EC-RAC: Enriching a Capacious RFID Attack Collection

Ton van Deursen* and Saša Radomirović

University of Luxembourg

Abstract. We demonstrate two classes of attacks on EC-RAC, a growing set of RFID protocols. Our first class of attacks concerns the compositional approach used to construct a particular revision of EC-RAC. We invalidate the authentication and privacy claims made for that revision. We discuss the significance of the fact that RFID privacy is not compositional in general.
Our second class of attacks applies to all versions of EC-RAC and reveals hitherto unknown vulnerabilities in the latest version of EC-RAC. It is a general man-in-the-middle attack executable by a weak adversary.
We show a general construction for improving narrow-weak private protocols to wide-weak private protocols and indicate specific improvements for the flaws of EC-RAC exhibited in this document.

Key words: RFID; attacks; privacy; authentication; compositionality;

1 Introduction

Secure communication protocols are essential for every networked application. Yet, after more than thirty years of cryptographic protocol design, we appear to be still struggling with the design of novel, secure three-message protocols. The same applies to the *privacy* property of RFID protocols. Indeed, the design and verification of privacy-preserving protocols is closely related to the much wider studied classes of protocols aiming to achieve secrecy or authentication. While it is true that the complexity of verification algorithms for any of these three properties is exponential in the number of messages exchanged in a protocol, it is frequently possible to find flaws "by hand" by simply considering a small number of attack classes, most famously replay attacks or man-in-the-middle attacks. Such an approach has led to a collection of attacks on RFID protocols and to the discovery of RFID-specific attacks patterns, such as quality-time attacks, algebraic replay attacks, and desynchronization attacks [1].

* Ton van Deursen was supported by a grant from the Fonds National de la Recherche (Luxembourg).

A simple strategy to decrease the design and verification complexity is to construct protocols from smaller and simpler building blocks. It is then essential, however, to prove that these building blocks do not break each others' security properties. In fact, it is well known [2–5] that protocols satisfying a security property when executed in isolation do not necessarily satisfy the same security property when they are executed in an environment containing other protocols. In particular, it has been shown that composition of secrecy-preserving protocols may introduce attacks [6]. Similar results have been obtained for the composition of authentication protocols [7].

In the present paper, as a first contribution, we demonstrate that privacy is not compositional. The mechanism we use to show this is simple. Given two protocols P_1 and P_2, both satisfying privacy in isolation, we use protocol P_1 as an oracle to break protocol P_2.

Our second contribution is an analysis of EC-RAC II [8], a set of elliptic-curve based RFID protocols aiming to provide privacy and authentication. The protocols in the set are built from simple components which are individually claimed to provide privacy or authentication. We show that the EC-RAC II protocols nevertheless fail to satisfy privacy and authentication. This failure is exhibited by applying the mechanism outlined above to the simple components comprising the EC-RAC II protocols

As a third contribution, we reiterate the difficulty of designing secure protocols by showing a man-in-the-middle attack on all versions of EC-RAC [8–11]. The attack can be executed by a weak adversary and breaks the privacy of all protocols in the set. This shows that the privacy claims made by the respective authors are incorrect.

Our final contribution is a demonstration of how to improve the privacy of a class of three-message RFID protocols to which the EC-RAC protocols belong.

Our paper is organized as follows. We briefly review Vaudenay's privacy model and the EC-RAC family in Section 2. We demonstrate non-compositionality of RFID privacy in Section 3 and apply the result to attack EC-RAC II in Section 4. We discuss wide-weak man-in-the-middle attacks on all revisions of EC-RAC in Section 5. We show a general construction for improving narrow-weak protocols to wide-weak protocol in Section 6 and suggest improvements specific to the EC-RAC protocols in Section 7. We present our conclusion in Section 8.

2 Preliminaries

We set the scene for our paper by briefly recalling Vaudenay's privacy model and then giving an overview of the different versions of EC-RAC.

2.1 The RFID privacy model of Vaudenay

Intuitively, an RFID protocol provides privacy (also referred to as location privacy or untraceability) if an adversary cannot recognize an RFID tag he previously observed or interacted with. The formalization of this intuition is, however, tricky and has been carried out in several different ways [12–17]. At present, the model by Vaudenay [14] can be considered to be the most comprehensive privacy model.

Vaudenay's model captures eight classes of adversary capabilities ranging over four different types of tag corruption and two modes of observation. Corrupting a tag means extracting the tag's cryptographic material as well as its state. An adversary is a probabilistic polynomial Turing Machine whose strength is defined by the set of oracles he is allowed to query. A *weak* adversary is not allowed to corrupt a tag. A *forward* private adversary may corrupt a tag at the end of the attack. A *destructive* adversary may corrupt a tag at any time, which leads to the destruction of the tag, that is, the adversary may no longer interact with the tag. A *strong* adversary may corrupt a tag at any time without destroying it. Corresponding to the two modes of observation, an adversary is called *wide* if he may observe whether the protocol ended successfully, and *narrow* else. Since the four types of corruption are orthogonal to the narrow/wide separation, eight different adversarial classes are considered.

Privacy is defined by comparing the adversary to a special adversary which makes no use of protocol messages, as follows. An adversary is called *blinded* if he is not allowed to communicate with tags and reader. An adversary is *trivial* if there exists a blinded adversary which essentially performs equally well at guessing a tag's identity. A protocol is P *private*, where P is one of the eight adversary classes, if all adversaries that belong to that class are trivial.

