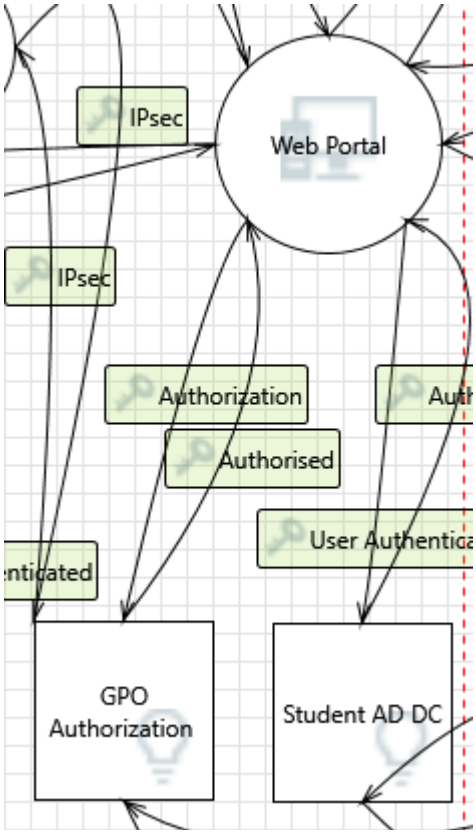
17. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Mitigate vulnerabilities by enforcing PKCE (Proof Key for Code Exchange) in OAuth implementations. Use short-lived tokens and secure transmission channels like HTTPS.

Interaction: Authorised



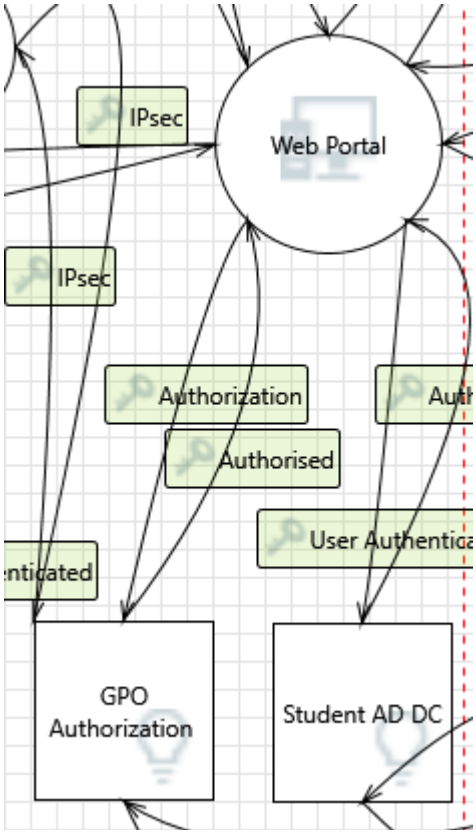
18. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of GPO Authorization in order to gain additional privilege.

Justification: Deploy role-based access control (RBAC) to ensure web portals cannot access unauthorized components like GPO Authorization. Leverage audit trails to detect impersonation attempts and investigate anomalies.

Interaction: Authorization



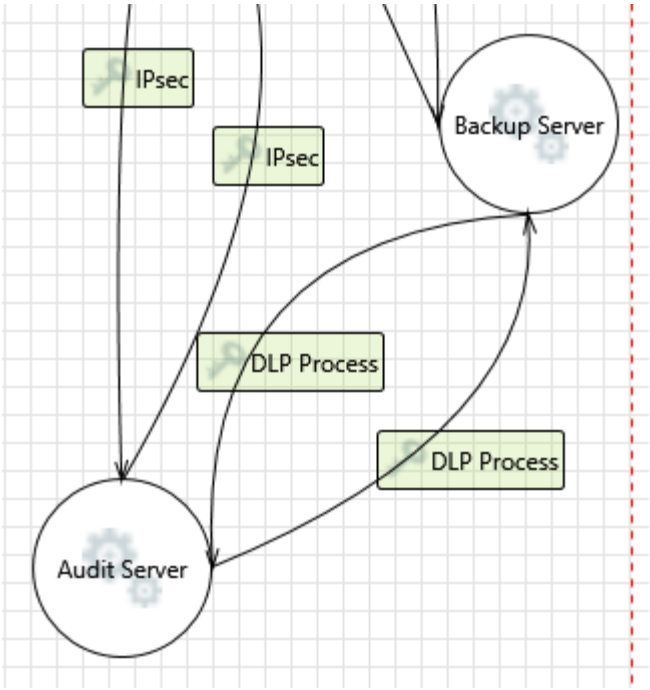
19. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Mitigate vulnerabilities in SSO systems by enforcing HTTPS for all communication, implementing PKCE (Proof Key for Code Exchange) for OAuth, and securing tokens with short lifetimes. Regularly patch and monitor SSO systems for emerging exploits.

Interaction: DLP Process



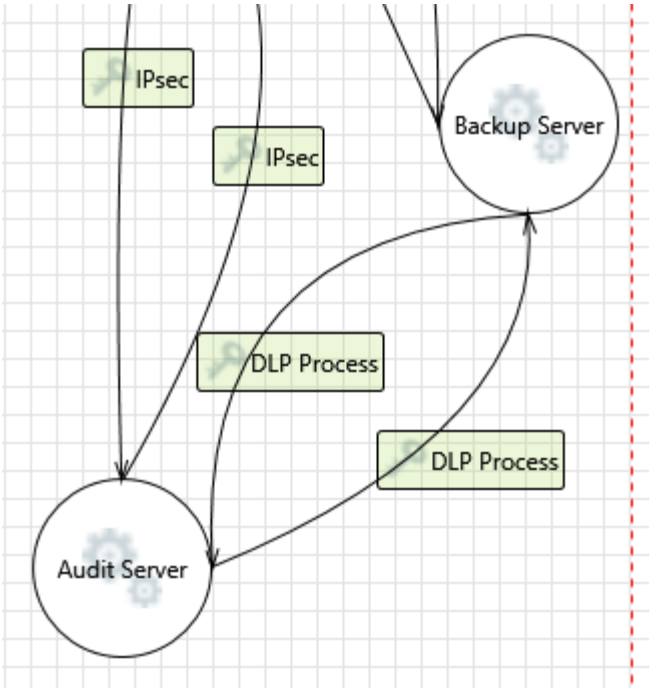
20. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Audit Server may be able to impersonate the context of Backup Server in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: DLP Process



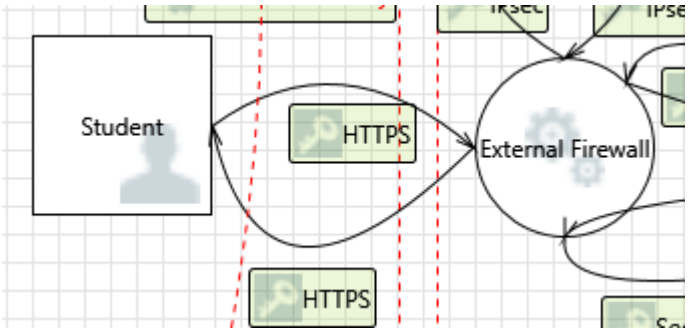
21. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Backup Server may be able to impersonate the context of Audit Server in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: HTTPS



22. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: External agents could disrupt HTTPS traffic, causing interruptions and potential data loss. Precedent: DoS and MitM attacks frequently target HTTPS communications. Likelihood: High, especially in systems exposed to public networks. Impact: Severe, affecting service reliability and user trust

23. External Entity User Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: The external entity might deny receiving data, leading to repudiation issues. Precedent: Repudiation threats are prevalent where logging mechanisms are insufficient. Likelihood: Medium, especially without robust non-repudiation measures. Impact: Moderate to severe, depending on the importance of the data.

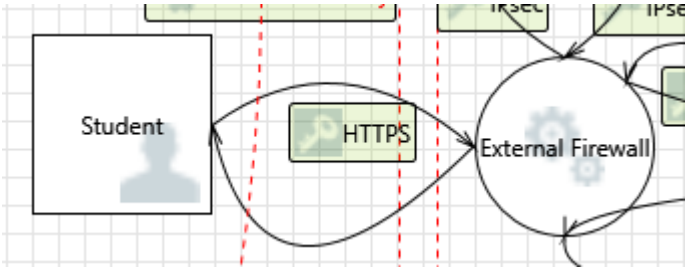
24. Spoofing of the User External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of User. Consider using a standard authentication mechanism to identify the external entity.

Justification: Risk Explanation: Attackers could spoof the destination entity, causing data to be sent to malicious targets. Precedent: Spoofing attacks are common in systems without robust entity validation. Likelihood: High, given the simplicity of such attacks. Impact: Severe, potentially leading to data leakage or manipulation.

Interaction: HTTPS



25. Elevation by Changing the Execution Flow in Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into External Firewall in order to change the flow of program execution within External Firewall to the attacker's choosing.

Justification: Risk Explanation: Attackers may inject data to alter the firewall's execution flow, enabling privilege escalation. Precedent: Execution flow manipulation is a known attack vector in poorly secured systems. Likelihood: Medium to high, depending on the system's safeguards. Impact: High, as it could compromise the entire firewall.

26. Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: User may be able to remotely execute code for External Firewall.

Justification: Risk Explanation: Attackers could exploit implementation bugs to execute unauthorized code on the external firewall. Precedent: Remote Code Execution (RCE) is a common method for compromising systems. Likelihood: High if the system lacks regular updates and monitoring. Impact: Severe, as it could lead to complete control over the firewall.

27. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to impersonate the context of User in order to gain additional privilege.

Justification: Risk Explanation: The external firewall could impersonate user contexts, allowing unauthorized privilege escalation. Precedent: Privilege escalation attacks are prevalent in systems with weak identity verification. Likelihood: High, particularly if there are exploitable vulnerabilities or weak authentication mechanisms. Impact: Severe, as unauthorized access could lead to data manipulation or theft

28. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: The firewall could crash or stop functioning due to resource exhaustion or targeted attacks, leading to a Denial of Service (DoS). Precedent: DoS attacks targeting firewalls are well-documented in cybersecurity. Likelihood: Medium to high, depending on the robustness of the firewall and existing safeguards. Impact: High, as it directly affects network availability

29. Potential Process Crash or Stop for Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: External Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Risk Explanation: The firewall could crash or stop functioning due to resource exhaustion or targeted attacks, leading to a Denial of Service (DoS). Precedent: DoS attacks targeting firewalls are well-documented in cybersecurity. Likelihood: Medium to high, depending on the robustness of the firewall and existing safeguards. Impact: High, as it directly affects network availability

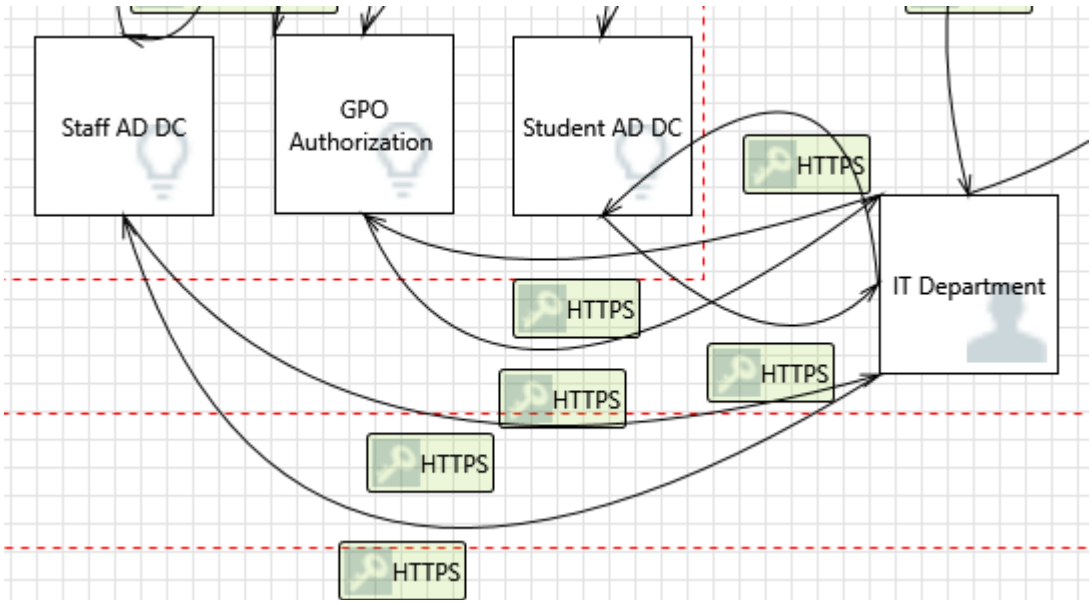
30. Potential Data Repudiation by Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: External Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: This threat can lead to a lack of accountability and create gaps in incident response processes. By implementing logging and auditing mechanisms, the source, time, and nature of data received can be recorded. This ensures that every transaction is traceable, verifiable, and auditable, reducing the risk of data repudiation.

