IoT Security and Privacy

Overview of IoT

Learning Outcomes

Upon completion of this unit:

- Student will understand different visions of the Internet of Things (IoT) paradigm
- Students will understand the enabling technologies, their advantages and disadvantages
- Students will understand different aspects of IoT security and privacy

Outline

- Different visions of the Internet of Things (IoT) paradigm
- Enabling technologies, their advantages and disadvantages
- IoT Applications
- End-to-end view of IoT security and privacy
- Example IoT hack

Impact of IoT

- US National Intelligence Council (NIC) lists IoT as one of six ‘‘Disruptive Civil Technologies” giving US the edge in terms of national power
- NIC foresees both benefits and threats
  - ‘‘by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more”.
  - ‘‘popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development”.
  - ‘‘to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date”.

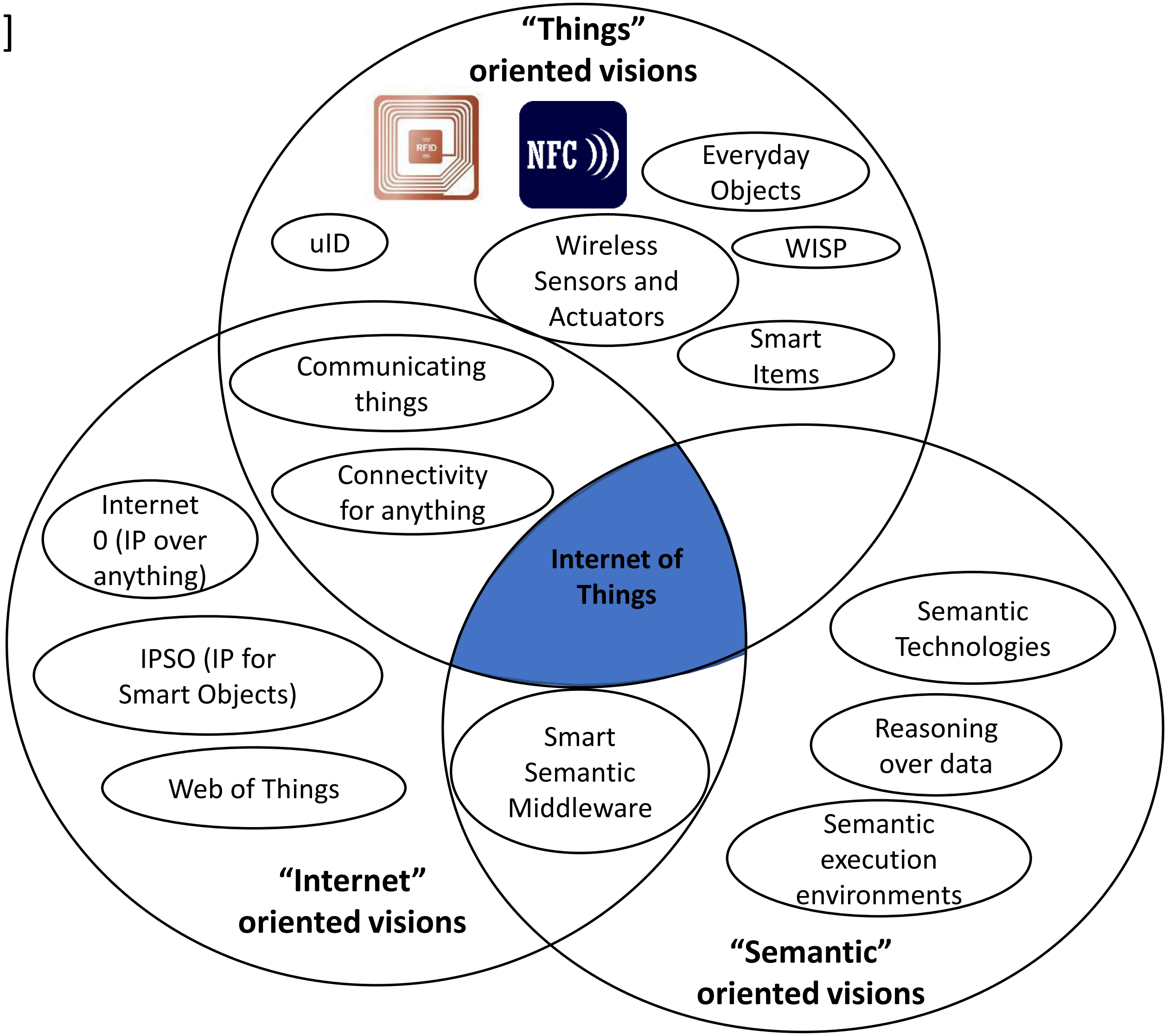
Challenges of IoT

- Fully interoperate a large number of heterogeneous interconnected devices, which may
  - have low computation and energy capacity
  - require resource efficient solutions
  - require scalable solutions
- Integrates high degree of smartness with adaptation and autonomous-ness
- Guarantee trustworthiness with security and privacy

Views of IoT

- Internet oriented
    - Interconnect things with standard communication protocols
- Things oriented
    - Uniquely address things
- Semantic oriented
    - Represent and store exchanged information

Internet of Things from different visions [1]


"Things" oriented visions
RFID
NFC
Everyday Objects
uID
Wireless Sensors and Actuators
WISP
Smart Items
Communicating things
Connectivity for anything
Internet 0 (IP over anything)
Internet of Things
Semantic Technologies
IPSO (IP for Smart Objects)
Reasoning over data
Smart Semantic Middleware
Web of Things
Semantic execution environments
"Internet" oriented visions
"Semantic" oriented visions

First definition of IoT

- Comes from a ‘‘Things oriented” perspective
  - Interconnecting simple Radio-Frequency IDentification (**RFID**) tags
- Coined by *Auto-ID Labs*, which
  - Are a world-wide organization of academic research laboratories on networked RFID and emerging sensing technologies.
  - Advocate the Electronic Product Code™ (EPC) for broad adoption of RFID in world-wide modern trading networks
  - Create the industry-driven global standards for the EPCglobal Network™

uID

- Unique/Universal/Ubiquitous IDentifier (uID) is a competing architecture
  - Development of middleware based solutions for a globally addressable objects
- RFID is the mainstream driving the vision
  - RFID is mature, of low cost, and has strong support from the business community.

Future of IoT

- Will contain diverse device, network, and service technologies
- Driving components linking the real world with the digital world
    - Near Field Communications (NFC)
    - Wireless Sensor and Actuator Networks (WSAN)
    - RFID
- Ongoing major projects developing relevant platforms
    - WISP (Wireless Identification and Sensing Platforms) project.
- Spime, a concept related to IoT, refers to an object
    - trackable through space and time throughout its lifetime
    - Sustainable
    - Enhanceable
    - Uniquely identifiable

the ITU vision of the IoT

- ITU (International Telecommunication Union)
- ‘‘from anytime, anyplace connectivity for anyone, we will now have connectivity for anything”
- ‘‘Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”

Outline

- Different visions of the Internet of Things (IoT) paradigm
- Enabling technologies, their advantages and disadvantages
- IoT Applications
- End-to-end view of IoT security and privacy
- Example IoT hack

Enabling technologies

- Identification
- Sensing
- Communication technologies
- Middleware

RFID

- Architecture: one or more reader(s) and multiple RFID tags
- Tags
  - A small microchip[1] attached to an antenna, e.g. Hitachi tag 0.4 mm x 0.4 mm x 0.15 mm
  - Attached objects (including persons or animals).
  - A unique identifier
- Readers
  - Generate a radio frequency signal to query tags
  - Trigger the tag transmission by the emitting signal
  - Receive tag IDs.
- Properties
  - Monitor objects in real-time
  - No need of line-of-sight
  - Mapping objects into the virtual world
- Various applications including logistics, e-health and security.

