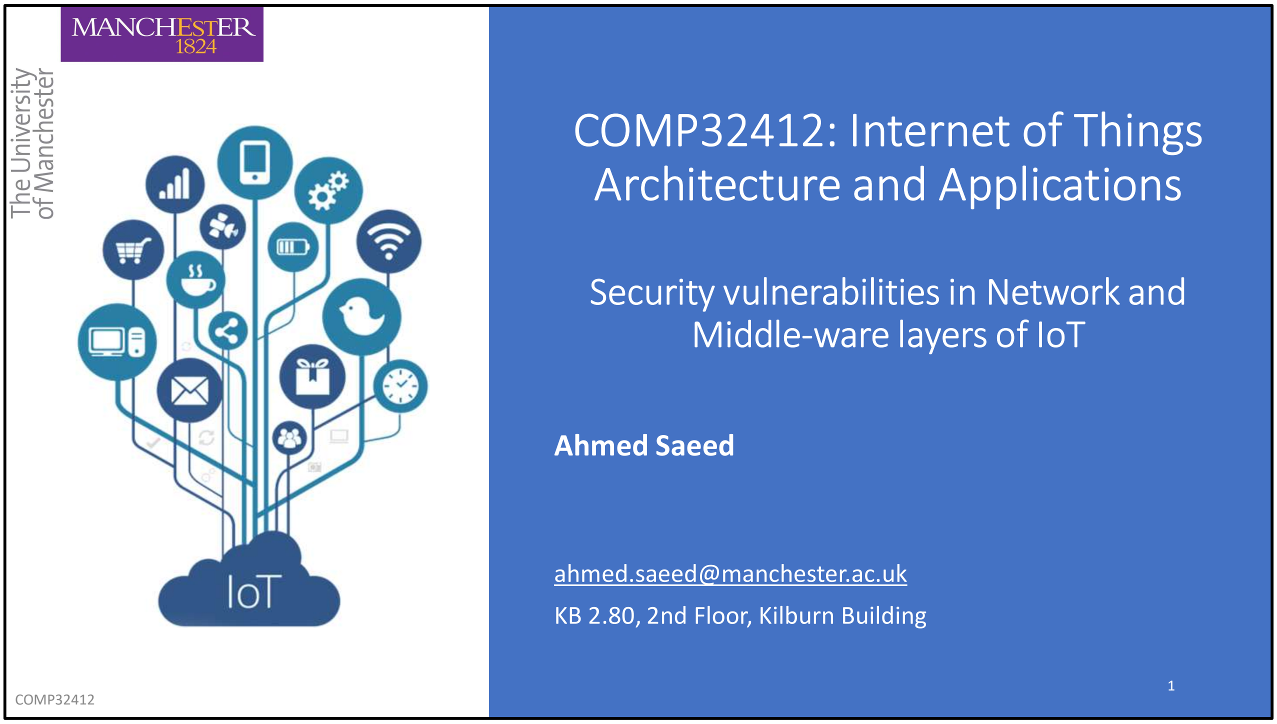


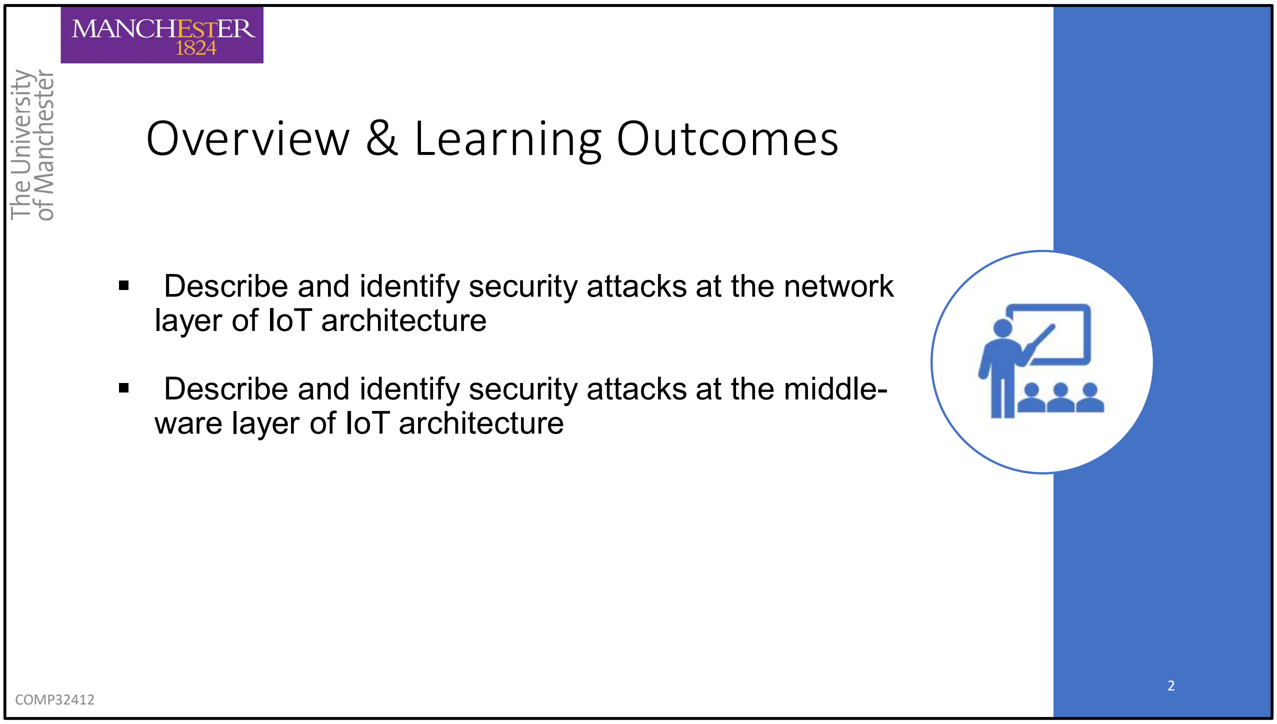
COMP32412: Internet of Things Architecture and Applications

