Assessment of Authentication- and Access Control Issues of IoT in Context of Security

Bewertung von Authentifizierungs- und Zugriffskontrollproblemen des IoT im Sicherheitskontext

Author’s Name: Elior Vila
*Affiliation: Department of Informatics, University of Elbasan “Aleksander Xhuvani”
Elbasan, Albania, elior.vila@uniel.edu.al

Abstract – The next-generation global network, known as the Internet of Things (IoT), is thought to connect all vital items to improve and simplify people's lives. Even if it still is only a somewhat concrete idea, several pertinent ongoing studies will make this design more widespread in the future. IoT makes use of ubiquitous computing, radio frequency identification, mobile ad hoc networks, wired and wireless sensor networks etc. Before the IoT is extensively used, security and privacy concerns should be considered and resolved due to the internet's inherent weaknesses and malicious cyber threats. Two essential methods for preventing a computer, device, or network component from being accessed without authorization are authentication and access control. Also, the security of internetworking shared data is a crucial problem that cannot be ignored since such data contains a significant quantity of confidential and private information. The main goal of this paper is to conduct a security assessment of authentication and access control as two central elements responsible for the correct and reliable operation of IoT system in context of security. The paper starts with an overview of IoT's general history before moving on to the issues that IoT faces. Finally, the potential future research directions for extending current security solutions will be highlighted.

Zusammenfassung – Das globale Netzwerk der nächsten Generation, bekannt als Internet der Dinge (IoT), soll alle wichtigen Elemente verbinden, um das Leben der Menschen zu verbessern und zu vereinfachen. Auch wenn es sich noch um eine einigermaßen konkrete Idee handelt, werden mehrere einschlägige laufende Studien dafür sorgen, dass dieses Design in Zukunft weiterverbreitet wird. Das IoT nutzt Ubiquitous Computing, Radiofrequenzidentifikation, mobile Ad-hoc-Netzwerke, drahtgebundene und drahtlose Sensornetzwerke usw. Bevor das IoT umfassend genutzt wird, sollten Sicherheits- und Datenschutzbedenken berücksichtigt und aufgrund der inhärenten Schwächen und böswilligen Cyberbedrohungen des Internets gelöst werden. Zwei wesentliche Methoden, um den unbefugten Zugriff auf einen Computer, ein Gerät oder eine Netzwerkkomponente zu verhindern, sind Authentifizierung und Zugriffskontrolle. Auch die Sicherheit gemeinsam genutzter Daten im Internet stellt ein entscheidendes Problem dar, das nicht ignoriert werden darf, da diese Daten eine erhebliche Menge vertraulicher und privater Informationen enthalten. Das Hauptziel dieses Beitrags besteht darin, eine Sicherheitsbewertung der Authentifizierung und Zugangskontrolle als zwei zentrale Elemente durchzuführen, die für den korrekten und zuverlässigen Betrieb des IoT-Systems im Sicherheitskontext verantwortlich sind. Der Beitrag beginnt mit einem Überblick über die allgemeine Geschichte des IoT, bevor es zu den Problemen geht, mit denen das IoT konfrontiert ist. Abschließend werden mögliche zukünftige Forschungsrichtungen zur Erweiterung aktueller Sicherheitslösungen hervorgehoben.

I. INTRODUCTION

Internet of Things (IoT) is a global Internet-based information service platform, while as a term it was coined by Kevin Ashton in 1999. According [1], IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. Such physical objects may also be appliances which play important roles in our daily life, and therefore security, privacy and safety should be outstanding concerns for the makers of these devices and for their users. Broadly speaking, one wants to be assured that use of such interconnected devices will not risk harm to person or property. Industrial IoT systems have also similar security requirements since nowadays millions of embedded devices are used in safety and security critical applications such as industrial control systems, modern vehicles, and critical infrastructure [2]. IoT systems are high security risks for several reasons. They do not have well-defined perimeters, are highly dynamic, and continuously change because of mobility. In addition, IoT systems are highly heterogeneous with respect to the communication medium and protocols, platforms, and devices [3].

