Threat Modeling Report

Created on 01/03/2025 10:06:52

Threat Model Name: UFS Threat Model

Owner: Abdelaziz El-Sheikh

Reviewer: Dr. Mohamed A. Elsayed

Contributors: Abdelaziz El-Sheikh

Description: The project involves a newly developed web-based portal for university students to access financial services. This portal allows students to view their current balance, review payment history, set up payment accounts, make one-time payments, and configure automatic payments. The university's financial system is already operational and hosted in its data center. Staff access this system through a secure internal network or remotely via a VPN-secured web portal. The system ensures security through encrypted communication between its components and uses Active Directory (AD) for authentication and role-based access. The new student portal is hosted in the data center's DMZ and connects securely to internal resources using HTTPS. It introduces a separate Active Directory domain for student authentication, managed by a dedicated controller within the DMZ. Students log in using their credentials, and the portal displays services they are authorized to use based on predefined security groups. The portal enforces security by requiring remote devices to have updated operating systems, security software, and supported browsers. This implementation provides a secure and user-friendly way for students to access financial services while maintaining the university's strict security standards.

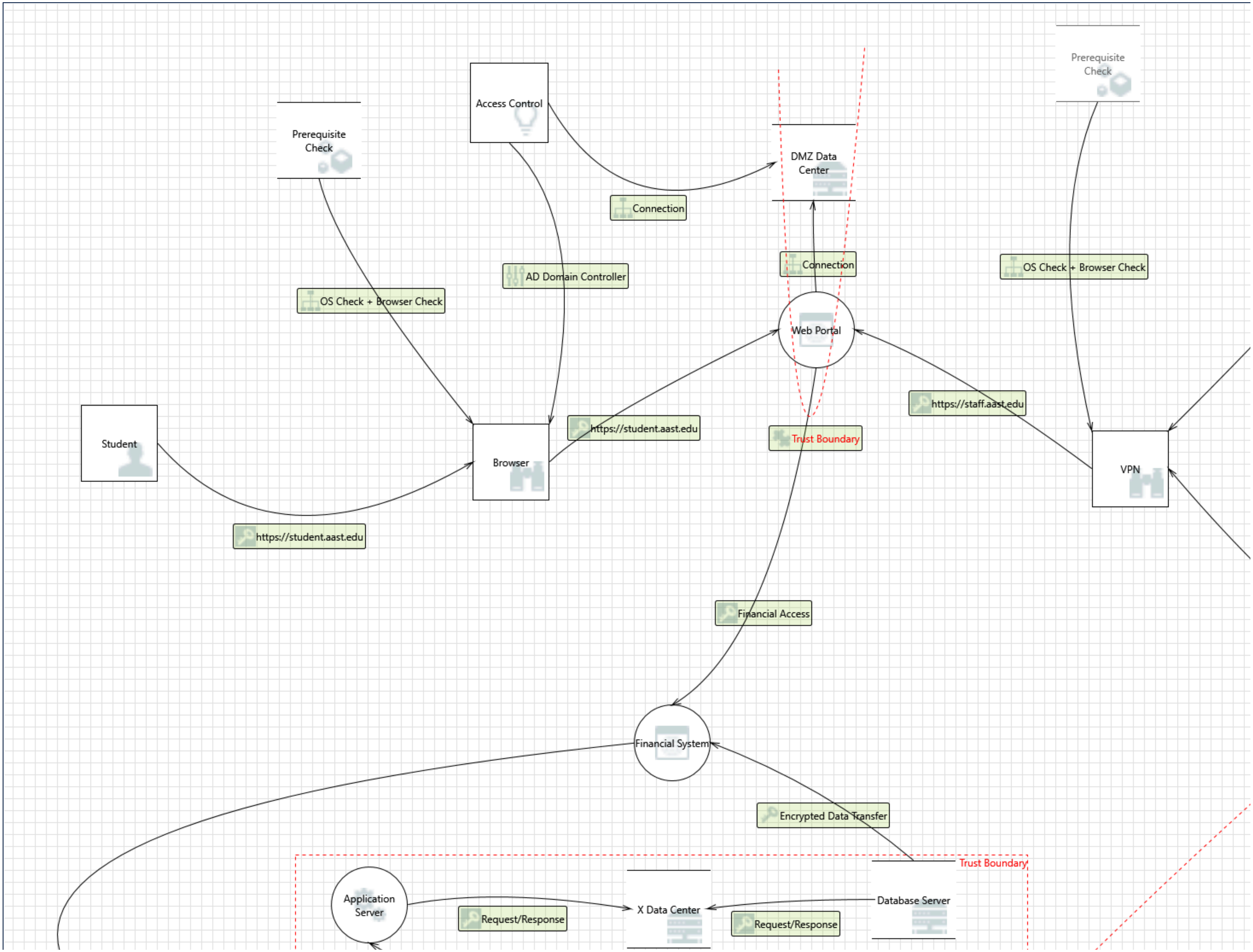
Assumptions: - The Prerequisite Check (including the Operating System version and the Browser version) is not part of the Threat Model since it doesn't directly affect the environment; it either checks those two conditions and finds them applicable so access to the Web Portal is granted, or the conditions aren't applied so access is denied. - There is more than one available Internal Workstation, so the staff user can use another Internal Workstation if his/her machine crashed or got suspended. - There is a Trust Boundary between the Staff and his/her Workstation because the Staff User is authenticated when entering the University. - The operations permitted for the student when granting access to the web portal (viewing their current balance and payment history, setting up payment accounts, making one-time payments, and setting up automatic payments) are considered inside the Financial System Entity