Different RFID Based on Power Capability

- Passive RFID tags
  - No onboard power supplies
  - Harvest the energy from the query signal of a RFID to transmit their IDs
- Semi-passive RFID tags
  - Batteries powered reception
  - Reader signal powered transmission
- Active RFIDs
  - Battery powered reception and transmission
  - Highest radio coverage with higher production costs

Sensor networks

- A sensor network
  - Sensing nodes communicate in a multi-hop fashion wirelessly.
  - Nodes report sensing results to sink nodes.
- Design objectives of layers of communication
  - Energy efficiency, given energy is scarce
  - Scalability for the large number of nodes
  - Reliability in data transmission in case of urgent events
  - Robustness in case of failures

IEEE 802.15.4 Sensor Networks

- Defines the physical and MAC layers for low-power, slow communications in wireless personal area networks (WPAN)
- No specifications on the higher layers of the protocol stack, .e.g. connecting sensor nodes into the Internet.
- Challenges for standardizing up-layer protocols
  - A very large number of nodes v.s. IP
  - 802.15.4 physical layer packet is 127 bytes and too small for IP
  - Sensor nodes often in a sleep mode for energy saving are anomalous for IP networks.

Use of Sensor Networks

- Integration of sensing technologies into passive RFID tags
  - New IoT applications into the IoT context, e.g. e-health
- Intel wireless identification and sensing platforms (*WISP*).
  - Powered and read by passive RFID readers (no need of batteries),
  - Used to measure quantities such as light, temperature, acceleration, strain, and liquid level.

Comparison between RFID, wireless sensor networks, and RFID sensor networks

- RFID sensor networks (RSN)
  - Small, RFID-based sensing and computing nodes
  - RFID readers as sink nodes and power source

Table 1 Comparison between RFID systems, wireless sensor networks, and RFID sensor networks. [1]

	Processing	Sensing	Communication	Range (m)	Power	Lifetime	Size	Standard
RFID	No	No	Asymmetric	10	Harvested	Indefinite	Very small	ISO 18000
WSN	Yes	Yes	Peer-to-peer	100	Battery	<3 years	Small	IEEE 802.15.4
RSN	Yes	Yes	Asymmetric	3	Harvested	Indefinite	Small	None

Middleware

- A software layer or a set of sub-layers between underlying technological and application levels.
- Hiding the details of lower layer technologies
    - Exempt programmers from hardware and system details
    - Enable programmer to focus on their applications enabled by the infrastructure

Service Oriented Architecture (SOA)

- Decompose complex and monolithic systems into simpler and well-defined components.
  - Often not layered structure
- Use common interfaces and standard protocols for easy interconnection
- Abstract devices functionalities and communications functionalities
  - Common set of services
  - An environment for service composition

SOA-based Architecture [1]

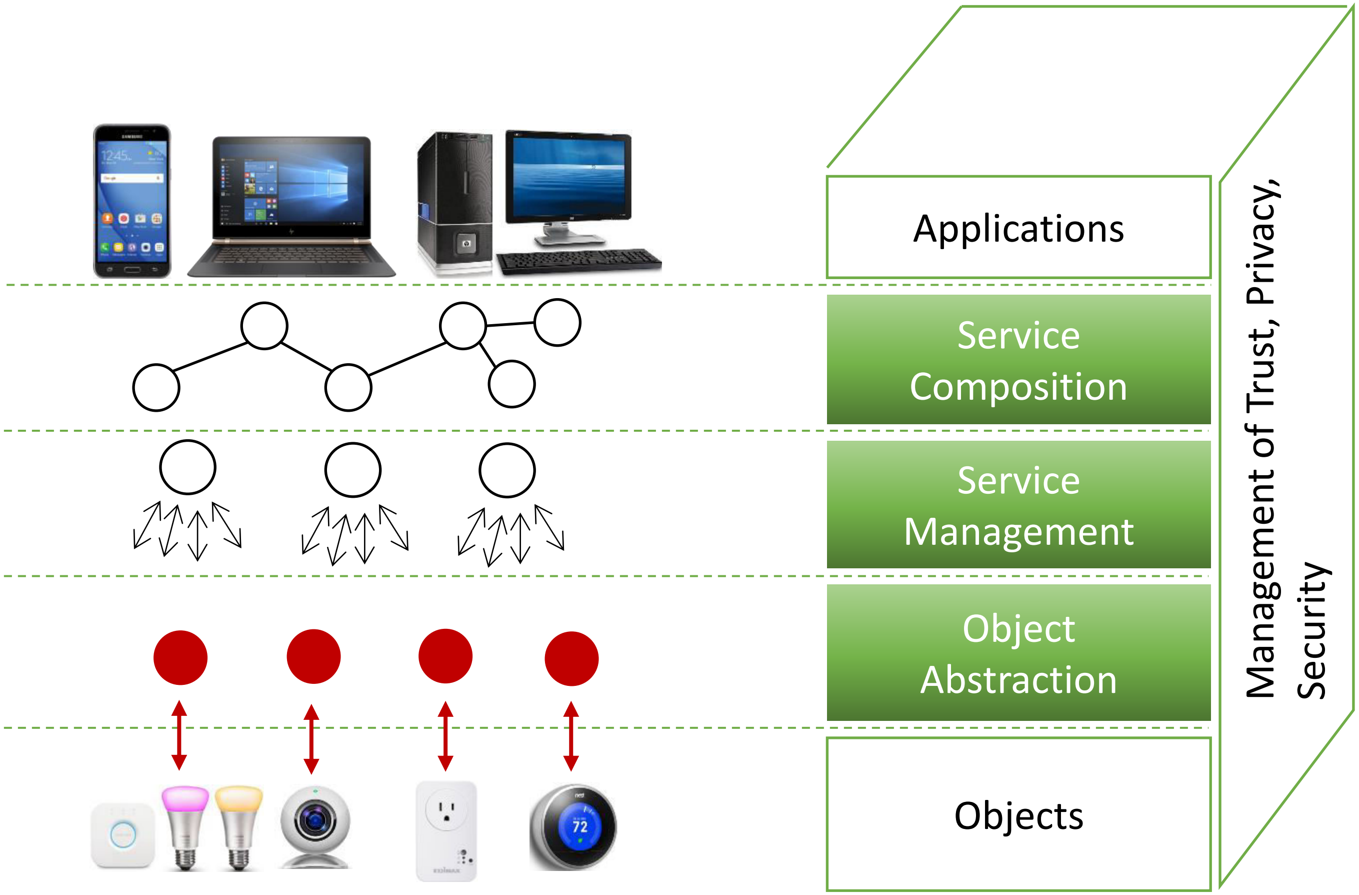


Fig.2. SOA-based architecture for the IoT middleware

SOA Components

- Applications – implementing the (distributed) system’s functionalities by using
  - Standard web service protocols
  - Service composition technologies
- Service composition - Composition of single services for applications
  - Services are visible assets
  - Use business workflow languages to compose complex services

SOA Components (Cont’d)

- Service management – providing object dynamic discovery, status monitoring, and service configuration
  - A service repository lists the catalogue of services and associated objects for easy reference
- Object abstraction: standardizing access to different devices through a common language and procedure
  - Interface layer – use a web interface exposing the methods; manages communications with the external world.
  - The communication sub-layer – implementing the web service methods and communicating with the real-world objects

SOA Components (Cont'd)

- Trust, privacy and security management
  - For example, malicious query of RFID tags for surveillance of our lives.
  - Managed by the middleware for all the exchanged data.
  - Built on one specific layer or distributed through all layers,
  - No obvious degradation of system performance

Other Architectures - Fosstrak

- Management of **RFID** related applications
- An open source RFID infrastructure implementing the EPC Network specifications
  - Data dissemination, aggregation, filtering, interpretation
  - Writing to a tag, trigger RFID reader from external sensors
  - fault and configuration management
  - Sharing RFID triggered business events, lookup and directory service
  - Tag identifier management, and privacy

