Monthly Research

Latest Security Reports of Automobile and Vulnerability Assessment by CVSS v3

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

Background

- Automobile security is hot topic in many conferences.
- Cyber security measures are essential for the automobile.
- We summarize the following topics based on the above background.
  - Presentations at the conferences other than Black Hat USA 2015 and DEF CON 23.
  - Introduction of vulnerability assessment methods of automobile security by CVSS v3.

Agenda

- 24th USENIX Security Symposium Survey
- escar Asia 2015 Survey
- CVSS v3 Overview
- Vulnerability assessment example by CVSS v3
- Conclusions

24th USENIX Security Symposium

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

- Presentation to demonstrate the attack (decipher) for encryption that is used to immobilizer.

- The researchers pointed out two problems (the attack techniques)
  - Partial Key-update Attack
    - Lock bit is not set. (writable)
    - Unlock possible in the default PIN.
    - In addition to the above, it is possible to perform decryption of the cipher in verifying the key bits for each block of 16bits.
  - Weak key attack
    - The secret key that is used in some vehicles was possible to search in a few seconds.

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer (cont.)

- Although this report was to be published in two years ago originally, it has become impossible to publish for injunction was issued by the court.

- Our comments
  - Among the researchers pointed out problems:
    - “Partial Key-update Attack” possible measures by the user.
    - “Weak key attack” measures by experts, such as dealers.

  - When using the encryption, it should also be sufficiently considered the generation and management of (secret) keys.

Fast and Vulnerable: A Story of Telematic Failures

- Vulnerability report of telematics device using OBD-II port.
- Multiple vulnerabilities have been pointed out.
  - CVE-2015-2906, CVE-2015-2907, CVE-2015-2908
- The following issues have been pointed out:
  - The devices it is possible access to the debug console (e.g. Web UI, Telnet) via USB, but there is no authentication.
  - Weak password has been found in the “/etc/shadow”.
    - this also allows access by SSH
  - Possible to send arbitrary CAN messages.

Fast and Vulnerable: A Story of Telematic Failures (cont.)

- Each network services have been bound to all network interfaces.
  - Therefore, some of the attacks might be possible to be carried out over the Internet.

- The device can execute the following commands via SMS.
  - Status, GPS, Reset, Update

- Update process is performed without authentication, not be encrypted.
  - As a result, it is possible to execute any command by exploiting the update process.

Fast and Vulnerable: A Story of Telematic Failures（cont.）

- Our comments
  - Cases of threats that have been pointed out in the “Attacking and Defending Autos Via OBD-II” later became a reality.
  - In the report, researchers are searching for vulnerable devices using SHODAN (http://www.shodanhq.com/)
    - Attackers also are likely to do the same.
  - Cyber security measures of the vehicle is not only OEM and suppliers, should be considered also in the product side of using an interface such as OBD-II.

escar Asia 2015

Attacking and Defending Autos Via OBD-II

- Lecture about vulnerability and threats of OBD-II devices that insurance company had provided.

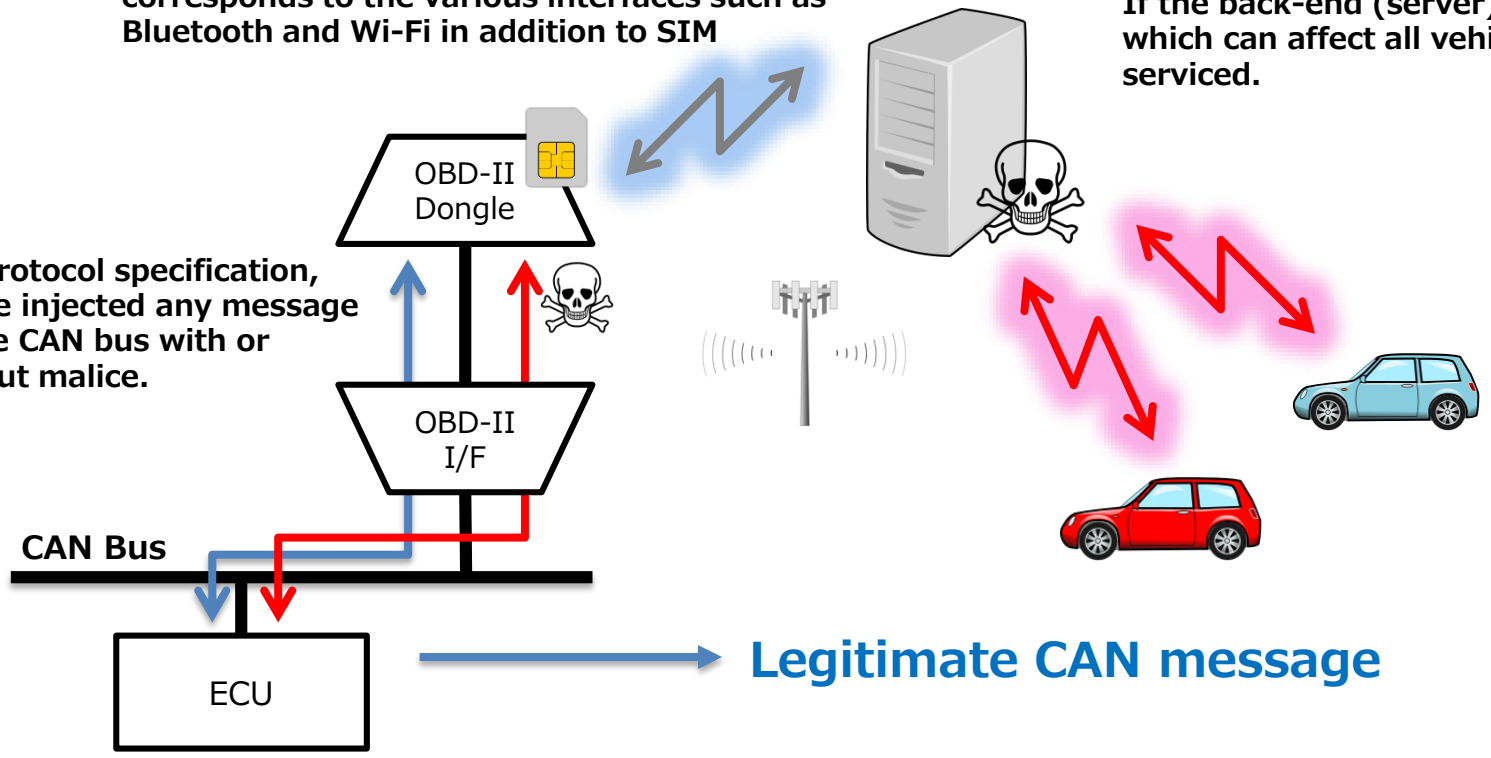
- In the lecture following problems have been pointed out:
  - Data to be sent to the server is not encrypted.
  - It does not have the update function, vulnerability of measures impossible.
  - There is a risk to be sent to any of the CAN message by attack.
  - If the server is attacked, the possibility that there is an impact on all vehicles that use the service.