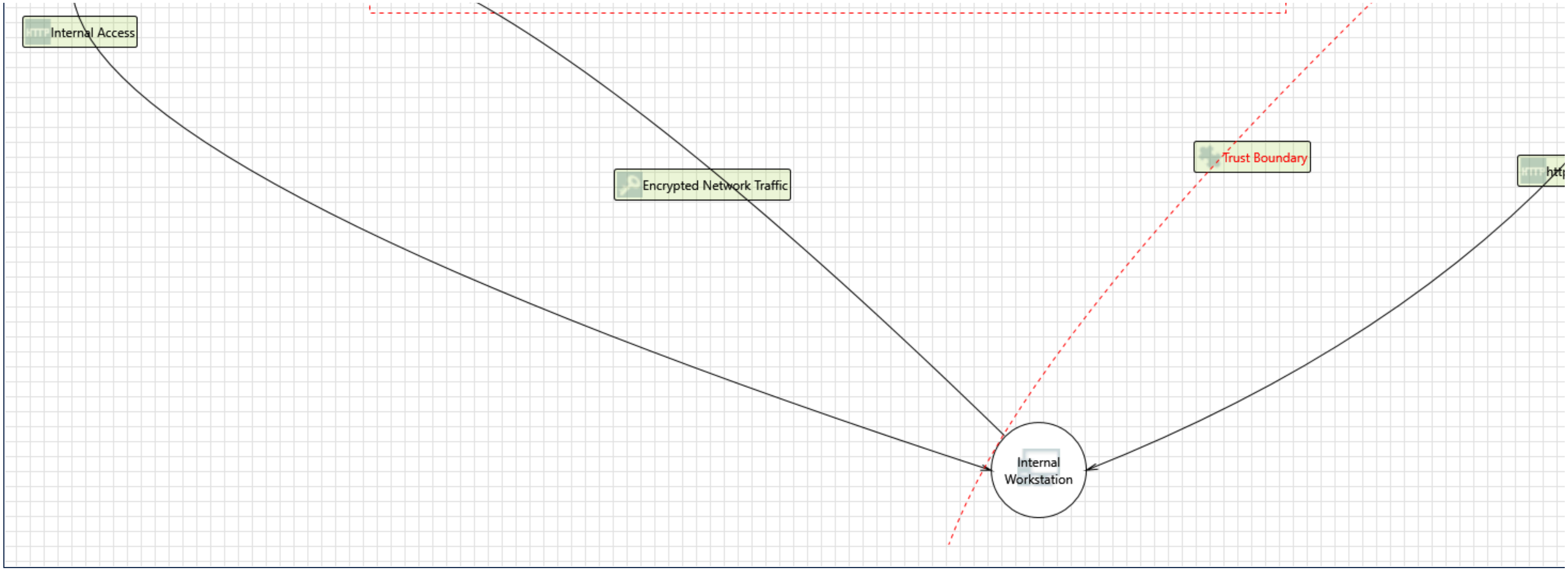
External Dependencies: - Active Directory Presence - Existing Financial System - University Data Center Infrastructure - Encryption Mechanisms - Student Devices and Browsers - Third-Party Security Tools - Physical Security Guards - Backup and Recovery Systems

Threat Model Summary:

Not Started	0
Not Applicable	5
Needs Investigation	15
Mitigation Implemented	54
Total	74
Total Migrated	0