Other Architectures - e-SENSE project

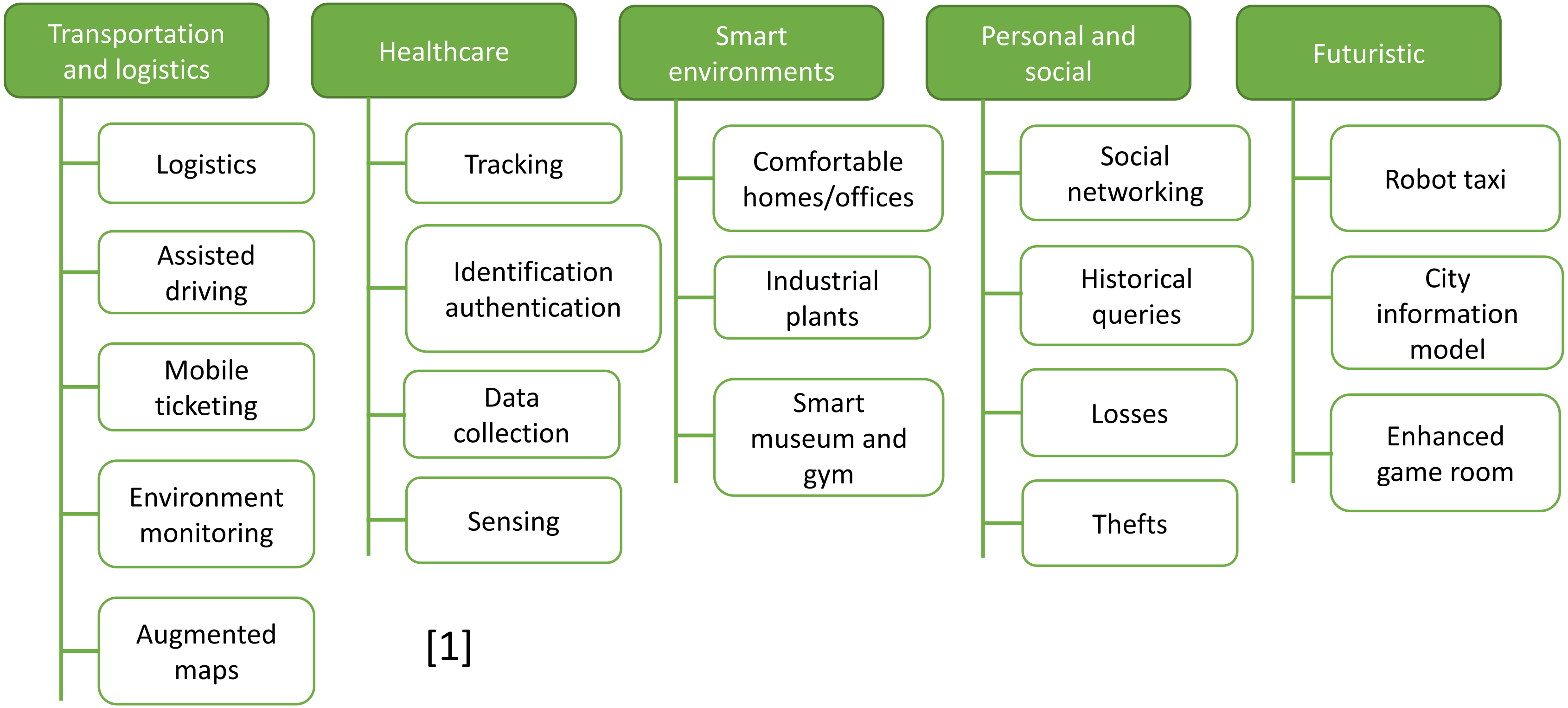
- Capturing ambient intelligence through **WSNs**
- Four logical subsystems
  - Application, management, middleware, and connectivity.
  - Each subsystem uses service access points to provide access to other subsystems
- This entire stack is implemented in a full function sensor node and a gateway node?
  - A reduced-function sensor node has fewer functions.
- The middleware subsystem works in a distributed fashion
- The result can be sent to an actuating node and/or to the fixed infrastructure through a gateway

Outline

- Different visions of the Internet of Things (IoT) paradigm
- Enabling technologies, their advantages and disadvantages
- IoT Applications
- End-to-end view of IoT security and privacy
- Example IoT hack

Applications and Example Scenarios

- Transportation and logistics domain.
- Healthcare domain.
- Smart environment (home, office, plant) domain.
- Personal and social domain



[1]

Transportation and Logistics

- **Logistics**: Real-time monitoring of the supply chain, such as raw material purchasing, transportation storage, and after-sales service, for example by use of RFID and NFC
- **Assisted driving**: Collision avoidance, monitoring of transportation of hazardous materials, road traffic patterns
- **Mobile ticketing**: NFC tag
- **Monitoring environmental parameters**: transportation of fruits, fresh-cut produce, meat, and dairy product with monitored environment
- **Augmented maps**: Tagged touristic maps for read by NFC-equipped phones

Healthcare Domain

- **Tracking**: the identification of moving person or object **Identification and authentication**: patient identification, electronic medical record maintenance, and infant identification to prevent mismatching
- **Data collection**: automatic form processing, process automation, automated care and procedure auditing, and medical inventory management
- **Sensing**: diagnosing patient conditions, providing real-time information on patient health indicators

Smart Environments

- Comfortable homes and offices
- Industrial plants: automation through tagged production parts
- Smart museum
  - Monitored museum environment good for expositions
- Smart gym
  - Personalized training with loaded health parameters to prevent overtraining or ensure appropriate exercises.

Personal and Social

- **Social networking**: RFID tags
- **Historical queries** of where, how, and with whom or what through for example the Google Charts API
- **Losses**: view the last recorded or real-time location of tagged objects
- **Thefts**: similar to the loss

Futuristic applications domain

- **Robot taxi**: adapt to real-time traffic, reduce congestion reduce congestion of busy roads
- **City information model**: monitoring the status and performance of buildings and urban fabrics – such as pedestrian walkways, cycle paths and heavier infrastructure like sewers, rail lines, and bus corridors
- **Enhanced game room**: body sensor network to sense location, movement, acceleration, humidity, temperature, noise, voice, visual information, heart rate and blood pressure.

Open Issues [1]

Table 2 Open research issues

Open issue	Brief description of the cause	Details in
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework	Section 5.1
Mobility support	There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems	Section 5.2
Naming	Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa*	Section 5.2
Transport protocol	Existing transport protocols fails in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects*	Section 5.2
Traffic characterization and QoS support	The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes	Section 5.2
Authentication	Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is serious problem	Section 5.3
Data integrity	This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection	Section 5.3
Privacy	A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques	Section 5.3
Digital forgetting	All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years	Section 5.3

Standardization activity [1]

- Different sections of the Auto-ID Lab scattered all over the world
- European Commission and European Standards Organizations (ETSI, CEN, CENELEC, etc.) and international counterparts ISO, ITU
- IETF, EPCglobal, etc.

Standard	Objective	Status	Comm. Range(m)	Data rate (kbps)	Unitary cost ($)
EPCglobal	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products	Advanced	~ 1	~ 10^2	~ 0.01
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things*	Ongoing	~ 1	~ 10^2	~ 0.01
M2M	Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off	Ongoing	N.S.	N.S.	N.S.
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 networks	Ongoing	10 - 100	~ 10^2	~ 1
ROLL	Definition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	N.S.	N.S.	N.S.
NFC	Definition of a set of protocols for low range and bidirectional communications	Advanced	~ 10^2	Up to 424	~ 0.1
Wireless Hart	Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices	Advanced	10 - 100	~ 10^2	~ 1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10 - 100	~ 10^2	~ 1