Security vulnerabilities in Network and Middle-ware layers of IoT

Ahmed Saeed

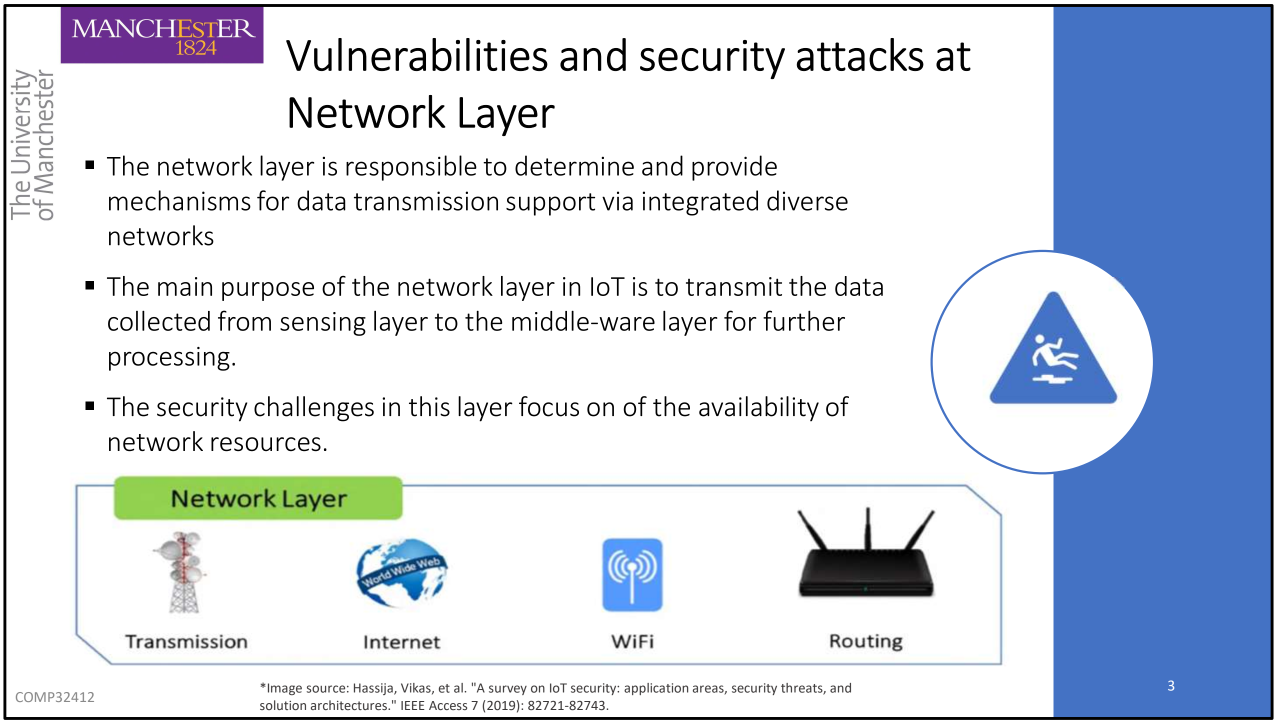
ahmed.saeed@manchester.ac.uk

KB 2.80, 2nd Floor, Kilburn Building



Overview & Learning Outcomes

- Describe and identify security attacks at the network layer of IoT architecture
- Describe and identify security attacks at the middle-ware layer of IoT architecture



MANCHESTER
1824
The University of Manchester

Vulnerabilities and security attacks at Network Layer

- The network layer is responsible to determine and provide mechanisms for data transmission support via integrated diverse networks
- The main purpose of the network layer in IoT is to transmit the data collected from sensing layer to the middle-ware layer for further processing.
- The security challenges in this layer focus on of the availability of network resources.

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.

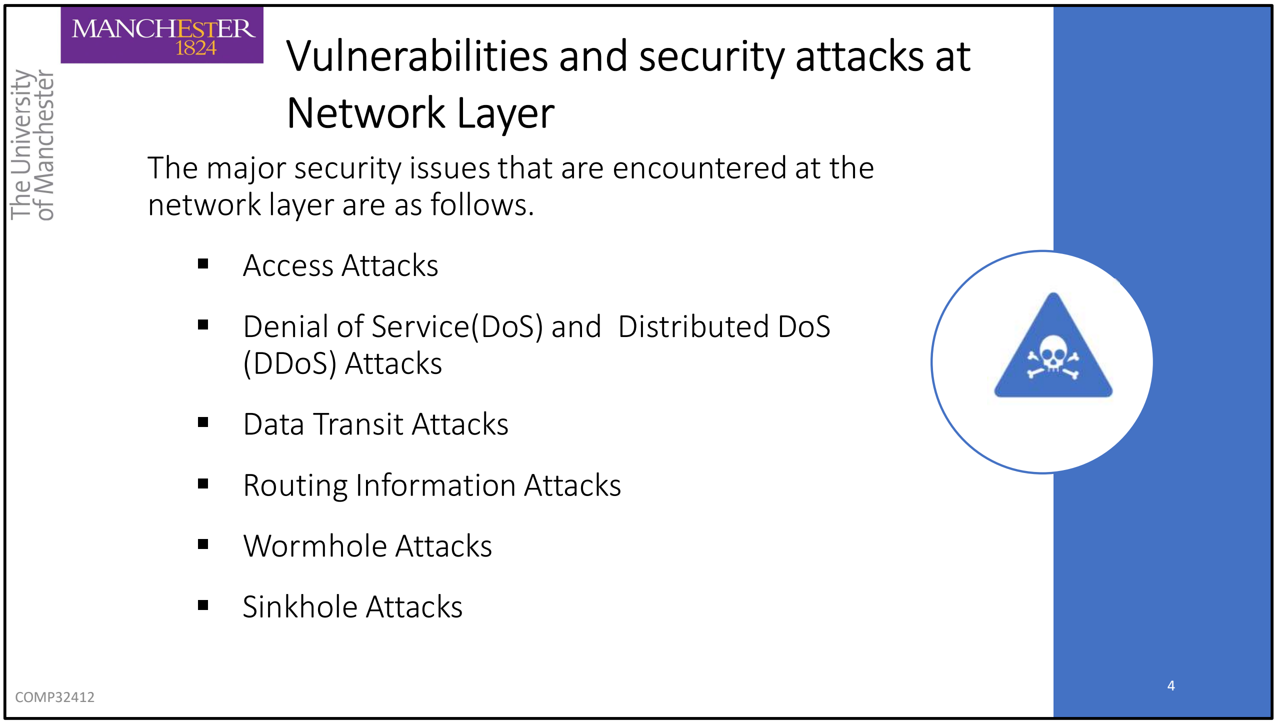
3

- Most devices in IoT are connected to IoT networks via wireless communication links. Thus, most security challenges in this layer are related to wireless networks in IoT.

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.



