IoT Security: A comparative analysis

Sachin Gaur

oneM2M High Level Conference, CDOT Campus

27/08/19

Flow of the presentation

- Literature survey (research papers)
- IRTF 8576 (2019)
- ENISA report (2017)
- NIST (2019)
- Summary

Quality (read security) in IoT is difficult…

“Why information security is hard – an economic perspective” –Ross Andersson

“Market for security products is a market where both buyer and seller have incomplete information” - Griggs

“Trusted Computing as Treacherous Computing” – Richard Stallman

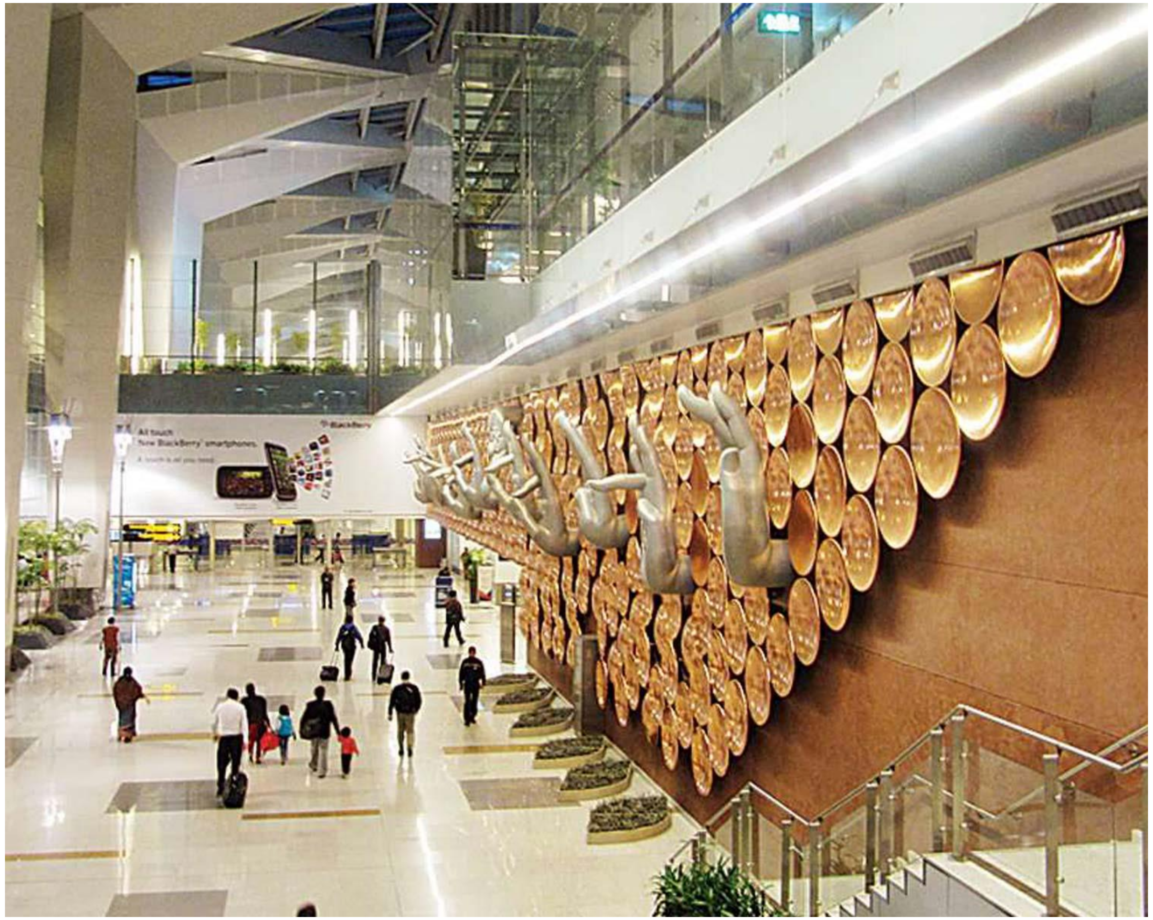
“Design for Security Testing / Design for User Trust” -- Aurelien Francillon, Eurecom, France

Now reflect on this statement?