Diagram: UFS TM

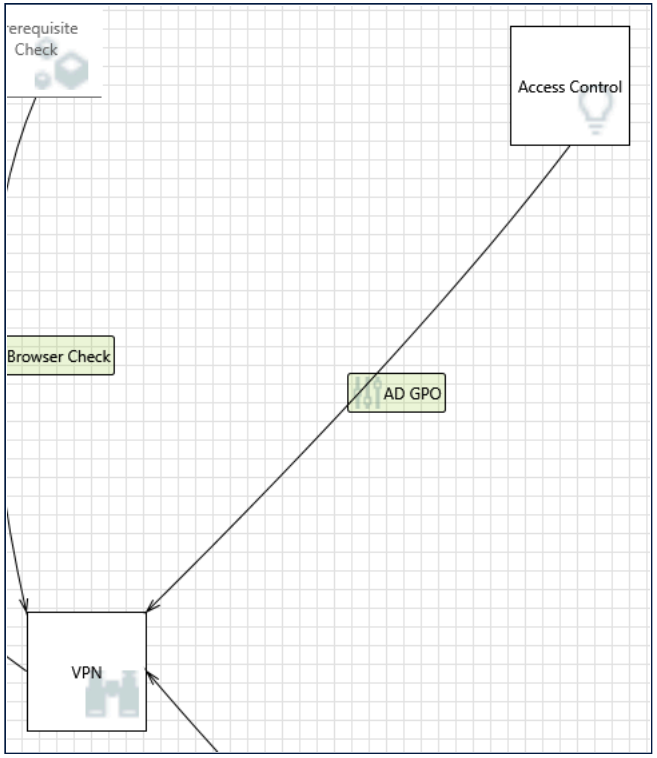

Prerequisite Check
Access Control
DMZ Data Center
Connection
Prerequisite Check
AD Domain Controller
Connection
OS Check + Browser Check
OS Check + Browser Check
Web Portal
https://staff.aast.edu
Student
Browser
https://student.aast.edu
Trust Boundary
VPN
https://student.aast.edu
Financial Access
Financial System
Encrypted Data Transfer
Trust Boundary
Application Server
X Data Center
Database Server
Request/Response
Request/Response



UFS TM Diagram Summary:

Not Started	0
Not Applicable	5
Needs Investigation	15
Mitigation Implemented	54
Total	74
Total Migrated	0

Interaction: AD GPO



1. Authenticated Data Flow Compromised [State: Mitigation Implemented] [Priority: High]

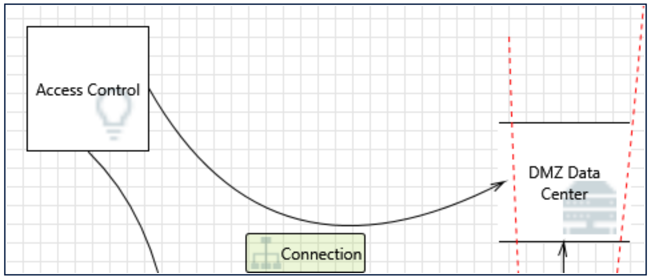
Category: Tampering

Description: An attacker can read or modify data transmitted over an authenticated dataflow.

Justification: The Destination must not be trusted.

- Destination Authenticated (No)

Interaction: Connection



2. Data Logs from an Unknown Source [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.
Justification: The connection between the AD Domain Controller &amp; the DMZ Data Data Center must provide Confidentiality &amp; Integrity.

1- Enable Provides Confidentiality
2- Enable Provides Integrity

3. Authenticated Data Flow Compromised [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: An attacker can read or modify data transmitted over an authenticated dataflow.
Justification: Integrity must be provided through the Connection.

Provides Integrity (Yes)

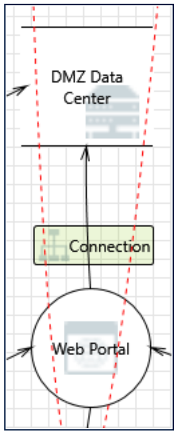
4. Lower Trusted Subject Updates Logs [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.
Justification: The DMZ Data Center should either store log files securely or discard them.

5. Spoofing of Destination Data Store DMZ Data Center [State: Needs Investigation] [Priority: Medium]

Category: Spoofing
Description: DMZ Data Center may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DMZ Data Center. Consider using a standard authentication mechanism to identify the destination data store.
Justification: A stronger Authentication Technique should be available to authenticate the destination.

Interaction: Connection



6. Weak Credential Storage [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored

Justification: The DMZ Data Center should store credentials and log files in a more secure way.

7. Potential Excessive Resource Consumption for Web Portal or DMZ Data Center [State: Needs Investigation] [Priority: Medium]

Category: Denial Of Service

Description: Does Web Portal or DMZ Data Center 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: Although a backup option is available to mitigate this type of threat, a stronger way of implementing Availability is needed.

8. Potential Weak Protections for Audit Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect

Justification: The DMZ Data Center should either store log files securely or discard them.

9. Insufficient Auditing [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.

Justification: The DMZ Data Center should either store log files securely or discard them.

10. Data Logs from an Unknown Source [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.

Justification: The DMZ Data Center should either store log files securely or discard them.

11. Lower Trusted Subject Updates Logs [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.

Justification: The DMZ Data Center should either store log files securely or discard them.

12. Risks from Logging [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.

Justification: The DMZ Data Center should either store log files securely or discard them.

13. Authenticated Data Flow Compromised [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: An attacker can read or modify data transmitted over an authenticated dataflow.
Justification: The destination shouldn&#39;t be automatically authenticated.

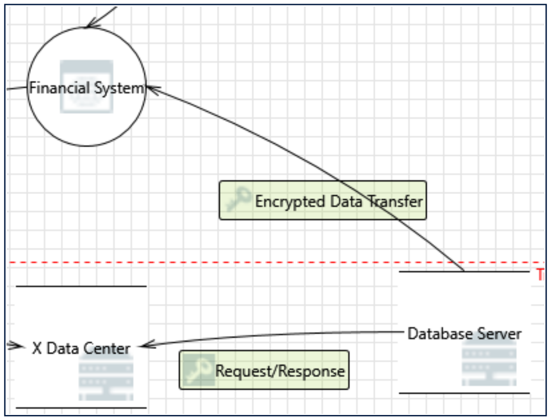
14. Spoofing of Destination Data Store DMZ Data Center [State: Needs Investigation] [Priority: Medium]

Category: Spoofing
Description: DMZ Data Center may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DMZ Data Center. Consider using a standard authentication mechanism to identify the destination data store.
Justification: A stronger Authentication Technique should be available to authenticate the destination.