Interaction: HTTPS



31. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Harden SSO systems with secure configurations, including encrypted token storage, regular token invalidation, and server-side validations for tokens. Employ HSTS (HTTP Strict Transport Security) to ensure only secure HTTPS communications.

32. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Use DoS prevention techniques, such as load balancing and rate-limiting, to mitigate interruptions in HTTPS flows. Implement redundancy in network paths to ensure service availability during attacks.

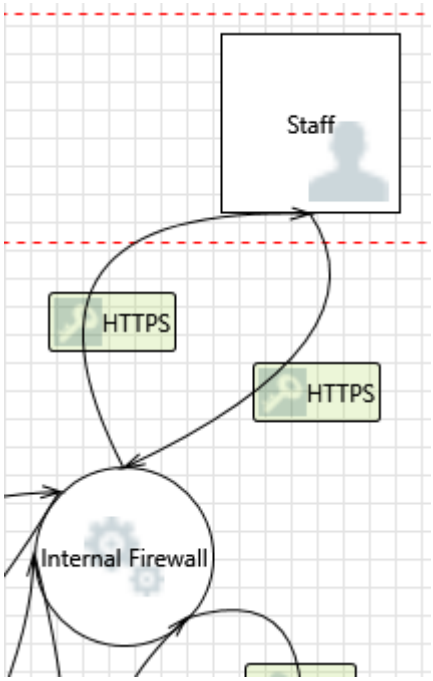
33. External Entity Staff AD DC Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff AD DC claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Record all data exchanges with Staff AD DC through detailed logs, including timestamps and source identifiers. Cryptographic methods like HMAC can authenticate and validate data transmissions.

Interaction: HTTPS



34. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Introduce redundancy in the network infrastructure and enable load balancing. Use intrusion prevention systems (IPS) to identify and mitigate external agents attempting to disrupt data flow.

35. External Entity Staff Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Implement logging and auditing mechanisms to track all data exchanges. Use cryptographic techniques, such as HMACs or digital signatures, to verify data delivery and prevent repudiation claims.

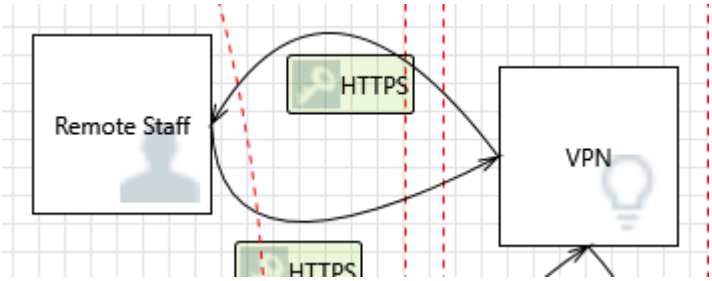
36. Spoofing of the Staff External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Staff may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Staff. Consider using a standard authentication mechanism to identify the external entity.

Justification: Deploy mutual TLS authentication to verify the identity of Staff before any data exchange. Use signed messages or digital certificates to ensure the authenticity of the external destination entity and prevent spoofing attacks.

Interaction: HTTPS



37. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: External agents could disrupt HTTPS traffic across trust boundaries, leading to service interruptions. Precedent: Similar interruptions have been observed in MitM and network-level DoS attacks. Likelihood: High, particularly in public-facing systems. Impact: Severe, as interruptions can impact service reliability and user trust.

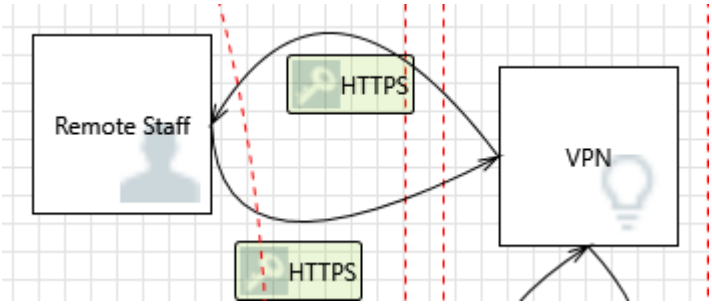
38. External Entity External Staff Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Remote Staff claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: External staff could deny receiving data from trusted sources, leading to repudiation issues. Precedent: Repudiation threats are common in distributed systems with insufficient auditing. Likelihood: Medium, especially without non-repudiation measures. Impact: Moderate to severe, depending on the criticality of the denied data.

Interaction: HTTPS



39. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Risk Explanation: Vulnerabilities in SSO implementations may allow attackers to exploit session tokens or credentials. Precedent: Numerous breaches have leveraged SSO weaknesses to escalate privileges. Likelihood: High, given SSO's widespread use and complex implementation. Impact: Severe, as it compromises the entire authentication mechanism.

40. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: External agents could interrupt HTTPS traffic, leading to a Denial of Service (DoS). Precedent: DoS attacks targeting encrypted traffic are well-documented. Likelihood: High, given the high value of secure traffic. Impact: Severe, affecting service availability and data transmission reliability

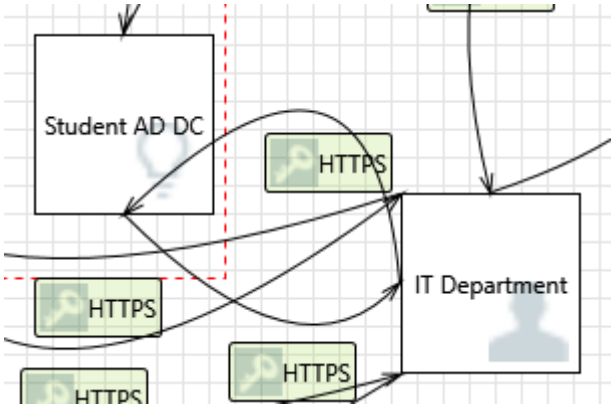
41. External Entity VPN Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: VPN claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: The VPN may deny receiving data from processes, creating a repudiation scenario. Precedent: Repudiation threats are common where logging and auditing are insufficient. Likelihood: Medium to high, depending on the quality of the logging mechanisms. Impact: Moderate to severe, as data flow issues can disrupt operations

Interaction: HTTPS



42. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Exploiting weaknesses in SSO systems can enable attackers to bypass authentication and gain unauthorized access. To counter this, use secure practices such as enabling multi-factor authentication (MFA), employing token encryption, and adhering to up-to-date standards for SSO protocols.

43. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Repeated interruption of HTTPS data flow can lead to significant downtime and disrupt critical processes. Solutions such as implementing a robust failover strategy, securing communication channels, and continuously monitoring network health are crucial to maintaining uninterrupted service.

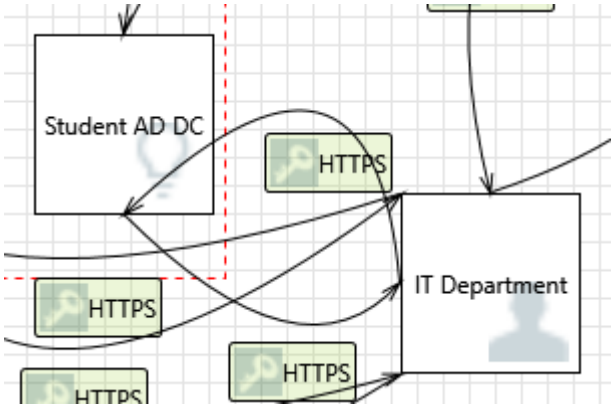
44. External Entity Student AD DC Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Student AD DC claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Student AD DC's denial of data receipt can undermine trust and operational continuity. Detailed logging of transactions, including timestamps, source details, and data summaries, ensures accountability and supports post-incident investigations.

Interaction: HTTPS



45. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Interruption in HTTPS data flow compromises the availability of services and potentially exposes sensitive information to exploitation. Mitigating measures

include robust traffic monitoring, secure transport protocols, redundancy, and anomaly detection mechanisms to maintain service integrity.

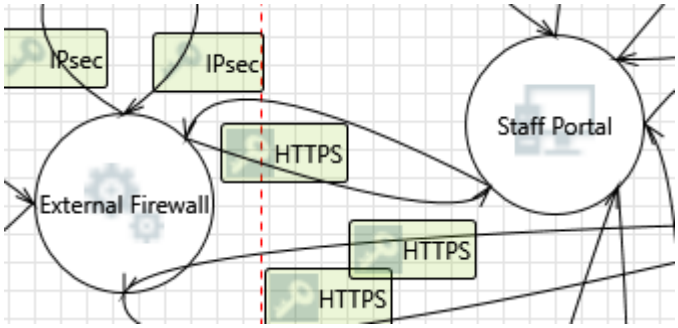
46. External Entity IT Manager Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: IT Department claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The denial of receiving data by the IT Manager entity raises concerns about accountability and trust. Implementing comprehensive logging and audit trails ensures the traceability of all data exchanges, supporting verification and non-repudiation in disputes.

Interaction: HTTPS



47. Elevation by Changing the Execution Flow in External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into External Firewall in order to change the flow of program execution within External Firewall to the attacker's choosing.

Justification: Use security mechanisms like ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) to protect against execution flow alteration. Validate all data inputs and outputs.

48. External Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to remotely execute code for External Firewall.

Justification: Regularly patch the External Firewall to address vulnerabilities. Apply input validation and secure configurations to reduce the risk of exploitation.

49. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to impersonate the context of Staff Portal in order to gain additional privilege.

Justification: Implement RBAC and enforce strong authentication protocols between the External Firewall and connected systems to prevent impersonation attempts.

50. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Use content delivery networks (CDNs) and geographically distributed servers to ensure uninterrupted data flow. Apply denial-of-service (DoS) protection solutions to detect and mitigate attacks.

51. Potential Process Crash or Stop for External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: External Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Deploy failover mechanisms and redundant firewalls to maintain service availability. Monitor resource usage and apply patches to address known vulnerabilities.

52. Potential Data Repudiation by External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: External Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Implement logging and auditing mechanisms to capture all interactions with the External Firewall. Use cryptographic signatures to verify data integrity and non-repudiation.

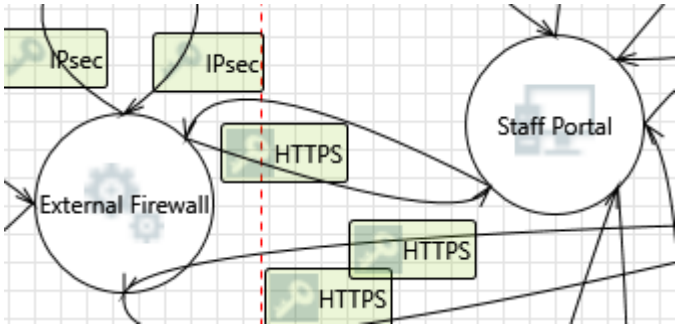
53. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: HTTPS



54. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web

site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: Implement CSRF tokens for all state-changing requests. Secure cookies with HttpOnly and SameSite attributes to limit exposure to CSRF attacks.

55. Elevation by Changing the Execution Flow in Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Staff Portal in order to change the flow of program execution within Staff Portal to the attacker's choosing.

Justification: Use control flow integrity (CFI) mechanisms to ensure program execution adheres to intended paths. Validate and sanitize all user inputs to prevent injection of malicious data that could alter execution flow.

56. Staff Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to remotely execute code for Staff Portal.

Justification: Harden the Staff Portal by applying secure coding practices, such as input validation and sanitization. Regularly patch software and apply runtime application self-protection (RASP) mechanisms to prevent exploitation of vulnerabilities.

57. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to impersonate the context of External Firewall in order to gain additional privilege.

Justification: Enforce mutual TLS authentication between the Staff Portal and External Firewall to prevent impersonation. Use role-based access control (RBAC) to restrict privilege escalation attempts.

58. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Deploy load balancers and redundant network paths to ensure high availability of data flow. Use intrusion prevention systems (IPS) to detect and block malicious attempts to disrupt HTTPS traffic.

59. Potential Process Crash or Stop for Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Staff Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Implement rate-limiting, request throttling, and timeout mechanisms to manage high traffic or resource-intensive requests. Use server monitoring tools to detect resource spikes and mitigate risks through auto-scaling or service restarts.

60. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Strengthen authentication through MFA and secure password hashing techniques. Review and patch custom authentication mechanisms regularly to address newly discovered vulnerabilities.