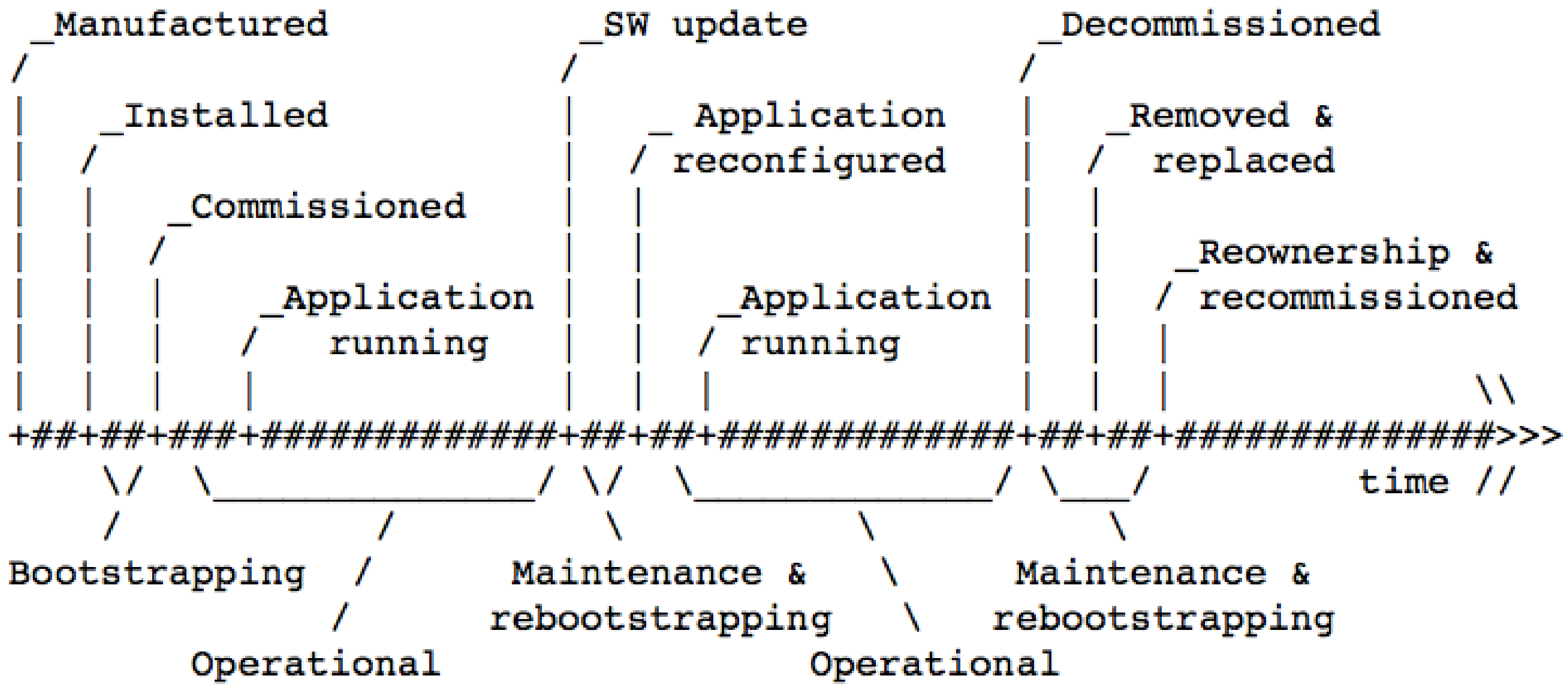
“People will eventually be unable to know how many devices they are carrying, which ones are currently connected and what data they contain. Is the data personal or not? Who is able to access it? Who is able to perform software update without the user’s knowledge? “

