Audit of an IoT system using Penetration testing

Jonathan Tournier

jonathan.tournier@algosecure.fr

Team: Dynamid

CITILab-INRIA INSA Lyon AlgoSecure

Supervisors:

Frédéric Le Mouël (CITI)
François Lesueur (CITI)
Hicham Ben-Hassine (AlgoSecure)
Laurent Guyon (AlgoSecure)

Context

IoT development

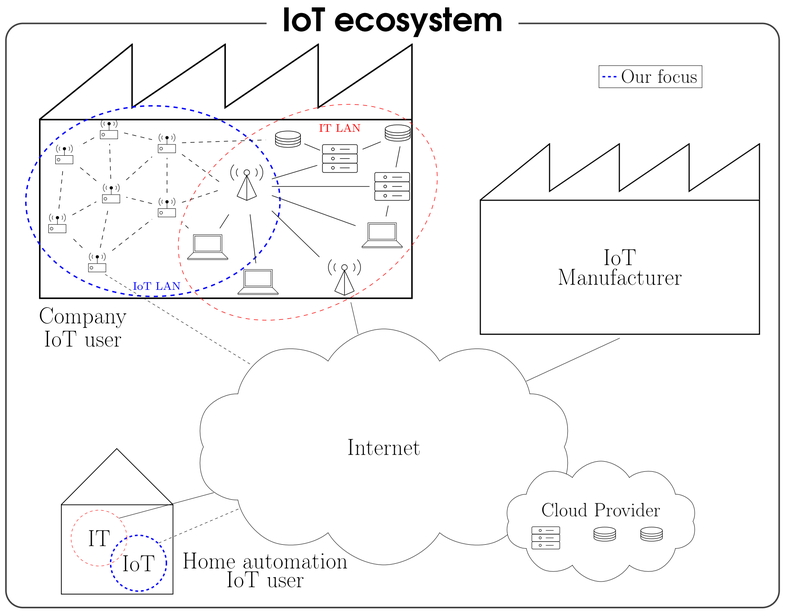
Fast growth

- Billions of devices expected
- Everything gets connected
- Market pressure

What about security ?

- Mirai botnet:
  - 148000 hacked devices
  - Used to block access to Twitter, Facebook
- Recall of 500 000 pacemakers
  - Produced by Abbott
  - Updated only by medical staff

IoT ecosystem



IoT security by penetration testing

Pentest ?

- A solution to evaluate security of complex systems (1)
- An authorized simulated attack

Pentest steps

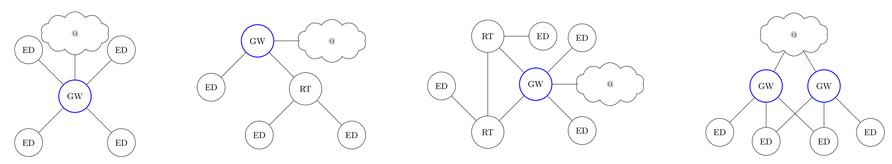
1. Information gathering
2. Threat Modelling
3. Vulnerabilities analysis
4. Exploitation
5. Post-exploitation
6. Reporting