61. Potential Data Repudiation by Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Introduce logging and monitoring solutions within Staff Portal to track data interactions. Use signed acknowledgments for received data, ensuring non-repudiation and accountability.

62. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Enable replay attack prevention through unique session identifiers and time-based tokens within HTTPS communications. Regularly audit communication protocols for adherence to secure implementation standards.

63. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: The web server 'Staff Portal' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Sanitize all user inputs on the Staff Portal to prevent XSS vulnerabilities. Implement a content security policy (CSP) to restrict the execution of unauthorized scripts and validate all incoming data.

64. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Leverage cryptographic protocols with collision-resistant properties to protect against message alteration or injection. Validate and verify packet order and integrity before processing.

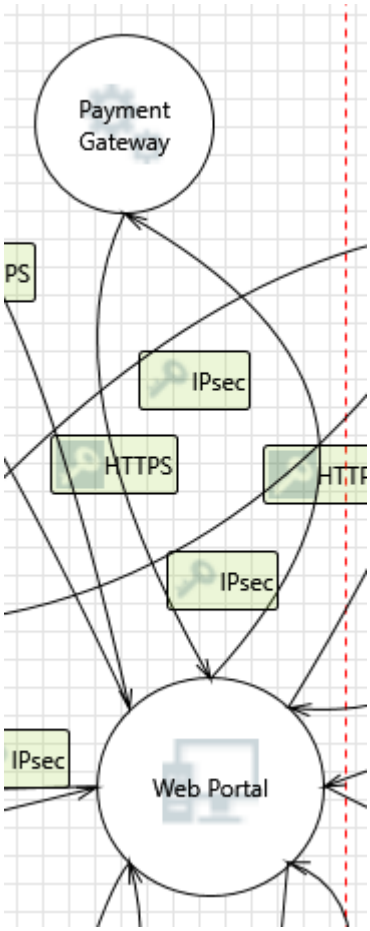
65. Spoofing the External Firewall Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: External Firewall may be spoofed by an attacker and this may lead to unauthorized access to Staff Portal. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

Interaction: HTTPS



66. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Payment Gateway may be able to impersonate the context of Web Portal in order to gain additional privilege.

Justification: Risk Explanation: The payment gateway may impersonate the web portal to alter user interactions or data flows. Precedent: Impersonation threats in interconnected financial systems are well-documented. Likelihood: Medium, given the complexity of these systems. Impact: Severe, as it could lead to data breaches or unauthorized transactions.

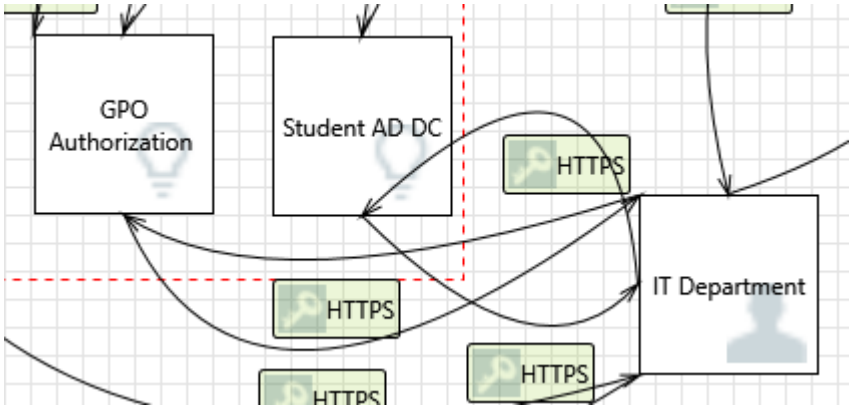
67. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: HTTPS



68. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Vulnerabilities in SSO implementations like OAUTH2 and OAUTH Wrap expose systems to Man-in-the-Middle (MitM) attacks. These attacks allow an adversary to intercept or alter communications, leading to unauthorized privilege escalation. To prevent this, use robust encryption (TLS), implement additional verification measures (e.g., PKCE), and continuously assess and update authorization protocols.

69. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: An external agent disrupting HTTPS data flow can severely compromise the system's availability and reliability, creating a Denial of Service (DoS) condition. To mitigate this threat, employ end-to-end encryption, redundancy in data paths, and intrusion detection systems to identify and address potential interruptions promptly.

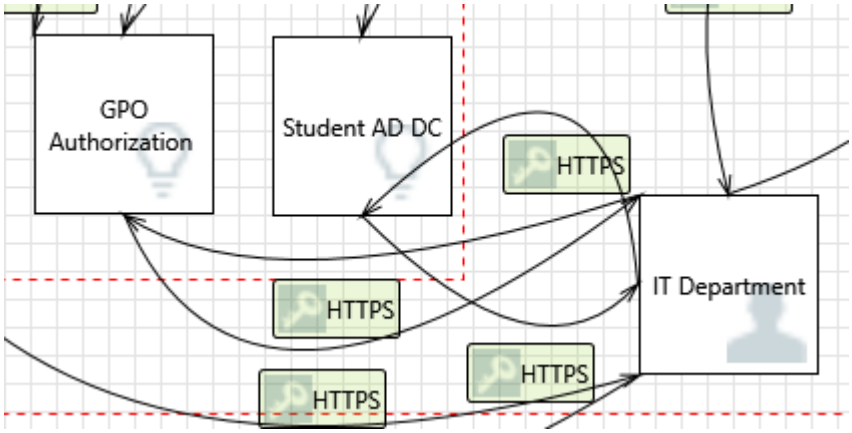
70. External Entity GPO Authorization Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: GPO Authorization claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Repudiation by the GPO Authorization component creates a significant accountability gap, potentially leading to miscommunication and unauthorized access or denial of service. Implementing logging and auditing mechanisms ensures that every interaction with the GPO Authorization is recorded, including the source, time, and type of data transmitted. These records provide evidence to validate data exchanges and aid forensic investigations in the event of disputes or incidents. Additionally, using a secure communication protocol such as HTTPS ensures data integrity and mitigates the risk of tampering during transmission.

Interaction: HTTPS



71. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Interruptions in HTTPS data flow disrupt service and expose vulnerabilities. Redundant pathways, encryption, and monitoring help to maintain uninterrupted and secure data flow.

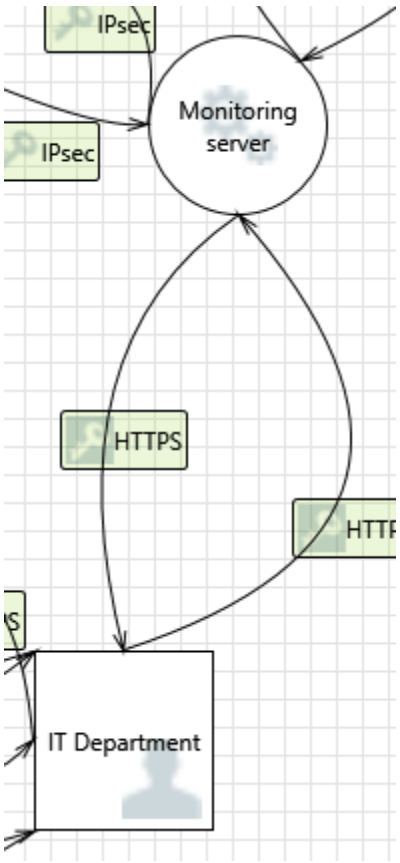
72. External Entity IT Manager Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: IT Department claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Claims of not receiving data from the IT Manager could affect accountability. Implementing detailed logging and audit trails ensures all interactions are verifiable, supporting non-repudiation.

Interaction: HTTPS



73. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Monitoring server may be able to impersonate the context of IT Department in order to gain additional privilege.

Justification: If the Monitoring Server impersonates the IT Department, it could gain unauthorized privileges. Mitigations include role-based access control and continuous monitoring to detect impersonation attempts.

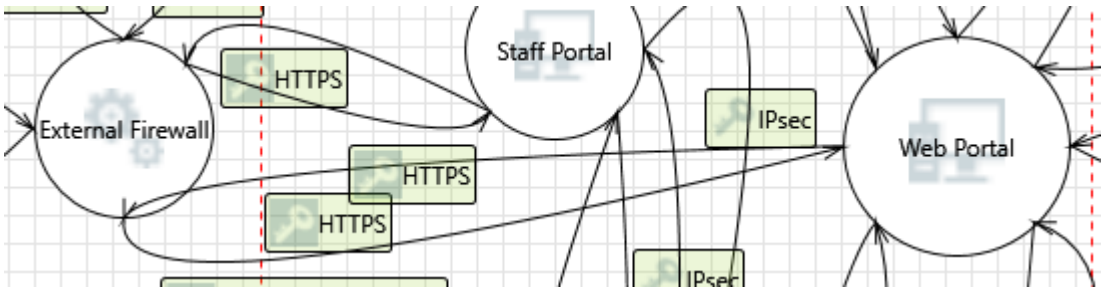
74. Spoofing the IT Manager External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: IT Department may be spoofed by an attacker and this may lead to unauthorized access to Monitoring server. Consider using a standard authentication mechanism to identify the external entity.

Justification: If an attacker spoofs the IT Manager entity, they could gain unauthorized access to critical systems. Utilizing authentication mechanisms, such as certificates or tokens, ensures the entity's identity and protects against spoofing.

Interaction: HTTPS



75. Elevation by Changing the Execution Flow in External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into External Firewall in order to change the flow of program execution within External Firewall to the attacker's choosing.

Justification: An attacker manipulating the execution flow within the External Firewall compromises its functionality and security. Adopting secure coding practices and runtime protections can minimize these risks.

76. External Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to remotely execute code for External Firewall.

Justification: The Web Portal potentially executing code on the External Firewall could lead to privilege escalation and system compromise. Employing secure

coding, monitoring for abnormal behavior, and implementing strict boundary controls can mitigate this threat.

77. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Interruption of HTTPS data flow affects both availability and security. Utilizing redundancy, robust encryption protocols, and real-time monitoring ensures data flows without unauthorized interruptions.

78. Potential Process Crash or Stop for External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: External Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: A crash or halt in the External Firewall could interrupt critical security functions, creating a DoS scenario. This underscores the need for fault-tolerant design, monitoring, and timely updates to prevent such occurrences.

79. Potential Data Repudiation by External Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: External Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The External Firewall's denial of receiving data undermines accountability and system reliability. Logging and auditing the data source, time, and context ensures traceability and prevents repudiation claims.

80. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to impersonate the context of Web Portal in order to gain additional privilege.

Justification: Risk Explanation: The external firewall could impersonate the web portal, allowing attackers to access sensitive information or manipulate traffic. Precedent: Firewall misconfigurations have historically been exploited for impersonation. Likelihood: High, particularly in environments with weak configurations. Impact: Severe, with potential for wide-reaching operational disruption.

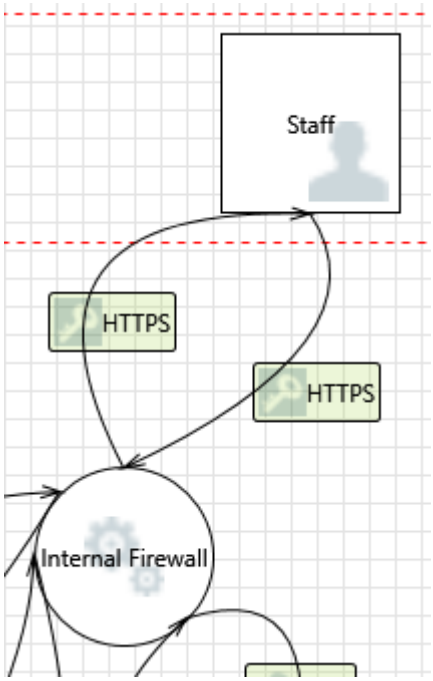
81. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: HTTPS



82. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to impersonate the context of Staff in order to gain additional privilege.

Justification: The risk arises from the Internal Firewall potentially exploiting a flaw to impersonate Staff context. This would allow unauthorized elevation of privilege, which could compromise sensitive systems or data. To mitigate this, strict authentication and authorization checks should be applied to prevent context spoofing and ensure role integrity.

83. Elevation by Changing the Execution Flow in Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Internal Firewall in order to change the flow of program execution within Internal Firewall to the attacker's choosing.

Justification: Protect against execution flow alterations using techniques like CFI and DEP (Data Execution Prevention). Apply strict validation checks on all inputs and log unusual activities for rapid response.

84. Internal Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff may be able to remotely execute code for Internal Firewall.

