On the claimed privacy of EC-RAC III

Junfeng Fan, Jens Hermans, and Frederik Vercauteren

Department of Electrical Engineering
K.U.Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

Abstract. In this paper we show how to break the most recent version of EC-RAC with respect to privacy. We show that both the ID-Transfer and ID&PWD-Transfer schemes from EC-RAC do not provide the claimed privacy levels by using a man-in-the-middle attack. The existence of these attacks voids the presented privacy proofs for EC-RAC.

Keywords: RFID, Protocols, EC-RAC, Privacy

1 Introduction

In [2] Lee, Batina, Singelée and Verbauwhede presented an improved version of EC-RAC, after the previous versions [3, 4] were broken.

The first version of the EC-RAC protocol [3] was broken in [5] and [1], which show that a tag could be traced by an attacker using a quality-time attack [5]. The attacker can generate a *unique attribute* of a tag by sending the same challenge twice, and the *unique attribute* can then be used to identify the tag.

The subsequent version of EC-RAC [4] introduced three different sub-protocols: ID-transfer, Pwd-Transfer and server authentication. These sub-protocols were combined into several protocols. One of the fundamental problems is that protocols, which in isolation are secure and/or untraceable, are not necessarily secure and/or privacy preserving when combined. The second version of EC-RAC was broken in [6]. The ID-transfer scheme was broken with respect to untraceability using a man-in-the-middle attack, in which the attacker uses a previous, valid, execution of the protocol to modify the communication. If the reader accepts the modified values, the attacker can identify the previously eavesdropped tag. The ID&Pwd-Transfer protocols were broken with respect to tag-to-server authentication, allowing the attacker to impersonate a tag. The main cause of this attack is the reuse of the same keys for both the ID- and Pwd-Transfer sub-protocol.

To resolve this issue a non-linearity was introduced in the ID-Transfer protocol and the ID&Pwd-Transfer protocol was modified to exclude the usage of the same key and to ensure that different randomness was used. The paper [2] claims that the ID-transfer protocol (protocol 1 from [2]) and the ID&Pwd-Transfer protocol (protocol 3 from [2]) provide *wide-strong* privacy (see [7] for definition).

Throughout this paper, we also use the privacy notions from Vaudenay [7]. A *wide* attacker has access to the result of the verificication by the server while a *narrow* attacker does not. A *strong* attacker can extract the secrets from a tag and can keep reusing the tag, while a *weak* attacker cannot.

We show in this paper that the new EC-RAC protocols [2], including the ID&Pwd-Transfer protocols (protocol 2,3) and the ID-Transfer protocol (protocol 1), do not provide the claimed privacy properties. The ID&Pwd-Transfer protocols are broken by a (wide) man-in-the-middle attack, and a tag can be traced by the attacker. The introduction of the non-linearity was ineffective. Since our attacks on the ID&Pwd-Transfer scheme do not require access to the tag's secrets, not even *wide-weak* privacy is provided by the protocols. $Narrow$*-weak* privacy might be provided by these protocols, but no formal proof for this is included. Also the ID-transfer protocol does not provide the claimed *wide-strong* privacy. An attacker that knows the identity of a certain tag, can always identify this tag using a man-in-the-middle attack. The highest privacy levels that could be provided by the ID-Transfer scheme are *narrow-strong* privacy or *wide-destructive*, although no formal proof for this exists.

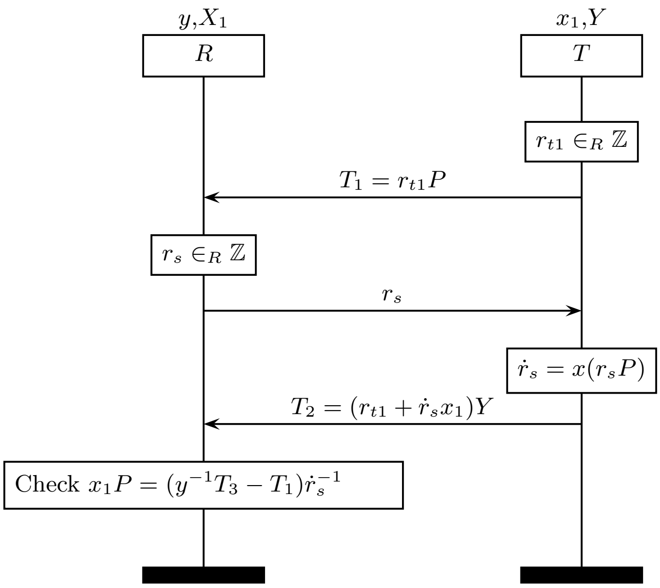
2 Untraceable authentication protocols for RFID

The EC-RAC protocols are all based upon elliptic curve cryptography. Let P be a generator of the elliptic curve group. Every tag has two private-public key pairs $x_1, X_1 = x_1P$ and $x_2, X_2 = x_2P$. In this case x_1 serves as the identity of the tag and is also known by the reader. The reader has a private-public key pair $y, Y = yP$.