- Aurelien Francillon, Eurecom, France

Trust: handling complexity



IRTF RFC 8576 : IoT Security State of the Art and Challenges



```
 _Manufactured           _SW update          _Decommissioned
/                       /                   /
|   _Installed          |   _ Application   |   _Removed &
|  /                    |  / reconfigured   |  /  replaced
|  |   _Commissioned    |  |                |  |
|  |  /                 |  |                |  |   _Reownership &
|  |  |    _Application |  |   _Application |  |  / recommissioned
|  |  |   /   running   |  |  / running     |  |  |
|  |  |   |             |  |  |             |  |  |             \\
+##+##+###+#############+##+##+#############+##+##+##############>>>
    \/  \______________/ \/  \_____________/ \___/         time //
    /           /         \          \          \
Bootstrapping  /      Maintenance &   \     Maintenance &
              /     rebootstrapping    \   rebootstrapping
        Operational                Operational
```

Figure 1: The Lifecycle of a Thing in the Internet of Things

Figure taken from the RFC document

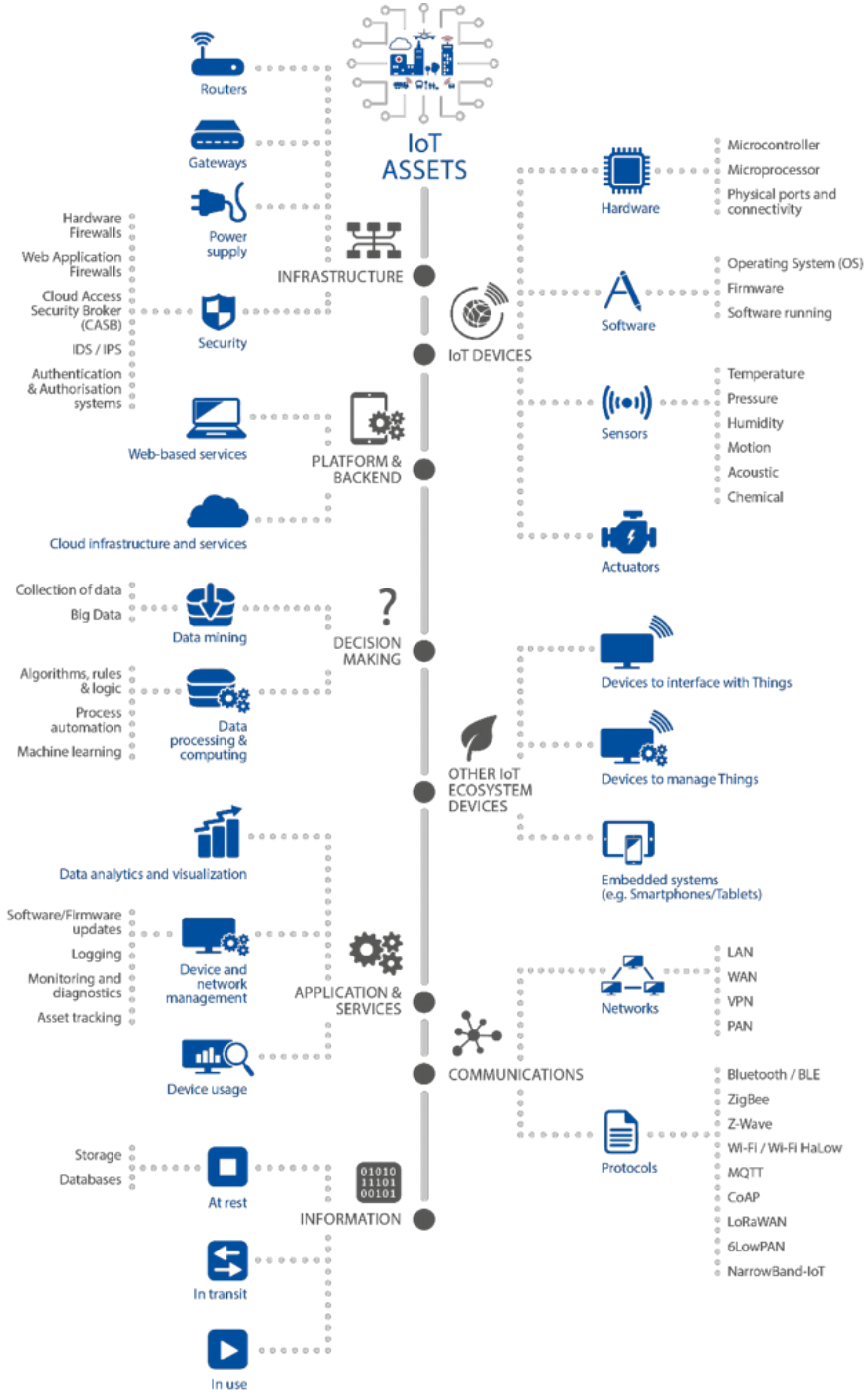
IoT Threats that it mentions

- Vulnerable software / code
- Privacy threat
- Cloning of things
- Malicious substitution of things
- Eavesdropping attack
- Man in the middle attack
- Firmware attack
- Extraction of private information
- Routing attack
- Elevation of privilege
- Denial of Service