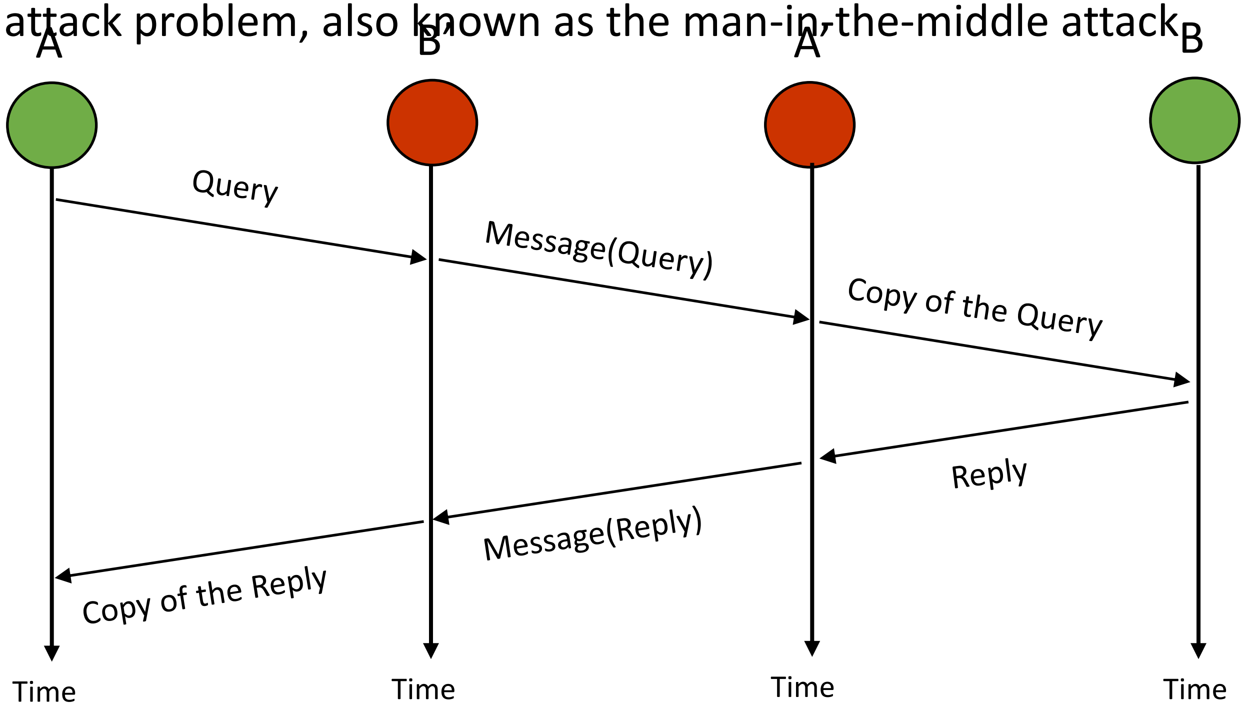
Table 3 Characteristics of the most relevant standardization activities

Addressing and Networking Issues

- 6LoWPA: IPV6 addressing for low-power wireless
  - Enough?
- Integration of RFID tags through 64–96 bit identifiers by EPCglobal, solutions into IPv6 networks
- Open issues:
  - Mobility support
  - Object Name Service (ONS) like DNS
  - Reliable transmission and congestion control: tcp too costly in terms of overhead and buffering?

Security

- Physical attack, eavesdropping, weak security schemes because of poor computation power
  - authentication and data integrity
  - proxy attack problem, also known as the man-in-the-middle attack



Man in the middle attack

Security (Cont’d)

- Data integrity to detect the data change
    - Unattended RFID systems
    - Data modified while stored in the node or during transmission
- Typical cryptographic algorithms too costly for low energy and bandwidth IoT nodes

Privacy

- IoT devices are pervasive
- Privacy solutions
  - individuals control their data in terms of collection by who and when
  - Personal data should be used for only authorized services by authorized service providers
  - Personal data should be stored only when really needed

Privacy (Cont'd)

- Challenges
  - Pervasive sensor networks monitoring individuals entering. How to control?
- Solutions
  - Privacy broker
  - digital forgetting? (delete on purpose automatically)

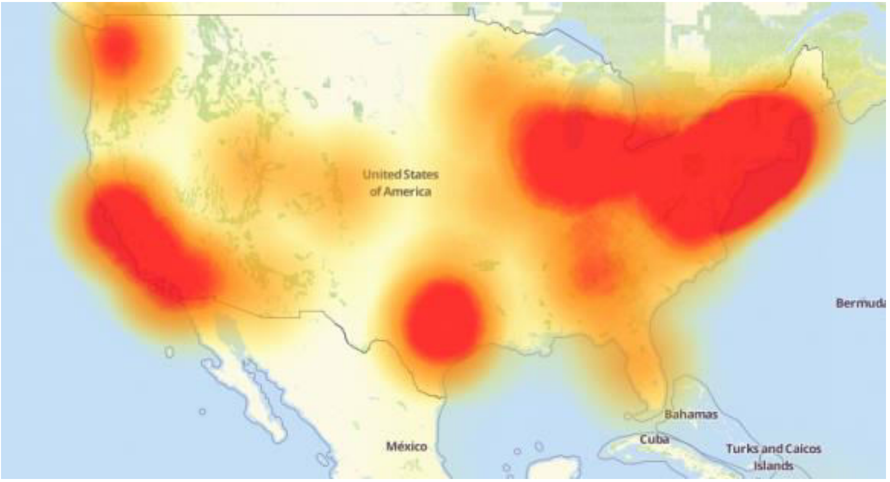
Outline

- Different visions of the Internet of Things (IoT) paradigm
- Enabling technologies, their advantages and disadvantages
- IoT Applications
- End-to-end view of IoT security and privacy
- Example IoT hack