Attacking and Defending Autos Via OBD-II（cont.）

OBD-II for the adapter there is a product that corresponds to the various interfaces such as Bluetooth and Wi-Fi in addition to SIM

If the back-end (server) is attacked, which can affect all vehicles that are serviced.

The protocol specification, can be injected any message on the CAN bus with or without malice.



Attacking and Defending Autos Via OBD-II（cont.）

- Our comments
  - Recently, devices using the OBD-II has been around for many, these usage should be recognized that there is a possibility that any of the CAN message is injected.
  - In the case of cloud services, security of server-side also should be considered sufficient.

CVSS v3

Overview

- CVSS v3 is a method to evaluate vulnerability of component units.
  - For more information refer to the following URL.
  - https://www.first.org/cvss

- In CVSS v3, impact assessment and attack difficulty evaluation by the attack are separated.
  - Furthermore, the assessment of the impact “extent of influence (scope)” is taken into account.

  - CVSS v3 to risk assessment in the component unit is considered to be effective in the information security analysis for automotive.

- As a risk assessment of the vulnerabilities reported by USENIX, we calculate each of the base score of CVSS v3 and v2.

The risk assessment example by CVSS v3

(1) Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer

(2) Fast and Vulnerable: A Story of Telematic Failures (Same as CVE-2015-2906, 2907 and 2908)

評価項目	(1)		(2)	
	CVSS v3	CVSS v2	**CVSS v3**	CVSS v2
AV：Access/Attack Vector	**Adjacent**	Adjacent	**Network**	Network
AC：Access/Attack Complexity	**High**	High	**Low**	Low
Au：Authentication	**—**	None	**—**	Single
PR：Privileges Required	**None**	—	**Low**	—
UI：User Interaction	**Required**	—	**None**	—
S：Scope	**Unchanged**	—	**Unchanged**	—
C：Confidentiality Impact	**High**	Complete	**High**	Complete
I：Integrity Impact	**None**	None	**High**	Complete
A：Availability Impact	**High**	Complete	**High**	Complete
Base Score	**6.4**	**6.2**	**8.8**	**9.0**

Conclusions

- Devices that directly connect to the CAN bus also should consider security measures enough.
- To consider the risk of wireless sniffing. (Similar to wired)
- Considerations of encryption
  - Method of generating a secret key.
  - Generate key management, protection method.
- CVSS v3 is effective possibilities even on to examine the information security analysis and measure of automotive from the fact that can vulnerability assessment in the component units.

References

- Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer
  - https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/verdult
- Fast and Vulnerable: A Story of Telematics Failures
  - https://www.usenix.org/conference/woot15/workshop-program/presentation/foster
- Vulnerability Note VU#209512
  Mobile Devices C4 OBD2 dongle contains multiple vulnerabilities
  - https://www.kb.cert.org/vuls/id/209512
- Welcome to escar Asia The leading automotive Cyber Security conference
  - http://techon.nikkeibp.co.jp/seminar/escar_e/
- Common Vulnerability Scoring System v3.0: Specification Document
  - https://www.first.org/cvss/specification-document
- CVSS Calculator >> English Version
  - http://jvndb.jvn.jp/cvss/en.html
- CVSS v3 Calculator >> English Version
  - http://jvndb.jvn.jp/cvss/v3/en.html