OTA Basic

Owner: Yasho
Reviewer: Phil
Contributors:
Date Generated: Thu Oct 10 2024

Executive Summary

High level system description

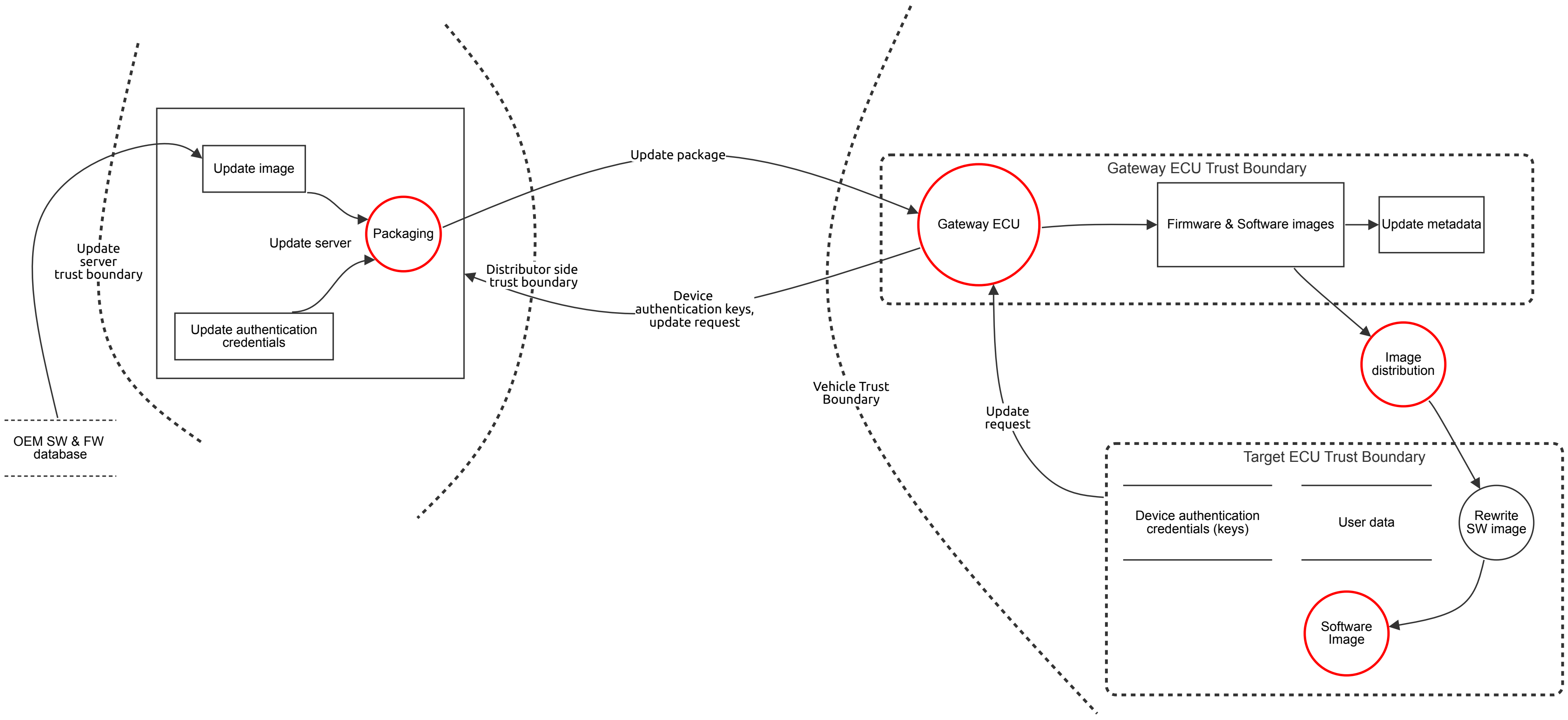
OTA update system and threats associated with it.

Summary

Total Threats	84
Total Mitigated	72
Not Mitigated	12
Open / High Priority	1
Open / Medium Priority	10
Open / Low Priority	0
Open / Unknown Priority	0

Strawman OTA Stride 2

Strawman model of an OTA update system. This does not include a "gateway ECU". It is assumed that the update package is to be installed on the same ECU that receives the payload from the update server.