In this paper, we will primarily consider a wide-weak adversary, since this is the adversary against which the latest revision of EC-RAC [11] is claimed to be secure. The attacks related to compositionality flaws will be executable by a narrow-weak adversary.

2.2 EC-RAC

The EC-RAC protocols aim to provide private tag authentication. They are one of the first published and implemented asymmetric-key RFID protocols. The construction of such protocols is interesting for several reasons. Public-key-based protocols aim to maintain privacy against strong attackers. It has been shown that it is impossible to achieve narrow-strong privacy with symmetric key cryptography alone [14]. Asymmetric protocols also enable efficient tag lookup procedures on the reader's side. In fact, Damgård and Pedersen have shown that in a system relying on symmetric keys, either privacy, security, or efficiency has to be sacrificed [18].

To distinguish the various revisions of EC-RAC, we will call the original publication EC-RAC I [9], the first revision EC-RAC II [8], the second revision EC-RAC III [10], and the latest revision EC-RAC IV [11].

EC-RAC I is a challenge-response protocol on which several attacks have been published [19, 1, 20]. EC-RAC II introduced a commitment-challenge-response structure and four sub-protocols which were individually claimed to satisfy authentication or privacy properties. These sub-protocols were then composed into the six protocols shown in Figure 2. We will discuss EC-RAC II in Section 4. EC-RAC III consists of slightly modified versions of protocols 1, 2, and 3 of EC-RAC II. The modification only concerns the use of the RFID reader's challenge nonce in computations, but the protocol flow remains the same. Protocols 1 and 3 of EC-RAC III were claimed to be wide-strong private, protocol 2 to be wide-weak private. Fan et al. [21] showed that all these claims are false. In particular, they showed that protocols 2 and 3 are not wide-weak private and that protocol 1 is not wide-strong private. As a consequence, for EC-RAC IV weaker claims have been made about protocol 1 (now claimed wide-weak), protocol 2 was removed, and protocol 3 revised and claimed wide-weak [11].

Regarding EC-RAC III, it is worth noting that Vaudenay had already shown [14] that in his model there cannot be a correct[1] protocol that is wide-strong private. This explains the existence of the wide-*strong* man-in-the-middle attack of Fan et al. [21] on EC-RAC III. In Section 5, we will show that none of the EC-RAC IV protocols are even wide-*weak* private, thus invalidating the latest revisions [11]. The attacks we show are sufficiently general to be applicable to all protocols in the EC-RAC I through IV set.

[1] A protocol is correct if it allows the RFID reader to infer a legitimate tag's identity from the communication with the tag.

2.3 Message sequence charts

We use message sequence charts, such as in Figure 1, for the description of protocols as well as attacks on protocols.

Every message sequence chart shows the role names, framed, near the top of the chart. Above the role names, the terms known to the role, but not known to the adversary, are shown. Actions, such as nonce generation, computation, verification of terms, and assignments are shown in boxes. Messages to be sent and expected to be received are specified above arrows connecting the roles. It is assumed that an agent continues the execution of its run only if it receives a message conforming to its role. Other conditions that need to be satisfied are shown in diamond boxes.

For example, for protocol A in Figure 1, the role names are R and T, corresponding to the RFID reader and tag, respectively. Both reader and tag know the secret term ID_T. The picture represents the following execution flow. R sends a query to T. After receiving the query, T generates a random value nt, then sends the message $nt, h(nt, ID_T)$ to R.

We use primes to distinguish messages from different executions. For instance, $nt, h(nt, ID_T)$ and $nt', h(nt', ID_{T'})$ represent the second message of protocol A (Figure 1) for two different executions.

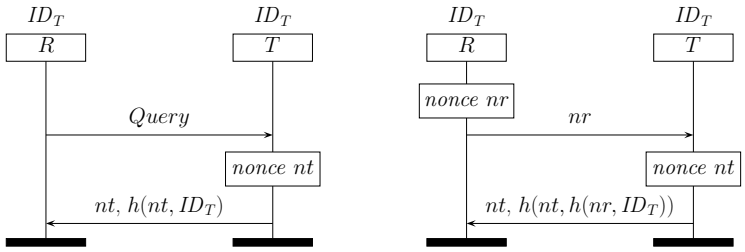
3 RFID privacy is not compositional

We first demonstrate that the composition of two private protocols may break the privacy of a tag. We then discuss the significance of this fact for RFID systems by showing two scenarios in which RFID privacy would be violated. In Section 4 we illustrate further implications of this result on the EC-RAC II protocols.

Consider the two protocols shown in Figure 1. The first protocol (A) is a tag identification protocol and the second protocol (B) is a tag authentication protocol. In both protocols we assume that a reader R and a tag T share a secret ID_T, not known to the adversary. The reader initiates the protocol by querying the tag. Then the tag generates a random number nt and sends its response to the reader.

If h is a cryptographically secure hash function, each of the protocols can be shown to be private in isolation. In a common environment, the protocols are not private.

Compositionality attack on protocols A and B. An attacker uses protocol A to build a database of tags he's interested in tracing. By querying a tag T, he obtains $nt, h(nt, ID_T)$ which he stores in the database. In



(a) Protocol A (b) Protocol B

Fig. 1: Protocols private in isolation, not in a common environment.

order to test whether a random tag T' is equal to a particular tag T in his database, the attacker uses protocol B. He sends the challenge nt to the tag. In protocol B the tag answers with $nt', h(nt', h(nt, ID_{T'}))$. The attacker can then obviously determine whether $ID_T = ID_{T'}$ by computing $h(nt', h(nt, ID_T))$ and comparing it with $h(nt', h(nt, ID_{T'}))$.

