Securing the IoT

Fundamentals of Internet of Things

Andrea Omicini
andrea.omicini@unibo.it

Bologna Business School, Università di Bologna

Master in Digital Technology Management 2020/2021

Disclaimer

- most of the ideas here are extracted from [Hanes et al., 2017] and [Jabraeil Jamali et al., 2020]
- however, any mistake should be attributed to the author of these slides

Next in Line...

Security for IoT Systems

- on the one hand, IoT systems have all the security issues that standard distributed systems nowadays have
- on the other hand, they also have peculiarities that makes them especially vulnerable to specific threats
- this is why in the following we are going to
  - shortly recap the main elements of security for computer and network systems
  - point out IoT peculiar security issues

Next in Line...

Focus on...

Security

What is security?

- *secure* means a state of being free from care, anxiety, or fear
- an object can be in a *physical state* or a *theoretical state* of security

Physical State of Security I

- a facility is secure if it is protected by a *barrier* like a fence
- has *secure areas* both inside and outside
- can resist *penetration* by intruders
- four *protection mechanisms* are in place
  - deterrence
  - prevention
  - detection
  - response

Deterrence

- first line of defense against intruders who may try to gain access
- works by creating an atmosphere intended to frighten intruders
- may involve warnings of severe consequences if security is breached

Prevention

- the process of trying to stop intruders from gaining access to the resources of the system
- barriers include: firewalls, demilitarised zones (DMZs), and the use of access items like keys, access cards, biometrics, and others to allow only authorised users to use and access a facility

Detection

- occurs when the intruder has succeeded or is in the process of gaining access to the system
- signals from the detection process include alerts to the existence of an intruder
- sometimes these alerts can be real time or stored for further analysis by the security personnel

Response

- is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms
- works by trying to stop and/or prevent future damage or access to a facility

Theoretical State of Security

- based on *oscurity* and secrecy
- based on few trusted people
- and on ignorance by others
- e.g., Coca Cola, KFC
- does not really work in general

Objects of Security in a Computer Network

- computer security
- network security
- information security

Computer Security

- creating a secure environment for the use of computers
- focuses on the user behaviour
- four areas
  - study of *computer ethics*
  - development of both software and hardware *protocols*
  - development of *best practices*

Network Security

- the object is a computer network, not just a computer
- broader than computer science, computer security
- involves creating an *environment* in which a *network-based system*– including all many resources – is *secure*

Information Security

- involves the creation of a state in which *information* and *data* are secure
- includes computer and computer network security
- involves a variety of disciplines, including computer science, business management, information studies, and engineering

Security of a Resource

- a resource is secure, based on the above definition, if that resource is protected from both internal and external *unauthorised access*
- resources are either *tangible* or *nontangible*
- in a computer network model
  - the tangible objects are the *hardware resources* in the system
  - the intangible object is the information and data in the system, both in transition and static in storage

Hardware Security

Protecting hardware resources include protecting

- *end-user objects* that include the user interface hardware components such as all client system input components, including a keyboard, mouse, touch screen, light pens, and others
- *network objects* like firewalls, hubs, switches, routers, and gateways which are vulnerable to hackers
- network *communication channels* to prevent eavesdroppers from intercepting network communications

Software Security

Protecting software resources includes protecting

- hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property stored on network storage disks and databases
- client software such as investment portfolios, financial data, real estate records, images or pictures, and other personal files commonly stored on home and business computers communications

Focus on...

Forms of Protection

Protecting system resources and overall operation is achieved via a number of services including

- access control
- authentication
- confidentiality
- integrity
- nonrepudiation
- availability
- privacy
- trust

Access Control

A service the system uses, together with a user pre-provided identification information such as a password, to determine who uses what of its services.

