Module 8: Activity 5

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

"Ira A. Fulton School of Engineering, Arizona State University"

"IFT 520: Advanced Information Systems Security"

"Prof. Upakar Bhatta"

"Oct 10, 2023"

“Challenges for IoT Security”

“Authorize and Authenticate Devices”

Introduction

The Internet of Things (IoT) has ushered in a period of connectedness that is unmatched because of the development of devices that are seamlessly interacting throughout the digital ecosystem. Although there are many prospects for innovation and efficiency due to this interconnection, there are also significant security concerns. In order to protect Internet of Things (IoT) systems against unauthorized access, data loss, and potential breaches, device authentication and authorization are essential.

It explores the critical importance of device authentication and authorisation in the security of IoT systems, describing potential problems and solutions. “An IoT platform that offers security by default can help allay these worries by enabling two-factor authentication (2FA) and prohibiting the use of passwords or other credentials. The IoT platform offers device permissions to define which services, apps, or resources each device may access across the board” [1].

Issue

It is not authentication based on flimsy numbers or pre-set passwords that causes problems with device authentication and authorisation in a secure IoT scenario. Effective solutions are required for some of these problems and shortcomings. Device authentication and authorisation are essential to IoT system security because multiple devices act as access points to IoT systems. A device has to be set up before it can access portals, services, and apps. However, a lot of IoT devices have issues with device authentication, such as using passwords that are not changed from the default value or weak password authentication.

The biggest problem with IoT security is that without appropriate authentication and authorisation procedures in place, devices cannot be used. In commercial, smart home, or healthcare applications, many IoT devices have automation problems. “One possible problem is continuing to use password-based authentication or, even worse, using the default password. These apps put IoT networks at risk from a variety of dangers, such as brute force assaults, unauthorized device access, and exposed critical data” [1].

Discussion

The process by which a device authenticates itself before being granted access to a network or system is known as device authentication. Unfriendly actors can take advantage of vulnerabilities provided by weak or unauthenticated systems. “An IoT platform with security by default is necessary to lessen these risks. These systems encourage the use of two-factor (2FA) authentication as well as strong passwords and certificates. In particular, 2FA adds an additional layer of security by requiring users and devices to provide two different authentication methods” [2].

Device authorization for management: Device authorization is just as important for managing services as authentication. The application or resources of the IoT system are accessible to all devices. This is essential to prevent damage in the event that the device is hacked. “Permissions define which devices may access which data and do which actions. IoT systems are equipped to set the authorisation rules required to ensure that only permitted devices may connect to certain resources” [3].

- **Proliferation of IoT devices:** Numerous IoT devices are being used in a variety of applications. Many of these devices are produced by different companies and may have different levels of security. All of these tools must meet quality assurance and licensing requirements, which must be ensured.

- **Compatibility with Legacy Devices:** IoT ecosystems may include a mix of older, less secure technology. “Older devices might not have the hardware or firmware necessary to execute sophisticated authentication techniques. Organizations find it challenging to maintain security throughout their IoT infrastructure as a result” [2].

- **Supply chain weaknesses:** IoT devices might be compromised even before they are used by a customer. Poor delivery, such as halted manufacturing or ineffective product placement, offers a significant risk. These security issues will affect the device's reliability and integrity.

- **Interoperability problems:** IoT systems depend on interoperability since it makes it possible for various goods and platforms to coexist peacefully. However, if this “relationship is not well managed, it might have negative effects. Making sure that gadgets from multiple providers can interact and communicate safely is difficult” [4].

- Establishing tools and permissions is just as important as ensuring data privacy and compliance. Sensitive information is regularly captured and sent by IoT devices. The security balance becomes even more complicated when it comes to making sure that this data is adequately protected and complies with IoT data protection.

While the idea of using powerful tools and permissions is logical, actually implementing these measures may be challenging. “In environments with a sizable number of IoT devices, coordination is required to manage passwords and authentication procedures. In order to address vulnerabilities as they emerge, it is crucial to make sure that IoT platforms and devices receive timely security updates and fixes” [3].

Summary and Conclusions

In order to improve the security of networked systems throughout the IoT's explosive expansion, device authentication and authorisation are essential. IoT networks are vulnerable to many security issues when authentication methods based on unencrypted or weak passwords are developed. IoT solutions that provide security by default must be used to address this issue. These technologies not only provide strong authentication but also make it simpler and more secure to use 2FA.

Device permissions are also essential for minimizing the effects of security breaches. IoT systems can ensure that each device only gets the resources it needs thanks to granular permissions. Although these indications are essential, they can be difficult to implement, especially in a situation where IoT is prevalent. But for the IoT ecosystem to continue to grow and remain stable, these problems must be fixed. For the protection of IoT systems and an understanding of the relevance of IoT security and accountability, device authentication and authorisation are essential.

References

[1] Schneier, Bruce. (1996). "Applied Cryptography: Protocols, Algorithms, and Source Code in C."

[2] Ferguson, Niels, and Schneier, Bruce. (2003). "Practical Cryptography."

[3] https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/

[4] Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols documentation.