IoT Protocols

2

INTRODUCTION

Internet of Things (IoT):

a wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement.

- by 2020 18 billion devices
- 40 Zettabytes data exchanged

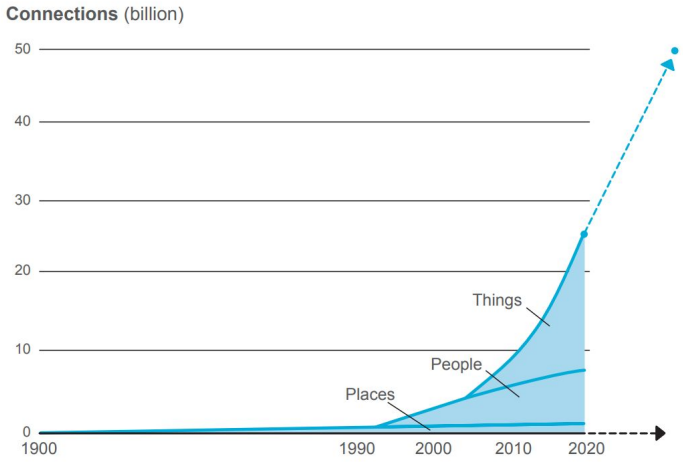

Figure 5: Connecting places, people, and things

3

INTRODUCTION

Mobile Ecosystem Forum Global Customer Survey:

62% Privacy

54% Security

27% Physical safety

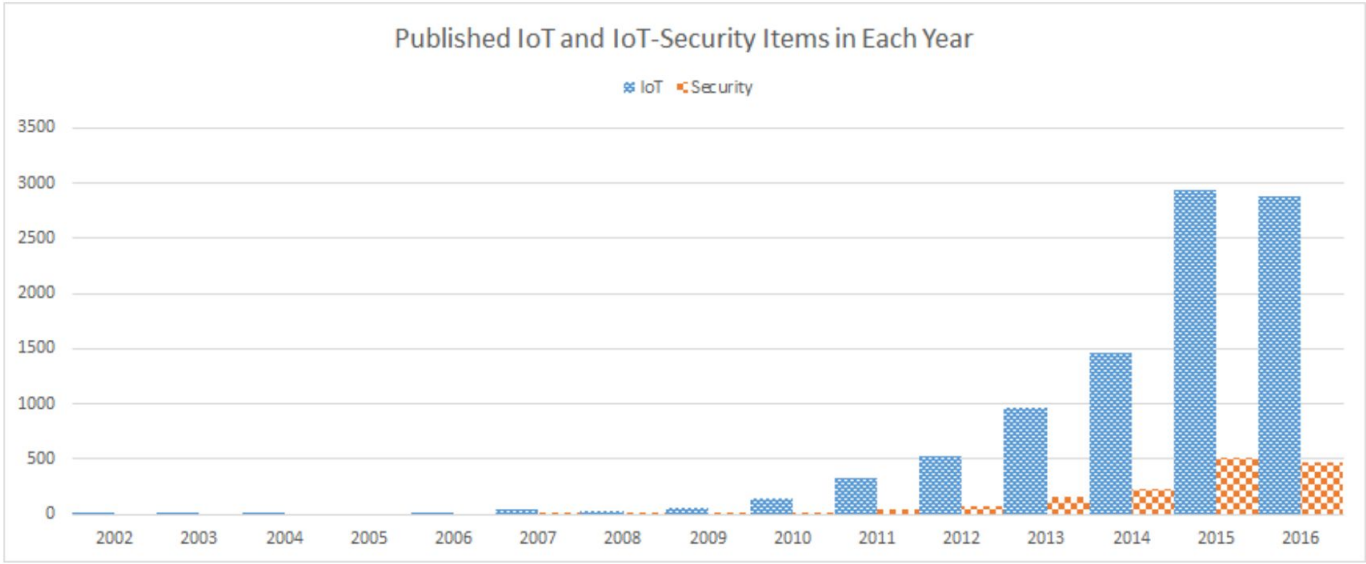

Fig. 3. Number of publications for Internet-of-Things and Internet-of-Things Security related articles. As of December 2016 [14].

