


MANCHESTER
1824

The University
of Manchester



COMP32412: Internet of Things Architecture and Applications

Security requirements and challenges in IoT

Ahmed Saeed

ahmed.saeed@manchester.ac.uk
KB 2.80, 2nd Floor, Kilburn Building

COMP32412

1

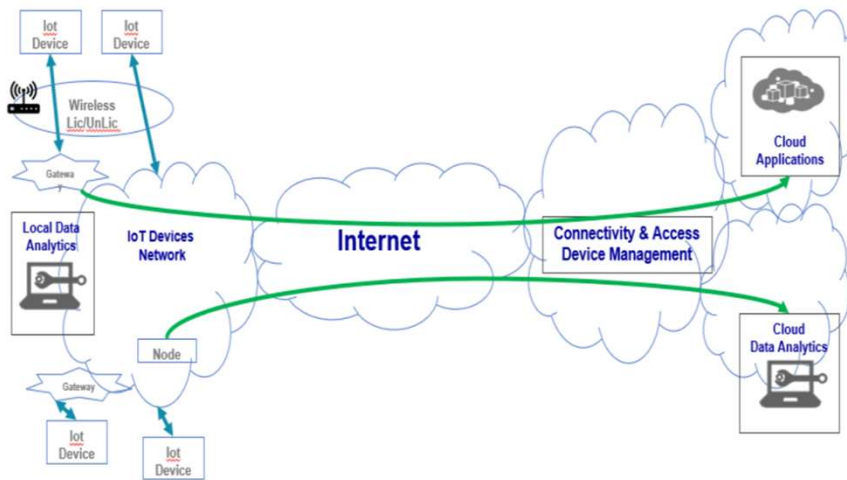
Lectures from this week onwards will be focused on understanding and identifying the security threats at all levels of the IoT and respective security techniques used to mitigate these threats

Overview & Learning Outcomes

- Understand security and privacy challenges in IoT
- Describe and Identify security requirement in IoT
- Describe and identify security attacks at the sensing layer of IoT architecture



Overview of IoT Architecture



COMP32412

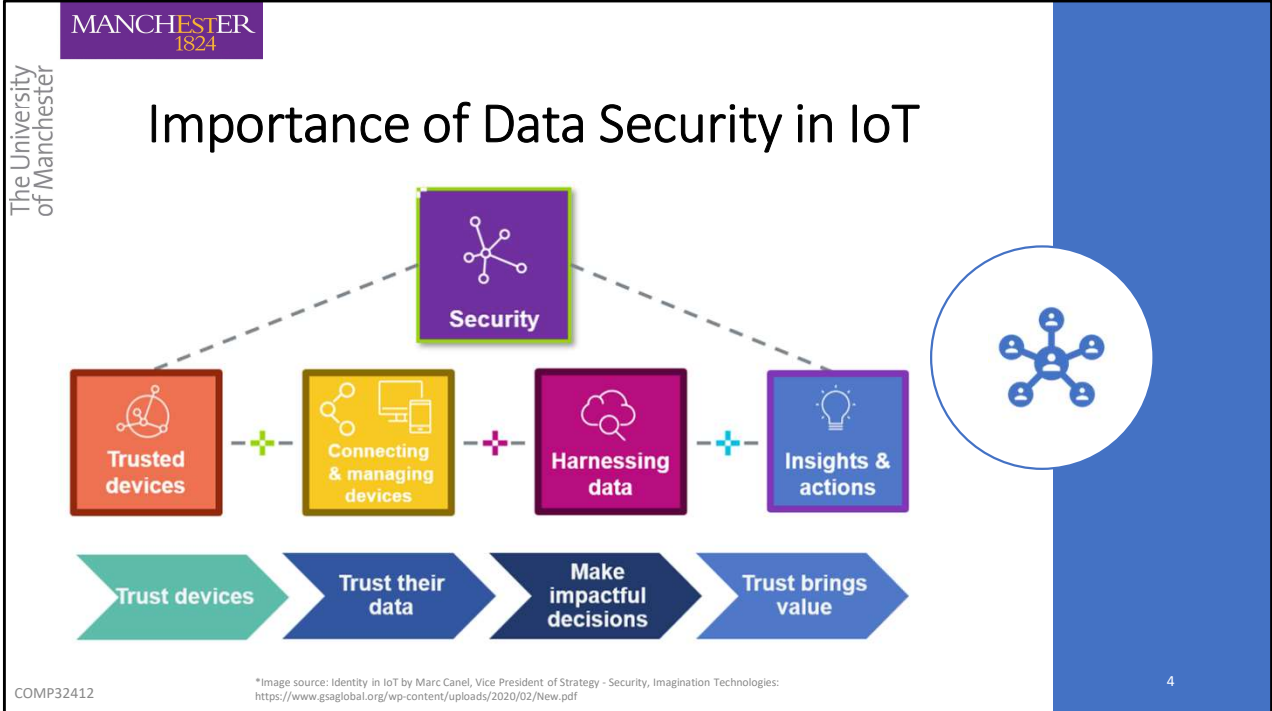
*Image source: Identity in IoT by Marc Canel, Vice President of Strategy - Security, Imagination Technologies:
<https://www.gsaglobal.org/wp-content/uploads/2020/02/New.pdf>

