Group-Scanning for Supply Chain Management

Mike Burmester, *Senior member, IEEE,* and Jorge Munilla

Abstract—The integrity of shipments in the supply chain may have to be tracked remotely by carriers that are not necessarily trusted. We present an RFID framework architecture for applications when multiple scanned tags generate concurrently a proof of "simultaneous" presence that cannot be forged by untrusted carriers.

Index Terms—Distributed RFID systems, supply chain management, grouping-scanning proofs.

1 Introduction

Radio Frequency Identification (RFID) is a wireless technology widely deployed for inventory, retail and supply chain management. There are many advantages of RFID over barcode technology: *e.g.*, RFID does not require line-of-sight alignment with readers for proper scanning and RFID tags can be interrogated at greater distances, faster and concurrently [1]. RFID tags and sensors can also be used to enable computers to observe/identify/understand for situational awareness without the limitations of a human in the loop. Furthermore RFID technology extends the scope of the Internet of Things to capture intelligent processes and cyber-physical applications.

Although initial designs of RFID protocols focused on performance and efficiency, this technology has found use in many applications that require the implementation of security mechanisms. The recent ratification of the standard Gen2v2 highlights these security concerns [2]. Several RFID authentication protocols that address security have been proposed in the literature. Most use hash functions [4], [5], [6], and others use pseudorandom functions [7], [8]. The Flyweight authentication protocol [9] is one of a few which only requires a pseudorandom number generator.

For supply chain management, RFID tags have to be tracked remotely. Ownership Transfer Protocols may be used but there are cases when the owner does not want to cede control. For example, the owner may use the services provided by a carrier who, in turn, uses other carriers. In such cases it is desirable that the owner and carrier can periodically check the integrity of a shipment of tagged products. This requirement is known as *group-scanning* and involves the tags of a group generating a proof of simultaneous presence in the range of an RFID reader [10].

There are several practical scenarios where group scanning can substantially expand the capabilities of RFID-based systems. For example, some products may need to be shipped together in groups and one may want to monitor their progress through the supply chain—*e.g.*, hardware components of a system or kits. Alternatively, safety regulations may require that drugs be shipped, or dispensed, together with information leaflets. Since public key cryptography is beyond the capability of most RFID tags, such proofs can only be checked by a verifier that shares private information with the group of tags (GoT).

Our main contribution in this paper is to:

a) Present a framework for group-scanning that addresses practical settings, in particular supply chain management.
b) Present a lightweight group-scanning proof that is generated concurrently by tags of a group without sharing any private information with the reader.

The organization of this paper is as follows. The literature is reviewed in Section 2. In Section 3 we discuss RFID deployments for supply chain management and present a high-level description of the security requirements and procedures for group scanning, and discuss the threat model. In Section 4 we propose two RFID protocols for group scanning: a non-anonymous group-scanning proof and a version that adds support for anonymity. In Section 5 we show how these can be integrated into RFID supply chain management systems.

- *M. Burmester is with the Department of Computer Science, Florida State University, Tallahassee, FL, 32306. E-mail: burmeste@cs.fsu.edu*
- *J. Munilla is with Universidad de Málaga, Campus de Excelencia Internacional Andalucía Tech. Spain, 29070.*

This material is partly based upon work supported by: Universidad de Málaga, Campus de Excelencia Internacional Andalucía Tech, Ministerio de Ciencia e Innovación and the European FEDER Fund under project TIN2011-25452, and the National Science Foundation Grants No. 1347113, 1241525 and 1027217.

2 Background

2.1 Group-Scanning Proofs

Ari Juels introduced in 2004 the security context of a new RFID application—which he called a yoking-proof [11], that generates evidence of simultaneous presence of two tags in the range of an RFID reader. This first protocol was later found to be insecure [12], but the simultaneous scanning application triggered considerable interest in the research community. Yoking-proofs have been extended to *group-scanning proofs* in which multiple tags prove simultaneous presence in the range of an RFID reader.

Burmester et al. presented a group-scanning proof that uses randomized pseudonyms and updates secret keys after each session for forward-secrecy [13]. This is essentially a proof-of-concept and not appropriate for lightweight applications. Huang and Ku [14] presented a group-scanning proof for low-cost tags that uses a pseudorandom number generator to authenticate flows and a cyclic redundancy code to randomize strings. This has several weaknesses, some of which were addressed by Chien et al. [15] who, in turn, proposed a new group-scanning proof. Peris-Lopez et al. [16] found other security flaws in these protocols and proposed security guidelines. More recently, Liu et al. proposed a group-scanning proof for multiple readers and tags [10]. This proof requires the reader to be a contributing party that shares private keys with the tags of the group.