Update image
Update server
Packaging
Update authentication credentials
Update server trust boundary
OEM SW & FW database
Update package
Distributor side trust boundary
Device authentication keys, update request
Gateway ECU Trust Boundary
Gateway ECU
Firmware & Software images
Update metadata
Image distribution
Vehicle Trust Boundary
Update request
Target ECU Trust Boundary
Device authentication credentials (keys)
User data
Rewrite SW image
Software Image

Strawman OTA Stride 2

Firmware & Software images (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Spoofing identity of legitimate source	Spoofing	Medium	Mitigated		An attacker may attempt to spoof the identity of the legitimate update source and trick the devices into downloading and installing firmware from a malicious source	Use digital signatures and certificates to verify the identity of the source before accepting and applying the update. Employing cryptographic mechanisms ensures that only firmware signed by a trusted entity is installed.
21	New STRIDE threat	Repudiation	Low	Mitigated	3	The update server could deny supplying a particular firmware version or the device could deny receiving and installing the update	Ensure secure logging and auditing on both the OEM's update server and the ECU installing an update. Logs should be tamper proof and include details of the firmware updates, including sources and checksums

Update server (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	Spoofing	Spoofing	Medium	Mitigated		An attacker may try to spoof the identity of the update server and trick devices into thinking they are communicating with the legitimate server.	Use strong authentication mechanisms like TLS certificates to verify the identity of the update servers.
27	New STRIDE threat	Repudiation	Medium	Mitigated		The update server could deny sending a firmware version or deny having sent it.	Implement logging and auditing on both, the ECU and the update server. Logs should be secure and should record all information regarding the firmware update, including timestamp, firmware numbers, hashes, filenames, etc.

OEM SW & FW database (Store) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations
70	Tampering	Tampering	Medium	Mitigated		Software images stored on the OEM's server can be modified, thereby compromising ALL updates to ALL vehicles under the OEM.	Ensure strong network and physical security practices

Update authentication credentials (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
50	New STRIDE threat	Spoofing	Medium	Mitigated		Update authentication credentials could be stolen or forged to impersonate a legitimate (or older) update, tricking devices to install malicious updates.	Store authentication credentials securely on the device, using hardware-based security modules such as TPM (Trusted Platform Module) or HSM (Hardware Security Module). Implement multi-factor authentication where possible.

Gateway ECU (Process)

(the internet)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
39	Spoofing identity of endpoints	Spoofing	Medium	Mitigated		An attacker could impersonate either endpoints and trick the other into thinking they have established a connection with the legitimate endpoint and then intercept traffic between the update server and device.	Use mutual authentication protocols (like TLS certificates) to ensure that both the update server and the TLS client verify each others' identities before transmitting data.
41	New STRIDE threat	Tampering	Medium	Mitigated		An attacker could intercept and alter the data being sent over the communication channel	Employ end-to-end encryption using protocols like TLS to protect data integrity and confidentiality during transmission. Use cryptographic hash functions and digital signatures to ensure data has not been tampered with.
42	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker could read the data being transmitted over the communication channel and capture sensitive information such as firmware details, keys, personal data, etc.	Use strong encryption protocols like TLS to encrypt the data being transmitted. Implement access control and monitor network traffic for detecting eavesdropping/MITM scenarios.
43	New STRIDE threat	Repudiation	Medium	NotApplicable		Either party could deny having sent or received any the firmware update/other data sent over the channel.	Mitigations such as implementation of strong logging mechanisms on both ends won't be for the communication channel, but for the two parties involved
44	New STRIDE threat	Denial of service	Medium	Mitigated		An attacker could flood the gateway ECU with traffic, overwhelming it and preventing any legitimate flow of traffic, disrupting the update process.	Implement rate limiting, traffic filtering, anomaly detection, etc. to detect and avoid DoS attacks. Use load balancing and redundancy to ensure that legitimate traffic can reach its destination.
45	New STRIDE threat	Elevation of privilege	Medium	Mitigated		Elevation of privilege on the network could give the attacker unauthorized access to the server or the device and alter the update process.	Segment network traffic and enforce strict firewall rules to limit communication paths. Use intrusion detection and prevention systems (IDPS) to monitor and respond to suspicious activities. Ensure that communication channels are secured using strong, up-to-date cryptographic protocols.
81	Slow retrieval attack	Denial of service	Medium	Open		An attacker or someone claiming to be the vehicle can slow down network traffic, sending only enough packets to avoid timeouts.	

