Journal of Network and Computer Applications 35 (2012) 826–843

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Privacy-friendly synchronized ultralightweight authentication protocols in the storm

Gildas Avoine, Xavier Carpent*, Benjamin Martin

Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium

ARTICLE INFO

Article history:
Received 16 February 2011
Received in revised form
25 July 2011
Accepted 1 December 2011
Available online 10 December 2011

Keywords:
Cryptography
Authentication
Radio frequency identification
Lightweight protocols
Privacy

ABSTRACT

In the recent years, there has been an increasing interest in the development of secure and private authentication protocols for RFID. In order to suit the very lightweight nature of RFID tags, a number of proposals have focused on the design of very efficient authentication protocols using no classical cryptographic primitives.

This article presents the state of the art in this field by summarizing this family of protocols and the most important attacks against them. The contribution also consists of a passive full-disclosure attack on the SASI and Yeh–Lo–Winata ultralightweight authentication protocols.

© 2011 Elsevier Ltd. All rights reserved.

1. Introduction

1.1. Forewords

Radio Frequency Identification (RFID) is a wide-sense concept that applies to low-resource devices (tags) that are remotely queryable when present in the vicinity of a reader. RFID can be used in a variety of applications such as supply chain management, access control, payment, retail inventory control or product tracking. For a mass deployment of RFID, the cost of the tags must be kept low, implying some very limited storage and computational capabilities.

In this work, we consider very low-cost tags where classical cryptographic primitives such as ciphers and hash functions cannot be used. The development of low-footprint protocols is thus needed. These must not only ensure authentication, but also privacy as the ubiquity of RFID may be perceived by the customers as a threat to their personal information. Indeed, RFID tags answer indiscriminately, and an attacker may capture some sensitive information, or trace the holder of a tag. Current proposals rely on bitwise operations, additions, or bit rotations (Chien, 2007; Peris-Lopez et., 2006a,b,c, 2009; David and Prasad, 2009; Lee et al., 2009; Yeh et al., 2010).

1.2. Contributions

In the following, we synthesize existing solutions in the field of synchronized ultralightweight mutual authentication protocols. We provide a clear description of each protocol and present the most important attacks on them. Up to our knowledge, this is the first comprehensive analysis and comparison of this family of protocols.

Additionally, we propose a passive full-disclosure attack on SASI that works with any definition of the rotation. Besides highlighting several weaknesses in the design of SASI, we develop an approach to attack ultralightweight authentication protocols, namely building progressive knowledge on a quantity given a series of observations. We also provide some tools to analyze equations mixing bitwise operations with additions and subtractions, which could prove useful in the cryptanalysis of other similar protocols. This second contribution is a revised version of Avoine et al. (2010), published in the proceedings of the RFIDSec 2010 workshop.

Finally, we present an efficient passive full-disclosure attack on the Yeh–Lo–Winata protocol, using the same technique than the attack on SASI.

1.3. Organization

This paper is organized as follows. In Section 2, we provide some background in RFID and authentication. Readers familiar with these topics may wish to proceed directly to Section 3, which introduces the framework of the analyzed protocols. Section 4

* Corresponding author. Tel.: +32 10479102.
E-mail addresses: gildas.avoine@uclouvain.be (G. Avoine), xavier.carpent@uclouvain.be (X. Carpent), benjamin.martin@uclouvain.be (B. Martin).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.12.001

consists in the state of the art in the field of synchronized ultralightweight protocols. It presents the protocols of the UMAP family and the SASI, the Gossamer, the David–Prasad, the Lee–Hsieh–You–Chen and the Yeh–Lo–Winata protocols, as well as the main results to date in their cryptanalysis. In Section 5, we present our attack on the SASI protocol, and our method of analysis of equations mixing bitwise operations with additions and subtractions. We present our attack on the Yeh–Lo–Winata protocol in Section 6. Finally, we conclude in Section 7.

2. Preliminaries

2.1. RFID in a nutshell

An RFID system consists of three main entities (Weis, 2003): a tag, a reader, and a back-end system.

The tag (or transponder) typically has a microchip for computation and storage and an antenna for communication. It is attached to an object or person, and is uniquely identifiable in the RFID system. Characteristics such as computational power, storage capabilities, or communication distance, strongly vary with price and usage, but are usually very limited. They can be split in two main categories: active and passive tags. Active tags contain a small battery used for computation and communication, and are usually much more powerful and expensive than passive ones. Passive tags rely exclusively on the reader's electromagnetic field to perform computation and communication operations.

