Chapter 1
Implications of Cybersecurity Breaches in LPWANs

Åke Axeland
Chalmers University of Technology, Sweden

Henrik Hagfeldt
Chalmers University of Technology, Sweden

Magnus Carlsson
Chalmers University of Technology, Sweden

Lina Lagerquist Sergel
Chalmers University of Technology, Sweden

Ismail Butun
https://orcid.org/0000-0002-1723-5741
Chalmers University of Technology, Sweden & Konya Food and Agriculture University, Turkey & Royal University of Technology, Sweden

ABSTRACT

With the contrast of limited performance and big responsibility of IoT devices, potential security breaches can have serious impacts in means of safety and privacy. Potential consequences of attacks on IoT devices could be leakage of individuals daily habits and political decisions being influenced. While the consequences might not be avoidable in their entirety, adequate knowledge is a fundamental part of realizing the importance of IoT security and during the assessment of damages following a breach. This chapter will focus on two low-powered wide area network (LPWAN) technologies, narrow-band iot (NB-IoT) and long-range wide area network (LoRaWAN). Further, three use cases will be considered—healthcare, smart cities, and industry—which all to some degree rely on IoT devices. It is shown that with enough knowledge of possible attacks and their corresponding implications, more secure IoT systems can be developed.

DOI: 10.4018/978-1-7998-7468-3.ch001

INTRODUCTION

Technology is steadily emerging with our everyday lives. People are more connected now than ever and the prediction for mobile connected devices is expected to increase from 50 billion in 2020 to around 125 billion by 2030. This is due to several factors like the adoption of 5G, the continuously increasing number of people connected to the internet, adoption of IoT devices in the homes and in the enterprise world (Brent, 2020). For these IoT devices to be able to operate as intended they need to communicate via a gateway. This is often done by using cloud infrastructure with an IoT communication protocol. Which protocol to use boils down to several factors such as environment, hardware, and energy requirements (Hasan, 2020).

IoT devices located in private homes often run on the electrical grid and communicate over Wi-Fi granting a high supply of energy and bandwidth. The communication range is seldom a problem given that conventional network routers can cover an entire home. However, there are IoT devices that need to operate without these conveniences since they are usually running on batteries and communicate over a long-range communication network.

This is where the Low-Powered Wide Area Network (LPWAN) protocols come into play. With these protocols, we solve the problem of range and power by compensating with reduced bandwidth (Butun, Pereira, 2019). A system implementing LPWAN technologies should therefore be a system that only requires a handful of light-weight transmissions a day. This trade-off enables LPWAN connected devices to have longer battery life (> 10 years).

Two of the currently most popular LPWAN technologies are Long-Range Wide Area Network (LoRaWAN) and Narrow-Band IoT (NB-IoT), which will be the ones that this chapter focuses on (Lora Alliance, 2017), (GSM Alliance, 2020). NB-IoT is an LPWAN standard that focuses on specifically low-cost, energy-efficient, and indoor coverage. The challenges, opportunities, and research trends showed LPWAN communication mechanisms and functionalities targeted in low-end devices (IoT) are deployed widely and LoRaWAN (a subset of LPWAN) is known to be secure for most of the known cyber-attacks (Sari, 2020). However, recent research has presented some of the possible attacks that threaten these protocols and how to stay protected from them.

This chapter builds upon this research; however, it will not present any new vulnerabilities. Instead, the goal is to extend the knowledge these papers bring by analyzing possible resulting practical implications of security breaches from various vulnerabilities. This is done by matching real-world examples of actual security breaches to present vulnerabilities of the papers.

Decision Support Systems (DSS), sometimes also referred to as Expert Systems, are strategically located at the heart of a network or a management system, in which