CIS 700/002 : Special Topics : A survey of secure middleware for the Internet of Things

Hyo Jin Jo
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

March 31, 2017

Overview

- Introduction to IoT devices
- Security challenges of IoT environment
- Security requirements for IoT environment
- Reviews the existing IoT middleware

IoT devices

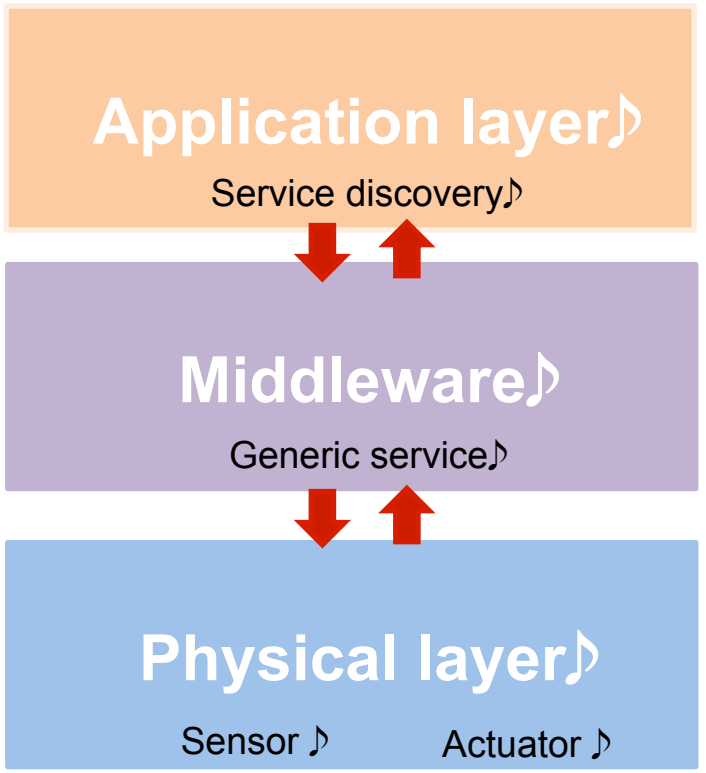
[Source : One trillion IoT devices expected by 2025: What development tools to use for development of internet connected IoT products?, Atollic.com]♪

[Smart bulb]

[Macchina : CAN-to-X]

What is middleware?

- These solutions are highly diverse
  - Design approaches
    - e.g., sub/pub, database
  - Implementation level
    - e.g., local or node level, global or network level
  - Implementation domains
    - e.g., WSNs, RFID, M2M, and SCADA♪



Security challenges of IoT

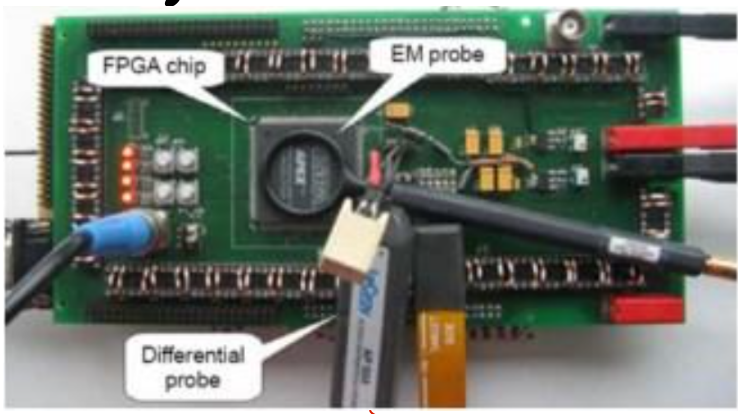
- Attack on IoT devices may have critical impact because the devices can affect the physical world
- Some IoT devices collect personal information which may lead to potential privacy concerns
- IoT devices have constrained memory and computation power compared to the traditional IT system♪