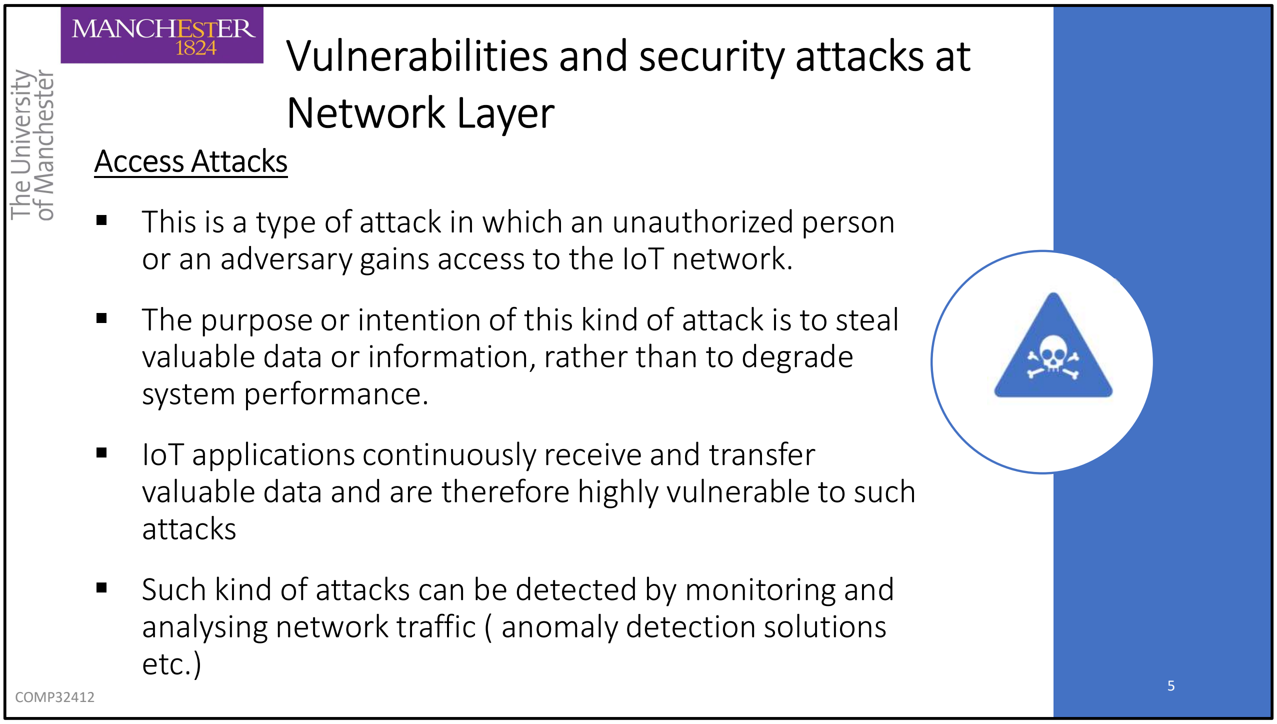
MANCHESTER
1824

The University of Manchester

Vulnerabilities and security attacks at Network Layer

The major security issues that are encountered at the network layer are as follows.

- Access Attacks
- Denial of Service(DoS) and Distributed DoS (DDoS) Attacks
- Data Transit Attacks
- Routing Information Attacks
- Wormhole Attacks
- Sinkhole Attacks



MANCHESTER 1824

The University of Manchester

Vulnerabilities and security attacks at Network Layer

Access Attacks

- This is a type of attack in which an unauthorized person or an adversary gains access to the IoT network.
- The purpose or intention of this kind of attack is to steal valuable data or information, rather than to degrade system performance.
- IoT applications continuously receive and transfer valuable data and are therefore highly vulnerable to such attacks
- Such kind of attacks can be detected by monitoring and analysing network traffic (anomaly detection solutions etc.)

COMP32412

5

- Access attack is also referred to as advanced persistent threat (APT). The attacker can continue to stay in the network undetected for a long duration.

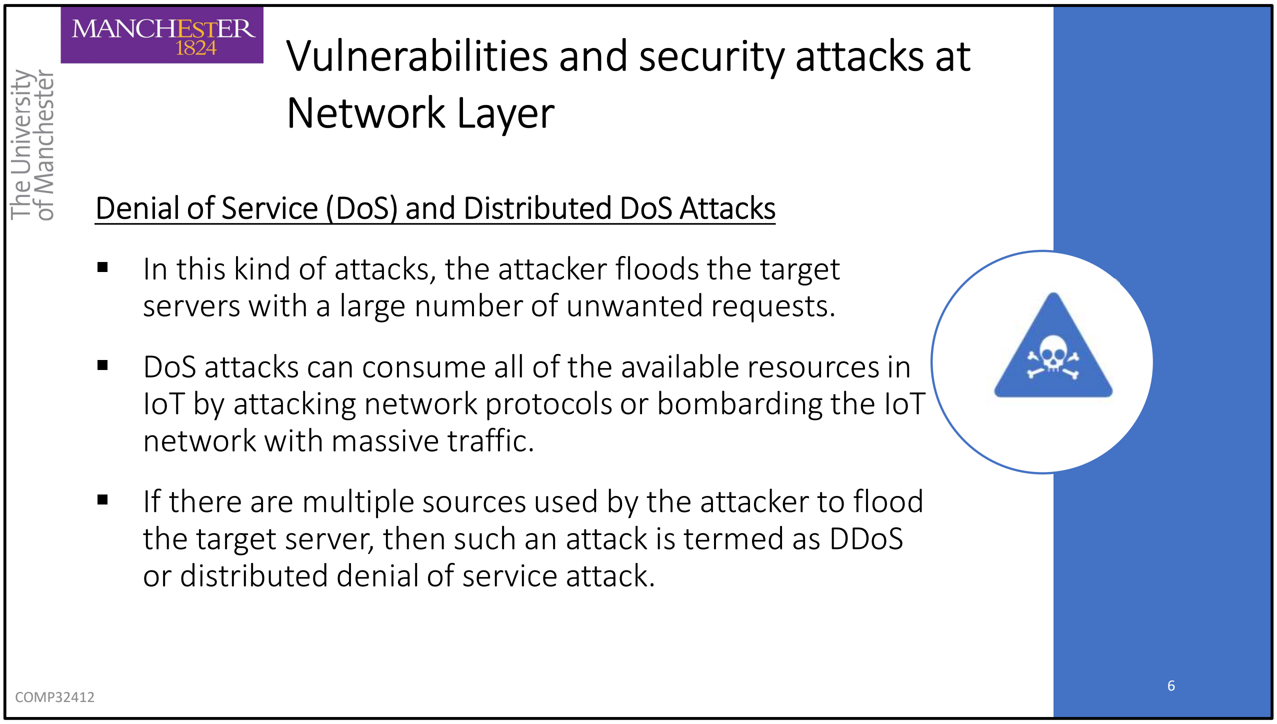
- Advanced persistent threats are also distinguished by their focus on establishing multiple points of compromise. APTs usually attempt to establish multiple points of entry to the targeted networks, which enables them to retain access even if the malicious activity is discovered and incident response is triggered.

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.

- https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT



Vulnerabilities and security attacks at Network Layer

Denial of Service (DoS) and Distributed DoS Attacks

- In this kind of attacks, the attacker floods the target servers with a large number of unwanted requests.
- DoS attacks can consume all of the available resources in IoT by attacking network protocols or bombarding the IoT network with massive traffic.
- If there are multiple sources used by the attacker to flood the target server, then such an attack is termed as DDoS or distributed denial of service attack.

COMP32412 6

- These kind of attacks incapacitates the target server, thereby disrupting services to genuine users. Such attacks are not specific to IoT applications, but due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks.

