Computer Communications 88 (2016) 84–88

Contents lists available at ScienceDirect

Computer Communications

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

Attacks on ownership transfer scheme for multi-tag multi-owner passive RFID environments

J. Munilla[a,*], M. Burmester[b], A. Peinado[a]

[a] E.T.S.I. Telecomunicación, Universidad de Málaga, Málaga, Spain
[b] Department of Computer Science, Florida State University, Tallahassee, Florida, USA

ARTICLE INFO

Article history:
Received 20 November 2014
Revised 24 June 2015
Accepted 14 May 2016
Available online 16 May 2016

Keywords:
RFID
EPCC1G2
Ownership transfer
Cryptanalysis

ABSTRACT

Sundaresan et al. proposed recently a novel ownership transfer protocol for multi-tag multi-owner RFID environments that complies with the EPC Class1 Generation2 standard. The authors claim that this provides individual-owner privacy and prevents tracking attacks. We show that this protocol falls short of its security objectives, and describe attacks that allow: (*a*) an eavesdropper to trace a tag, (*b*) the previous owner to obtain the private information that the tag shares with the new owner, and (*c*) an adversary that has access to the data stored on a tag to link this tag to previous interrogations (violating forward-secrecy). We analyze the security proof and show that while the first two cases can be addressed with a more careful design, strong privacy remains an open problem for lightweight RFID applications.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

The term "Internet of Things" (IoT) was coined in 1999 by Kevin Ashton, a cofounder of the Auto-ID [1] center that promoted the development of tracking products for supply-chain management by using low-cost RFID tags. RFID tags and sensors enable computers to observe, identify and understand situational awareness without requiring human intervention. Initial designs focused on performance with less attention paid to resilience and security. However this technology is currently used in many applications that need to be protected. Protection must take into account the special features of RFID, such as the vulnerabilities of the radio channel, power-constraints, low-cost, limited functionality, reply upon request, as well as resistance to the risks of RFID, such lack of privacy, malicious traceability and data corruption. The increasing concern with security is evidenced by the inclusion of some optional cryptographic features in the recently ratified second version of the EPCglobal Gen2 specificiations [2].

Ownership Transfer Protocols (OTPs) allow the secure transfer of tag ownership from a current owner to a new owner. They support distributed RFID applications and are a basic component of the IoT. Three entities are present in an OTP: the tag $\mathcal{T}$, whose rights are being transferred, the current owner, who has the initial control of $\mathcal{T}$, and the new owner, who will get control of $\mathcal{T}$ when the protocol is completed. OTPs must incorporate security requirements that protect the privacy of both the new and the previous owner of the tag. To prevent previous owners from accessing a tag once ownership has been transferred either a Trusted Third Party (TTP) is employed or an Isolated Environment (IsE). The first provides security for stronger adversarial scenarios while the second is more appropriate when tags belong to independent authorities.

For RFID applications privacy addresses *anonymity* that protects the identity of tags, and *untraceability* that protects past interrogations (partial or completed) of a tag being linked. Formal definitions for secure ownership and ownership transfer are provided by van Deursen et al. [3] while several theoretical models have been proposed in the literature to address the privacy of RFID systems [4–7]. The theoretical framework of Vaudenay [7] distinguishes between strong and weak attackers. Privacy preserving protocols against strong adversaries support *forward secrecy* [8].

Molnar et al. [9] and Saito et al. [10] presented the first OTP for RFID applications in 2005. This was followed by several OTPs that address practical scenarios. Recently Sundaresan et al. [11] proposed an OTP for multi-tag multi-owner RFID environment that provides individual-owner-privacy. The protocol uses a TTP for secure management and an IsE for verifying ownership transfer. This complies with the EPCglobal Gen2 specifications, with protection afforded by simple XOR and 128-bit PRNGs. The protocol is claimed to provide tag anonymity, tag location privacy, forward secrecy, and forward untraceability; while being resistant to replay, desynchronization, server impersonation and active attacks. We shall show in this paper that this protocol falls short of these claims. In particular that it is subject to:

* Corresponding author.
E-mail address: munilla@ic.uma.es (J. Munilla).

http://dx.doi.org/10.1016/j.comcom.2016.05.007
0140-3664/© 2016 Elsevier B.V. All rights reserved.