15. Authorization Bypass [State: Needs Investigation] [Priority: Medium]

Category: Information Disclosure
Description: Can you access DMZ Data Center 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: There should be a stronger encryption present in the connection.

Interaction: Encrypted Data Transfer



16. Risks from Logging [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.
Justification: The Database should either store log files securely or discard them to avoid this type of attacks.

17. Weak Access Control for a Resource [State: Needs Investigation] [Priority: Medium]

Category: Information Disclosure

Description: Improper data protection of Database Server can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: There must be a stronger confidentiality implementation available to avoid this Information Disclosure threat.

18. Spoofing of Source Data Store Database Server [State: Needs Investigation] [Priority: Medium]

Category: Spoofing
Description: Database Server may be spoofed by an attacker and this may lead to incorrect data delivered to Financial System. Consider using a standard authentication mechanism to identify the source data store.
Justification: Although an IPsec connection is present, but a stronger Authentication process must be present &amp; implemented.

19. Elevation by Changing the Execution Flow in Financial System [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Financial System in order to change the flow of program execution within Financial System to the attacker's choosing.
Justification: The Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

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

Category: Elevation Of Privilege
Description: Database Server may be able to remotely execute code for Financial System.
Justification: The Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

21. 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: The Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

22. Data Flow Encrypted Data Transfer 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: The Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

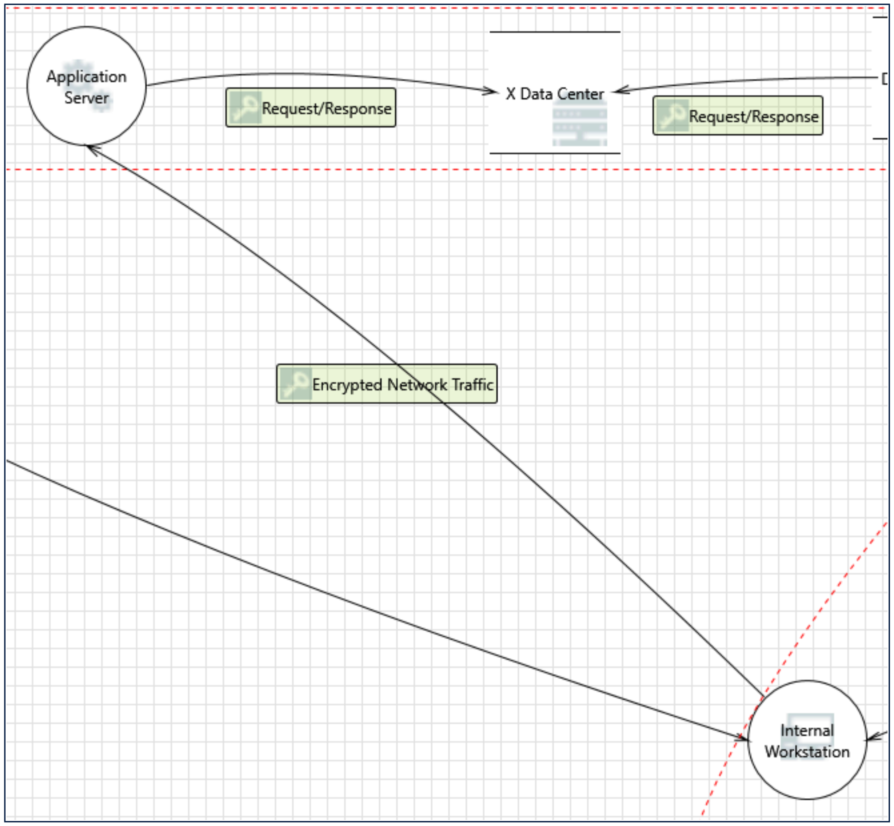
23. Potential Process Crash or Stop for Financial System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Financial System crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

24. Potential Data Repudiation by Financial System [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Financial System 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 Trust Boundary must be adjusted to exclude the connection from the Database Server to the Financial System.

Interaction: Encrypted Network Traffic



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

Category: Elevation Of Privilege
Description: An attacker may pass data into Application Server in order to change the flow of program execution within Application Server to the attacker's choosing.
Justification: The Trust Boundary must be adjusted to exclude the connection between the Internal Workstation and the Application Server.

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

Category: Elevation Of Privilege
Description: Internal Workstation may be able to remotely execute code for Application Server.
Justification: The Trust Boundary must be adjusted to exclude the connection between the Internal Workstation and the Application Server.

27. Elevation Using Impersonation [State: Needs Investigation] [Priority: Medium]

Category: Elevation Of Privilege
Description: Application Server may be able to impersonate the context of Internal Workstation in order to gain additional privilege.
Justification: There must be a stronger Authenticating System available to avoid this threat.

28. Data Flow Encrypted Network Traffic 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: The Trust Boundary must be adjusted to exclude the connection between the Internal Workstation and the Application Server.

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

Category: Denial Of Service

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

Justification: The Trust Boundary must be adjusted to exclude the connection between the Internal Workstation and the Application Server.

