Threat Modeling Report

Created on 11/11/2021 3:36:03 PM

Threat Model Name:
Owner:
Reviewer:
Contributors:
Description:
Assumptions:
External Dependencies:

Notes:

Id	Note	Date	Added By
2	https://developers.home-assistant.io/docs/config_entries_index/	11/9/2021 8:51:40 AM	UNL-AD\nzetocha2
3	https://www.home-assistant.io/integrations/alert/	11/9/2021 8:51:45 AM	UNL-AD\nzetocha2
4	https://developers.home-assistant.io/docs/config_entries_options_flow_handler/	11/9/2021 8:51:55 AM	UNL-AD\nzetocha2
5	https://developers.home-assistant.io/docs/integration_fetching_data/	11/9/2021 8:52:00 AM	UNL-AD\nzetocha2

Threat Model Summary:

Not Started	0
Not Applicable	2
Needs Investigation	0
Mitigation Implemented	4
Total	6
Total Migrated	0

Diagram:

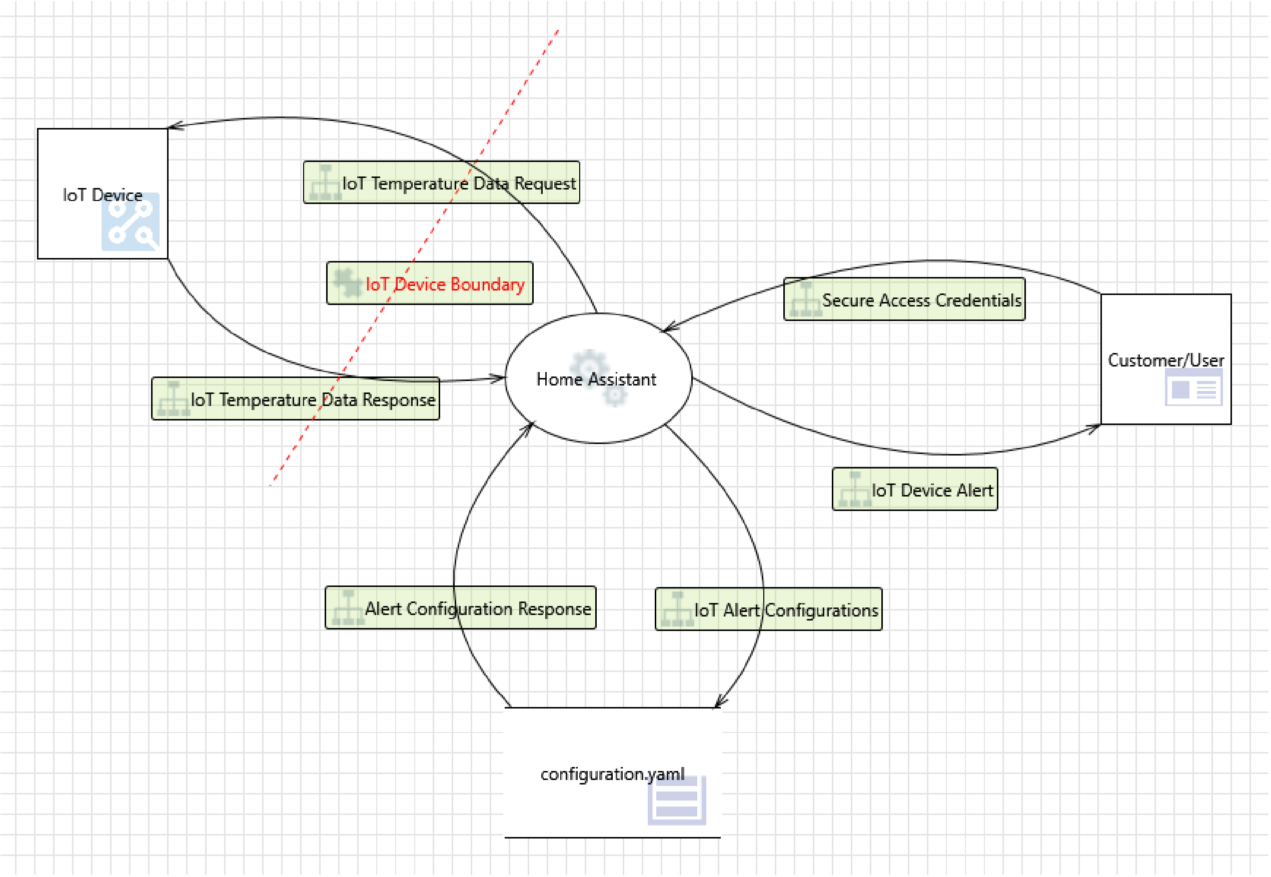
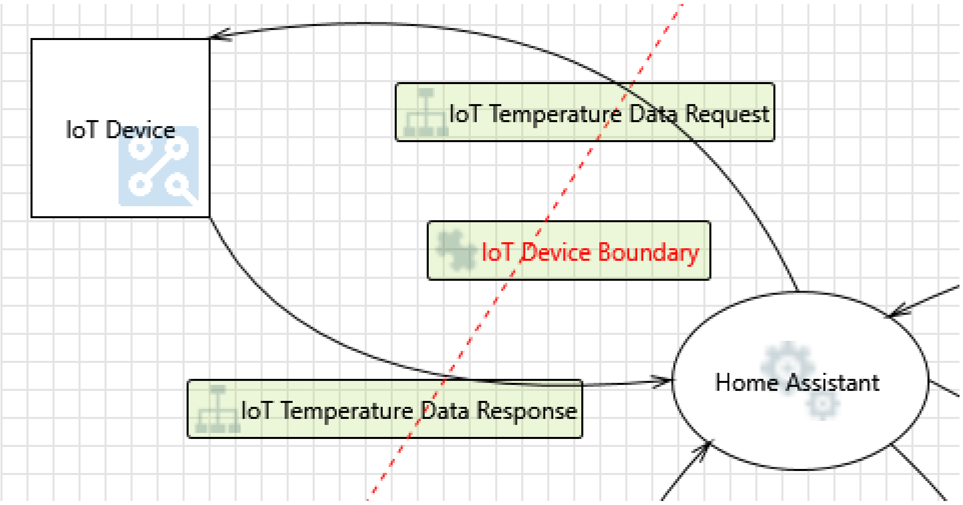