4

CHALLENGES AND LIMITATIONS

Challenges	Limitations
Mobility	Limited processors
Reliability	Small amounts of memory
Scalability	Low throughput
Management	Limited power
Availability, Integrity, Confidentiality	Limited cryptography
Interoperability	Intermediaries

5

HARDWARE

Hardware - root of trust:

- automatically protect functioning and data
- encryption and integrity
- cryptographic verification

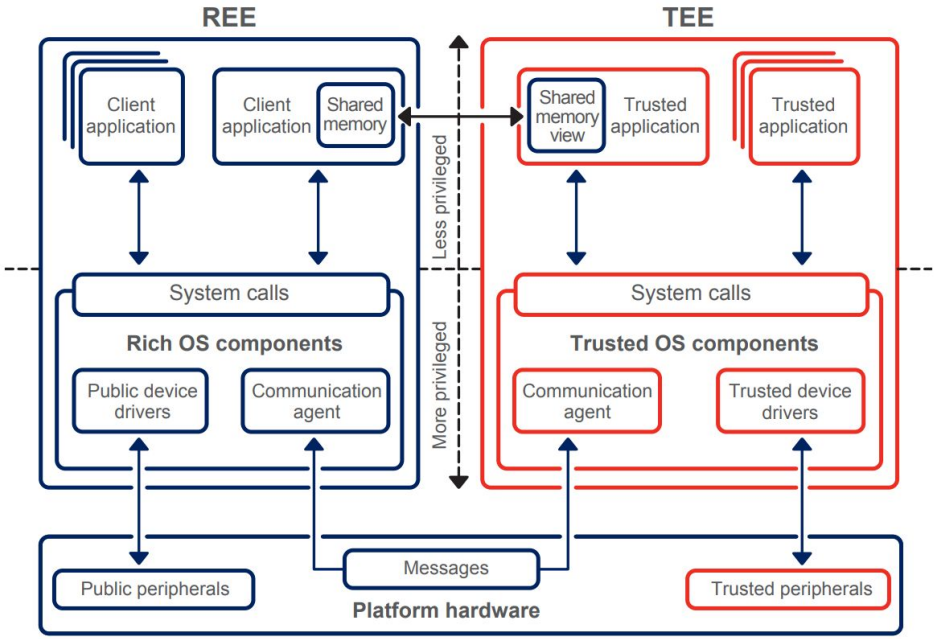

Figure 4: Hardware isolation using TEE

6

HARDWARE

IoT platforms should supervise devices' lifecycles from manufacture to decommission:

- During manufacturing, each device should have credentials (keys and identifiers) stored in a secure hardware module, application processor, or baseband processor.
- In the installation phase, the device uses the pre-configured credentials to automatically bootstrap itself to services. The IoT platform should perform initial configuration, including update of firmware, configuration of applications, and provisioning of credentials for application layer services.
- During operation, the platform should monitor the device, provide software updates, and enforce security policies such as authorization and access control. To save bandwidth and storage, firmware and software updates should be delta encoded.
- Before the device is taken out of service, the IoT platform should remotely erase all the sensitive data on it. Remote decommissioning is almost as important as remote provisioning, and should be a requirement for IoT devices.

7

ARCHITECTURE

The foundation for ubiquitous computing, whose goal is to connect everyday life objects to the network using technological platforms, is made up of three components:

- Hardware
- Middleware - software that provides services to applications beyond those available from operating system
- Presentation

It translates to three layer architecture:

- The application layer
- The network layer
- The perception layer

8

LANDSCAPE

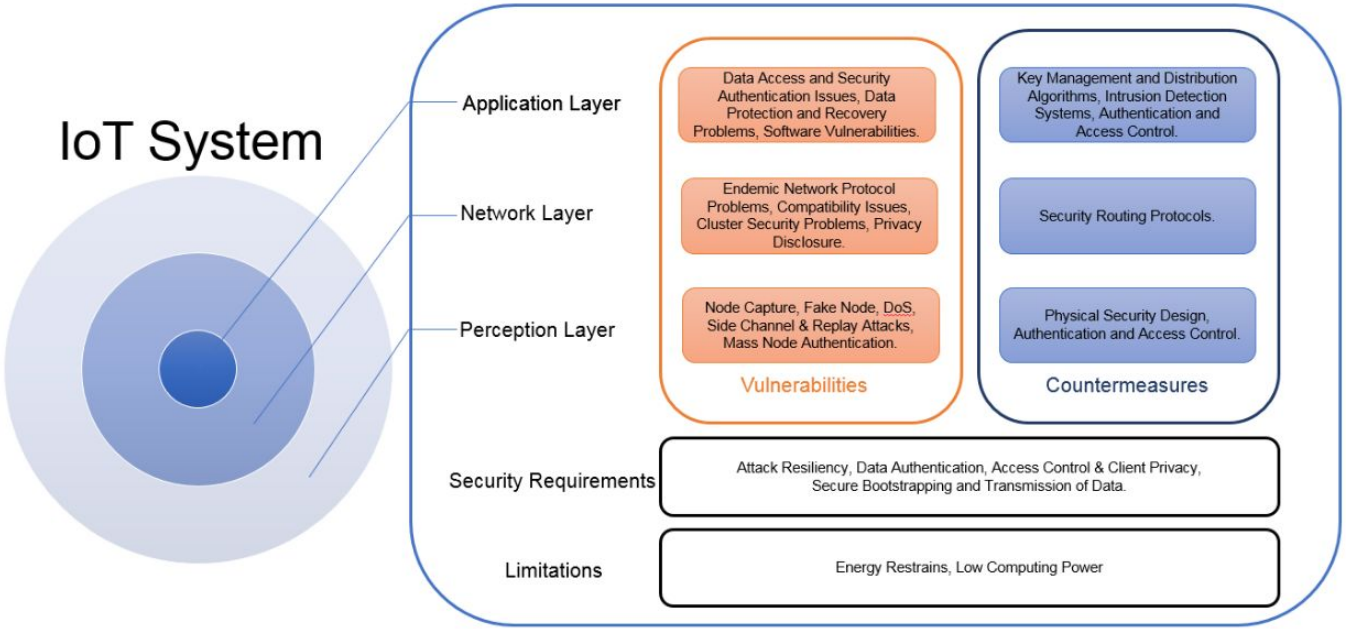

Fig. 2. Internet of Things Security Landscape.

9

PERCEPTION LAYER TECHNOLOGIES AND PROTOCOLS

Wireless Sensor Networks (WSN) is a group of independent nodes communicating wirelessly offer limited frequency and bandwidth

Limitations of WSN:

- power management,
- network discovery,
- control and routing,
- collaborative signal and information processing,
- tasking and queering,
- security

Threats:

- DDoS,
- Traffic analysis,
- Node replication (Sybil attack),
- Black hole routing,
- Physical damage

10

PERCEPTION LAYER TECHNOLOGIES AND PROTOCOLS

Bluetooth is a wireless technology standard for exchanging data over short distances

- Bluetooth operates at frequencies between 2402 and 2480 MHz
- Range: 10 - 240 meters
- The Bluetooth protocol it is designed to provide security in 3 ways: use of pseudo-random frequency hoping, Restricted authentication and Encryption
- Vulnerabilities: optional or weak encryption, non-secure default settings, weak PIN use, insecure unit keys, flawed integrity protections and predictable number generation
- Pairing policy - version < 2.1 encryption can be turned off
- Sometimes encryption has to be turned off

11

PERCEPTION LAYER TECHNOLOGIES AND PROTOCOLS

Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves.

Secure RFID:

- access control
- data encryption,
- IPSec protocol utilization,
- cryptography technology scheme

RFID vulnerabilities:

- attacks on authenticity - unauthorized tag disabling,
- attacks on integrity - unauthorized tag cloning,
- attacks on confidentiality - unauthorized tag tracking
- attacks on availability - replay attacks

12

MIDDLEWARE

Seven categories for discussion based on design principles:
1) Event-based
2) Service-oriented
3) Virtual Machine (VM) based
4) Agent-based middleware is composed of modular programs that “facilitate injections and distribution through the network using mobile agents”. Agent-based middleware deserve as well a security-focused analysis for features and vulnerabilities.
5) Tuple-spaces middleware each component
contains a data repository or tuple space that can be accessed simultaneous
6) Database-oriented - the sensor network acts as a “virtual relational database system” that can be queried by SQL-alike language.
7) Application - specific middleware specializes on managing resources for specific requirements demanded by the application or by the domain it works on

