On a New Formal Proof Model for RFID Location Privacy

Ton van Deursen and Saša Radomirović

Université du Luxembourg
Faculté des Sciences, de la Technologie et de la Communication
6, rue Richard Coudenhove-Kalergi
L-1359, Luxembourg

Abstract. We discuss a new formal proof model for RFID location privacy, recently proposed at ESORICS 2008.
We show that protocols which intuitively and in several other models are considered *not* to be location private (or untraceable), are provably location private in this model, and vice-versa.
Specifically, we prove a protocol in which every tag transmits the same constant message to not be location private in the proposed model. Then we prove a protocol in which a tag's ID is transmitted in clear text to be weakly location private in the model. Finally, we consider a protocol with known weaknesses with respect to location privacy and show it to be location private in the model.

Keywords: Location privacy, untraceability, RFID.

1 Introduction

The ubiquity of radio frequency identification (RFID) systems has given rise to concerns about the privacy of RFID tag bearers. These privacy concerns are often expressed by requiring that an adversary must not be able to trace the movements of a tag or its bearer. This can be made more specific by requiring that an adversary cannot recognize a tag he previously observed. If a protocol satisfies this requirement, we say that it satisfies *untraceability* [1, 2]. In the RFID setting, the notion of untraceability is also known as *(strong) privacy* [3–5]. In the Bluetooth setting, it is known as *location privacy* [6, 7]. The proposed model that we discuss additionally uses *indistinguishability* and *weak location privacy* to represent untraceability.

In this paper, we discuss a recently proposed formal proof model for location privacy [8]. We design two example protocols that we believe show weaknesses in the proposed proof model. The first example is an intuitively traceable protocol that we prove to be location private in the proposed model. The second example is an intuitively untraceable protocol which we show to not be location private. Finally, we consider a protocol with known weaknesses with respect to location privacy and show it to be location private in the considered model.

2 The Proposed Model

In this section we shortly outline the proposed model. The reader is referred to [8] for full details.

The model defines two attack games: one for indistinguishability and one for forward secrecy. For simplicity, we will restrict ourselves to the author's definition of *weak location privacy*, but similar results can be obtained when considering the author's notion of strong location privacy. The simplifying restriction allows us to only focus on the indistinguishability game proposed by the authors.

The indistinguishability attack game consists of three phases. In the initialization phase, the RFID system is initialized, that is, tags are created and the database is populated. In the learning phase, the adversary may, depending on his capabilities, query a set of oracles allowing him to interact with tags and database. In the challenge phase, the adversary chooses a target tag T and may again query a the set of oracles. Additionally, he may query the *reveal*-oracle that reveals the contents of the tag, for every tag except T. At the end of the challenge phase, the adversary calls the *test*-oracle. The oracle tosses a fair coin b:

- If $b = 1$: the message that T would send after being queried is given to the adversary.
- If $b = 0$: a random value of the same bit length as T's messages.

It is then the adversary's task to guess the value of b. The adversary wins the game if his guess is correct.

The protocol is defined to be *weakly location private* if the adversary does not have a non-negligible advantage of winning the indistinguishability game.

3 Analysis of the Proposed Model

3.1 Example 1

Our first example is a protocol that is intuitively and by the notions in [1–7] untraceable (strongly private, or location private), but which can be proven not to be location private in the proposed model.

The protocol is a challenge-response protocol that conforms to the general model of 3-round RFID protocols suggested by the authors of this model. For simplicity, we will omit the communication between reader and database, since it is assumed to be secure.

The protocol description is as follows. The reader R and tag T share a secret ID and c is a public, system-wide constant. The protocol starts by R querying T for a response. T responds with the constant c, after which R sends c to the tag. Figure 1 depicts the protocol. Note that every tag will respond with the same constant c.

The protocol is intuitively location private because every tag responds with the same message. In fact, the tags in this protocol could be identically built and

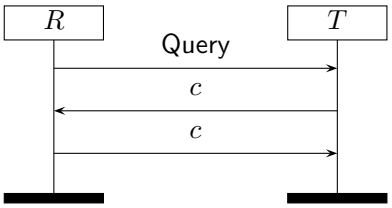

Fig. 1. Protocol 1.

may not even have an ID. Thus, regardless of his behavior, it is not possible for the adversary to recognize a tag he previously observed, since every tag sends the same message c.