- hardware access control systems—e.g., identification cards, biometric identification, video surveillance
- software access control systems—e.g., point of access (POA) monitoring, remote monitoring

Authentication

A service used to identify a user—to verify that a user is the very one he/she claims to be based on what the user is, knows, and has

- user name / password
- retinal images
- fingerprints
- physical location
- identity cards

Confidentiality

A service protecting system data and information from unauthorised disclosure

- to avoid sniffing, communication channels are *encrypted*
- encryption algorithm can either be *symmetric* – e.g., common key – or *asymmetric*—e.g., public/private key

Integrity

A service protecting data against active threats such as those that may *alter* it

- through encryption and hashing algorithms, ensures that the integrity of the transient data is intact
- a hash function takes an input message M and creates a code from it
- the code is commonly referred to as a hash or a message digest
- a one-way hash function is used to create a signature of the message
- the signature is attached to the message
- then used to check the message's integrity and authenticity

Nonrepudiation

A service that provides proof of origin and delivery of service and/or information

- through *digital signature* and encryption algorithms
- ensures that digital data may not be repudiated
- by providing proof of origin that is difficult to deny
- a *digital signature* is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender

! it is not exactly the same than nonrepudiation in legal environment

Availability

A service that is available to legitimate users

- data and equipment can be made available to authorised users and services when data and equipment are requested
- some services are requested to be available in real time, or, in a reasonable measure of time
- so, attack like DoS (*denial of service*) can be used to harm systems
- generally speaking, any serious threat to availability should be considered
- improved techniques – such as secure and efficient routing protocols – should be studied and applied to ensure availability

Privacy

A service that allows users to control their own data, both directly and indirectly

- data privacy can ensure that
  - the user only can control his/her own data
  - no other user can access or process the data
- unlike confidentiality – intended to encrypt data to prevent tampering by by unauthorised users – privacy should also ensures that no further knowledge about the user can be inferred from the data received

Trust

A service that provides some measure of the *dependability* of some component, user, or portion of the system

- trust is quite a broad and "risky" notion
  - someone claims that trust is the main threat to security
- yet, we need to trust systems just to start using them
  - so, let alone to depend on them
- *implicit* trust is always there, explicit trust services can be implemented
- trust concerns interactions between various objects, different IoT layers, different applications

What about IoT?

- everything applies to IoT systems, too
- yet, IoT has peculiarity that should be addressed specifically
- which we will mention shortly in the next slides

Next in Line...

New Security Issues

Main sources

- heterogeneity of components, connectors, and data
- heterogeneity of architectures
- large scale

Impact factors

- diversity of things
- communication of things
- number of things

Specific Sources of Security Issues: Objects

- smart objects have limitations in terms of computational capabilities, energy, power, connections, protocols
  - so, state-of-the-art security measures might be not generally applicable
- smart objects are first of all physical object, whose shape and operation (including computation and networking) is dictated by their primary function, rather than by security issues
  - so, "security first" may be not always applicable—at least not straightforwardly, without a significant re-design that may also affect the overall object usage
  - and again, state-of-the-art security measures may be not generally applicable
- e.g., we may understand that a certain sort of connection / protocol is required for the secure networking of a given object, and at the same time we may recognise that the object itself cannot even be equipped with the required antenna

Specific Sources of Security Issues: Data

- data are typically acquired in day-by-day usage situations
- providing a huge amount of information about *individuals*, *organisations*, and *processes*
  - which may help harm them deeply
- particularly because objects involved in the acquisition have typically limitations that requires them to transmit most of the data away