Justification: Implement endpoint security measures to prevent unauthorized execution of remote code. Use strict whitelisting for allowable processes and connections.

85. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Apply content delivery networks (CDNs) and redundant paths to ensure resilience against interruptions. Use secure communication protocols like HTTPS with robust error handling to maintain data integrity.

86. Potential Process Crash or Stop for Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Internal Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Deploy redundancy systems and use predictive monitoring tools to preemptively address potential crashes. Regularly test the firewall under stress conditions to optimize stability.

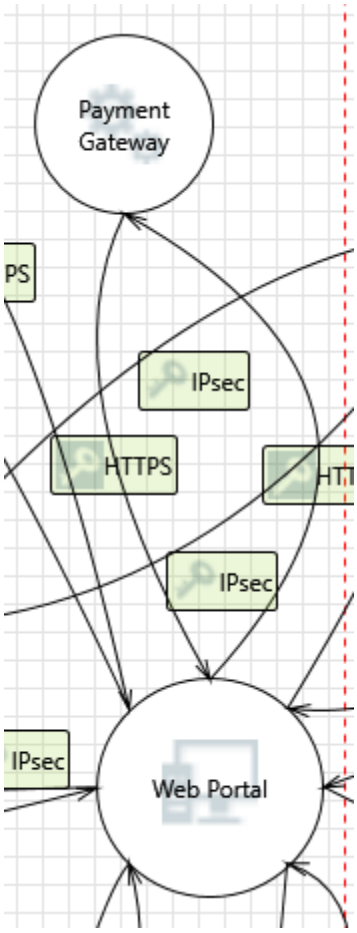
87. Potential Data Repudiation by Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Internal Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Implement logging and auditing of all interactions with the Internal Firewall. Use signed acknowledgments to confirm receipt of data and prevent denial claims.

Interaction: HTTPS



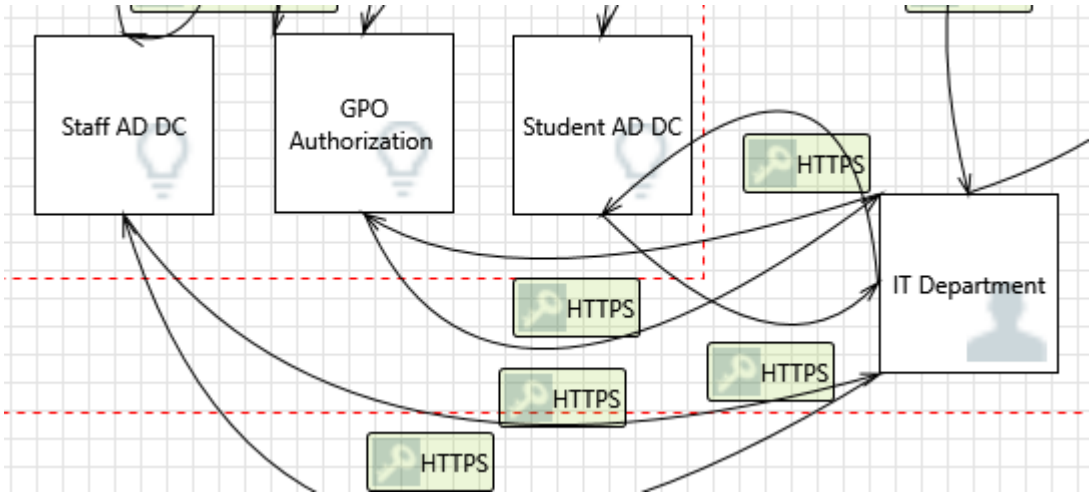
88. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of Payment Gateway in order to gain additional privilege.

Justification: Risk Explanation: The web portal could impersonate the payment gateway, enabling unauthorized financial transactions. Precedent: Impersonation of financial systems is a common attack method in online payment environments. Likelihood: High due to the high value associated with such systems. Impact: Severe, as it can lead to financial loss and erosion of user trust.

Interaction: HTTPS



89. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Deploy denial-of-service (DoS) protection tools such as firewalls with rate-limiting features. Configure intrusion detection and prevention systems (IDPS) to monitor for and block suspicious traffic.

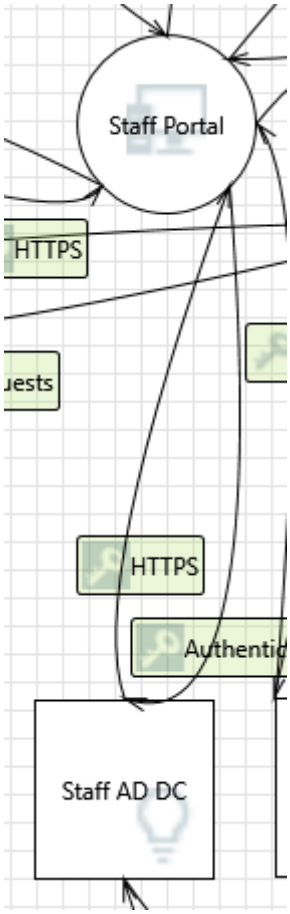
90. External Entity IT Manager Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: IT Department claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Enable logging and auditing mechanisms on IT Manager's systems to track data received and processed. Use cryptographic signatures to validate the authenticity of transmitted data and verify its origin.

Interaction: HTTPS



91. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to impersonate the context of Staff AD DC in order to gain additional privilege.

Justification: Use secure authentication and logging mechanisms to monitor for unauthorized attempts to impersonate the Staff AD DC from the Staff Portal.

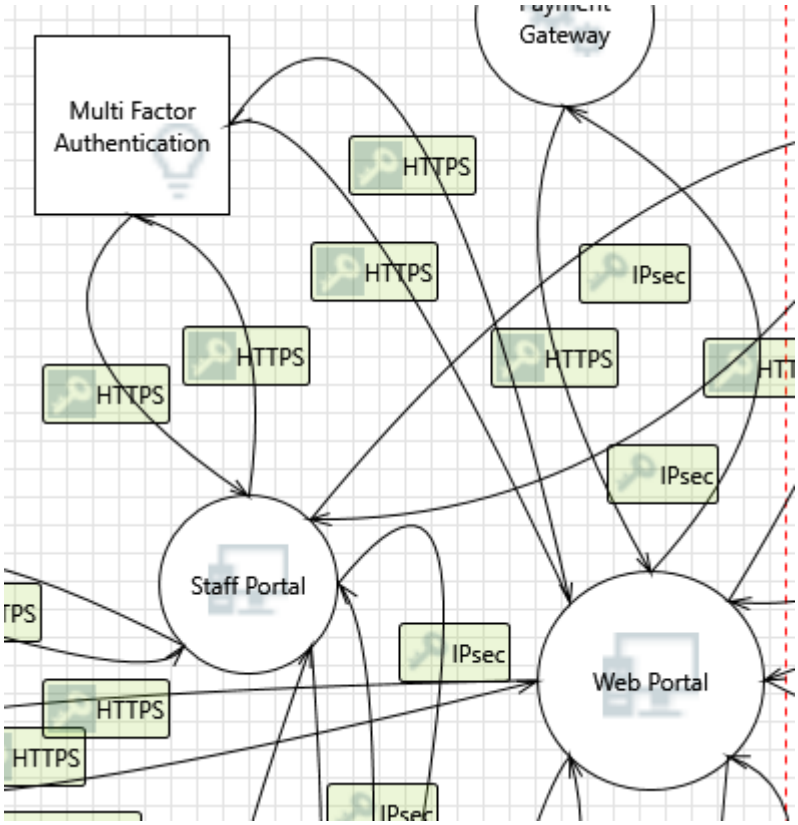
92. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: The web server 'Staff Portal' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Sanitize all user inputs and outputs to prevent XSS attacks. Apply a Content Security Policy (CSP) to restrict script execution on the Staff Portal.

Interaction: HTTPS



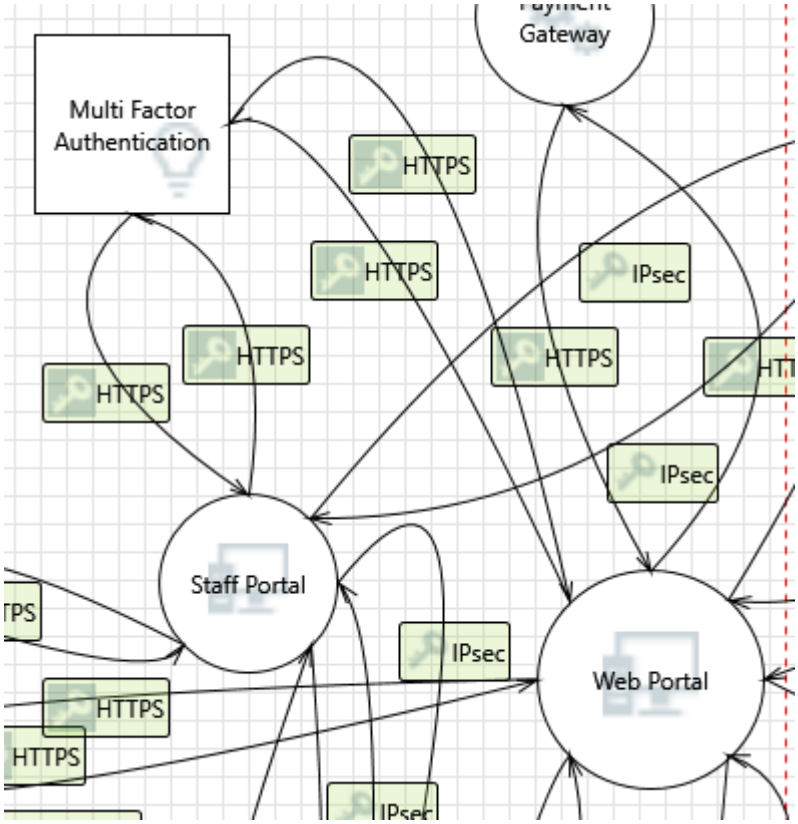
93. Weakness in SSO Authorization [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: <no mitigation provided>

Interaction: HTTPS



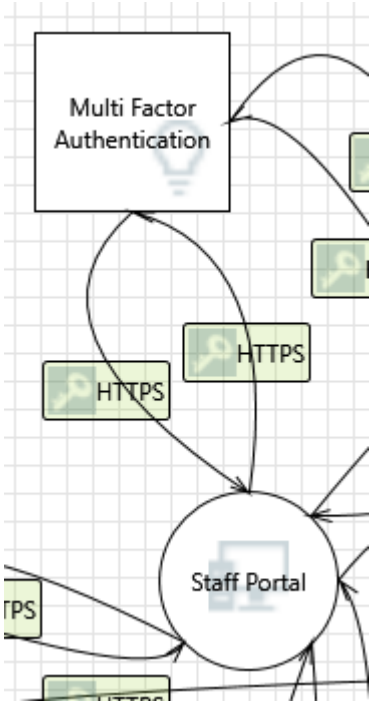
94. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of Multi Factor Authentication in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: HTTPS



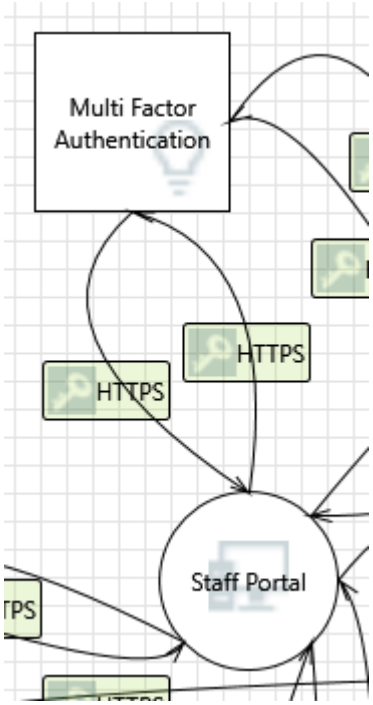
95. Weakness in SSO Authorization [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: <no mitigation provided>

Interaction: HTTPS



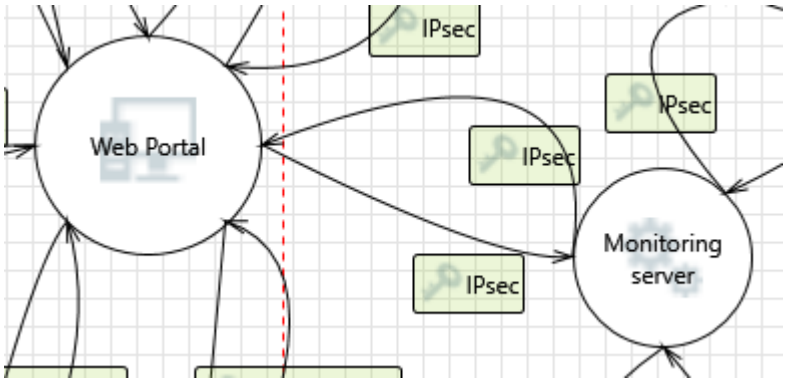
96. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to impersonate the context of Multi Factor Authentication in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: IPsec



97. Elevation by Changing the Execution Flow in Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Web Portal in order to change the flow of program execution within Web Portal to the attacker's choosing.

