IoT Security

Nov 9, 2022

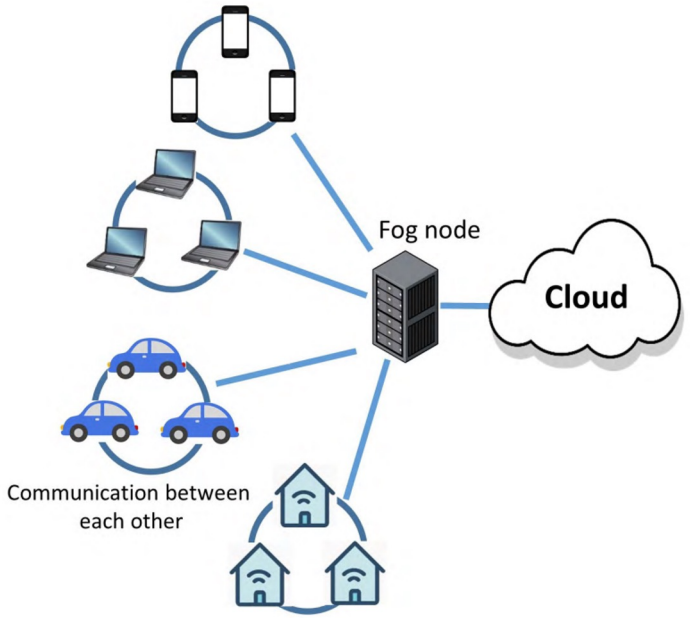
Aaron Bergen, Xinglei Liu

USC Viterbi
School of Engineering

University of Southern California

IoT Security

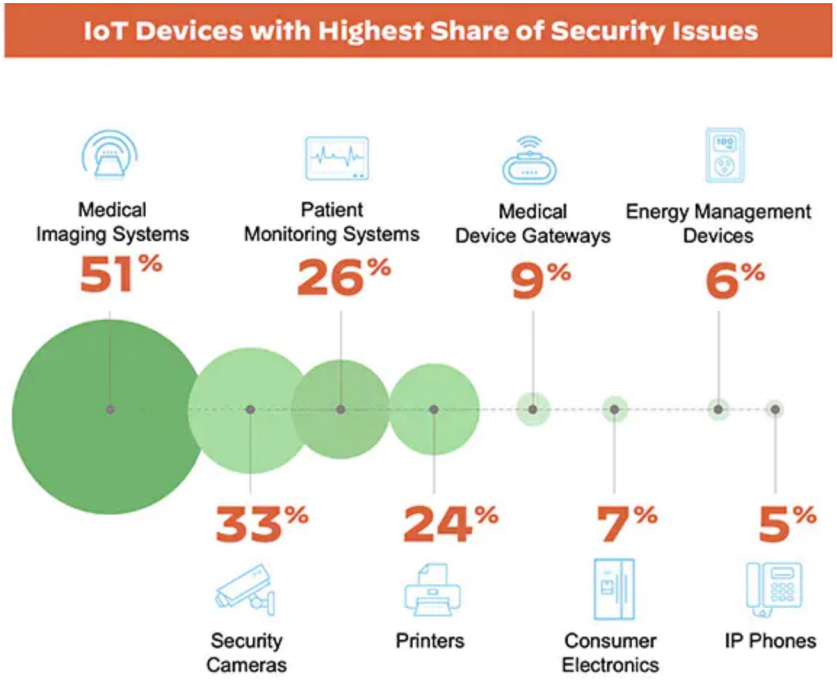
- Internet of Thing (IoT) devices are internet-connected or network-based physical objects
- IoT security is a collection of security measures to secure IoT devices



