Cyber Security and the Internet of Things : vulnerabilities and Security requirements

Siham Aouad, Abderrahim Maizate, Abdelouahed Zakari

Cyber Security and the Internet of Things : vulnerabilities and Security requirements

S. Aouad, A. Maizate, A. Zakari
Lab. RITM/ESTC. CED Science de l'ingénieur, ENSEM, Université Hassan II
Casablanca, Morocco.
Siham.aouad@outlook.fr

Abstract— **The Internet of Things (IoT) enables billions of embedded computing devices to connect to each other. It includes various kinds of devices, e.g., sensors, actuators, RFID tags, or smartphones, which are very different in terms of size, weight, functionality and capabilities.**
Their success is very noticed and the number of threats and attacks against IoT devices and services are on the increase as well.
In IoT, The objects can be discovered, controlled and managed from the Internet. This articulation, which represents a strong point of the IoT, also inherit all the problematic of the security already present in the Internet. The latter rests even with renewed acuteness in this new environment, because of its characteristics special. It is important to analyze how conventional security requirements (CIA, AAA, etc.) as well as those related to respect for privacy can be broken down in this new environment.

This paper is an attempt to classify different vulnerabilities, besides analyze and characterize security requirements.

Keywords— The Internet of Things (IoT),AAA,IoT security .

I. INTRODUCTION

The Internet of Things (IoT) is designed as a network of highly connected devices (things). In today's perspective, The smart things cover our everyday friendly devices, such as, thermostats, fridges, ovens, washing machines, and TV sets. IoT devices are increasingly deployed.

Several studies show that the number of connected objects deployed on the Internet will experience a exponential growth in the coming years [1], thus leading to an architecture of IoT complex and subject to significant traffic. From a qualitative point of view, the IoT has the characteristics following [2]:

1. IoT is an uncontrolled environment mainly because of the mobility of objects and possibilities extended to physically access them.
2. Heterogeneity: an IoT environment can integrate entities of very variable origins (different platforms, communication protocols, suppliers ...). Scalability related to the amount of objects that can be interconnected.
3. Limited resources in energy, computing capacity and storage space

The IoT presents many challenges. This article provides an overview of the main issues related to the security of IoT. We first recall the major vulnerabilities related to IoT. We are interested in the security of a connected object. Finally we introduce the minimum safety requirements specific to IoT ;

II. THE VARIOUS VULNERABILITIES RELATED TO IOT

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks [3,4]. Vulnerabilities can be found in variety of areas in the IoT systems. In particular, they can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves [5].

Une étude réalisée par HP [6] sur les problèmes de sécurité de l'IoT, en s'appuyant sur l'analyse de 10 équipements parmi les plus populaires dans les plateformes IoT les plus répandues, montre que :

- 90% of the devices collect at least one personal information via the equipment, the cloud, or the mobile application. These informations can be a user name, his address, his date of birth, health information, and even credit card numbers.
- Six out of 10 devices offer user interfaces. These devices all have vulnerabilities, including XSS vulnerabilities and weak identifiers.
- 70% of devices do not encrypt their outbound communications.
- 70% of devices associated with a cloud and a mobile application allow an attacker to know if a user account is valid via the enumeration of accounts.
- 80% of devices associated with a cloud and a mobile application do not require a password of sufficient length and complexity, therefore there are likely to use weak passwords.

According to HP these problems are mainly related to insufficient authentication or authorization, a lack of message transfer encryption, an insecure web interface and vulnerable software / firmware.

III. PRIMARY SECURITY AND PRIVACY GOALS

An attacker who has physical access to a connected object is able to collect a lot of his sensitive information. For example, if he managed to recover his encryption keys, he could access all incoming and outgoing traffic, and could also inject malicious code for other network objects. Each connected object thus appears as a critical point in the architecture of the IoT. In the following we list the various security and privacy features that should be guaranteed in order to secure a connected object.[7].

a) Confidentiality

Confidentiality is an important security feature in IoT, but it may not be mandatory in some scenarios where data is presented publicly[8]. However, in most situations and scenarios sensitive data must not be disclosed or read by unauthorized entities. For instance patient data, private business data, and/or military data as well as security credentials and secret keys, must be hidden from unauthorized entities.

b) Integrity

To provide reliable services to IoT users, integrity is a mandatory security property in most cases. Different systems in IoT have various integrity requirements [9]. For instance, a remote patient monitoring system will have high integrity checking against random errors due to information sensitivities. Loss or manipulation of data may occur due to communication, potentially causing loss of human lives [10]

c) Authentication and authorization

Authentication and authorization are essential parts of basic security processes and are sorely needed in the Internet of Things (IoT). Different authentication requirements necessitate different solutions in different systems. Some solutions must be strong, for example authentication of bank cards or bank systems. On the other hand, most will have to be international, e.g., ePassport, while others have to be local [10]

d) Availability

The vision of IoT is to connect as many smart devices as possible. The users of the IoT should have all the data available whenever they need it. However data is not the only component that is used in the IoT; devices and services must also be reachable and available when needed in a timely fashion in order to achieve the expectations of IoT. [11]

e) Accountability

When developing security techniques to be used in a secure network, accountability adds redundancy and responsibility of certain actions, duties and planning of the implementation of network security policies. Accountability itself cannot stop attacks but is helpful in ensuring the other security techniques are working properly. Core security issues like integrity and confidentiality may be useless if not subjected to accountability. Also, in case of a repudiation incident, an entity would be traced for its actions through an accountability process that could be useful for checking the inside story of what happened and who was actually responsible for the incident.[12]

IV. ATTACKS

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools.

An attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; passive attacks such as monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication information; close-in attacks; exploitation by insiders, and so on. Common cyber-attack types are:

- DoS: DoS attempts to make the IoT devices inaccessible to its intended users through temporary or indefinite interruption [20]. The different types of DoS attacks that can be launched against the IoT include jamming, collision, and malicious internal attacks; the last type can create more havoc because it controls part of the infrastructure[21].
- Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud [22, 5 , 23].
- Device end-point: Smart applications on the IoT domain include smart city items (e.g., e-governance, street lighting, and water and waste management), SG items (e.g., smart meters and smart energy), smart health-care items (e.g., smart health cards), and intelligent transportation of items (e.g., traffic control, parking, and public transportation), which are physically situated in a specific domain. An active attacker can easily hack these items, extract information, and target other infrastructure that store information as alternatives to destroying these items [24].
- Supervisory Control and Data Acquisition (SCADA) Attacks: As any other TCP/IP systems, the SCADA [25] system is vulnerable to many cyber attacks 26, 27]. The system can be attacked in any of the following ways:
  - ✓ Using denial-of-service to shut down the system.
  - ✓ Using Trojans or viruses to take control of the system. For instance, in 2008 an attack launched on an Iranian nuclear facility in Natanz using a virus named Stuxnet [28].
- Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.
- Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.

- Reconnaissance attacks – unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports [29], packet sniffers [30], traffic analysis, and sending queries about IP address information.
- Counterfeiting attacks: Counterfeiting simply means imitation or forgery. The IoT devices, such as smart watches and smart lighting systems, are fragile and require lightweight security. However, an active attacker can easily duplicate and modify the contents of the IoT devices because of the security nature of these devices [31].
- Attacks on privacy: Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available through remote access mechanisms. The most common attacks on user privacy are:
  - ✓ Data mining: enables attackers to discover information that is not anticipated in certain databases.
  - ✓ Cyber espionage: using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.
  - ✓ Eavesdropping: listening to a conversation between two parties [32].
  - ✓ Tracking: a users movements can be tracked by the devices unique identification number (UID). Tracking a users location facilitates identifying them in situations in which they wish to remain anonymous.
  - ✓ Password-based attacks: attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways: 1) dictionary attack – trying possible combinations of letters and numbers to guess user passwords; 2) brute force attacks – using cracking tools to try all possible combinations of passwords to uncover valid passwords.
  - ✓ MitM attack: MitM attacks create challenges in maintaining data security and privacy. Given the different attacks on the IoT devices, the security problem in the IoT involves the active interference of intruders on the devices (i.e., allowing unauthorized users to spy on data through a backdoor). Lightweight cryptographic protocols are considered to provide communication security for the IoT devices over a computer network as part of the DTLS. Nevertheless, MitM attacks take advantage of the weaknesses in the authentication protocols utilized by the communicating parties[33].

V. IoT SECURITY REQUIREMENTS

We take inspiration from [2], which elegantly organizes security requirements into three categories: Network Security, Authentication, Authorization, Accounting (AAA) and Privacy.

Network security

Data exchanged over the Internet between two objects, or between an object and a user, is exposed to various attacks such as eavesdropping, falsification and denial of service, hence the importance of securing the network. These attacks, which have a direct impact on the confidentiality and integrity of the data, can be countered by establishing secure channels between the various IoT entities.

Traditionally, several technologies based on encryption such as IPSec or TLS have proved their effectiveness to ensure the confidentiality of data exchanged over the Internet. They also guarantee the integrity of the data. However, these techniques require significant cryptographic computations that often exceed the limited capabilities of connected objects. The ideal network protocol stack for IoT should provide robust encryption protocols with low computing requirements. Most current solutions tend to offload constrained nodes by using an intermediate trust node with sufficient processing capacity to perform computational tasks.

Finally, whatever the circumstances, the availability of objects must always be preserved. A secure routing protocol such as RPL [13] allows for example to obtain this by guaranteeing the resilience of connected objects.

AAA

Authentication relies on identity management and is one of the most important operations, and probably the first to be performed by a node when it joins a new network, for example for a first deployment or in case of mobility from one network to another. Often, authentication is done via an authentication server with an access protocol such as PANA [14] or EAP [15].

Access control to resources associated with connected objects can rely on mechanisms such as DCAF (Delegated CoAP Authentication Authorization Framework) [16] or OAUTH 2.0 [17]. More generally, access control solutions can be declined in two ways, either via an intermediary located between the object and the access requester, or by the object itself, often through a simple control of access. access token provided by an authorization server.