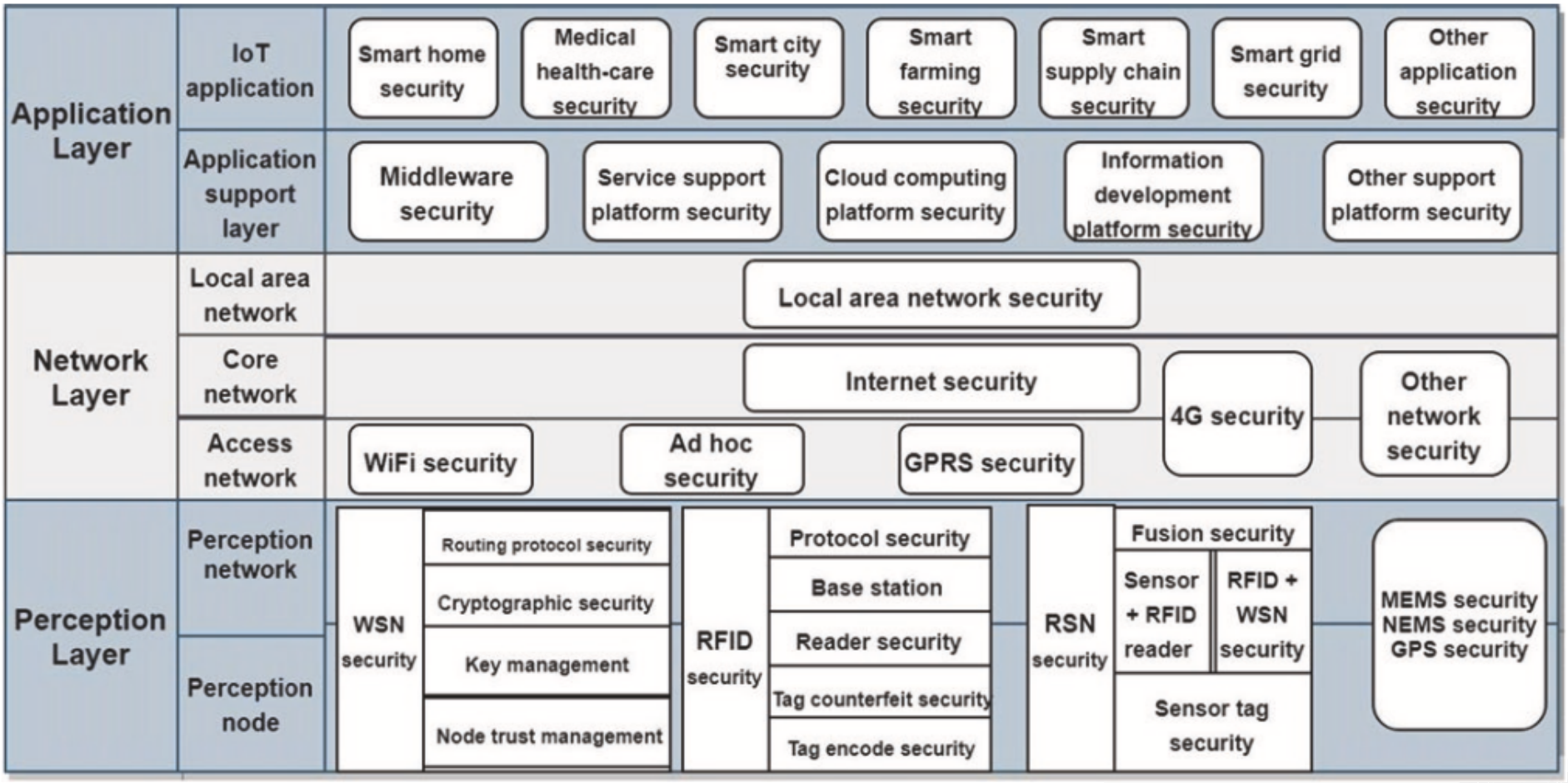
Specific Sources of Security Issues: Systems

- objects in a IoT systems are mostly *heterogenous* in origin, nature, structure, operation, capabilities, ...
  - so, general-purpose security measures may not work in practice
  - an overall model of security may not be viable, too
- security requirements could be put in place, yet specific security model for each sort of object are likely to be required
  - clashing with the problem of *scale*, however
  - given that IoT systems may be composed of huge numbers of different individual devices
- also, the piecemeal nature of most IoT systems makes it difficult to design an stable overall security strategy
  - making the need for pre-defined security requirements almost mandatory

The Architecture of Security I

- first reference: three-layer IoT architecture
- then, as expected, a more refined layering is required to point out the many different level of security concerns that have to be taken into account