Matrix of security challenges for IoT

Security / Characteristic♪	A. Device & Hardware♪	B. Network♪	C. Cloud & Server-side♪
1. Confidentiality♪	A1. Hardware attacks♪	B1. Encryption with low capability devices♪	C1. Key disclosure, Data leakage♪
2. Integrity♪	A2. Lack of attestation♪	B2. Signatures with low capability device♪	C2. No common device identity♪
3. Availability♪	A3. Physical attacks♪	B3. Unreliable networks, DDoS, Radio jamming♪	C3. DDoS♪
4. Authentication♪	A4. Lack of UI, Default passwords, Hardware secret retrieval♪	B4. Default passwords, Leakage of secret♪	C4. No common device identity, Insecure flows♪
5. Access Control♪	A5. Physical access; Lack of local authentication♪	B5. Lightweight distributed protocol for Access control♪	C5. Inappropriate use of traditional ACLs, Weak access control♪
6. Privacy♪	A6. Zero permission attack♪	B6. Profiling network logs, Trace location♪	C6. Data/Meta-data sharing♪

Confidentiality : Device & Hardware

- Physical attacks on IoT devices are possible
- Even though some devices have a tamperproof function, attackers can often break them in many ways
  - Side-channel attacks



Large prime numbers (eg., 512 or 1024 bits)♪

RSA algorithm $C \uparrow S \equiv M \bmod n$, $(n=p*q)$♪

Input = Secret value (100011101…)

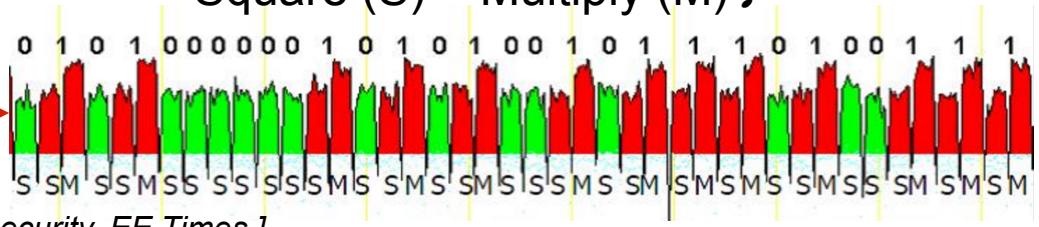
If Secret Exponent = 0

Square (S)

Else

Square (S) + Multiply (M) ♪

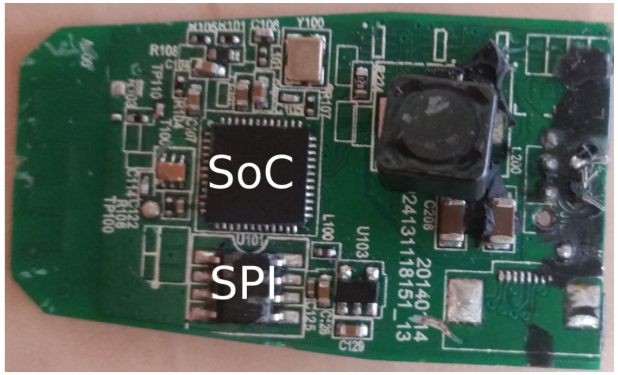
Power consumption♪



[Source : News & Analysis New Advances in FPGA Security, EE Times]

Confidentiality : Device & Hardware

Philips Hue **gateway**, lights**, and switch**♪



AES – Counter with CBC-MAC **is used for encryption/integrity of firmware update**

→ **All light bulbs use a universal key**

→ **Extract the key using a side-channel attack**♪

Worm spread by a compromised bulb♪

[Reference 1 : IoT Goes Nuclear: Creating a ZigBee Chain Reaction, eprint 2016]♪

Confidentiality : Network

- Many security protocols use public key algorithms to provide confidentiality of communication channels
  - RSA , ECDSA (Elliptic Curve Digital Signature Algorithm), …
- However, performing public key algorithms on IoT device is one of challenges

