Title: Comprehensive Experimental Analyses of Automotive Attack Surfaces
Venue: USENIX Security '11
Name: Sujin Han 한수진 **Student ID**: 20223705

Summary

- Target System & Service
  - Automobiles. The attack surface is limited to external surface.
  - Attacks can be delivered through one of the following modalities:
    - Indirect physical access
      - OBD-II, devices used for entertainment (Disc, USB and iPod)
    - Short-range wireless access
      - Bluetooth, Remote Keyless Entry, Tire Pressure Monitoring Systems (TPMS), RFID car keys, Emerging short-range channels (Wifi, DSRC)
    - Long-range wireless access
      - Broadcast channels (GPS, Satellite Radio, Digital Radio, RDS, TMC), Addressable channels (used to connect cellular voice and data networks)

- Vulnerability
  - Most automobile operations are controlled by ECUs (Electronic Control Units) and ECUs are interconnected by common wired networks (usually CAN).
  - Indirect physical channels
    - **Media Player** – (1) latent update capability allows flashing media player (2) parses complex files and contains BOF
    - **OBD-II** – connects to PassThru device, which can compromise vehicle through OBD-II /two ways to compromise PassThru (1) attacker on the same Wifi network as PassThru can connect to it (2) PassThru itself can be compromised
  - Short-range wireless channels (**Bluetooth**)
    - unchecked strcpy vulnerability exist in custom -built part of telematics system
  - Long-range wireless channels (**Cellular**)
    - discrepency between set of packet sizes supported by aqLink and buffer allocated by the telematics client code results in BOF / logic flaw in authentication system

- Exploitation (Attacks)
  - Indirect physical channels
    - **Media Player** – flash media player or exploit BOF to execute arbitrary code
    - **OBD-II** – executed shell injection through the reported vulnerabilities
  - Short-range wireless channels (**Bluetooth**)

        - Implemented a Trojan Horse application for indirect attack
        - Pair attacker's device to car using car's Bluetooth MAC address for direct attack
    - Long-range wireless channels (**Cellular**)
        - Implemented end-to-end attack on laptop running custom aqLink-compatible system modem calls

- Evaluation and Experimental Method
    - Moderately priced late sedan was used.
    - To obtain exploit, performed (1) raw code analyses, (2) in situ observations, and (3) interactive debugging with controlled inputs on each firmware extracted and reverse-engineered from ECUs in target vehicle.
    - Implemented attack and tested whether authors were able to gain complete control over the vehicle systems with the attack

- Defense (Potential Solutions for the Attacks)
    - Restrict access
        - Require device to be physically placed in car first before Bluetooth pairing
        - Use inbound calls only to "wake up" the car, not for data transfer…etc
    - Improve code robustness
        - Do not use unsafe functions like strcpy
        - Adopt anti-exploitation mitigations (ex. Stack cookies, ASLR) …etc
    - Fix interface boundary problem
        - Car manufacturers should be aware of code in ECUs and how they work together

- Question to the Presenter
    - Were there any reported incidents of remote hacking of a car?
    - Authors mention improving code robustness as a defense strategy. Since automobiles consist of millions of lines of code, do you think this is a reasonable solution?
    - Authors identify that most of the vulnerabilities stem from interface boundary problem. Are there any effective solutions to this problem? (other than the car manufacturer taking care of everything?)