The Architecture of Security II



Security architecture in the IoT [Jabraeil Jamali et al., 2020]

The Architecture of Security III

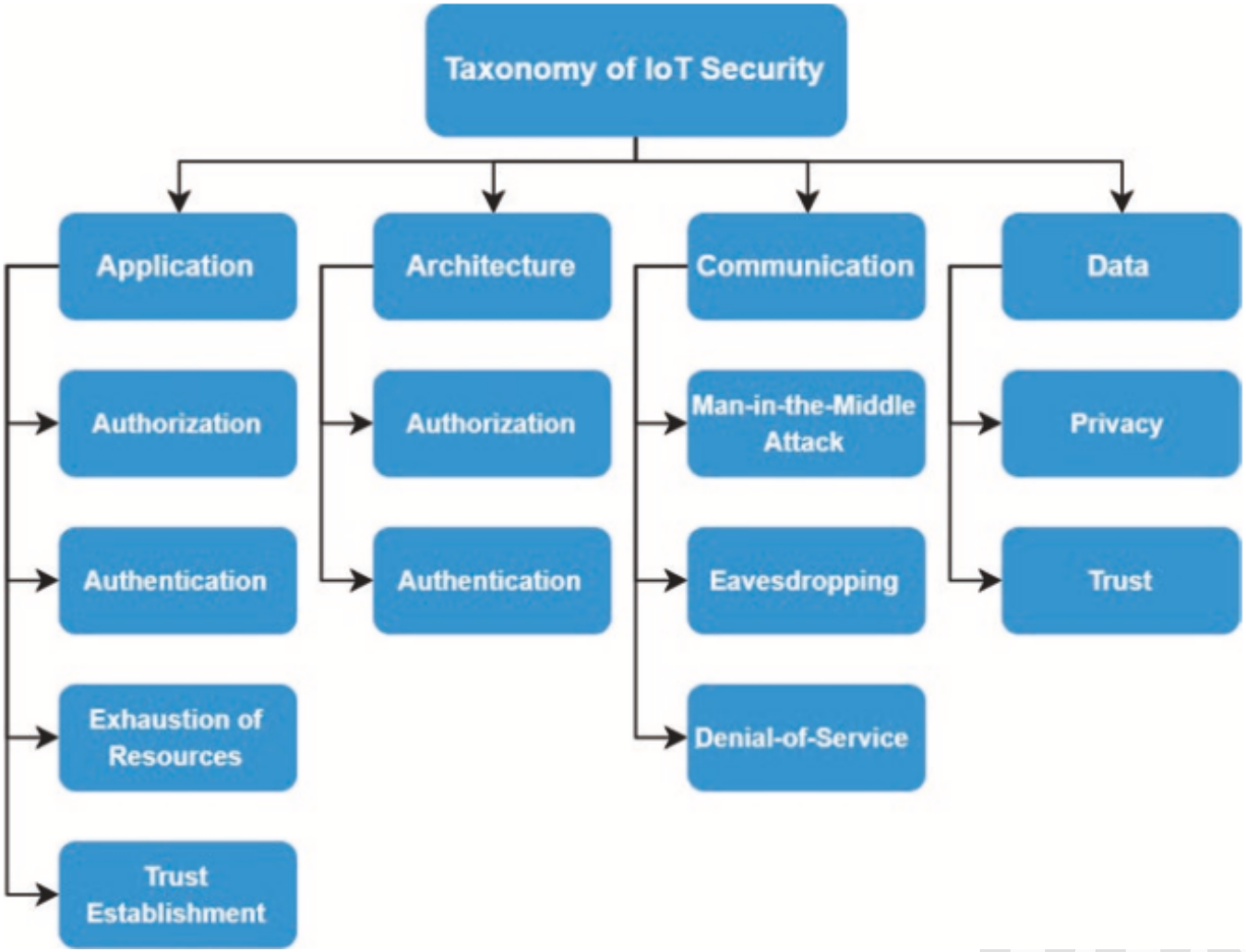
- first remark: so many levels and concerns means first of all so many potential attacks
- then, they also mean trouble for system and security engineers, as well as concerns for designers and users
- finally: is anything missing, anyway?