There are at least two scenarios in which this type of attack can become a significant problem.

Chosen protocol attack. It is not uncommon for smart cards to implement a protocol suite in order to host several applications. Therefore it is plausible that in the future RFID tags will host an implementation of several protocols or even protocol versions. Additionally, in the RFID setting, ownership transfer systems [22–24] are frequently constructed by implementing several protocols on the RFID tag. In view of the compositionality attack, however, it is obvious that a tag which implements protocols A and B does not provide privacy, in spite of the fact that both protocol A and B are private in isolation.

Protocol revision attack. Consider an RFID-based system where a large number of RFID tags implementing protocol A have been deployed. Suppose the RFID tag's ID_T value is linked to a particular customer in any of several participating companies' databases. Since protocol A is private, the RFID tag identifies the customer to an authorized entity, such as a retailer, a transportation company, or the local post office, but not to any entity the customer has not signed up with.

At a certain point in time it is decided that for future applications the identification protocol's security does not suffice, since its messages can be replayed. Protocol B is thus developed for applications which need to authenticate an RFID tag. To avoid the chosen protocol attack, customers will be provided with new RFID tags implementing

protocol B, but not protocol A, and their old tags will be destroyed. For convenience and in order not having to update all the customer entries in all distributed databases, the new tags will use the same credentials as the old tags. In particular, the tag identity communicated by a customer's RFID tag remains the same for each customer. This way, each retailer merely needs to update the firmware of its RFID readers to communicate using protocol B.
The compositionality attack described above, however, still applies. Anybody interested in tracing customers merely needs to be near a customer's tag once before the customer's RFID tag is replaced. This suffices to record the tag's protocol A message. Long after the transition to new tags has been completed and all protocol A tags are destroyed, the message recorded from protocol A can still be used to test whether a tag implementing protocol B belongs to the previously observed customer.

The protocols in Figure 1 are specially crafted protocols, designed to show that privacy is not a safely composable property and to illustrate the principle of using one protocol as an oracle to attack another protocol. In the following section the same principle will be used to show that the protocols comprising EC-RAC II [8] do not satisfy privacy nor security.

4 Compositionality attacks on the EC-RAC II protocols

4.1 Detailed description of EC-RAC II

EC-RAC II consists of six protocols shown in Figure 2. Common to all protocols are the publicly known points P and $Y = yP$ on a fixed, system-wide elliptic curve. The point yP can be considered as the RFID reader's public key, y being a scalar only known to the RFID reader. In protocols 1 and 4, RFID tags store a secret x_1. The corresponding public key is x_1P and is used by the reader to identify a tag. In protocols 2, 3, 5, and 6, RFID tags have two secrets x_1, x_2 with the corresponding public keys x_1P and x_2P uniquely identifying a particular RFID tag. In these four protocols the RFID reader knows the scalar x_1 of each tag.

All protocols follow the same commitment-challenge-response structure. More precisely, in all protocols the tag sends out a random point on the elliptic curve which serves as a commitment. The RFID reader challenges the tag with a random integer upon which the tag answers with a point depending on the commitment and the challenge. The idea of such schemes is that anybody able to produce the correct response can also

compute a particular secret. Thus successful completion of the protocol constitutes a proof of knowledge for the secret. A moment's thought shows that for the six protocols, knowledge of the points x_1Y and x_2Y allows an agent to authenticate itself as the tag whose public keys are x_1P and x_2P. Thus the intractability of the computational Diffie–Hellman problem is necessary in order for the schemes to provide tag authentication.

Protocols 1 through 3 are claimed to provide tag privacy and tag authentication. We will consider these claims in Section 5. In this section, we will assume correctness of these claims and investigate protocols 4 through 6 closer. Each of these protocols is, respectively, a composition[2] (or "superimposition") of protocols 1 through 3, with the following challenge-response protocol: The tag challenges the reader with a random point $T_1 = r_{t1}P$ on the elliptic curve and the reader answers with a related point $S_1 = yT_1$ on the curve in order to prove knowledge of its secret key y. We will refer to this challenge-response loop as O. Thus protocols 4 through 6 are additionally claimed to satisfy reader authentication.

