AISHWARYA MELATUR—ELECTRICAL DEPARTMENT—CDSID: AMELATUR

SecOC: the crucial cybersecurity feature on our autonomous cars

The Department and my team

The Department of **Electrical Engineering** is located in B523. This department deals with everything from ADAS to networks, through software and hardware, infotainment and more.

I spent my placement in the **Software Architecture** team (SOAR), located in G01. As a general definition, software architecture deals with the design and implementation of different software components, their development environment, the system as a whole and the link between these different software components.

The AutoSAR strategy behind securing messages between ECUs

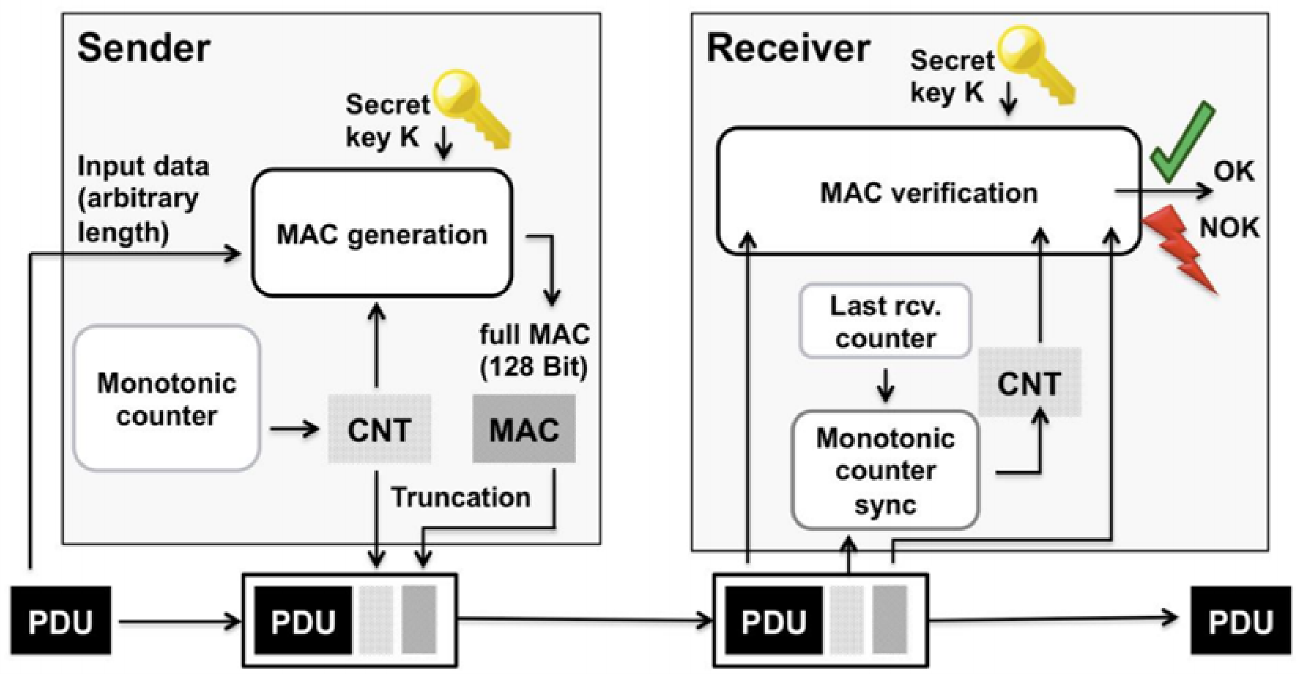


Figure 3: Message Authentication and Freshness Verification

My sub-team is SecOC, whose name is a reference to **the software module in AutoSAR**. This project team is composed of five people, who work on implementing the different strategies used for the SecOC project.

Secure Onboard Communications and its importance in autonomous cars

A vehicle's functionalities and features stem from the hundreds of ECUs that it is comprised of. ***In a car that is increasingly autonomous, the network communications between these ECUs need to be secured.***

SecOC is hence the cybersecurity feature chosen to fulfil that goal. Through the authentication of packets of data being sent, SecOC-enabled ECUs make sure that only the correct messages are being interpreted by other ECUs, **thus limiting any kind of possible hacking.**

In a level 3 autonomous car, on the road, hacking ECU messages and **effectively hijacking the car not only tarnishes the image of JLR, but also threatens the security and the life of our customers.** SecOC is hence a crucial project in the context of the autonomous vehicle.