Trustworthy IoT Operations

- How to avoid vulnerabilities in IoT devices that can lead to large scale attacks?
- How to detect sophisticated attacks against IoT devices?
- How to prevent developers from exploiting known vulnerabilities at a large scale?

ENISA: Baseline Security Recommendations for IoT



IoT ASSETS

INFRASTRUCTURE
Routers
Gateways
Power supply
Security
Hardware Firewalls
Web Application Firewalls
Cloud Access Security Broker (CASB)
IDS / IPS
Authentication & Authorisation systems

IoT DEVICES
Hardware
Microcontroller
Microprocessor
Physical ports and connectivity
Software
Operating System (OS)
Firmware
Software running
Sensors
Temperature
Pressure
Humidity
Motion
Acoustic
Chemical
Actuators

PLATFORM & BACKEND
Web-based services
Cloud infrastructure and services

DECISION MAKING
Data mining
Collection of data
Big Data
Data processing & computing
Algorithms, rules & logic
Process automation
Machine learning

OTHER IoT ECOSYSTEM DEVICES
Devices to interface with Things
Devices to manage Things
Embedded systems (e.g. Smartphones/Tablets)

APPLICATION & SERVICES
Data analytics and visualization
Device and network management
Software/Firmware updates
Logging
Monitoring and diagnostics
Asset tracking
Device usage

COMMUNICATIONS
Networks
LAN
WAN
VPN
PAN
Protocols
Bluetooth / BLE
ZigBee
Z-Wave
Wi-Fi / Wi-Fi HaLow
MQTT
CoAP
LoRaWAN
6LowPAN
NarrowBand-IoT