Authentication and access control are recognized as two key mechanisms for addressing security and privacy problems in computer networks and internet [4][5]. They can prevent unauthorized users from gaining access to resources and enable legitimate users to access resources in an authorized manner. It's crucial to make sure that only approved users or systems can access the network and its resources to protect IoT devices and the data they generate. Using a secure authentication protocol like OAuth or OpenID Connect [5] is one technique to establish authentication and access control even in an IoT network. With the help of these protocols, devices and users can log in to the network and approve access to resources.

Role-based access control (RBAC) is a crucial component of access control in an IoT network. This entails allocating various levels of access to various users or gadgets in accordance with their functions and responsibilities within the network. A typical user might only have access to some devices or data, whereas an administrator might have complete access to all devices and data.

Along with these precautions, it's critical to make sure that any network-connected devices are adequately secured using encryption and strong passwords. Regular network auditing and monitoring can also aid in identifying and preventing illegal access.

In conclusion, putting robust authentication and access control procedures into place is essential for protecting an IoT network's sensitive data and securing the infrastructure itself.

II. Common Vulnerabilities in IoT Networks

IoT networks have several potential flaws that attackers could take advantage of [7][8]. These are a few of the most typical:

- Weak authentication and passwords: Default usernames and passwords on IoT devices frequently may be guessed or are well-known. Attackers can quickly access these devices and the network by taking advantage of lax authentication procedures.
- Unsecured communications: IoT devices frequently communicate through open channels that are susceptible to being eavesdropped on by hackers. This may result in the loss of confidential information or the introduction of malicious software onto the network.
- IoT devices frequently rely on obsolete software that may have known vulnerabilities due to a lack of software upgrades or patching. Attackers may use these weaknesses to compromise devices or gain access to the network.
- Devices with insecure default setups are common on the Internet of Things (IoT), making them vulnerable to attack. Devices, for instance, can have open ports that intruders can utilize to enter the network.
- Physical attacks: IoT equipment could be physically susceptible to crimes like theft or tampering. Attackers can utilize physical access to tamper with equipment and compromise the network, or they can steal devices to obtain access to data.
- Attacks using malware and ransomware: Malware and ransomware can infect IoT devices and be used to control equipment, steal data, or demand ransom payments.
- Distributed Denial-of-Service (DDoS) Attack: In this type of attack, IoT networks could be targeted by thousands of fake requests generated by controlled and coordinated botnets to block or shut down the service from other legitimate customers.

Strong security measures must be put in place to mitigate these vulnerabilities, including reliable authentication procedures, communication encryption, and regular software upgrades and patching. Regular security audits and penetration tests can also aid in locating weaknesses and guaranteeing network security.

III. Security Measurements and Authentication Protocols

IoT networks frequently employ several security mechanisms, in addition to authentication and access control, to safeguard devices and data. Some of these actions consist of:

1. Sensitive data is protected via encryption, which turns it into a code that can only be unlocked with a certain key. To protect data both in transit and at rest, IoT networks frequently use encryption.

2. Regular firmware updates can assist in addressing security flaws and enhancing the general security of IoT devices. As soon as these updates are made available, they should be implemented.

3. Firewall: To monitor and manage incoming and outgoing traffic to and from IoT devices, as well as to prevent unwanted access and assaults, a firewall can be utilized.

4. Physical security: Using tamper-resistant hardware or locking cabinets are two physical security techniques that can help shield IoT devices from assaults.