Private life

Direct access by connected objects to the personal information of individuals and organizations raises issues of privacy. IoT must provide data protection transmitted traffic over the Internet, so that captured traffic does not expose the content of this data. For this reason, mechanisms for data anonymity, pseudonymity and non-traceability must be used to ensure both the protection of private data as well as the protection of the entities themselves [18].

VI. CONCLUSION

The security and privacy protection of connected objects, however, raises several issues that may pose serious obstacles to the deployment or acceptance of IoT. The security and privacy protection of connected objects, however, raises several issues that may serious obstacles to deploying or accepting IoT. The main cause lies in the weakness of computing capabilities of connected objects, which prevents them from using traditional security techniques implemented in the Internet. In this paper, vulnerabilities related to IoT and security requirements were introduced. The relationship between IPv6 and IoT is another point to note. The security of the communication between the different IoT objects via IPv6 is reinforced by the IPSec protocol. However, the implementation of IPSec for 6LoWPAN type equipment, characterized by energy and resource constraints, still poses problems. For this reason, several works have been done to obtain a version of IPSec light and especially compatible with the constrained nodes of the IoT, such as that proposed in [19]

REFERENCES

[1] D. Evans, « The internet of things: How the next evolution of the internet is changing everything », CISCO, 2011.

[2] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier et P. Kikiras,« On the Security and Privacy of Internet of Things Architectures and Systems », International Workshop on Secure Internet of Things, Vienna, Austria, septembre 2015.

[3] D. L. Pipkin, Information security. Prentice Hall PTR, 2000.

[4] E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.

[5] J. M. Kizza, Guide to Computer Network Security. Springer, 2013.

[6] « Internet of things research study 2015 report », Hewlett Packard, 2015.

[7] A. F. Skarmeta, J. Luis Hernández Ramos et J. Bernal Bernabe, « A required security and privacy framework for smart objects », ITU Kaleidoscope: Trust in the Information Society, Barcelona, Spain, décembre 2015

[8] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in Foundations of Security Analysis and Design V.Springer, 2009, pp. 289–338.

[9] B. Jung, I. Han, and S. Lee, "Security threats to internet: a korean multi-industry investigation," Information & Management, vol. 38, no. 8, pp. 487–498, 2001.

[10] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.

[11] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, "Internet of Things (IoT) security: Current status challenges and prospective measures", Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST), pp. 336-341, Dec. 2015.

[12] Abomhara M, Kien G (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur 4:65–88.

[13] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano et M. Richardson, «A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)», RFC 7416, IETF, janvier 2015.

[14] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig et A. Yegin, « Protocol for Carrying Authentication for Network Access (PANA) », RFC 5191, IETF, mai 2008.

[15] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson et H. Levkowetz, « Extensible Authentication Protocol (EAP) », RFC 3748, IETF, juin 2004.

[16] S. Gerdes, O. Bergmann et C. Bormann « Delegated CoAP authentication and authorization framework (DCAF) », IETF Draft, Expire: 21 avril 2016.

[17] D. Hardt, « The OAuth 2.0 Authorization Framework », IETF RFC 6749, octobre 2012.

[18] A. Pfitzmann et M. Hansen, « A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management » , 2010.

[19] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt and U. Roedig, « Securing communication in 6LoWPAN with compressed IPsec », 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, 2011, pp. 1-8.

[20] Wood, A. D., and Stankovic, J. A. (2012). Denial of service in sensor networks. Computer, 35(10), 54–62.

[21] Kasinathan, P., Pastrone, C., Spirito, M. A., and Vinkovits, M. (2013). Denial-of-Service detection in 6LoWPAN based Internet of Things. International Conference on Wireless and Mobile Computing, Networking and Communications, (October), 600–607.

[22] B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2011.

[23] C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress." DTIC Document, 2008.

[24] Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., and Ylianttila, M. (2014). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. *IEEE Wireless Communications and Networking Conference, WCNC, 2014*, 2728–2733.

[25] A. Daneels and W. Salter, "What is scada," in International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339–343.

[26] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "Scada security in the light of cyber-warfare," *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.

[27] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.

[28] M. Kelleye, "Business Insider. The Stuxnet attack on Irans Nuclear Plant was Far more Dangerous Than Previously Thought," http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11/,2013, [Online; accessed 03-Sep-2014].

[29] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," *Potentials, IEEE*, vol. 21, no. 5, pp. 17–19, 2002.

[30] M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, "A review of port scanning techniques," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 2, pp. 41–48, 1999.

[31] Whitmore, A., Agarwal, A., and Da Xu, L. (2014). The Internet of Things: A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.

[32] I. Naumann and G. Hogben, "Privacy features of european eid card specifications," Network Security, vol. 2008, no. 8, pp. 9–13, 2008.

[33] Mahmood, K., Ashraf Chaudhry, S., Naqvi, H., Shon, T., and Farooq Ahmad, H. (2016). A lightweight message authentication scheme for Smart Grid communications in power sector. *Computers and Electrical Engineering*, *52*, 114–124.