Figure 1 shows the ID-transfer protocol from [2]. This protocol should identify the tag as x_1 in a secure and *wide-strong* privacy preserving way. The main difference with the previous versions of the protocol is the introduction of the non-linearity $\dot{r}_s = x(r_sP)$, with $x(\cdot)$ the x-coordinate function for an elliptic curve point.

Figure 2 shows the ID&Pwd-Transfer protocol from [2]. In addition to the reader identifying the tag correctly as x_1, it also authenticates

Fig. 1. Protocol 1 from [2]



the tag using the public-private key pair $x_2, X_2 = x_2P$. (Note that the secret x_1 is known to both the tag and the reader and cannot be used for authentication.)

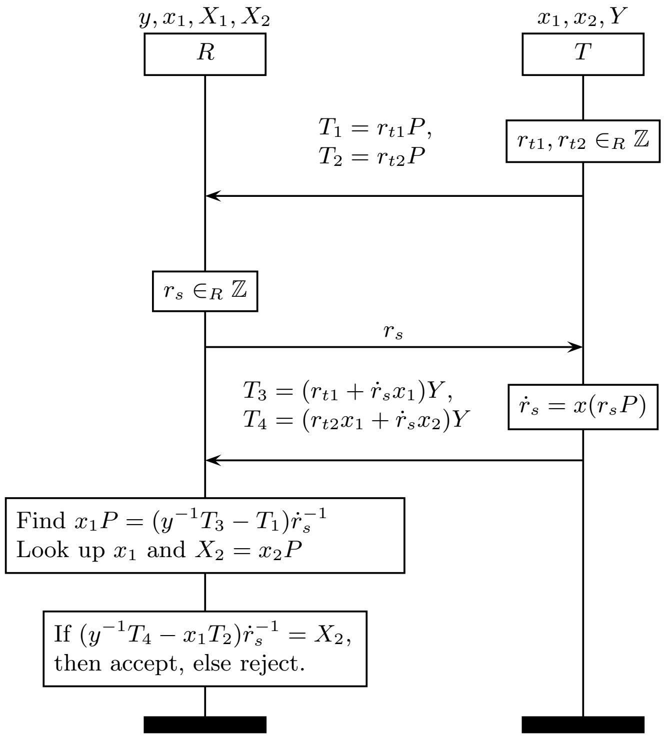
3 Attacks on the protocols

The main flaw in the ID&Pwd-Transfer scheme is the fact that the "hash" of the challenge, i.e. $\dot{r}_s$ does not mask all of the secret keys x_1 and x_2. Indeed, in the response T_4, the x_1 part is only masked by the randomness r_{t2}.

3.1 First attack

The first attack exploits the fact that it is possible to force $\dot{r}_s$ to become 0. Indeed, note that the protocol does not verify whether r_s is a multiple of the order of P. As such, it is possible for an attacker impersonating

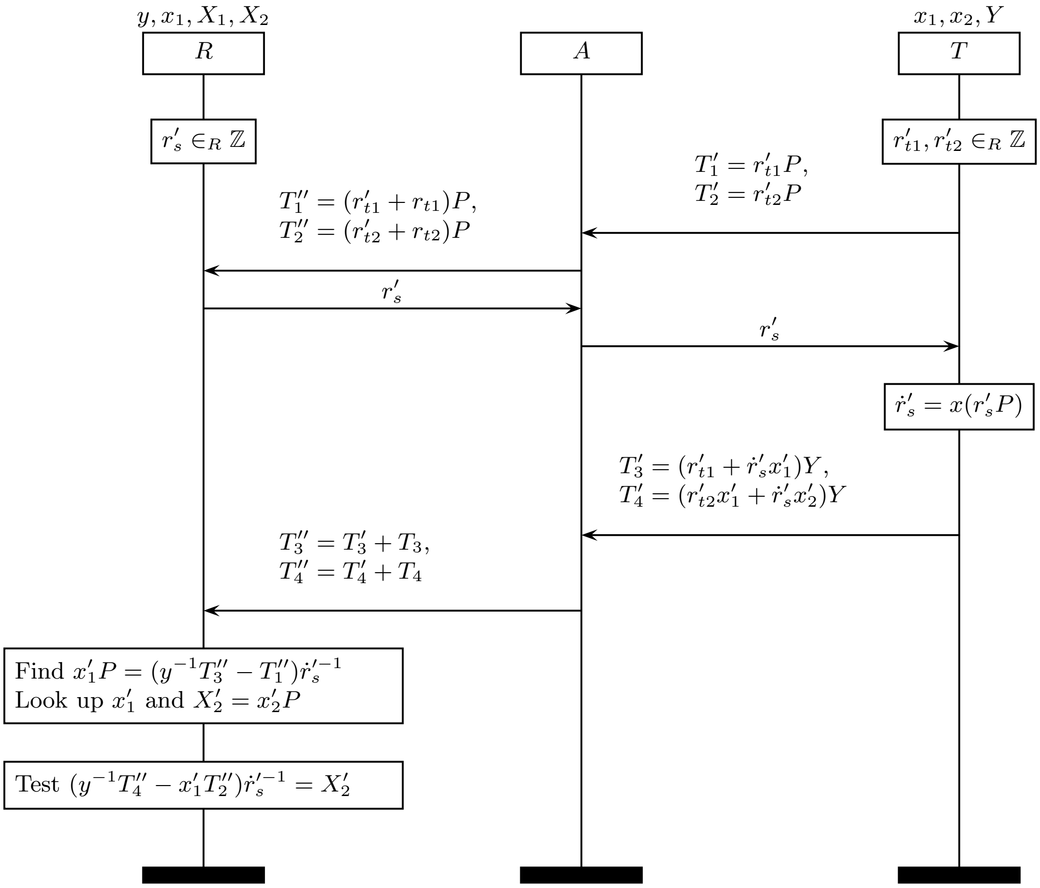
Fig. 2. Protocol 3 from [2]



a reader to send $r_s = k \cdot \text{ord}(P)$ to the tag, who will then compute $\dot{r}_s = x(r_sP) = 0$ and therefore return $T_3 = r_{t1}Y$ and $T_4 = r_{t2}x_1Y$. Using the messages ($T_1 = r_{t1}P$, $T_2 = r_{t2}P$, $T_3 = r_{t1}Y$, $T_4 = r_{t2}x_1Y$), it is then possible to mount a man-in-the-middle attack on a second communication to test whether the same tag from the first run is present or not. This attack is described in Figure 3 where the tag's secret keys are now denoted by x_1' and x_2'.

The adversary adds T_1 and T_2 to the messages T_1' and T_2' obtained from the unknown tag and forwards these to the reader. The reader responds with a nonce r_s', which the attacker simply forwards to the tag. The tag responds with valid messages T_3' and T_4' which the attacker uses to obtain $T_3'' = T_3' + T_3$ and $T_4'' = T_4' + T_4$ and sends these to the reader. The reader

Fig. 3. Man-in-the-middle attack on protocols 2 and 3



then computes

$$(y^{-1}T''_3 - T''_1)\dot{r}'^{-1}_s = (r_{t1} + r'_{t1} + \dot{r}'_s x'_1 - r_{t1} - r'_{t1})\dot{r}'^{-1}_s P = x'_1 P\,,$$

and looks up x'_1 and $X'_2 = x'_2 P$. Note that this step always verifies. The reader then tests whether $(y^{-1}T''_4 - x'_1 T''_2)\dot{r}'^{-1}_s = X'_2$, which is equivalent with

$$(r'_{t2}x'_1 + \dot{r}'_s x'_2 + r_{t2}x_1 - x'_1(r'_{t2} + r_{t2}))\dot{r}'^{-1}_s P = x'_2 P\,.$$

The test will succeed if and only if $x_1 = x'_1$, i.e. if the tag is the same as the one from the first run.

3.2 Second attack

The second attack even works when the tag adds an extra verification that $\dot{r}_s \neq 0$. Note that the first attack worked because the attacker obtained $(T_1 = r_{t1}P, T_2 = r_{t2}P, T_3 = r_{t1}Y, T_4 = r_{t2}x_1Y)$, so it suffices to explain how such a tuple can be obtained when the tag verifies whether $\dot{r}_s \neq 0$. In fact, obtaining such a tuple is trivial by querying the tag twice with the same r_s and subtracting the results, since the parts involving $\dot{r}_s$ will cancel out. As such we obtain a valid tuple $(T_1^* = r_{t1}^*P, T_2^* = r_{t2}^*P, T_3^* = r_{t1}^*Y, T_4^* = r_{t2}^*x_1Y)$, which can then be used in the first attack.

3.3 Third attack

The third attack shows that the ID-transfer scheme (protocol 1 from [2]) is not wide-strong. A *strong* attacker is able to read a tag's ID x_1 without destroying the tag. We will now show how a *strong* attacker can then be used to track a particular tag using a man-in-the-middle attack.

This attack is described in Figure 4. By definition of *strong*, the attacker knows x_1 of a certain tag. In order to test if a random tag is the corrupted one, she plays a man-in-the-middle attack as follows. The attacker replaces the value r_s with another random value r'_s and replaces $T_2 = (r_{t1} + \dot{r}'_s x'_1)Y$ by

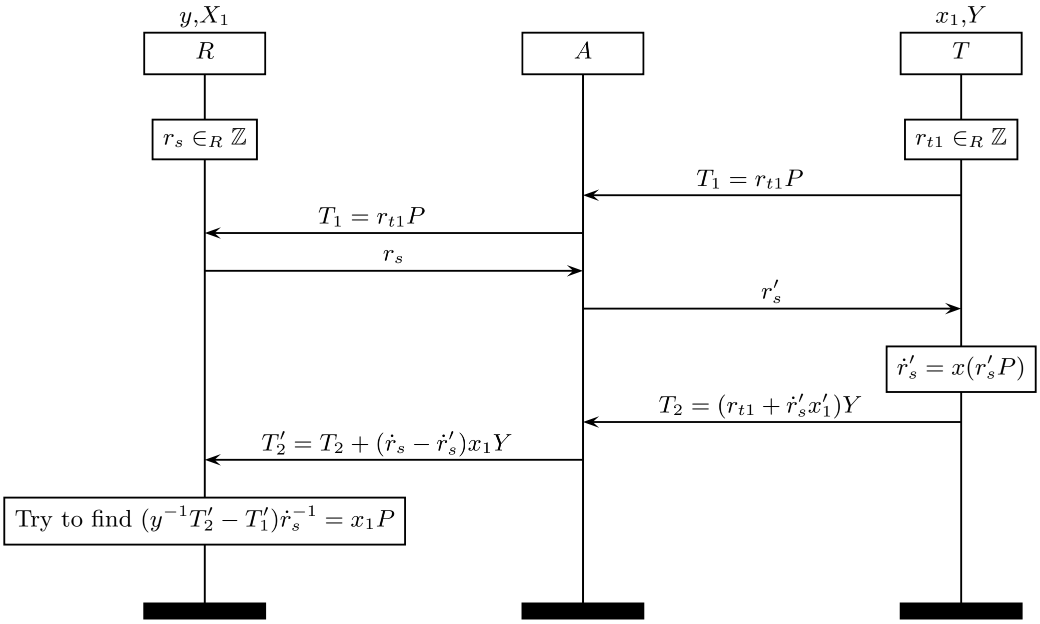
$$T'_2 = T_2 + (\dot{r}_s - \dot{r}'_s)x_1Y = (r_{t1} + \dot{r}'_s(x'_1 - x_1) + \dot{r}_s x_1)Y$$

The reader will accept this only if $x_1 = x'_1$ (provided $\dot{r}'_s \neq 0$, which the attacker can assure). This allows the attacker to identify the tag x_1 upon acceptance by the reader. The ID-transfer protocol is thus not *wide-strong* private. Since our attacker is both *wide* and *strong*, the ID-transfer might be *narrow-strong* private or *wide-destructive* private, although no proof for this is given in the original paper.

4 Conclusions

In this paper we have shown three successful attacks on the latest version of EC-RAC [2]. We prove that the ID&PWD-Transfer scheme is not *wide-strong* private and is not even *wide-weak* private. The highest possible

Fig. 4. Man-in-the-middle attack on protocol 1



privacy level that might be achieved by the ID&PWD-Transfer scheme is *narrow-weak* privacy.

We also prove that the ID-transfer scheme is not *wide-strong* private as claimed and can be at most *wide-destructive* or *narrow-strong* private.

References

1. Julien Bringer, Hervé Chabanne, and Thomas Icart. Cryptanalysis of EC-RAC, a RFID identification protocol. In *CANS*, volume 5339 of *Lecture Notes in Computer Science*, pages 149–161. Springer, 2008.
2. Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID. In *Proceedings of the 3rd ACM conference on Wireless network security (WiSec 2010)*, Hoboken,NJ,USA, 2010. ACM. Preprint.
3. Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In

IEEE International Conference on RFID 2008, pages 97–104, Las Vegas,NA,USA, 2008. IEEE.
4. Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. Untraceable RFID Authentication Protocols: Revision of EC-RAC. In *IEEE International Conference on RFID 2009*, pages 178–185, Orlando,FL,USA, 2009. IEEE.
5. Ton van Deursen and Sasa Radomirovic. Attacks on RFID protocols. Cryptology ePrint Archive, Report 2008/310, 2008. http://eprint.iacr.org/.
6. Ton van Deursen and Sasa Radomirovic. Untraceable RFID protocols are not trivially composable: Attacks on the revision of EC-RAC. Cryptology ePrint Archive, Report 2009/332, 2009. http://eprint.iacr.org/.
7. Serge Vaudenay. On privacy models for RFID. In *ASIACRYPT*, pages 68–87, 2007.