ArduinoLibs –
Benchmark (Arduino UNO, 16 MHz)♪

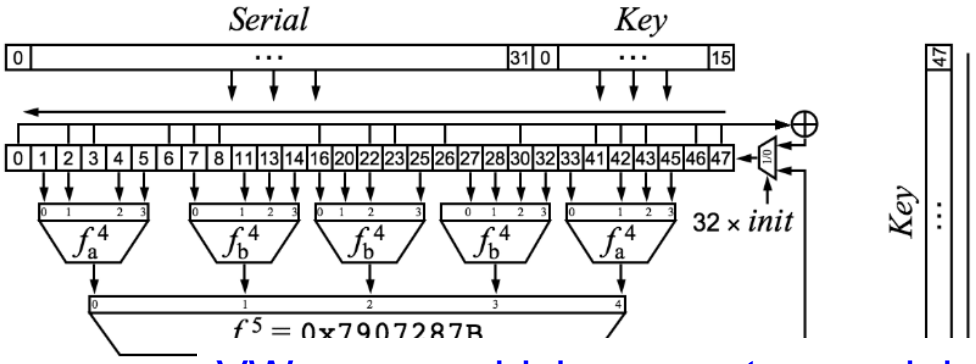
Ed25519::sign()	5148ms	Digital signature generation
Ed25519::verify()	8196ms	Digital signature verification

[Source : https://rweather.github.io/arduinolibs/crypto.html]♪

Confidentiality : Network

- Vulnerabilities of protocols
  - The emergence of new protocols for IoT devices is another security challenge

- Examples
  - BLE (Bluetooth Low Energy), Protocols for smart keys♪



VW group vehicles use stream cipher "Hitag2" which is not secure against cryptanalysis using network flows♪

[Reference 2 : Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems, Usenix Security'16]♪

Confidentiality : Cloud & Server

- The company Fitbit made data about users sexual activity available and easily searchable online

[Reference 3 : Fitbit users are unwittingly sharing details of their …, TNW News, 2011]♪

- ♪Many cloud hosting systems have been forced to hand over encryption keys to the security services♪

Integrity : Hardware & Device

- The challenges are in maintaining IoT device's codes and stored data
  - Smart TV, Telematics device, Smart bulb …
    - Hacking, surveilling, and deceiving victims on Smart TV, Blackhat, 2013
    - Vulnerabilities of Android OS-Based Telematics System, Wireless personal communication, 2016
    - IoT Goes Nuclear: Creating a ZigBee Chain Reaction, eprint 2016
    - …♪

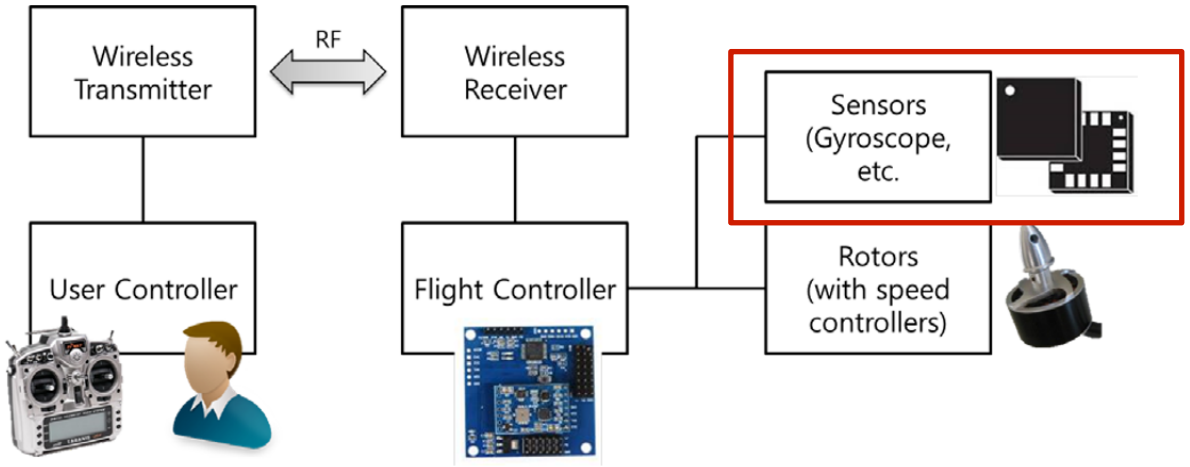
Integrity : Network / Cloud & Server

- Maintaining integrity of network data is related to cryptographic algorithms
  - MAC (Message Authentication Code)
  - Digital Signature (RSA, ECDSA, …)