Update metadata (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update package (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Device authentication keys, update request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
68	Tampering with update request	Tampering	Medium	Mitigated		An attacker can modify the requested updates by the vehicle and make the update server send inaccurate images back to the vehicle	Ensure that communication channels are encrypted using strong protocols like TLS. Implement integrity checks like digital signatures to detect any tampering upon receipt by the server.
69	Stealing device keys	Information disclosure	Medium	Mitigated		Unauthorized access can lead to the device's keys and other credentials (like VIN) to be stolen by an attacker	Encrypt the communication channel with strong, standard encryption protocols like TLS.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update package (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
29	New STRIDE threat	Tampering	Medium	Mitigated		An attacker could tamper with the information being sent over the communication channel and send potentially malicious software to the device	Ensure that communication channels are encrypted using strong protocols like TLS. Implement integrity checks like digital signatures to detect any tampering upon receipt by the device.
31	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker could intercept the data being sent over the communication channel and potentially gain access to privileged information or intellectual property.	Use encryption for data at rest and in transit and implement RBAC for files on the server.
32	New STRIDE threat	Denial of service	Medium	Mitigated		An attacker could overload the update server with requests, making it unavailable to legitimate devices attempting to download updates	Implement rate limiting, traffic filtering and load balancing to measure server traffic. Monitor users to detect, flag and avoid DoS attacks

Update request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update image (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Packaging (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
52	New STRIDE threat	Tampering	Medium	Mitigated		Unauthorized access to alter the items to package will lead to potentially malicious/harmful items getting packaged as part of the update payload.	Verify cryptographic hashes of each item to pack before packaging them.
53	New STRIDE threat	Information disclosure	Medium	Mitigated		Unauthorized parties may be able to read the update to be packaged, leading to loss of sensitive information or intellectual property.	Encrypt all packages to be packaged, and then the final package. Implement RBAC and monitor the network for any anomalies.
59	DoS	Denial of service	Medium	Mitigated		Packaging service may be overburdened by creation of a large number of processes, causing it to prevent packaging the required items to be shipped.	Implement redundancy of packaging service to ensure it is up in case of DoS. Implement network monitoring and rate limiting to detect and prevent attacks.
88	endless data attack	Denial of service	Medium	Open		Send ECU a large amount of data and flood its memory, possibly causing the ECU to fail to operate	

Image distribution (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
82	Freeze attack	Denial of service	Medium	Open		An attacker may alter the functioning of the distribution software (if present on gateway ECU or through an update for the image distribution software) to send properly signed, but old update bundle to the ECUs, even if newer updates exist	

Rewrite SW image (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Software Image (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
77	Arbitrary software attack	Elevation of privilege	Medium	Open		A malicious software bundle can cause an ECU to run arbitrary code of the attacker's choice	
78	Rollback attack	Denial of service	Medium	Open		Deny the ECU of the latest update by causing it to install a previously valid software	
80	Mix-and-Match attack	Denial of service	Medium	Open		An attacker can install a malicious software bundle in which some of the packages do not interoperate properly, by installing mismatched packages.	

Device authentication credentials (keys) (Store)