We now use the proposed model to prove that the protocol is not location private.

Lemma 1. *Protocol 1 does not satisfy indistinguishability for an active adversary.*

Proof. The adversary's strategy is as follows. He does not query any oracle during the learning phase. In the challenge phase, he selects one of the tags at random, and he only queries the *Test*-oracle, in order to obtain an answer x. The adversary guesses $b = 1$ if $x = c$, and $b = 0$ otherwise.

The adversary wins this game with probability $1 - 2^k$, where k is the bit length of the constant. He thus has a non-negligible advantage to win the game. Therefore, Protocol 1 does not satisfy location privacy. □

The example shows a weakness in the game that is played by the adversary. At the end of the challenge phase, the adversary must be able to distinguish a tag's response from a random value. The set of possible tag answers is not considered in the game. Intuitively, for location privacy, the adversary should not be able to distinguish a tag's response from other tags' responses, but not necessarily from any arbitrary value.

3.2 Example 2

Our second example concerns a protocol that is not location private, but can be proven location private with respect to the proposed model.

Let R and T share a secret ID, particular to a certain tag. Let nr be a reader-generated nonce, and nt a tag-generated nonce. Let $pk(R)$ be a reader's public key with corresponding private key $sk(R)$. Let $\{m\}_{pk(R)}$ denote an IND-CCA public-key encryption of m with the public key $pk(R)$. We further assume that the encryption scheme has the *ciphertext pseudo-randomness* property, such as the scheme in [9] which makes ciphertexts indistinguishable from pseudorandom strings of equal length.

Figure 2 depicts the protocol.

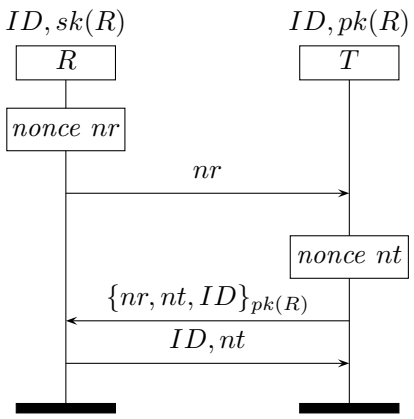

Fig. 2. Protocol 2.

It is easy to see that the protocol is not untraceable, location private, or strongly private, not only in an intuitive sense, but also by the notions of [1–7], since the identity ID of the tag is transmitted in every execution of the protocol. Thus a merely eavesdropping adversary can trace tags.

We now use the proposed model to prove that the protocol *is* weakly location private.

Lemma 2. *Protocol 2 satisfies indistinguishability for a passive adversary.*

Proof. In the learning phase, the adversary may query the *execute*-oracle to build a list of tuples $(nr, \{nr, nt, ID\}_{pk(R)}, ID, nt)$, corresponding to observed communications.

In the challenge phase, the adversary selects a challenge tag T and queries the *reveal*-oracle for all tags except T. He further extends his list of tuples $(nr, \{nr, nt, ID\}_{pk(R)}, ID, nt)$ by querying the *execute*-oracle.

Finally, the adversary queries the *Test*-oracle on T. The oracle tosses a fair coin b and

- for $b = 1$ it outputs the message $\{nr, nt, ID\}_{pk(R)}$,
- for $b = 0$ it outputs a random value of the same length as the second protocol message.

The adversary must now make a guess of bit b. If the adversary can guess this bit with a non-negligible advantage, then he can distinguish $\{nr, nt, ID\}_{pk(R)}$ from a random value with a non-negligible advantage which contradicts the ciphertext pseudo-randomness assumption on the encryption scheme.

This example shows a weakness in the challenge phase of the indistinguishability game. The adversary's capability is limited, in that he may not use information that in standard models would be available to a passive adversary. In

the present model, the adversary must base his decision solely on the message that was sent by the tag.

Note that if the reader would, in the third message, additionally transmit sufficient information for the adversary to be able to *verify* whether the encryption in message two is indeed an encryption of ID, then the proof would still go through, while the location privacy property would seem even less plausible.

