Monthly Research 2016.12

Black Hat Europe 2016 Survey Report

F F R I , Inc.
http://www.ffri.jp/en

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

Contents

- About Black Hat
- Intriguing reports
  - Breaking BHAD: Abusing Belkin Home Automation Devices
  - (PEN)TESTING VEHICLES WITH CANTOOLZ YACHT – YET ANOTHER CAR HACKING TOOL
  - Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks
- Conclusions
- References

About Black Hat

- The Black Hat is the most famous security conference in the world

- Researchers from various countries talk a cutting-edge of technology which is focused cyber security in this conference
  - They talk various genres such about new threats, exploit techniques, defense technologies and so on
  - They have breakthrough or advantage
  - Their presentations are public on the web

- The conference is held annually in the US, Europe, Asia

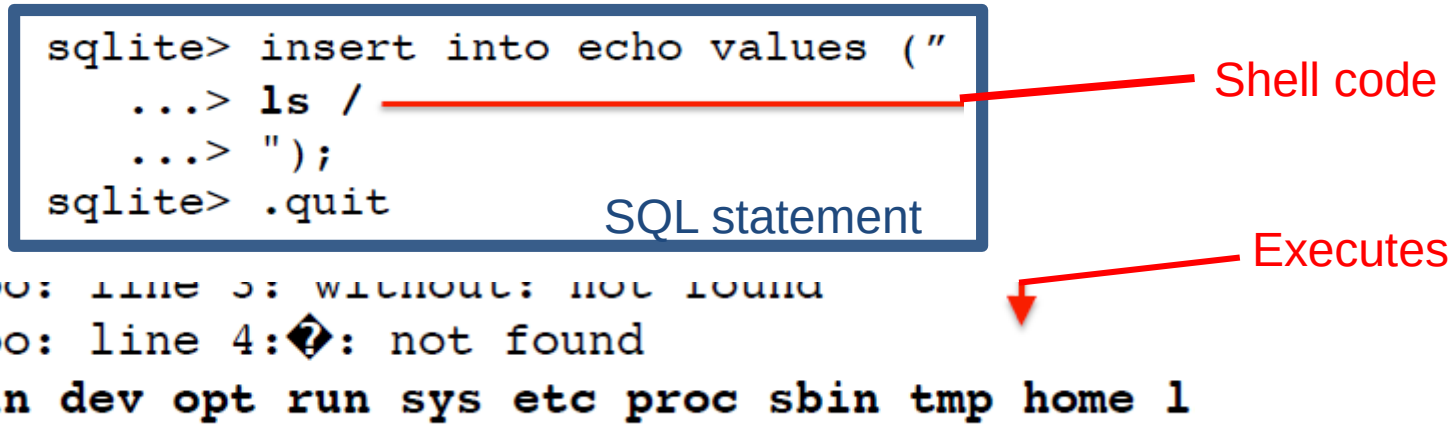
- In this report, we introduce some presentations relative to IoT, automotive security, targeted threat at Black Hat Europe 2016

Intriguing reports

- IoT
  - Breaking BHAD: Abusing Belkin Home Automation Devices
    - Joe Tanen, Scott Tenaglia
- Vehicle
  - (PEN)TESTING VEHICLES WITH CANTOOLZ YACHT – YET ANOTHER CAR HACKING TOOL
    - Alexey Sintsov
- Targeted threat
  - Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks
    - Andrew Blaich, Max Bazaliy, Seth Hardy

Breaking BHAD: Abusing Belkin Home Automation Devices

- The researcher talked about the vulnerability involved SQL injection and executing arbitrary code in the WeMo
- About WeMo
  - WeMo enables to remotely control the switch of home devices (e.g., TVs, lamps, etc.) connected it via a smartphone app
- OpenWRT in the WeMo is using “ash” as the default shell
- SQL injection technique is used to execute a shellcode in the WeMo
  - WeMo had been found a similar vulnerability in the past



Breaking BHAD: Abusing Belkin Home Automation Devices

- The mechanism of root login using telnet
  - An attacker uses SQL statement including two shellcodes
    - Shellcode1 provides a backdoor to shell access over telnet
    - Shellcode2 writes the shellcode1 to script in /lib/network
  - The script will be executed when the network service is restarted using StopPair command
  - As the result, an attacker will be able to infiltrate to WeMo as the root user

- The mechanism of getting local root by physical access
  - In order to access the boot loader named U-Boot needs to connect to a substrate of WeMo directly and press “4” key repeatedly during the startup
  - The mini_fo restricts to write to root file system in JFFS2 from the SquashFS
  - On the other hands, mini_fo does not restrict read, therefore it can get the /etc/passwd file
  - Mount the newly created JFFS2 that is not including root password using loadb command in U-Boot