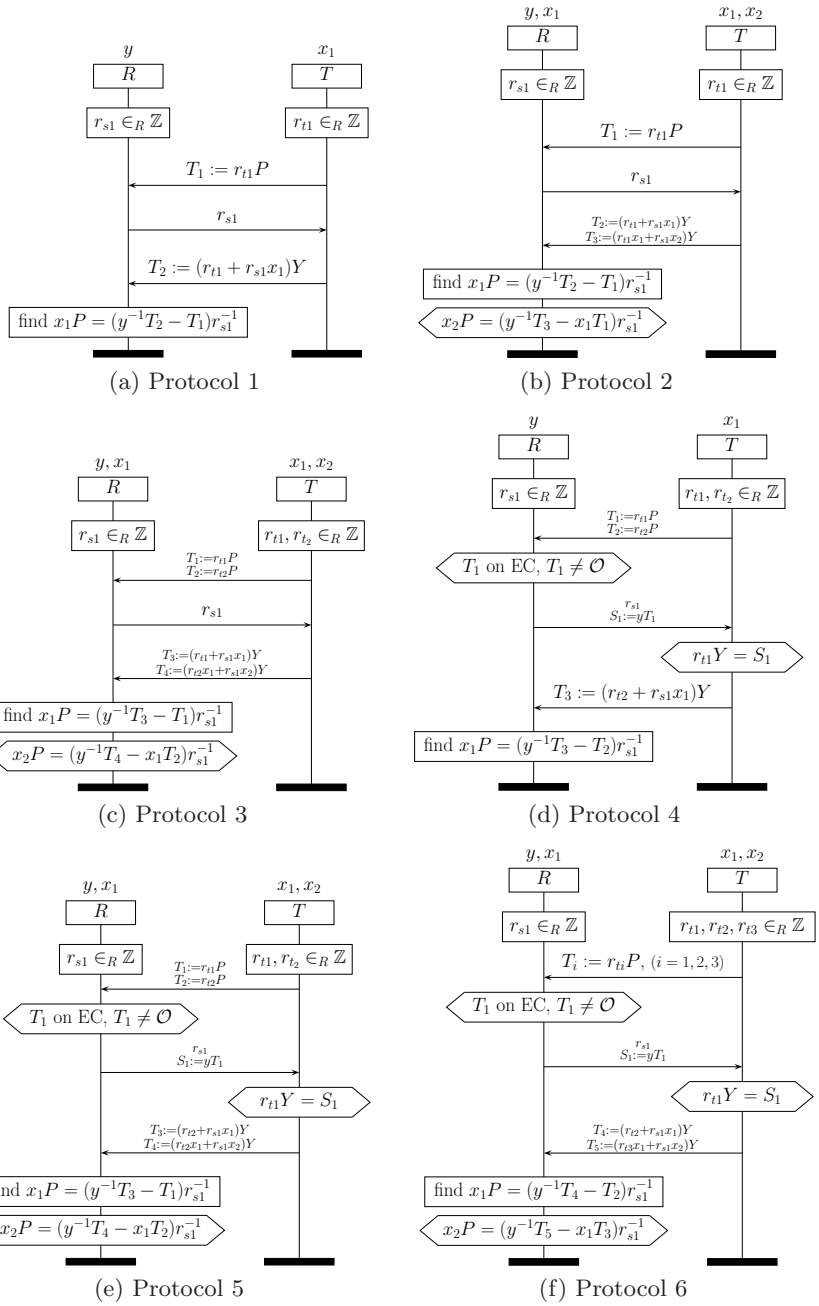
4.2 Compositionality attacks

We show that the privacy and tag authentication claims made for protocols 4 through 6 are false by exhibiting attacks which are analogous to the attack shown in Section 3. That is, we will use the challenge-response loop O as an oracle for the commitment-challenge-response flow of the protocols inherited from protocols 1 through 3.

The particular computation the oracle performs for the adversary is the multiplication of any nonzero point X by the reader's secret y. To use the loop O in the first two messages of protocols 4, 5, and 6 for this purpose, the adversary sends a nonzero point $T_1 = X$, along with a random point T_2 (and T_3 in protocol 6), on the system's elliptic curve to the reader. The reader replies with r_{s1} and $yT_1 = yX$, the multiple of the point X by the reader's secret key y. The adversary then simply drops the connection to the reader. In the following we will write this loop oracle as the function $X \to O(X) = yX$.

Privacy. Consider the messages $r_{t2}P$, r_{s1}, $(r_{t2} + r_{s1}x_1)Y$ an attacker learns from protocols 4, 5, and 6 by eavesdropping on a communication between an RFID reader and a tag. In order to trace the tag, the attacker

[2] To prevent confusion, we have preserved the naming scheme of EC-RAC II. As a consequence, the term T_1 in protocols 1, 2, 3 corresponds to term T_2 in protocols 4, 5, 6, respectively.



(a) Protocol 1 (b) Protocol 2

(c) Protocol 3 (d) Protocol 4

(e) Protocol 5 (f) Protocol 6

Fig. 2: The six EC-RAC II protocols

needs to be able to decide whether a tag presented to him is the same as the one he eavesdropped on earlier. By eavesdropping on another communication of a tag and reader (or by querying a tag himself) the attacker learns $r'_{t2}P$, r'_{s1}, $(r'_{t2} + r'_{s1}x'_1)Y$. He then computes

$$r_{s1}(r'_{t2} + r'_{s1}x'_1)Y - r'_{s1}(r_{t2} + r_{s1}x_1)Y \tag{1}$$

For $r_{s1}, r'_{s1} \neq 0$, the term in (1) is equal to $(r_{s1}r'_{t2} - r'_{s1}r_{t2})Y$ if and only if $x_1 = x'_1$, that is, if the tag being queried by the attacker later is the same tag as the one that was observed earlier. The attacker uses the oracle to decide whether this is the case or not: $O(r_{s1}r'_{t2}P - r'_{s1}r_{t2}P) = O((r_{s1}r'_{t2} - r'_{s1}r_{t2})P) = (r_{s1}r'_{t2} - r'_{s1}r_{t2})Y$. This equals the term in (1) if and only if the tag has been observed before.

Thus none of the protocols 4, 5, and 6 are narrow-weak private, which is the weakest privacy notion in Vaudenay's model. The attacker is narrow, since he is not relying on information related to the reader accepting or rejecting a tag. He is weak since he does not corrupt any tags.