3.3 Example 3

Our final example concerns a published protocol [10] with known location privacy weaknesses [11] that can be shown to be location private in this model.

The protocol aims to mutually authenticate RFID tag and reader, keep the tag untraceable, and resist a particular form of denial-of-service attacks, known as desynchronization attacks.

The protocol assumes that the reader R and tag T share a secret ID, which is updated at the end of a successful protocol execution. For efficiency reasons, the reader also stores the hash of the ID in HID and the value of ID before the last update in ID'. Additionally, the tag keeps track of whether its last protocol run ended successfully or not. For this purpose, the variable S is used.

Table 1. Reader's verification and update procedure in protocol 3.

Tag response	Update
$h(ID), nt$	$ID' := ID$; $ID := h(ID, nr)$; $HID := h(ID)$
$h(ID, nt, nr), nt$	$ID' := ID$; $ID := h(ID, nr)$; $HID := h(ID)$
$h(ID', nt, nr), nt$	$ID := h(ID', nr)$; $HID := h(ID)$
other	reject tag

In case the tag's previous run ended successfully, the value of S is 0 and the tag responds to a reader's query nr with $(h(ID), nt)$ allowing the reader to look up the tag in constant time. In case it did not end successfully, the value of S is 1 and the tag responds with $(h(ID, nt, nr), nt)$. This case should occur only rarely. In either case, the tag sets S to 1. The reader accepts the tag if the response, aside from the nonce nt, is equal to HID, $h(ID, nt, nr)$, or $h(ID', nt, nr)$ for any stored value of HID, ID or ID'. The reader then updates the information for the tag according to Table 1 and sends $h(ID', nt)$ to the tag. Finally, if the received message matches $h(ID, nt)$, the tag replaces its ID by $h(ID, nr)$ and sets S to 0. The protocol is depicted as a message sequence chart on the left in Figure 3.

One flaw of the protocol is that an active attacker can find out whether a tag's state is $S = 0$ or $S = 1$. Combined with the facts that under normal circumstances tags tend to be in state $S = 0$ and that an active adversary can *flag* tags by setting them into state $S = 1$, and thus recognize previously flagged tags. More formally, using the notion of strong privacy in [4] it can be

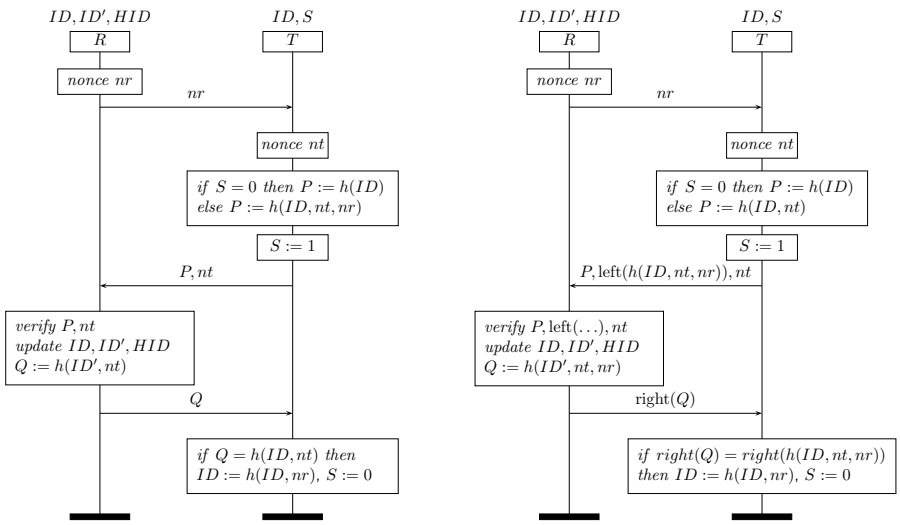

Fig. 3. Protocol 3 (left) and the LRMAP protocol (right).

shown [11] that the tags are not strongly private. Important for this attack is that the adversary has access to the reader's third message. If a tag is in state $S = 0$, the reader does not (and cannot) verify the integrity of the nonce nt, while if the tag is in state $S = 1$, the verification of the nonce's integrity occurs implicitly.