A reader (or transceiver) communicates with RFID tags, in order to perform identification and authentication. As stated above, they provide most of the power used by a tag, and usually have much larger computational capabilities. Depending on the protocol used, they may perform heavy computation, such as cryptographic calculation, on behalf of the tag.

The back-end system stores records associated with tag contents. In the physical world, it is usually connected to many readers in an RFID system. However most analyses assume that the communication channel between a reader and the back-end system is *secure*, to the point that we usually consider that the reader and the database are only one entity.

2.2. Threats in RFID

We can roughly divide attacks into four categories: denial of service, impersonation, information leakage, and malicious traceability. Other threat classifications exist (Chatmon et al., 2006; Thompson et al., 2006), but we will focus on the following attack types.

2.2.1. Denial of service

This attack occurs when an adversary attempts to prevent the application to function properly. In the framework of RFID, this can be done using various techniques such as using blocker tags (Juels et al., 2003), introducing electromagnetic noise on the channel, etc. Electronic DoS attacks are extremely difficult to avoid, but are usually not taken into account in the security analysis of authentication protocols. This is due to the fact that they are often applicable regardless of protocol details. Some types of denial of service attacks are due to weaknesses in the protocol design, though. For instance, desynchronization attacks in stateful protocols make further authentication of a tag–reader pair impossible. In this specific case, other attacks are sometimes possible after a tag–reader pair has been desynchronized. This kind of DoS attacks must be taken into account in the analysis of authentication protocols.

2.2.2. Impersonation

This attack consists in being authenticated as someone else without being authorized to do so. This can be achieved by replay attacks, for instance, or any other weakness in the protocol, including those that allow an attacker to acquire knowledge of the secret of a tag (key recovery). The attacker can then disguise an expensive product into a cheap one, or gain access to restricted areas.

2.2.3. Information leakage

This problem appears as a scenario in which an attacker gains information deemed private on the product or the tag holder. For instance, an attacker could get the user's specifics, such as his SSN, address, etc. She could for instance acquire the identity of a user's personal belongings, in order to spot a potential robbery victim. Other possible reasons are political, industrial, or personal espionage, blackmailing, etc. Information leakage is usually prevented by mapping a real product or person ID in the database by an anonymous ID in the tag, which only the database can pair.

2.2.4. Malicious traceability

This attack has somewhat less dangerous consequences, but it is also the hardest problem to deal with. It consists in tracing a tag (and its holder) and therefore violating user's location privacy (in space and time). This can be performed if the attacker is able to find a correlation between authentication sessions of a tag. This is especially hard to prevent, because the response of the tag must change with each session and have negligible correlation with previous (and future) responses. Again, many privacy models have been proposed (Avoine, 2005; Canard et al., 2010; Juels and Weis, 2007; Vaudenay, 2007), but two characteristics are usually required: *indistinguishability* (Ohkubo et al., 2003) (or *untraceability* Avoine, 2005), and *forward security* (Ohkubo et al., 2003) (or *forward untraceability*, Avoine, 2005). Untraceability is the fact that an adversary is not able to tell two tags apart, given a set of authentication sessions of these tags. Forward untraceability is the fact that if an adversary acquires the secret of a tag, she is not able to trace past authentication sessions of that tag.

These two last attacks are to be prevented when designing protocols for which privacy is a concern.

3. Synchronized ultralightweight authentication protocols

Classical challenge–response protocols used in symmetric-key cryptography are stateless. Therefore, they cannot be applied in scenarios where forward untraceability is required. Indeed, in order to ensure it, it should be impossible for an attacker to guess a tag's past secret given its current one, because this would allow him to identify past public messages of that tag. Since secrets of a tag do not change in a stateless protocol, guessing previous secrets is straightforward.

This fact indicates the use of *synchronized* protocols, that is protocols in which both the prover and the verifier share a secret that is variable and forms the *state* of the prover/verifier pair. This stateful property implies that the two entities are synchronized, and since keys are variable, they have to be the same in both the prover and the verifier.

3.1. Synchronized protocols

There have been several proposals using this approach recently, like OSK (Ohkubo et al., 2003), O-FRAP/O-FRAKE (van Le et al., 2007), YA-TRAP (Tsudik, 2007), C^2 (Canard and Coisel, 2008), or PFP (Berbain et al., 2009), as well as a series of ultralightweight protocols using index pseudonyms (see Section 3.3).

Download English Version:

https://daneshyari.com/en/article/457372

Download Persian Version:

https://daneshyari.com/article/457372

Daneshyari.com