Trusted Third Party $(ST_s, T_{id_j}, O_{id_i}, N_{s_i})$	Each Tag j in Tag-Group $(ST_s, ST'_s, T_{id_j}, O_{id_i}, OT_{s_i}, OT'_{s_i})$
Step 2A Generate $S1_r$ Generate a new Tag-Group secret ST_{sn} For each New Owner i $M5_i = N_{s_i} \oplus PRNG(ST_s \oplus S1_r)$ $M6_i = O_{id_i} \oplus PRNG(N_{s_i} \oplus ST_s \oplus S1_r)$ $M^c_i = PRNG(M5_i \oplus S1_r \oplus ST_{sn}) \oplus PRNG(M6_i \oplus ST_s)$ Next Owner For each Tag j in Tag-Group $M7_j = T_{id_j} \oplus PRNG(T_{id_j} \oplus ST_s \oplus S1_r)$ $M8_j = S1_r \oplus PRNG(T_{id_j} \oplus ST_s)$ $M9_j = ST_{sn} \oplus PRNG(M7_j \oplus T_{id_j} \oplus ST_{sn})$ $\xrightarrow{M5_{(1..i)}, M6_{(1..i)}, M7_j, M8_j, M9_j, M^c_{(1..i)}}$ Next Tag **Step 2C** For each Tag's reply $T1_r \leftarrow RND_t \oplus T_{id_j} \oplus ST_s$ If $T_{id_j} \oplus (O_{id} \| N_i)_{(1..i)} = ACK_t \oplus PRNG(ST_s \oplus T1_r)$ Tag Authenticated New Owners & Secrets Successfully Inserted If ALL_ACK NOT Received then Goto Step 2A else $ST_s \leftarrow ST_{sn}$	**Step 2B** $S1_r \leftarrow M8_j \oplus PRNG(T_{id_j} \oplus ST_s)$ if $T_{id_j} = M7_j \oplus PRNG(T_{id_j} \oplus ST_s \oplus S1_r)$ TTP Authenticated & Message is for this tag else Use ST'_s in the above steps and try again; if unsuccessful, abort. $ST_{sn} \leftarrow M9_j \oplus PRNG(M7_j \oplus T_{id_j} \oplus ST_s)$ For all i if $PRNG(M5_i \oplus S1_r \oplus ST_{sn}) \oplus PRNG(M6_i \oplus ST_s) = M^c_i$ $N_{s_i} \leftarrow M5_i \oplus PRNG(ST_s \oplus S1_r)$ $O_{id_i} \leftarrow M6_i \oplus PRNG(N_{s_i} \oplus ST_s \oplus S1_r)$ else abort Remove Previous Owner's IDs & Secure Secrets from Tag Insert $O_{id_{(1..i)}}, OT_s \leftarrow N_{s_{(1..i)}}, OT'_s \leftarrow N_{s_{(1..i)}}$ Generate $T1_r$ $RND_t = T1_r \oplus T_{id_j} \oplus ST_s$ $ACK_t = T_{id_j} \oplus (O_{id} \| OT_s)_{(1..i)} \oplus PRNG(ST_s \oplus T1_r)$ $\xleftarrow{RND_t,\ ACK_t}$ If T_{id_j} matches using ST_s $ST'_s \leftarrow ST_s$ $ST_s \leftarrow ST_{sn}$

Fig. 1. Step 2 of the Sundaresan *et al.* protocol.

(a) De-synchronization and/or replay attacks (Theorem 1);
(b) Traceability (tag location privacy) attacks: an eavesdropper can trace a tag (Theorems 2, 3);
(c) Impersonation attacks: a previous owner can compute the secret data that tags share with the new owner (Theorems 4, 5);
(d) Forward secrecy attacks: compromised tags can be linked to earlier interrogations (Theorem 6);
(e) De-synchronization attacks: if the shared secrets are generated using a random non-deterministic process (Theorem 7).

The rest of the paper is organized as follows. Section 2 discusses the Sundaresan et al. protocol and describes the phase that is cryptanalyzed. Section 3 describes the security flaws listed above. Section 4 analyzes the cryptographic causes of these weaknesses and Section 5 concludes the paper.

