Threat Modeling Report

Created on 11/11/2021 2:56:18 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	18
Needs Investigation	0
Mitigation Implemented	14
Total	32
Total Migrated	0

Diagram: Diagram 1

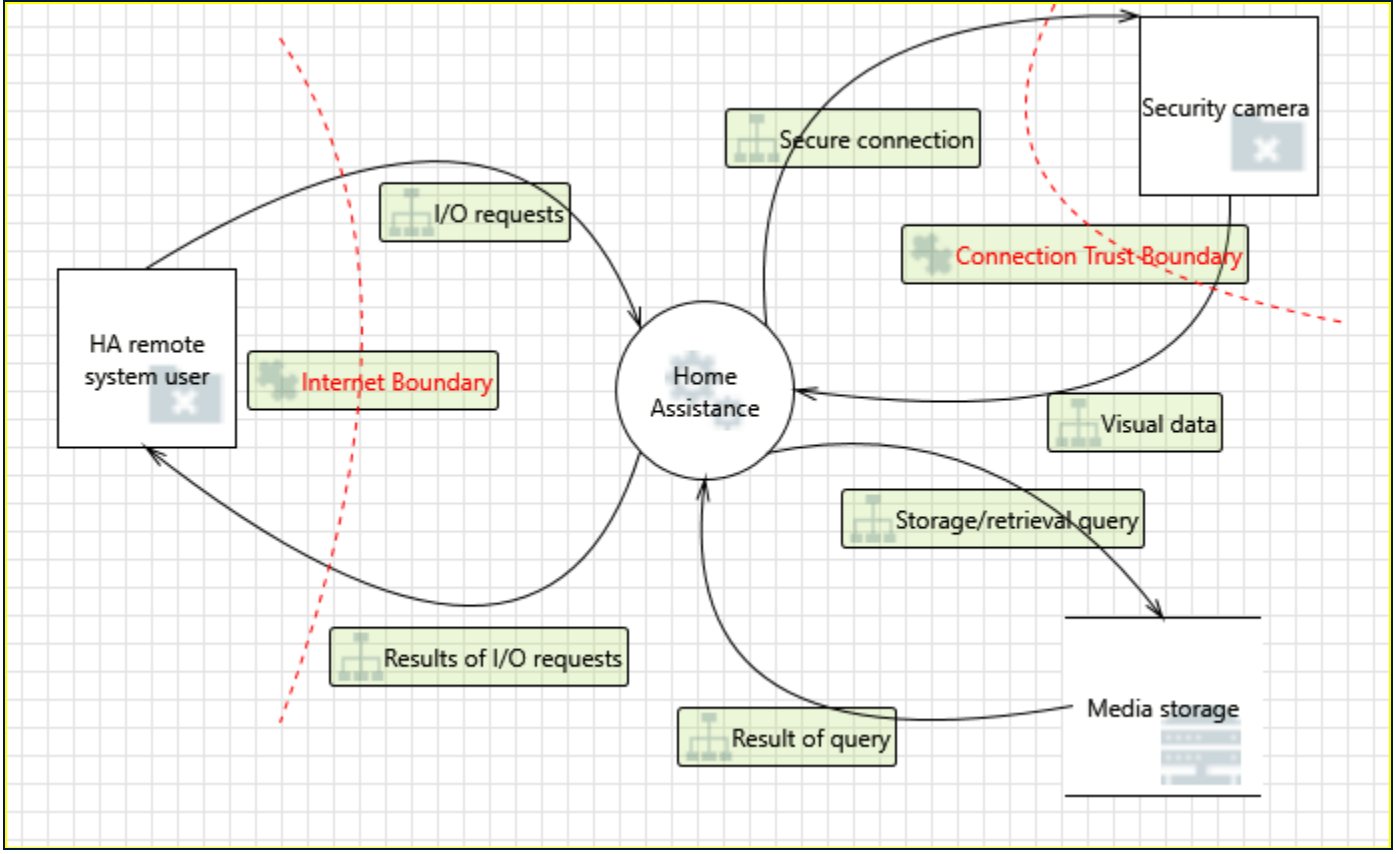
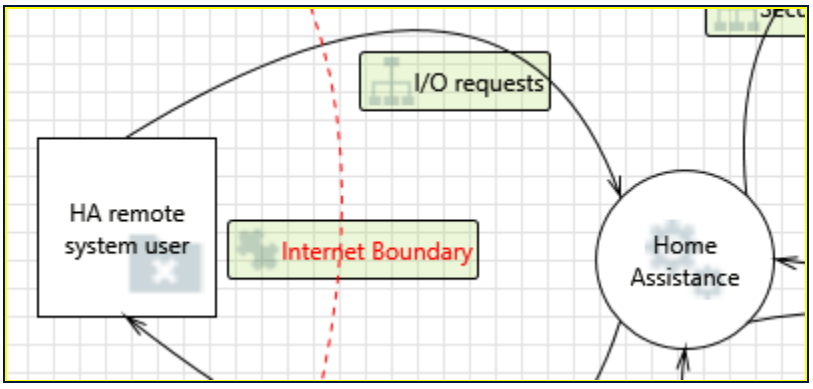