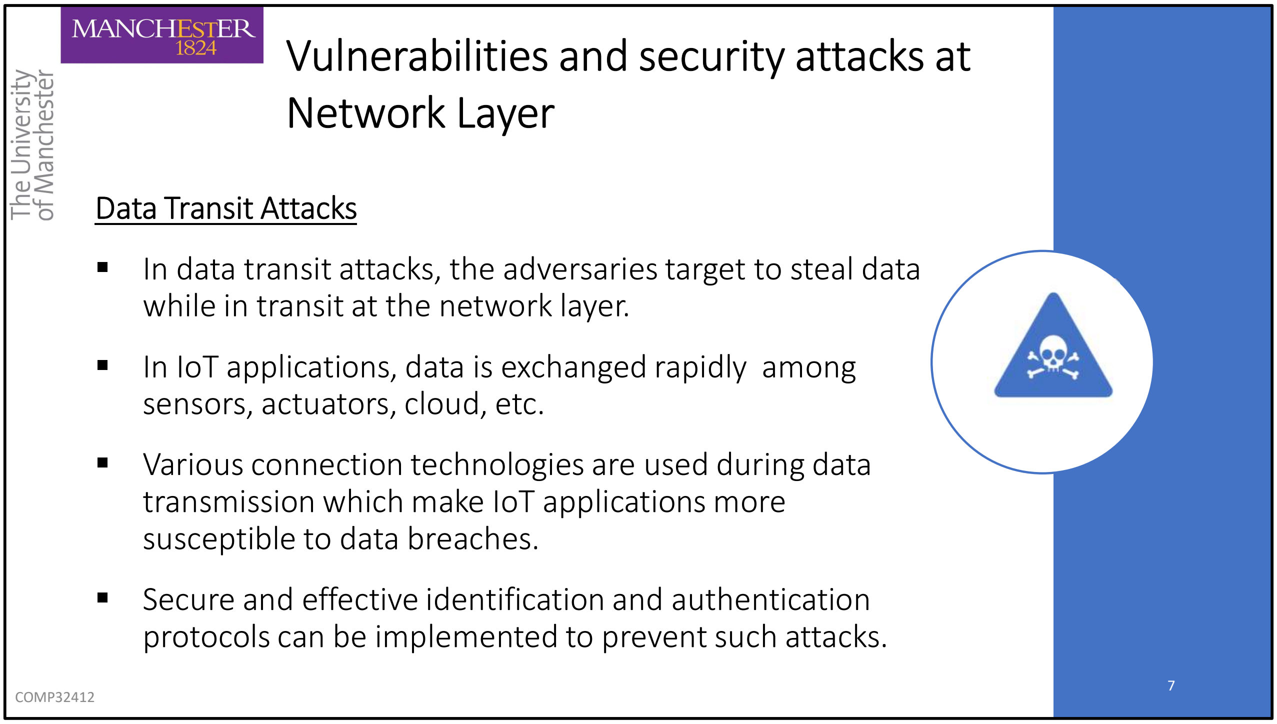
- The Mirai botnet is an infamous DDoS attack that exploits vulnerable IoT devices within a network and can block critical services by constantly propagating requests to such weak devices.

- To defend against DoS/DDoS attacks, attacking schemes need to be carefully investigated first, and then the efficient defensive schemes to mitigate attacks need be developed to secure IoT systems

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 Network Layer

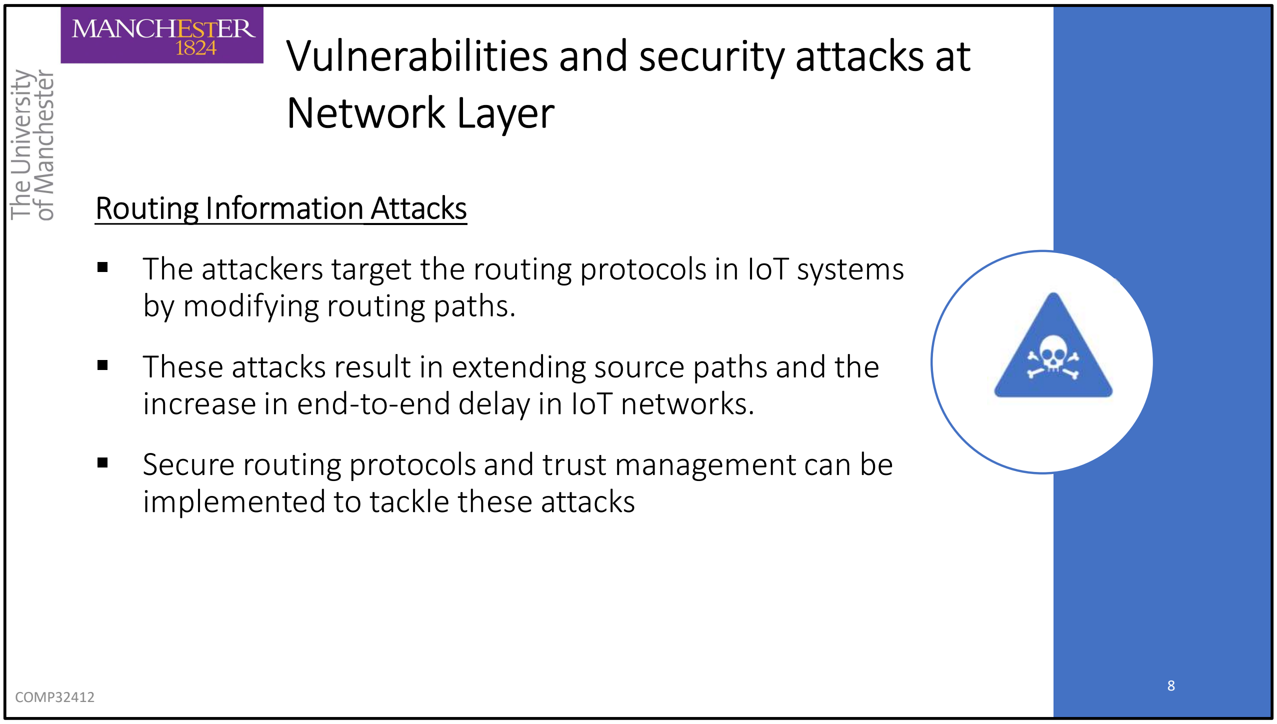
Data Transit Attacks

- In data transit attacks, the adversaries target to steal data while in transit at the network layer.
- In IoT applications, data is exchanged rapidly among sensors, actuators, cloud, etc.
- Various connection technologies are used during data transmission which make IoT applications more susceptible to data breaches.
- Secure and effective identification and authentication protocols can be implemented to prevent such attacks.

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.



MANCHESTER 1824

The University of Manchester

Vulnerabilities and security attacks at Network Layer

Routing Information Attacks

- The attackers target the routing protocols in IoT systems by modifying routing paths.
- These attacks result in extending source paths and the increase in end-to-end delay in IoT networks.
- Secure routing protocols and trust management can be implemented to tackle these attacks