As alluded to in section 3.2, the adversary is not given access to the reader's third message to make a guess in the challenge phase. Thus this attack cannot be detected.

The authors propose in the same work [8] that includes the model discussed here, the so called LRMAP protocol, shown on the right in Figure 3 (update procedure shown in table 2). This protocol does not suffer from the above mentioned flaw, because the reader *always* checks the integrity of the nonce nt, due to the inclusion of an extra term $\text{left}(h(ID, nt, nr))$ in the second message. Further differences between the LRMAP protocol and protocol 3 above are minor and indistinguishable in this model. Thus the proof of location privacy for LRMAP given in [8] can also be applied to the flawed protocol 3, to prove it location private.

The observations on protocol 3 above can be generalized to all protocols which fit the three message pattern considered in the present model and are not location private only due to a desynchronization attack. To trace tags in such protocols the attacker needs to evaluate the reader's response.

Table 2. Reader's verification and update procedure in the LRMAP protocol.

Tag response	Update
$h(ID), \text{left}(h(ID, nt, nr)), nt$	$ID' := ID$; $ID := h(ID, nr)$; $HID := h(ID)$
$h(ID, nt), \text{left}(h(ID, nt, nr)), nt$	$ID' := ID$; $ID := h(ID, nr)$; $HID := h(ID)$
$h(ID', nt), \text{left}(h(ID', nt, nr)), nt$	$ID := h(ID', nr)$; $HID := h(ID)$
other	reject tag

4 Conclusion

We have shown that a new formal proof model for location privacy, proposed at ESORICS 2008 [8], differs from several existing notions of location privacy and does not coincide with an intuitive notion of location privacy.

Firstly, we have used the model to prove lack of location privacy of a protocol which should satisfy every notion of location privacy. This was possible because of the way in which the indistinguishability game is defined. The adversary wins the game if he can distinguish a tag's response from a random value, while intuitively, an adversary should be able to win the game if he can distinguish a tag's response from other tags' responses.

Secondly, we have used the model to prove location privacy of a protocol which transmits a tag's ID in each execution. This was possible because in the indistinguishability game, the adversary has to make a guess without being given the information contained in the last message of the protocol.

We note that this unintuitive notion of location privacy does not only affect specially crafted protocols. In example 3, we have shown a published protocols which can be proven location private in this model, but which is susceptible to a location privacy attack.

References

1. Avoine, G.: 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)
2. Deursen, T.v., Mauw, S., Radomirović, S.: Untraceability of RFID protocols. In: Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks. Volume 5019 of Lecture Notes in Computer Science., Seville, Spain, Springer (2008) 1–15
3. Vaudenay, S.: On Privacy Models for RFID. In: Advances in Cryptology - Asiacrypt 2007. Volume 4833 of Lecture Notes in Computer Science., Kuching, Malaysia, Springer-Verlag (December 2007) 68–87
4. Juels, A., Weis, S.: Defining Strong Privacy for RFID. In: International Conference on Pervasive Computing and Communications – PerCom 2007, New York, USA, IEEE, IEEE Computer Society Press (March 2007) 342–347
5. Damgård, I., Pedersen, M.Ø.: RFID security: Tradeoffs between security and efficiency. In: CT-RSA. (2008) 318–332

6. Wong, F.L., Stajano, F.: Location privacy in Bluetooth. In: ESAS. (2005) 176–188
7. Jakobsson, M., Wetzel, S.: Security weaknesses in Bluetooth. In: CT-RSA. (2001) 176–191
8. Ha, J., Moon, S., Zhou, J., Ha, J.: A new formal proof model for RFID location privacy. In: ESORICS. (2008) 267–281
9. Möller, B.: A public-key encryption scheme with pseudo-random ciphertexts. In: ESORICS. (2004) 335–351
10. Ha, J., Moon, S.J., Nieto, J.M.G., Boyd, C.: Low-cost and strong-security RFID authentication protocol. In: Embedded and Ubiquitous Computing (EUC) Workshops. (2007) 795–807
11. Deursen, T.v., Radomirović, S.: Security of RFID protocols – A case study. In: Proceedings of the 4th International Workshop on Security and Trust Management, STM 2008 (to appear). ENTCS, Elsevier (June 2008)