3 A Group-Scanning Architecture

3.1 Group-Scanning Deployments

A typical deployment of an RFID supply chain involves three types of legitimate entities.

a) A *group of tags* (GoT).
b) The *owner* of GoT, who keeps the digital rights of the tags; in particular the owner knows the private information stored by the tags.
c) The *carrier*, whose services are contracted by the owner. The carrier has physical possession of the GoT, can access it through his reader(s) and should be able to check its integrity, but does not have control over it.

3.2 Group-Scanning Capabilities

We assume the following regarding the environment that characterizes RFID group-scanning applications.

3.2.1 RFID Tag Capabilities

Passive UHF tags are the most common for supply chain applications. They have no power of their own, operate in the far assumptfield, and use backscatter communication. Such tags work at greater distances (than inductive tags) but the delivered power is low, and therefore lightweight cryptographic tools should be utilized. However, we shall assume that tags are able to perform basic symmetric-key cryptographic operations such as selecting pseudorandom numbers and evaluating a pseudorandom function.

Public key cryptography, tamper-resistant shielding and on-board clocks are beyond the capabilities of most tags. However, the activity time span of a tag during a single session can be limited using techniques such as measuring the discharge rate of capacitors [11].

3.2.2 RFID Reader and Verifier/Server Capabilities

Readers and verifiers/servers are able to perform complex cryptographic operations. Although in practice these may be implemented on the same device with two communication ports, in our model we shall regard them as independent. In particular, readers just manage the communication between tags, and interface between the verifier and the GoT.

3.2.3 RFID Communication Channels

Tags can only communicate with readers that are in wireless range (they backscatter the reader's electromagnetic signal). Thus, direct communication between passive RFID tags is not possible. However readers can establish logical wireless channels that link the tags of a group.

To establish a channel, the tags must provide the reader with identifying origin information to define an association. After the tags get identified (not necessarily authenticated), they get linked with a wireless communication channel via the reader (in practice: origin and destination tag information is appended to all exchanged messages). We shall not discuss physical/link layer details such as the coupling design, the power-up and collision arbitration processes. For details on these issues the reader is referred to [2].

RFID wireless channels are particularly vulnerable because tags are restricted to lightweight cryptographic protection. By contrast, the communication channel between high level entities (readers and verifiers) is secure since fully-fledged cryptographic techniques can be used.

3.2.4 Integrity of Group-Scanning Proofs

A group-scanning proof provides evidence of temporal events that corroborate the "simultaneous" presence of a GoT. Let G be a non-compromised GoT and R an authorized reader. There are two basic integrity requirements regarding interrogation evidence and how it is compiled:

- (*Completeness*) If all tags of G are in range of R within the same time window then a group-scanning proof is generated.
- (*Soundness*) If when R interrogates the tags of G a group-scanning proof is generated then all tags of G were scanned by R.

Fig. 5. An anonymous group-scanning proof

PHASE 1

READER $\rightarrow *:$ r_{sys} (a random number)

PHASE 3

For each $1 < i \leq n$

tag_i: Set timer; execute Triangle protocol as root & passive child.
If successful (within timeout) as a root then become an active child at the higher level.

tag_1: Set timer and execute Triangle protocol (as root)
If successful, then compute $mac = f(k; ID_{gp}||r_{sys})$
$tag_1 \rightarrow$ READER: mac ; timeout
else timeout

READER: If mac is received from tag_1 then compile:
$MAC = (r_{sys}, mac)$

are equally likely. If $\mathcal{A}$ decides correctly then $Exp_{\mathcal{A}}$ outputs 1, otherwise it outputs 0.

For *u*nlinkability we require that, $\forall$ PPT $\mathcal{T}$; $\forall$ PPT $\mathcal{R}$; $\forall$ pair of interrogations $int1$, $int2$: $\nexists$ a PPT $\mathcal{A}$ such that, $Pr\left[Exp_{\mathcal{A}} = 1\right] > \frac{1}{2} +$ negligible.

Session unlinkability [9] is a weak form of unlinkability for which we require additionally that either $int1$ completed, or $int1, int2$ are separated by a completed interrogation involving the tag of $int1$. This guarantees that an adversary cannot link sessions separated by a completed interrogation.

4.6 An Anonymous group-scanning proof

The Triangle protocol, as the Flyweight protocol on which it is based, provides session unlinkability. To capture this we modify the basic group-scanning proof by removing Phase 2 (in which the tags are linked via the reader) and have the reader broadcast all messages. Furthermore ID_{gp} is not included in the compiled group-scanning proof. Figure 5 describes the protocol.

