



Monthly Research 2016.08
Black Hat USA 2016
Survey Report

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

E-Mail: [research-feedback\[at\]ffri.jp](mailto:research-feedback[at]ffri.jp)

Twitter: @FFRI_Research

Contents

- About Black Hat USA
- Hot Research
- Vehicle
 - CANSPY: A Platform For Auditing CAN Devices
 - Advanced CAN Injection Techniques For Vehicle Networks
 - Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle
- IoT
 - 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
- Conclusions
- References

About Black Hat USA

- The world's largest security conference in Las Vegas at every August
 - Briefings of cutting-edge security research
 - Threat demo, exploit technique, defense technology
 - They have breakthrough or advantage
 - Slides and papers are public on the Web
 - Yuji Ukai, CEO of FFRI, Inc. is a member of the review boards
 - There was published many tools and projects
 - Apple launches bug bounty project the Apple Security Bounty
- Many security events (DEFCON, BSideLV, USENIX) were held near term
- In This Slide, we introduce hot research in Black Hat USA 2016

Hot Research (1)

- Vehicle
 - CANSPY: A Platform For Auditing CAN Devices
 - Jonathan-Christofer Demay & Arnaud Lebrun
 - Advanced CAN Injection Techniques For Vehicle Networks
 - Charlie Miller & Chris Valasek
 - Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (DEFCON 24)
 - Jianhao Liu, Chen Yan, Wenyuan Xu

Hot Research (2)

- IoT
 - Into The Core – In-Depth Exploration of Windows 10 IoT Core
 - Paul Sabanal
 - GATTacking Bluetooth Smart Devices Introducing a New BLE Proxy Tool
 - Slawomir Jasek
 - GreatFET: Making GoodFET Great Again
 - Michael Ossmann

CANSPY: A Platform For Auditing CAN Devices (1)

- Capture tool for the CAN bus
 - Circuit board data and software are open source
 - <https://bitbucket.org/jcdemay/canspy>
- Connect to OBD-II
 - It intercepts like server-client MITM attack
 - Intercept in-between bus for ECU-ECU
- Analyze of captured frame
 - CAN protocol stack is SocketCAN
 - SocketCAN is supported by the Wireshark
 - We are able to analyze captured frame by writing a dissector

CANSPY: A Platform For Auditing CAN Devices (2)

