Threat Modeling Report

Created on 10/20/2019 11:30:12 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	21
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	22
Total Migrated	0

Diagram: Diagram 1

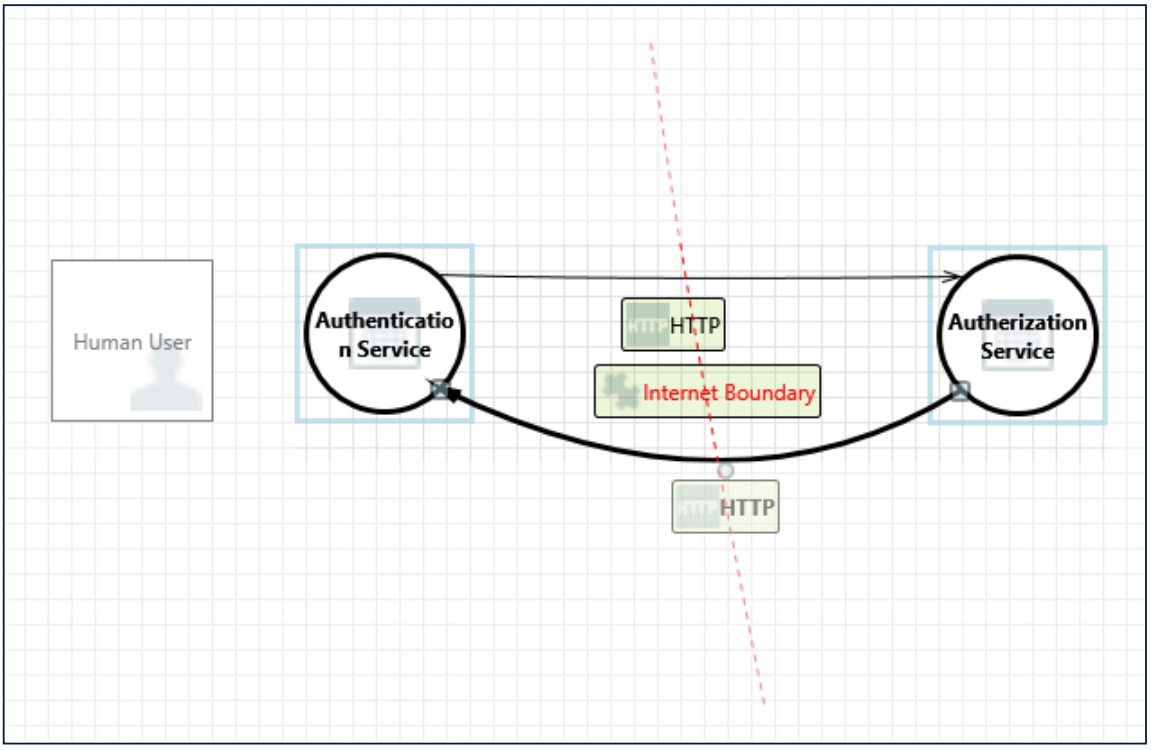
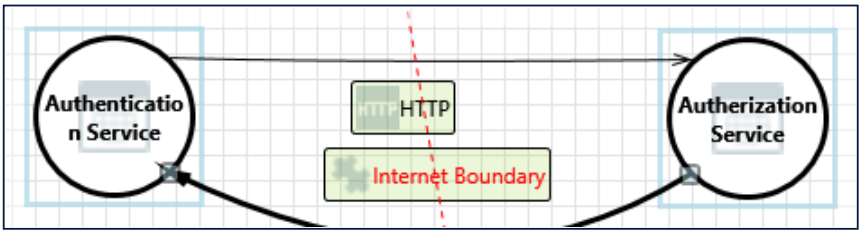


Diagram 1 Diagram Summary:

Not Started	21
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	1
Total	22
Total Migrated	0

Interaction: HTTP



1. Authentication Service Process Memory Tampered [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: If Authentication Service is given access to memory, such as shared memory or pointers, or is given the ability to control what Autherization Service executes (for example, passing back a function pointer.), then Authentication Service can tamper with Autherization Service. 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: <no mitigation provided>

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

Category: Elevation Of Privilege

Description: Autherization Service may be able to impersonate the context of Authentication Service in order to gain additional privilege.

Justification: <no mitigation provided>

3. Spoofing the Authentication Service Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Authentication Service may be spoofed by an attacker and this may lead to unauthorized access to Autherization Service. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

4. Spoofing the Autherization Service Process [State: Not Started] [Priority: High]

Category: Spoofing

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

Justification: <no mitigation provided>

5. Potential Lack of Input Validation for Autherization Service [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Autherization Service or an elevation of privilege attack against Autherization Service or an information disclosure by Autherization Service. 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: <no mitigation provided>

6. Potential Data Repudiation by Autherization Service [State: Not Started] [Priority: High]

Category: Repudiation

Description: Autherization Service 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: <no mitigation provided>

7. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Data flowing across HTTP 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: <no mitigation provided>

8. Potential Process Crash or Stop for Autherization Service [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

9. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

10. Autherization Service May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Authentication Service may be able to remotely execute code for Autherization Service.

Justification: <no mitigation provided>

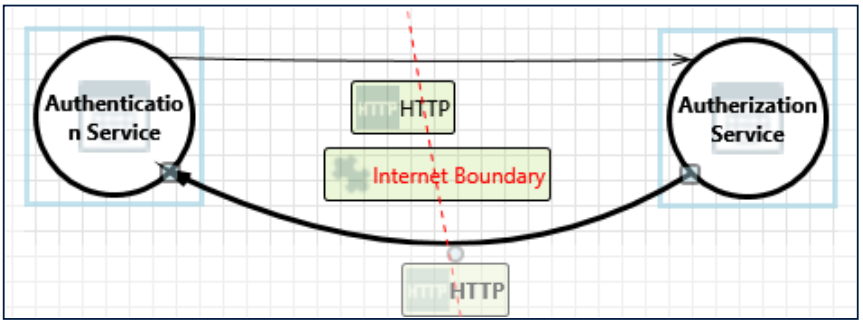
11. Elevation by Changing the Execution Flow in Autherization Service [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

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

Justification: <no mitigation provided>

Interaction: HTTP



12. Autherization Service Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering

Description: If Autherization Service is given access to memory, such as shared memory or pointers, or is given the ability to control what Authentication Service executes (for example, passing back a function pointer.), then Autherization Service can tamper with Authentication Service. 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: <no mitigation provided>

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

Category: Elevation Of Privilege

Description: Authentication Service may be able to impersonate the context of Autherization Service in order to gain additional privilege.

Justification: <no mitigation provided>

14. Spoofing the Autherization Service Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Autherization Service may be spoofed by an attacker and this may lead to unauthorized access to Authentication Service. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

15. Spoofing the Authentication Service Process [State: Not Started] [Priority: High]

Category: Spoofing

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

Justification: <no mitigation provided>

16. Potential Lack of Input Validation for Authentication Service [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Authentication Service or an elevation of privilege attack against Authentication Service or an information disclosure by Authentication Service. 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: <no mitigation provided>

17. Potential Data Repudiation by Authentication Service [State: Not Started] [Priority: High]

Category: Repudiation

Description: Authentication Service 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: <no mitigation provided>

18. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Data flowing across HTTP 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: <no mitigation provided>

19. Potential Process Crash or Stop for Authentication Service [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

20. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

21. Authentication Service May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Autherization Service may be able to remotely execute code for Authentication Service.

Justification: <no mitigation provided>

22. Elevation by Changing the Execution Flow in Authentication Service [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

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

Justification: <no mitigation provided>