Monthly Research

Current state of automotive network security

FFRI,Inc.

http://www.ffri.jp

Ver 2.00.01

Background

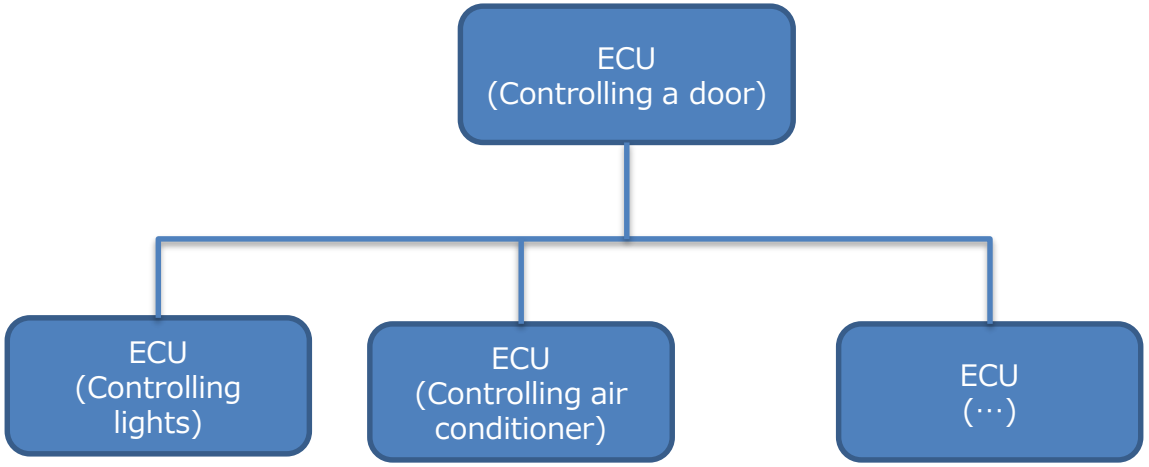
- Many electronic devices have been used by automobiles
- These devices are connected each other and communicate to control automobiles
- Recent years, automotive network has been connected to smartphones and the internet. It makes new threats turn up.
- This slides summarizes how automotive network security have been and what is expected as incoming threats.

Automotive networks

- Contemporary automobiles consist of many electronic devices.
- Electronic controls are used in many parts of automobiles such as engines, brakes and doors and they are connected each other.
  - They communicate each other and do proper controls
    - Display current speed
    - Locking a door and so on
- Representative automotive networks are CAN, LIN and FlexRay

CAN (Controller Area Network)

- De facto standard of automotive networks
- It connects ECUs(Electronic Controller Unit) and provides communication by broadcasting
- ODB-II port(for diagnostic use) can be used to access CAN



Reported problems about automotive networks 1

- In 2010, K. Koshcer at University of Washington published "Experimental Security Analysis of a Modern Automobile"
  - Shows practical security risks of CAN
  - Accesses CAN via ODB-II
  - DoS attack and rewriting memory on ECUs are feasible
  - Shows threats such as faking speed meter, disable brakes
  - Points out a possibility of malicious code injection into ECU

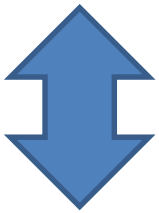
Reported problems about automotive networks 2

- In 2013 at DefCon21, Charlie Miller presented actual proof of threats for automotive networks
  - Presented concrete methods of analyzing CAN packets and result of the analysis
    - Ford Escape
    - Toyota Prius are the actual targets
  - Showed actual proof of stopping engines and rewriting firmware

Problems and threats of CAN and ECU

- CAN is broadcast base protocol. It is easy to eavesdrop communications
- CAN's specification does not have an authentication process
  - Arbitrary packet can be sent to ECU
  - ECU do not have method to authenticate it

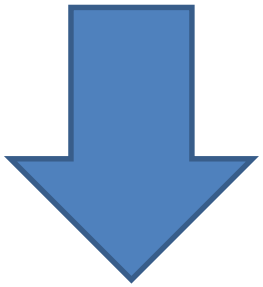
  (However, diagnostic protocol (UDS) has an authentication standard for ECU implementation)
- Rewriting ECU programs is possible



Trade-off against requirements for automotive networks such as real-time processing, maintainability, cost

New threats

- Recent years, automotive network has been connected to smartphones and the internet
- It is now more likely to happen malware attacking and remote attack via smartphones
- Android devices connected to automotive and wireless adaptors also have been appearing



Possibility to access automotive networks remotely

Proposed measures

- Mainly 2 directions
  - Making conventional network more secure

    Example:
    - Cyber-Security for the Controller Area Network (CAN)Communication Protocol http://www.eecs.berkeley.edu/~cwlin/publications/40108_13.pdf
      - Securing CAN communication itself. Make it possible to authenticate packets between ECUs.
  - New measures for new threats

    Example:
    - Towards a Secure Automotive Platform http://www.secunet.com/fileadmin/user_upload/Download/Printmaterial/english/sn_Whitepaper_Secure_Automotive_Platform_E.pdf
      - Access control to automotive network using ARM TrustZone
      - Devices connected to automotive networks such as Android devices are the target (Threats as an attack vector)
      - Virtually switch CPU running Android and CPU communicates automotive networks.
      - No influence to automotive network when Android side has a problem

Summery

- Recent years, they point out the problems on CAN which is de facto standard of automotive networks
- Currently there are actual proof of intrusion into CAN via ODB-II port
- In future, it may be realized to the intrude as connection to automotive networks from more smartphones and the internet accelerates.
- It is proposed to secure network protocols (authentication, tampering detection) and to make access control to automotive network using TrustZone
- As more devices are connected to automotive networks, to keep taking actions to new threats are required

References

- 車載ネットワーク・システム徹底解説 (佐藤道夫 CQ出版社 2005)
- Experimental Security Analysis of a Modern Automobile
  http://www.autosec.org/pubs/cars-oakland2010.pdf
- Adventures in Automotive Networks and Control Units
  http://www.exploit-db.com/download_pdf/27404/
- 2011年度自動車情報セキュリティの動向に関する調査
  http://www.ipa.go.jp/files/000024413.pdf
- 2012年度自動車情報セキュリティの動向に関する調査
  http://www.ipa.go.jp/files/000027274.pdf
- 組み込みシステムのセキュリティ～～自動車情報セキュリティの視点から～～
  http://www.ipa.go.jp/files/000013557.pdf
- Cyber-Security for the Controller Area Network (CAN) Communication Protocol
  http://www.eecs.berkeley.edu/~cwlin/publications/40108_13.pdf
- Towards a Secure Automotive Platform
  http://www.secunet.com/fileadmin/user_upload/Download/Printmaterial/englisch/sn_Whitepaper_Secure_Automotive_Platform_E.pdf

Contact Information

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