Chapter 28
A Lightweight Authentication and Encryption Protocol for Secure Communications Between Resource-Limited Devices Without Hardware Modification:
Resource-Limited Device Authentication

Piotr Ksiazak
Letterkenny Institute of Technology, Ireland

William Farrelly
https://orcid.org/0000-0002-6675-2040
Letterkenny Institute of Technology, Ireland

Kevin Curran
Ulster University, UK

ABSTRACT

In this chapter, the authors examine the theoretical context for the security of wireless communication between ubiquitous computing devices and present an implementation that addresses this need. The number of resource-limited wireless devices utilized in many areas of the IT industry is growing rapidly. Some of the applications of these devices pose real security threats that can be addressed using authentication and cryptography. Many of the available authentication and encryption software solutions are predicated on the availability of ample processing power and memory. These demands cannot be met by most ubiquitous computing devices; thus, there is a need to apply lightweight cryptography primitives and

DOI: 10.4018/978-1-7998-7705-9.ch028

lightweight authentication protocols that meet these demands in any application of security to devices with limited resources. The analysis of the lightweight solutions is divided into lightweight authentication protocols and lightweight encryption algorithms. The authors present a prototype running on the nRF9E5 microcontroller that provides necessary authentication and encryption on resource-limited devices.

INTRODUCTION

Resource-Limited Wireless Device use is growing rapidly. This growth rate is expected to rise even higher when RFID transponders begin to replace Barcodes on a larger scale (Tanwar & Kumar, 2017). Some of the applications of these devices pose a security threat which can be addressed using cryptographic techniques (Kumawat et al., 2017). Most of the currently used cryptographic solutions are predicated on the existence of ample processing power and memory. These demands cannot be met by most ubiquitous computing devices, thus there is a need to apply lightweight cryptography primitives that meet security demands when considering devices with low resources.

A Risk Analysis of threats associated with the usage of Wireless Sensor Networks or RFID systems for the item-level stock control and temperature monitoring include the following:

- **Tag/Sensor Cloning:** A serious threat related to the counterfeiting of medicines with a high likely-hood of occurrence (Juels, 2005). Can be addressed with a strong encryption and authentication system.
- **Tag/Sensor Tracing:** A threat related to unauthorised Track & Trace of a Sensor/Tag movement throughout a given area, which has negative privacy implications. It can be addressed with a proper Authentication system that does not allow the disclosure of a Tag's/Sensor's unique ID (Sing et al., 2017).
- **Data Eavesdropping:** Unauthorized retrieval of sensor/tag data. A strong encryption algorithm provides a counter-measure to this threat (McBrearty et al., 2016).
- **Denial of Service Attack:** Affects the operation of the entire network or a group of Tags/Sensors. The likely-hood of occurrence can be regarded as medium. Such an attack would require appropriate hardware and in-depth knowledge of the radio protocol used. A proper Authentication system provides counter-measures to this threat.
- **Rogue-Data Injection:** An adversary can inject malicious data into the network causing improper configuration of the sensors for example. The probability of occurrence can be low as this kind of attack is not valuable to an adversary in most cases. A Mutual-Authentication system prevents accepting rogue data from unknown sources.
- **Cryptanalysis Attack:** Secret key discovery through a cryptanalysis attack on the authentication and/or encryption system's secret data. Such an attack compromises the whole security and leads to a full disclosure of all data. The likelihood of such an event is very low if the encryption key-space is large enough to prevent brute-force attacks (assumes unbreakable algorithm).

Figure 1 illustrates an example of a Risk Analysis concerning the threats associated with the usage of Wireless Sensor Networks or RFID systems for the item-level stock control and temperature monitoring. Typically, the application of security to wireless networks, such as the Wi-Fi Protected Access specifica-