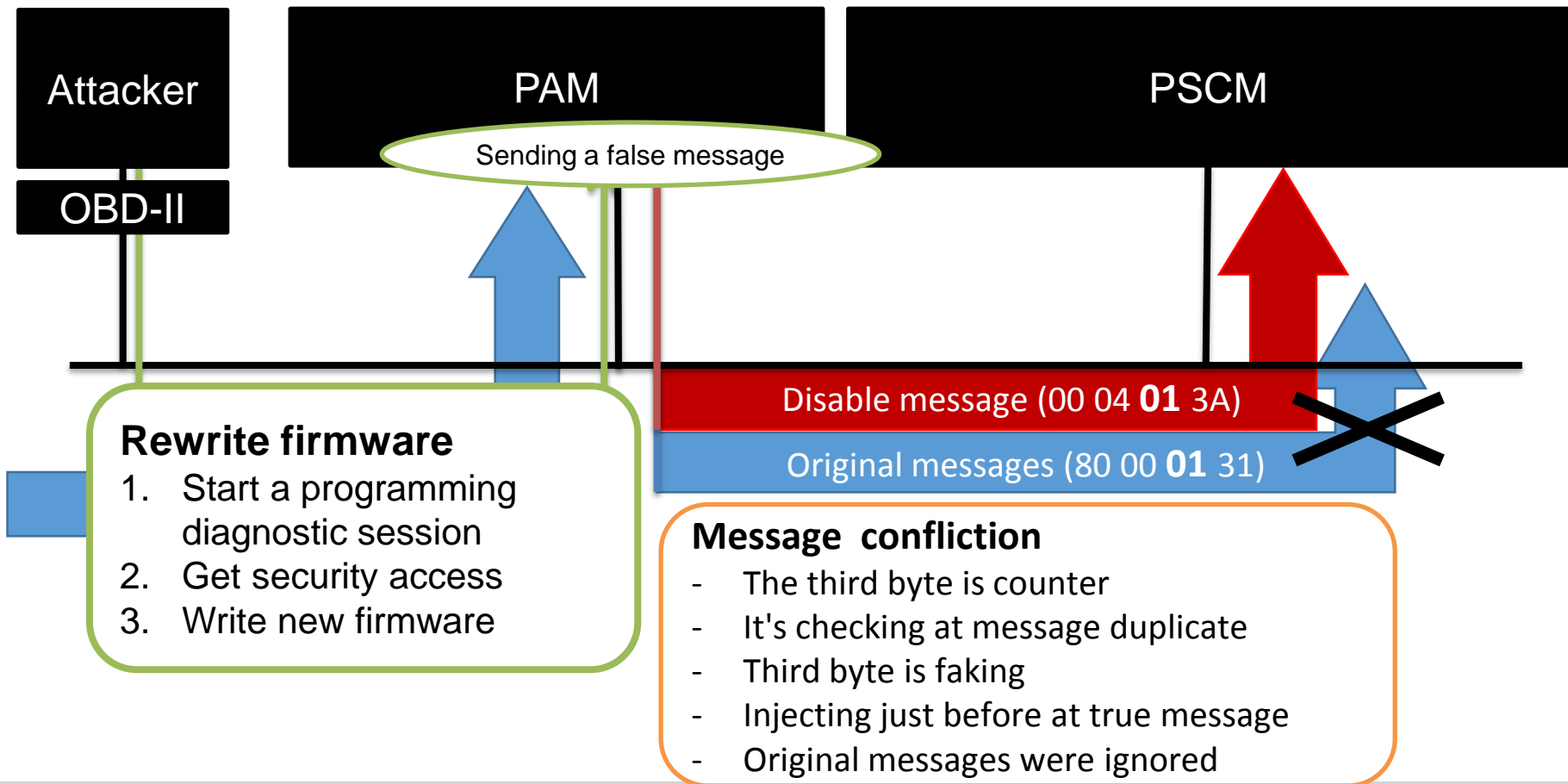
- PC-ECU connection(CAN over Ethernet)
 - Sniffing and bridging CAN bus from PC
 - Inject CAN message using bridge service
 - Rewrite frame and packet using Scapy
- **Comments of FFRI researcher**
 - CANSPY is high-quality analysis tool
 - Point of improvement
 - The internal filtering capabilities
 - This tool is useful for analysis for non real time function
 - E.g.) Fault diagnosing function and device

Advanced CAN Injection Techniques For Vehicle Networks (1)

- Continued research called "Jeep Hack" by Charlie Miller and Chris Valasek
 - That is drawing any attention and extensively quoted in the media
- Researchers were getting a "Pwnie for Best Junk or Stunt Hack" on The Pwnie Awards for 2016
- They were able to control steering even when the car is driving at high speed
- Brake, accelerator and steering were bypassed restriction at the Parking Assist Module(PAM) and the Adaptive Cruise Control
 - They disguised packet for speed camouflaging
 - PAM haven't gotten speed from the legitimate ECU
- Rewrite firmware on the Power Steering Control Module (PSCM) ECU
 - PSCM firmware has a 16bit checksum
 - It is bypassed in less than 9 hours
- Message injection and confliction
 - PAM disables message and restart ECU at message confliction
 - E.g.)The car is stopped > Attacker suddenly injected "100 mph" > Confliction

Advanced CAN Injection Techniques For Vehicle Networks (2)

Rewriting firmware and measuring message conflict



Advanced CAN Injection Techniques For Vehicle Networks (3)