Tag authentication. In order to break tag authentication in these protocols, an adversary needs to know the term x_1Y and in protocols 5 and 6 the adversary additionally needs to know the term x_2Y. The adversary learns these two terms from the tag's public keys x_1P, x_2P by computing $O(x_iP_1) = x_iY$, $(i = 1, 2)$. According to the attacker model specified for these protocols [8], an attacker is initially only allowed to know Y, P, and the order of the system's elliptic curve, but not the tags' public keys. Under this restriction, only a rogue reader in the system is able to impersonate tags. Protocol 4, however, is even vulnerable if the adversary does not know the tag's public keys. In this case the adversary can learn x_1Y by eavesdropping on one protocol execution between a tag and a reader and performing the following computation.

By eavesdropping on one communication between a tag and a reader, an attacker obtains $r_{t2}P$, the challenge r_{s1}, and $(r_{t2} + r_{s1}x_1)Y$. He then computes $r_{s1}^{-1}r_{t2}P$ and $r_{s1}^{-1}(r_{t2} + r_{s1}x_1)Y = (r_{s1}^{-1}r_{t2} + x_1)Y$. Using the oracle, the attacker obtains $O(r_{s1}^{-1}r_{t2}P) = r_{s1}^{-1}r_{t2}Y$ and computes the difference $(r_{s1}^{-1}r_{t2} + x_1)Y - r_{s1}^{-1}r_{t2}Y = x_1Y$. After learning x_1Y and x_2Y by using the oracles as described above, an attacker can impersonate a tag as follows.

Protocol 4. The attacker chooses a random integer r_{t1}, submits $r_{t1}P$ to the reader, and is challenged by r_{s1}. To answer this challenge, the attacker computes $r_{s1}x_1Y$, and $r_{t2}Y$ and sends back the sum of these two points.

Protocol 5. The attacker chooses random integers r_{t1}, r_{t2}, submits T_1, T_2 to the reader, and is challenged by r_{s1}. To answer this challenge, the attacker computes T_3 from the sum of $r_{s1}x_1Y$, and $r_{t2}Y$. To compute T_4, the attacker multiplies x_1Y by r_{t2} and x_2Y by r_{s1} and computes the sum of these two points.

Protocol 6. The attacker chooses random integers r_{t1}, r_{t2}, r_{t3}, submits T_1, T_2, T_3 to the reader, and is challenged by r_{s1}. To answer this challenge, the attacker computes T_4 from the sum of $r_{s1}x_1Y$, and $r_{t2}Y$. To compute T_5, the attacker multiplies x_1Y by r_{t3} and x_2Y by r_{s1} and computes the sum of these two points.

5 Privacy attacks on all EC-RAC protocols

We demonstrate a man-in-the-middle attack that allows a wide-weak adversary to trace a tag in all of the six protocols of EC-RAC II, as well as in EC-RAC III and IV. Fan, Hermans, and Vercauteren have shown that EC-RAC III is vulnerable to a man-in-the-middle attack by a *wide-strong* attacker [21]. Our man-in-the-middle attack can be executed by *any* wide attacker, in particular a wide-*weak* one.

Consider protocol 1 of EC-RAC II (Figure 2a) which is called the *ID-transfer protocol* in [8]. The equally named protocol of EC-RAC III and EC-RAC IV is a revision of this protocol designed to mitigate man-in-the-middle attacks. The main difference is that in EC-RAC III and IV a non-linear operation is applied to the reader challenge before it is used in the computation of the response.

Consider now protocol π in Figure 3. By specifying the function h used in the protocol, the ID-transfer protocols of EC-RAC II, III, and IV can be obtained. For EC-RAC II, h is simply the identity function. The specification of the h function in EC-RAC III and IV will be discussed below. Our attacks do not depend on the choice of the function h used in the protocol and work even if h is a cryptographic hash function.

To attack privacy, a *wide-weak* adversary eavesdrops on two protocol executions between a tag and a reader. In these executions he observes $T_1 = r_tP$, r_s, $T_2 = (r_t + h(r_s)x_1)Y$ in the first execution and $T_1' = r_t'P$, r_s', $T_2' = (r_{t1}' + h(r_s')x_1')Y$ in the second execution. Then the adversary computes $T_Y = h(r_s')T_2 - h(r_s)T_2'$ which is equal to $(h(r_s')r_t - h(r_s)r_t')Y$ if and only if $x_1 = x_1'$.

To find out whether this is the case, i.e. whether the two executions were carried out by the same tag, the adversary uses a communication

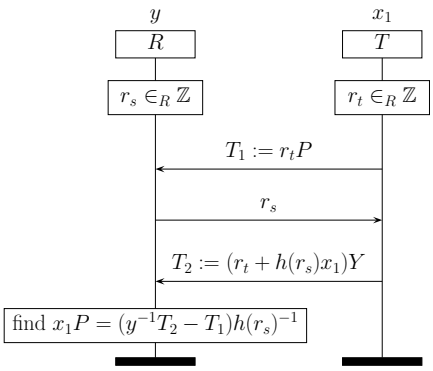


Fig. 3: Protocol π: A generalization of protocol 1

between *any legitimate tag* and a reader as an oracle, as shown in Figure 4. For brevity, in the MSC we have set $T_P = h(r'_s)T_1 - h(r_s)T'_1$ and $T_Y = h(r'_s)T_2 - h(r_s)T'_2$. Recall that a *wide* adversary can observe whether a tag was accepted by the reader or not, that is, whether the authentication protocol between the tag and reader was carried out successfully. If the reader accepts the legitimate tag, the adversary knows that $x_1 = x'_1$, otherwise $x_1 \neq x'_1$.