IoT networks can be protected from a variety of threats by deploying a variety of security measures, which can also assist secure the security and privacy of users and their data. In IoT networks, numerous authentication mechanisms are frequently used, including:

- The open standard for permission known as OAuth (Open permission) offers secure access to resources without disclosing user credentials. It is frequently used in IoT networks to give devices access to APIs or cloud-based services.
- OpenID Connect: OAuth 2.0 is the foundation upon which the OpenID Connect authentication protocol is built. It offers an industry-standard method for IoT devices to identify themselves to a server and collect user data.
- TLS (Transport Layer Security) is a protocol that offers secure internet connection. It is frequently used in IoT networks to authenticate servers and clients and encrypt data in transit.
- Tickets are used by the network authentication system known as Kerberos to identify users and devices. It frequently provides safe access management and authentication in enterprise IoT networks.
- Security Assertion Markup Language, or SAML, is an XML-based system that allows parties to exchange authentication and authorization information. It frequently offers single sign-on (SSO) features in IoT networks.
- The networking protocol known as RADIUS (Remote Authentication Dial-In User Service) offers centralized authentication, authorization, and accounting management for remote access. To safeguard access to wireless networks, it is frequently used in IoT networks.

Layered security and access control can be provided in IoT networks by combining these authentication mechanisms. Many IoT networks safeguard their devices and data using one or more of these authentication mechanisms. Here are a few instances:

- To authenticate devices and grant access to AWS services like Amazon S3 and Amazon DynamoDB, Amazon Web Services (AWS) IoT employs OAuth.
- Google Cloud IoT: Google Cloud IoT employs OAuth to authorize access to Google Cloud Platform services and TLS to encrypt data in transit and authenticate devices.
- Microsoft Azure IoT: Microsoft Azure IoT employs OAuth to authorize access to Azure services and TLS to protect device connections and authenticate devices.
- Philips Hue: OpenID Connect and TLS are used by Philips Hue to authenticate users and grant access to Hue services.

The overall goal of these IoT networks is to provide secure access control and safeguard critical data from unauthorized access.

IV. ASSESSMENT OF AUTHENTICATION OF ACCESS CONTROL

The security of an IoT network must include access control and authentication. IoT devices commonly handle critical systems or collect sensitive data because they are designed to be connected to the internet. As a result, it is imperative to guarantee that these systems can only be accessed by authorized entities or individuals. Authentication is the process of confirming a user's or a device's identity when they attempt to access a system. To do this, several methods can be applied, including passwords, biometric authentication, smart cards, tokens, or certificates. An IoT network may employ authentication at different levels, including the device-level, communication-level, and user-level levels.

Contrarily, access control describes the procedure of approving or rejecting access to a system or resource based on verified identification. Different approaches, such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or Access Control Lists (ACLs), can be used to provide access control.

5. Device-level authentication: To ensure that only authorized devices may access the network, IoT devices should be authenticated using unique IDs and certificates. The device firmware can be verified using digital signatures during boot-up utilizing secure boot methods, or hardware-based security mechanisms like Trusted Platform Modules (TPMs) can be used.
6. User-level authentication: Users using the IoT network should also be authorized to use strong authentication mechanisms, such as two-factor authentication or biometric authentication, in addition to device-level authentication.
7. Communication-level authentication: It's crucial to make sure that IoT devices' network communications with servers and one another are secure. Secure communication methods like TLS, which encrypt data in transit and provide authentication of the conversing parties, can be used to do this.
8. Access control policies: Access control policies specify which IoT network resources can be accessed by which users. As previously indicated, these policies can be implemented utilizing RBAC or ABAC techniques. To make sure that access control policies are current and effective, they should be evaluated frequently.
9. Risk assessment: By regularly conducting risk analyses, it is possible to spot potential security threats in the IoT network. A security breach's potential impact can be evaluated along with the system's vulnerabilities and potential attack routes.
10. Security monitoring and incident response: Consistent IoT network monitoring can assist in identifying potential security risks and lapses. Log analysis, intrusion detection, and vulnerability scanning are a few examples of activities that might be part of security monitoring. To guarantee that any security events are addressed promptly and successfully, an incident response strategy should also be in place.
11. In conclusion, access control and authentication are essential elements of safeguarding IoT networks. Organizations can make sure that their IoT networks are safe and secure by putting strong authentication systems, access control policies, and security monitoring in place.

