Journal of Network and Computer Applications 34 (2011) 853–863

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

An optimal probabilistic solution for information confinement, privacy, and security in RFID systems

Roberto Di Pietro [a,b,*], Refik Molva [c]

[a] UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Tarragona, Spain
[b] Università di RomaTre, Dipartimento di Matematica, L.go S. L. Murialdo n. 1 00149, Roma, Italy
[c] Institut EURECOM, 2229 route des crêtes, BP 193, F-06560, Sophia-Antipolis cedex, France

ARTICLE INFO

Article history:
Received 1 November 2009
Received in revised form
10 April 2010
Accepted 28 April 2010
Available online 11 May 2010

Keywords:
RFID systems
Information confinement
Security
Privacy
Probabilistic algorithm

ABSTRACT

In this paper, we provide the following contributions to enhance the security of RFID based systems. First, we assume that among multiple servers storing the information related to the tags some of them can be compromised. For this new threat scenario, we devise a technique to make RFID identification server dependent, providing a different unique secret key shared by a tag and a server. The solution proposed requires the tag to store just a single key, thus fitting the constraints on tag's memory. Second, we provide a probabilistic tag identification scheme that requires the server to perform just bitwise operations and simple list manipulation primitives, thus speeding up the identification process. The tag identification protocol assures privacy, security and resilience to DoS attacks thanks to its stateless nature. Moreover, we extend the tag identification protocol to achieve mutual authentication and resilience to replay attacks. The proposed identification protocol, unlike other probabilistic protocols, never rejects a legitimate tag. Furthermore, the identification protocol requires the reader to access the local database (DB) of tags' keys $O(n)$ times—where n is the number of tags in the system—while it has been shown in the literature that a privacy preserving identification protocol requires a reader to access $\Theta(n)$ times this DB. In this sense, our protocol is optimal. Finally, the three features suggested in this paper, namely, reader-dependent key management, tag identification, and mutual authentication, can be independently adopted to build alternative solutions.

1. Introduction

Radio Frequency IDentification (RFID) is a technology for automated identification of objects and people. An RFID device, also known as *tag*, is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. The applications of RFID range from cattle monitoring to e-passport (Juels, 2006). Further, the advantages provided by RFID technology (e.g. inventory visibility and business process automation) are also pushing towards the design, implementation, and deployment of large-scale RFID infrastructures (Mo et al., 2009).

The other components of an RFID system are readers and servers. A reader is a device querying tags for identification information, while all information about tags (ID, assigned keys, etc.) are maintained on servers. A server can be assigned multiple readers; in this case it only engages in communication with its constituent readers. It is generally assumed to have a single logical server that might resolve to multiple physically replicated servers. All communications between server and readers is assumed to be over private and authentic channels. Both readers and server do not suffer of constraints on power, processing, memory, and bandwidth.

Furthermore, based on a widely agreed assumption, servers, readers and the link between them are assumed to be trusted in that only the tags and the communication channel between the tag and the readers are assumed to be potentially vulnerable to malicious attacks (Juels, 2006; Tsudik, 2006). In this paper, we relax this hypothesis by assuming a more general setting whereby tags, servers and readers can be subject to malicious attacks. In that context, we focus on the problem of tag identification by multiple servers that are either replicas of the same logical server or different servers governed by independent authorities. As a result of the relaxed security hypothesis, the new requirement in this setting is to cope with the compromise of servers. Apart from the obvious need to perform mutual authentication, as opposed to one-way authentication of the tag by the server, server compromise calls for new measures to prevent possible attacks originating

[*] Corresponding author at: Università di Roma Tre, Dipartimento di Matematica, L.go S. L. Murialdo n. 1 00149, Roma, Italy. Tel.: +39 3293758764.
E-mail addresses: roberto.dipietro@urv.cat, dipietro@mat.uniroma3.it (R. Di Pietro), molva@eurecom.fr (R. Molva).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.04.015