The Taxonomy of Security I

- the picture above is mostly unmanageable, at a first glance
- is there any possibly more tractable view of the security issues of the IoT that could be used?
- a new classification
  - application domain
  - architecture domain
  - communication channel
  - data domain

  for a taxonomy

The Taxonomy of Security II



Security taxonomy in the IoT [Jabraeil Jamali et al., 2020]

Security Challenges & Issues

- *physical security* — including sensor security, sensor interference, and signal towards the sensor
- *safe operation* — that is, ensuring that elements (such as sensor operation, transmission systems, and treatment systems) can operate safely
- *information security* — so that data within sensor, transmission system, and processing devices cannot be stolen or tampered

Perception Layer Challenges I

Three main security problems in the IoT perception layer—the physical one

- strength of wireless signals
  - signals are mostly transmitted between IoT sensor nodes using wireless technologies, whose efficiency can be impaired by disturbing waves
- physical security of sensors
  - which are typically external, and possibly accessible by attackers
- mobility of sensors
  - limited storage capacity, power consumption, and computing capabilities—making them vulnerable to threats and attacks

Perception Layer Challenges II

Unauthorised access to tags

- due to the lack of a proper authentication mechanism in a wide range of RFID systems, tags can be accessed without authorisation by a person
- the attacker can not just simply stole the data, but even change or delete records

Node capture attacks

- the opponent can capture and manage the node or tool by physically replacing the whole node or by tampering with the node or device hardware
- this attack can also be referred to as a *node response attack*

Perception Layer Challenges III

Tag cloning

- since tags are displayed on various objects and their information can be checked and changed using a few hacking techniques, they can easily be captured by any cybercriminal
- who can reproduce the tag and subsequently tamper it in a way that the reader cannot distinguish between the original and the compromised one

False data injection attacks

- with the node or device captured, the opponent can inject fake facts near regular facts measured by the node or tool captured and transmit the fake facts to IoT applications
- after receiving the fake information, IoT applications can behave wrongly, and possibly go undetected

Network Layer Challenges I

- since the primary purpose of the IoT network layer is to transmit gathered data, the security challenges in this layer focus on the impact of network resources availability
- when the network layer consists of the WSN, security problems concern transmission of data from sensors

Spoofing attack

- *spoofing* is the act of disguising a communication from an unknown source as being from a known, trusted source
- the reason for spoofing attacks is that the opponent gets the right to enter the IoT system and can send malicious records to the system
- e.g.
  - IP spoofing
  - RFID spoofing

Network Layer Challenges II

Sinkhole attack

- the attacker makes the compromised node look attractive to the nearby nodes
- all data drift from any particular node to the compromised node
- all traffic is silenced

Sleep deprivation attack

- sensor nodes within WSN are powered by batteries with a given lifetime, and corresponding routine
- sleep deprivation keeps the nodes wakeful, leading to extra battery intake and reduces the battery life as a result
- in the end, causing the nodes to close down

Network Layer Challenges III

Denial-of-Service (DoS) attack

- the attacker flood the network with extra-amount of traffic, resulting in resource depletion of the targeted system,
- when the amount is huge enough, the network is made unavailable to the users

Application Layer Challenges I

Phishing attack

- in a phishing attack, the opponent can retrieve personal information of users, such as identity and passwords, by spoofing the user's authentication credentials via infected emails and phishing websites

Malicious virus/worm

- a malicious virus/worm a self-propagating software that infects the IoT application
- typically aimed at damaging/blocking a system behaviour, or, stealing data for users

Application Layer Challenges II

Sniffing attack

- an attacker can force a machine attack by introducing a sniffer tool into the device that can benefit network facts that lead to system corruption

Malicious scripts

- malicious scripts can be installed by users inadvertently and then used to install malware and to damage the behaviour of IoT components