V. BEST PRACTICES FOR SECURING IOT

A complete strategy that combines technological, operational, and organizational measures must be used to secure IoT networks. Here are a few top recommendations for protecting IoT networks:

- Implement strong authentication methods: Strong authentication methods can help prevent unauthorized access to IoT devices and networks, including two-factor authentication, biometric authentication, and certificates.
- Encrypt communications when possible. Encrypting communications between IoT devices and servers helps guard against man-in-the-middle attacks and help prevent data breaches.
- Consistently update software and firmware: Updating software and firmware can boost IoT devices and networks' security by addressing identified vulnerabilities.
- Implement access control policies: In the IoT network, access control policies like RBAC or ABAC can be used to manage who has access to resources. This can lessen the possible effects of a security breach and help prevent unwanted access.
- Conduct routine security audits: Routine security audits and penetration testing can assist in finding potential security holes in the IoT network and guarantee that security precautions are working properly.
- Use firewalls and intrusion detection systems: These tools can be used to track network traffic and find potential security risks.

Organizations may strengthen the security of their IoT networks and guard against potential security threats by putting these best practices into practice.

VI. CONCLUSIONS

In conclusion, authentication and access control are critical components of securing IoT networks. With the increasing number of connected devices and the sensitive data they transmit, it is crucial to ensure that only authorized users and devices have access to the network and its resources.

Authentication mechanisms like passwords, biometric authentication, and two-factor authentication can help ensure that only authorized users can access the network. Access control mechanisms like firewalls, virtual private networks (VPNs), and network segmentation can help ensure that only authorized devices can access specific parts of the network.

However, it is important to note that IoT devices often have limited processing power and memory, which can make it difficult to implement robust security measures on these devices. Furthermore, convenience is frequently prioritized over security in the design of IoT devices, which can lead to security gaps that attackers may exploit. Strong IoT device authentication can only be ensured by trustworthy device identity provisioning techniques and data flows safeguarded by public key infrastructure. As a result, it's crucial to develop a multi-layered security strategy that includes not only authentication and access control but also encryption, intrusion detection and prevention, and frequent security updates. Users should be informed about the best practices for protecting their devices and networks, as human error can frequently play a big part in security breaches.

VII. REFERENZEN

[1] https://www.gartner.com/en/information-technology/glossary/internet-of-things [Accessed in October. 2023]

[2] A.R. Sadeghi, Ch. Wachsmann, and M. Waidner. 2015. Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference (DAC '15). Association for Computing Machinery, New York, NY, USA, Article 54, 1–6.

[3] E. Bertino, K.R. Choo, D. Georgakopolous, and S. Nepal. 2016. Internet of Things (IoT): Smart and Secure Service Delivery. ACM Trans. Internet Technol. 16, 4, Article 22, 7 pages.

[4] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, issue 1, Jan. 2010, pp. 23-30.

[5] J. Liu, Y. Xiao, and C. L. Philip Chen. 2012. Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW '12). IEEE Computer Society, USA, 588–592.

[6] W. Li, Chris J. Mitchell, and Th Chen. 2019. OAuthGuard: Protecting User Security and Privacy with OAuth 2.0 and OpenID Connect. In Proceedings of the 5th ACM Workshop on Security Standardization Research Workshop (SSR'19). Association for Computing Machinery, New York, NY, USA, 35–44.

[7] W. H. Hassan et al. 2019. Current research on Internet of Things (IoT) security: A survey. Computer networks 148 (2019), 283–294.

[8] H. Mustapha and A. M. Alghamdi. 2018. DDoS attacks on the internet of things and their prevention methods. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18). Association for Computing Machinery, New York, NY, USA, Article 4, 1–5.