(PEN)TESTING VEHICLES WITH CANTOOLZ YACHT – YET ANOTHER CAR HACKING TOOL

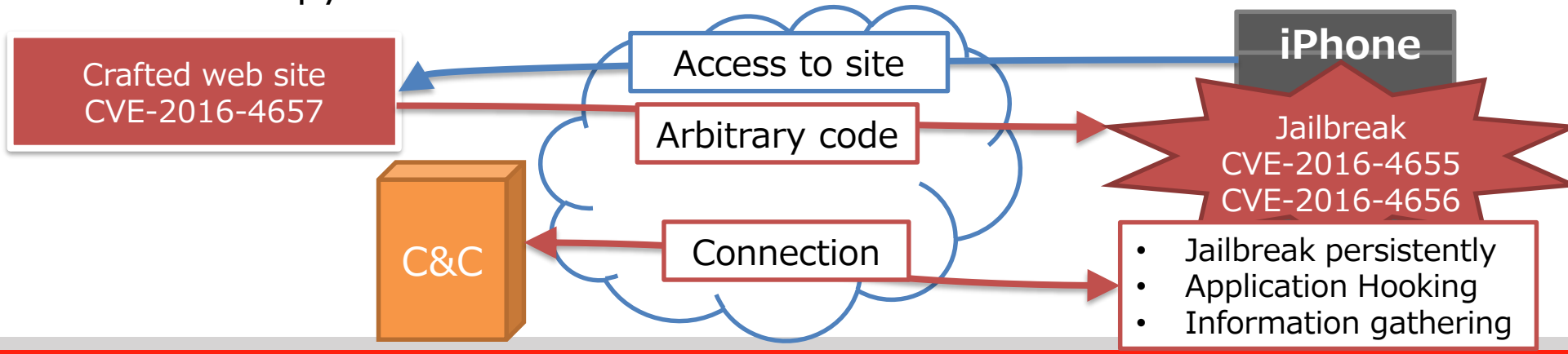
- A vehicle has many attack surfaces
  - For example, remote attack from Wi-Fi inside HU, physical attack to CAN bus from a disguised ECU, etc.
- Various researchers who interest automotive security feel the need for an integrated analyzing tool
- About CANToolz
  - Open source framework
    - https://github.com/eik00d/CANToolz
  - Various modules are ready-to-use
    - MITM, fuzzer, UDS(Unified Diagnostic Services) scanner, CAN firewall, etc.
  - Hardware I/O modules support USBTin and CANBus Triple

(PEN)TESTING VEHICLES WITH CANTOOLZ YACHT – YET ANOTHER CAR HACKING TOOL

- CAN over TCP module
  - This module provides remote control with TCP
- Car emulator module
  - The module emulates a vehicle ECU to provide to simulate the CAN network
  - It can control from WebUI
- Various modules in CANToolz provide efficiently reverse-engineering and black-box testing for the CAN network in actual vehicle
  - CAN messages analysis
  - MITM (UDS session hijacking)
  - Fuzz testing, etc.

Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks

- Mr. Ahmed Mansoor who is an internationally recognized human rights defender was attacked in this summer
- Pegasus for iOS spyware was used that attack
  - The researchers analyzed the source code of Pegasus
  - They talked about the spyware and vulnerabilities it exploited
- About the Pegasus
  - The spyware jailbreaks the iOS persistently and enables executing arbitrary code with administrative privileges
  - The spyware uses three vulnerabilities called "Trident"



Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks

- Function of the Pegasus
  - Techniques to gather data
    - Records any microphone usage, video from camera
    - Gathers sim card, cell network information, GPS location, keychain passwords
  - Application Hooking
    - After Jailbreak, Pegasus installs the “hooks” app
  - Anti Analysis
    - Techniques to prevent detection and analysis
      - One time use links
      - Source code is obfuscated and encrypted with a different key on each download
      - Spyware components are hidden as system services
      - Clears Mobile Safari history and caches
    - Techniques to stay undetectable
      - Blocks iOS system updates
      - Removes itself

Conclusions

- IoT
  - A remotely controllable device for security or heating (e.g., surveillance camera, electric heater, etc.) may cause greater damages
  - Vulnerable IoT devices may be joined a botnet by an attacker
- Vehicle
  - We expect that the CANToolz help us to find vulnerabilities more efficiently and more researchers interest the automotive security
- Targeted threat
  - The iOS was believed to be relatively safe
  - This session clarified the targeted threat to iOS
  - The mobile device need to attention to the targeted threat
- Throughout the report
  - These sessions which we introduced are independent of each other
  - Different genre will become relevant by advance of the IoT
  - Security experts need to review security from a wider perspective

References

- Black Hat Europe 2016
  - https://www.blackhat.com/eu-16/
- (PEN)TESTING VEHICLES WITH CANTOOLZ YACHT – YET ANOTHER CAR HACKING TOOL
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Sintsov-Pen-Testing-Vehicles-With-Cantoolz.pdf
- Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Bazaliy-Mobile-Espionage-in-the-Wild-Pegasus-and-Nation-State-Level-Attacks.pdf
- Breaking BHAD: Abusing Belkin Home Automation Devices
  - https://www.blackhat.com/docs/eu-16/materials/eu-16-Tenaglia-Breaking-Bhad-Abusing-Belkin-Home-Automation-Devices.pdf