- Integrity of cloud & server data
  - How to maintain data integrity
    - Using hash algorithms, Regular data back-up … ♪
  - Identity management
    - Without knowing who or what created data, cloud & server cannot trust that data

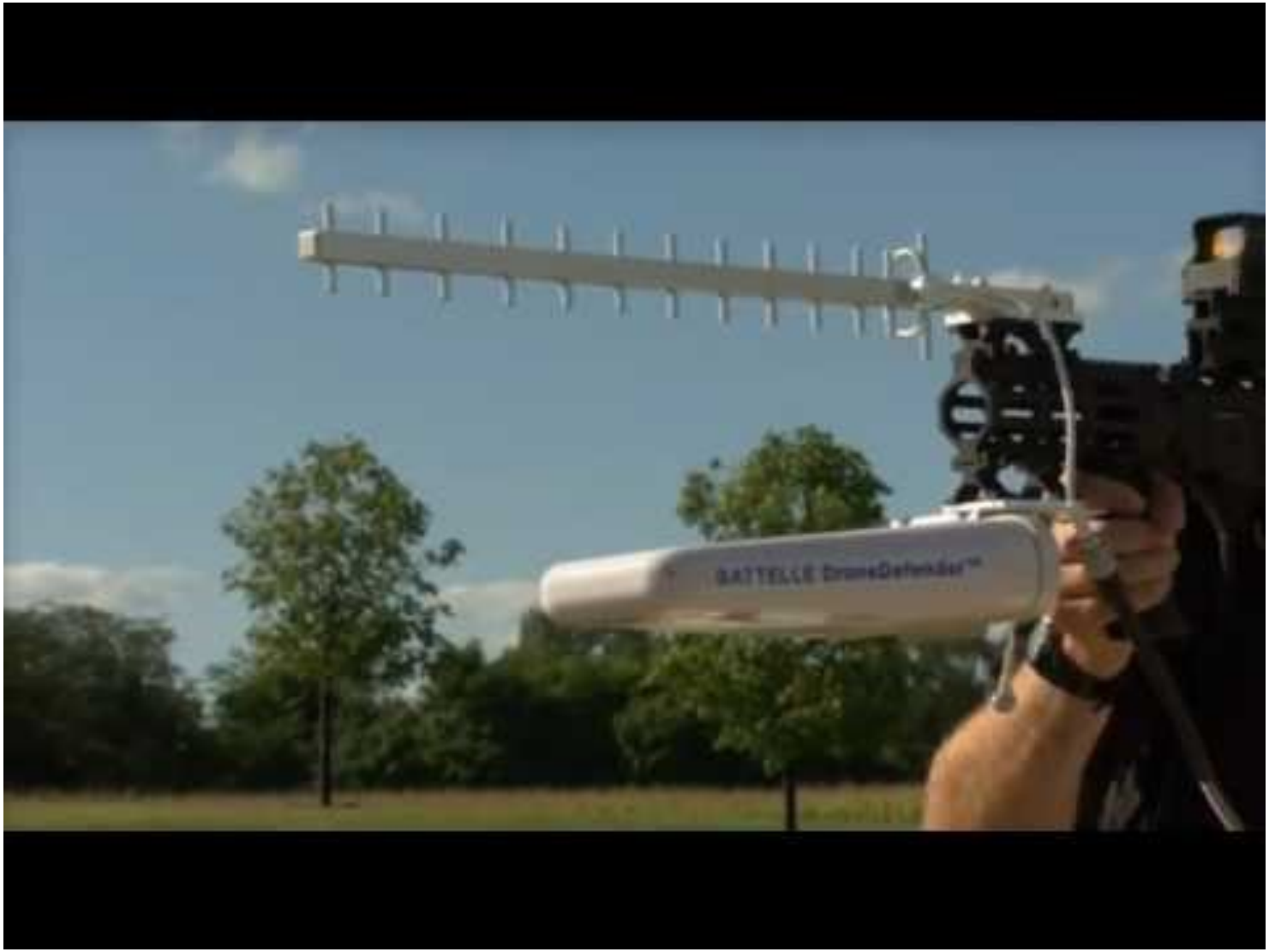
Availability : Device & Hardware

- Availability of IoT devices
  - Resource consumption attacks (Consumption of battery)
  - Physical attacks on device♪



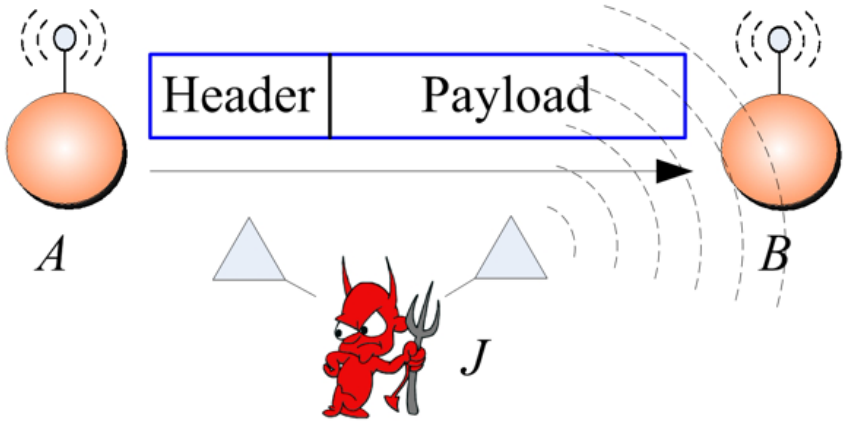
[Reference 4 : Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors, Usenix Security'16]♪

Availability : Device & Hardware



Availability : Network / Cloud & Server

- Jamming attacks on network are possible



[Source : http://www2.engr.arizona.edu/~aaproano/research.php]♪

- The biggest challenge is DDoS attacks on a server
  - IoT devices generate lots of connection requests to the server ♪

Authentication

- Hardware & Device authentication
  - The use of default passwords
  - E.g., Raspberry PI → ID : pi , Password : raspberry
- Network authentication
  - Sybil attacks
- Cloud & Server authentication
  - Identity management
    - Mange a lot of identifier of IoT devices
  - Privacy-aware identification

Access Control

- Access control of IoT devices
  - Physical access : Lack of local access control♪
- Access control of Cloud/Server
  - Remote attacks using weak access control
    - The companies, Sprint and Jeep, allows a femtocell to scan vehicles and send attack messages

