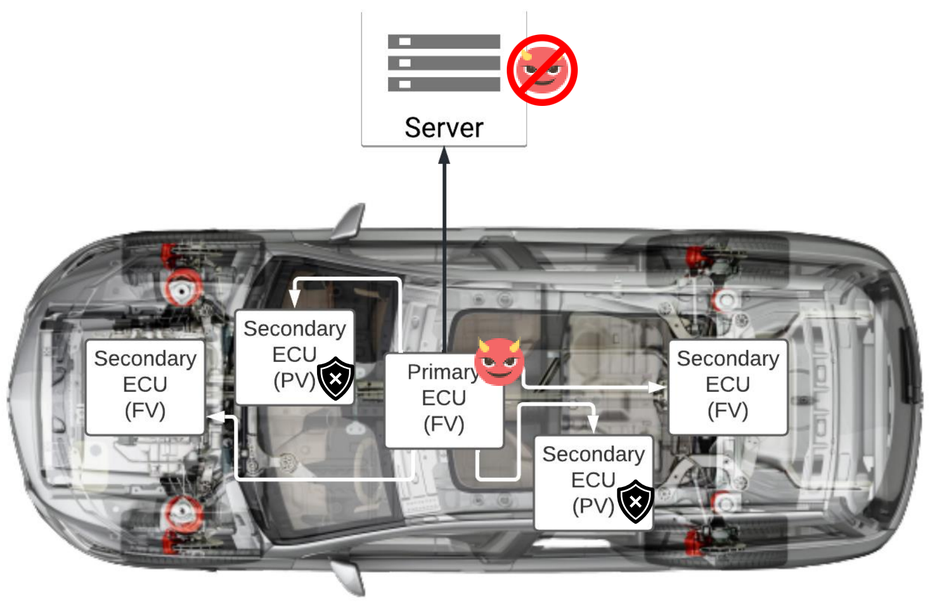
Secure Over-the-Air Vehicle Updates using Trusted Execution Environments (TEE)

Augusto Henriques[1] **| Hugo Pacheco**[1] **| Fernando Alves**[1]
[1]Faculdade de Ciências da Universidade do Porto

Introduction

- In automotive industry, one of the challenges in updating firmware Over The Air (OTA), has always been protection against external attacks.
- TUF was designed as an Open Sources Framework to address the main risks in the OTA process and successive framework, Uptane is similar but more specialized for automotive. [1]
- Uptane utilizes multiple repositories containing metadata and images that are sent to Primary ECU. After download, the Primary will run Full verification (FV) process. Then, if no issues occurred, broadcast the data to Secondaries ECUs where some of them perform Full verification (FV) or Partial verification (PV).
- One of the main problems is, Secondaries with PV does not provide FV guarantees, especially if the Primary is corrupted. [2]

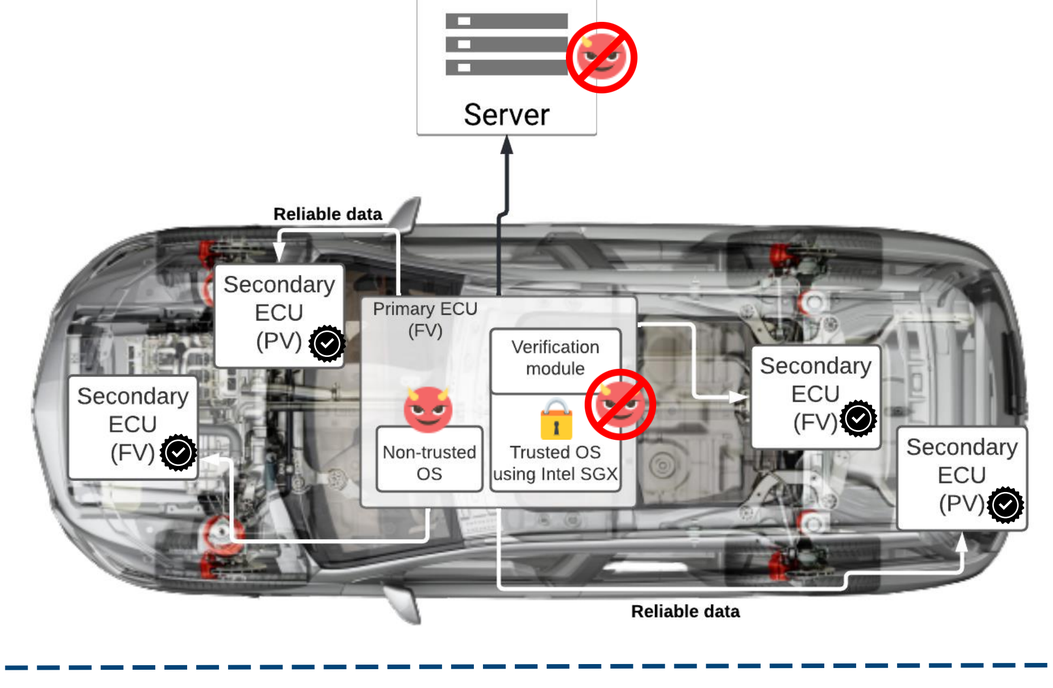


- Full verification (FV) : Verifies and caches the timestamp, snapshot, root, targets and director metadata.
- Partial verification (PV) : Verifies and caches only director metadata.

