

Over-the-air Updates for Vehicles An Uptane implementation

Fernando Aves, João Salgado, Munkenyi Mukhandi

Introduction

The automotive industry is changing with vehicle digitalisation. The internal structure of the vehicle is moving from multiple individual Electronic Control Units (ECU) to centralised high-performance computers that manage multiple systems. This push, combined with the customer demand for digital maintenance and novel in-vehicle features is driving the automotive industry to implement over-the-air updates for all vehicle components.

However, this is not a simple task due to safety and security issues. In this work we focus on the latter by implementing the state-of-the-art protocol Uptane [1]. This protocol is designed for secure updates for the automotive industry, and features:

- > Server-side redundancy for backend robustness
- > Detailed signed manifests with well defined roles to avoid damages from partial compromises
- > Support for multiply providers: vehicles are composed of parts from many manufacturers, and these need to be considered on the update chain
- > In-vehicle responsibility separation considering available ECU connectivity and computational capabilities

Background and Motivation

Devices without traditional interaction modes (typically screen and keyboard) pose challenges to maintain since there is no clear method to recover the device when facing issues. This is amplified when considering cyberphysical or critical systems, where the device availability is crucial—a vehicle cannot function properly with faulty breaks. Since the update process can face errors that render devices unusable, manufacturers typically avoid updating the aforementioned types of devices, invoking safety and availability reasons.

However, costumers have been putting pressure on manufacturers to include updates on devices' lifecycle due to:

- > Security: devices face security issues due to novel vulnerabilities being discovered or due to faulty designs
- > Requests for novel features: costumers do not want to have to buy new devices to have state-of-the art features
- > Environmental concerns about digital waste, which can be lowered by increase devices' lifecycle

The automotive industry faces pressure to implement over-the-air solutions for the vehicles since with the digital transformation they face all of these issues.

Objectives

Implement a state-of-the art over-the-air updates protocol; study its security features and possible extensions to improve its security, application scenarios, and safety.

References

[1] The Uptane standard: <https://uptane.org/>

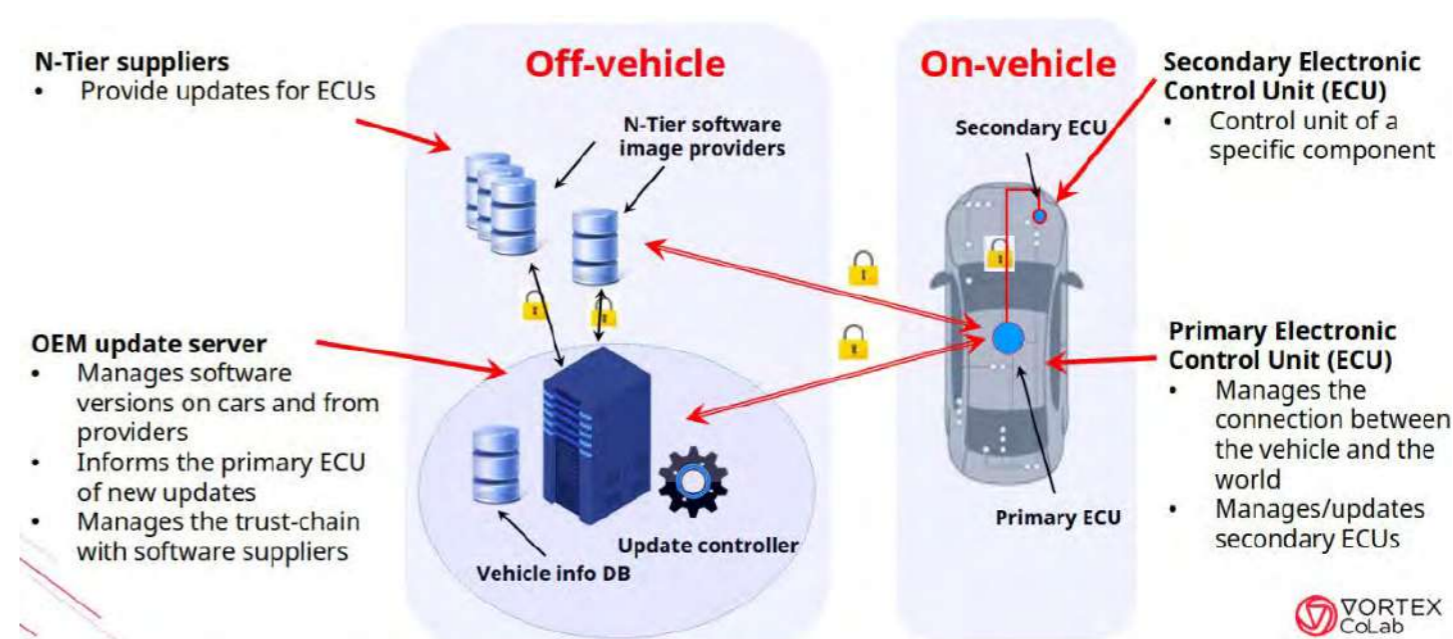
Proposed Approach

The Uptane architecture is composed of the server side and the vehicle side. On the server side:

- > The director server stores vehicle version information, and instructs the vehicles to which updates they should install
- > The image server stores the update images, to be transferred to the vehicles
- > The suppliers link their update repositories to the image server, so the vehicle can fetch updates from multiple sources

On the vehicle side:

- > The primary Electronic Control Unit (ECU) is typically the only unit on the vehicle with Internet access, and therefore the one that interacts with the servers and fetches the updates for the whole vehicle
- > The secondary ECUs receive updates from the primary



Benefits and Innovations

- > Uptane offers a comprehensive trustchain to guarantee the security of update images to be installed
- > This trustchain includes multiple vehicle stakeholders providing updates to the vehicle
- > An attacker must control all servers to compromise a vehicle

Acknowledgment

This work is supported by the European Union/Next Generation EU, through the Recovery and Resilience Plan (PRR) [Project Route25 with Nr. C645463824-00000063].

Future Work and Next Steps

- > Guarantee safety for the updates
- > Guarantee update compatibility: either all units or no units are updated
- > Use hardware security modules to increase the resilience of the system