Reverse social engineering attack

- a person-to-person attack in which an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem

Defending IoT Systems I

Intrusion Detection Systems (IDS)

- how do we deal with all of that?
- *intrusion detection* is a process for monitoring and inspecting events in a computer network system for signs of potential threats
- an IDS is a device or software application to detect intrusions

Defending IoT Systems II

Four main sort of IDS

anomaly-based — normal behaviour is profiled, anomalies are detected via statistical analysis or machine learning techniques

signature-based — known threats are classified and their signature network behaviour is detected and matched against suspect system behaviour

specification-based — expected behaviour defined by set of rules and thresholds – usually expert-defined – for nodes, components, routing tables, ...

hybrid — signature- plus anomaly-based—for both known and unknown attacks

Next in Line...

Smart Home I

- *smart home* aims at adding intelligence and communicate with the existing home infrastructures made of everyday home objects such as appliances, door locks, cameras, furniture, and garage doors
- the addition of data-driven intelligence to physical objects offers many advantages for a better human life, including greater convenience, security, and resource efficiency
- for example, smart home can adjust the blinds to save energy based on environmental changes, open the garage door automatically when an authorised vehicle approaches, or order medical services automatically when emergencies are detected

Smart Home II

Security issues

- *actuators* (intelligent locks, microwaves, heaters) can actually harm physically people at home if hacked
- *sensors* (and data collectors) can actually disclose sensitive personal informations about the inhabitants of a IoT-enabled building
- privacy being the most natural target for attacks

Smart Connected Health I

- by integrating intelligent medical devices into the existing medical infrastructure, healthcare professionals can more effectively monitor patients and use the data collected from these devices to determine who needs the greatest care
- IoT infrastructure allows health professionals to develop a proactive real-time management system based on the data collected, promoting prevention as well as early intervention
- availability of body sensors makes it possible to constantly monitor people's health
- also, behavioural changes can be detected on the spot in patients with diseases and during treatments

Smart Connected Health II

Security issues

- life-threatening attacks can be conceived and performed both through actuators (body implants) or indirectly by tampering with information and signalling
- here, too, however, privacy looks like the most natural target for attacks

Smart Energy Grid I

- the limits of traditional energy grid systems have been overcome by IoT-enhanced *smart grids*
- improving reliability, reducing costs, and optimising performance
- greener and renewable energy such as wind, geothermal, and solar energy can be more easily and effectively integrated
- there, intelligent grid data communication networks connecting many smart grid devices play a key role, by
  - collecting energy consumption data
  - monitoring the state of the intelligent grid system

  it can improve distribution and load balancing based on the collected energy usage information
- also, it also helps to design a fair but scaled price model by taking into account unbalanced space and time consumption

Smart Energy Grid II

Security issues

- smart grid intrusion and the cutting of electricity supplies to a wide area can cause enormous physical and economic damage to society
- analysing data on power user can also reveal the private day-by-day activities of people
- in addition, attacks on data integrity and false data injection can disturb the smart grid billing system and disrupt grid estimation, torture the power flow, and delay the demand response

Next in Line...

Overall

- standard security issues appìly to IoT systems
- also, specific issues emerge, due to the IoT specificity
- and even more specific in the context of IoT application scenarios

Securing the IoT

Fundamentals of Internet of Things

Andrea Omicini
andrea.omicini@unibo.it

Bologna Business School, Università di Bologna

Master in Digital Technology Management 2020/2021

References

[Hanes et al., 2017] Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., and Henry, J. (2017).

IoT Fundamentals. Networking Technologies, Protocols, and Use Cases for the Internet of Things.

Cisco Press.

[Jabraeil Jamali et al., 2020] Jabraeil Jamali, M. A., Bahrami, B., Heidari, A., Allahverdizadeh, P., and Norouzi, F. (2020).

Towards the Internet of Things. Architectures, Security, and Applications.

EAI/Springer Innovations in Communication and Computing (EAISICC). Springer International Publishing.