[Airave 2.0 femtocell]♪

2013 RAM CHASSIS 5500
2014 DODGE DURANGO
2014 DODGE VIPER
2014 JEEP CHEROKEE
2014 JEEP GRAND CHEROKEE
2014 RAM 1500

[Scan result]♪

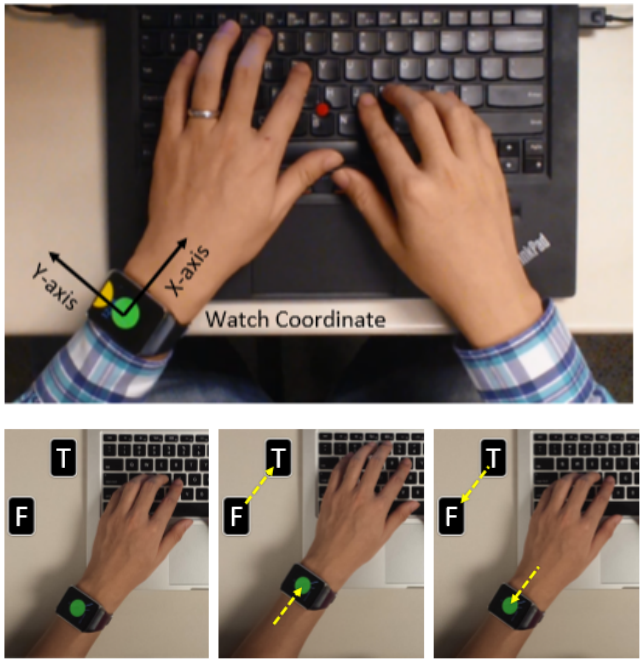
[Jeep's Uconnect]♪

[Reference 5 : Remote Exploitation of an Unaltered Passenger Vehicle, Defcon 23 (2015)]♪

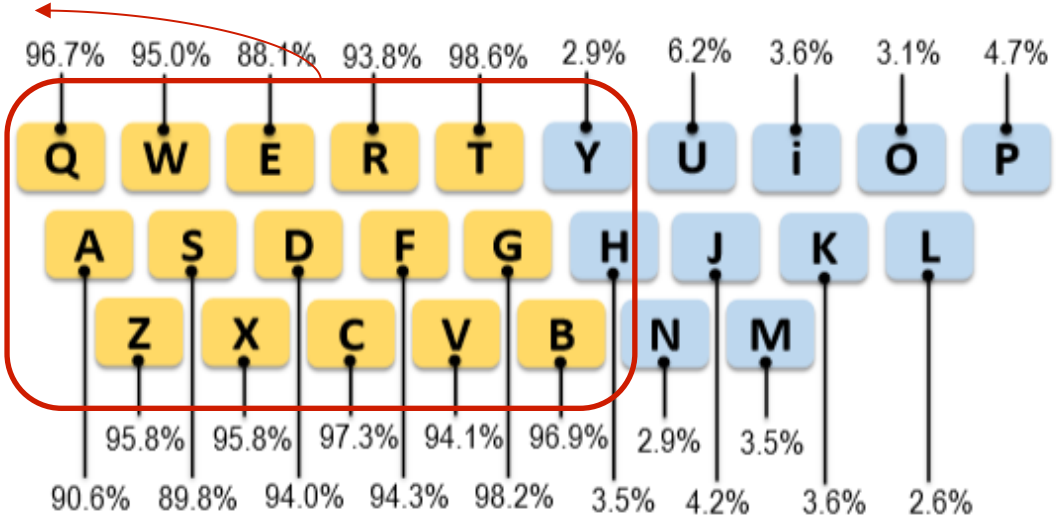
  - Conditional access control
    - A doctor may view a patient's record if they are treating that patient i n the emergency room♪

Privacy : Hardware & Device

- Management of permissions
  - Accelerometer and gyroscope can be used without permissions



These key stroke well identified
To infer other key, context and dictionaries are used♪