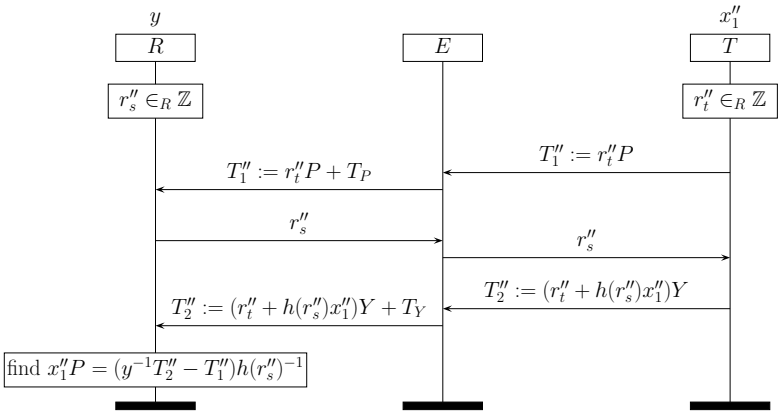


Fig. 4: Abusing any tag-reader communication of Protocol π as an oracle

The attack can be applied to protocol 1 of EC-RAC II by taking the identity map for the function h. Since protocols 2 through 6 are extensions of protocol 1 they inherit the vulnerability and can be attacked in the same way. The attacker merely forwards all terms that have been ad-

ditionally introduced in these protocols. To attack EC-RAC III and IV, the function h is instantiated by the following non-linear function introduced in EC-RAC III [10]. Let $x(P)$ denote the x-coordinate of a point P. Then $h(a) = x(aP)$. The attack can also be applied to the "Pwd-Transfer Scheme" of EC-RAC II and III. The only difference is that the adversary cannot use a communication between any tag and a reader as oracle, but only between the same tag and a reader. The combined "ID&Pwd-Transfer Scheme" of EC-RAC III and IV inherit the vulnerabilities of the ID-Transfer Scheme (and the Pwd-Transfer Scheme). The attack is applicable to EC-RAC I with a minor modification, since EC-RAC I does not follow a commitment-challenge-response structure.

6 Wide-weak privacy from narrow-weak privacy

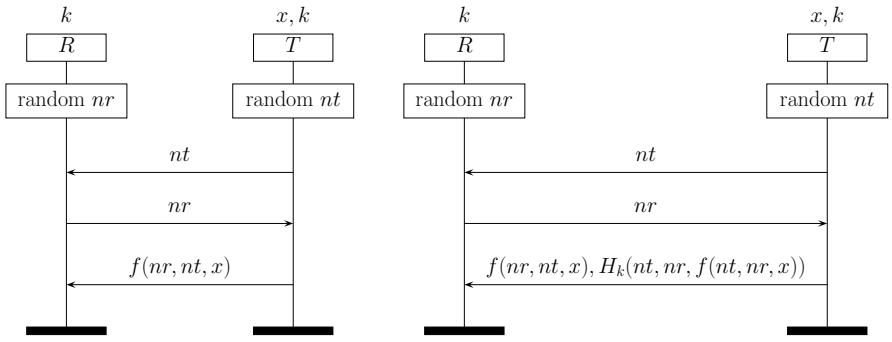
The man-in-the-middle attacks presented in the preceding section show that the EC-RAC family of protocols is not private against a *wide* attacker. Achieving narrow-weak privacy, however, appears to be significantly easier. In this section, we will show how to transform narrow-weak private protocols into wide-weak private protocols.

We consider three-message protocols such as protocol ρ_0 shown in Figure 5a. Note that protocol π shown in Figure 3 in Section 5 (and thus most EC-RAC protocols) as well as the Bringer et al. protocol [19], which has been formally shown to be narrow-weak private, follow this structure. Assuming that protocol ρ_0 is narrow-weak private, we show that protocol ρ, shown in Figure 5b is *wide*-weak private. Protocol ρ extends protocol ρ_0 by including a message authentication code in the third message. The message authentication code is a keyed hash $H_k(\cdot)$ computed over all previous messages (including the payload of the current message). The keyed hash depends on a secret k known only to reader and tag, unique to each tag.

Theorem 1. *If protocol ρ_0 is narrow-weak private then protocol ρ is wide-weak private in the random oracle model.*

Proof. We use the random oracle model and assume that the keyed hash function $H_k(m)$ is implemented as the random oracle $\mathcal{H}(k, m)$. We need to show that the addition of a hash preserves the narrow-weak privacy of protocol ρ_0 and that protocol ρ satisfies Vaudenay's definition of security [14]. The theorem then follows from Vaudenay's Lemma 8 [14].

Narrow-weak privacy of protocol ρ. Let ρ_0 be a narrow-weak private protocol. It follows that the probability of a tag generating the



(a) Protocol ρ_0 (b) Protocol ρ

Fig. 5: Extending a narrow-weak private protocol to a wide-weak private protocol

same bit string nt more than once in protocol ρ_0 is negligible, or else a narrow-weak adversary would have a non-negligible advantage in breaking a tag's privacy.