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	18
Needs Investigation	0
Mitigation Implemented	14
Total	32
Total Migrated	0

Interaction: I/O requests



1. Spoofing the HA remote system user External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: HA remote system user may be spoofed by an attacker and this may lead to unauthorized access to Home Assistance. Consider using a standard authentication mechanism to identify the external entity.

Justification: Remote user is authenticated

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

Category: Elevation Of Privilege

Description: Home Assistance may be able to impersonate the context of HA remote system user in order to gain additional privilege.

Justification: HA remote system user is authenticated

3. Spoofing the Home Assistance Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Home Assistance may be spoofed by an attacker and this may lead to information disclosure by HA remote system user. Consider using a standard authentication mechanism to identify the destination process.

Justification: HA has authorized access to security camera device

4. Potential Lack of Input Validation for Home Assistance [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across I/O requests may be tampered with by an attacker. This may lead to a denial of service attack against Home Assistance or an elevation of privilege attack against Home Assistance or an information disclosure by Home Assistance. 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>

5. Potential Data Repudiation by Home Assistance [State: Not Applicable] [Priority: High]

Category: Repudiation

Description: Home Assistance 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>

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

Category: Information Disclosure

Description: Data flowing across I/O requests 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: dataflow is encrypted using VPN tunneling

7. Potential Process Crash or Stop for Home Assistance [State: Not Applicable] [Priority: High]

Category: Denial Of Service
Description: Home Assistance crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: <no mitigation provided>

8. Data Flow I/O requests 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: Secured by trust boundaries

9. Home Assistance May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: HA remote system user may be able to remotely execute code for Home Assistance.
Justification: <no mitigation provided>

10. Elevation by Changing the Execution Flow in Home Assistance [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Home Assistance in order to change the flow of program execution within Home Assistance to the attacker's choosing.
Justification: <no mitigation provided>

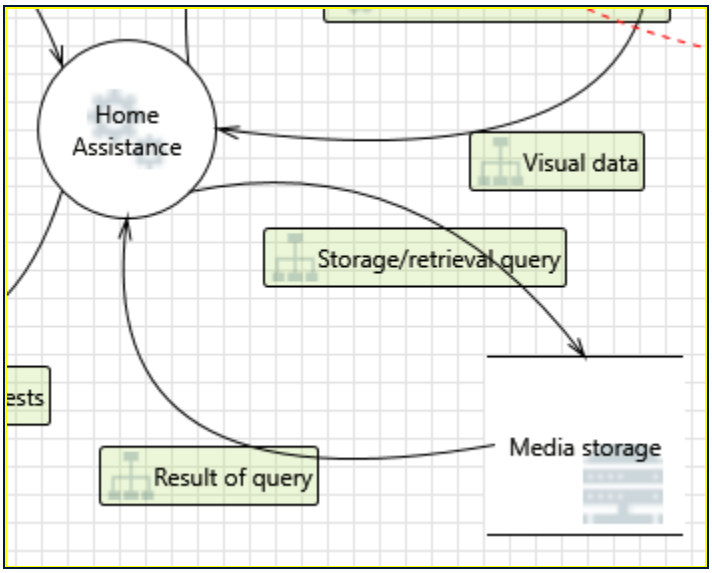
11. Cross Site Request Forgery [State: Not Applicable] [Priority: High]

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: <no mitigation provided>

Interaction: Result of query



12. Spoofing of Source Data Store Media storage [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Media storage may be spoofed by an attacker and this may lead to incorrect data delivered to Home Assistance. Consider using a standard authentication mechanism to identify the source data store.