Justification: Risk Explanation: An attacker may inject data to alter the Web Portal's execution flow, enabling unauthorized actions. Precedent: Execution flow manipulation is a known vulnerability in systems without robust input validation. Likelihood: Medium to high, depending on input validation and system configuration. Impact: Severe, potentially compromising system functionality and security.

98. Web Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Monitoring server may be able to remotely execute code for Web Portal.

Justification: Risk Explanation: Remote code execution (RCE) vulnerabilities may allow attackers to execute arbitrary code with elevated privileges. Precedent: RCE attacks have been exploited to compromise systems entirely. Likelihood: High, especially in systems without timely security patches. Impact: Severe, risking full system compromise and data breaches.

99. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of Monitoring server in order to gain additional privilege.

Justification: Risk Explanation: The Web Portal may impersonate the context of the Monitoring Server, gaining unauthorized privileges. Precedent: Impersonation attacks are common where identity verification is insufficient. Likelihood: High, given the interconnected nature of the systems. Impact: Severe, allowing unauthorized actions with elevated privileges.

100. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: An external agent may disrupt IPsec traffic, causing service availability issues. Precedent: Disruptions in secure communication channels can lead to denial-of-service attacks. Likelihood: Medium, depending on network configurations and exposure. Impact: High, risking service interruptions and operational delays.

101. Potential Process Crash or Stop for Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Web Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Risk Explanation: Resource exhaustion or targeted attacks may cause the Web Portal to crash or stop functioning. Precedent: Similar incidents have been observed where systems lacked resilience mechanisms. Likelihood: High, especially under high loads or targeted DoS attacks. Impact: Severe, affecting availability and user experience.

102. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Risk Explanation: Weak authentication schemes, such as using guessable or null credentials, can enable unauthorized access. Precedent: Many breaches have occurred due to inadequate authentication mechanisms. Likelihood: High, especially in systems relying on custom or outdated authentication protocols. Impact: Severe, risking unauthorized data access and system compromise.

103. Potential Data Repudiation by Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Web Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: The Web Portal could deny receiving data from a source, creating a repudiation scenario. Precedent: Repudiation issues are common when logging mechanisms are absent or weak. Likelihood: Medium, depending on the implementation of non-repudiation techniques. Impact: Moderate, affecting accountability and data integrity.

104. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Risk Explanation: Attackers may exploit overlapping or colliding data packets, causing corruption or unintended behavior. Precedent: Collision attacks are common in systems with inadequate input validation. Likelihood: Medium, depending on system robustness. Impact: High, potentially leading to data corruption or manipulation.

105. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Risk Explanation: Packets or messages without anti-replay protections can be intercepted and replayed to perform unauthorized actions. Precedent: Replay attacks are widely exploited in systems without sequence numbers or timestamps. Likelihood: High, given the simplicity of the attack method. Impact: Severe, risking unauthorized transactions or access.

106. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

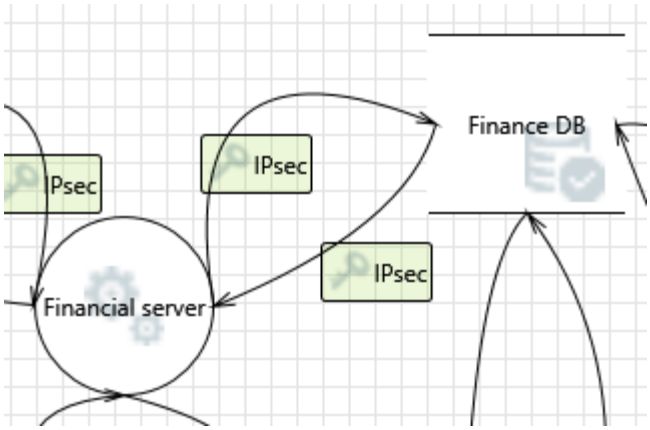
Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all

authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: CSRF attacks can exploit the trust relationship between a user and a website, leading to unauthorized actions such as privilege escalation. To mitigate this, implement CSRF tokens for all state-changing requests and ensure they are unique per session. Enforce secure cookies with the HttpOnly and Secure attributes to protect session data.

Interaction: IPsec



107. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Finance DB can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Weak access control can expose sensitive financial data to unauthorized users. To mitigate this, enforce role-based access control (RBAC), regularly audit access permissions, and use encryption for data at rest and in transit.

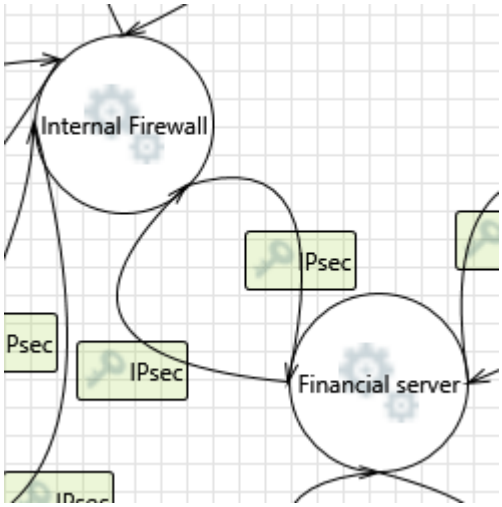
108. Spoofing of Source Data Store Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to incorrect data delivered to Financial server. Consider using a standard authentication mechanism to identify the source data store.

Justification: Spoofing attacks can deliver incorrect data to the Financial Server, leading to operational failures or financial discrepancies. Use mutual authentication between the Finance DB and the Financial Server, such as certificate-based authentication or secure tokens, to verify identities.

Interaction: IPsec



109. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Implement MFA and secure password policies to strengthen the authentication scheme. Regularly test for vulnerabilities like brute force or credential stuffing, and ensure robust session management.

110. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Incorporate data integrity checks using cryptographic methods (e.g., HMAC with SHA-256). Reassembly procedures must verify and validate overlapping packets, ensuring malicious data is not injected or corrupted.

111. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Enable secure protocols like TLS/SSL with anti-replay features, such as sequence numbers and unique session IDs. Ensure timestamps are applied to sensitive data flows, preventing duplication or retransmission of intercepted messages.

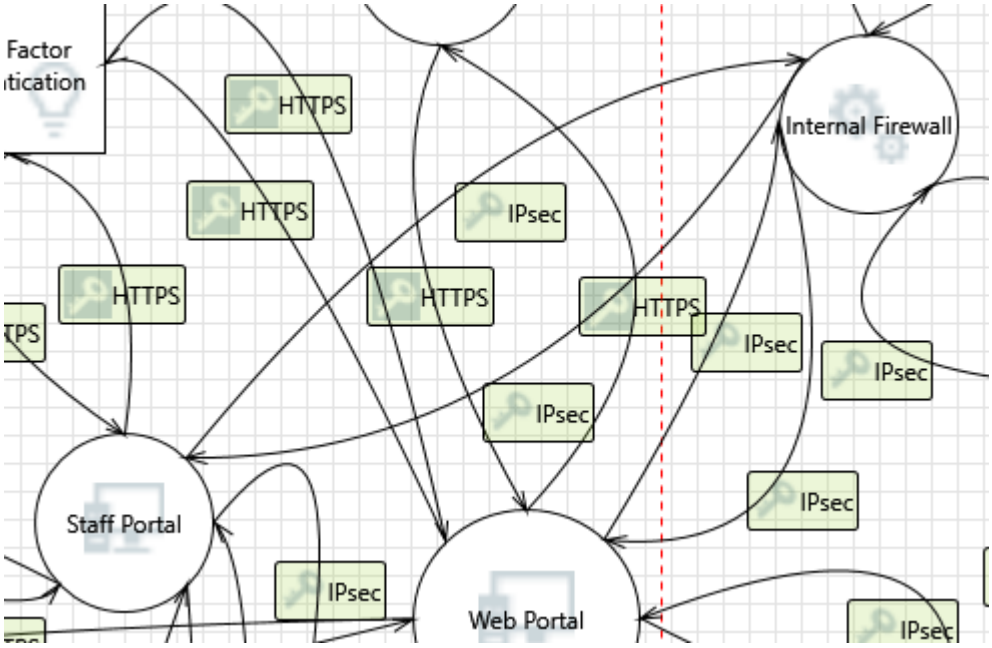
112. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to impersonate the context of Financial server in order to gain additional privilege.

Justification: Risk Explanation: The internal firewall could impersonate the financial server, gaining unauthorized access to sensitive financial operations. Precedent: Impersonation within internal networks is a frequent attack strategy in lateral movement scenarios. Likelihood: Medium, especially without strong authentication protocols. Impact: Severe, given the potential financial and operational risks

Interaction: IPsec



113. Elevation by Changing the Execution Flow in Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Staff Portal in order to change the flow of program execution within Staff Portal to the attacker's choosing.

Justification: Use Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) to mitigate execution flow attacks. Validate all inputs and use secure coding practices.

114. Staff Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to remotely execute code for Staff Portal.

Justification: Harden the application against exploits by validating inputs and applying runtime application self-protection (RASP). Conduct regular security assessments and patch known vulnerabilities.

115. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to impersonate the context of Internal Firewall in order to gain additional privilege.

Justification: Enforce mutual authentication between the Staff Portal and Internal Firewall. Use access control lists (ACLs) to restrict elevated privileges and monitor for suspicious behavior.

116. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Deploy redundant network paths and failover configurations to maintain uninterrupted data flows. Use IPsec's built-in anti-tampering and integrity mechanisms to secure communication.

117. Potential Process Crash or Stop for Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Staff Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Introduce failover systems and resource allocation mechanisms to manage demand spikes. Conduct regular vulnerability assessments to address weaknesses that could lead to crashes.

118. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Strengthen authentication through multi-factor authentication (MFA) and enforce strong password policies. Regularly test and update authentication mechanisms to address emerging vulnerabilities.

119. Potential Data Repudiation by Staff Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Staff Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Use secure logging mechanisms to document all data exchanges. Digital signatures on transmitted data ensure authenticity and prevent denial claims.

120. Cross Site Scripting [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: The web server 'Staff Portal' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Sanitize all user inputs and implement a Content Security Policy (CSP) to restrict the execution of unauthorized scripts. Monitor user activity for anomalies that may indicate XSS attempts.

121. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Use collision-resistant hash functions, such as SHA-256 or SHA-3, for all cryptographic operations. Validate incoming data to detect and reject overlapping packets.

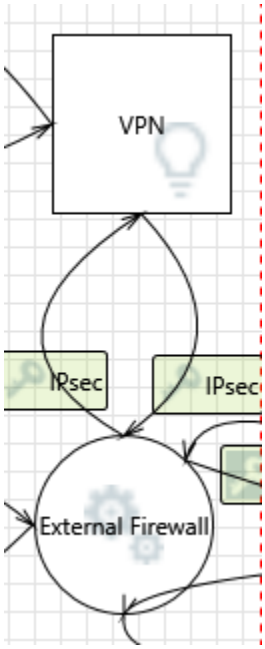
122. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Apply anti-replay mechanisms such as sequence numbers or unique session tokens within the IPsec protocol. Ensure transmitted data includes integrity checks.

Interaction: IPsec



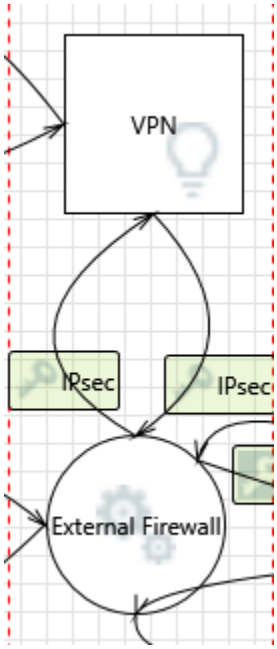
123. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to impersonate the context of VPN in order to gain additional privilege.

Justification: Risk Explanation: The external firewall may impersonate the VPN, potentially intercepting or altering encrypted traffic. Precedent: VPN and firewall impersonation attacks are common targets for MitM attacks. Likelihood: Medium, based on the strength of VPN and firewall configurations. Impact: Severe, affecting data confidentiality and trust.