2. The Sundaresan et al. ownership transfer protocol

This is a TTP-based scheme developed for multi-tag multi-owner RFID environments [11]. Two kinds of associations are considered: tags with multiple owners and owners with multiple tags. Every tag and owner is setup with identifiers and several shared and private secrets in the initialization phase. The protocol begins when a group of owners sends an ownership transfer (OT) request to the TTP. The protocol has two steps: Step 1 involves the TTP and new owners while Step 2 involves the TTP and the tags in Tag-Group, and is intended to transfer the identifiers of the new owners and the secret keys to the tags. In this paper we are only concerned with Step 2, since our analysis will focus on its weaknesses. This step is shown in Fig. 1, and is described below. For convenience we use the abbreviations $(O_{id}||OT_s)_{(1..i)}$ for $(O_{id_1}||OT_{s_1}) \oplus (O_{id_2}||OT_{s_2}) \oplus \cdots \oplus (O_{id_i}||OT_{s_i})$.

2.1. Step 2 of the Sundaresan et al. OTP: TTP → Tag-Group → TTP

TTP uses the values: $\{ST_s, T_{id_j}, (O_{id}, N_s)_{(1..i)}\}$, with ST_s a secret shared with Tag-Group, T_{id_j} an identifier for tag j in Tag-Group, O_{id_i} an identifier for each new owner i of tag j, and N_{s_i} a new secret for this owner.

Each tag j in Tag-Group uses the values: $\{ST_s, ST'_s, T_{id_j}, (O_{id}, OT_s, OT'_s)_{(1..i)}\}$, with ST'_s the value of ST_s used in the previous interaction (initially $ST_s = ST'_s$), and O_{id_i}, OT_{s_i} and OT'_{s_i} the identifier of its (previous) owner i, and the current and the previous secret shared with this owner. The execution of the protocol will result in the updating of these later values.

Step 2A TTP generates a pseudorandom number $S1_r$ and a new secret ST_{sn} to be shared with the tags in Tag-Group. Then TTP computes:
for each new owner i,
$M5_i = N_{s_i} \oplus PRNG(ST_s \oplus S1_r)$, $M6_i = O_{id_i} \oplus PRNG(N_{s_i} \oplus ST_s \oplus S1_r)$ and $M^c_i = PRNG(M5_i \oplus S1_r \oplus ST_{sn}) \oplus PRNG(M6_i \oplus ST_s)$,
and for each tag j,
$M7_j = T_{id_j} \oplus PRNG(T_{id_j} \oplus ST_s \oplus S1_r)$, $M8_j = S1_r \oplus PRNG(T_{id_j} \oplus ST_s)$, and $M9_j = ST_{sn} \oplus PRNG(M7_j \oplus T_{id_j} \oplus ST_s)$.
Then, TTP sends $M_{TG} = (M5_{(1..i)}, M6_{(1..i)}, M7_j, M8_j, M9_j, M^c_{(1..i)})$ to each tag j in Tag-Group:
TTP → Tag-Group: M_{TG}.

Step 2B Each tag j in Tag-Group checks if for its T_{id_j}: $T_{id_j} \stackrel{?}{=} M7_j \oplus PRNG(T_{id_j} \oplus ST_s \oplus S1_r)$, where $S1_r = M8_j \oplus PRNG(T_{id_j} \oplus ST_s)$. If this fails it uses ST'_s instead of ST_s. If both fail, it aborts. Otherwise *TTP is authenticated* and the tag knows that the message is for itself. For the remainder of the protocol, either ST_s or ST'_s is used, depending on which one returned a match.
Tag j checks if for all i: $M^c_i \stackrel{?}{=} PRNG(M5_i \oplus S1_r \oplus ST_{sn}) \oplus PRNG(M6_i \oplus ST_s)$, where $ST_{sn} = M9_j \oplus PRNG(M7_j \oplus T_{id_j} \oplus ST_s)$. If this fails for some i, it aborts. Otherwise it computes $O_{id_i} = M6_i \oplus PRNG(N_{s_i} \oplus ST_s \oplus S1_r)$ and $N_{s_i} = M5_i \oplus PRNG(ST_s \oplus S1_r)$, and replaces the previ-

Download English Version:

https://daneshyari.com/en/article/449890

Download Persian Version:

https://daneshyari.com/article/449890

Daneshyari.com