Comprehensive Experimental Analyses of Automotive Attack Surfaces

1. Target system & service (Contributed by YongHwa Lee)

- Target System : Target system itself.
- Target Service : target services running on the target system.

* Modern automobiles with various remote attack surfaces

  * Especially those automotive systems with indirect physical access, short & long range wireless access

    * Indirect physical access

      * OBD-II / Entertainment (Disc, USB, iPod)

    * Short-range wireless access

      * Bluetooth / Remote Keyless Entry / TPMS / RFID / 802.11 WiFi, etc.

    * Long-range wireless access

      * Broadcast channels / Addressable channels

2. Vulnerability (Contributed by YongHwa Lee)

- Vulnerability : What is the bug of the system? What is the main problem of the system?

* Practical vulnerabilities in external attack surfaces that permit arbitrary automotive control without direct physical access

  * Indirect physical channels

    * Media player

      * CD-based firmware update attack / ISO 9660 filesystem arbitrary code execution / WMA (CD) parser buffer overflow

    * OBD-II

* Using PassThru device, malicious binary can be installed in target car, then CAN buses can be hacked and finally, malformed CAN packets install malwares onto the car's telematics units.

* Short-range wireless channels - Bluetooth

* Unsafe strcpy functions in the Bluetooth configuration command can be exploited and they can be used in execution of arbitrary code on the telematics unit.

* Long-range wireless channels - Cellular

* Stack-based buffer overflow vulnerability in the aqLink modem's Gateway program / Vulnerable authentication process

3. Exploitation (attacks) (Contributed by YongHwa Lee)

- How to trigger the vulnerabilities mentioned in Section 2?

* Vulnerable diagnostics equipment, modified songs in WMA format, hands-free Bluetooth, crafted audio signals, etc can be used in various exploit scenarios.

* TPMS ECU via CAN installs malicious code / Modified Bluetooth exploit code for ECU / Exploit packets on FM RDS channels / etc.

4. Evaluation and experimental method (Contributed by TA)

- How the authors exploited target services? (the environment and evaluation methodologies)

* CDs : Reverse Engineering on the same device what embedded on the vehicle because the device can be obtained easily from major companies and embed bad WMA file to the player

* OBD-II port : Reverse Engineering on PassThru Device and implement malicious shell injection binary

* Bluetooth : Reverse Engineering on bluetooth module and implement simple Trojan application on the mobile

* Cellular : Implement malicious exploitation code to trigger vulnerability

5. Defense (potential solutions for the attacks) (Contributed by YongHwa Lee)

- How to prevent those vulnerabilities and exploitation?

* Simply setting a small limitation to vulnerable attack surfaces

* Let the driver manually place the vehicle in pairing Bluetooth / Using inbound calls only to "wake up" the car (never for data transfer)

* Using application-level authentication and encryption (e.g., OpenSSL) in the PassThru configuration protocol

* Simple anti-exploitation mitigations (Stack Cookies, ASLR)

* Reducing attack surfaces of several units in vehicles like 'telnetd', 'ftp', 'vi' which are installed basically with no reason.

* Secure software updates

6. Question to the presenter (Contributed by Hyunsik, JoonHa, Taehwa)

* Because the paper presented in 2011, there are many differences on automobiles from the present. What attack surfaces can be added more, in 2021?

* If you look at modern cars, the OBD2 port is a fairly open port. I wonder if there is a follow-up study or paper that analyzes whether an IEMI attack is possible against this port.

* Can an attacker exploit just with the external charging cable?