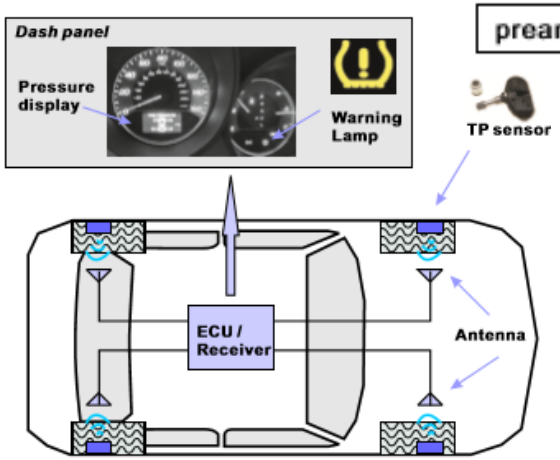


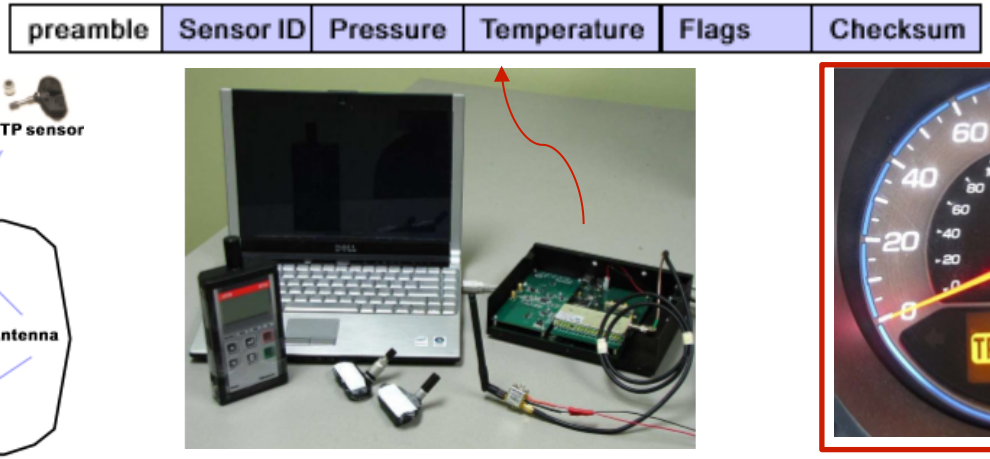
[Reference 6 : MoLe: Motion Leaks through Smartwatch Sensors, MobiCom'15] ♪

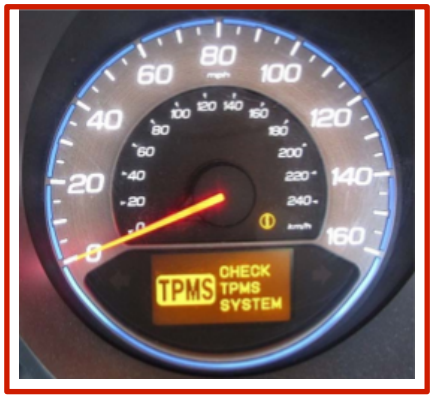
Privacy : Network

- Bluetooth and WiFi systems use unique identifiers called MAC address
  - These can be identified by scanning → effectively can follow users geographically around

- TPMS (Tire Pressure Monitoring System) was used for location trace (But, Attack range is up to 40 meters)







[Reference 7 : Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, IEEE Security and Privacy 2010]♪

Privacy : Cloud & Server

- Metadata **= Surveillance by Bruce Schneier ♪**
  - Any data other than the contents of a communication
  - E.g., the time a file was created, IP address, …

- Cross-device tracking : computer, smartphone, tablet, smart TV, and, IoT devices♪

[Reference 8 :The Internet of Things that Talk About You Behind Your Back, Schneier on Security, 2016]♪

[Source : https:// uwnthesis.wordpress.com/]♪

[Source : https://www.gizmodo.com.au]

Security & functionality requirements for IoT

- REQ1 - Integrity and Confidentiality
- REQ2 - Access Control
  - REQ2.1 - Consent
  - REQ2.2 - Policy-based access control
- REQ3 - Authentication
  - REQ3.1 - Federated Identity
  - REQ3.2 - Secure Device Identity → Management of secret values
  - REQ3.3 - Anonymous Identities
- REQ4 - Attestation
- REQ5 - Summarization and Filtering
- REQ6 - Context-based security and Reputation
- REQ7 - IoT-specific Protocol Support

Middleware for IoT

- 213 papers for IoT middleware were identified
  - 54 middleware systems
  - 35 middleware systems had no published discussion or architecture for security
  - 19 middleware systems that implement or describe security architecture

