Chapter 34
The Impact of Internet of Things Self-Security on Daily Business and Business Continuity

Hasan Emre Yılmaz
BTCTurk.com, Turkey

Altan Sirel
BTCTurk.com, Turkey

M. Fevzi Esen
https://orcid.org/0000-0001-7823-0883
Istanbul Medeniyet University, Turkey

ABSTRACT

The number of devices operating on IoTs has exceeded billions globally. This chapter aims to examine the cyber security risks of such systems with widespread use and investigate some IoT vulnerabilities. It examines the effects of these vulnerabilities on business life and personal life, and the precautions to be taken to eliminate them. In addition, the regulations and measures to be applied at the state level is discussed. The safe use of IoT systems cannot be achieved solely by individual awareness. An awareness and sense of responsibility in the manufacturing layer is also a must. This chapter investigates the reasons behind the lack of security precautions taken in the manufacturing phase of IoT devices and suggests solutions. It also discusses the details of malwares such as Mirai, whose targets are mainly IoT vulnerabilities.

DOI: 10.4018/978-1-6684-4503-7.ch034

INTRODUCTION

With the growth of Internet bandwidth, many new technologies have emerged which have profound effects on daily life. These new technologies, which facilitate not only our business life but also our social life, are based on high speed internet. Evolution of 3G and 4G mobile internet speeds have already exceeded terrestrial line speeds. Hence, the geographical / physical conditions in which terrestrial lines have difficulties are also overcome. It turned out that the Internet is not just a server/client specific requirement, and that other 'things' can also easily communicate over the Internet. Thus, the concept of 'Internet of Things' (IoT) has emerged.

According to Gartner (2017), it is estimated that up to 8.4 billion IoT devices are connected to the Internet in 2017, since the day a remote controlled coke machine was converted to IoT. Security of IoT devices are often ignored by both manufacturers and end users as a result of their price and their intended purpose of use. The significance of IoT security was realized more heavily after Mirai malware which is a malicious software that creates botnet networks using IoT weaknesses (known as the IoT Hunter), started to create extremely large botnets to carry out the biggest DDoS (Distributed Denial of Service) attacks recorded in history. Mirai showed how dangerous an IoT device, which is configured in the manufacturing phase and has a selling price of $10, can be.

Mirai has performed the largest DDoS attacks ever recorded using IoT devices in its botnet, devices it already confiscated. In 2016, scale of DDoS attack, realized using 175,000 IoT devices, was measured at 620 Gbps. Developers of Mirai released the source code of the malware around the same date, making Mirai a framework that can be used and developed by everyone. Another large attack targeted DNS service provider Dyn. Thus, Twitter, Netflix and other large organizations that use Dyn, were also victims of Mirai (Woolf, 2016).

Purdy & Davarzani (2015) claims that the IoT triggers the emerge of new market segments and business models. IoT can accelerate productivity, design, security and efficiency through innovation in circural economies. These smart systems cause changes in the way of business by exceeding the standard limits business models for firms (Schuh et al., 2014). With highly flexible and centrally controlled smart devices, product – service – material and information will be adapted to the real time processes by vertical integration between or inside the coorporations. The organizational structure of companies and interaction types of smart devices, sensors and machines classified the tasks and goals of autonomous systems by implementing security and privacy protocols (Khan et al., 2018).

Securing IoT connected networks is as important as ensuring IoT's own security (IoT's-Communication Security). For the security of individually used IoT's (camera, TV, baby radio, fitness t-shirt, smart Jacuzzi, smart home systems etc.), it may be advisable to connect the IoT to the internet only when it is used, or even to activate it only when necessary. An IoT that is 'on' even though it is not in use, is always a target for the exploiters. Timed on and off features of some IoTs can be helpful in this context (Pan et al., 2016). Furthermore, network structures of IoTs used in a large network (companies, factories, public spaces) should be physically isolated completely from the corporate network, if possible. Separating networks with VLANs in some implementations is also an acceptable security measure under certain circumstances.

The vulnerabilities of internal software are as important as the security of the networks where IoTs are located. It is rarely possible to have a firewall or a packet filtering software inside these devices since they're limited in terms of processor, storage and RAM in order to reduce costs. The urge of the producer to release its product -which has a high market demand- without any further research, surpasses the