- Jeep and Prius are different correspondence to the unreliable sudden braking messages
 - Jeep: Cancel messages and restart ECU
 - Prius: Non check, activate the brakes
 - Toyota seems to give priority to safety
- CAN injection countermeasures
 - Automobile manufacturers fix the danger algorithm
 - Monitoring of CAN message frequency
- **Comments of FFRI researcher**
 - Vehicle has many system, so it is necessary to take measures and threat analysis of the various points of view
 - Research related to "arrival frequency of message" is already exist

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (1)

- This research was published DEF CON 24
- Presented by Chinese university and the Qihoo360 researchers
- Attack various sensors in vehicle
 - This attack has been verified in the actual vehicle sensors
 - The Tesla, The Audi and others
 - Similar research was published the Black Hat EU 2015
- Vehicle sensors are important for ADAS
 - E.g.) Ultrasonic sensors, Millimeter Wave Radars
- Attacking methods
 - Jamming
 - Common frequency intense noise to denial of service
 - Spoofing
 - Signal which was disguised as a valid signal
 - Relay
 - Relay received signal

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (2)

- Attacking Ultrasonic Sensors
 - This sensor measures the distance to obstacle
 - Researchers experimented two types of attack
 - Jamming
 - Irradiate the ultrasonic wave to the sensor
 - The sensor can't receive reflected wave
 - Therefore, Sensor doesn't recognize the obstacle
 - Spoofing
 - Irradiate ultrasonic waves of equivalent the output and waveform to the sensor
 - The sensor was misidentified the obstacle distance
 - Experiment equipment was made with the Arduino and ultrasonic transducer
 - This attack can provoke crash deliberately

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (3)

- Attacking Millimeter Wave Radar
 - This sensor measures distance to the obstacle of front
 - For Front collision avoidance and traffic-aware cruise control
 - Researchers experimented two types of attack
 - Jamming (76 - 77 GHz)
 - Obstacle couldn't detect
 - Spoofing
 - The Sensor was mistaking the distance between the obstacle and car
- **Comments of FFRI researcher**
 - The result has big impact, because it verified at the actual vehicle
 - Equipment for attacking the ultrasonic sensors is not expensive
 - We feel the possibility of actually attack

Into The Core – In-Depth Exploration of Windows 10 IoT Core (1)

- Research of Windows 10 IoT Core
- The security features
 - Windows Defender is unsupported
 - Microsoft Passport is unsupported
 - Two-factor authentication by Windows Hello (biometric) or PIN
 - Secure boot
 - If the boot target hadn't attestation, the system wouldn't boot
 - It's protected system from rootkit and bootkit
 - BitLocker
 - Encryption of user and system files
 - Windows Update is forced, but the Pro edition can postponement

Into The Core – In-Depth Exploration of Windows 10 IoT Core (2)

- Network services and drivers
 - It has many wireless driver (Wi-Fi, Bluetooth, ZigBee, Z-Wave)
 - If the driver was attacked, system privilege will be hijacked
 - UDP multicast
 - Windows IoT devices are informing oneself by using the UDP multicast
 - Anyone can check the device name, IP address and others in the packet
- Debugging with PC
 - IoT device (Raspberry Pi 3), USB-UART adapter(Shikra)
 - Activates serial debug on the device by using SSH or PowerShell
 - Debugging kernel using WinDbg at the COM port
 - Other approaches, debugging user mode process, analyzing crash dump

Into The Core – In-Depth Exploration of Windows 10 IoT Core (3)

- How to mitigate security risk of the Windows 10 IoT device
 - Network segmentation
 - You should separate PC and server from IoT devices
 - Measures against the infection from the internal network
 - Using firewall to protect network services
 - Using hardware which support the TPM
 - E.g.) Minnowboard + Dragonboard, Raspberry Pi + Discrete TPM
 - Using BitLocker and Secure boot
- Conclusion
 - Device maker should be careful about security setting
- **Comments of FFRI researcher**
 - We also pointed out that the security of Win10 IoT Core in the past
 - This research has novelty as proposing various hardware and research technique

GATTacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool (1)

- Gattacker is a proxy tool for BLE
- This tool can attack the device of Unencrypted communication
 - It is possible to attack the device of unencrypted communication by MITM
- For example
 - Sniffing and DoS for BLE smartLock
 - Attacker can unlock smartlock house or car at any time by sniffed data
 - Attacker, also it is possible to interfere with the locking by inhibiting the valid operation
 - Attacker can intrude payment process on BLE
- MITM flow
 - GATTacker will monopolize advertising packet of BLE device
 - GATTacker also sends advertising packet
 - GATTacker receives an application request
 - GATTacker bridges the device without being noticed
 - As a result of the above, allows sniffing and modification of communication

GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool (2)

- Countermeasure to attacks on exposed services(E.g. payment)
 - Provider is setting the deadline for expose the services
- Countermeasure to attacks on pairing
 - Encryption of BLE
 - Random MAC Address
 - Whitelist of MAC addresses
- **Comments of FFRI researcher**
 - You should combine whitelist filtering and other countermeasure because MAC address can camouflaged

GreatFET: Making GoodFET Great Again (1)

- GeatFET is improved version of the GoodFET
- GoodFET is an open-source JTAG adapter
 - More than twenty variants of the GoodFET hardware platform were developed
 - <http://goodfet.sourceforge.net/>
- Issue of GoodFET
 - Software is complex and difficult to maintain
 - Higher speed peripherals not available
 - Interfaces such as SPI are implemented by bit-banging

GreatFET: Making GoodFET Great Again (2)

- GreatFET Advantages
 - This tool is using LPC4330 of higher performance microcontroller with USB interface
 - LPC4330 can use the USB boot loader at just push one button
 - It supports the tractable expansion interface at called a "neighbor"
- GreatFET demerits
 - GreatFET takes longer to hand-assemble than GoodFET because parts are increased
- **Comments of FFRI researcher**
 - This tool is good is that the high-performance peripheral device can be used
 - The cost take more than GoodFET
 - It is recommended if you require higher performance
 - Hand-assemble takes the technique of electronic work

Conclusions

- Cyberattack for Vehicle and IoT got to more realistic
 - The vehicle was hijacked from remote during high-speed driving
 - Tool was released for BLE MITM Attack more easily
 - BLE is one of the most important protocol for IoT
- Research of defense technology is also making progress
 - Each country is doing research for defense based on the previous research
 - Each industry are conducted the bug bounty program for getting the advantage against the attacker side
- The Black Hat USA was excellent again this year
 - There are many other interesting research are published

References

- Black Hat USA 2016
 - <https://www.blackhat.com/us-16/>
- DEF CON
 - <https://www.defcon.org/html/defcon-24/dc-24-schedule.html>
- CANSPY: A Platform For Auditing CAN Devices
 - <https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platform-For-Auditing-CAN-Devices-wp.pdf>
- Advanced CAN Injection Techniques For Vehicle Networks
 - <https://www.blackhat.com/us-16/briefings.html#advanced-can-injection-techniques-for-vehicle-networks>
- Into The Core – In-Depth Exploration of Windows 10 IoT Core
 - <https://www.blackhat.com/docs/us-16/materials/us-16-Sabanal-Into-The-Core-In-Depth-Exploration-Of-Windows-10-IoT-Core-wp.pdf>
- GATTacking Bluetooth Smart Devices Introducing a New BLE Proxy Tool
 - <https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf>
- GreatFET: Making GoodFET Great Again
 - <https://www.blackhat.com/docs/us-16/materials/us-16-Ossmann-GreatFET-Making-GoodFET-Great-Again-wp.pdf>
- Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle
 - <https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles-WP.pdf>