30. 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: The Authentication Process should be replaced with a stronger process in the Internal Workstation.

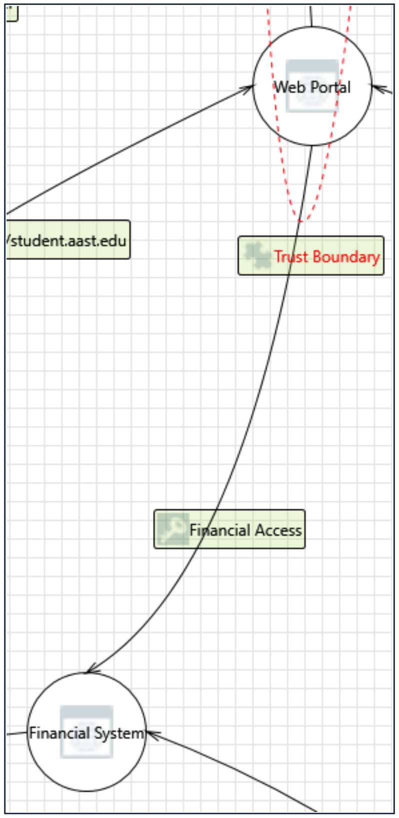
31. Potential Data Repudiation by Application Server [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Application 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: The Trust Boundary must be adjusted to exclude the connection between the Internal Workstation and the Application Server.

Interaction: Financial Access



32. Weak Authentication Scheme [State: Needs Investigation] [Priority: Medium]

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: Web Portal should use a stronger Authentication System.

33. Web Portal Process Memory Tampered [State: Needs Investigation] [Priority: Medium]

Category: Tampering

Description: If Web Portal is given access to memory, such as shared memory or pointers, or is given the ability to control what Financial System executes (for example, passing back a function pointer.), then Web Portal can tamper with Financial System. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: Tampering is solved by applying Integrity, the connection used is HTTPS which supports this feature, but a stronger way of implementation is required.

34. Elevation Using Impersonation [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

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

Justification: The Financial System is the core system of this environment, since the Web Portal uses it to power itself.

35. Elevation by Changing the Execution Flow in Financial System [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Financial System in order to change the flow of program execution within Financial System to the attacker's choosing.
Justification: Adjust the Trust Boundary between the Web Portal &amp; the DMZ Data Center to exclude the Financial Access Data Flow.

36. Financial System 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 Financial System.
Justification: Adjust the Trust Boundary between the Web Portal &amp; the DMZ Data Center to exclude the Financial Access Data Flow.

37. Data Flow Financial Access 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: Adjust the Trust Boundary between the Web Portal &amp; the DMZ Data Center to exclude the Financial Access Data Flow.

38. Potential Process Crash or Stop for Financial System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Financial System crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Adjust the Trust Boundary between the Web Portal &amp; the DMZ Data Center to exclude the Financial Access Data Flow.

39. Potential Data Repudiation by Financial System [State: Mitigation Implemented] [Priority: Medium]

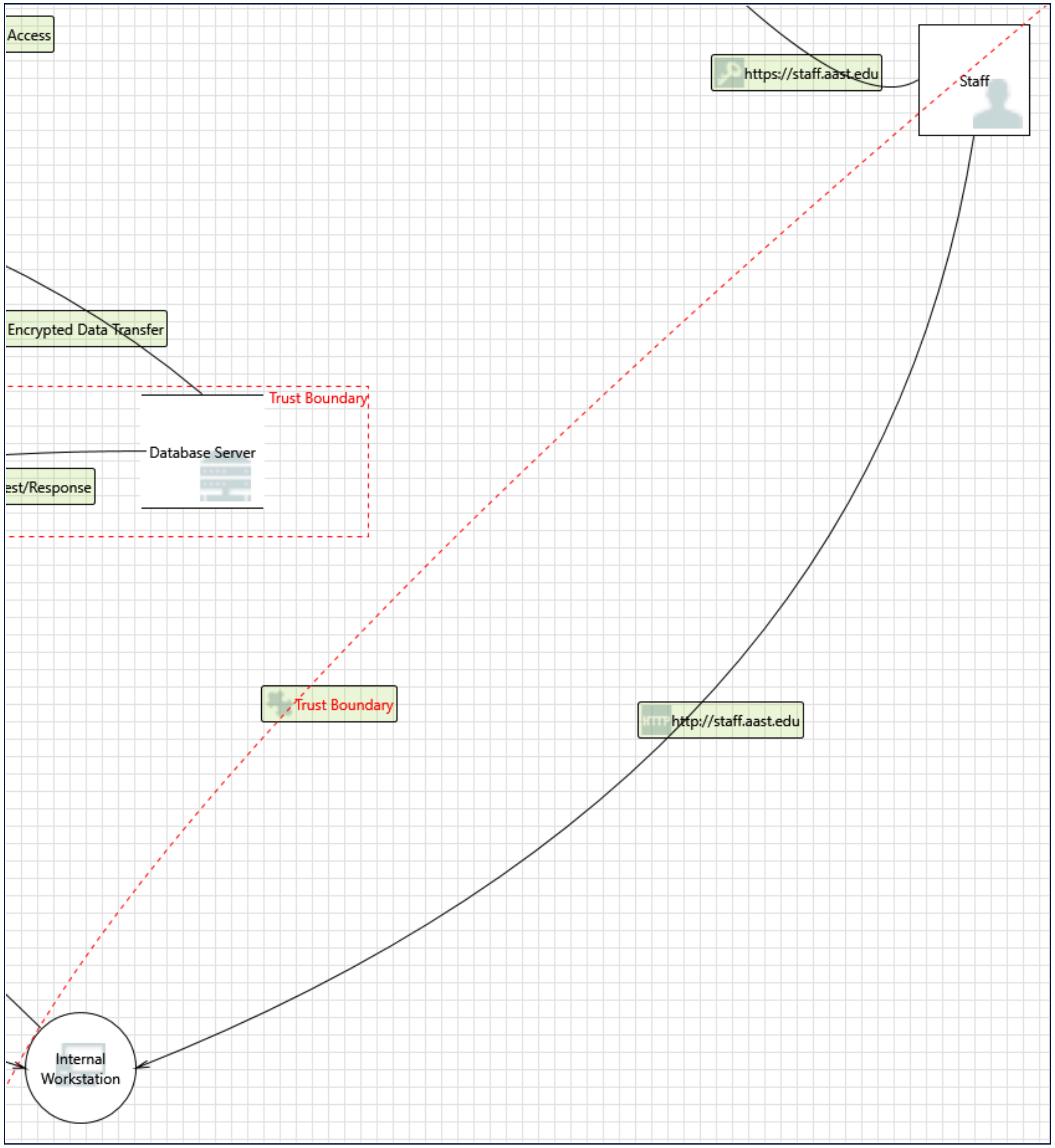
Category: Repudiation
Description: Financial System claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Adjust the Trust Boundary between the Web Portal &amp; the DMZ Data Center to exclude the Financial Access Data Flow.

40. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: Medium]

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: The Financial Access Data Flow must not trust the Web Portal to prevent CSRF.

- Source Authenticated (No)

Interaction: http://staff.aast.edu



41. Elevation Using Impersonation [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege
Description: Internal Workstation may be able to impersonate the context of Staff in order to gain additional privilege.
Justification: This won&#39;t happen because the Internal Workstation is secured by the university.

42. Spoofing the Staff External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Staff may be spoofed by an attacker and this may lead to unauthorized access to Internal Workstation. Consider using a standard authentication mechanism to identify the external entity.

Justification: Staff User must be authenticated inside the University.

Staff Entity -&gt; Authenticates itself (Yes)

43. Spoofing the Internal Workstation Process [State: Mitigation Implemented] [Priority: Medium]

Category: Spoofing

Description: Internal Workstation may be spoofed by an attacker and this may lead to information disclosure by Staff. Consider using a standard authentication mechanism to identify the destination process.

Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Spoofing.

44. Potential Lack of Input Validation for Internal Workstation [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across http://staff.aast.edu may be tampered with by an attacker. This may lead to a denial of service attack against Internal Workstation or an elevation of privilege attack against Internal Workstation or an information disclosure by Internal Workstation. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Tampering.

45. Potential Data Repudiation by Internal Workstation [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: Internal Workstation 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 Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Repudiation.

46. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across http://staff.aast.edu may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Information Disclosure.

47. Potential Process Crash or Stop for Internal Workstation [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

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

Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Denial Of Service.

48. Data Flow http://staff.aast.edu Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Medium]

Category: Denial Of Service

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

Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Denial Of Service.

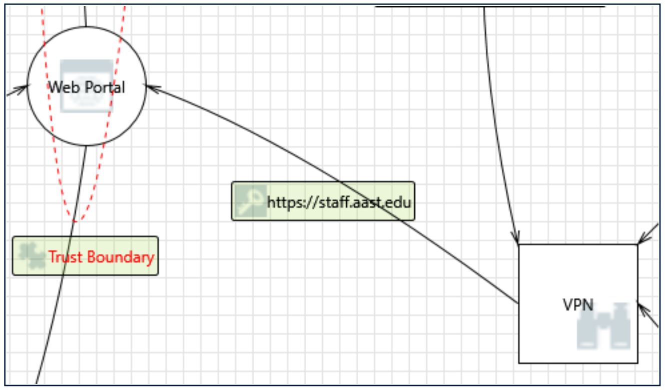
49. Internal Workstation May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege
Description: Staff may be able to remotely execute code for Internal Workstation.
Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Elevation Of Privilege.

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

Category: Elevation Of Privilege
Description: An attacker may pass data into Internal Workstation in order to change the flow of program execution within Internal Workstation to the attacker's choosing.
Justification: The Trust Boundary must be adjusted to include the Internal Workstation entity to prevent Elevation Of Privilege.