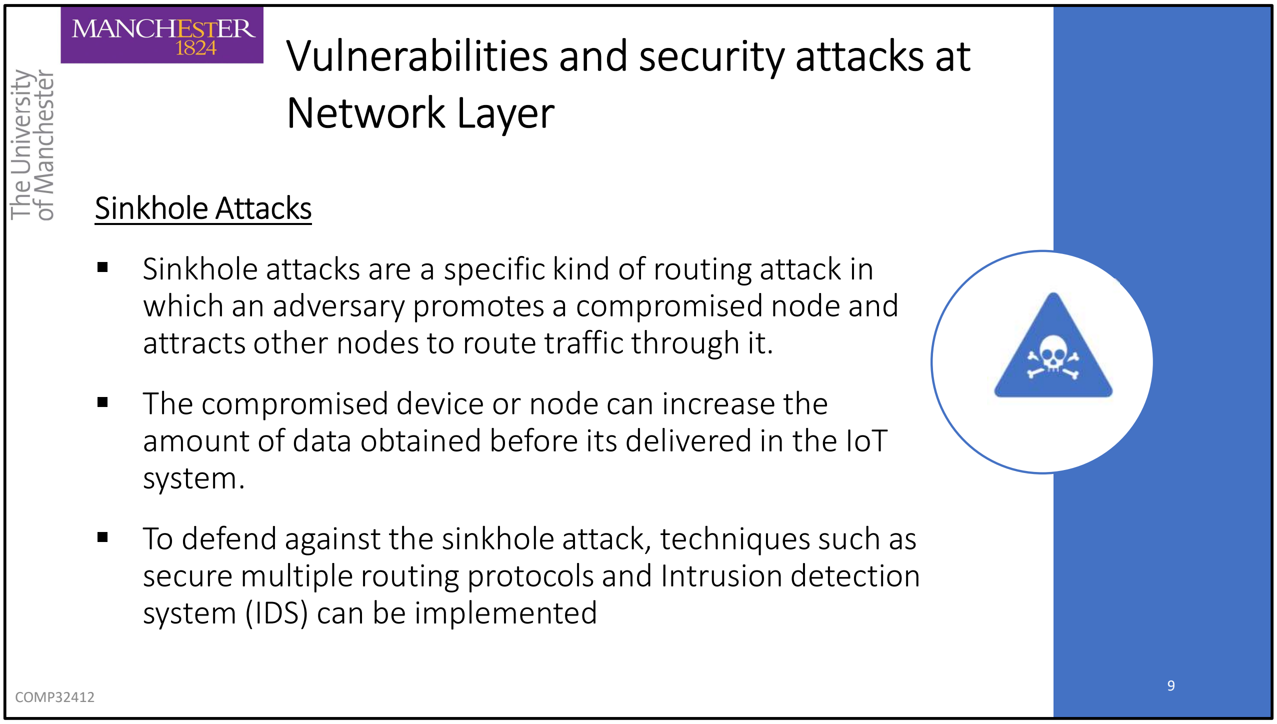
COMP32412

8

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.



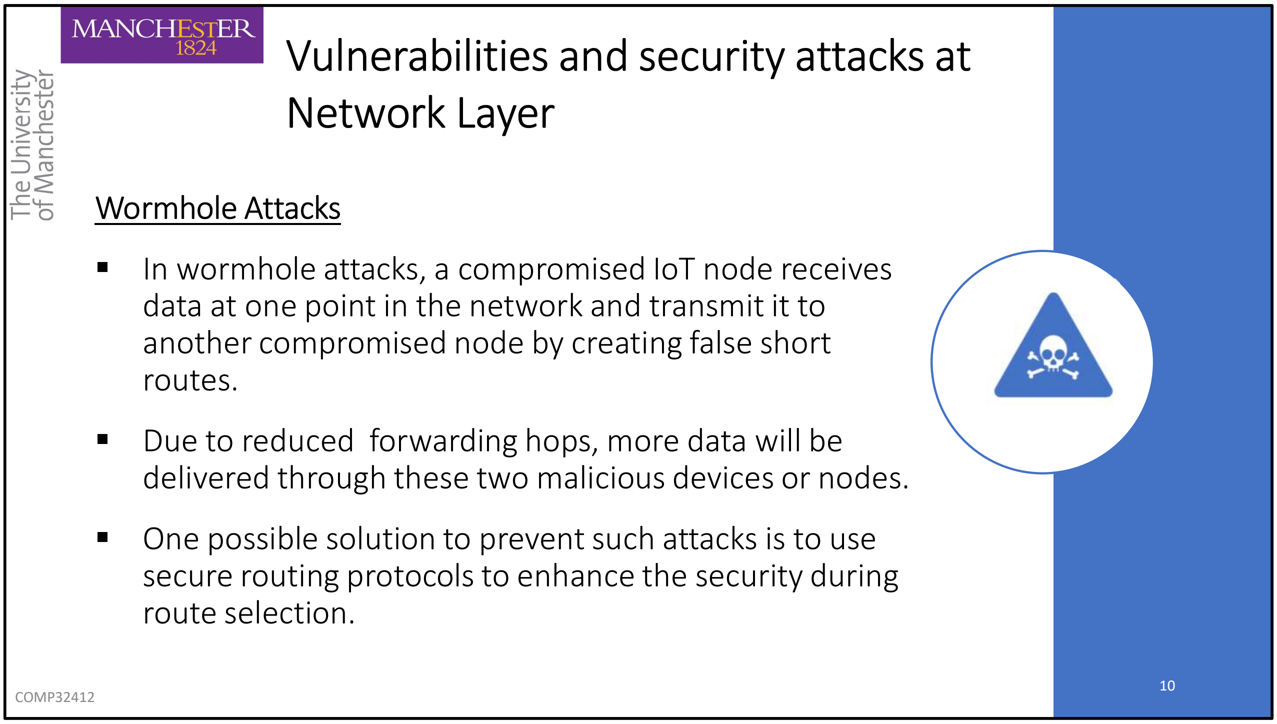
Vulnerabilities and security attacks at Network Layer

Sinkhole Attacks

- Sinkhole attacks are a specific kind of routing attack in which an adversary promotes a compromised node and attracts other nodes to route traffic through it.
- The compromised device or node can increase the amount of data obtained before its delivered in the IoT system.
- To defend against the sinkhole attack, techniques such as secure multiple routing protocols and Intrusion detection system (IDS) 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 Network Layer

Wormhole Attacks

- In wormhole attacks, a compromised IoT node receives data at one point in the network and transmit it to another compromised node by creating false short routes.
- Due to reduced forwarding hops, more data will be delivered through these two malicious devices or nodes.
- One possible solution to prevent such attacks is to use secure routing protocols to enhance the security during route selection.

COMP32412

10

- Wormhole attack can be launched by two malicious IoT devices in different locations and they can exchange routing information with private links to achieve a false one-hop transmission between them, even if they are located far away from each other.

- This can become serious security threat if combined with other attacks such as sinkhole attacks. An attacker can create a warm-hole between a compromised node and a device on the internet and try to bypass the basic security protocols in an IoT application.

- To defend against wormhole attack, one technique is to modify the routing protocols to enhance the security in the route selection process, while other techniques involve deploying secure hardware

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 Middle-ware Layer

- The role of the middleware in IoT is to create an abstraction layer between the network layer and the application layer.
- This layer is responsible to process the data received from the network layer and provide services to the application layer as per the IoT applications requirements
- Database security and cloud security are other main security challenges in the middleware layer.

