An error in "On a new formal proof model for RFID location privacy"

Da-Zhi Sun [a, *]

[a] *School of Computer Science and Technology, Tianjin University, No. 92 Weijin Road, Nankai District, Tianjin 300072, PR China*

Abstract

In Information Processing Letters 110 (2) (2009) 57-61, Deursen and Radomirović evaluated five formal RFID privacy models. One main result is that Ha *et al.*'s RFID privacy model is incorrect. The supporting fact is that a constant-response protocol cannot pass the test of Ha *et al.*'s RFID privacy model. However, we demonstrate that the constant-response protocol is artificial, and the corresponding result is therefore unwarranted. It means that Ha *et al.*'s RFID privacy model is not a trivial model. Hence, more effort still can be made to improve Ha *et al.*'s RFID privacy model.

Keywords: *Cryptography; Location privacy; Untraceability; RFID protocol; Formal proof model*

1. Introduction

Radio Frequency Identification (RFID) systems are a promising automatic identification technology. Basically, RFID systems consist of two main components: tags and readers. Tags are radio transponders attached to physical objects. Readers are radio transceivers, and query these tags for some identifying information about objects, which tags are attached to. Many RFID protocols are designed to identify tags through wireless channels.

Although the tags have allowed the widespread adoption, the consumer applications of RFID systems have created the threats to the user's location privacy, because the tag's information can be read or traced by malicious readers from a distance without its owner's awareness. It is critical to investigate the formal RFID privacy models, which are fundamental to the design and analysis of RFID protocols with the location privacy

[*] Corresponding author. Tel.: +86 22 27406538; fax: +86 22 27406538.
E-mail addresses: sundazhi1977@126.com, sundazhi@tju.edu.cn (D.-Z. Sun).

protection. In 2009, Deursen and Radomirović (DR) [1] evaluated five formal RFID privacy models [2-6]. Their main result is that Ha *et al.*'s RFID privacy model [5] does not coincide with the intuitive notion of location privacy. On the one hand, Ha *et al.*'s RFID privacy model is incorrect. The supporting fact is that a constant-response protocol cannot pass the test of Ha *et al.*'s RFID privacy model, *i.e.* **Lemma 1** of [1]. On the other hand, Ha *et al.*'s RFID privacy model is weak. The supporting fact is that an identity plaintext protocol passes the test of Ha *et al.*'s RFID privacy model, *i.e.* **Lemma 2** of [1].

In this short letter, we demonstrate that DR's constant-response protocol is artificial, and **Lemma 1** of [1] is therefore unwarranted. It means that Ha *et al.*'s RFID privacy model is perhaps a weak model, but is not a trivial model. Hence, more effort still can be made to improve Ha *et al.*'s RFID privacy model.

2. Comments on DR's constant-response protocol and analysis

For a self-contained discussion, we simply review DR's constant-response protocol and employ the same notions and the figure style as [1]. The reader is referred to [1, 5] for full technique details. DR's constant-response protocol can be described as Fig.1. The

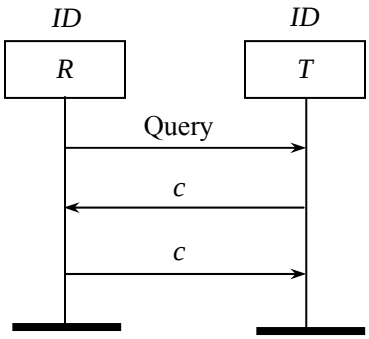

Fig. 1. Protocol 1.

reader *R* and tag *T* share a secret value *ID*. The value *c* is a public system-wide constant. The protocol run starts by *R* querying *T* for a response. Upon receiving *c* from *T* as a response, *R* also sends *c* back to *T*. Here, every tag in the RFID system responds the same constant. The location privacy property of DR's constant-response protocol is proposed as follows:

Lemma 1. *Protocol 1 does not satisfy indistinguishability for an active adversary under Ha et al.'s RFID privacy model.*

Based on this observation, DR's claim is that RFID protocols with the location privacy protection possibly do not pass the test of Ha *et al.*'s RFID privacy model.

However, we argue that Protocol 1 does not involve the location privacy problem, because Protocol 1 is not a RFID protocol. Hence, it is inappropriate to examine any RFID privacy model using Protocol 1 as an instance, and then deduce the characteristic of the RFID privacy model from it.

As the opinion in [1], Vaudenay [3] proposed a strongest and most complete RFID privacy model. Vaudenay's RFID privacy model defines the RFID protocol as follows.

Definition 1 (Definition 1 of [3]). *A RFID protocol is a polynomial-time interactive protocol between a reader and a tag, in which the reader ends with a tape Output. An RFID protocol is correct if its output is correct except with negligible probability for any polynomial time experiment, which can be described as follows.*

1. Set up the reader.

2. Create a number of tags including a subject one named ID for each tag.

3. Execute a complete protocol run between the reader and a tag.

The output is correct if and only if Output= $\perp$ *and ID is not legitimate, or Output=ID and ID is legitimate.*

We use **Definition 1** to check Protocol 1. Since all tags only send the same constant *c* during the runs of Protocol 1, the reader actually cannot identify any tag and output the corresponding $\perp$ or *ID* in the tape at the end of a protocol run. Obviously, according to **Definition 1**, we conclude that Protocol 1 is not a RFID protocol at all. To contradict Ha *et al.*'s RFID privacy model, it still need enumerate other protocol with the location privacy protection, which simultaneously satisfies **Definition 1** and fails to pass the test of Ha *et al.*'s RFID privacy model.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61003306 and in part by the Natural Science Foundation of Tianjin under Grant No. 11JCZDJC15800.

References

[1] T. van Deursen, S. Radomirović, On a new formal proof model for RFID location privacy, Information Processing Letters 110(2) (2009) 57-61.

[2] G. Avoine, Adversary model for radio frequency identification, Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005.

[3] S. Vaudenay, On Privacy models for RFID, in: Proceedings of 13th International Conference on the Theory and Application of Cryptology and Information Security-ASIACRYPT 2007, LNCS 4833, Springer-Verlag, Germany, 2007, pp. 68-87.

[4] T. van Deursen, S. Mauw, S. Radomirović, Untraceability of RFID protocols, in: Proceedings of Information Security Theory and Practices: Smart Devices, Convergence and Next Generation Networks-WISTP 2008, LNCS 5019, Springer-Verlag, Germany, 2008, pp. 1-15.

[5] J. Ha, S. Moon, J. Zhou, J. Ha, A new formal proof model for RFID location privacy, in: Proceedings of European Symposium on Research in Computer Security-ESORICS 2008, LNCS 5283, Springer-Verlag, Germany, 2008, pp. 267-281.

[6] A. Juels, S.A. Weis, Defining strong privacy for RFID, ACM Transactions on Information and System Security 13(1) (2009) 7:1-7:23.