Chapter 9

Security Aspects in Radio Frequency Identification Systems

Győző Gődor
Budapest University of Technology and Economics, Hungary

Sándor Imre
Budapest University of Technology and Economics, Hungary

ABSTRACT

Radio frequency identification technology is becoming ubiquitous, and as an unfortunate side effect, more and more authentication solutions come with more security issues. In former contributions, the authors introduced a solely hash-based secure authentication algorithm that is capable of providing protection against most of the well-known attacks and performs exceptionally well even in very large systems. The authors gave a theoretical analysis of Simple Lightweight Authentication Protocol (SLAP) protocol from security and performance point of view. This chapter gives a detailed examination of small computational capacity systems from the point of view of security. The authors define the model of attacker and the well-known attacks which can be achieved in these kinds of environments. Furthermore, the chapter gives a summary of the significant RFID authentication protocols which are found in literature. The authors present several lightweight authentication protocols and some novel elliptic curve cryptography based methods. Besides, the chapter illustrates the SLAP protocol’s performance characteristics with measurements carried out in a simulation environment and compares with the theoretical results. The authors show the effects of numerous attacks and the system’s different parameters on the authentication time. Finally, the chapter examines the performance and security characteristics of two other protocols chosen from the literature in order to compare to SLAP algorithm and give proper explanation for the differences between them.

DOI: 10.4018/978-1-61350-477-2.ch009
INTRODUCTION

In the last decade the RFID (Radio Frequency Identification) technology has developed apace. Accordingly, the usage of these systems is very widespread. RFID applications can be found in various fields of our common life, e.g. personal identification in passports, access control, thief prevention, payment systems, tickets for transportation, supply-chain management, asset tracking, retailing etc. Common RFID systems consist of three main functional units: Tags, Reader and Back-End. From these three parts the Tags possess the most vulnerable computational capacity. RFID systems operate via air-interface, which has numerous security risks. Since this medium can be easily accessed by everyone, the messages between the communicating parties can be observed, eavesdropped or forged and later the fake messages can be replayed. Furthermore, customers (possessing a Tag) can be tracked or their transactions can be recorded.

In order to prevent the unauthorized access to any kind of protected database or system, or any sensitive data, authentication and encryption have to be applied. As Back-End and Reader have higher performance and power properties, therefore the secure communication between them can be solved. However, Tags have very limited memory and very low computational capacity, therefore new solutions are needed, which require less operation and fewer messages. These methods are the so-called lightweight authentication protocols. These algorithms apply only hash functions and simple logical operations. There are a lot of lightweight protocols presented in the literature, however, each one has its drawbacks. The major weaknesses are the decrease of anonymity level and the necessity of very high computational capacity.

In (Gódor, Antal, & Imre, 2008) we have already introduced our SLAP protocol (Simple Lightweight Authentication Protocol) and we have given a detailed security analysis by which we verified the correctness of SLAP. Our solution provides an efficient mutual authentication method by which a given Tag and the Back-End can authenticate each other easily, quickly and securely even if large amount of Tags are stored in the database. The protocol can defy the well-known attacks and does not demand high computational capacity.

In (Gódor & Imre, 2009) we have already examined our proposed authentication method’s performance characteristics with measurements carried out in a simulation environment and these results were compared with the theoretical results.

In this contribution, which is an enhanced version of our formerly published article (Gódor & Imre, 2010), we give a detailed examination of small computational capacity systems from the point of view of security. We define the model of attacker and the well-known attacks which can be achieved in these kinds of environments. Furthermore, we give a detailed overview about the well-known lightweight and elliptic curve cryptography based authentication protocols which have already been proposed in the literature. Additionally, we propose our SLAP protocol again briefly and we introduce its security and performance characteristics. We show the effects of numerous attacks and the system’s different parameters on the authentication time. Finally, we examine the performance of two other protocols chosen from the literature in order to compare with SLAP algorithm and give proper explanation for the differences between them. For this reason we have implemented the SLAP protocol and the others in OMNeT++ so that we can make a comparison between them from the aspects of performance and security. We will prove that our protocol possesses better security and performance parameters than the other ones.
37 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

[Link to purchase]

This title is available in InfoSci-Books, InfoSci-Multimedia Technologies, Communications, Social Science, and Healthcare, InfoSci-Select, InfoSci-Media and Communication Science and Technology. Recommend this product to your librarian:

[Link to recommend to librarian]

Related Content

Slot Allocation Algorithms for Minimizing Delay in Alarm-Driven WSNs Applications

[Link to article]

Fairness Analysis and Improvement of Transport Layer Protocols

[Link to article]

Communication Networks to Connect Moving Vehicles to Transportation Systems to Infrastructure

[Link to article]

Evaluation of GALS Methods in Scaled CMOS Technology: Moonrake Chip Experience

[Link to article]