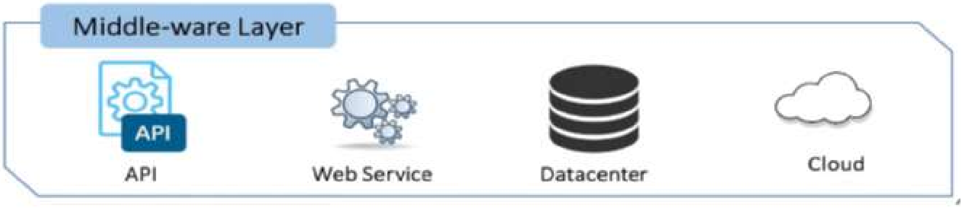
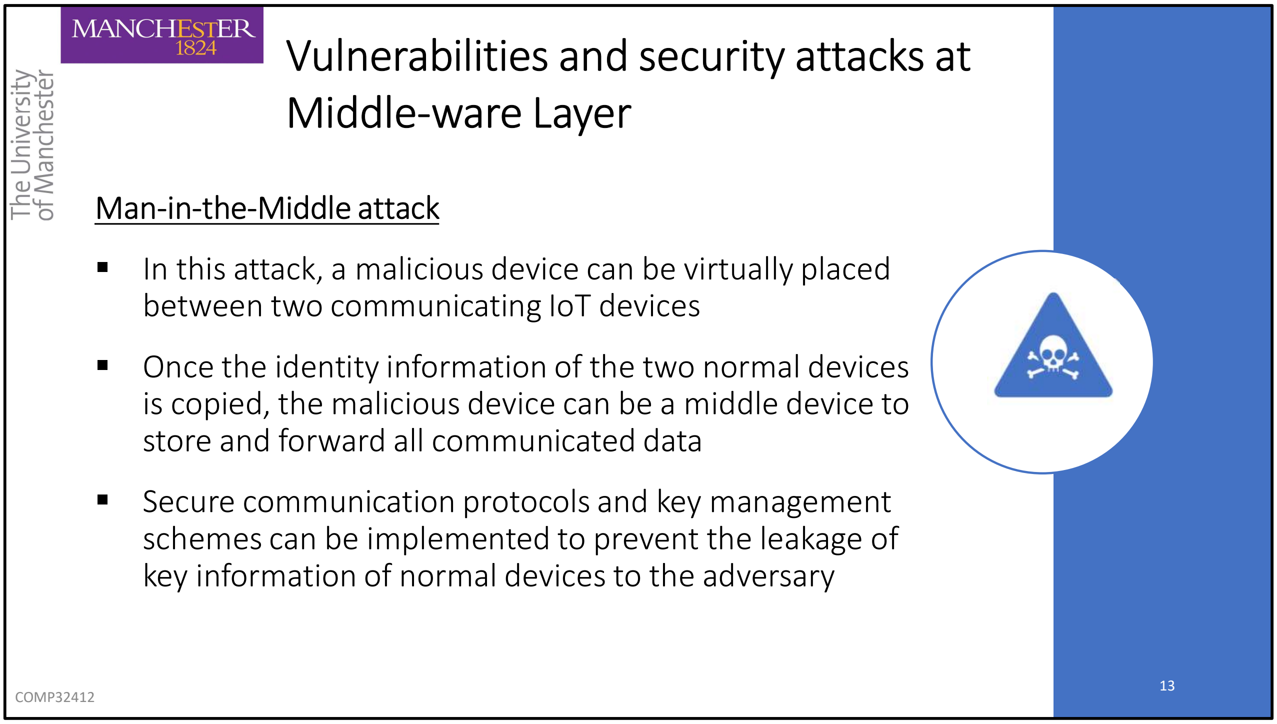


*Image source: Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

Vulnerabilities and security attacks at Middle-ware Layer

The major security attacks that are encountered at the middle-ware layer are as follows

- Man-in-the-Middle Attacks
- SQL injection Attacks
- XML Signature Wrapping Attacks
- Cloud Malware Injection Attacks
- Flooding Attacks in Cloud



Vulnerabilities and security attacks at Middle-ware Layer

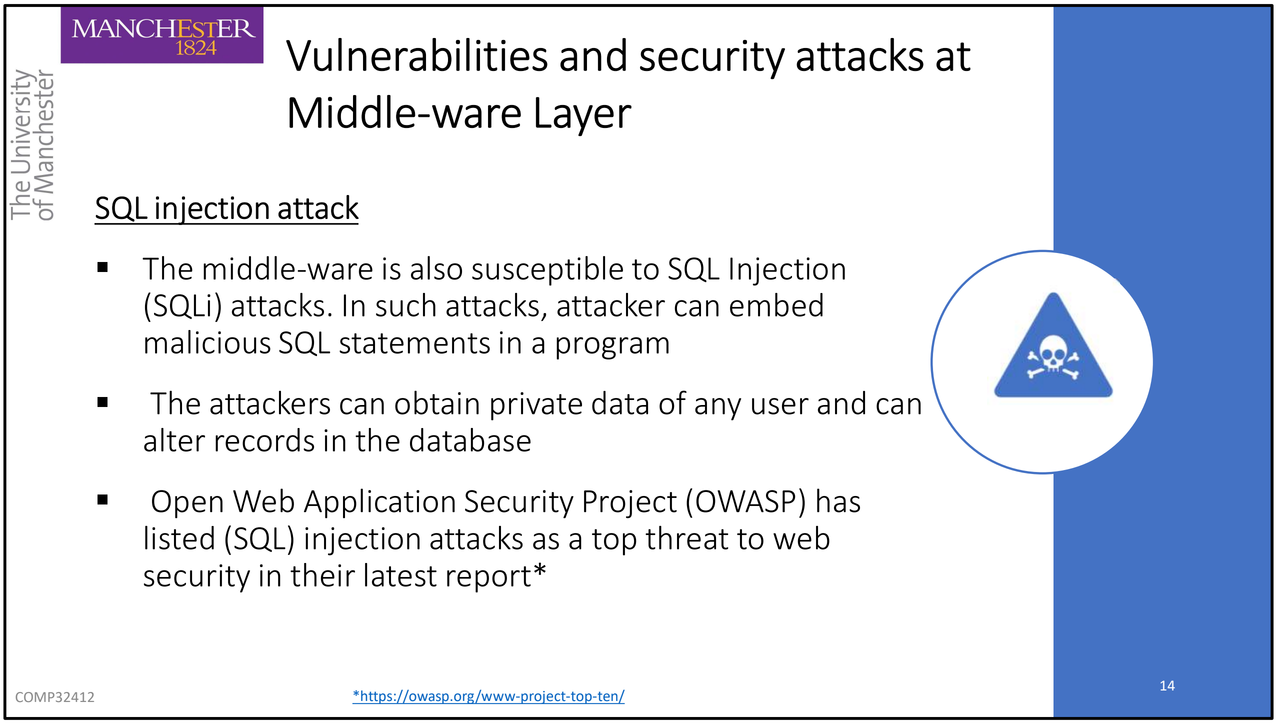
Man-in-the-Middle attack

- In this attack, a malicious device can be virtually placed between two communicating IoT devices
- Once the identity information of the two normal devices is copied, the malicious device can be a middle device to store and forward all communicated data
- Secure communication protocols and key management schemes can be implemented to prevent the leakage of key information of normal devices to the adversary

- The two normal devices cannot detect the existence of the malicious device, and instead believe that they directly communicate with each other.
- Unlike malicious node capture attacks that need to physically tamper with the hardware of devices, the man in middle attack can be launched by only relying on the communication protocols used in IoT networks.

