Monthly Research 2016.5

Current state of IoT device security

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

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

Agenda

- Backgrounds
- Case Study related to IoT
  - Security incidents
  - Security research
- Threats on IoT devices
  - Threats
  - Causes of the threats
  - Countermeasures
- Considerations
- References

Backgrounds

- IoT(Internet of Things) is a concept that all devices are connected to the Internet
- There are various IoT devices, these are used in many places
  - office, factory, farm, hospital, home, etc.
  - There are also IoT devices which are controllable by mobile app
- These are convenient, but it has been concerned about threats of cyber security
- In this research, we show some security incidents of IoT devices

Security incidents related to IoT(2015 - 2016)

- Alert of attacks on IoT devices – National Police Agency(15/Dec/2015)
  - Most targeted service/port is telnet in Linux
  - Exploited IoT devices have become bots
- Anyone is able to look at pictures of 6,000 security cameras on the internet – INTERNET COM(22/Jan/2016)
  - These cameras are using default password or no authentication mode
- Password reuse problem of remote gas management system – Tokyo Gas(25/Mar/2016)
  - There is a possible in illegal access by previous residents
  - If attacker abuses this vulnerability they are able to shut off gas valve

Security research related to IoT(2014 - 2016)

- LIGHTS OFF! THE DARKNESS OF THE SMART METERS
  - This research was published in the Black Hat EU 2014
  - It was possible to shut off power, because many meters used same encryption key

- IoTPOT: Analysing the Rise of IoT Compromises
  - This research was published in the USENIX WOOT 2015
  - Research of IoT device emulation honeypot and collected malware

- HACKING A PROFESSIONAL DRONE
  - This research was published in the RSA conference 2016 and the Black Hat Asia 2016
  - Vulnerability was found by reverse engineering of mobile app for control drone
  - MITM attack was demonstrated

Threats on IoT devices

- Malware infection
  - BOT
    - There is a risk of abuse in DDoS attacks
  - Ransomware
    - It is not found yet, but there is a potential of appearance
- Physical invasion
  - If smart lock is exploited, thief can intrude into house
- Leak of information
  - invasion of privacy

Causes of the threats

- Malware infection
  - Insecure settings(default password, non authentication)
  - Unencrypted communication(HTTP, FTP, Telnet, etc.)
  - Vulnerability of software(OS, middleware, application)

- Physical invasion
  - Non hardware protection, Exposure of debugging interface
  - Unencrypted firmware
  - Usage of same encryption key

- Leak of private information
  - Operation mistake
  - Lack of understanding about IoT device
  - Reuse of password

Countermeasures

- Common measures
  - Update of software to fix vulnerability
- Encryption of communication
  - Using TLS
  - Using security chip(TPM)
- Hardware security
  - Protection of enclosure
  - Disabling debugging interface
- Software obfuscation
  - Obfuscating firmware, library and applications(PC, mobile)

Considerations

- IoT devices have been targeted on cyber attacks

- Users should recognize security risk on IoT devices
  - There are remote device hijacking, leak of information, invasion of privacy
  - Manage data on IoT devices
  - Back up important data

- Developers should implement security based on guideline
  - Hardware security is also required in addition to the conventional measures

References

- A Simple Explanation Of 'The Internet Of Things'
  - http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#52f161566828
- How the Internet of Things Got Hacked
  - https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/
- NPA
  - https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf
- Tokyo Gas
  - http://www.tokyo-gas.co.jp/important/20160325-06.pdf
- Target such as Panasonic products — Japan's security camera, the subject peep at about 6,000 in internet – NITERNET COM(2016/01/22)
  - http://internetcom.jp/200103/insecam-again
- HACKING A PROFESSIONAL DRONE - Nils Rodday
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf
  - LIGHTS OFF! THE DARKNESS OF THE SMART METERS - Alberto Garcia Illera & Javier Vazquez Vidal
  - https://www.blackhat.com/eu-14/briefings.html#lights-off-the-darkness-of-the-smart-meters
- Improving IoTPOT for Observing Various Attacks Targeting Embedded Devices
  - Shogo Suzuki, Yin Minn PA PA, Yuta Ezawa, Ying Tie, Sou Nakayama, Katsunari Yoshioka, Tsutomu Matsumoto, ICSS2015
- Security design of IoT development guide - IPA
  - https://www.ipa.go.jp/files/000052459.pdf