Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 7 (2009) 136–152
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Public key cryptography based privacy preserving multi-context RFID infrastructure ☆

Selim Volkan Kaya, Erkay Savaş [1], Albert Levi [*,2], Özgür Erçetin

Faculty of Engineering and Natural Sciences, Sabancı University, Orhanli, Tuzla, 34956 Istanbul, Turkey

Received 7 November 2007; accepted 31 December 2007
Available online 1 February 2008

Abstract

In this paper, we propose a novel radio frequency identification (RFID) infrastructure enabling multi-purpose RFID tags realized by the use of privacy preserving public key cryptography (PKC) architecture. The infrastructure ensures that the access rights of the tags are preserved based on the spatial and temporal information collected from the RFID readers. We demonstrate that the proposed scheme is secure with respect to cryptanalytic, impersonation, tracking, replay, and relay attacks. We also analyze the feasibility of PKC implementation on passive class 2 RFID tags, and show that the requirements for PKC are comparable to those of other cryptographic implementations based on symmetric ciphers. Our numerical results indicate PKC based systems can outperform symmetric cipher based systems, since the back end servers can identify RFID tags with PKC based systems approximately 57 times faster than the best symmetric cipher based systems.

Keywords: RFID; Privacy; Security; Public key cryptography; Spatio-temporal attacks

1. Introduction

Remote identification of objects based on radio signals is welcomed with an enthusiastic acceptance in various numbers of applications due to its ease of use and efficiency. Compared with previous technologies for object identification such as barcodes and smart cards, radio frequency identification (RFID) does not require the objects to be in the line of vision. The amount and variety of information that can be stored in an RFID tag are unimaginable in the traditional technologies. These features render the use of RFID tags as popular (and inevitable to a great extent) in large and diverse set of applications such as supply chain, toll collection, payment

☆ A preliminary version of this work has been presented at IFIP Networking 2007 Conference, held in Atlanta, Georgia, May 14–18, 2007.

* Corresponding author. Tel.: +90 216 483 9563; fax: +90 216 483 9550.
E-mail addresses: selimvolkan@su.sabanciuniv.edu (S.V. Kaya), erkays@sabanciuniv.edu (E. Savaş), levi@sabanciuniv.edu (A. Levi), oercetin@sabanciuniv.edu (Ö. Erçetin).

[1] Erkay Savaş is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under project number 105E089.
[2] Albert Levi is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under project number 104E071.

1570-8705/$ - see front matter © 2008 Published by Elsevier B.V.
doi:10.1016/j.adhoc.2007.12.004

tokens, etc. A common characteristic of these RFID-based applications is that the tags are used for a single purpose and in a single context, in the sense that only designated readers can challenge/query the tags. This does not necessarily prevent other unauthorized readers from participating in privacy-violating activities such as tracking the movements of the tags, and hence, the individuals associated with them.

Therefore, the usage of RFID in a single context puts certain limitations on the versatility of the tags while adding to the privacy problems. For instance, if an object needs to be identified by different readers for different purposes, multiple RFID tags are required for the same object. However, this approach is clearly not scalable, since not only attaching multiple tags increases the cost of the system, but also makes the management of multiple tags more difficult. Moreover, privacy breaches are more likely to occur with multiple tags, since the attacker has more opportunities to track the movement of the object.

In this paper, we propose a multi-purpose RFID infrastructure, where a single RFID tag is interrogated by various readers for different purposes. This infrastructure is more flexible, since in real life an object does not have a single purpose in a single isolated context, but it is related to multiple parties in some way as a result of cooperative and collaborative structure of the society. For example, consider the example given in Fig. 1, where an RFID tag is used to identify the individuals. In this example, the same RFID tag can be queried in different sites for different purposes. The police department should be able to identify each person to find out whether that person has a crime record or not. The hospital should be able to identify each person in case of health emergency to learn about previous health record of that person. The security department of a building should identify the person to decide whether to give her access to the building. We can easily extend this example with tens of different usage scenarios, where the identification of a person or object (e.g., car) is needed. From the scenarios outlined above, each party with a reader queries the RFID tag to retrieve information of interest for the person or object whose identification information is stored in the tag. Clearly, there must be some rules and limitations that govern the kind of information, and the circumstances under which this information can be obtained for the individuals.

As demonstrated in the previous example, increasing the versatility of RFID tags by enabling multi-purpose access by different parties emphasizes the importance of privacy. Note that RFID tags can provide access to a large amount of private information which may be compromised if the access rights of each querying party are not clearly defined, and if the RFID infrastructure is vulnerable to security attacks. In this work, we address several security

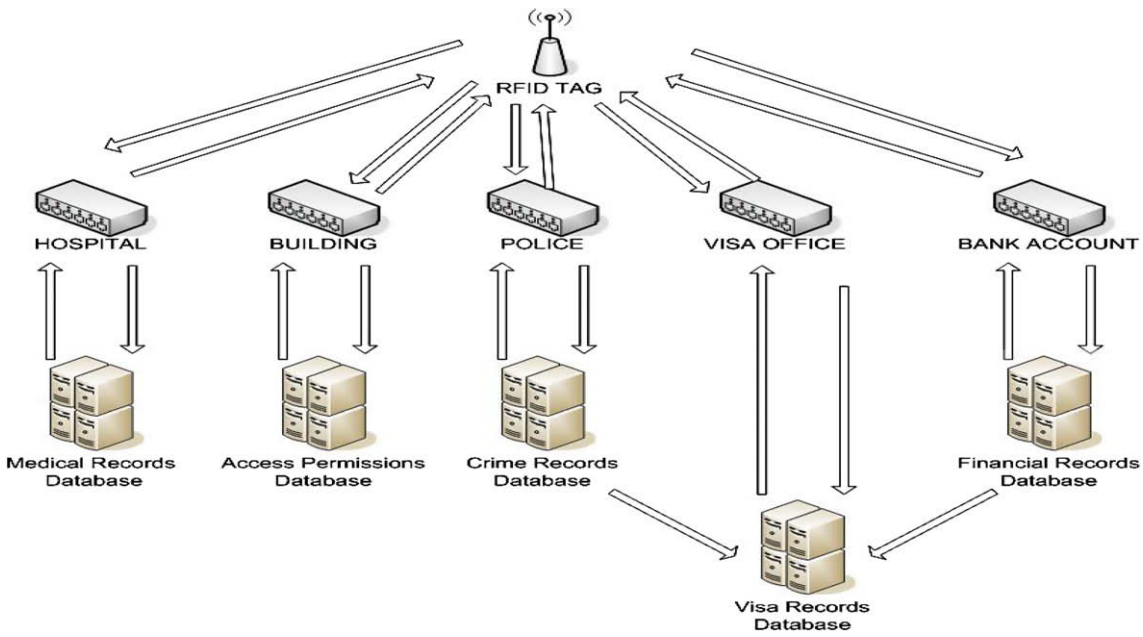

Fig. 1. Multi-context RFID infrastructure.