Threat Modeling Report

Created on 11/15/2021 8:28:20 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

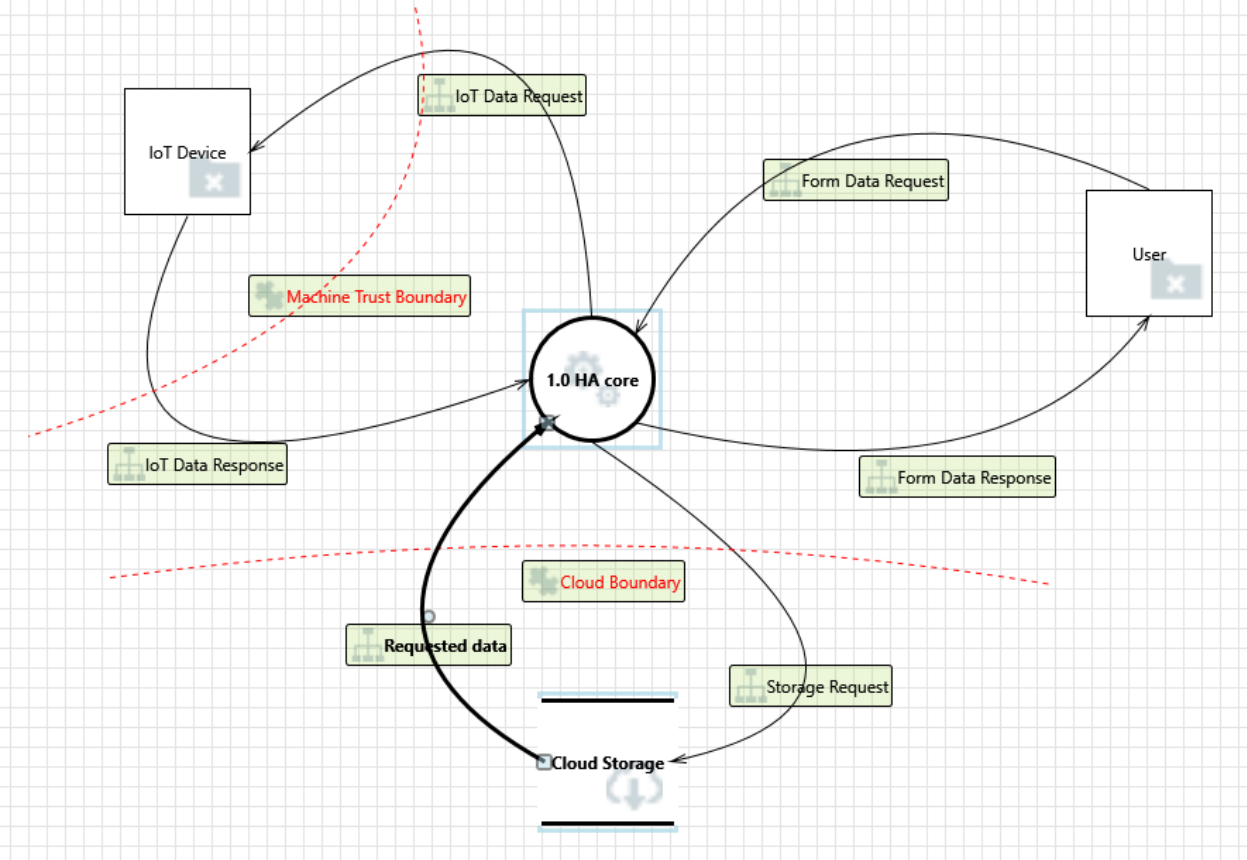
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	20
Needs Investigation	0
Mitigation Implemented	12
Total	32
Total Migrated	0