Interaction: https://staff.aast.edu



51. Spoofing the VPN External Entity [State: Mitigation Implemented] [Priority: High]

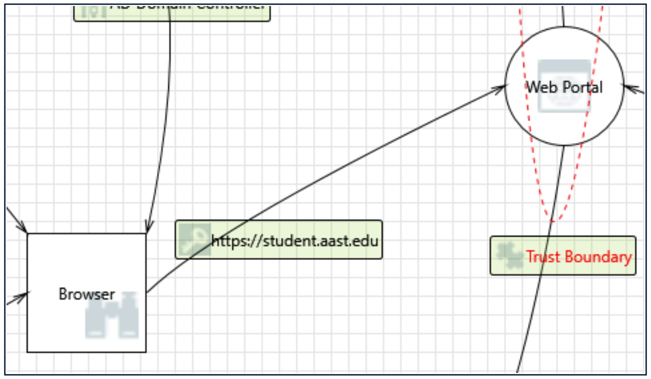
Category: Spoofing
Description: VPN may be spoofed by an attacker and this may lead to unauthorized access to Web Portal. Consider using a standard authentication mechanism to identify the external entity.
Justification: The Staff User must use a trusted &amp; a secure VPN service to avoid the mentioned threat.

1- Authenticates Itself (Yes)
2- Staff must work through a HTTPS connection

52. Elevation Using Impersonation [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege
Description: Web Portal may be able to impersonate the context of VPN in order to gain additional privilege.
Justification: The Web Portal System is under the university&#39;s control.

Interaction: https://student.aast.edu



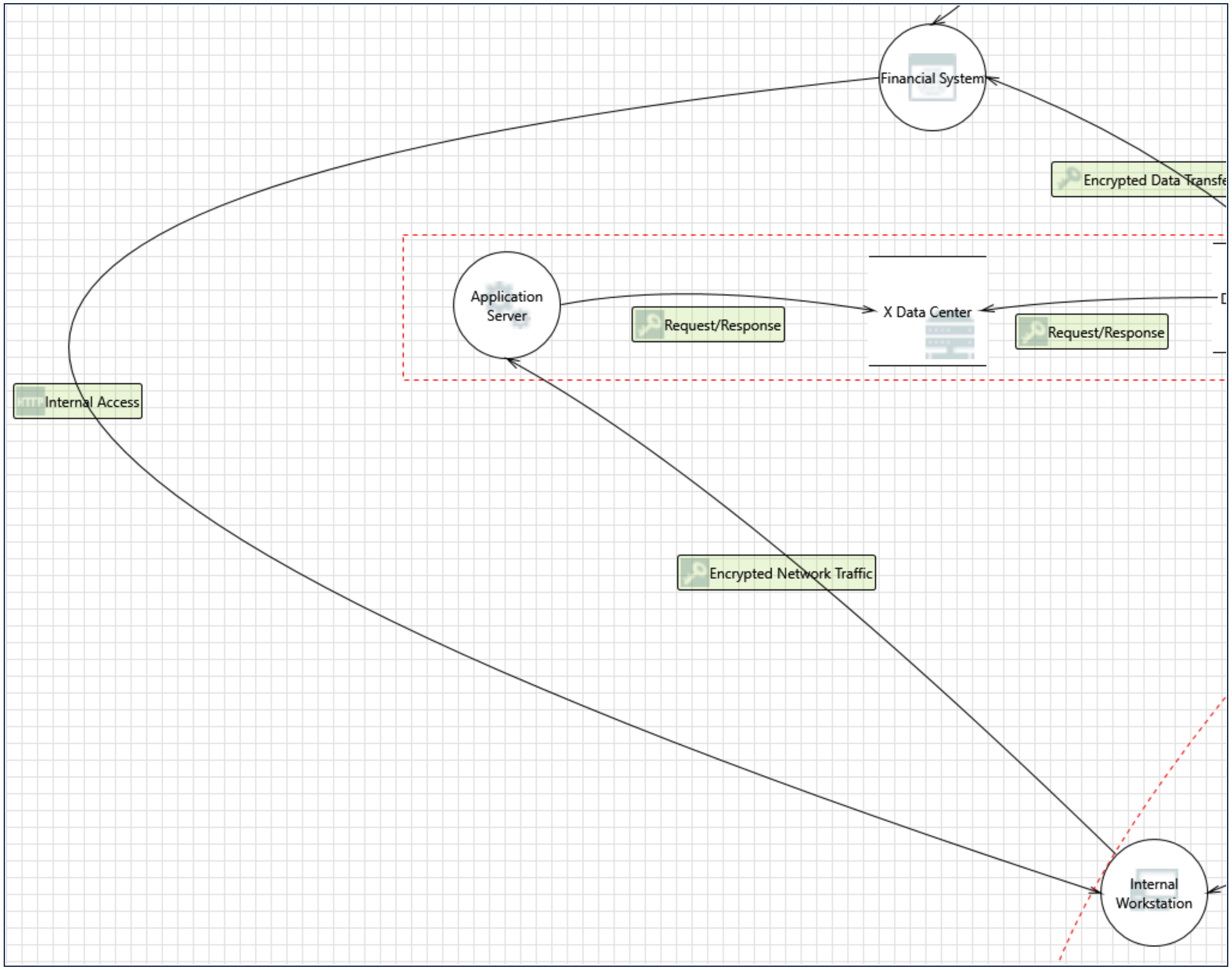
53. Elevation Using Impersonation [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

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

Justification: The Web Portal System is under the university&#39;s control.