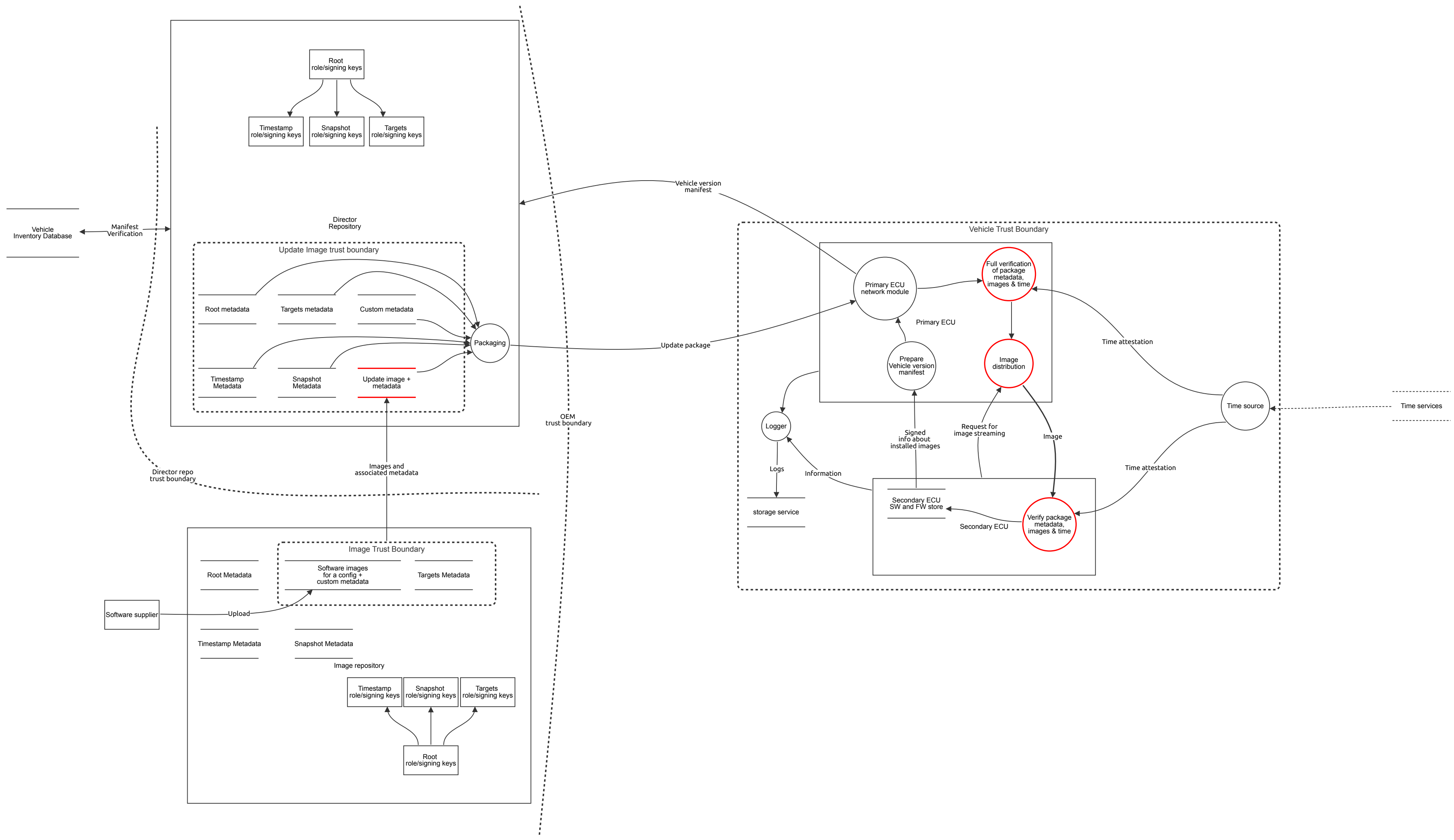
should be on an HSM or TPM

Number	Title	Type	Priority	Status	Score	Description	Mitigations
83	Key leak	Information disclosure	Medium	Mitigated		An attacker could steal the ECU's authentication credentials and use them to impersonate a legitimate device.	Store authentication credentials on a hardware-based security enclave like an HSM or TPM.
84	New STRIDE threat	Tampering	Medium	Mitigated		An attacker may try to alter device's authentication credentials, giving them access to redirect updates and gain unauthorized access to sensitive data	Use cryptographic techniques to protect the integrity of credentials. Implement effective access control to prevent unauthorized modification

User data (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
85	New STRIDE threat	Tampering	Medium	Mitigated		An attacker could modify user data by exploiting vulnerabilities in the system, leading to data corruption and possible unavailability of the vehicle's functioning.	Use integrity checks such as cryptographic hashes to detect unauthorized changes to the data. Implement secure storage solutions
86	New STRIDE threat	Information disclosure	Medium	Mitigated		Unauthorized access to user data can lead to leaking of sensitive information such as personal details, affecting the user's privacy.	Encrypt user data at rest and in transit to protect it from unauthorized changes. Implement effective access control mechanisms for this store.
87	New STRIDE threat	Denial of service	Medium	Mitigated		An attacker could disrupt access to the user's data, making it unavailable and/or causing loss of data. This could impact the vehicle's functionality and UX	Implement redundancy and backup mechanisms to ensure availability of user data.