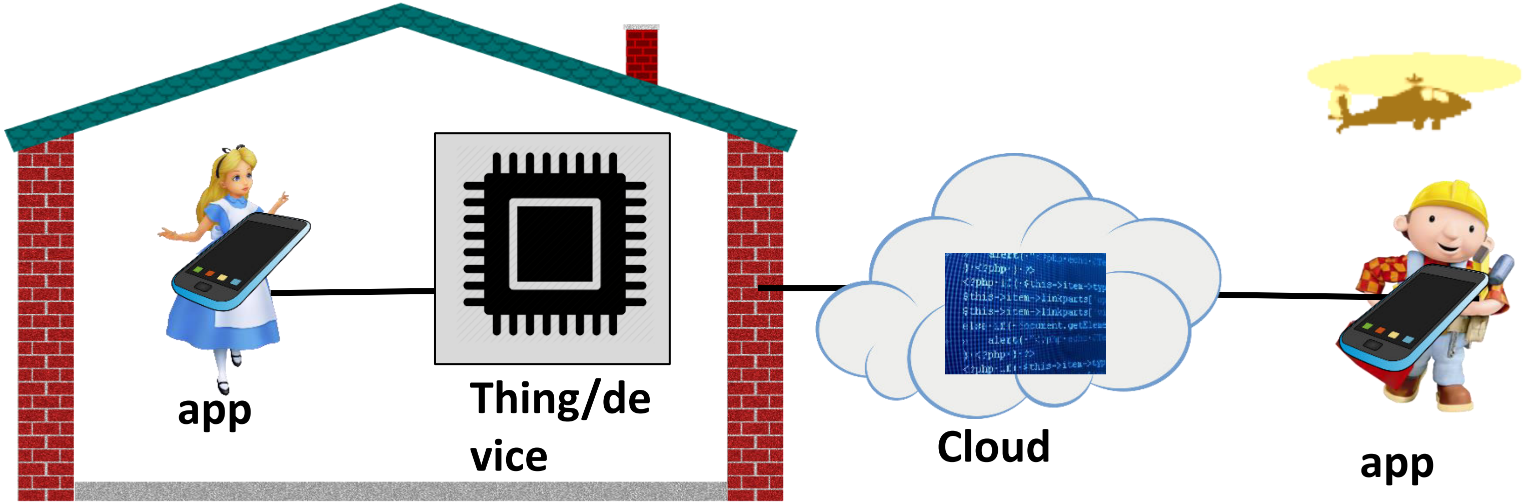
IoT Challenge: Security and Privacy

- Threats from IoT
  - Intrusion into mobiles
  - Drone
  - Skynet

- Threats against IoT
  - Smart bulbs
  - Mirai botnet



An End-to-End View of IoT



1 Upgrading

2 Pairing

3 Binding

4 Local authentication

5 Local control

10 Sensing & Notification

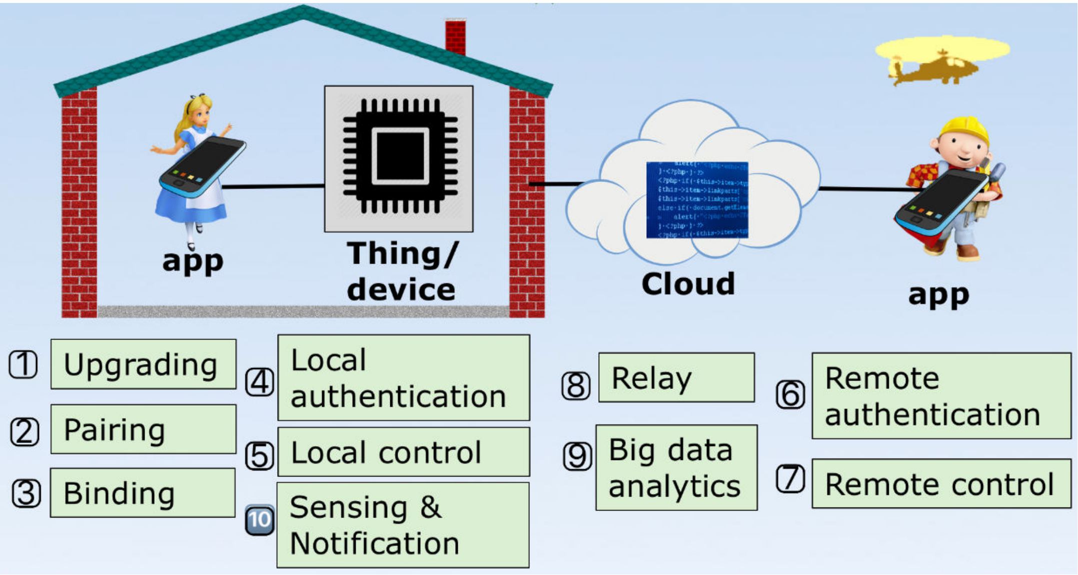
8 Relay

9 Big data analytics

6 Remote authentication

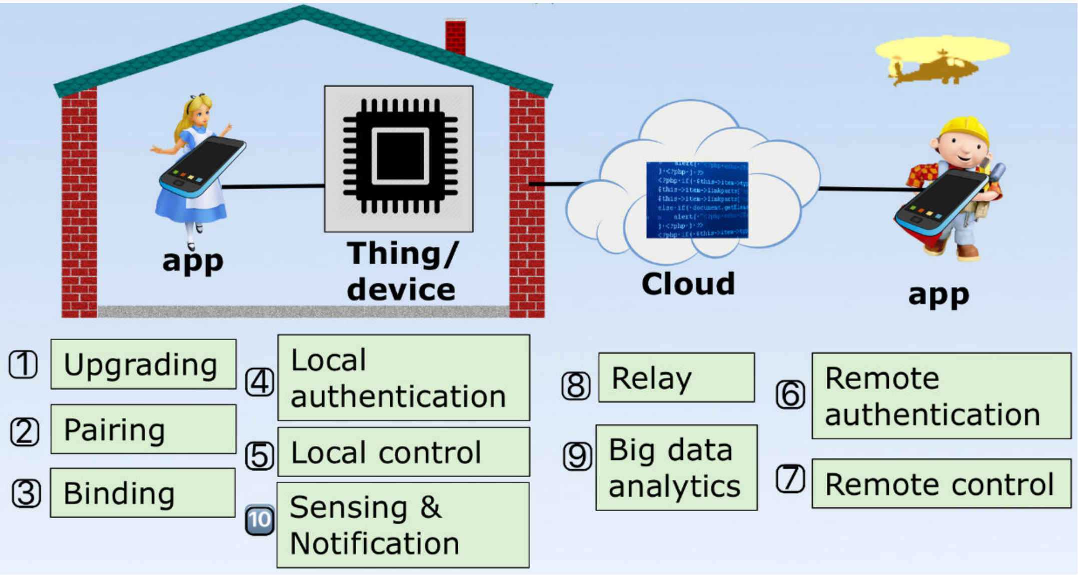
7 Remote control

IoT System/Software Security and Privacy



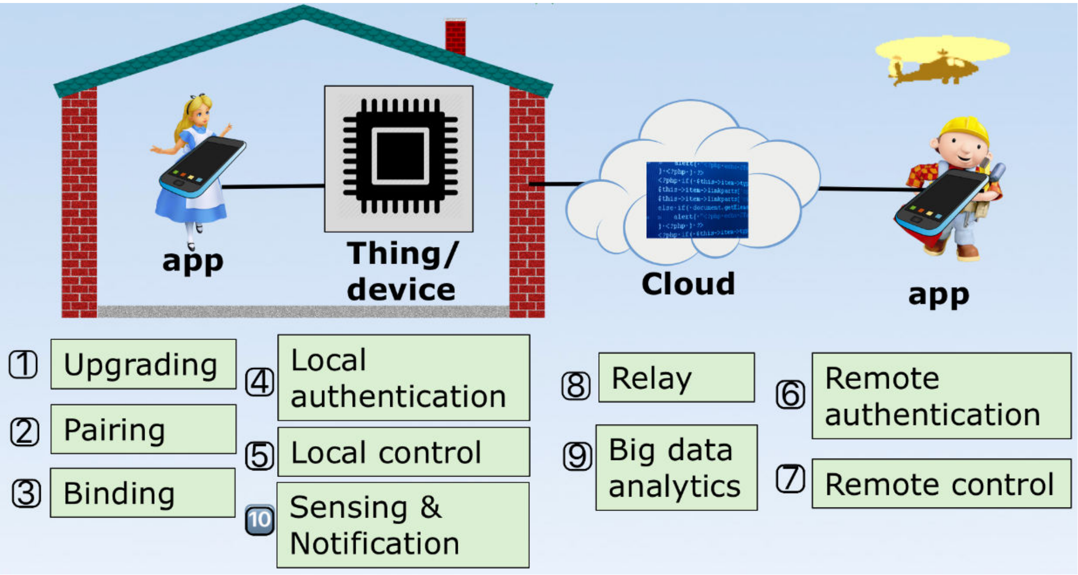
- Systems and software: control app, cloud, thing in both private and public setup
- Security measures: trustworthy OS, trust platform module (TPM), trust zone, software security

IoT Network Security and Privacy



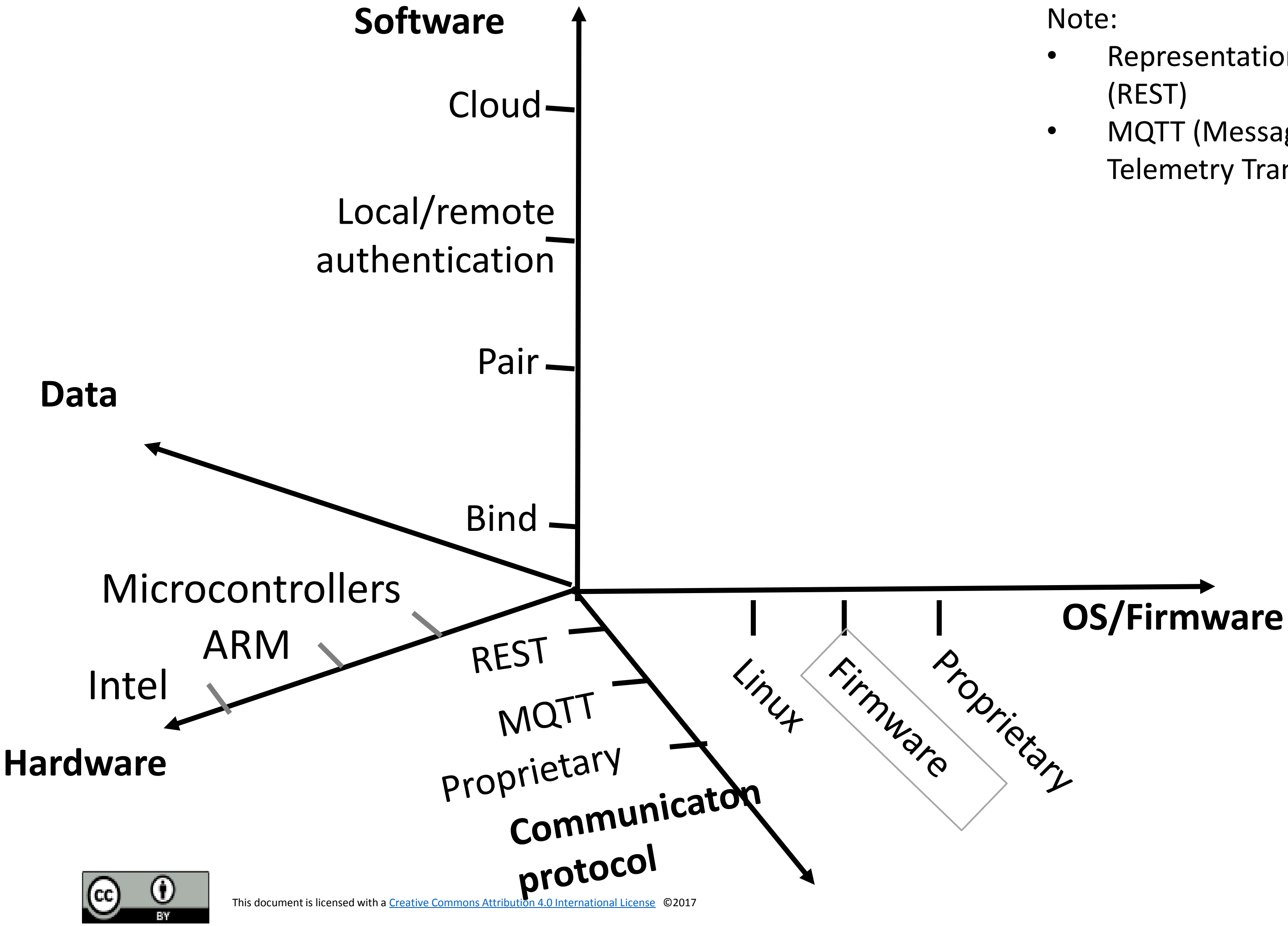
- Pairing – why should the thing trust the connecting hardware? Things in public settings?
- Binding – End-to-end authentication or through the cloud?
- Local or remote control/relay – communication privacy