Diagram Summary:

Not Started	0
Not Applicable	2
Needs Investigation	0
Mitigation Implemented	4
Total	6
Total Migrated	0

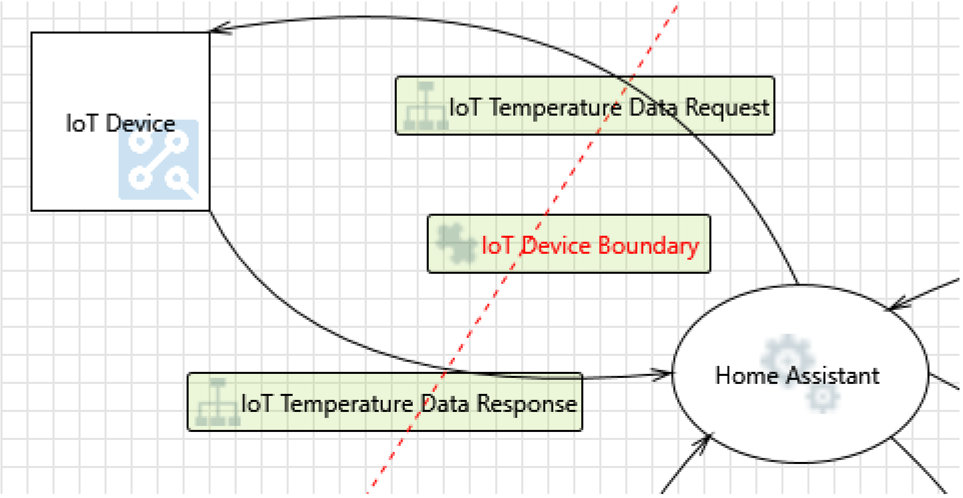
Interaction: IoT Temperature Data Request



1. An adversary may execute unknown code on IoT Device [State: Mitigation Implemented] [Priority: High]

Category:	Tampering
Description:	An adversary may launch malicious code into IoT Device and execute it
Justification:	IoT device requires credentials and proximity to access.
Possible Mitigation(s):	Ensure that unknown code cannot execute on devices.
SDL Phase:	Design

Interaction: IoT Temperature Data Response



2. An adversary may tamper the OS of a device and launch offline attacks [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	An adversary may launch offline attacks made by disabling or circumventing the installed operating system, or made by physically separating the storage media from the device in order to attack the data separately.
Justification:	<no mitigation provided>
Possible Mitigation(s):	Encrypt OS and additional partitions of IoT Device with Bitlocker.
SDL Phase:	Design

3. An adversary may tamper IoT Device and extract cryptographic key material from it [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	An adversary may partially or wholly replace the software running on Home Assistant , potentially allowing the replaced software to leverage the genuine identity of the device if the key material or the cryptographic facilities holding key materials were available to the illicit program. For example an attacker may leverage extracted key material to intercept and suppress data from the device on the communication path and replace it with false data that is authenticated with the stolen key material.

Justification: <no mitigation provided>

Possible Mitigation(s): Store Cryptographic Keys securely on IoT Device.

SDL Phase: Design

4. An adversary may exploit known vulnerabilities in unpatched devices [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: An adversary may leverage known vulnerabilities and exploit a device if the firmware of the device is not updated

Justification: IoT device will need credentials and/or proximity.

Possible Mitigation(s): Ensure that the Cloud Gateway implements a process to keep the connected devices firmware up to date.

SDL Phase: Design

5. An adversary may exploit unused services or features in Home Assistant [State: Mitigation Implemented] [Priority: High]

Category: Elevation of Privileges

Description: An adversary may use unused features or services on Home Assistant such as UI, USB port etc. Unused features increase the attack surface and serve as additional entry points for the adversary

Justification: Services and features are established by authenticated users.

Possible Mitigation(s): Ensure that only the minimum services/features are enabled on devices.

SDL Phase: Implementation

6. An adversary may gain unauthorized access to privileged features on IoT Device [State: Mitigation Implemented] [Priority: High]

Category: Elevation of Privileges

Description: An adversary may get access to admin interface or privileged services like WiFi, SSH, File shares, FTP etc., on a device

Justification: IoT device requires credentials and proximity to access.

Possible Mitigation(s): Ensure that all admin interfaces are secured with strong credentials.

SDL Phase: Implementation