Uptane OTA solution



Uptane OTA solution

Primary ECU network module (Process)

Has public network access.
Verifies images by checking that the hashes of the images match the hash specified by the director's target metadata

Number	Title	Type	Priority	Status	Score	Description	Mitigations
152	New STRIDE threat	Spoofing	Medium	Mitigated		An attacker may spoof the identity of the primary's network module and trick the director into thinking that it is communicating with a vehicle.	Use mutual authentication protocols (like TLS with certificates), to ensure that primary ECU and the server ensure each other's identities.
155	Slow retrieval attack	Denial of service	Medium	Mitigated		Slow down network traffic outside of the vehicle, such that barely enough packets are sent to avoid a timeout.	All ECUs shall monitor the download speed of image metadata and image binaries to detect a slow retrieval attack.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manifest Verification (Data Flow)

Verifies if the vehicle version manifest provided by the vehicle is accurate according to records in the inventory database

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Upload (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Images and associated metadata (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Signed info about installed images (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Time attestation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
173	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker can sniff the packets being sent over the bus to pick up on patterns of how and when the time attestations are sent to the secondary ECU in order to plan an attack on either of the devices.	Ensure that the time attestations are encrypted at rest and in transit between the onboard source of time and the secondary ECU.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
172	New STRIDE threat	Tampering	Medium	Mitigated		An attacker with (physical) access can tamper with the time attestation data being sent over the channel, and throw the secondary ECU's synchronization off, leading to a disruption of the update cycle.	Implement cryptographic hash functions and digital signatures to verify and ensure the integrity of the time attestation. The secondary should only use this time attestation if the signature and hashes are verified.

Information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Logs (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Image (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
208	Eavesdrop attack	Information disclosure	Medium	Mitigated		An attacker can get access to and read sensitive/confidential information intended for a particular ECU	Ensure that the information being sent over any medium is encrypted, both in transit and at rest.
209	New STRIDE threat	Tampering	Medium	Mitigated		An attacker can intercept and alter the information (including signatures, hashes, files, logs, etc.) being sent over the medium and provide the secondary ECU incorrect information	Use encryption and verification methods like verification of digital signatures and cryptographic hashes to ensure the integrity of the data.

Update package (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Eavesdrop attack	Information disclosure	Medium	Mitigated		An attacker may attempt to intercept the data being sent over the communication channel, such as update packages and firmware images	Ensure that the data being transmitted across the channel is encrypted using strong encryption protocols (eg, TLS) to protect data confidentiality and integrity.
106	New STRIDE threat	Tampering	Medium	Mitigated		An attacker may intercept and alter the data being shared over the channel, such as altering the software image or update package	Employ end-to-end encryption for all data being transmitted. Use cryptographic hash functions and digital signatures as data integrity checks.
212	Endless data attack	Denial of service	Medium	Mitigated		An attacker may send the ECU a large amount of data until it runs out of storage, rendering it useless/Inoperative.	Implement a limit of the maximum possible downloadable file size when receiving anything on the ECU

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request for image streaming (Data Flow)

For secondary ECUs with insufficient storage, Primary SHOULD wait for a request from the Secondary to stream the new image file to it.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Timestamp Metadata (Store)

Contains the filename and version number of the LATEST snapshot metadata file, along with at least one hash of the snapshot metadata file, with the hashing function used.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Snapshot Metadata (Store)

Lists version numbers and filenames of all Targets metadata files.

On director for a vehicle, there will be only 1 Targets metadata file.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Targets metadata (Store)

Metadata about all images to be installed on target vehicle

Number	Title	Type	Priority	Status	Score	Description	Mitigations
202	New STRIDE threat	Tampering	Medium	Mitigated		An attacker might tamper with targets metadata to alter the list of authorized updates, version information, or cryptographic hashes, allowing the distribution of unauthorized or malicious firmware.	Implement cryptographic signatures and hash functions to ensure the integrity of targets metadata. Devices should verify these signatures and hashes before accepting and processing the metadata. Use secure storage and transmission channels to protect metadata from tampering.

Root metadata (Store)

root of trust for generating keys to be used by all other roles for signing metadata

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Image repository (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
178	New STRIDE threat	Spoofing	Medium	Mitigated		An attacker can spoof the image repository's identity and trick the director into thinking that it is communicating with the legitimate image server.	Use mutual authentication protocols (like TLS with certificates), to ensure that primary ECU and the server ensure each other's identities.
180	New STRIDE threat	Repudiation	Medium	Mitigated		The image repository can deny having received a software package from the supplier, and deny having sent the image and metadata to the director	Employ secure, proper logging and auditing mechanisms on the image repository.