The challenges

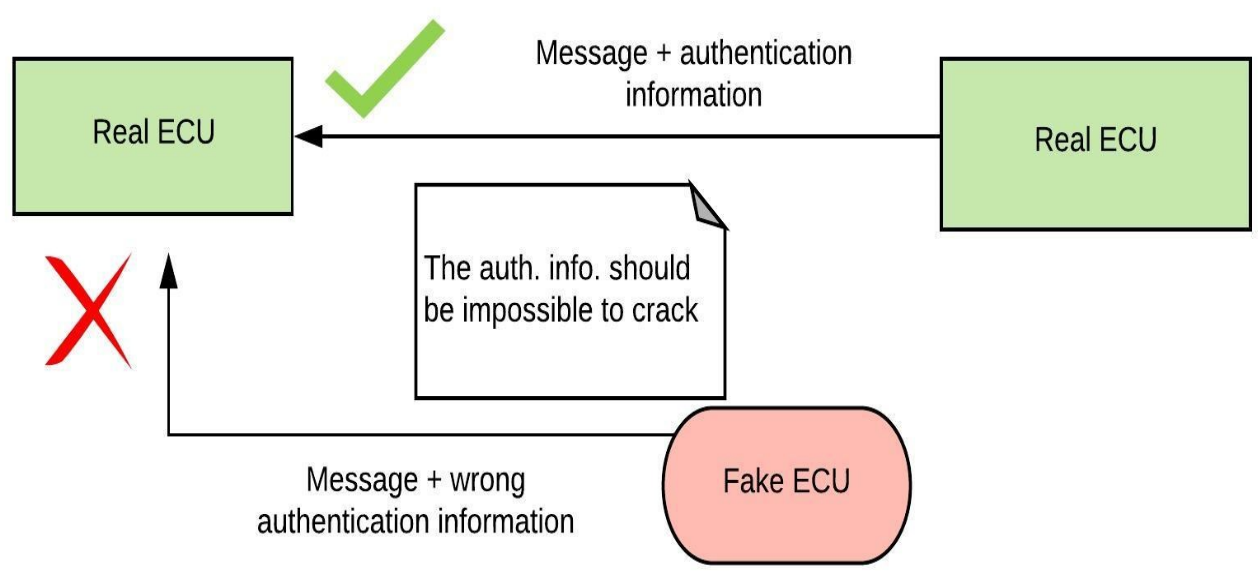
- A lot of **very specific and niche information** was needed for this project, hence making Google/StackExchange not very useful
- Reading AutoSAR and STJLRs were only the foundation of the task. **Reaching out to suppliers themselves** (Bosch) **and tool providers** (Vector) was crucial in order to **understand their side of the implementation** and simulate the same on my side
- A lot of unknowns meant a lot goes wrong on the daily. It is a task involving mainly **trial and error.**

Software Architecture and its links to other teams in JLR

Software architecture is a critical piece of the machinery that is the design and production of the modern car, with its now hundreds of ECUs and features that are more and more complex. At JLR, our team needs to communicate and **collaborate with other teams** in the company in order to further our projects:

- the **Networks team** is vital for us in order to understand how the ECUs will communicate, through what channels, and using what protocols.
- the **cybersecurity team,** while also part of the software architecture larger team, is one of the key players for the SecOC project (detailed further below).
- **Electrical Architecture**, **ADAS**, **Powertrain** and **Chassis** teams are also very important to collaborate with as the software system ultimately needs to be integrated on a vehicle
- Testing teams like **Software Process and Quality** along with **VITAL** (Virtual Integration and Test Automation Laboratory) are crucial to test and improve our work.

Authentication information that is protected against replication helps the ECU distinguish real message data from hacks



My Project: SecOC Testing

- **Writing CAPL to create a testing suite** for SecOC-enabled ECUs on the CANoe simulation environment
- This was to test ECUs across all three channels used on the target vehicle: **CAN, FlexRay and Ethernet**
- Needed deep knowledge of all of those communication protocols in order to **implement time synchronisation mechanisms over all channels**
- **Writing the key and freshness manager strategy** on CAPL
- Supporting the SecOC strategy, offering insight and a pair of fresh eyes
- Helping the team setting up the test bench and supporting workshops with suppliers

ALL THE INFORMATION IN THIS DOCUMENT IS PUBLIC AND NOT SENSITIVE IN NATURE . THE STRATEGIES ARE BY AUTOSAR, AND ARE PUBLIC AND ACCESSIBLE ONLINE.