AUTOCRYPT

# Potential Cyberattacks in Connected Cars and Mobility

### Entry Point I.

## Head Unit

The vehicle's head unit is the closest entry point to its internal system, often containing a mainboard ECU that serves the infotainment system, and a gateway ECU that directs application requests to the CAN bus. If a hacker gains access to the head unit, they are only one step away from gaining control of the CAN buses and ECUs, potentially taking over the vehicle.

### Risks?

Vehicle hijacking, vehicle takeover

### By who?

Criminals

### Solution?

AutoCrypt IVS

- Intrusion detection and protection system (IDPS)
- ECU protection
- Vehicle security operations center (vSOC)

### Entry Point II.

## V2X Messages

In the C-ITS environment, V2X messages are transmitted between road participants like vehicles, infrastructure, and pedestrians in real-time. Attackers can attempt to spoof the V2X messages broadcasted from these participants, leading to wrong judgments and even potentially controlling the targeted vehicles. They could also sniff the messages to steal data.

### Risks?

Vehicle hijacking, vehicle takeover, theft, terrorism, data breach

### By who?

Nation-states, criminals, thieves

### Solution?

AutoCrypt V2X

- Message encryption
- User verification via Security Credential Management System (SCMS)
- Integrated certificate management

### Entry Point III.

## EV Charging Station

When an EV is plugged into a public charging station, the charging operator collects the owner's membership and payment card information for transaction processing. An attacker can target the Plug&Charge (PnC) system to steal membership credentials and credit card details, or potentially attack the power grid.

### Risks?

Data breach, payment card fraud

### By who?

Nation-states, criminals

### Solution?

AutoCrypt PnC

- PKI-based Plug&Charge user verification
- Message encryption
- OCPP support

### Entry Point IV.

## OBD-II Port

Onboard diagnostics (OBD) tracks a vehicle's condition and driving behaviour. Such information is used by fleet operators and technicians for management and maintenance. The OBD-II port provides access to information on the powertrain, emission control systems, Vehicle Identification Number (VIN), and all kinds of driving information. When targeting the OBD-II port, an attacker could gain access to these sensitive data and possibly even inject malicious code into the CAN bus.

### Risks?

Vehicle hijacking, data breach

### By who?

Nation-states, criminals

### Solution?

AutoCrypt IVS

- Intrusion detection and protection system (IDPS)

AutoCrypt FMS

- Secure fleet management through machine learning and AI
- Proprietary OBD-II units

## Entry Point V.

# Smart Key

Smart keys unlock a vehicle with electronic signals. Unlike keys with buttons, smart keys continuously release signals to allow keyless entry. Thieves could hack the smart key and redirect the signals to unlock and even turn on a car.

### Risks?

Vehicle theft

### By who?

Thieves

### Solution?

AutoCrypt Digital Key

- PKI-based certification and user verification
- Carsharing and restriction settings

## Entry Point VI.

# Telematics Control Unit

The TCU facilitates all wireless communications between the vehicle and the outside world, normally containing an eSIM, radio data system (RDS), Bluetooth, Wi-Fi, and a V2X connectivity unit. When the attacker access the telematics of a vehicle, possibly by injecting malware through a malicious app on a connected smartphone, they could attack the head unit directly.

### Risks?

Vehicle hijacking, vehicle takeover

### By who?

Criminals

### Solution?

AutoCrypt IVS

- Intrusion detection and protection system (IDPS)

AutoCrypt V2X

- User verification via Security Credential Management System (SCMS)