3

The world of the Internet of Things (IoT) is characterized by a very large number of devices extracting data from their operational environment and reporting information to analytics systems in their network or in the cloud.

Source:

Identity in IoT by Marc Canel, Vice President of Strategy - Security, Imagination Technologies: <https://www.gsaglobal.org/wp-content/uploads/2020/02/New.pdf>



The data plays a key role and it is very crucial that the data is trusted as it is. The decisions are made based upon this data which will impact the safety of the system and its users. If the data cannot be relied upon, it is not worth much.

Expensive and complex systems making decisions on safety or operations need to trust the data that they process.

Effective reliance on the data from the IoT devices is built upon a security architecture that will start with the devices. Trusted devices enable trusted data.

Source:

Identity in IoT by Marc Canel, Vice President of Strategy - Security, Imagination Technologies:
<https://www.gsaglobal.org/wp-content/uploads/2020/02/New.pdf>

Security Requirements of IoT



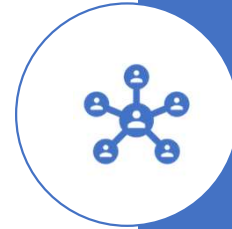
CONFIDENTIALITY



INTEGRITY



AVAILABILITY



AUTHENTICITY



PRIVACY



TRUST

Following are the key security requirements to ensure that the IoT users can trust the system and its data

Security requirements of IoT

- **Confidentiality** ensures that the system data is only available to the authorised users and no other user can read the data.
- **Integrity** ensures that the system data can not be modified through illegal means and that the authorized users receive accurate data.
- **Availability** ensures that the system devices and the data is always available to its valid users whenever required.



Confidentiality is an important security feature of an IoT system which ensures that the information generated within the system is only available to its approved users. This information should not be accessed by unauthorized users. This is a key security challenge in an IoT system as it is very important to ensure that the system data should be protected all the time from any illegal read requests. For instance, the data captured by a sensor device should be transmitted securely to the base station.

Integrity is another important security feature of an IoT system guaranteeing that the system data can not be tampered during transmission. It is the process of ensuring and preserving the validity and accuracy of data to its end users. The IoT applications should not receive erroneous or corrupted data as this could malfunction the system. To achieve data confidentiality and integrity, one solution is to use encryption all the time while transmitting the data.

Availability can ensure that the system devices and the data are available to its valid users and services whenever the data and devices are requested. As the IoT applications can request services at any time so it is very crucial to make the system available. This can not be achieved if the system resources are compromised either due to faults and failures or security attacks. Denial-of-service (DoS) attacks are one of the most common threats that can disrupt the systems services. To handle these threats, enhanced techniques (secure and efficient routing

protocols, device behaviour monitoring etc.) can be deployed within the system to ensure availability.

Source:

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.

Security requirements of IoT

- **Identification and Authentication** ensures that only valid and authorised devices can connect to the system and gain access to data and resources.
- **Privacy** ensures that the data can only be controlled by its corresponding user only and no other user can access or process the data
- **Trust** ensures that the aforementioned security and privacy objectives are achieved such as among different layers of an IoT system architecture.



Identification and Authentication is a two-step security feature where in the first step Identification ensures that only genuine and valid devices or applications can gain access to the IoT system whereas in the second step, authentication ensures that the devices or applications that request the data are legitimate as well. In IoT, identifying and authenticating each data and object is difficult, because a large number of diverse objects can comprise an IoT. Thus, designing efficient mechanisms to deal with the authentication of objects or things is critical in IoT.

