Journal of Network and Computer Applications 34 (2011) 833–845

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Flaws on RFID grouping-proofs. Guidelines for future sound protocols

Pedro Peris-Lopez [a,*], Agustin Orfila [a,b], Julio C. Hernandez-Castro [c], Jan C.A. van der Lubbe [a]

[a] Information Security and Privacy Lab, Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, P.O. Box 5031, 2600 GA, Delft, The Netherlands
[b] Department of Computer Science, Carlos III University of Madrid, Leganes, Madrid 28911, Spain
[c] School of Computing, Buckingham Building, Lion Terrace, Portsmouth PO1 3HE, UK

ARTICLE INFO

Article history:
Received 31 October 2009
Received in revised form
25 March 2010
Accepted 28 April 2010
Available online 7 May 2010

Keywords:
RFID
Grouping-proof
Security
Privacy
Cryptanalysis

ABSTRACT

During the last years many RFID authentication protocols have been proposed with major or minor success (van Deursen and Radomirović, 2008). Juels (2004) introduced a different and novel problem that aims to evidence that two tags have been simultaneously scanned. He called this kind of evidence a yoking-proof that is supposed to be verifiable offline. Then, some authors suggested the generalization of the proof for a larger number of tags. In this paper, we review the literature published in this research topic and show the security flaws of the proposed protocols, named RFID grouping-proofs generally. More precisely, we cryptanalyze five of the most recent schemes and we also show how our techniques can be applied to older proposals. We provide some guidelines that should be followed to design secure protocols and preclude past errors. Finally, we present a yoking-proof for low-cost RFID tags, named Kazahaya, that conforms to the proposed guidelines.

1. Introduction

A typical RFID system consists of three different types of entities: tags, readers and a verifier. The tags are embedded in, or attached to, objects to be identified. The most expensive are active, i.e. have power supply (usually a battery) that is used to energize the microchip's circuitry and to broadcast a signal to the reader. As they have their own power source, active tags support large memory and processing capabilities. Semi-passive tags, which are also too expensive to place on low-cost items, use a battery to run the microchip's circuitry but communicate by drawing power from the reader. The remaining ones are passive, i.e., have no internal power source neither to energize the microchip nor to communicate to the reader. Thus, the computation and communication capabilities of the latter are very limited. Nevertheless, it is generally assumed that they are able to perform basic cryptographic operations such as generating pseudo-random numbers and evaluating pseudo-random functions (Burmester et al., 2008). RFID tags do not have clocks. However, the activity time of a tag during a single session can be limited using techniques such as measuring the discharge rate of capacitors, as described in Juels (2004). Accordingly timeouts can be implemented on RFID passive tags. FCC regulations require the termination of tag-reading within 400 ms. The readers provide power to the tags in order to communicate with them. The verifier (a back-end server) is a trusted entity that maintains a database containing the information needed to identify tags (e.g. their unique identifiers and their secret keys).

A grouping-proof is an evidence that two or more RFID tags were scanned simultaneously by a reader within its broadcast range. For example, in the pharmaceutical sector, it can prove that a medicine has been sold with its prescription or with the patient information leaflet. The proof should be verifiable by the corresponding verifier. During a grouping-proof protocol execution, the verifier can be in two different modes: online or offline. In the first mode the verifier can send and receive messages from specific tags (via the reader) throughout the protocol execution. In contrast, in offline mode the verifier can only broadcast challenges to the reader. Thus, the verifier in offline mode never unicasts messages to tags. Although it is straightforward to design solutions for the online mode (indeed a proper RFID authentication protocol is enough (Chien et al., 2010), some research has focused on the protocol design for this mode (Leng et al., 2009; Huang and Ku, 2009; Chien et al., 2010). Nevertheless, the interesting case is the offline mode because it does not need the persistent presence of the verifier to generate grouping-proofs.

Some assumptions are generally accepted for the design of grouping-proofs (Burmester et al., 2008):

- RFID readers are potentially untrusted. The only trusted entity is a verifier.

* Corresponding author. Tel.: +31 15 27 87241.
E-mail addresses: P.PerisLopez@tudelft.nl (P. Peris-Lopez), A.OrfilaDiazPabon@tudelft.nl (A. Orfila), Julio.Hernandez-Castro@port.ac.uk (J.C. Hernandez-Castro), J.C.A.vanderLubbe@tudelft.nl (J.C. van der Lubbe).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.04.008