Timestamp Metadata (Store)

Contains filename and version number of latest snapshot metadata file, along with one or more hashes of the snapshot metadata file, with the hashing function

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Snapshot Metadata (Store)

Contains metadata about all targets metadata files in the image repository

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Targets Metadata (Store)

Information about all images to be installed on ECUs. On the Image repository, there will be multiple targets metadata files

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Root Metadata (Store)

root of trust for generating keys to be used by all other roles for signing metadata

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Vehicle Inventory Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
141	New STRIDE threat	Tampering	Medium	Mitigated		An attacker may alter the inventory database contents and affect mapping of VINs and associated software images.	Employ strong physical security, ensure strong and effective access control is in place.
205	New STRIDE threat	Repudiation	Medium	Mitigated		The OEM's vehicle inventory database can deny having received the vehicle version manifest for verification.	Ensure secure and proper logging mechanisms are in place. Ensure that logs are timestamped
206	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker can gain unauthorized access to the database and steal sensitive information such as VINs, their mapping with ECU IDs or owner names or software versions, etc.	Ensure that the data stored on the database is encrypted using strong encryption protocols. Implement strict access control mechanisms and make sure that only authorized personnel can access the inventory database

Number	Title	Type	Priority	Status	Score	Description	Mitigations
207	New STRIDE threat	Denial of service	Medium	Mitigated		An attacker can execute a denial of service attack on the inventory database by flooding it with too many requests, making it unavailable for working for a legitimate user	Implement rate-limiting, traffic monitoring and filtering, etc. Use redundancy to ensure that the server to ensure availability.

Director Repository (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
118	Spoofing	Spoofing	Medium	Mitigated		An attacker can spoof the identity of the director role to impersonate an OEM and trick a vehicle into thinking that it is communicating with the OEM.	Use mutual authentication protocols (like TLS with certificates), to ensure that primary ECU and the server ensure each other's identities.
142	New STRIDE threat	Repudiation	Medium	Mitigated		The director can deny having ever received a vehicle version manifest or an updated image from the image repository.	Ensure secure logging and auditing mechanisms are implemented on the director, where all incoming messages must be able to be traced back to at least their immediate previous source.
150	New STRIDE threat	Repudiation	Medium	Mitigated		The director can deny having sent any update package to the vehicle	Ensure secure logging and auditing mechanisms are implemented on the director, where all incoming messages must be able to be traced back to at least their immediate previous source.

Packaging (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
108	Freeze attack	Denial of service	Medium	Mitigated		Continue to send a properly signed, but old, update bundle to the ECUs, even if newer updates exist.	Check the root and targets metadata files to ensure that the the update package being sent to the ECU is up to date. Also, if the new Timestamp metadata file has expired, discard it, abort the update cycle, and report the potential freeze attack.
182	New STRIDE threat	Repudiation	Medium	Mitigated		Deny having packaged the metadata and update images together or having sent the package out to the primary ECU	Ensure proper and secure logging and auditing mechanisms are in place

Software images for a config + custom metadata (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Time source (Process)

A secure way for ECUs to know the time. Could be any implementation of time

Number	Title	Type	Priority	Status	Score	Description	Mitigations
133	New STRIDE threat	Spoofing	Medium	Mitigated		An attacker can spoof the identity of this time source and lead an ECU to believe that it is interacting with the legitimate source of time	Use mutual authentication mechanisms like TLS certificates, etc. to verify the authenticity of the source of time onboard the vehicle.
134	New STRIDE threat	Repudiation	Medium	Mitigated		The time source could deny having received a particular time attestation from the external time server.	Ensure descriptive and secure logging and auditing mechanisms are in place. These logs should be tamper-proof and include details of all attestations of time, including their sources and checksums.
135	New STRIDE threat	Tampering	High	Mitigated		An attacker can intercept the time sent by the server to the vehicle and alter it in order to provide the incorrect time to the vehicle.	Time data being transmitted must be encrypted and signed. Verify the checksum for the attestation received and forward the time to ECUs iff verification is successful.
137	New STRIDE threat	Elevation of privilege	High	Mitigated		An attacker could potentially gain elevated access to the onboard time source, allowing them to alter its functionality and manipulate system behavior, enabling further malicious activities.	Implement proper access control for the onboard time source. Use secure, authenticated time sources and regularly verify the accuracy of the device's system time against trusted servers.
138	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker can intercept when and how the onboard time source synchronizes with the external time server, which can potentially aid in profiling and conducting attacks	Encrypt time synchronization traffic to protect it from eavesdropping. Use secure protocols like NTS to ensure that time data is transmitted securely. Limit the disclosure of detailed time synchronization logs to authorized personnel.
170	Denial of time	Denial of service	Medium	Mitigated		An attacker can launch a denial-of-service attack on the onboard time source by flooding it's memory, sending endless requests, etc. in an attempt to throw off the synchronization of the ECUs	Employ DoS attack detection and prevention methods, implement rate-limiting, use redundancy if possible to ensure availability.

