Audit of an IoT system using Penetration testing

Context

**IoT development**
- Fast growth
- Billions of devices expected
- Everything gets connected
- Market pressure

What about security?
- Mirai botnet
  - 148 000 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

**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

Step 3: patterns discovery
- Sensor/actuator
- Data exfiltration
- Monitoring

**Vulnerabilities analysis**

Attacks (4) against IoT networks based on the **CA** principle

**Protocols & messages**

**Passive attacks**
- Traffic analysis based on the quality of encryption

**Active attacks**
- Cryptographic attacks
- MITM

**Topology**

**Alteration**
- Sinkhole
- Flooding
- Sybil
- Spoofing

**Attacks**
- Blackhole
- Selective forwarding
- Eavesdropping
- Injection

References


RESSI - May 23rd 2018