Computer Communications 34 (2011) 2248–2249

Contents lists available at SciVerse ScienceDirect

Computer Communications

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

Short Communication

A note on the security of PAP

Mu'awya Naser [a], Pedro Peris-Lopez [b,*], Rahmat Budiarto [a], Benjamín Ramos Álvarez [c]

[a] School of Computer Sciences, Main Campus, Universiti Sains Malaysia, 11700 Penang, Malaysia
[b] Information Security and Privacy Lab, Delft University of Technology, Mekelweg 4, 2628 CD, Delft, The Netherlands
[c] Computer Science Department, Carlos III University of Madrid, Avenida de la Universidad 30, 28911 Leganés (Madrid), Spain

ARTICLE INFO

Article history:
Received 13 June 2011
Received in revised form 4 July 2011
Accepted 5 July 2011
Available online 29 July 2011

Keywords:
RFID
Privacy
Authentication
Cryptanalysis

ABSTRACT

In this letter, we analyze the security of an RFID authentication protocol proposed by Liu and Bailey [1], called privacy and authentication protocol (PAP). We present two traceability attacks and an impersonation attack.

1. Introduction

Liu and Bailey [1] proposed PAP, a privacy and authentication protocol for passive RFID tags. We urge the reader to consult the original paper for details. In this letter, we analyze the security of this protocol and its associated sub-protocols and show important security faults.

2. Traceability attacks

One of the main concerns linked to privacy is the location-privacy or traceability protection. In PAP, the proposed sub-protocols were weakly designed and are vulnerable to traceability attacks despite using random numbers and computing authentication tokens by running a hash function. The traceability deficiencies are described below:

1. In the in-store and out-store sub-protocols, the tag always sends fixed values corresponding to the tag's *ID* and tag names, respectively. In the former, the tag's holder can be tracked because the *ID* is unique and constant. In the latter, tag name is constant but not a unique value. Nevertheless, the tag's holder can be tracked using constellations of tag names that are unequivocally linked to a specific user. Note that the use of a cover-coding mechanism does not protect the values transmitted by the tag.
2. In the check-out and return sub-protocols, the adversary can track the tag by setting one of the random numbers used in the protocol (i.e. n_t or n_r) to a constant value "c". According to Abadi and Needham guidelines for designing cryptographic protocols, principles four and five about the use of encryption and predictable quantities respectively are dissatisfied [2]. Specifically, we can track either the reader's answer or the tag's answer. In a forward-channel tractability attack, the adversary can intercept the tag's reply to the reader's query. Then, she replaces n_t with constant value c, and finally forwards the message (ID/name, c) to the reader. The rest of the protocol would conclude normally. We emphasize here that the hashed value H_1 is the same every time the attack is executed because the adversary fixes n_t to c ($H_1 = hash(c,k)$). If the adversary runs the attack twice, she is able to track the tag by checking the equality between the H_1 values. Similarly, in the backward-channel a successful traceability attack can be conducted by replaying n_r with a c constant value.

3. Impersonation attacks

An adversary can impersonate a tag using the answers provided by a second legitimate reader and exploiting the symmetry of the messages computed by the reader and the tag in the PAP–see principle four for designing cryptographic protocols [2]. So, an impersonation attack can be conducted between an adversary and two legitimate readers. The second reader generates the messages of the supplanted tag. We assume that before launching the attack,

[*] Corresponding author. Tel.: +31 (0) 15 27 83878.
E-mail address: P.PerisLopez@tudelft.nl (P. Peris-Lopez).

0140-3664/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2011.07.002

the adversary eavesdrops on the *ID*/name of its target tag. The attack is described below.

First, reader_1 sends a request query to the adversary. The adversary replies with $\{ID/\text{name}, n_t\}$, where n_t represents an arbitrary random value. Then, reader_1 computes its authentication token H_1, generates a random value n_r, and sends both values to the adversary. The adversary simulates that she received a request from reader_2 and sends the tuple $\{ID/\text{name}, n_r\}$. The adversary uses the random number n_r received from reader_1. The reader_1 computes its authentication token $(H_1^* = hash(n_r, k))$ and sends it to the adversary. Finally, the adversary forwards H_1^* value to reader_1. The reader_1 checks the token received and authenticates the adversary.

4. Conclusions

In this letter, some of the main security objectives of PAP protocol are ruined. The proposed attacks could have been avoided by following well-known principles for designing cryptographic protocols [2].

References

[1] A.X. Liu, L.A. Bailey, PAP: a privacy and authentication protocol for passive RFID tags, Comput. Commun. 32 (7–10) (2009) 1194–1199.

[2] M. Abadi, R. Needham, Prudent engineering practice for cryptographic protocols, IEEE Trans. Softw. Eng. 1 (22) (1996) 6–15.