Interaction: Internal Access



54. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Internal Access may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: Change the connection from HTTP to HTTPS when connecting the Internal Workstation to the Financial System.

55. Potential Lack of Input Validation for Internal Workstation [State: Mitigation Implemented] [Priority: Low]

Category: Tampering

Description: Data flowing across Internal Access may be tampered with by an attacker. This may lead to a denial of service attack against Internal Workstation or an elevation of privilege attack against Internal Workstation or an information disclosure by Internal Workstation. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: Change the connection from HTTP to HTTPS when connecting the Internal Workstation to the Financial System.

56. Spoofing the Internal Workstation Process [State: Mitigation Implemented] [Priority: Medium]

Category: Spoofing

Description: Internal Workstation may be spoofed by an attacker and this may lead to information disclosure by Financial System. Consider using a standard authentication mechanism to identify the destination process.

Justification: Change the connection from HTTP to HTTPS when connecting the Internal Workstation to the Financial System.

57. Elevation by Changing the Execution Flow in Internal Workstation [State: Mitigation Implemented] [Priority: Medium]

Category: Elevation Of Privilege

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

Justification: The Internal Workstation must go out of the Trust Boundary to check it&#39;s identity and data output.

58. Weak Authentication Scheme [State: Needs Investigation] [Priority: Medium]

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: The Authentication System used isn&#39;t enough to avoid this threat, a stronger scheme is needed.

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

Category: Elevation Of Privilege

Description: Financial System may be able to remotely execute code for Internal Workstation.

Justification: The Internal Workstation must go out of the Trust Boundary to check it&#39;s identity and data output.

60. Data Flow Internal Access Is Potentially Interrupted [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

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

Justification: The Internal Workstation must go out of the Trust Boundary to check it&#39;s identity and data output.

61. Elevation Using Impersonation [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

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

Justification: The Financial System doesn&#39;t accept elevations.

62. Potential Process Crash or Stop for Internal Workstation [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

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

Justification: The Internal Workstation must go out of the Trust Boundary to check it&#39;s identity and data output.

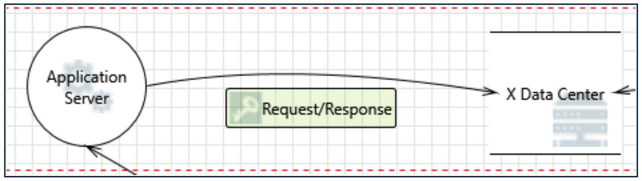
63. Potential Data Repudiation by Internal Workstation [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: Internal Workstation 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 Internal Workstation must go out of the Trust Boundary to check it&#39;s identity and data output.

Interaction: Request/Response



64. Potential Excessive Resource Consumption for Application Server or X Data Center [State: Needs Investigation] [Priority: Medium]

Category: Denial Of Service

Description: Does Application Server or X Data Center 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: There is a backup option enables to prevent this type of attack but a stronger way of providing Availability is needed.

65. Weak Credential Storage [State: Needs Investigation] [Priority: Medium]

Category: Information Disclosure

Description: Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored

Justification: The HTTPS connection used provides confidentiality but this isn&#39;t enough to avoid an Information Disclosure attack.

66. Potential Weak Protections for Audit Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect

Justification: The Data Center should either store log files securely or discard them preventing this type of attack.

67. Insufficient Auditing [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.

Justification: The Data Center should either store log files securely or discard them preventing type of attack.

68. Data Logs from an Unknown Source [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.
Justification: The Data Center should either store log files securely or discard them preventing this type of attack.

69. Lower Trusted Subject Updates Logs [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.
Justification: The Data Center should either store log files securely or discard them preventing this type of attack.

70. Risks from Logging [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.
Justification: The Data Center should either store log files securely or discard them preventing this type of attack.

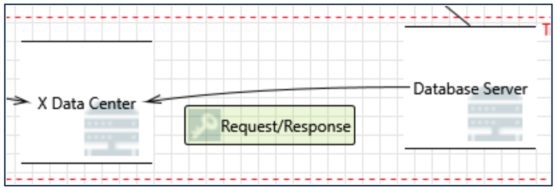
71. Spoofing of Destination Data Store X Data Center [State: Needs Investigation] [Priority: Medium]

Category: Spoofing
Description: X Data Center may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of X Data Center. Consider using a standard authentication mechanism to identify the destination data store.
Justification: A stronger authentication method is needed.

72. Authorization Bypass [State: Mitigation Implemented] [Priority: Low]

Category: Information Disclosure
Description: Can you access X Data Center 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: Application Server -&gt; Authorization System must be disabled.

Interaction: Request/Response



73. Spoofing of Destination Data Store X Data Center [State: Needs Investigation] [Priority: Medium]

Category: Spoofing
Description: X Data Center may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of X Data Center. Consider using a standard authentication mechanism to identify the destination data store.
Justification: A stronger Authentication Method is required.

74. Spoofing of Source Data Store Database Server [State: Needs Investigation] [Priority: Medium]

Category: Spoofing

Description: Database Server may be spoofed by an attacker and this may lead to incorrect data delivered to X Data Center. Consider using a standard authentication mechanism to identify the source data store.

Justification: A stronger Authentication Method is required.