INFORMATION
At rest
Storage
Databases
In transit
In use

Figure taken from the ENISA document

ENISA: Baseline Security Recommendations for IoT

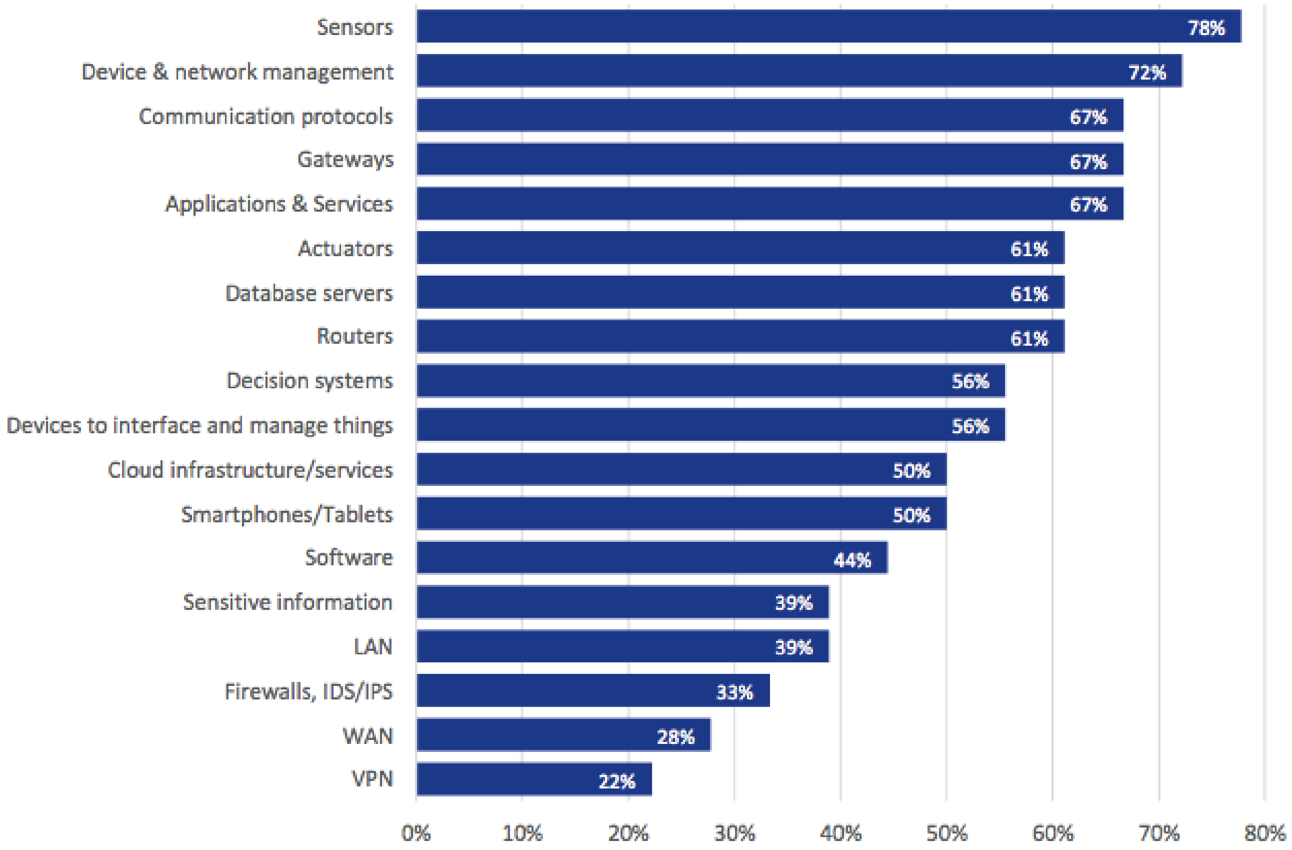


Figure 6: Asset criticality

Figure taken from the ENISA document

ENISA: Baseline Security Recommendations for IoT

Best Practices	Best Practices
Security by design	Access Control – Physical and Environmental Security
Privacy by design	Cryptography
Asset Management	Secure and trusted communications
Risks and Threats Identification and Assessment	Secure interfaces and network services
Hardware Security	Secure input and output handling
Trust and Integrity Management	Logging
Strong default security and privacy	Monitoring and Auditing
Data protection and compliance	End of life support
System safety and reliability	Proven Solutions
Secure Software/firmware update	Management of security vulnerabilities
Authentication	Human resources security testing and Awareness
Authorization	Third Party relationships

NIST IR 8259

- **Many IoT devices interact with the physical world in ways conventional IT devices usually do not.** The potential impact of some IoT devices making changes to physical systems and thus affecting the physical world needs to be explicitly recognized and addressed from cybersecurity and privacy perspectives. Also, operational requirements for performance, reliability, resilience, and safety may be at odds with common cybersecurity practices for conventional IT devices.
- **Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.** This can necessitate doing tasks manually or significantly differently than for conventional IT for some IoT devices, expanding staff knowledge and tools to include a much wider variety of IoT device software, and addressing risks with manufacturers and other third parties having remote access or control over IoT devices.
- **The availability, efficiency, and effectiveness of cybersecurity features are often different for IoT devices than conventional IT devices.** This means organizations may have to select, implement, and manage additional controls, as well as determine how to respond to risk when sufficient controls for mitigating risk are not available.

Features that it talks about

- Device identification
- Device configuration
- Data Protection
- Logical access to Interfaces
- Software and Firmware update
- Cybersecurity Event Logging

Summary

- Since the length and breadth of security issues is very large, it will take a considerable effort to map various frameworks available and do the gap analysis. As they cover different aspects
- How do we bring trust?
  - Easy to understand security classification / labels
  - Certification
  - Capabilities to monitor and proactive mitigation of threats
  - Domain specific standard operating procedures

Questions

- Sachin Gaur
    - Local coordinator: India EU ICT Standards Collaboration Project
    - www.IndiaEU-ICTStandards.in
    - +91 99999 79349
    - sachin@mixorg.com