Present IoT Architecture

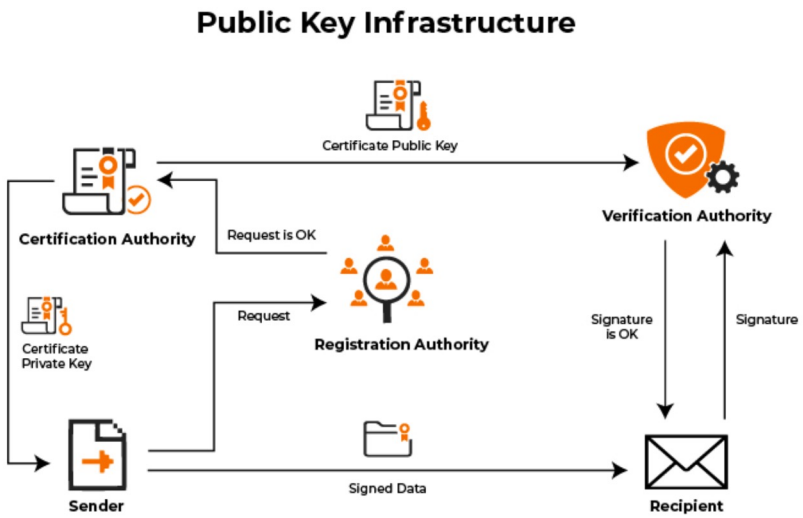
Challenges

- Inventory
- Threats
- Data volume
- Ownership
- Diversity
- Operations



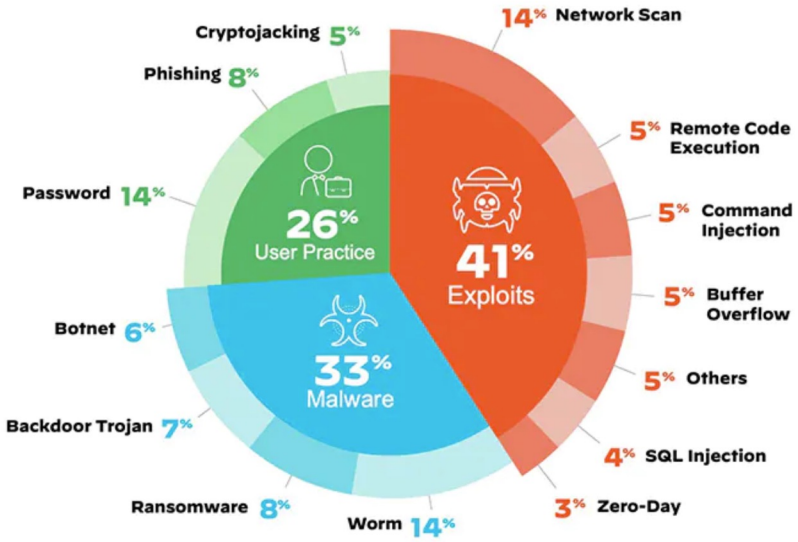
IoT Security Measures

- Enable security in design phase
- Public Key Infrastructure (PKI) and Digital Certificates
  - Protect the client-server connections between multiple networked devices
- Network Security
  - Port security, Firewall, IDS…
- API security
  - Protect data sent from IoT devices to backend



Potential Threats

- Sensing Layer
  - Node Capture Attack
  - Malicious Code Injection
- Network Layer
  - Phishing Site Attack
  - Access Attack
  - DDOS Attack
- Data Processing Layer
  - Flooding Attack
  - SQL Injection
- Application Layer
  - Data Theft Attack
  - Access Control Attack

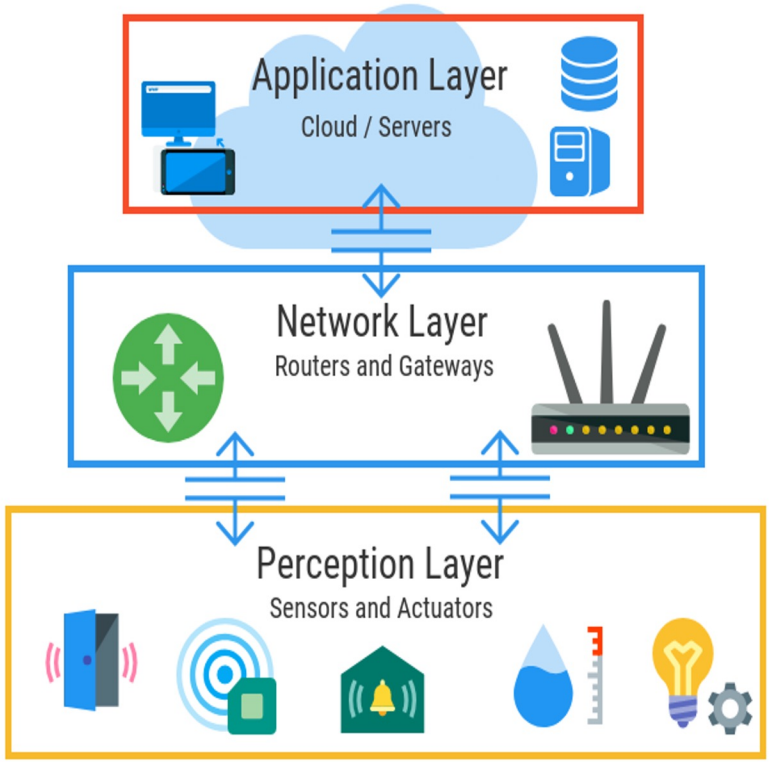


Current Weaknesses

Source: Juniper Research

IoT Characteristics	Potential Security Weakness & Targets
Closed / open platforms Variable policies High data volume handling	Code Lack of penetration testing Weak User / Third Party Authentication
Public / private / hybrid cloud deployment	Code Policy management
2G, 3G, LTE, 5G DSL, Fibre, LPWAN Wi-Fi, Bluetooth MQTT, IP, ZigBee, Mesh RF, Wi-Fi etc	Insecure communications
Variable communications protocols Time-sensitive data analysis	Policy management Denial-of-service No / insecure updates Poor hardware design
Limited power Low bandwidth Constrained capabilities	Design faults Software / firmware implementation faults Inability to update
Sensitive data: video, audio, location, personal information Technical data: environmental measurement, uptime reports	Users Policy management Data storage

