KOFFEE
Kia OFFensivE Exploit

G. Costantino
I. Matteucci

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Automotive attacks

Remote Exploitation of an Unaltered Passenger Vehicle.
C.Miller and C. Valasek, BlackHat 2015

2014

2018

0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars
BlackHat 2019

2020

TBONE – A zero-click exploit for Tesla MCUs
R. Weinmann and B. Schmotzle

2021

2022

Synacktiv Team **@PWN2OWN**
David Berard and Vincent Dehors

What is needed?

Filling the gap between the **current standard and regulation** and **the lack of security solutions** for onboard communications

Automotive Standards and Regulations

AUTOSAR™
Enabling continuous innovations

SAE INTERNATIONAL® J3061

ISO 21434

UNECE WP29/155

2014 2016 2021 2022 2024

ISO 24089 still under development

UNECE R155 - ISO21434

- **R155** - Uniform provisions concerning the approval of vehicles with regards to *cyber security* and *cyber security management system*

March 2021

- **ISO/SAE DIS 21434** - Road vehicles — Cybersecurity engineering

August 2021

UNECE R155 All. 5 - Some Threats

10

Viruses embedded in communication media are able to infect vehicle systems

11

Messages received by the vehicle or transmitted within it, contain malicious content

15

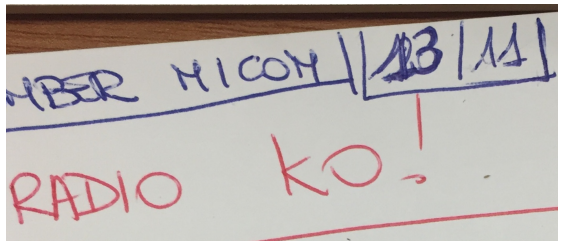
Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack

Timeline \ Responsible Disclosure

07/2019

KIA
Ceed@CNR

13/11/2019



02/2020

KOFFEE

04/2020

Movement that inspires

09/2020

Updated
HU software

11/2020

Technical
paper

12/2020

CVE-2020-8539

04/2021

05/2022

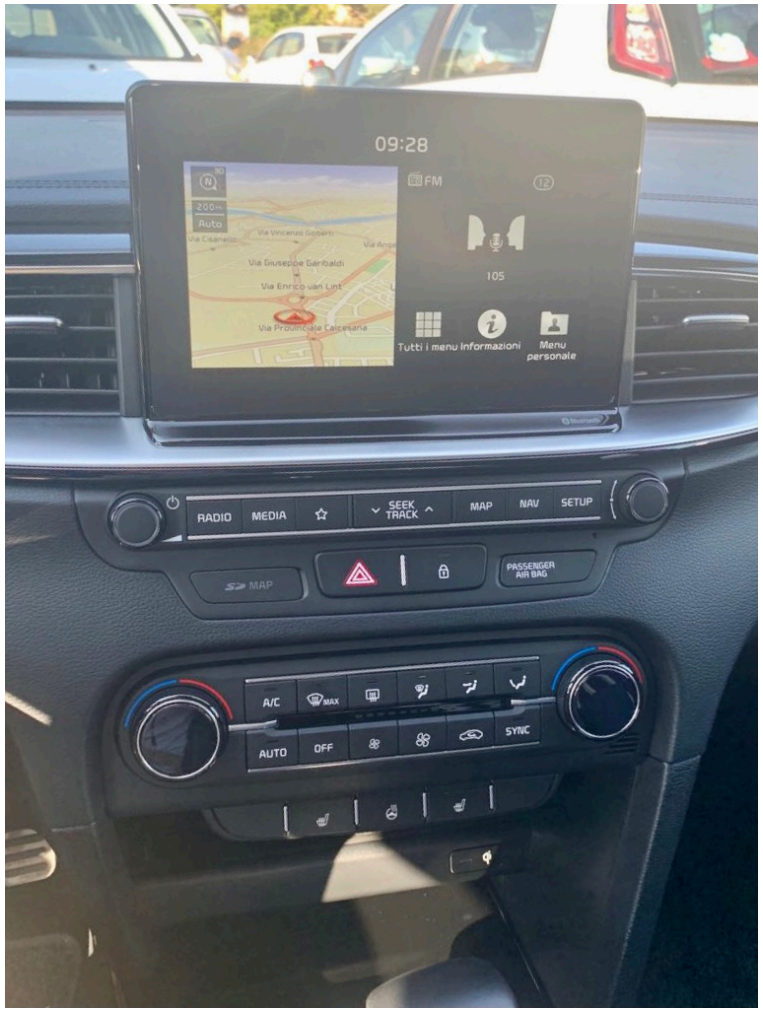
Full paper online

KIA Ceed \ Why?