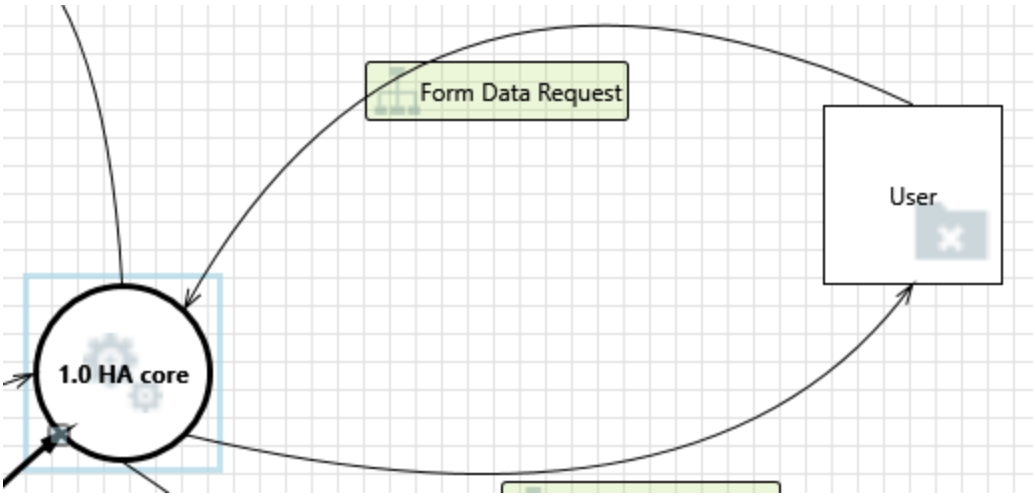
Diagram: DFD Level 1.3 IoT



DFD Level 1.3 IoT Diagram Summary:

Not Started	0
Not Applicable	20
Needs Investigation	0
Mitigation Implemented	12
Total	32
Total Migrated	0

Interaction: Form Data Request



1. Spoofing the User External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: User is authenticated using a standard username/password combination. Timeout counter. Authentication is available, https://www.home-assistant.io/docs/authentication.

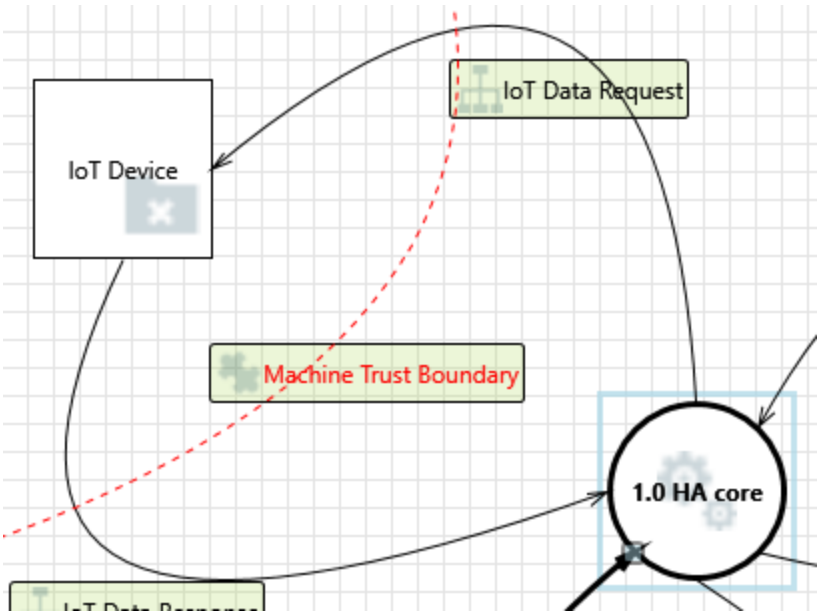
2. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

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

Justification: HA core is trusted system. Not applicable.

Interaction: IoT Data Request



3. Spoofing of the IoT Device External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	IoT Device may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of IoT Device. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Check for standard authentication mechanism. Many IoT devices like EcoBee have registration and authentication for the devices on their site.

4. External Entity IoT Device Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category:	Repudiation
Description:	IoT Device 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:	Check if logging and auditing record is kept. Data logging from both the core and IoT devices is available with the logger integration, https://www.home-assistant.io/integrations/logger.

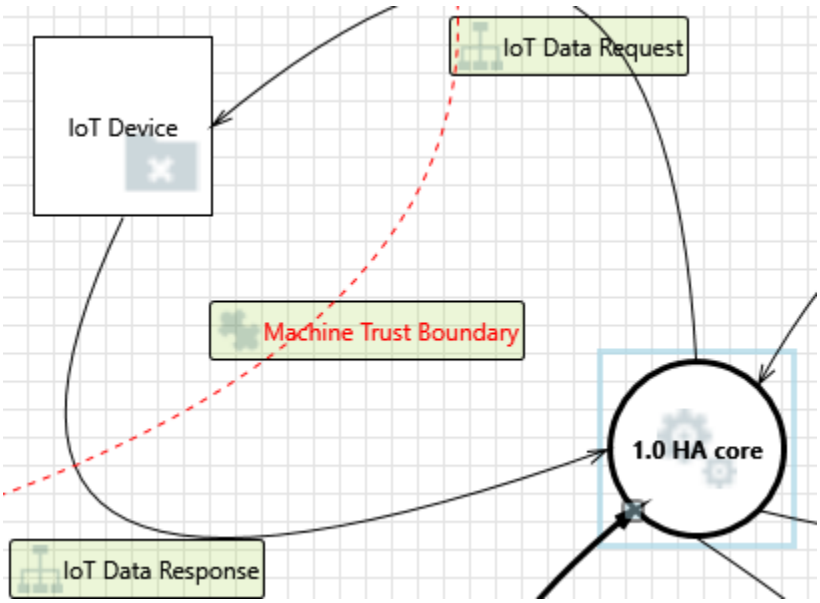
5. Data Flow IoT Data Request Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category:	Denial Of Service

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

Justification: Iot device are connected through secured connection. Not applicable.