IoT Big Data Analytics



- Should the cloud know everything?
- How about intrusion detection and prevention based on big data?

Risk Analysis of Internet of **Things**



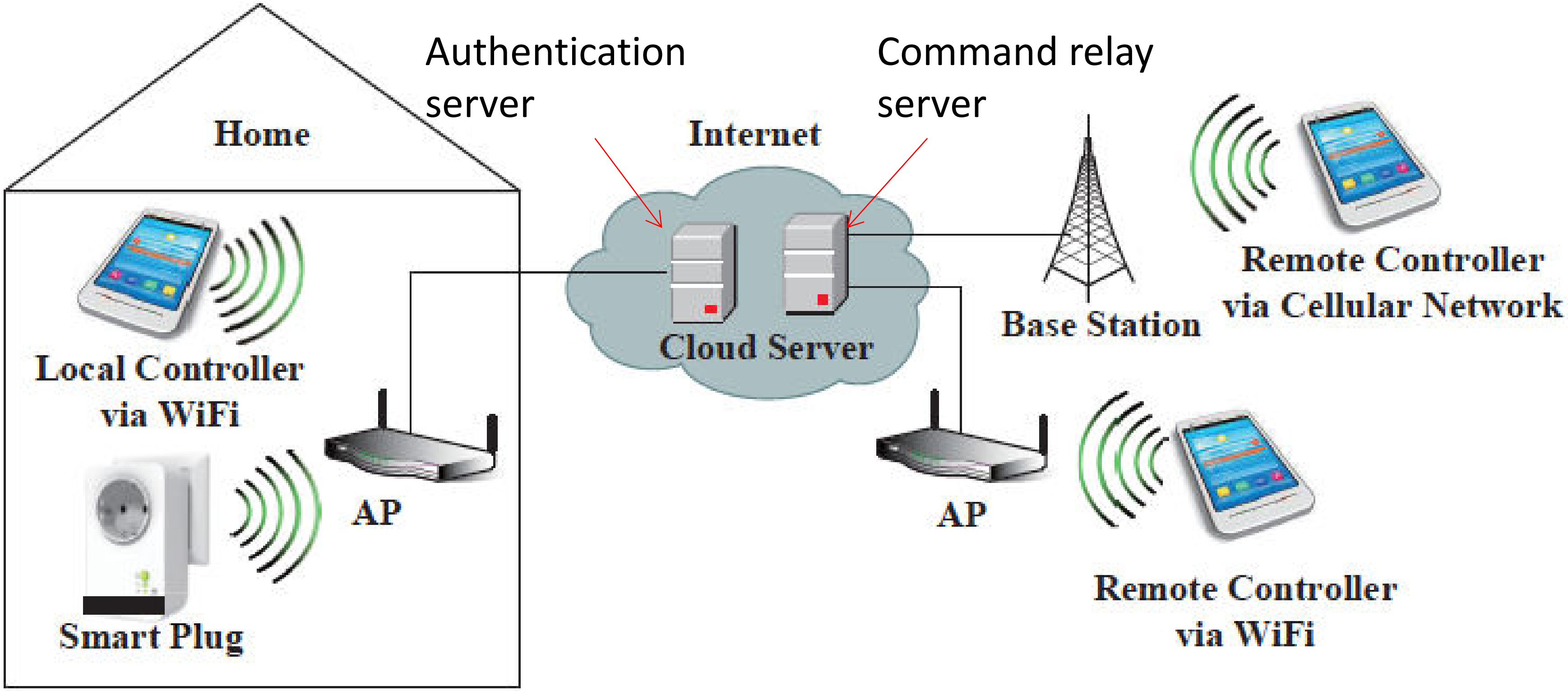
Note:

- Representational state transfer (REST)
- MQTT (Message Queuing Telemetry Transport)

Outline

- Different visions of the Internet of Things (IoT) paradigm
- Enabling technologies, their advantages and disadvantages
- IoT Applications
- End-to-end view of IoT security and privacy
- Example IoT hack [3]

Edimax Smart Plug


Home
Internet
Local Controller via WiFi
Smart Plug
AP
Cloud Server
Base Station
Remote Controller via Cellular Network
AP
Remote Controller via WiFi

Authentication server

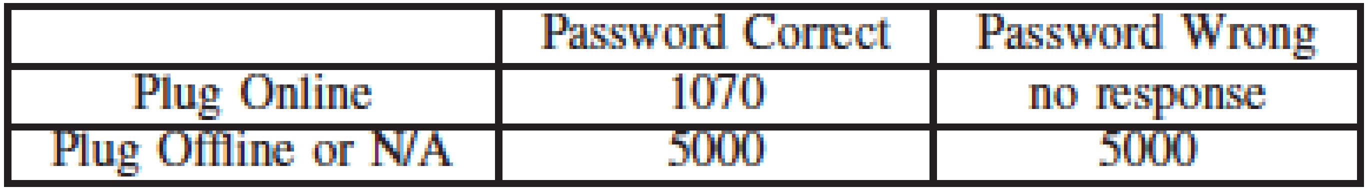
Command relay server

Insecure Communication Protocols

- No cryptographic mechanisms for the communication protocols
  - No encryption
  - Obfuscation based on a bit shifting strategy
- Reverse engineering attack
  - Communication protocol details
- Traffic analysis attacks
  - Password, user name if the traffic can be monitored