We give now a step-wise transformation of protocol ρ_0 into protocol ρ. Concatenate with the last tag-to-reader message the keyed hash $H_c(nr, nt, f(nr, nt, x))$ of all preceding messages. Assuming that the adversary knows c and that all tags use the same keyed hash function H_c, this protocol is still narrow-weak private, since the adversary could have computed the hash himself. Now replace the key c of the hash function by a random key k_0, unknown to the adversary. Call this protocol ρ_1. This protocol is still narrow-weak private, because k_0 is independent of all tag identities.

Given that $\mathcal{H}$ is a random oracle, $H_k(m)$ does not reveal any information about k. Furthermore, for two inputs $m \neq m'$, given $H_k(m)$ and $H_{k'}(m')$, it is impossible for the adversary to decide whether $k = k'$. Let ρ be equal to ρ_1, except that k_0 is replaced with a key k, unique to every tag and chosen independently at random. Thus, since the probability of a tag generating the same random bit string nt twice is negligible and k is never used outside of $H_k(m)$, protocol ρ is a narrow-weak private protocol.

Security of protocol ρ. We verify the security property of ρ by using that ρ satisfies Lowe's agreement property [25] in a Dolev-Yao model. Recall that a protocol guarantees to an RFID reader R *agreement* with a tag T on the exchanged messages m_1, m_2, m_3, if whenever R completes a protocol run, apparently with T, then T has previously been running the protocol, apparently with R, using the same values

for the messages m_1, m_2, m_3 and there is a one-to-one relationship between the runs of R and T.
The agreement property of protocol ρ can be automatically verified with symbolic verification tools, such as Scyther [26] or Proverif [27]. We may then transfer the security property from the symbolic Dolev-Yao model to the random oracle model by using the fact that the Dolev-Yao model with hashes is sound in the random oracle model [28]. Security of ρ now follows by noticing that Lowe's agreement property implies Vaudenay's *matching conversation* definition for his security property (Definition 4 in [14]).

□

7 Repairing the flaws

We indicate how to repair all the flaws discovered in the preceding sections. The primary purpose is to illustrate prudent design principles for composing protocol components in Section 7.1 and to give an application of Theorem 1 in Section 6 showing how to improve narrow-weak privacy to wide-weak privacy. The wide-weak privacy of the resulting protocols, thus, depends on the original protocols' narrow-weak privacy. It is known that EC-RAC I is not narrow-weak private [1, 20, 19] and it has already been improved upon in [19]. Since the protocol in [19] has been proven narrow-strong private (implying narrow-weak privacy) and since it is also more efficient than EC-RAC II, III, and IV, we do not attempt to prove narrow-weak privacy of these protocols.

7.1 Compositionality

In view of existing results on compositionality [2–5], the attacks shown in Section 3 are not surprising, because one secret key y is being used for two different purposes. Both the tag authentication and the reader authentication depend on y.

The security of the protocol compositions can be improved by using independent secrets for the two components. The independence of the secrets assures that one component in the composition cannot be used as an oracle for the other. This can be achieved without compromising efficiency of the scheme. We equip the reader with a second secret y_2, generated randomly and independently of y, and store the point y_2P in every tag. In the second message, the reader sends y_2T_1 instead of yT_1, to prove reader authenticity to the tag. This modification improves the

authentication property of the protocols. With respect to privacy, the flaws shown in Section 5 still persist. Thus the improvements suggested in the following subsection need to be applied as well.

7.2 Man in the middle

To defend against the man-in-the-middle attacks, message authentication seems to be unavoidable. In its current form, protocol 1 provides recent aliveness [25]: the reader is guaranteed that the tag has recently produced a message. However, agreement [25] is clearly not satisfied as shown by the attack in Figure 4. At the end of the run, the reader believes the following messages were exchanged

$$r''_t P + T_P, \quad r''_s, \quad (r''_t + h(r''_s)x''_1)Y + T_Y,$$

while for the tag the transcript reads

$$r''_t P, \quad r''_s, \quad (r''_t + h(r''_s)x''_1)Y.$$

As shown in Section 5, the adversary abuses this discrepancy and the reader's reaction to trace tags. To foil the attack, we need to make sure that reader and tag agree on the contents of all messages.

The simplest solution is to use message authentication codes based on an independent, shared secret, as shown in Section 6. Let k denote a secret known only to reader and tag, unique to each tag. Assuming that protocol π satisfies narrow-weak privacy, the addition of the hash $H_k(r_t P, r_s, (r_t + h(r_s)x_1)Y)$ to the last message thus guarantees wide-weak privacy. The non-linear function introduced in EC-RAC III can be omitted, thus h can be chosen to be the identity function. Although our solution prevents the man-in-the-middle attacks described, it is more resource intensive, since it additionally requires a secure hash function to be computed by the tag.

8 Conclusion

We have shown that protocols that are private in isolation, are in general not private when executed in a common environment. This insight is of particular significance in systems which need to be upgraded to newer protocol versions and in systems which require more than one protocol to be implemented on the RFID tag, such as ownership transfer applications [22–24]. We have further demonstrated the implication of our result

on EC-RAC II, a recently published family of RFID protocols. We have shown attacks whose existence is a direct consequence of the attempt to trivially compose private or authenticating components.