Interaction: IoT Data Response



6. Spoofing the HA core Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: HA core may be spoofed by an attacker and this may lead to information disclosure by IoT Device. Consider using a standard authentication mechanism to identify the destination process.

Justification: To spoof an already installed application the attacker would need admin rights to HA Core. Authentication is available on HA https://www.home-assistant.io/docs/authentication/.

7. Spoofing the IoT Device External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: IoT Device may be spoofed by an attacker and this may lead to unauthorized access to HA core. Consider using a standard authentication mechanism to identify the external entity.

Justification: Many IoT devices like EcoBee have registration and authentication for the devices on their site.

8. Potential Lack of Input Validation for HA core [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across IoT Data Response may be tampered with by an attacker. This may lead to a denial of service attack against HA core or an elevation of privilege attack against HA core or an information disclosure by HA core. 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: Input is verified as Iot device is connected through secured network. Not applicable

9. Potential Data Repudiation by HA core [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: HA core 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: Check for logging and audit. Data logging from both the core and IoT devices is available with the logger integration, https://www.home-assistant.io/integrations/logger.

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

Category: Information Disclosure

Description: Data flowing across IoT Data Response 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: Check if dataflow is encrypted. Dependent upon the IoT device encryption mechanism. Dataflow with example device EcoBee is always encrypted. The device also manages vulnerabilites.

11. Potential Process Crash or Stop for HA core [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: HA core uses IoT device whenever requested. Prevent excess disk or CPU consumption.

12. Data Flow IoT Data Response 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: Secured with machine trust boundary. Not applicable

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

Category: Elevation Of Privilege
Description: HA core may be able to impersonate the context of IoT Device in order to gain additional privilege.
Justification: HA core is secure system. Not applicable

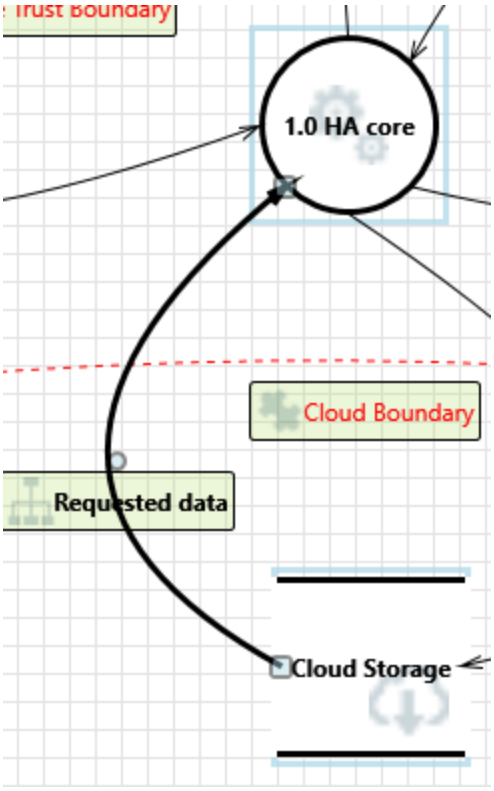
14. HA core May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: IoT Device may be able to remotely execute code for HA core.
Justification: IoT devices are connected over secure network. HA should not allow IoT devices more than the least amount of privilge required.

15. Elevation by Changing the Execution Flow in HA core [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into HA core in order to change the flow of program execution within HA core to the attacker's choosing.
Justification: IoT devices are connected over secured network. HA should not allow IoT devices more than the least amount of privilege required.

Interaction: Requested data



16. Spoofing the HA core Process [State: Not Applicable] [Priority: High]

Category:	Spoofing
Description:	HA core may be spoofed by an attacker and this may lead to information disclosure by Cloud Storage. Consider using a standard authentication mechanism to identify the destination process.
Justification:	To spoof an already installed application the attacker would need admin rights to HA Core. Not Applicable.