The elimination of Phase 2 has, as explained in Section 4.2, a significant impact on the execution of the Triangle protocol, as the messages of tags must be broadcast by the reader. Broadcast messages are checked by all tags in range, triggering a reply only by the intended destination tag (the one that accepts RN as the correct number). The verifier matches the group by exhaustive search over all pairs (k, ID_{gp}) in its database, by using the mac and r_{sys}.

4.7 Proof of security

By using the argument in Section 4.4 we get integrity. Session unlinkability is inherited from the Flyweight protocol that (also) realizes this functionality in the UC framework [9]. □

5 Supply Chain Management

Our group-scanning proofs can be integrated into a high-level supply chain management system in which the owner shares with each GoT a group identifier and a private key (ID_{gp}, k) stored in a database DB, while the carrier does not share any private information with GoT. To check the integrity of tagged products with online batch connectivity, the owner generates a pseudorandom challenge $r_{sys} = r_o$ and queries the GoT via the carrier. The GoT then executes the group-scanning proof with r_o, and the carrier forwards the generated proof.

The owner can also provide the carrier with a specific key so that the integrity of a shipment of tagged products can be checked. For this application the owner selects a random number r_t, computes $k_t = f(k; r_t)$, and then sends to the carrier (ID_{gp}, r_t, k_t). The carrier generates a random number r_c and challenges the GoT with: r_t, r_c. This information enables the authenticator tag to compute k_t, and thus, the GoT can execute the grouping proof with $k = k_t$ and $r_{sys} = r_c$. The generated proof can be verified by the carrier.

References

[1] K Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, John Wiley, 2003.

[2] EPC Global, http://www.epcglobalinc.org/standards/EPCglobal_Tag_Data_Standard_TDS_Version_1.3.pdf

[3] D Dolev, A.C.C. Yao, "On the Security of Public Key Protocols," *IEEE Tran Inf Theory*, vol 29, no 2, pp 198207, 1983.

[4] M Ohkubo, K Suzuki, S Kinoshita, "Cryptographic approach to privacy-friendly tags," *Proc RFID Privacy Workshop*, 2003.

[5] D Henrici and P M Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers." *Proc Int Conf Pervasive Computing and Communications*, 2004, pp 149–153.

[6] D Molnar, A Soppera, and D Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags," *Proc Workshop Selected Areas in Cryptography (SAC 2005)*, LNCS #3897, Springer, 2006.

[7] T van Le, M Burmester, B de Medeiros, "Universally Composposable and Forward-Secure RFID Authentication & Authenticated Key Exchange," *Proc ACM Symp Computer and Communications Security (ASIACCS 2007)*, 2007, pp 242–252.

[8] M Burmester and B de Medeiros, "The Security of EPC Gen2 Compliant RFID Protocols," *ACNS*, SM Bellovin, R Gennaro, AD Keromytis, and M Yung, Eds, LNCS #5037, Springer, 2008, pp 490–506.

[9] M Burmester and J Munilla, "Lightweight RFID authentication with forward and backward security," *ACM Trans Inf Syst Secur*, vol 14, no 1, pp 11:1–11:26, 2011.

[10] H Liu, H Ning, Y Zhang, D He, Q Xiong and L T Yang, "Grouping-proofs-based authentication protocol for distributed RFID systems," *IEEE Trans Parallel Distrib. Syst.*, vol 24, no 7, pp 1321–1330, 2013.

[11] A Juels, "Yoking-proofs for RFID tags," *Proc 2nd Annual Pervasive Computing and Communications Workshop*, IEEE Computer Society, 2004, pp 138–142.

[12] J Saito and K Sakurai, "Grouping proof for RFID tags," *19th Int Conf Advanced Information Networking and Applications, AINA 2005*, vol 2, 2005, pp 621–624.

[13] M Burmester, B de Medeiros, R Motta, "Provably secure grouping-proofs for RFID tags," *CARDIS*, G. Grimaud and F.X. Standaert, Eds, LNCS #5189, Springer, 2008, pp 176–190.

[14] H-H Huang and C-Y Ku, "A RFID grouping proof protocol for medication safety of inpatient," *J. Medical Systems*, 2008.

[15] H-Y Chien, C-C Yang, T-C Wu, and C-F Lee, "Two RFID-based solutions to enhance inpatient medication safety," *J. Medical Systems*, 2009.

[16] P Peris-Lopez, A Orfila, JC Hernandez-Castro, and JCA van der Lubbe, "Flaws on RFID grouping-proofs: guidelines for future sound protocols," *J Netw Comput Appl*, **[34]**(3), pp 833–845, 2011.