Device Scanning Attack

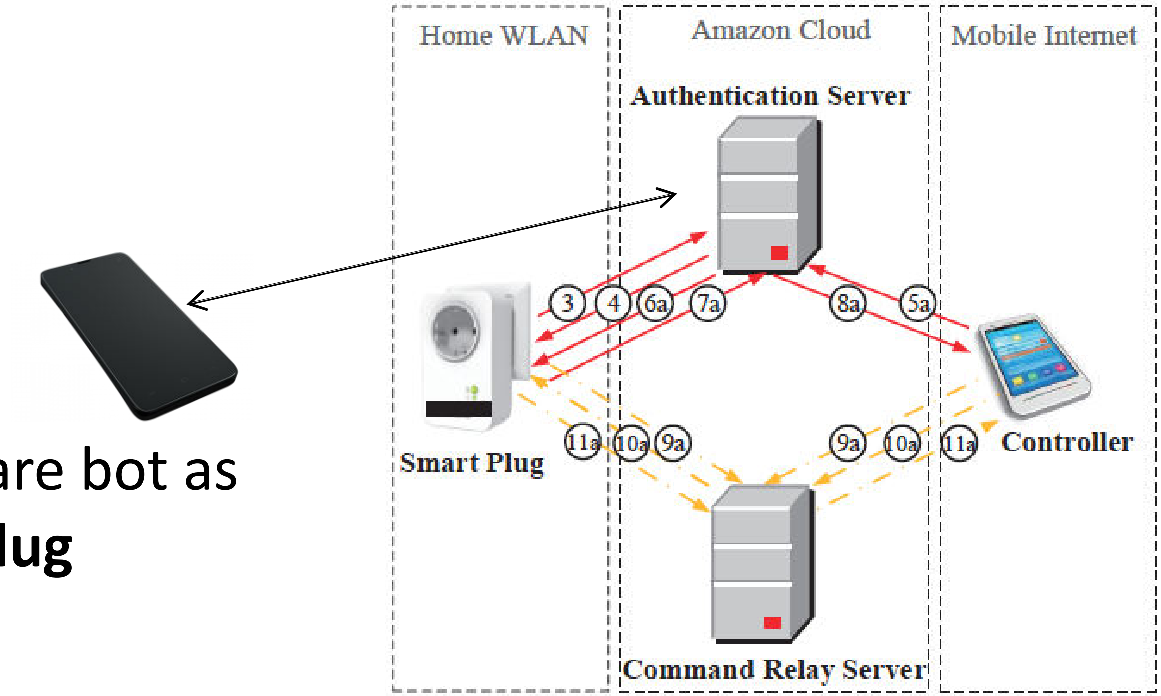
- Password based user authentication
  - User name: MAC address
  - Password: default “1234”
- Scanning the vendor’s MAC address space
  - Find the online status of all smart plugs
  - Reveal the use of default password
  - Many users do not change default passwords!!!
- Brute force attack against non-default passwords
  - No intrusion detection



	Password Correct	Password Wrong
Plug Online	1070	no response
Plug Offline or N/A	5000	5000

Device Spoofing Attack

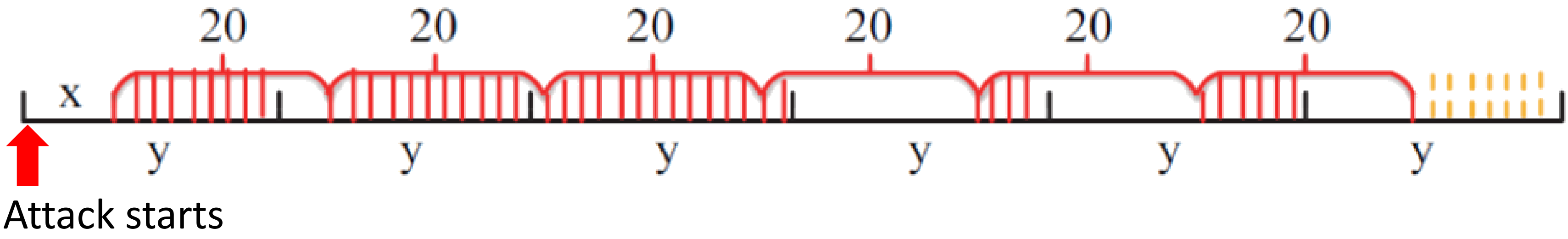
- A fake plug (program) registers itself with the cloud
  - The real device is pushed offline temporarily
- Credentials leak once users open the app



Software bot as **fake plug**

Success Rate of Device Spoofing Attack

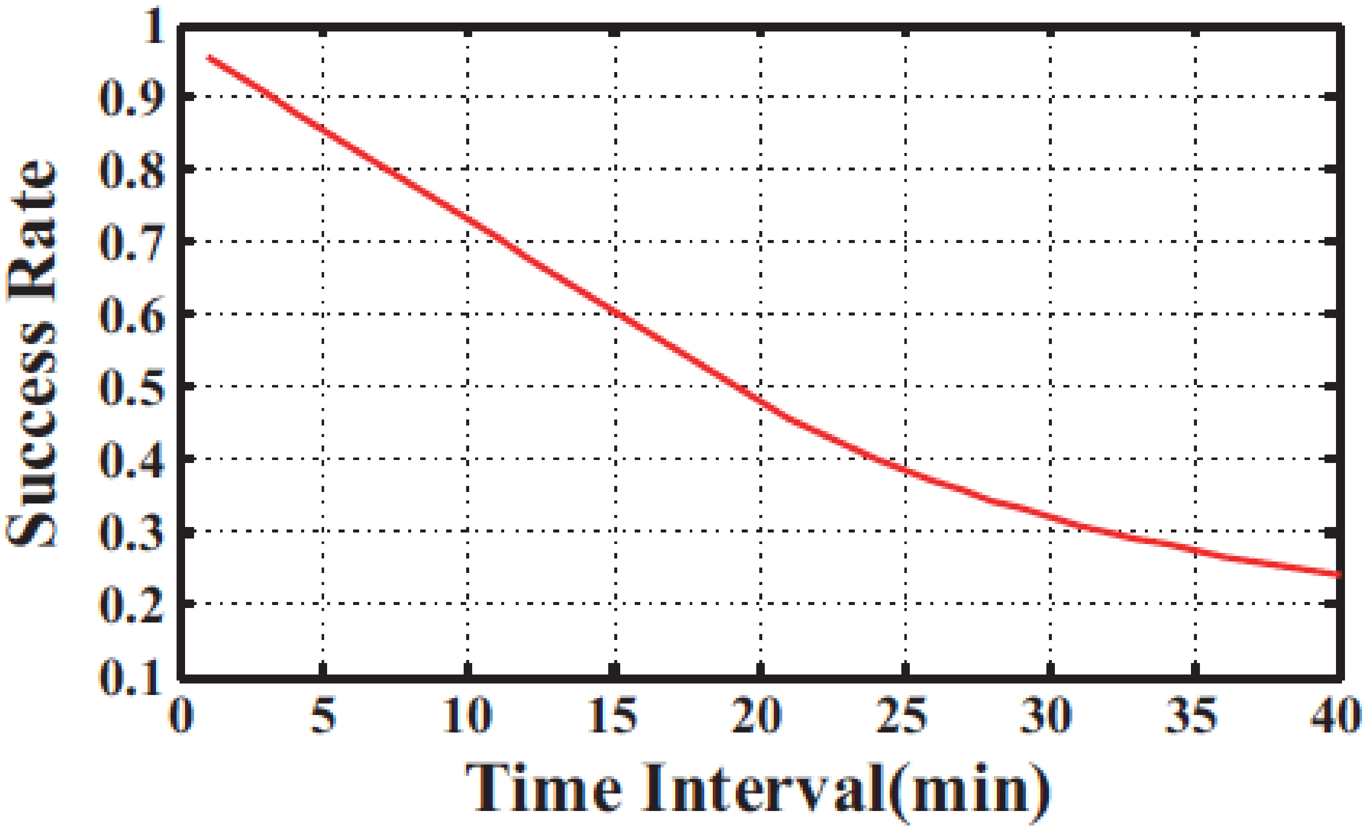
- Keep-alive messages from real plug every 20 minutes
- Keep-alive messages from fake plug every *y* minutes



- Success rate $S = 1 - \int_{x=0}^{20} \frac{\sum_{i=0}^{n-1} T(i) + T(n)}{20\lceil (x+20n)/y \rceil y} dx$, n>1
  - x: the time between first attack packet and real plug's first keep-alive message after the attack starts
  - T(i): the period in which real plug is active in i^th 20 minutes

Evaluation of Device Spoofing Attack

- Success rate vs fake registration packet time interval (y)