13

APPLICATION LAYER

MQTT (Message Queuing Telemetry Transport) is a lightweight publish/subscribe messaging protocol designed for M2M (machine to machine) telemetry in low bandwidth environments. Broker - filter messages based on topic and then distribute them to subscribers

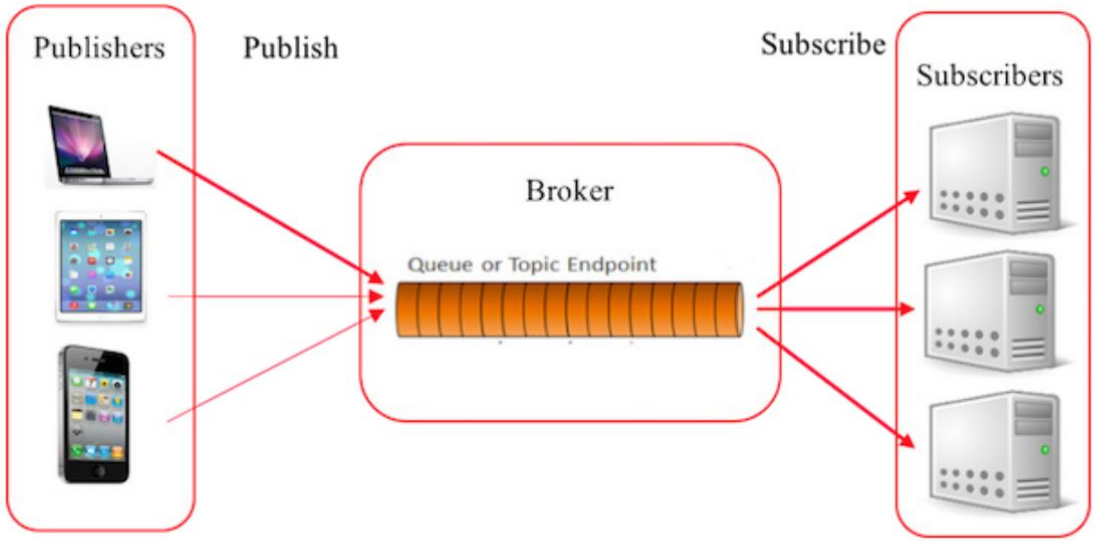

Figure 5: MQTT Architecture

14

APPLICATION LAYER

Blockchain can be applied in a distributed and trustless environment without the need of third party authentication or management

1) blockchain is a back-ordered hash list that is publicly shared in a peer-to-peer network
2) member is addressable by the hash value of its public key.
3) proof of the authenticity by encrypting the hash value of the record using its private key
4) The newly formed block is then appended to the existing blockchain and point to the previous block
5) Supported by the cryptographic properties of hash and asymmetric encryptions, a blockchain can therefore ensure each block is immutable and transaction is verifiable

15

CONCLUSION BEST PRACTISES

- Right to privacy
  Rules and legislation
- Need-to-know
  Restriction of sensitive data
- Logs
  Reliable and verifiable
- Standardization
  Common effort of:
  - Governments
  - Manufacturers
  - Scienitists
  - Institutions

- Securing devices:
  - Make hardware tamper resistant
  - Provide patches/updates
  - Perform dynamic testing
  - Specify procedures to protect data on device disposal
- Securing networks:
  - Strong authentication
  - Strong encryption and secure protocols
  - Minimize device bandwidth
  - Divide network into segments
- Secure overall IoT system:
  - Protect sensitive information
  - Encourage ethical hacking
  - Discourage blanket safe harbor
  - Institute an IoT security and privacy certification board

16

SOURCES

- https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
- http://www.meet-iot.eu/deliverables-IOTA/D1_3.pdf
- https://www.ericsson.com/assets/local/publications/white-papers/wp-iot-security-february-2017.pdf
- https://arxiv.org/pdf/1707.01879.pdf
- https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
- https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf