Attack on Liao and Hsiao's Secure ECC-based RFID Authentication Scheme integrated with ID-Verifier Transfer Protocol

A follow-up to a paper published by Elsevier's Ad Hoc Networks*

Roel Peeters & Jens Hermans

KU LEUVEN & iMinds, COSIC, Belgium

Abstract. We show that the Liao and Hsiao's protocol achieves neither tag-authentication nor privacy.

1 Introduction

Liao and Hsiao [5] proposed a private RFID authentication protocol based on Elliptic Curve Cryptography. Their motivation to switch from symmetric key cryptography to public key cryptography is that this a prerequisite to achieve forward private RFID authentication efficiently at the server (*i.e.* constant size look-up)[3]. To minimise the hardware implementation area, the authors only make use of an ECC co-processor and do not require additional cryptographic building blocks, *e.g.*, hash functions or block ciphers.

The authors claim that, albeit their protocol being very inefficient with 5 EC multiplications, it is the only ECC-based RFID authentication scheme satisfying all the requirements of RFID systems, including mutual authentication, confidentiality, anonymity, forward security and scalability. Instead of evaluating the privacy properties of RFID authentication protocols in a standard model as for instance the one of Hermans *et al.* [4], the authors decided to stick with deprecated, partial and informal definitions. In their comparison, the authors wrongly classified the protocols of Tuyls *et al.* [7] and Batina *et al.* [1] as not scalable. Furthermore, protocols which were designed with the same circuit size optimisation in mind, do not appear in their comparison: randomized Schnorr by Bringer *et al.* [2] and the zero-knowledge-based private RFID identification protocols by Peeters and Hermans [6]. These protocols do achieve all the above mentioned requirements except mutual authentication (proven in a general model) and provide even stronger privacy guarantees for only 2 EC multiplications.

We will show that the protocol by Liao and Hsiao does not achieve tag authentication, privacy (confidentiality, anonymity, forward security), server authentication, nor mutual authentication. As such their protocol is susceptible to tag masquerade attacks, server spoofing attacks, location tracking attacks and tag cloning attacks.

* See acknowledgements

2 Protocol Description

Figure 1 provides an overview of the protocol by Liao and Hsiao [5], we stick to their notation. The protocol is based on Elliptic Curve Cryptography for which additive notation is used. Points on the curve are represented by capital letters while scalars are represented by lower case letters. P is a generator of the elliptic curve of order n, while Z_T, x_T represent the public and private key of the tag, P_S, x_S the public and private key of the server. In their security analysis it is assumed that the public key of the server P_S is known.

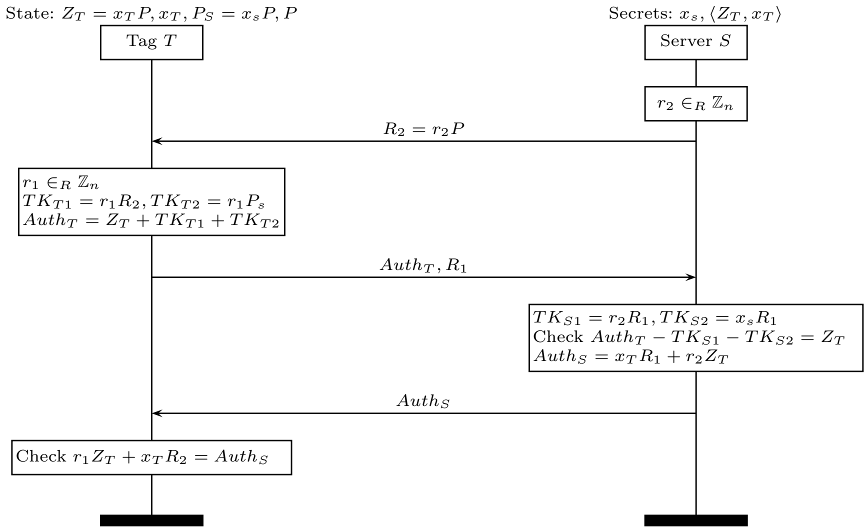
State: $Z_T = x_T P, x_T, P_S = x_s P, P$
Tag T
Secrets: $x_s, \langle Z_T, x_T \rangle$
Server S
$r_2 \in_R \mathbb{Z}_n$
$R_2 = r_2 P$
$r_1 \in_R \mathbb{Z}_n$
$TK_{T1} = r_1 R_2, TK_{T2} = r_1 P_s$
$Auth_T = Z_T + TK_{T1} + TK_{T2}$
$Auth_T, R_1$
$TK_{S1} = r_2 R_1, TK_{S2} = x_s R_1$
Check $Auth_T - TK_{S1} - TK_{S2} = Z_T$
$Auth_S = x_T R_1 + r_2 Z_T$
$Auth_S$
Check $r_1 Z_T + x_T R_2 = Auth_S$

Fig. 1. Private RFID authentication protocol of Liao and Hsiao [5].