Justification: Media storage is secured within HA application

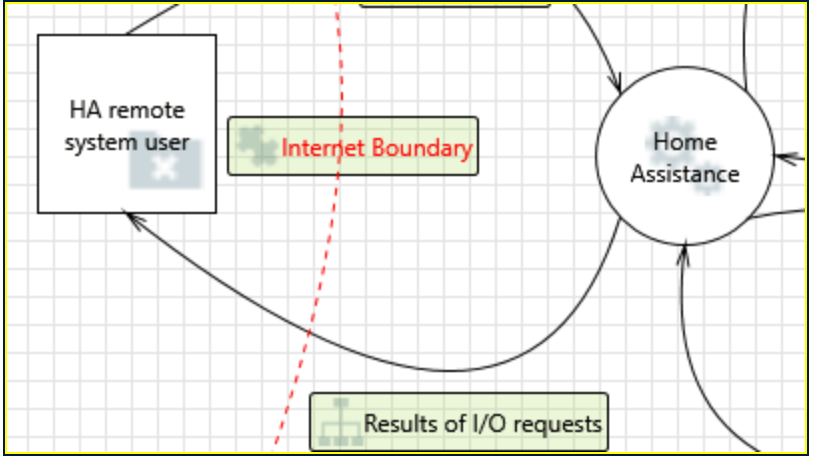
13. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

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

Justification: HA system is authrized to access database.

Interaction: Results of I/O requests



14. Spoofing of the HA remote system user External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	HA remote system user may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of HA remote system user. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Remote user is authenticated

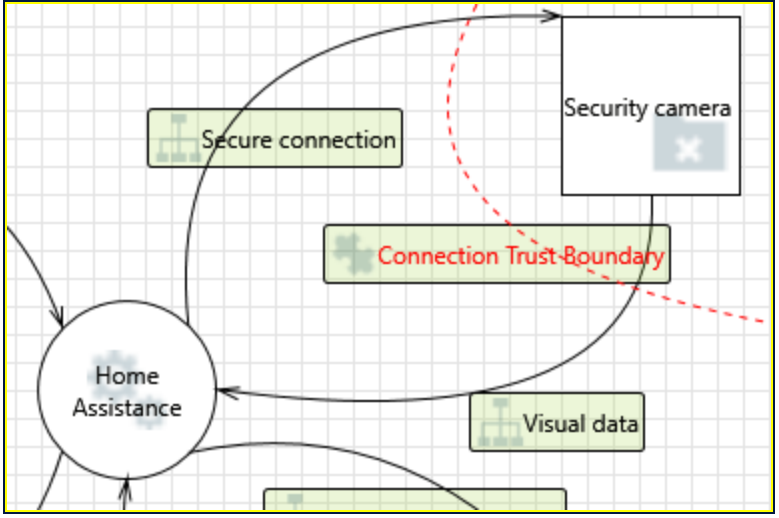
15. External Entity HA remote system user Potentially Denies Receiving Data [State: Not Applicable] [Priority: High]

Category:	Repudiation
Description:	HA remote system 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:	<no mitigation provided>

16. Data Flow Results of I/O requests Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	<no mitigation provided>

Interaction: Secure connection



17. Data Flow secure connection Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	<no mitigation provided>

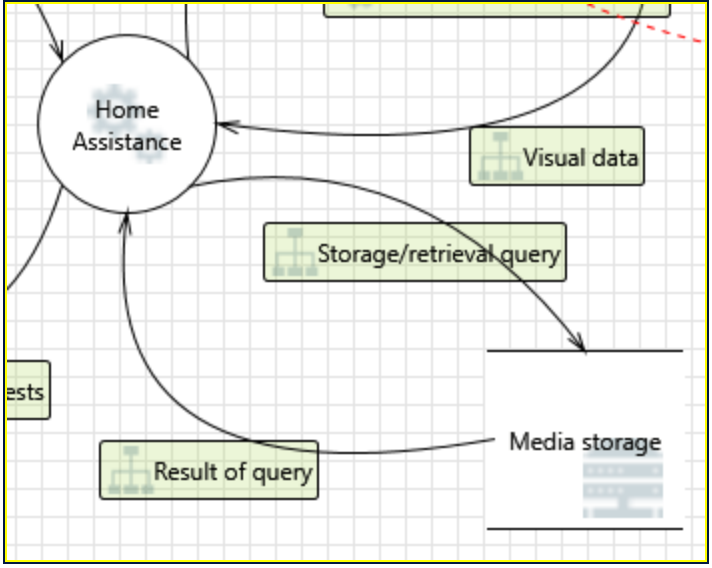
18. External Entity security camera Potentially Denies Receiving Data [State: Not Applicable] [Priority: High]

