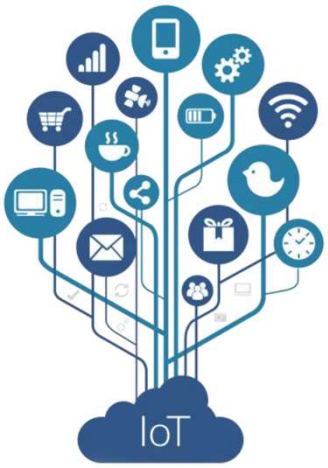
MANCHESTER 1824
The University of Manchester



COMP32412: Internet of Things Architecture and Applications

Security vulnerabilities in application layer in IoT

Mustafa A. Mustafa

mustafa.mustafa@manchester.ac.uk
KB 2.93, 2nd Floor, Kilburn Building

MANCHESTER 1824
The University of Manchester

Overview & Learning Outcomes

- Describe and identify security attacks at the application layer of IoT architecture

MANCHESTER 1824
The University of Manchester

Vulnerabilities and security attacks at Application Layer

- The application layer directly deals with and provides services to the end users
- IoT applications like smart homes, smart meters, smart cities, smart grids, etc. lie in this layer.
- This layer has particular security challenges such as data theft and privacy issues.

3

The privacy issues at the application layer level can lead to some serious concerns. For example, in the smart grid, if the adversary obtains the private data of the energy consumption of customers, he or she can infer the time when users are in the home or out of home, and conduct theft or other damage to users with a probability. Thus, privacy-preserving mechanisms need to be developed to ensure private data not to be leaked to the adversary 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.

MANCHESTER 1824
The University of Manchester

Vulnerabilities and security attacks at Application Layer

The major security attacks that are encountered at the application layer are as follows

- Data Theft Attacks
- Access Control Attacks
- Service Interruption Attacks
- Malicious code Injection Attacks
- Sniffing Attacks

MANCHESTER 1824
The University of Manchester

Vulnerabilities and security attacks at Application Layer

Data Theft Attacks

- IoT applications deal with large amounts of critical and private data making them more prone to data thefts
- The users will be reluctant to register their private data on IoT applications if these applications are vulnerable to data theft attacks.
- Techniques used to handle such attacks:
  - Data encryption, data isolation, robust user and network authentication, privacy management, etc.

5

This is quite a generic category of security attacks where the main aim of attackers is to steal important information. These type of attacks mainly target data confidentiality.

- In these kind of attacks, the integrity of data can be compromised by stealing credentials using phishing attacks, injecting code modifications and launching malwares at the application layer level.
- Data encryption, data isolation, user and network authentication, privacy management, etc. are some of the techniques and protocols being used to secure IoT applications against data thefts.

Source:
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 Application Layer

Access Control Attacks

- Access control is authorization mechanism that allows only legitimate users or processes to access the data or account.
- Access control attack is a critical attack in IoT applications as once the access is compromised, then the complete IoT application becomes vulnerable to attacks.
- Secure authorization access, and multi-layered identification and authentication protocols can be used to prevent such attacks

6

At application layer level, the adversary can obtain the confidential data of users, such as identification and passwords, by spoofing the authentication credentials of users via the infected e-mails and phishing websites

- IoT application users should be reminded to be more vigilant when accessing their data over the internet.

Source:
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 Application Layer

Service Interruption Attacks

- These attacks are also referred to as illegal interruption attacks or DDoS attacks
- *There have been various instances of such attacks on IoT applications.
- Such attacks deprive legitimate users from using the services of IoT applications by artificially making the servers or network too busy to respond.

* https://www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/

7

Source:

- 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 Application Layer

Malicious code Injection Attacks

- A malicious virus/worm is another challenges to IoT applications.
- The adversary can infect the IoT applications with malicious self propagating attacks (worms, Trojan Horse, etc.), and then obtain or tamper with confidential data.
- Reliable firewall, malicious code detection, and other defensive mechanisms need to be deployed to combat malicious virus/worm attacks in IoT applications

8

- These types of attacks can also target other layers of IoT architecture such as IoT devices at sensing layer
- Attackers generally go for the easiest or simplest method they can use to break into a system or network. If the system is vulnerable to malicious scripts and misdirections due to insufficient code checks, then that would be the first entry point that an attacker would choose.
- Generally, attackers use XSS (cross-site scripting) to inject some malicious script into an otherwise trusted website. A successful XSS attack can result in the hijacking of an IoT account and can paralyze the IoT system.

MANCHESTER 1824
The University of Manchester

Vulnerabilities and security attacks at Application Layer

Sniffing Attacks

- The attackers use sniffer applications to monitor the network traffic in IoT applications mainly targeting unencrypted communication.
- Sniffing attacks can be used to gain access to confidential user data if the devices are transmitting data with out encryption and there are not enough security protocols implemented
- To defend against such attacks, lightweight but effective encryption algorithms can be implemented within each of the IoT devices.

9

- Resource-constrained IoT devices are more prone to such attacks as these devices do not support encryption to transmit data securely to other nodes. Secure transmission protocols (such as HTTPS, Secure File Transfer Protocol (SFTP)) should be used
- IoT Devices using unsecure methods (plain text or simple encryption schemes etc.) can put entire system at risk because it leaves the data prone to attackers.
- Eavesdropping, traffic sniffing, man-in-the-middle based attacks and other exploits can be used to gain access to the device and launch more sophisticated attacks.

Source:

- 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

Summary

- The application layer is more vulnerable to security attacks as it directly deals with and provides services to the end users
- The application layer has specific security issues that are not well recognised in other layers, such as data theft and privacy issues.