Update image + metadata (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	New STRIDE threat	Tampering	Medium	Open		An attacker can intercept and alter the image being sent from the image repository and the director could receive an outdated/incorrect image.	Check all relevant metadata (potentially all 4) to ensure that the director receives the appropriate image from the image repo.
117	New STRIDE threat	Repudiation	Medium	Mitigated		The director could deny ever receiving the update package from the image repository.	Ensure clear, secure logging mechanisms are present on both parties to ensure that the origin of the package can be properly traced.

Root role/signing keys (Actor)

Root of trust for producing and distributing public keys to root, targets, snapshot and timestamp roles and signs the root metadata.
Must be an offline key

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Timestamp role/signing keys (Actor)

Responsible for signing the timestamp metadata for the image repository

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Snapshot role/signing keys (Actor)

Responsible for signing the snapshot metadata for the image repository

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Targets role/signing keys (Actor)

Responsible for signing targets metadata for each image package

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Root role/signing keys (Actor)

Root of trust for producing and distributing public keys to root, targets, snapshot and timestamp roles and signs the root metadata.
Must be an offline key.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Timestamp role/signing keys (Actor)

Responsible for signing the timestamp metadata for the director repository

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Snapshot role/signing keys (Actor)

Responsible for signing the snapshot metadata for the director repository

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Targets role/signing keys (Actor)

Responsible for signing targets metadata for each update package to send to a vehicle

Number	Title	Type	Priority	Status	Score	Description	Mitigations
140	New STRIDE threat	Spoofing	Medium	Mitigated		An attacker may spoof the targets role and make the director believe that it is interacting with the legitimate role.	Employ zero-trust principles - verify signatures every time the targets role signs any metadata and use strong mutual authentication protocols like TLS.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
151	New STRIDE threat	Repudiation	Medium	Mitigated		The targets role can deny having signed any of the targets metadata for the update package	Ensure secure logging and auditing mechanisms are implemented on the director, where all incoming messages must be able to be traced back to at least their immediate previous source.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Software supplier (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Full verification of package metadata, images & time (Process)

Primary ECUs have to perform full verification

Number	Title	Type	Priority	Status	Score	Description	Mitigations
164	Deny receiving update	Repudiation	Medium	Mitigated		The ECU can deny having performed a full verification on the package received from the director repository	Ensure proper, secure logging and auditing mechanisms are in place for every step of verification.
165	Skip verification	Elevation of privilege	High	Open		An attacker with unauthorized access can bypass the full verification of the primary and make it either skip the process or make it perform partial verification	
204	Rollback attack	Denial of service	Medium	Open		Cause an ECU to install a previously valid software revision that is older than the currently installed version.	

Secondary ECU SW and FW store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verify package metadata, images & time (Process)

Secondary ECUs can perform partial verification

Number	Title	Type	Priority	Status	Score	Description	Mitigations
111	Rollback attack	Denial of service	Medium	Mitigated		Cause an ECU to install a previously valid software revision that is older than the currently installed version	Compare the root metadata (and the incremental counter in it), timestamp metadata received from the director about this update package
112	Mix-and-max attack	Denial of service	Medium	Mitigated		Install a malicious software bunch in which some of the software packages fail to interoperate properly.	Check if the hashes and version number of the new Snapshot metadata file match the hashes and version number listed in the Timestamp metadata for the package. If they don't, raise a flag.
131	Arbitrary software attack	Elevation of privilege	Medium	Open		An attacker can cause an ECU to install and run an arbitrary piece of software of the attacker's choice	

Prepare Vehicle version manifest (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Image distribution (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
124	Freeze attack	Denial of service	Medium	Mitigated		Cause an ECU to install a previously valid software revision that is older than the currently installed version.	Check the root, timestamp and snapshot metadata to ensure that the package received is the latest update.
127	Mix-and-match attack	Denial of service	Medium	Mitigated		Install a malicious software bundle which causes the update to not interoperate properly	Compare the snapshots metadata from the director to ensure that all targets metadata files are the same as received from the update package.
162	Spoofing ECU identity to secondary ECU	Spoofing	Low	Mitigated		An attacker may spoof the identity of the primary's image distribution process, and trick the secondaries into believing that they are receiving updates from a legitimate source.	Use mutual authentication protocols (like TLS with certificates), to ensure that both ECUs ensure each other's identities.
203	Partial bundle installation attack	Denial of service	Medium	Open		Install a valid (signed) update bundle, and then block selected updates within the bundle.	