Ironically, the authors based their protocol on public key cryptography but did not realise that in fact 1) tag-authentication is based on the shared secret Z_T, and 2) server-authentication is based on the shared secret x_T. For tag-authentication the tag's public key is masked (not encrypted) using an unauthenticated Diffie-Helmann key agreement protocol to compute $TK_{T1} = TK_{S1}$ and an implicit authenticated variant to compute $TK_{T2} = TK_{S2}$. For server-authentication the sum of R_1 and R_2 is multiplied with the tag's secret x_T.

3 Attack

Both tag-authentication and privacy rely on the inability of the adversary to learn the tag's public key Z_T. However, this can easily be learned from the tag, without physical attacks, simply by sending $R_2 = -P_S$. This means that the tag will send back $Auth_T = Z_T - r_1 P_S + r_1 P_S = Z_T$. The adversary's ability to extract this unique identifier makes that no privacy properties can be achieved. This basic attack can be circumvented by the tag checking that $R_2 \neq -P_S$. However, the attack can easily be extended by randomising $R_2 = -P_S + \alpha P$ with $\alpha \in_R \mathbb{Z}_n$. The resulting answer from the tag will be $Auth_T = Z_T + r_1(-P_S + \alpha P) + r_1 P_S = Z_T + \alpha r_1 P$. The attacker can then recover $Z_T = Auth_T - \alpha R_1$.

Server-authentication can be achieved when using a shared secret. However, Liao and Hsiao define in their paper a server spoofing attack as an attack where the attacker is able to impersonate a server to a compromised tag (having access to the tag's internal state). Hence, the attacker has access to x_T of the tag and sends $x_T(R_1 + R_2)$, successfully authenticating as the legitimate server. Note that not even knowledge of r_2 is required for this attack.

Towards mutual authentication we argue that it is not an essential requirement for an private RFID authentication protocol. However, if the tag and server are to send additional data, *e.g.*, sensor readings, mutual authentication is important. Since neither tag- nor server-authentication is achieved, it follows that it does not achieve mutual authentication either.

4 Conclusions

The proposed protocol by Liao and Hsiao [5] suffers mainly from the existing homomorphic relations between the inputs and outputs that can be exploited. As a result, no security or privacy properties are achieved by this protocol. Furthermore, more efficient protocols achieving all properties put forward by Liao and Hsiao with the exception of mutual authentication exist, even providing stronger privacy guarantees [2,6].

Acknowledgements

We would like to thank the editors of Elsevier's Ad Hoc Networks who deemed this paper out of scope with as only comment that "The title is not professional and fair and nice." and the suggestion "Maybe you should communicate your concerns with the authors and resolve it among yourselves." Oddly enough the original paper was within scope of this journal.

References

1. L. Batina, J. Guajardo, T. Kerins, N. Mentens, and P. Tuyls. Public-key cryptography for rfid-tags. In *PerSec*, pages 217–222. IEEE Computer Society Press, 2007.
2. J. Bringer, H. Chabanne, and T. Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. In M. K. Franklin, L. C. K. Hui, and D. S. Wong, editors, *CANS*, volume 5339, pages 149–161, 2008.
3. I. Damgård and M. Ø. Pedersen. RFID Security: Tradeoffs between Security and Efficiency. In T. Malkin, editor, *CT-RSA*, volume 4964 of *LNCS*, pages 318–332. Springer, 2008.

4. J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel. A New RFID Privacy Model. In V. Atluri and C. Diaz, editors, *ESORICS 2011*, volume 6879 of *LNCS*, pages 568–587. Springer, 2011.
5. Y.-P. Liao and C.-M. Hsiao. A secure ecc-based {RFID} authentication scheme integrated with id-verifier transfer protocol. *Ad Hoc Networks*, 2013. `http://dx.doi.org/10.1016/j.adhoc.2013.02.004`.
6. R. Peeters and J. Hermans. Wide Strong Private RFID Identification based on Zero-Knowledge. Cryptology ePrint Archive, Report 2012/389, 2012. `http://eprint.iacr.org/`.
7. P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In 3860, editor, *CT-RSA*, LNCS, pages 115–131. Springer, 2006.