Objective(s)

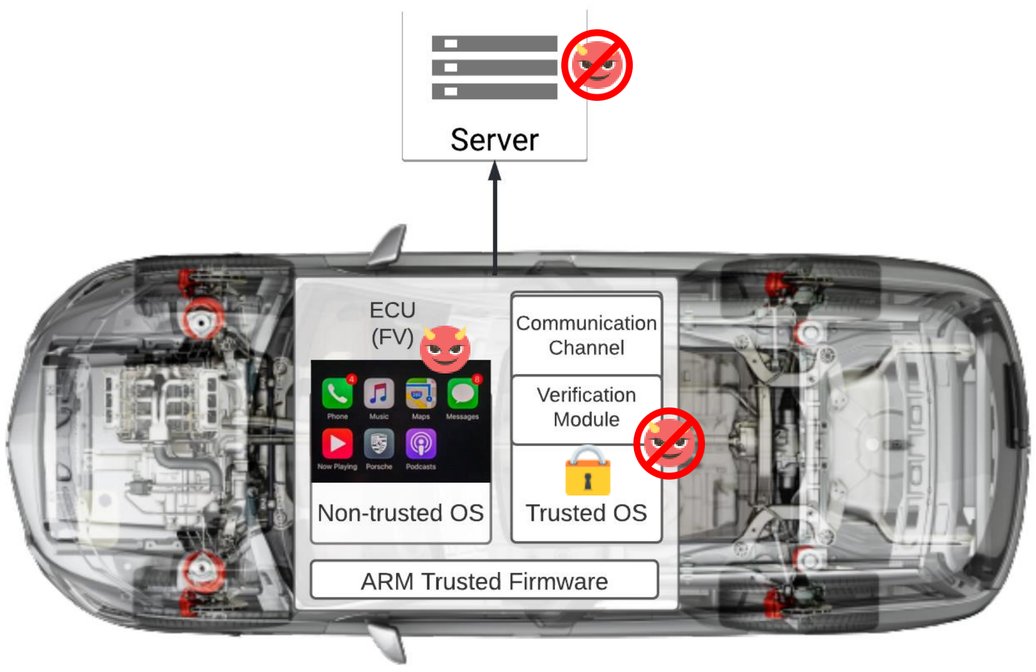
- The main objective of this investigation aims to isolate verification module (FV) using Intel SGX on a Primary ECU. The secondary ECUs can rely on the remote attestation provided by the Primary ECU to verify that updates are genuine.

1. Refactor Uptane in order to isolate core components and design an API for communication between Primary ECU TEE-enabled components and non-trusted components (within a Primary ECU or the Secondary ECUs).
2. Implement critical components (FV) within the TEE.
3. Implement remote attestation of Primary FV to Secondary PV



State-of-the-Art

- Even though Uptane provides security for the download process, an attacker that controls the Primary ECU can void the update process.
- One way to solve this issue was introduced by Mukherjee et al. [3], who propose to run the Uptane client inside a TEE (ARM Trustzone) in order to protect its integrity and avert any security breaches. However, it is not recommended to run networking code inside a TEE.



Workplan

Task Name	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July
Get familiar with the Uptane trust chain									
Analysis on suitable modified Uptane framework format									
Isolate core components									
Design an API for communication									
Implement Full verification componement within the TEE									
Implement remote attestation									
Thesis writing									

References

- [1] Kuppusamy, T. K., DeLong, L. A., & Cappos, J. (2018). Uptane: Security and Customizability of Software Updates for Vehicles. IEEE Vehicular Technology Magazine, 13(1), 66–73.
- [2] T. K. Kuppusamy, A. Brown, S. Awwad, D. McCoy, R.
- Bielawski, C. Mott, S. Lauzon, A. Weimerskirch, J. Cappos,
- “Uptane: Securing Software Updates for Automobiles,” 14th
- ESCAR Europe 2016: https://ssl.engineering.nyu.edu/papers
- /kuppusamy_escar_16.pdf.
- [3] Mukherjee, A., Gerdes, R., & Chantem, T. (2021). Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems. *Proceedings Third International Workshop on Automotive and Autonomous Vehicle Security*.

U.PORTO
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

[dcc]
DEPARTAMENTO DE CIÊNCIA DE COMPUTADORES
FACULDADE DE CIÊNCIAS DA UNIVERSIDADE DO PORTO

M:ERSI