Chapter 5
Security Aspects of the Internet of Things

Dominik Hromada
FBM, Brno University of Technology, Czech Republic

Rogério Luís de C. Costa
https://orcid.org/0000-0003-2306-7585
CIC, Polytechnic of Leiria, Portugal

Leonel Santos
https://orcid.org/0000-0002-6883-7996
CIIC, ESTG, Polytechnic of Leiria, Portugal

Carlos Rabadão
https://orcid.org/0000-0001-7332-4397
CIIC, ESTG, Polytechnic of Leiria, Portugal

ABSTRACT

The Internet of Things (IoT) comprises the interconnection of a wide range of different devices, from Smart Bluetooth speakers to humidity sensors. The great variety of devices enables applications in several contexts, including Smart Cities and Smart Industry. IoT devices collect and process a large amount of data on machines and the environment and even monitor people's activities. Due to their characteristics and architecture, IoT devices and networks are potential targets for cyberattacks. Indeed, cyberattacks can lead to malfunctions of the IoT environment and access and misuse of private data. This chapter addresses security concerns in the IoT ecosystem. It identifies common threats for each of IoT layers and presents advantages, challenges, and limitations of promising countermeasures based on new technologies and strategies, like Blockchain and Machine Learning. It also contains a more in-depth discussion on Intrusion Detection Systems (IDS) for IoT, a promising solution for cybersecurity in IoT ecosystems.

DOI: 10.4018/978-1-6684-7132-6.ch005

I. INTRODUCTION

Internet of Things (IoT) as a term was used for the first time in 1999 by Kevin Ashton, a British technology pioneer (Farooq, Waseem, Khairi, & Mazhar, 2015). He defines IoT as the system of physical objects in the world that connects to the internet via a sensor. This ecosystem is full of intelligent machines interacting with each other, with objects, environments, and infrastructures. This new technology has impacted the whole population from everyday people's lives to industry solutions, helping people to work smarter and efficiently, and giving them more control over monitored environments, objects, and infrastructures.

In several market areas, IoT became an essential part of business activities, e.g., providing real-time data about operation activities or measuring the performance of supply chain machines and logistic operations. The data collected by IoT devices can be analyzed later, and provide decision-makers with invaluable insights into their processes with the help of Business Intelligence (BI) to make business processes even more efficient, faster, environmentally friendly, and less expensive. Therefore, IoT opened new opportunities for data analysis and knowledge discovery (Gubbi, Buyya, Marusic, & Palaniswami, 2013). Main IoT applications areas include transportation and logistics, Smart Healthcare, Smart Environments, and City Information Modeling (Ullah, Ahmad, Ahmad, Ata-ur-Rehman, & Junaid, 2019).

On the other hand, the data collected are a double-edged sword. It may be a significant help, but also a threat to people's privacy and security, as their activity can be monitored everywhere and anytime (Neisse et al., 2015). Also, poorly secured devices may lead to attacks on other systems and lead to personal information leaks and misuses due to unauthorized access.

Some of the main security concerns in the context of IoT are related to basic processes (for example, identification, authentication, and access control), data integrity, data confidentiality, data privacy, and data availability (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Farooq et al., 2015). But the layered architecture of IoT is also subject to several attacks and threats, each of them being most common in or targeted to a specific layer (Weyrich & Ebert, 2016; Swamy, Jadhav, & Kulkarni, 2017).

Some of the *traditional* security countermeasures (e.g., the use of security protocols, authentication controls, and privacy by design) may fit in the IoT context. But the new solutions for IoT security include the use of Fog Computing, Blockchain Technology, Edge computing, and Machine Learning-based techniques (Baouya, Chehida, Bensalem, & Bozga, 2020; Ozay, Esnaola, Yarman Vural, Kulkarni, & Poor, 2016).

The use of Intrusion Detection Systems (IDS) in IoT networks is subject to some additional challenges. Deep packet inspection (DPI) and stateful packet inspection (SPI) are computationally expensive and not adequate for the IoT network. An alternative solution in IoT ecosystems may go through an IDS based on IP flow analysis. Additional challenges related to an efficient IDS for IoT networks include aspects related to chosen incident detection methodology, the IDS implementation strategy, and IDS's intrusion detection capabilities.

In the following section, we present the main aspects related to the IoT processing cycle. Then, Section III presents the main security concerns in the IoT context. The IoT layered architecture and the most common threats of each layer are described in Section IV. Section V discusses some current countermeasures based on *nontraditional* solutions and Section V presents open issues and future directions. Finally, Section VII concludes the chapter.