Source:

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



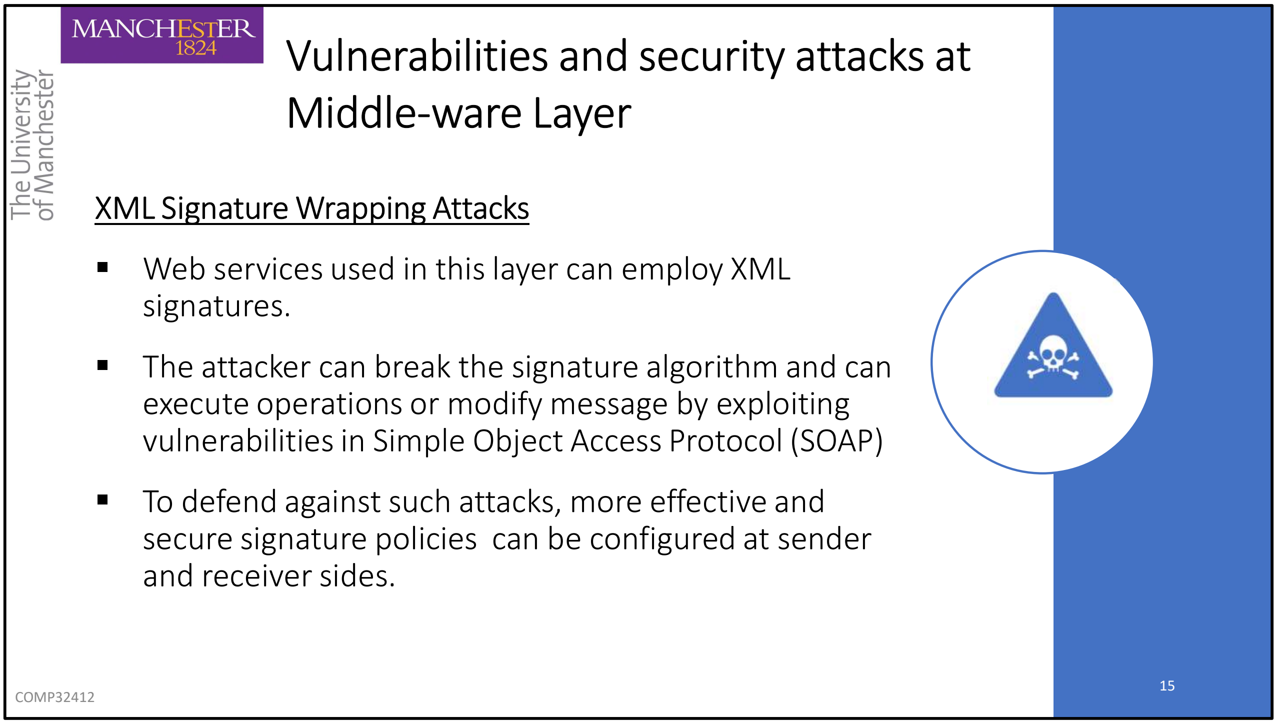
Vulnerabilities and security attacks at Middle-ware Layer

SQL injection attack

- The middle-ware is also susceptible to SQL Injection (SQLi) attacks. In such attacks, attacker can embed malicious SQL statements in a program
- The attackers can obtain private data of any user and can alter records in the database
- Open Web Application Security Project (OWASP) has listed (SQL) injection attacks as a top threat to web security in their latest report*

*https://owasp.org/www-project-top-ten/

- This is a type of code injection attack where the attacker targets database systems at the middle-ware layer of the IoT architecture by gaining access to the system.
- The attacker gain access to the vulnerable database services and inject malicious SQL statements. In return the requests are validated by the database. Finally the attacker gets access to view and can amend database entries by attaining administrative privileges if left undetected.
- The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software
-



Vulnerabilities and security attacks at Middle-ware Layer

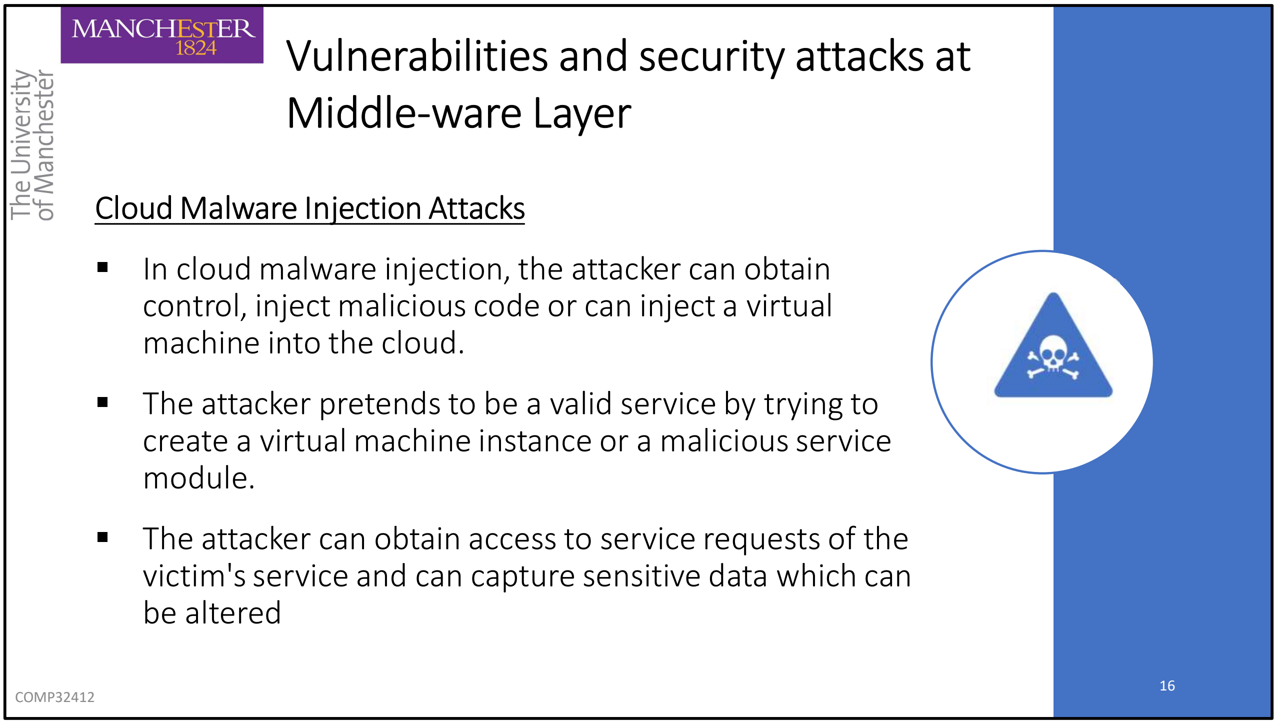
XML Signature Wrapping Attacks

- Web services used in this layer can employ XML signatures.
- The attacker can break the signature algorithm and can execute operations or modify message by exploiting vulnerabilities in Simple Object Access Protocol (SOAP)
- To defend against such attacks, more effective and secure signature policies can be configured at sender and receiver sides.

- XML Signature wrapping is not specific to IoT system as it generally target web services using SOAP
- SOAP is a message protocol that allows distributed elements of an application to communicate. SOAP can be carried over a variety of lower-level protocols, including the web-related Hypertext Transfer Protocol (HTTP).