Our second class of contributions concerns wide-weak privacy. We have first proven that none of the EC-RAC protocols published to date is secure against any wide adversary, implying that all EC-RAC protocols are at most narrow-strong private. We have shown this by exhibiting a general man-in-the-middle attack, applicable to all versions of EC-RAC. We have then shown how to improve typical three-message narrow-strong private RFID protocols to wide-weak private protocols in the random oracle model. This improvement applies in particular to the provably narrow-weak private protocol proposed in [19]. We thus conclude EC-RAC noting that it does not improve upon more efficient nor provably narrow-strong private protocols.

References

1. van Deursen, T., Radomirović, S.: Attacks on RFID protocols (version 1.1). Cryptology ePrint Archive, Report 2008/310 (August 2009) http://eprint.iacr.org/2008/310.
2. Heintze, N., Tygar, J.D.: A model for secure protocols and their compositions. IEEE Trans. Software Eng. **22**(1) (1996) 16–30
3. Kelsey, J., Schneier, B., Wagner, D.: Protocol interactions and the chosen protocol attack. In: Security Protocols Workshop. (1997) 91–104
4. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: FOCS. (2001) 136–145
5. Andova, S., Cremers, C., Gjøsteen, K., Mauw, S., Mjølsnes, S., Radomirović, S.: A framework for compositional verification of security protocols. Information and Computation **206** (February-April 2008) 425–459
6. Cremers, C.: Feasibility of multi-protocol attacks. In: Proc. of The First International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, IEEE Computer Society (April 2006) 287–294
7. Tzeng, W.G., Hu, C.M.: Inter-protocol interleaving attacks on some authentication and key distribution protocols. Inf. Process. Lett. **69**(6) (1999) 297–302
8. Lee, Y., Batina, L., Verbauwhede, I.: Untraceable RFID authentication protocols: Revision of EC-RAC. In: IEEE International Conference on RFID – RFID 2009, Orlando, Florida, USA (April 2009) 178–185
9. Lee, Y.K., Batina, L., Verbauwhede, I.: EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In: Proceedings of the 2008 IEEE International Conference on RFID. (2008) 97–104
10. Lee, Y.K., Batina, L., Singelée, D., Verbauwhede, I.: Low-cost untraceable authentication protocols for RFID. In: 3rd ACM Conference on Wireless Network Security – WiSec'10. (2010)
11. Lee, Y.K., Batina, L., Singelée, D., Verbauwhede, I.: Wide-weak privacy-preserving RFID authentication protocols. In: The 2nd International Conference on Mobile Lightweight Wireless Systems – Mobilight 2010, Springer-Verlag (2010)

12. 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)
13. 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
14. 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
15. van Deursen, T., 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
16. Ha, J., Moon, S., Zhou, J., Ha, J.: A new formal proof model for RFID location privacy. In: ESORICS 2008, 13th European Symposium on Research in Computer Security. Volume 5283 of Lecture Notes in Computer Science., Springer (2008) 267–281
17. Ma, C., Li, Y., Deng, R.H., Li, T.: RFID privacy: relation between two notions, minimal condition, and efficient construction. In: ACM Conference on Computer and Communications Security. (2009) 54–65
18. Damgård, I., Pedersen, M.Ø.: RFID security: Tradeoffs between security and efficiency. In: CT-RSA. (2008) 318–332
19. Bringer, J., Chabanne, H., Icart, T.: Cryptanalysis of EC-RAC, a RFID identification protocol. In: CANS. (2008) 149–161
20. van Deursen, T., Radomirović, S.: Algebraic attacks on RFID protocols. In: Information Security Theory and Practices. Smart Devices, Pervasive Systems, and Ubiquitous Networks (WISTP'09). Volume 5746 of Lecture Notes in Computer Science., Springer (2009) 38–51
21. Fan, J., Hermans, J., Vercauteren, F.: On the claimed privacy of EC-RAC III. Cryptology ePrint Archive, Report 2010/132 (2010) http://eprint.iacr.org/.
22. Song, B.: RFID Tag Ownership Transfer. In: Workshop on RFID Security – RFIDSec'08, Budapest, Hungary (July 2008)
23. Dimitriou, T.: rfidDOT: RFID delegation and ownership transfer made simple. In: Proc. 4th International Conference on Security and Privacy in Communication Networks, ACM (September 2008) 1–8
24. van Deursen, T., Mauw, S., Radomirović, S., Vullers, P.: Secure ownership and ownership transfer in RFID systems. In: ESORICS 2009, 14th European Symposium On Research In Computer Security. Volume 5789 of Lecture Notes in Computer Science., Springer (2009) 637–654
25. Lowe, G.: A hierarchy of authentication specifications. In: 10th Computer Security Foundations Workshop (CSFW '97), June 10-12, 1997, Rockport, Massachusetts, USA, IEEE Computer Society (1997) 31–44
26. Cremers, C.: Scyther - Semantics and Verification of Security Protocols. Ph.D. dissertation, Eindhoven University of Technology (2006)
27. Blanchet, B.: An efficient cryptographic protocol verifier based on prolog rules. In: 14th IEEE Computer Security Foundations Workshop (CSFW), IEEE Computer Society (2001) 82–96
28. Backes, M., Pfitzmann, B., Waidner, M.: Limits of the BRSIM/UC soundness of Dolev-Yao models with hashes. In: ESORICS 2006, 11th European Symposium

on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings. Volume 4189 of Lecture Notes in Computer Science., Springer (2006) 404–423