Steps with IoT specificities

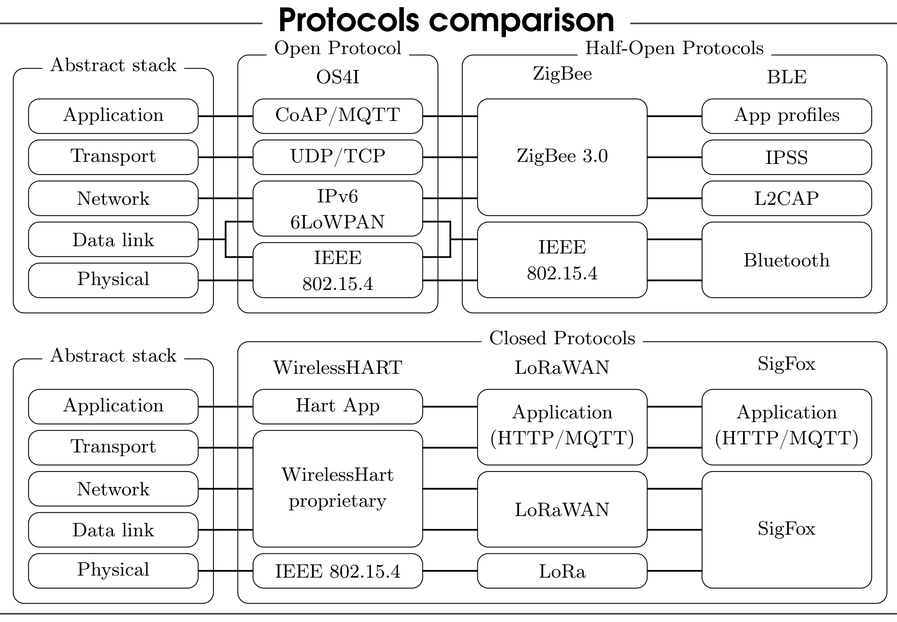
Information gathering

IoT protocols analysis

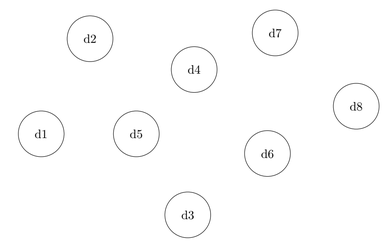
Topologies



Protocols comparison

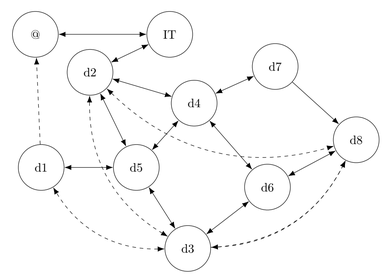


IoT Network modelling



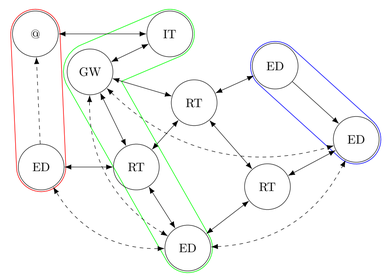
Step 1: network discovery

- Network coverage
- Devices discovery

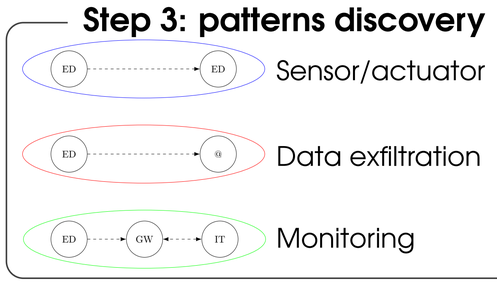


Step 2: devices connection

- Physical graph —
- Logical graph ----
- LiveNet (2), PMSW (6), IoTScanner (5), IoT Sentinel (3)



Step 3: patterns discovery



Vulnerabilities analysis

Attacks (4) against IoT networks based on the CIA principle

Protocols & messages

Passive attacks C

Traffic analysis based on the quality of encryption

Active attacks

- Cryptographic attacks CI
- MiTM CI

Topology

Alteration

- Sinkhole
- Flooding
- Sybil
- Spoofing

Attacks

- Blackhole A
- Selective forwarding A
- Eavesdropping C
- Injection I

References

(1) Matt Bishop. About penetration testing. *IEEE Security & Privacy*, 5(6):84–87, 2007.

(2) Bor-rong Chen, Geoffrey Peterson, Geoffrey Mainland, and Matt Welsh. Livenet: Using passive monitoring to reconstruct sensor network dynamics. In *DCOSS, Proceedings*, pages 79–98, 2008.

(3) Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. Iot SENTINEL: automated device-type identification for security enforcement in iot. In *ICDCS*, pages 2177–2184, 2017.

(4) G. Padmavathi and D. Shanmugapriya. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *CoRR*, abs/0909.0576, 2009.

(5) Sandra Siby, Rajib Ranjan Maiti, and Nils Ole Tippenhauer. Iotscanner: Detecting privacy threats in iot neighborhoods. In *IoTPTS@AsiaCCS*, pages 23–30, 2017.

(6) Xianghua Xu, Jian Wan, Wei Zhang, Chao Tong, and Changhua Wu. PMSW: a passive monitoring system in wireless sensor networks. *Int. Journal of Network Management*, 21(4):300–325, 2011.

RESSI - May 23rd 2018