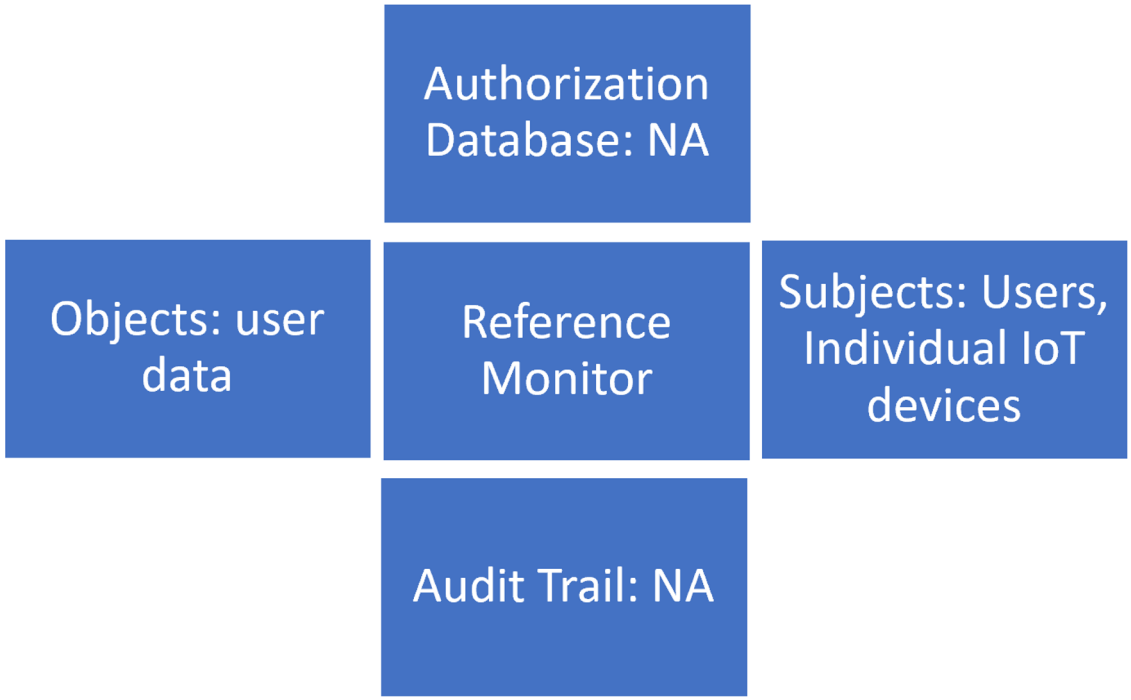
IoT Architecture



- **Sensing Layer:** The “Things” of the Internet of Things.
  - sensors, actuators, things that can represent the physical environment
- **Network Layer:** The “Edge”
  - Internet/Network gateways, Data Acquisition systems
  - Filtering data, aggregating data.
- **Data processing Layer**: “Edge analytics”
  - Data is analyzed and pre-processed before sending to the cloud or other data centers.
- **Application Layer**: end usage
  - Data is then used by end user applications like farming, agriculture, health care, defense, ect.

Note: There is no IoT architecture that is agreed on.

RM Comparison



Current Security Efforts:

- Password Protection
- Encryption
- Restrictive network communication policies
- Note, none of these efforts focus on creating an audit trail to track security violations or an authorization database to list the access attributes of subjects or objects

80% of IoT devices on the market do not have either a repository of subject object attributes or any record of security-related events.

RM 3 Principle Shortcomings

Tamperproof	✗
Non bypassable	✗
Verifiable	✗

Not tamper proof because while some IoT devices more concerned with security use encrypted communication or mandate strong passwords, the hardware or software production chain is often across multiple companies, all with differing, if any, regard to user security. Many opportunities to install malicious code and backdoors.

Not non-bypassable because not every access is mediated. If one IoT device is compromised, it can infect the entire network so that future accesses to the network are not mediated or authorized.

Not verifiable because there is little to no assurance that it can implement policy. Little to no IoT hardware devices are made with security in mind, and security is only added later at the data processing or application layer. Ad-hoc solution.

References

https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security
https://ieeexplore.ieee.org/abstract/document/8742551
https://www.cloudflare.com/learning/security/glossary/iot-security/
https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security
https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html
https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/
https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/