Source:

- Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.
- WS-Attacks. Attack Subtypes. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping



MANCHESTER 1824

The University of Manchester

Vulnerabilities and security attacks at Middle-ware Layer

Cloud Malware Injection Attacks

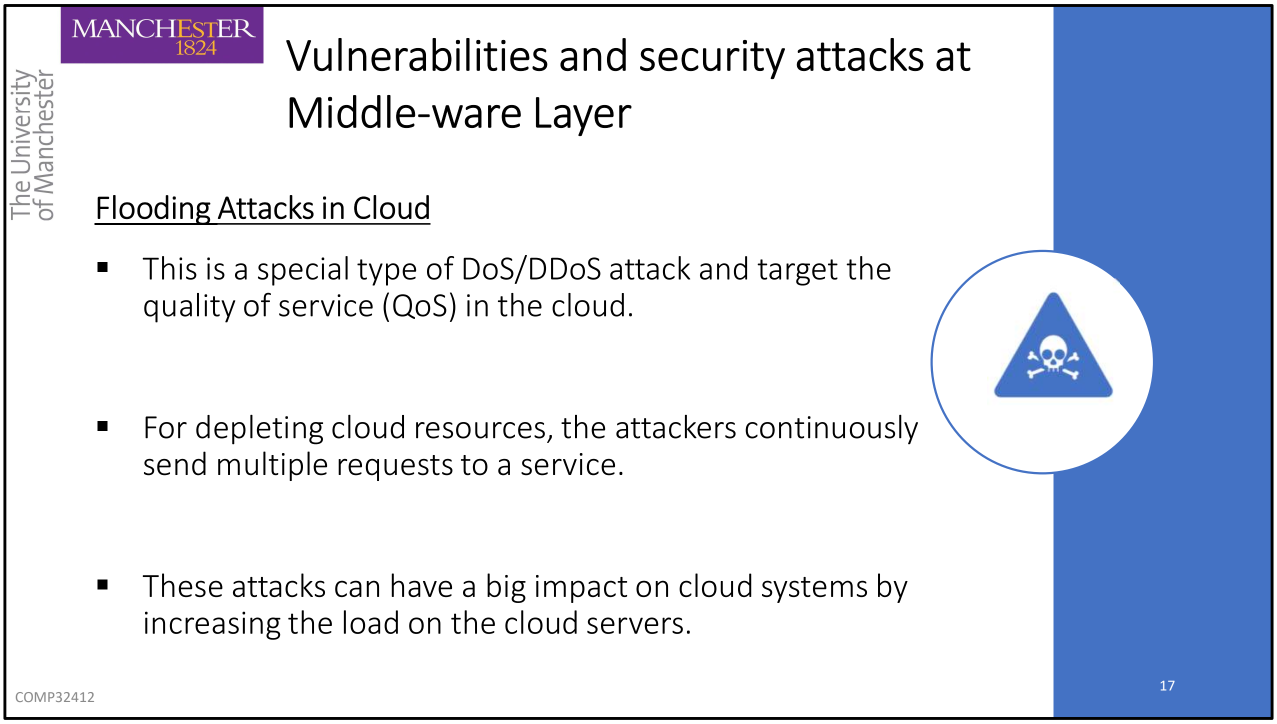
- In cloud malware injection, the attacker can obtain control, inject malicious code or can inject a virtual machine into the cloud.
- The attacker pretends to be a valid service by trying to create a virtual machine instance or a malicious service module.
- The attacker can obtain access to service requests of the victim's service and can capture sensitive data which can be altered

COMP32412

16

Source:

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



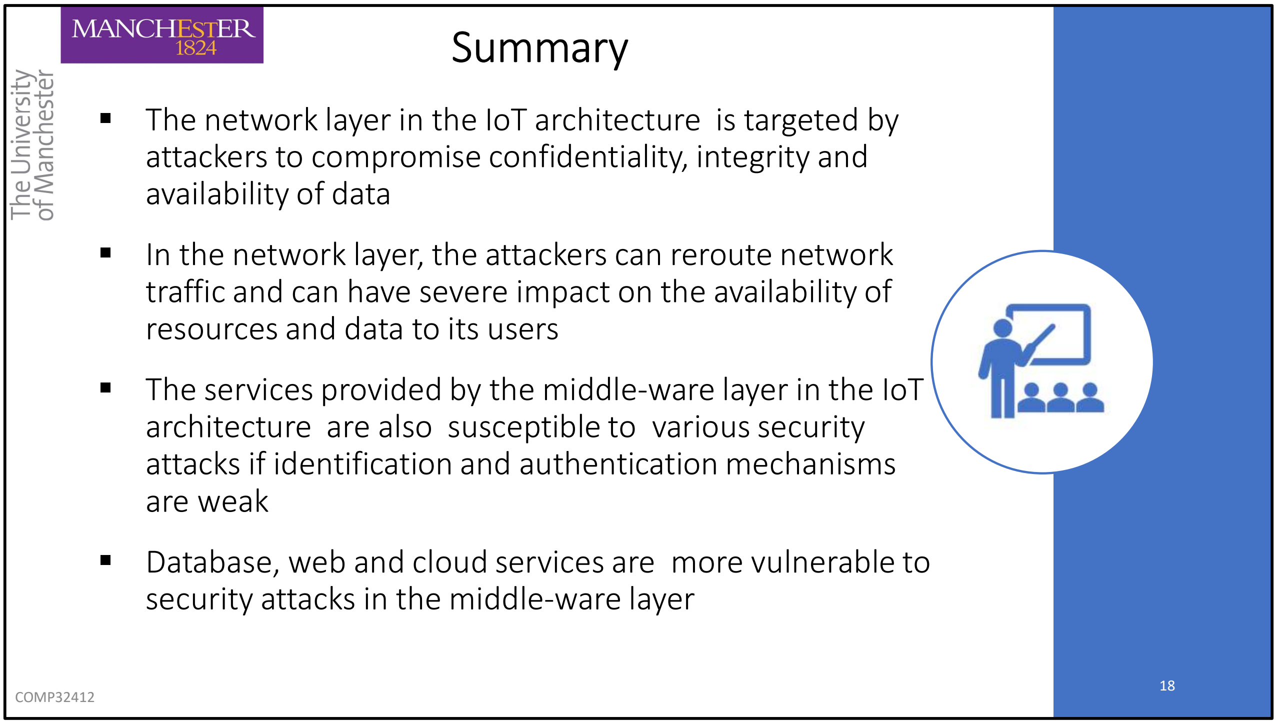
Vulnerabilities and security attacks at Middle-ware Layer

Flooding Attacks in Cloud

- This is a special type of DoS/DDoS attack and target the quality of service (QoS) in the cloud.
- For depleting cloud resources, the attackers continuously send multiple requests to a service.
- These attacks can have a big impact on cloud systems by increasing the load on the cloud servers.

Source:

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



Summary

- The network layer in the IoT architecture is targeted by attackers to compromise confidentiality, integrity and availability of data
- In the network layer, the attackers can reroute network traffic and can have severe impact on the availability of resources and data to its users
- The services provided by the middle-ware layer in the IoT architecture are also susceptible to various security attacks if identification and authentication mechanisms are weak
- Database, web and cloud services are more vulnerable to security attacks in the middle-ware layer