Monthly Research 2016.6

Black Hat USA 2016 Pre-Survey

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

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

Outline

- About Black Hat USA
- Featured Research
  - Vehicle Security
  - IoT Security
- Conclusions
- References

About Black Hat USA

- The world's most famous security conference in Las Vegas every August
  - This conference will be held from July 30 - August 4 in this year
  - Briefings of cutting-edge security research
  - Abstracts have been published

- About 20 sessions into the Internet of Things & Hardware/Embedded in this conference
  - There are 25/50 minute briefings

- In this report, we introduce some hot research

Featured Research

- Vehicle Security
  - CANSPY: A Platform For Auditing CAN Devices
  - Advanced CAN Injection Techniques For Vehicle Networks
- IoT Security
  - Into The Core – In-Depth Exploration of Windows 10 IoT Core
  - GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool
  - GreatFET: Making GoodFET Great Again

Vehicle Security (1)

- CANSPY: A Platform For Auditing CAN Devices
  - Arnaud Lebrun, Jonathan-Christofer Demay (Airbus Defence and Space)
  - Rewrite and block CAN messages on the fly
    - Like the Burp(security testing for web app)

- Advanced CAN Injection Techniques For Vehicle Networks
  - Charlie Miller, Chris Valasek (Uber ATC)
  - There are various restrictions on vehicle hijacking by CAN message injection
  - Meter hijack is easy, but steering and brake hijack is hard
  - This presentation will introduce bypass technique for brake, steering and acceleration hijacking

Vehicle Security (2)

Keyword is "CAN"

- CAN has no security
- Many people have concerned about security
  - Easy to send/receive CAN message
  - Various device are connected on CAN bus

Attention to vehicle hijack condition and strategy

- Abstract indicate has some conditions(car speed, etc.,) for vehicle hijacking
  - It is possible to control brake and steering by CAN message injection when the vehicle is slower
- Parking assist system will be abused for bypassing the restriction
- Related study
  - ADAS (emergency brake) was disabled by CAN messages injection from the research group of the Ritsumeikan University , Japan

IoT Security (1)

- Into The Core – In-Depth Exploration of Windows 10 IoT Core
  - Paul Sabanal (IBM Security X-Force)
  - This presentation introduces Windows10 IoT Core as an important new generation IoT Platform
    - Attack vector and malware attack
    - Announces security assessment technique by static/dynamic analysis and fuzzing

- GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool
  - Slawomir Jasek (SecuRing)
  - Disguised BLE device connects the victim device without consent of the mobile apps or devices
  - The BLE device intercepts BLE communication as proxy
  - This presentation interprets expected attack and announces BLE MITM proxy for debug and inspection

IoT Security (2)

- GreatFET: Making GoodFET Great Again
  - Michael Ossmann (Great Scott Gadgets)
  - In this presentation, announce about GoodFET for the open source JTAG adapter

Hardware knowledge is required for IoT security

- It is need to access to bus and I/O interface for IoT device assessment
  - General IoT devices have RJ45 Ethernet port for internet connection
  - The edge hardware (device as well as IC and LSI) are connect by bus (UART, SPI and I2C)
  - The open source hardware become help security engineer
    - GoodFET, Hardsploit, etc.,

IoT Security (3)

A threat analysis of new platform

- The FFRI Researcher have presented threat analysis of Win10 IoT Core in CODE BLUE 2015
- That presentation call was attention about non-attestation FTP and that abuse Malware
- We look forward to that research is announced

Bluetooth(BLE) is used for many IoT device

- We think BLE will be target of attack
- Related research
  - Smart Wars: Attacking SmartLocks with a Smart Phone
  - Research of smartlocks vulnerability at CanSecWest Vancouver 2016(Jan. 2016)
  - Technique for intervene to pairing
    - Use to DoS attack

Conclusions

- We have attention to vehicle security
  - The CAN requires additional security
- IoT security needs is increased in the continue
  - We have to get more hardware/embedded of knowledge
- Hardware hacking will become easy
  - Many open hardware hacking tools were released
    - GoodFET, Hardsploit and etc.
- The other conferences are also checked July and August, enjoy:)
  - Shakacon VIII, Bsides Las Vegas, DEFCON 24, USENIX ‘16, etc.,..

References

- Black Hat USA 2016 Official
  - https://www.blackhat.com/us-16/
- DEFCON 24
  - https://defcon.org/html/defcon-24/dc-24-index.html
- Bsides Las Vegas
  - https://www.bsideslv.org/
- REcon 2016
  - https://recon.cx/2016/
- Shakacon VIII
  - https://www.shakacon.org/
- USENIX
  - https://www.usenix.org/
- CanSecWest Vancouver 2016
  - https://cansecwest.com/
- Threat Analysis of Windows 10 IoT Core and Recommended Security Measures
  - http://codeblue.jp/2015/en/contents/speakers.html#speaker-waguri