- Head Unit (HU) with Android OS
- Connection to the Internet (via Hotspot or 4G/5G modem)
- Installation of third-party APPs (not officially)
- HU connected to the CAN bus?
  - *We did not know…*

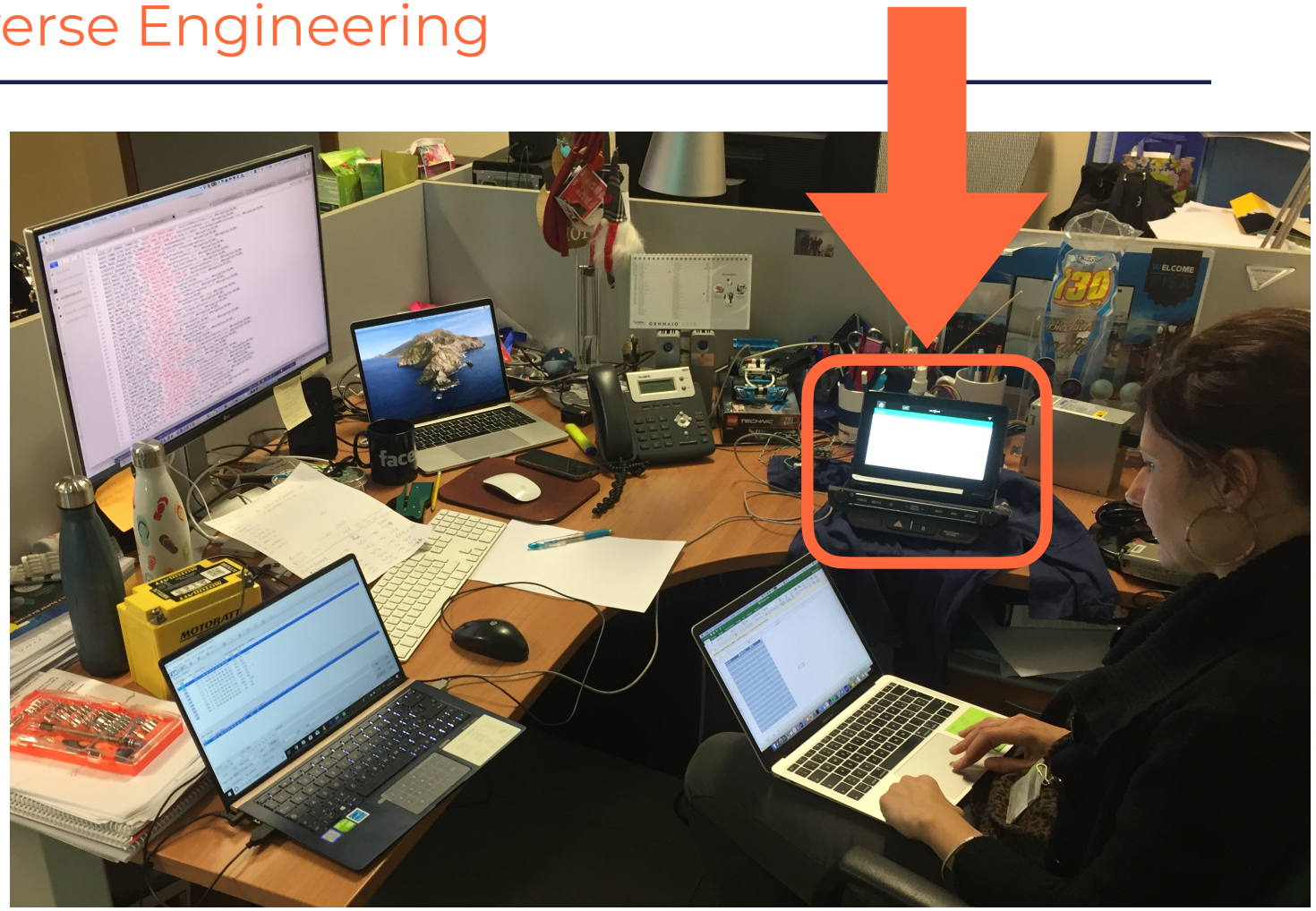
KIA Ceed \ Head Unit

- Gen 5.0, referred with the name *iAVN*
- Android OS version 4.2.2
- CPU ARM Cortex A9 @ 1.2 to 1.5 GHz
- Display 8" touch-screen
- Wi-Fi and bluetooth



KIA Ceed \ Head Unit \ Reverse Engineering

- HU in the lab
- Starting reverse eng:
  - File system
  - All HU apps
- SOP.003.30.18.0703
  - 98 apps
  - 2.654.557 source code lines (java + xml)
  -



KIA Ceed \ Head Unit \ Reverse Engineering \ Decompilation process

Fuzzy search

```
private boolean sendMicomMsg(String msg) {
    try {
        Process process = Runtime.getRuntime().exec("micomd -c inject " + msg);
        process.getErrorStream().close();
        process.getInputStream().close();
        process.getOutputStream().close();
        process.waitFor();
        Thread.sleep(1);
        return true;
    } catch (Exception e) {
        e.printStackTrace();
        Log.e(AutoTestService.LOG_AUTO_TOOL, "Micom command error (sendMicomMsg)!");
        return false;
    }
}
```

KIA Ceed \ Head Unit \ Reverse Engineering \ local attack \ micomd

Goal

- Locally injecting micom message to activate HU functionalities and sending CAN bus frames into M-bus

KOFFEE \ Exploit \ End2End attack

Goal

- Remotely Injecting micom message to activate HU functionalities and sending CAN bus frames into M-bus

KOFFEE

Thank you!