Local Firmware Attack

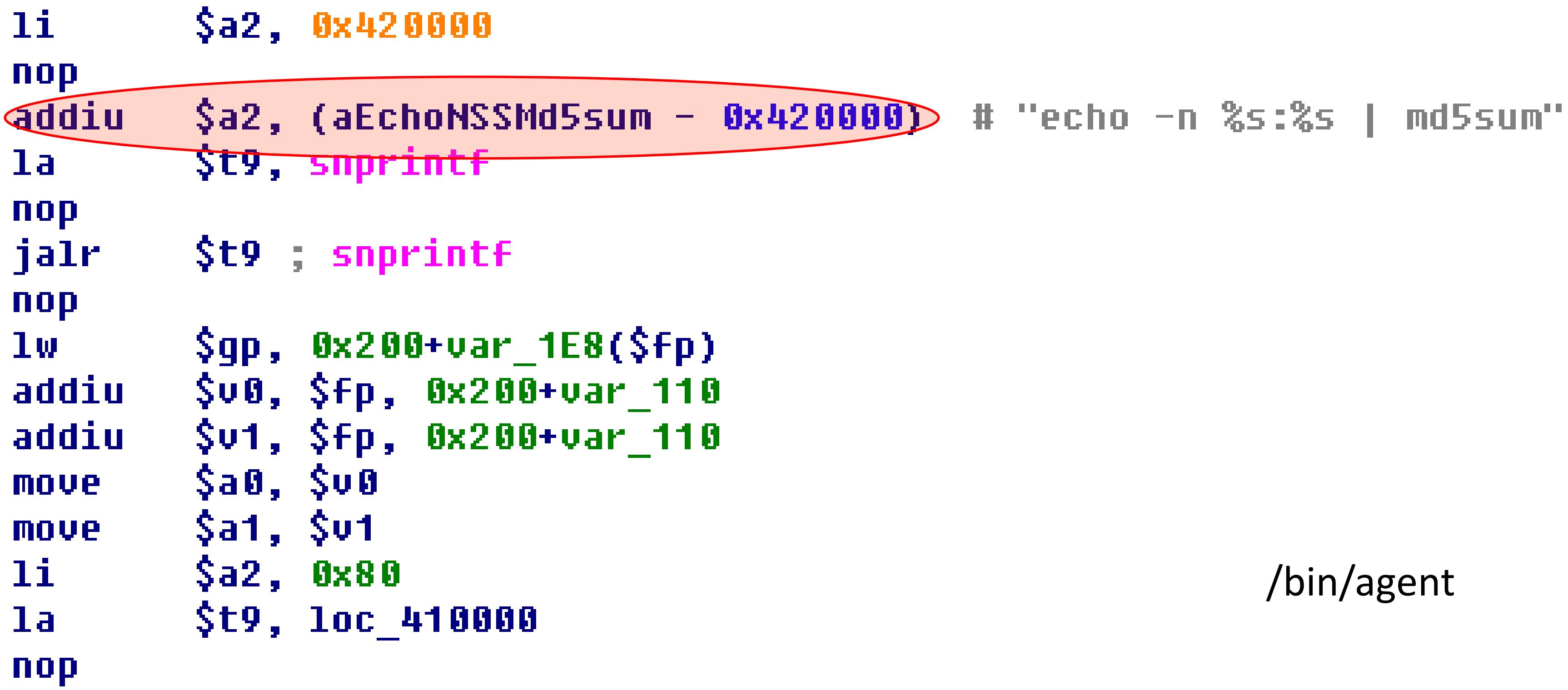
- Open port for firmware update in local networks

- No integrity checking and authentication for firmware upgrading/downgrading

- Installation of any malicious firmware
  - Reverse tunnel back to the attacker
  - Reverse root shell can be opened
  - Full control of the plug OS

Remote Command Injection Attack

- Vulnerability in password update
  - Calls a local md5 hash command to directly work on the user provided password with no sanitization

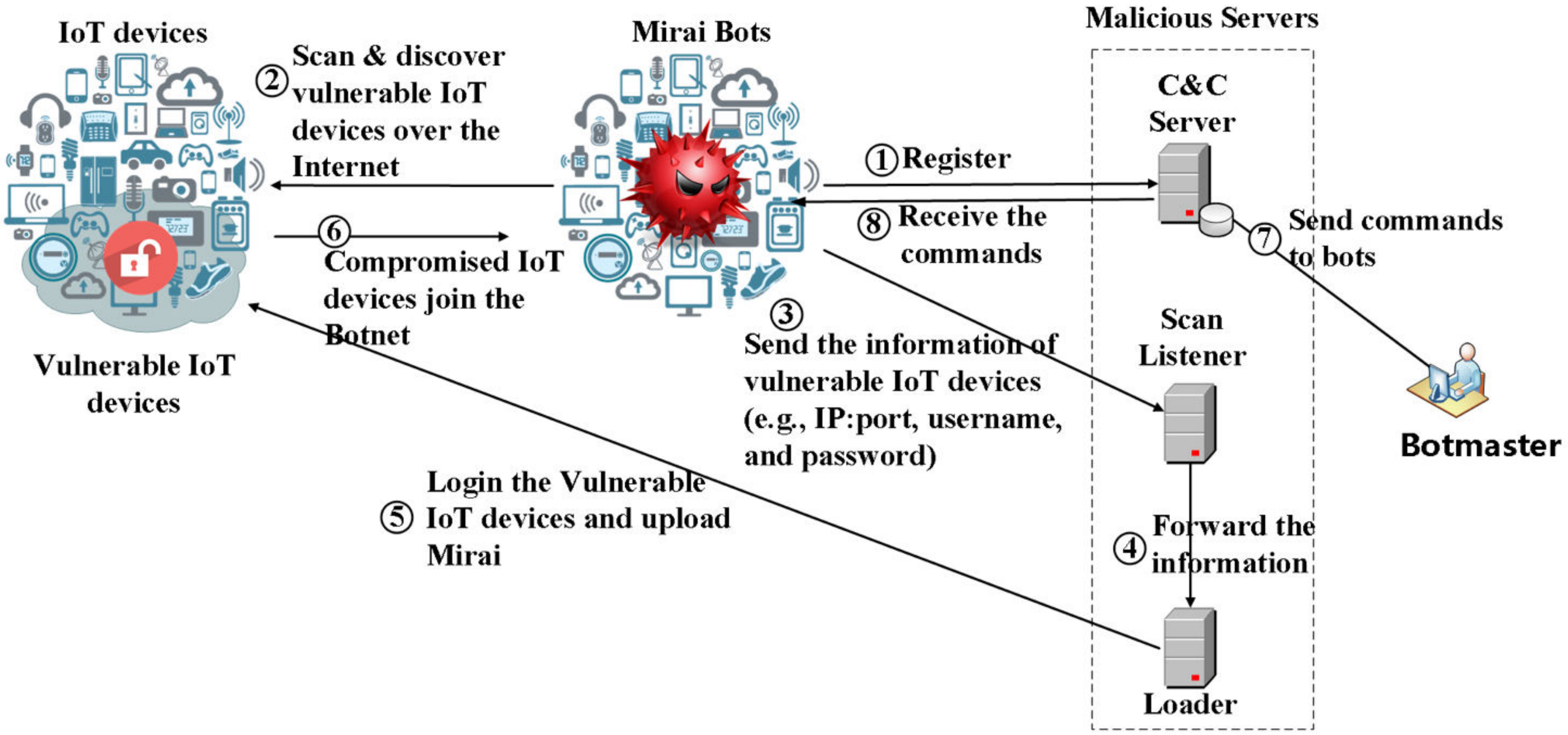


```
li      $a2, 0x420000
nop
addiu   $a2, (aEchoNSSMd5sum - 0x420000)  # "echo -n %s:%s | md5sum"
la      $t9, snprintf
nop
jalr    $t9 ; snprintf
nop
lw      $gp, 0x200+var_1E8($fp)
addiu   $v0, $fp, 0x200+var_110
addiu   $v1, $fp, 0x200+var_110
move    $a0, $v0
move    $a1, $v1
li      $a2, 0x80
la      $t9, loc_410000
nop
```

/bin/agent

Mirai Botnet over IoT

- Device spoofing attack + remote command inject attack
    - A new wave of Mirai DDoS!!!


IoT devices
② Scan & discover vulnerable IoT devices over the Internet
Mirai Bots
Malicious Servers
C&C Server
① Register
⑧ Receive the commands
⑦ Send commands to bots
⑥ Compromised IoT devices join the Botnet
Vulnerable IoT devices
③ Send the information of vulnerable IoT devices (e.g., IP:port, username, and password)
Scan Listener
Botmaster
⑤ Login the Vulnerable IoT devices and upload Mirai
④ Forward the information
Loader

References

[1] Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey, Computer Networks 54 (2010) 2787–2805

[2] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (2013) 1645–1660

[3] Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu, Xinwen Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", accepted to appear in *IEEE Internet of Things Journal* (*IoT-J*), 2017.