Category:	Repudiation
Description:	security camera 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:	<no mitigation provided>

19. Spoofing of the security camera External Destination Entity [State: Not Applicable] [Priority: High]

Category:	Spoofing
Description:	security camera may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of security camera . Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>

Interaction: Storage/retrieval query



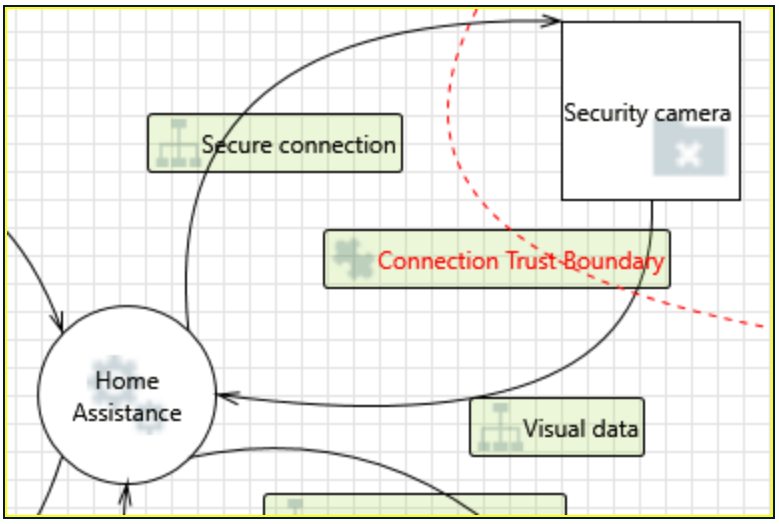
20. Spoofing of Destination Data Store Media storage [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Media storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Media storage. Consider using a standard authentication mechanism to identify the destination data store.
Justification:	Media storage is secure within HA application

21. Potential Excessive Resource Consumption for Home Assistance or Media storage [State: Not Applicable] [Priority: High]

Category:	Denial Of Service
Description:	Does Home Assistance or Media storage 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>

Interaction: Visual data



22. Spoofing the security camera External Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	security camera may be spoofed by an attacker and this may lead to unauthorized access to Home Assistance. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Connection trust boundary is placed between HA and Security camera device.

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

Category:	Elevation Of Privilege
Description:	Home Assistance may be able to impersonate the context of security camera in order to gain additional privilege.
Justification:	Connection trust boundary is placed between HA and security camera device.

24. Spoofing the Home Assistance Process [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Home Assistance may be spoofed by an attacker and this may lead to information disclosure by security camera . Consider using a standard authentication mechanism to identify the destination process.
Justification:	Connection is secured

25. Potential Lack of Input Validation for Home Assistance [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	Data flowing across Visual data may be tampered with by an attacker. This may lead to a denial of service attack against Home Assistance or an elevation of privilege attack against Home Assistance or an information disclosure by Home Assistance. 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>

26. Potential Data Repudiation by Home Assistance [State: Not Applicable] [Priority: High]

Category:	Repudiation
Description:	Home Assistance 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>

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

Category: Information Disclosure

Description: Data flowing across Visual data 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: Data flow is secured and encrypted

28. Potential Process Crash or Stop for Home Assistance [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

29. Data Flow Visual data Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: <no mitigation provided>

30. Home Assistance May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: security camera may be able to remotely execute code for Home Assistance.

Justification: <no mitigation provided>

31. Elevation by Changing the Execution Flow in Home Assistance [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

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

Justification: Connection is secured

32. Cross Site Request Forgery [State: Not Applicable] [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: <no mitigation provided>