Interaction: IPsec



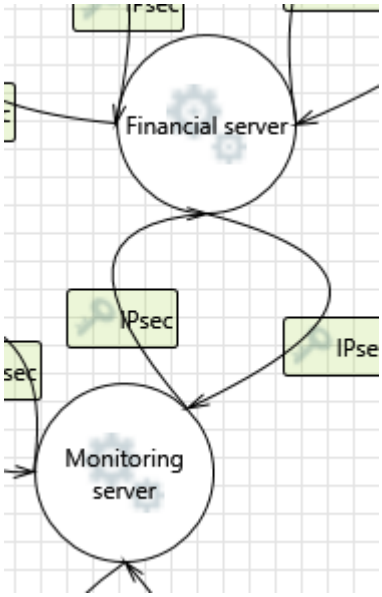
124. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Risk Explanation: Vulnerabilities in SSO implementations (e.g., OAUTH2) could allow attackers to intercept or manipulate user authentication. Precedent: SSO weaknesses have been exploited in several high-profile security breaches. Likelihood: High, given the popularity of SSO and its complexity. Impact: Severe, as it affects all systems relying on the compromised SSO.

Interaction: IPsec



125. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Monitoring server may be able to impersonate the context of Financial server in order to gain additional privilege.

Justification: Impersonation by the Monitoring Server poses a significant risk to the financial data's confidentiality, integrity, and availability. To mitigate this, ensure strong mutual authentication mechanisms between the Monitoring Server and Financial Server, such as certificates or shared keys. Implement robust role-based access control (RBAC) and log all access requests for auditing and detecting privilege escalation attempts.

126. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Weak authentication increases the risk of information disclosure. Use robust identity verification techniques, enforce periodic credential updates, and ensure all communication happens over secure protocols like HTTPS.

127. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Collision attacks can alter legitimate data during transmission. Use cryptographic hash algorithms to detect and prevent data overlap. Validate data integrity at each endpoint to mitigate this risk.

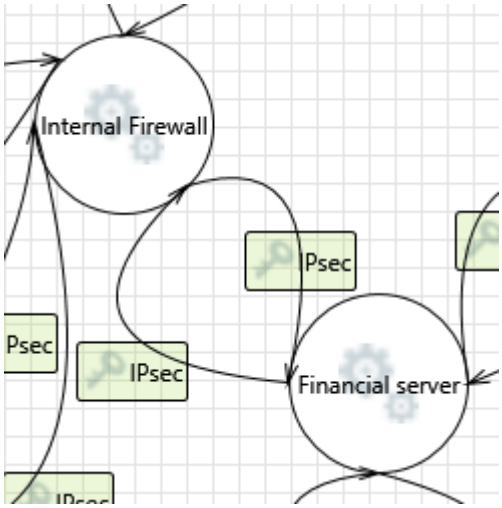
128. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Replay attacks can lead to unauthorized operations by reusing valid requests. Use session tokens, sequence numbers, or timestamps to prevent replays. Ensure all communication channels are encrypted to prevent interception.

Interaction: IPsec



129. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Financial server may be able to impersonate the context of Internal Firewall in order to gain additional privilege.

Justification: Risk Explanation: The financial server could impersonate the internal firewall to bypass security checks. Precedent: Systems with complex dependencies often see abuse of trust relationships. Likelihood: Medium, depending on system configuration. Impact: Severe, with potential for system-wide security breaches.

130. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Risk Explanation: Attackers can send overlapping or misaligned packets, corrupting data flows or triggering unintended behaviors. Precedent: Similar attacks have been documented in poorly defended network infrastructures. Likelihood: Medium, depending on the system's input validation. Impact: High, as data corruption or manipulation can disrupt operations.

131. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Risk Explanation: Packets or messages without proper anti-replay defenses can be intercepted and replayed by an attacker, potentially leading to unauthorized actions. Precedent: Replay attacks are widely exploited in systems lacking sequence numbers or timestamps. Likelihood: High, particularly in legacy or improperly secured communication protocols. Impact: Severe, as it could compromise system integrity or facilitate unauthorized actions.

132. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

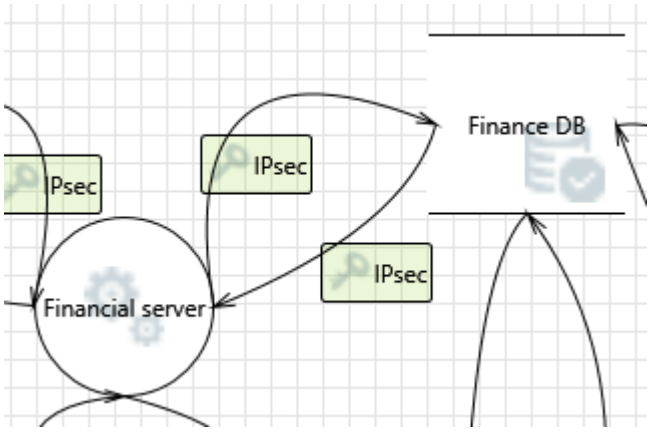
Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak

credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Implement a robust authentication framework such as OAuth 2.0 or SAML, ensuring strong credential policies (e.g., complexity, expiration). Multi-factor authentication (MFA) adds another layer of protection against credential-based attacks. Regular audits of authentication systems mitigate risks from weak credentials.

Interaction: IPsec



133. Potential Excessive Resource Consumption for Financial server or Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Financial server or Finance DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Resource exhaustion attacks can cause denial of service. To mitigate this, implement rate limiting, request throttling, and timeout mechanisms. Use load balancers and resource monitoring to ensure scalability and prevent overload scenarios.

134. Authorization Bypass [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Can you access Finance DB and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via

filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.

Justification: Unauthorized access to the Finance DB can lead to information disclosure or modification. Ensure the Finance DB is accessible only through the designated application interface with strong access controls. Implement encryption at rest and logging mechanisms to monitor unauthorized access attempts.

135. Potential SQL Injection Vulnerability for Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification: SQL Injection attacks can severely compromise database integrity and confidentiality. To mitigate this, use parameterized queries and stored procedures to avoid dynamic SQL execution. Employ input validation and sanitization to ensure only valid data is processed. Regularly update and patch database systems to address vulnerabilities.

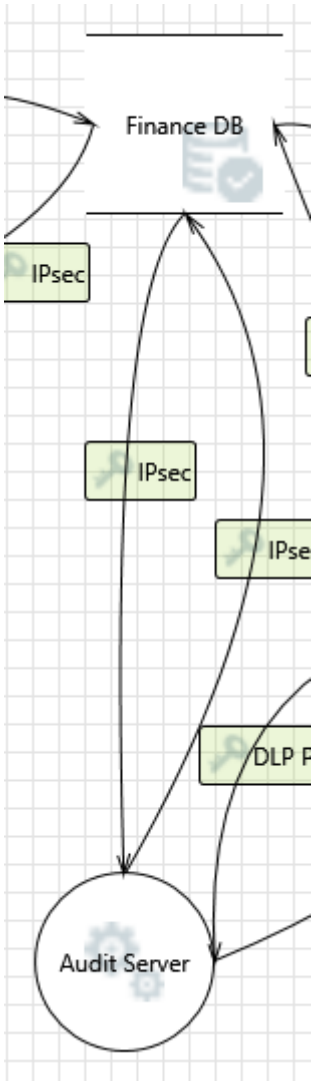
136. Spoofing of Destination Data Store Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Finance DB. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Risk Explanation: Finance DB may be spoofed by an attacker, leading to data being redirected to the attacker’s target instead of the intended destination. Precedent: Spoofing attacks are common in systems without robust authentication mechanisms. Likelihood: High, due to the high value of financial data and potential misconfigurations. Impact: Severe, risking loss of data integrity and confidentiality.

Interaction: IPsec



137. Potential SQL Injection Vulnerability for Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification: isk Explanation: SQL injection could allow attackers to manipulate or retrieve sensitive data. Precedent: SQL injection remains one of the most exploited vulnerabilities in database systems. Likelihood: High, especially in systems relying on dynamic query construction. Impact: Severe, risking data corruption, theft, or unauthorized changes.

138. Potential Excessive Resource Consumption for Audit Server or Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Audit Server or Finance DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Risk Explanation: Unchecked resource consumption can lead to service interruptions or denial of service (DoS) attacks. Precedent: Similar attacks have targeted under-resourced servers, causing outages. Likelihood: High, especially in environments with unpredictable traffic patterns. Impact: Severe, with potential downtime and inability to process data.

139. Authorization Bypass [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Can you access Finance DB and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reaching it via filesharing? Ensure that your program is the only one that can access the data, and that all other subjects have to use your interface.

Justification: Risk Explanation: Bypassing authorization mechanisms could allow unauthorized access to sensitive data. Precedent: Authorization flaws have been exploited in many high-profile breaches. Likelihood: High, particularly if access controls are poorly implemented. Impact: Severe, exposing sensitive financial records to unauthorized parties.

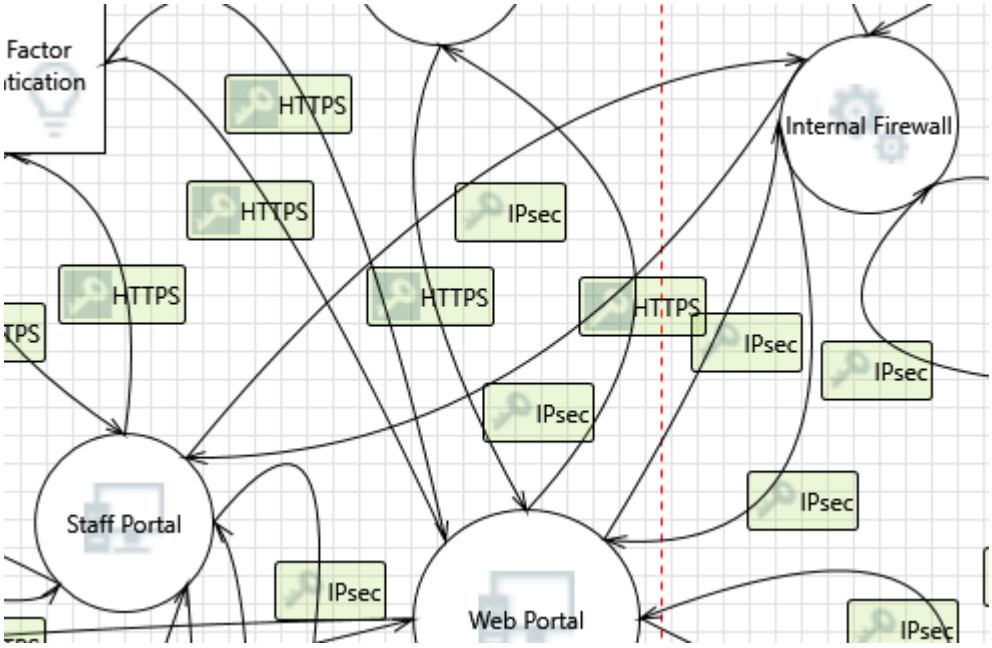
140. Spoofing of Destination Data Store Finance DB [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Finance DB. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Risk Explanation: Spoofing Finance DB can lead to sensitive data being written to a malicious destination. Precedent: Such attacks have been observed where entity authentication is absent or weak. Likelihood: High, given the value of financial data and potential for exploitation. Impact: Severe, risking confidentiality, integrity, and operational reliability.

Interaction: IPsec



141. Elevation by Changing the Execution Flow in Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Internal Firewall in order to change the flow of program execution within Internal Firewall to the attacker's choosing.

Justification: Risk Explanation: An attacker may inject data to alter the execution flow of the Internal Firewall, enabling unauthorized actions. Precedent: Similar vulnerabilities have been exploited to bypass security controls. Likelihood: Medium, based on the robustness of input validation. Impact: Severe, risking system compromise and unauthorized access.

142. Internal Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to remotely execute code for Internal Firewall.

Justification: Risk Explanation: Remote code execution vulnerabilities may allow attackers to execute unauthorized code on the Internal Firewall with elevated privileges. Precedent: RCE vulnerabilities have been exploited to gain complete control over systems. Likelihood: High, especially in systems lacking timely updates. Impact: Severe, risking full system compromise and data breaches.

143. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to impersonate the context of Staff Portal in order to gain additional privilege.

Justification: Risk Explanation: The Internal Firewall may impersonate the context of the Staff Portal to gain unauthorized privileges. Precedent: Impersonation threats often exploit weak identity verification mechanisms. Likelihood: High, given the interconnected nature of systems. Impact: Severe, allowing unauthorized privilege escalation.

144. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: An external agent could interrupt data flow through IPsec, leading to communication failures or service disruptions. Precedent: Data flow interruptions have been observed in denial-of-service (DoS) scenarios. Likelihood: Medium to high, based on network exposure and configuration. Impact: High, risking service unavailability and operational delays.

145. Potential Process Crash or Stop for Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Internal Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Risk Explanation: The Internal Firewall may crash or halt due to resource exhaustion or targeted attacks. Precedent: DoS attacks have often exploited resource vulnerabilities to crash systems. Likelihood: High, especially under heavy load or attack. Impact: Severe, risking network security and operational continuity.

146. Potential Data Repudiation by Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Internal Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: The Internal Firewall could deny receiving data, creating a scenario where accountability is compromised. Precedent: Repudiation threats are common in systems lacking proper logging mechanisms. Likelihood: Medium, depending on the robustness of audit trails. Impact: Moderate, affecting data integrity and operational accountability.

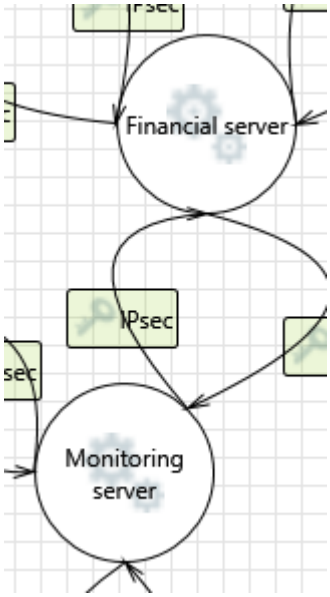
147. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: IPsec



148. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Financial server may be able to impersonate the context of Monitoring server in order to gain additional privilege.

Justification: Impersonation by the Financial Server could compromise monitoring integrity. Use mutual authentication protocols like certificates to ensure the

server's identity. Enforce RBAC and audit logs to detect and prevent privilege escalation.

149. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Weak authentication exposes systems to unauthorized access. Use secure and proven authentication mechanisms like OAuth, MFA, and strong passwords. Regularly update authentication protocols and avoid custom schemes unless thoroughly tested.

150. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Collision attacks can corrupt or overwrite legitimate data. To prevent this, use strong cryptographic hash functions such as SHA-256 or better. Ensure all data is validated and sanitized before processing to detect and prevent overlaps.

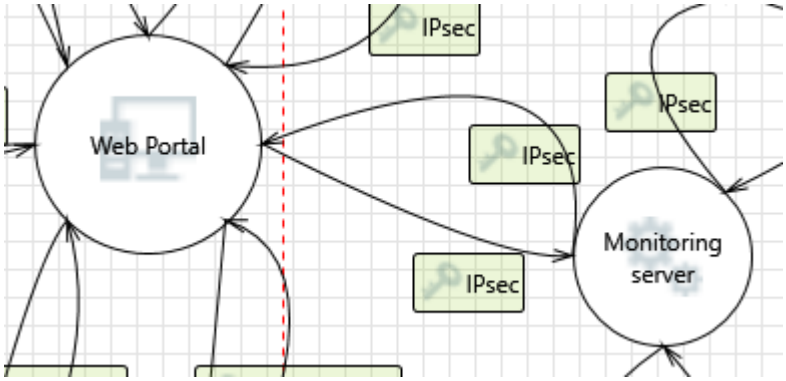
151. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Replay attacks can reuse valid communications to gain unauthorized access. Use protocols like IPsec with anti-replay mechanisms, including sequence numbers and timestamps, to mitigate this threat. Ensure strong cryptographic integrity checks on transmitted data.

Interaction: IPsec



152. Elevation by Changing the Execution Flow in Monitoring server [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Monitoring server in order to change the flow of program execution within Monitoring server to the attacker's choosing.

Justification: Risk Explanation: An attacker may inject data into the Monitoring Server to alter its execution flow, enabling unauthorized actions. Precedent: Similar attacks have been observed where input validation was inadequate. Likelihood: Medium to high, depending on system safeguards. Impact: Severe, potentially compromising system integrity.

153. Monitoring server May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to remotely execute code for Monitoring server.

Justification: Risk Explanation: Remote code execution (RCE) vulnerabilities may allow attackers to gain elevated privileges on the Monitoring Server. Precedent: RCE has been a common method for gaining unauthorized control of systems. Likelihood: High, especially without regular updates and patches. Impact: Severe, risking complete system compromise.

154. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Monitoring server may be able to impersonate the context of Web Portal in order to gain additional privilege.

Justification: Risk Explanation: The Monitoring Server may impersonate the context of the Web Portal to gain unauthorized privileges. Precedent: Impersonation attacks are common in interconnected systems with weak authentication. Likelihood: High, given the trust relationships between components. Impact: Severe, risking unauthorized actions and data manipulation.

155. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Risk Explanation: External agents may interrupt IPsec data flows, leading to service disruption. Precedent: Disruptions in secure communication channels have been observed in denial-of-service (DoS) attacks. Likelihood: Medium to high, depending on network configuration. Impact: High, risking service downtime and data transmission failures.

156. Potential Process Crash or Stop for Monitoring server [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Monitoring server crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Risk Explanation: The Monitoring Server may crash or halt due to resource exhaustion or targeted attacks, leading to availability issues. Precedent: DoS attacks targeting servers have often exploited resource limitations or software vulnerabilities. Likelihood: High, especially under heavy load or during an attack. Impact: Severe, causing service interruptions and operational delays.

157. Potential Data Repudiation by Monitoring server [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Monitoring server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Risk Explanation: The Monitoring Server could deny receiving data from a source, creating a repudiation scenario. Precedent: Repudiation threats are prevalent in systems without secure logging mechanisms. Likelihood: Medium, depending on the presence of non-repudiation measures. Impact:

Moderate, risking accountability and system reliability. Implement secure logging mechanisms with digital signatures. Audit logs regularly to ensure data integrity. Use cryptographic methods to verify data exchanges.

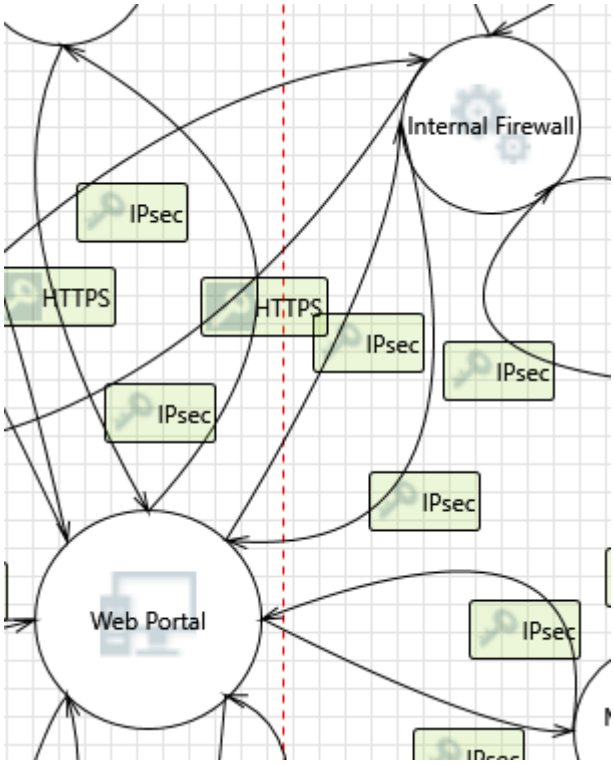
158. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: IPsec



159. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75

bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Risk Explanation: Attackers could overlap or overwrite data packets, causing data corruption or manipulation. Precedent: Collision attacks have been used in both network and application layers. Likelihood: Medium, depending on system defenses. Impact: High, with risks to data integrity and operational stability.

160. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Risk Explanation: Packets or messages without proper anti-replay mechanisms can be captured and replayed by attackers. Precedent: Replay attacks are common in systems without sequence numbers or timestamps. Likelihood: High, given the simplicity of such attacks. Impact: Severe, as it can lead to unauthorized actions or data corruption.

161. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of Internal Firewall in order to gain additional privilege.

Justification: Risk Explanation: The web portal could impersonate the internal firewall, bypassing network security controls. Precedent: Impersonation at trust boundaries is a known method for lateral movement in network attacks. Likelihood: Medium to high, depending on implemented safeguards.

162. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Risk Explanation: Custom authentication schemes may have inherent weaknesses, such as easily guessable credentials or poor credential management. Precedent: Weak authentication has been a primary cause of

many data breaches. Likelihood: High, especially for custom implementations. Impact: Severe, as it can lead to unauthorized access and data compromise.

163. Elevation by Changing the Execution Flow in Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Web Portal in order to change the flow of program execution within Web Portal to the attacker's choosing.

Justification: Use control flow integrity (CFI) to restrict unauthorized changes in execution flow. Validate all inputs to prevent injection attacks and apply strict access controls to sensitive areas of the application.

164. Web Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to remotely execute code for Web Portal.

Justification: Apply secure coding practices to minimize vulnerabilities. Enforce runtime application self-protection (RASP) and sandboxing to isolate code execution. Regularly patch and update the Web Portal to address known exploits.

165. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Deploy intrusion prevention systems (IPS) to detect and block attacks on IPsec communication. Implement redundancy in network paths to ensure uninterrupted data flow. Monitor and log network activity for anomaly detection.

166. Potential Process Crash or Stop for Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Web Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Implement resource monitoring and automated scaling to handle load spikes. Use failover mechanisms to maintain availability during crashes and conduct regular stress testing to identify and address vulnerabilities.

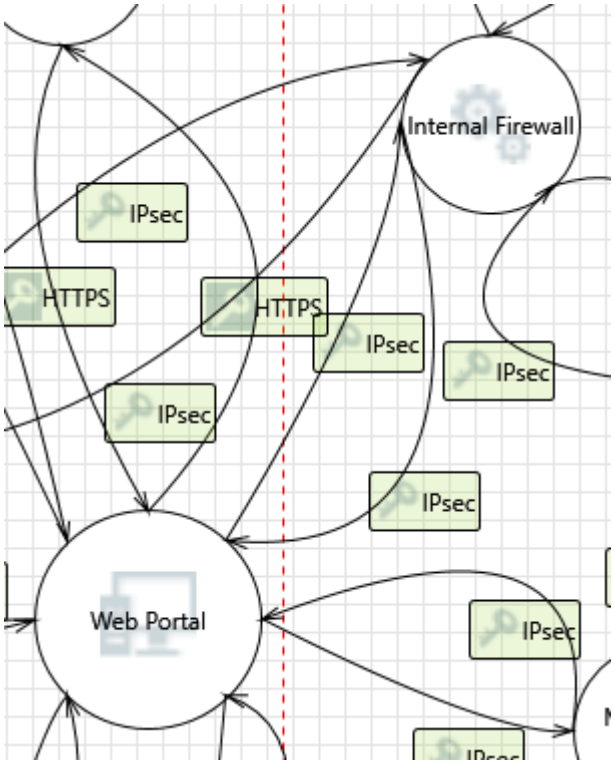
167. Potential Data Repudiation by Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Web Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Enable comprehensive logging on the Web Portal to capture incoming data transactions with timestamps and unique identifiers. Use digital signatures or cryptographic hashes to ensure data integrity and provide non-repudiation.

Interaction: IPsec



168. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Internal Firewall may be able to impersonate the context of Web Portal in order to gain additional privilege.

Justification: Risk Explanation: The internal firewall could impersonate the web portal, gaining unauthorized access to user-level operations. Precedent: Misuse of elevated privileges in internal systems is a frequent attack vector. Likelihood: Medium, especially without stringent access control. Impact: High, potentially leading to data exposure or manipulation.

169. Elevation by Changing the Execution Flow in Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Internal Firewall in order to change the flow of program execution within Internal Firewall to the attacker's choosing.

Justification: Enforce execution control mechanisms like ASLR (Address Space Layout Randomization) to limit an attacker's ability to alter execution flow. Log all requests and validate inputs to ensure compliance with expected behavior.

170. Internal Firewall May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to remotely execute code for Internal Firewall.

Justification: Secure the Internal Firewall by applying least privilege principles and restricting code execution permissions. Regularly audit and patch the firewall to address vulnerabilities and prevent exploitation.

171. Data Flow IPsec Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Utilize redundant connections and failover systems to maintain continuous data flow. Apply encryption with IPsec to secure communication and prevent tampering.

172. Potential Process Crash or Stop for Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Internal Firewall crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Implement load balancing and resource allocation strategies to avoid overloads. Use hardware redundancy and monitoring tools to detect and recover from crashes quickly.