17. Spoofing of Source Data Store Cloud Storage [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Cloud Storage may be spoofed by an attacker and this may lead to incorrect data delivered to HA core. Consider using a standard authentication mechanism to identify the source data store.
Justification:	Check for authentication. Home Assistant Cloud is done using NabuCasa, all data is encrypted and credentials are set up with NabuCasa, https://www.nabucasa.com/config/remote/.

18. Potential Data Repudiation by HA core [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: HA core 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: Check for logging and audit. Data logging from both the core and IoT devices is available with the logger integration, https://www.home-assistant.io/integrations/logger.

19. Weak Access Control for a Resource [State: Not Applicable] [Priority: High]

Category: Information Disclosure

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

Justification: Secured and authorized cloud settings are used. Data Encryption is vital.

20. Potential Process Crash or Stop for HA core [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: HA is secured system. Prevent excess disk or CPU consumption.

21. Data Flow Requested 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: Trusted cloud boundary is present. Firewalls mitigate this.

22. Data Store Inaccessible [State: Not Applicable] [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: Secure cloud is used. Firewalls mitigate this.

23. HA core May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Cloud Storage may be able to remotely execute code for HA core.

Justification: Secure cloud is used. HA should not allow cloud more than the least amount of privilege required.

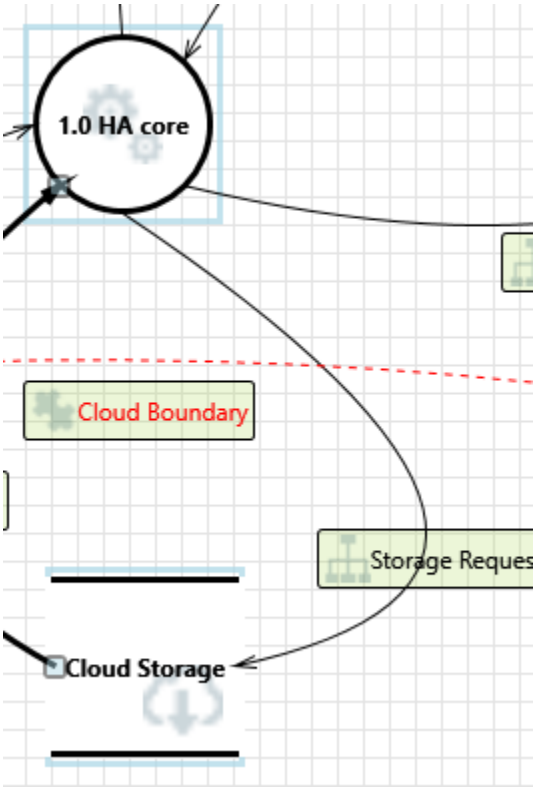
24. Elevation by Changing the Execution Flow in HA core [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

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

Justification: Connection is secured with cloud boundary. HA should not allow cloud more than the least amount of privilege required.

Interaction: Storage Request



25. Spoofing the HA core Process [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: HA core may be spoofed by an attacker and this may lead to unauthorized access to Cloud Storage. Consider using a standard authentication mechanism to identify the source process.

Justification: To spoof an already installed application the attacker would need admin rights to HA Core. Not Applicable.

26. Spoofing of Destination Data Store Cloud Storage [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Check for authentication. Home Assistant Cloud is done using NabuCasa, all data is encrypted and credentials are set up with NabuCasa, https://www.nabucasa.com/config/remote/. Data logging from both the core and IoT devices is available with the logger integration, https://www.home-assistant.io/integrations/logger.

27. The Cloud Storage Data Store Could Be Corrupted [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across Storage Request may be tampered with by an attacker. This may lead to corruption of Cloud Storage. Ensure the integrity of the data flow to the data store.

Justification: To tamper with Storage Request as it connects to an installed application the attacker would already need admin rights on the machine that HA Core is runnign on. Not applicable.

28. Data Store Denies Cloud Storage Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Cloud Storage 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: Check for the logging or auditing. Home Assistant Cloud is done using NabuCasa, all data is encrypted and credentials are set up with NabuCasa, https://www.nabucasa.com/config/remote/. Data logging from both the core and IoT devices is available with the logger integration, https://www.home-assistant.io/integrations/logger.

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

Category: Information Disclosure

Description: Data flowing across Storage Request 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: Check for encryption. Encryption can be set up with the Let's Encrypt integration.

30. Potential Excessive Resource Consumption for HA core or Cloud Storage [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Does HA core or Cloud 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: Secure cloud is used.

31. Data Flow Storage Request 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: Secured cloud boundary is present.

32. Data Store Inaccessible [State: Not Applicable] [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: data is stored at secured cloud.