Monthly Research
Research Trend of Automobile Security

FFRI,Inc.
http://www.ffri.jp

Agenda

- The following security conferences were held in Oct. and Nov. 2015.

    - SyScan360 2015 (China, Beijing)
    - Black Hat Europe 2015 (Netherlands, Amsterdam)
    - 13th escar Europe (Germany, Cologne)

- In this report, we introduce some presentations related to automobile security.

Car Hacking: Witness Theory to Scary and Recover From Scare

SyScan360 2015
[2015.10.21-22, China, Beijing]

- Presented by Jinhao Liu, who discovered vulnerabilities of Tesla and BYD in 2014 and 2015.

- There is a vulnerability in the cloud service provided by BYD, so it was possible to steal passwords.

- This problem is similar to "OwnStar" which have been presented at the DEFCON 23.
  - This problem is more dangerous because no special device is required.

Remote Exploitation of an Unaltered Passenger Vehicle

- Presented by Charlie Millar and Chris Valasek.

- It is detailed version of the "Jeep Hack" at Black Hat USA 2015.

- The Jeep Hack had a major impact on the automotive industry.
  - Many people had mentioned it in the escar Asia 2015.

- For specific details, see their white paper.

Self-Driving and Connected Cars:
Fooling Sensors and Tracking Drivers

Black Hat Europe 2015
[2015.11.10-13, Netherlands, Amsterdam]

- Presentation about attacking cameras and radar (LIDAR) for autonomous car technology by Jonathan Petit.

- The experiment target are cameras which used to lane departure warning and rear collision warning, pedestrian warning.
  - The cameras do not work if light of wavelength 650mn is irradiated.

- Also, radar (LIDAR) could allow spoofing by injecting a reflected signal which is disguised as the original signal.

Self-Driving and Connected Cars:
Fooling Sensors and Tracking Drivers (cont'd)

- A vehicle tracking result was shown by sniffing of IEEE 802.11p which is a key technology of connected car.

- A car was tracked with installing the stations in vehicle and intersections.

  - The results showed that the car was tracked highly accurately by sniffing of messages.

Source:https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf
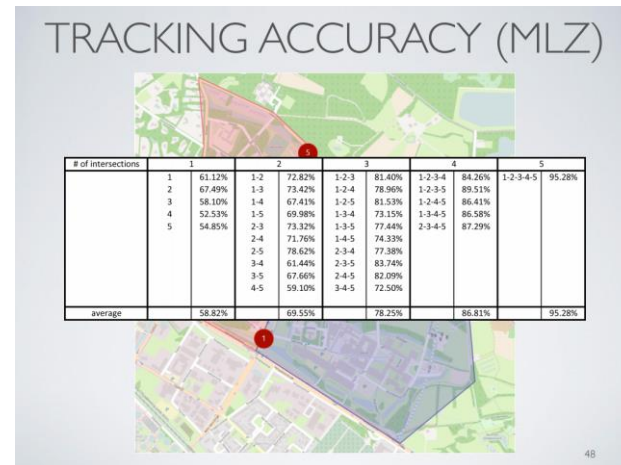
Don't Fuss about Fuzzing: Fuzzing in-Vehicular Networks

13th escar Europe
[2015.11.11-12, Germany, Cologne]

- Presented by Stephanie Bayer at ESCRYPT GmbH
- An idea and result of fuzzing for UDS (Unified Diagnosis Services).
  - UDS is an international standard for vehicle diagnostic protocol (ISO14229).
- They showed a stateful fuzzing which sending various pattern messages based on UDS specifications and the response from ECU.

Fault Severity	Fault Kind	Reproducible	Non-Reproducible
EXPLOITABLE	Garbage Response	6	-
	Server Stopped Responding	-	2
PROBABLY_EXPLOITABLE	Response Timed Out	203	492
PROBABLY_NOT_EXPLOITABLE	Request Not Delivered	1563	-

Table 1: Triggered faults organized by severity and kind

Source:https://www.escar.info/images/Datastore/2015_escar_EU_Papers/3_escar_2015_Stephanie_Bayer.pdf

Common Security Flaws in Connected Cars Systems

```
13th escar Europe
[2015.11.11-12, Germany, Cologne]
```

- Presented by ARGUS Cyber Security, Inc.

- It showed reverse engineering and discovered vulnerabilities of ECU firmware.

- The following vulnerabilities have been discovered.
  - Data leakage from RAM by a vulnerability in the boot loader
  - Known vulnerability in open source library
  - Code injection vulnerability in Operation System
  - Updating microcontroller firmware from application processor
  - Hardcoded JTAG password into the firmware

Summary and Discussions

- Threats in cloud and mobile services
  - Recently vehicles can use telematics service in cooperation with cloud and mobile app.

  - Some of mobile apps can control the vehicle remotely.
    - E.g. open door or start the engine

  - Therefore, security is necessary also in cloud and mobile app.
    - Web security and secure coding for Android/iOS apps are important.

Summary and Discussions (cont'd)

- Security testing approaches for automobile
  - Fuzz tesing
    - Vulnerability research by fuzz testing will not be easy.
    - Ordinary car sometimes shifts to fail-safe mode when it receives an abnormal CAN messages.
    - It might be easy to find vulnerabilities by fuzz testing upper protocols such as the UDS.
  - Penetration testing
    - Fostering of security experts is not easy because it requires time and cost.
    - Some security companies have provided already.
    - However, there is no criteria for these costs and test items.

References

SyScan360 (https://www.syscan360.org/en/)

- Car Hacking: Witness Theory to Scary and Recover From Scare
  - https://www.syscan360.org/slides/2015_EN_AutomotiveCyberSecurity_JianhaoLiu_JasonYan.pdf

Black Hat Europe 2015 (https://www.blackhat.com/eu-15/)

- Remote Exploitation of an Unaltered Passenger Vehicle
  - http://illmatics.com/Remote%20Car%20Hacking.pdf
- Black Hat USA 2015 Survey Report
  - http://www.ffri.jp/assets/files/monthly_research/MR201508_Black_Hat_USA_2015_Survey_Report_JPN.pdf
- SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf
  - https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp2.pdf

13th escar Europe (https://www.escar.info/escar-europe.html)

- Don't Fuss about Fuzzing: In-Vehicular Networks
- Common Security Flaws in Connected Cars Systems

* Requires user registration in order to view and download the slide (FREE)

Contact Information

E-Mail　: research—feedback@ffri.jp
Twitter : @FFRI_Research