Primary ECU (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
90	Spoofing of endpoints	Spoofing	Medium	Mitigated		An attacker could attempt to impersonate the legitimate communication endpoints (e.g., the update server or the device) to intercept or alter the data being transmitted over the communication channel	Use mutual authentication protocols (e.g., TLS with client certificates) to ensure that both the device and the server verify each other's identities before establishing communication.
143	New STRIDE threat	Repudiation	Medium	Mitigated		The primary ECU may deny having received an update package from the director.	Ensure secure logging and auditing mechanisms are implemented on the director, where all incoming messages must be able to be traced back to at least their immediate previous source.

Time services (Store) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Custom metadata (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Vehicle version manifest (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Eavesdrop attack	Information disclosure	Medium	Mitigated		An attacker may attempt to intercept the data being sent over the communication channel, such as update packages and firmware images	Ensure that the data being transmitted across the channel is encrypted using strong encryption protocols (eg, TLS) to protect data confidentiality and integrity.
106	New STRIDE threat	Tampering	Medium	Mitigated		An attacker may intercept and alter the data being shared over the channel, such as altering the software image or update package	Employ end-to-end encryption for all data being transmitted. Use cryptographic hash functions and digital signatures as data integrity checks.

Secondary ECU (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
90	Spoofing of endpoints	Spoofing	Medium	Mitigated		An attacker can spoof the identity of the secondary (to the primary) and cause the primary to think it is communicating with a legitimate secondary ECU.	Use mutual authentication protocols (e.g., TLS with client certificates) to ensure that both ECUs verify each other's identities before establishing communication.
143	New STRIDE threat	Repudiation	Medium	Mitigated		The secondary ECU may deny having received an update package from the primary.	Ensure secure logging and auditing mechanisms are implemented on the director, where all incoming messages must be able to be traced back to at least their immediate previous source.

storage service (Store)

onboard logger service - may or may not be a standalone process/device

Number	Title	Type	Priority	Status	Score	Description	Mitigations
193	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker/unauthorized actor can access and read logs and gain crucial information which can help plan out attacks, or provide the attacker confidential information	Use strong asymmetric key encryption when storing logs to ensure that nobody except intended parties are able to read the logs.
194	New STRIDE threat	Tampering	High	Mitigated		An attacker can try to alter the contents of the log, to hide any audit trail of attacks/malicious activity carried out elsewhere	Implement cryptographic techniques such as hashing and digital signatures to ensure the integrity of log files. Store logs in a secure, tamper-evident environment and use append-only logs where possible. Ensure strict access control for logs.
195	New STRIDE threat	Denial of service	Medium	Mitigated		An attacker could overwhelm the logging system with excessive data, making it difficult to store or analyze logs, thereby disrupting monitoring and incident response efforts.	Implement rate-limiting and log rotation to manage the volume of logging data. Monitor for abnormal logging patterns.

Time attestation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
173	New STRIDE threat	Information disclosure	Medium	Mitigated		An attacker can sniff the packets being sent over the bus to pick up on patterns of how and when the time attestations are sent to the secondary ECU in order to plan an attack on either of the devices.	Ensure that the time attestations are encrypted at rest and in transit between the onboard source of time and the secondary ECU.
172	New STRIDE threat	Tampering	Medium	Mitigated		An attacker with (physical) access can tamper with the time attestation data being sent over the channel, and throw the secondary ECU's synchronization off, leading to a disruption of the update cycle.	Implement cryptographic hash functions and digital signatures to verify and ensure the integrity of the time attestation. The secondary should only use this time attestation if the signature and hashes are verified.

Logger (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
197	New STRIDE threat	Elevation of privilege	High	Mitigated		An attacker can cause the logging process to do something that's out of it's scope, or make it cause harm. The attacker may also attempt to get access to sensitive information and bypass system controls	Use role-based access control (RBAC) to limit who can access and manage the logging systems. Ensure logging systems run with the least privilege necessary. Regularly audit the access and configuration of logging systems to detect unauthorized changes