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

- 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

- 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.

Don’t Fuss about Fuzzing: Fuzzing in Vehicular Networks

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.

```
<table>
<thead>
<tr>
<th>Fault Severity</th>
<th>Fault Kind</th>
<th>Reproducible</th>
<th>Non-Reproducible</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPLOITABLE</td>
<td>Garbage Response</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Server Stopped Responding</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>PROBABLY_EXPLOITABLE</td>
<td>Response Timed Out</td>
<td>203</td>
<td>492</td>
</tr>
<tr>
<td>PROBABLY_NOT_EXPLOITABLE</td>
<td>Request Not Delivered</td>
<td>1563</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Table 1: Triggered faults organized by severity and kind

Common Security Flaws in Connected Cars Systems

- 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 testing
    - 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.
Summary and Discussions (cont’d)

• Wireless communication for autonomous car
  – OTA update and V2X are the most innovative technologies for in the near future.

  – Therefore, security measures are required to protect safety and privacy naturally.

  – Encryption and authentication are very important for OTA update and V2X communications.
    • We are concerned about increase of attack vectors by evolution of the wireless technology.
References

SyScan360 ([https://www.syscan360.org/en/](https://www.syscan360.org/en/))
- Car Hacking: Witness Theory to Scary and Recover From Scare

- Remote Exploitation of an Unaltered Passenger Vehicle
- Black Hat USA 2015 Survey Report
- SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS

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