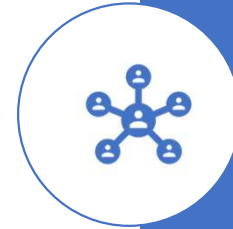
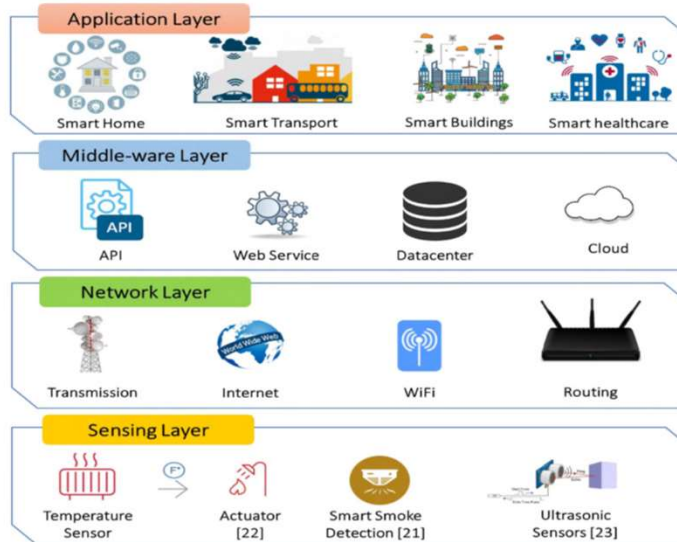
Privacy: Privacy can ensure that the data can only be controlled by the corresponding user, and that no other user can access or process the data. Unlike confidentiality, which aims to encrypt the data without being eavesdropped and interfered by nonauthorized users, privacy ensures that the user can only have some specific controls based on received data and cannot infer other valuable information from the received data.

Trust can ensure the aforementioned security and privacy objectives to be achieved during the interactions among different objects, different IoT layers, and different applications. The objectives of trust in IoT can be divided as trust between each IoT layer, trust between devices, and trust between devices and applications.

Source:

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.

Four-layer model of IoT architecture



COMP32412

*Image source: Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

8

- The architecture of an IoT system can be described using service-oriented architectures (SoAs). In an SoA-based IoT architecture, four layers exist and interact with each other as shown in this figure.
- Sensing layer sometimes referred as Perception Layer, Middle-ware layer is also known as Service Layer and Application Layer is also called Interface Layer.
- SoA is a component-based model, which can be designed to connect different functional units (also known as services) of an application via interfaces and protocols.
- The perception layer is performed as the bottom layer of the architecture, and used to measure, collect, and extract the data associated with physical devices.
- The network layer is used to receive the processed information provided by sensing layer and determine the routes to transmit the data and information to the IoT hub, devices, and applications via integrated networks.
- The network layer is the most important layer in IoT architecture, because various devices (hub, switching, gateway, cloud computing perform, etc.), and various communication

technologies (Bluetooth, Wi-Fi, long-term evolution, etc.) are integrated in this layer.

- The service layer is located between network layer and application layer, providing services to support the application layer. This layer is used to manage and determine the mechanisms to meet service requests from the application layer, and service interfaces are used to support interactions among all provided services.
- Middle-ware can also provide powerful computing and storage capabilities. This layer provides APIs to fulfil demands of the application layer.
- The application layer is used to support the service requests by users. The application layer can support a number of applications, including smart grid, smart transportation, smart cities, etc.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

- The sensing layer mainly deals with physical devices such as IoT sensors and actuators.
- The main purpose of this layer is to measure, collect, and extract the data associated with such devices.
- Security attacks can exploit vulnerabilities in this layer by
 - Tampering with collected data
 - Destroying sensing devices



COMP32412

*Image source: Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

9

Vulnerabilities and security attacks at Sensing/Perception Layer

Some of the main security attacks that can be encountered at this layers are

- Node capture attacks
- Malicious code injection attacks
- False data injection attacks
- Side channel attacks
- Eavesdropping and interference
- Sleep deprivation attacks



Vulnerabilities and security attacks at Sensing/Perception Layer

Node Capture attacks

- The attacker can capture and control the node or device in IoT by
 - Physically replacing the entire node
 - Tampering with the hardware of the node or device
- The new node may appear to be the part of the system but is controlled by the attacker.
- This may lead to compromising the security of the complete IoT application



COMP32412

11

- The term node refers to a physical IoT device such as sensors and actuators. If a node is compromised by the node capture attack, the important information (group communication key, radio key, matching key, etc.) can be exposed to the adversary.
- The attacker can also copy the important information associated with the captured node to a malicious node, and then fake the malicious node as an authorized node to connect to the IoT network or system.
- These kind of attacks are also known as the node replication attacks. To defend against the node capture attack, effective solutions (such as implementing identification and authentication protocols etc.) are required to monitor and detect malicious nodes.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

Malicious code injection attacks

- In addition to node capture attack, some malicious code can be injected into the memory of the compromised node or device
- The adversary can gain full access to the system and compromise integrity of entire IoT system.
- To defend against the malicious code injection attack, effective code authentication schemes need to be designed and integrated into IoT



- The adversary can use the node capture attacks to compromise a IoT device/node and then can control it by injecting malicious code into the memory of the node or device
- The firmware or software of IoT nodes are updated through remote access normally which gives a gateway to the attackers to inject malicious code
- The injected malicious code not only can perform specific functions, but can also grant the adversary access into the IoT system, and even gain the full control of the IoT system.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

False data injection attacks

- Once an IoT node or device is compromised, the attacker can inject false (sensor) data in place of normal data and transmit the false data to IoT applications
- Based on fabricated received data the IoT system can send incorrect signals to actuator devices or provide inaccurate information to its users
- To defend against such a malicious attack, techniques can be designed to efficiently detect and drop the false data before the data is received by the IoT applications



COMP32412

13

- Using such false data injection attacks, the attackers may force the nodes to send fabricated data and try to degrade the intended functionality of the IoT system and its performance
- After receiving the false data, IoT applications can return erroneous feedback commands or provide wrong services, which further affects the effectiveness of IoT applications and networks. This may lead to false results and may result in malfunctioning of the IoT application.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

Side channel attacks

- Side channel attacks require physical access to the sensing devices and can be based on monitoring and analysing its various physical parameters
- The attackers use the prior knowledge of microarchitectures of sensing devices.
- Power consumption and timing information can be used to disclose sensitive information (such as encryption key)
- To mitigate the side channel attack, efficient and secure encryption algorithms and key management schemes need to be developed in IoT



COMP32412

14

- For such side channel attacks the physical parameters of a IoT device could be its power consumption, timing information or electromagnetic emissions.
- One of the typical side channel attacks is the timing attack, in which the adversary can obtain the encryption key by analysing the time information required to execute the encryption algorithm.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

Eavesdropping and Interference attacks

- IoT applications often consist of various nodes deployed in open environments. As a result, such IoT applications are exposed to eavesdroppers.
- Once a IoT node or device is compromised, the attackers may eavesdrop and capture the data during different phases such as at the time of data transmission or authentication.
- To deal with eavesdropping, secure encryption algorithms, key management schemes and noise data adders can be implemented.



Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Sensing/Perception Layer

Sleep deprivation attacks

- In such type of attacks the attackers try to drain the battery of the low-powered IoT devices by keeping them awake unnecessarily.
- These attacks target IoT devices that are more vulnerable due to limited resources (low computational power and memory).
- To mitigate sleep deprivation attacks, techniques like secured duty-cycle mechanism can be used.



COMP32412

16

- In IoT, most devices or nodes have low power ability. To extend the life cycle of the devices and nodes, devices or nodes are programmed to follow a sleep routine to reduce the power consumption
- The sleep deprivation attack can break the programmed sleep routines and keep device or nodes awake all the time until they are shut down. This could lead to a denial of service from the nodes in the IoT application due to a dead battery. This can be done by running infinite loops in the IoT nodes/devices using malicious code and increasing the power consumption of the such devices.

Source:

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Summary

- The Internet of Things (IoT) is growing at fast rate and is becoming integral part of our lives.
- It is very crucial to protect IoT data to provide secure and trusted services to its users
- Confidentiality, integrity, availability, privacy, authenticity and trust are the key requirements of an IoT system
- The IoT architecture can be modelled using four (sensing, network, middle-ware and application) interconnected layers
- The IoT data is vulnerable to various types of attacks due to limited resources and weak protection schemes associated with IoT devices deployed at the sensing/perception layer of IoT architecture