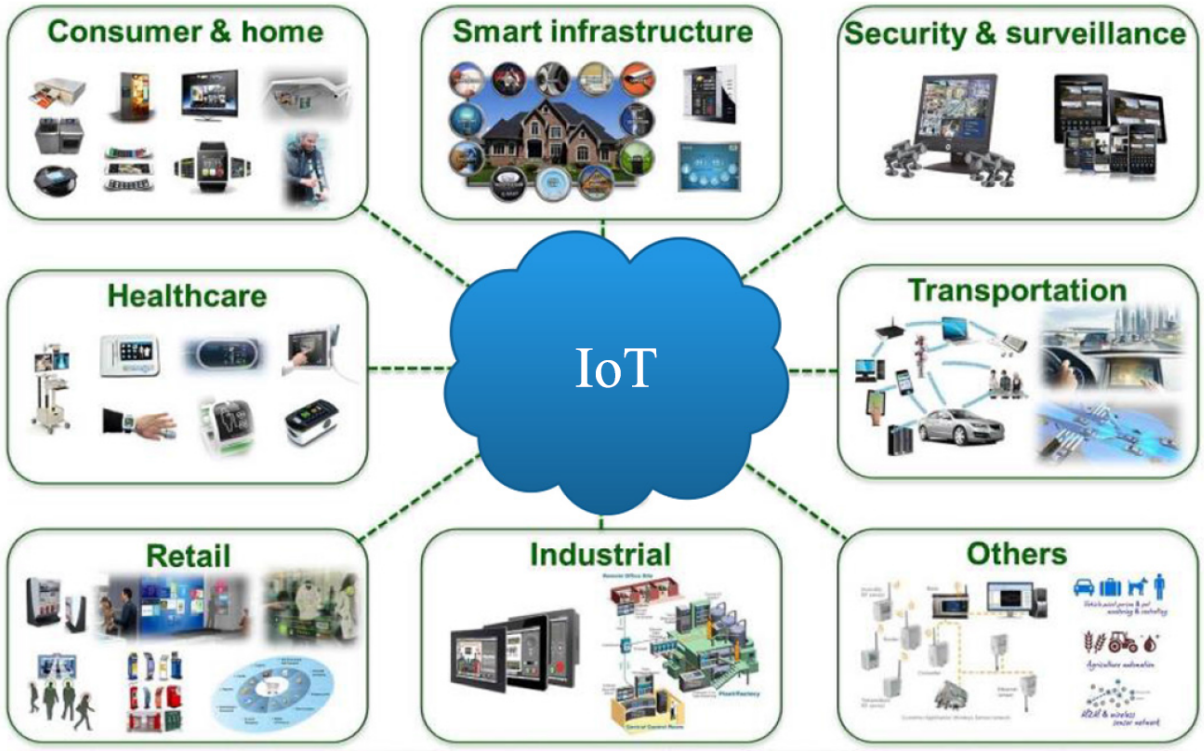
Reviewed middleware systems

- 19 middleware systems are evaluated by using the following security requirements

	REQ1 -Integrity and Confidentiality	REQ2 -Access Control	REQ2.1 -Consent	REQ2.2 -Policy-based security	REQ3 - Authentication	REQ3.1 -Federated Identity	REQ3.2 -Secure Device Identity	REQ3.3 - Anonymous Identities	REQ4 -Attestation	REQ5 - Summarisation and Filtering	REQ6 -Context-based security/ Reputation	REQ7 -IoT-specific Protocol Support
&Cube	Y	Y			Y							Y
Device Cloud	Y	Y	Y		Y	Y						Y
DREMS	Y	Y			Y							Y
DropLock		Y	Y		Y	Y						Y
FIWARE	Y	Y	Y	Y	Y	Y						Y
Hydra/Linksmart	Y	Y			Y		Y					
Income	Y	Y		Y	Y						Y	
IoT-MP	Y				Y							
NERD	Y				Y							Y
NOS	Y	Y			Y						Y	Y
OpenIoT					Y	Y						
SensorAct		Y		Y								
SIRENA	Y				Y							
SMEPP	Y	Y			Y							
SOCRADES	Y	Y			Y							
UBIWARE				Y								
WEBINOS	Y	Y		Y	Y	Y	Y					
XMPP	Y	Y			Y	Y						
VIRTUS	Y	Y			Y	Y						

Conclusion

- Each IoT device is designed for a specific purpose
- Thus, security requirements for IoT middleware also need to be classified according to IoT applications♪



[Source : https://bensontao.wordpress.com/2013/10/06/vivante-internet-of-things/]♪