173. Potential Data Repudiation by Internal Firewall [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Internal Firewall claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Enable detailed logging and auditing on the Internal Firewall to verify all received data. Use cryptographic methods to authenticate and track the source of incoming requests.

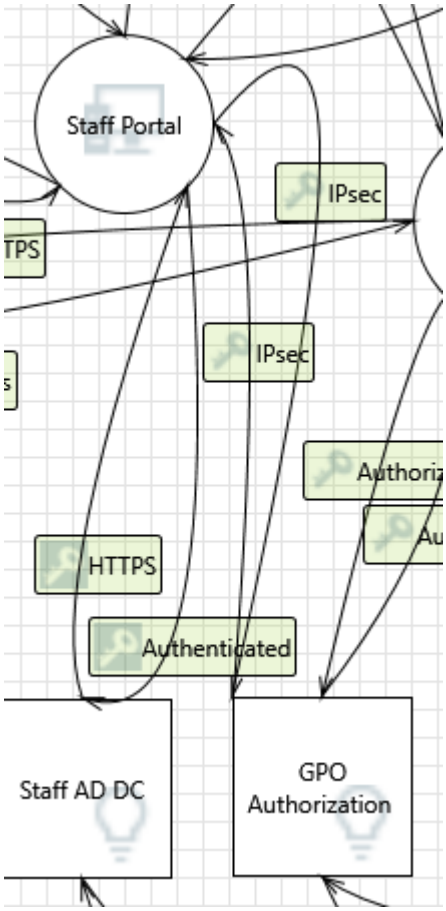
174. Weak Authentication Scheme [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: <no mitigation provided>

Interaction: IPsec



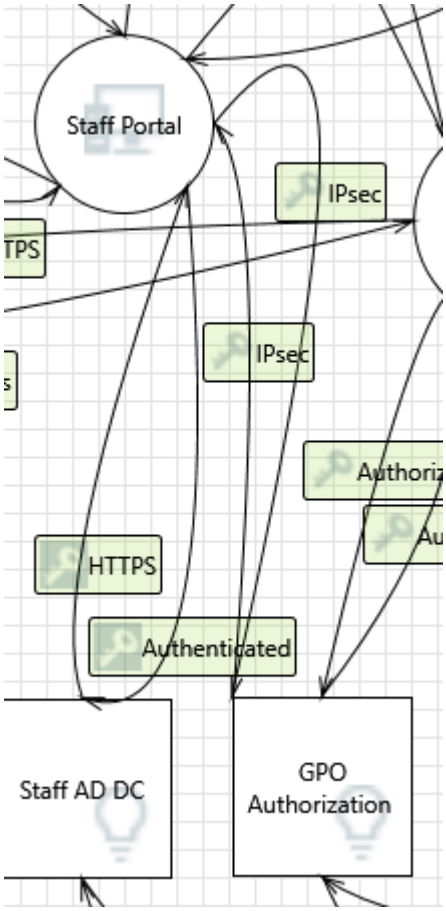
175. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Staff Portal may be able to impersonate the context of GPO Authorization in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: IPsec



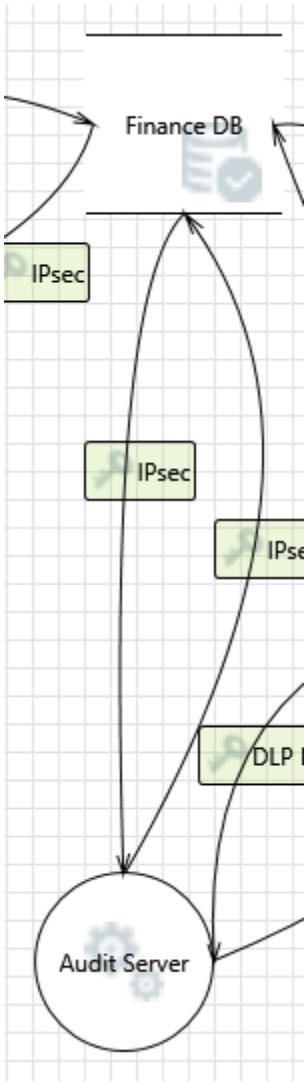
176. Weakness in SSO Authorization [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: <no mitigation provided>

Interaction: IPsec



177. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Finance DB can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: <no mitigation provided>

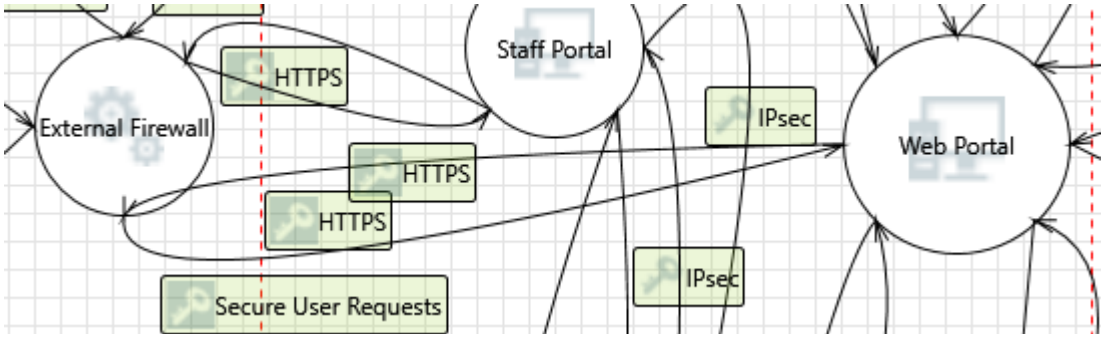
178. Spoofing of Source Data Store Finance DB [State: Not Started] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to incorrect data delivered to Audit Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

Interaction: Secure User Requests



179. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Justification: Ensure data flows use secure, collision-resistant hashing algorithms such as SHA-256 or SHA-3. Collision detection mechanisms can identify and reject overlapping or altered packets, maintaining the integrity of transmitted data.

180. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification: Utilize sequence numbers and timestamps within secure protocols like TLS/SSL to prevent replay attacks. Implement anti-replay mechanisms such as session-based tokens or message counters, ensuring unique and time-sensitive interactions.

181. Elevation by Changing the Execution Flow in Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Web Portal in order to change the flow of program execution within Web Portal to the attacker's choosing.

Justification: An attacker could alter the Web Portal's program flow by injecting malicious data, leading to privilege escalation or unintended behavior. Implementing strict input validation and secure coding practices can prevent execution flow manipulation.

182. Web Portal May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: External Firewall may be able to remotely execute code for Web Portal.

Justification: The ability of the External Firewall to execute code remotely on the Web Portal could lead to unauthorized privilege escalation. This poses severe security risks, including data breaches and system compromise. Regular security updates, rigorous code reviews, and input sanitization can reduce vulnerabilities.

183. Data Flow HTTPS Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Interruptions in HTTPS data flow, possibly caused by external agents, can compromise service availability and data integrity. Ensuring end-to-end encryption, redundancy, and real-time monitoring can minimize these risks and detect anomalies promptly.

184. Potential Process Crash or Stop for Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Web Portal crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: It could disrupt critical services. This could be exploited by attackers to create a Denial of Service (DoS) condition, affecting availability and potentially violating SLAs. Measures like load balancing, input validation, and monitoring should be employed to ensure resilience.

185. Potential Data Repudiation by Web Portal [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Web Portal claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Without robust logging and auditing mechanisms, the Web Portal's claim that it did not receive data cannot be disputed or verified. This could lead to operational issues or disputes over accountability. Implementing detailed logs ensures traceability and non-repudiation, essential for secure interactions.

186. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Web Portal may be able to impersonate the context of External Firewall in order to gain additional privilege.

Justification: Risk Explanation: The web portal could impersonate the external firewall, potentially altering inbound or outbound traffic flows. Precedent: Trust boundary impersonation is a recognized threat in complex networks. Likelihood: Medium, based on the strength of implemented network controls. Impact: High, with potential risks to data integrity and confidentiality.

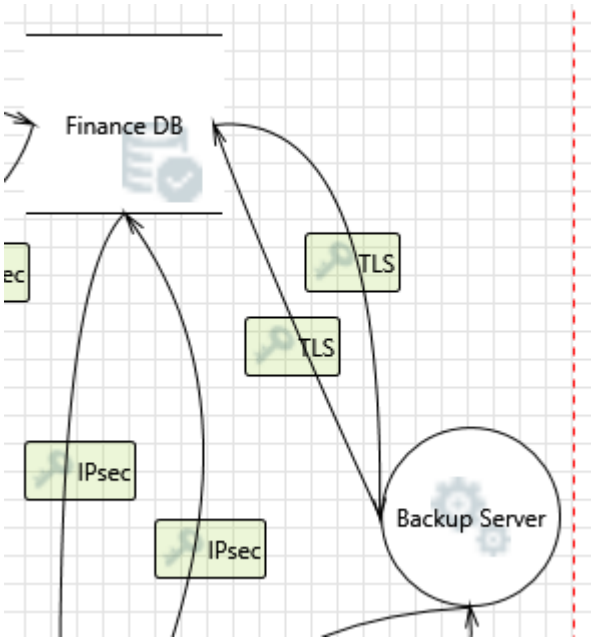
187. Weak Authentication Scheme [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.

Justification: Introduce strong authentication mechanisms with secure password storage (e.g., bcrypt or PBKDF2). Enforce account lockout policies for failed login attempts and continuously monitor for anomalies.

Interaction: TLS



188. Potential SQL Injection Vulnerability for Finance DB [State: Not Started] [Priority: High]

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification: <no mitigation provided>

189. Potential Excessive Resource Consumption for Backup Server or Finance DB [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does Backup Server or Finance DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: <no mitigation provided>

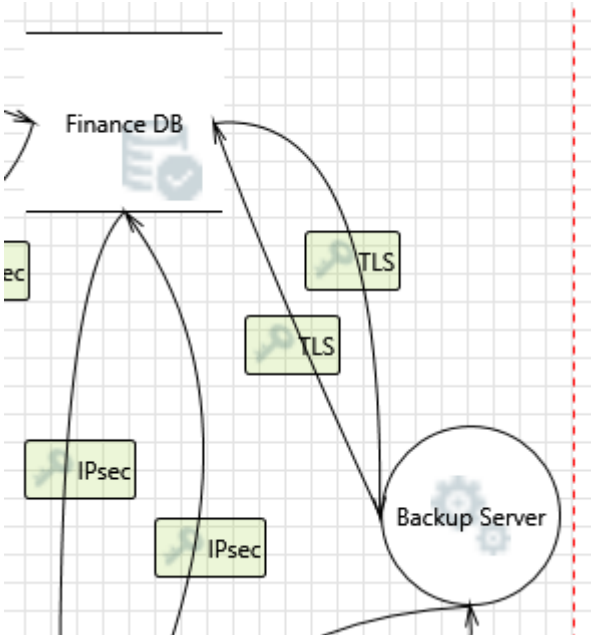
190. Spoofing of Destination Data Store Finance DB [State: Not Started] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Finance DB. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

Interaction: TLS



191. Spoofing of Source Data Store Finance DB [State: Not Started] [Priority: High]

Category: Spoofing

Description: Finance DB may be spoofed by an attacker and this may lead to incorrect data delivered to Backup Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

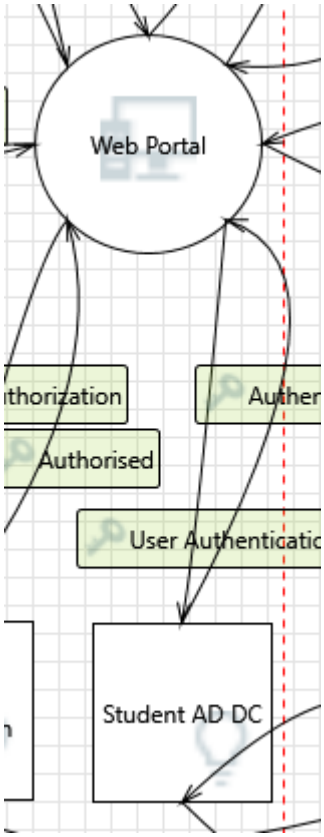
192. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Finance DB can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: <no mitigation provided>

Interaction: User Authentication



193. Weakness in SSO Authorization [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Risk Explanation: Vulnerabilities in SSO implementations, such as MitM attacks, can allow attackers to gain unauthorized access. Precedent: SSO systems have historically been targeted for session token theft and privilege escalation. Likelihood: High, due to the complex nature of SSO systems. Impact: Severe, compromising all systems reliant on the SSO framework.