Yet Another Ultralightweight Authentication Protocol that is Broken

Gildas Avoine, Xavier Carpent

Université catholique de Louvain
B-1348 Louvain-la-Neuve
Belgium

Abstract

Eghdamian and Samsudin published at ICIEIS 2011 an ultralightweight mutual authentication protocol that requires few bitwise operations. The simplicity of the design makes the protocol very suitable to low-cost RFID tags. However, we demonstrate in this paper that the long-term key shared by the reader and the tag can be recovered by an adversary with a few eavesdropped sessions only.

Keywords: Authentication, Ultralightweight protocol, RFID.

1. Introduction

The market pressure to lower the price of tags is such that it has become a major topic of research to design an RFID protocol requiring very few gates and little computational power on the tag side. Several families of protocols have been proposed, such as the influential HB family (see [2] for a thorough presentation of the HB family), and other "human authentication" protocols. In [4], Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, and Ribagorda introduced a mutual protocol, called LMAP, which is the first of what came to be known as the "ultralightweight protocols family". Many proposals followed (see [1] for a comprehensive introduction to this protocol family), but almost all of them have been broken. These protocols rely on very simple building blocks, such as bitwise operations ($\oplus$,$\vee$, $\wedge$), modular addition ($+$), or data-dependent rotations ($\mathrm{Rot}(x, y)$). They often do not require the tag to generate randomness, and require tags to update their state every successful authentication. Recently, Eghdamian and Samsudin proposed a new protocol in that family, claiming more security than its predecessors. We show in this paper how a passive attack can recover the 96-bit secret of a tag, using only 20 authentication sessions on average.

2. Eghdamian and Samsudin's Protocol

The protocol designed by Eghdamian and Samsudin [3] consists of four messages, represented on Fig. 1. First of all, the reader sends an hello message, then the tag sends its IDS, and finally the reader sends A and B, and the tag C. The content of A, B, and C is as follows:

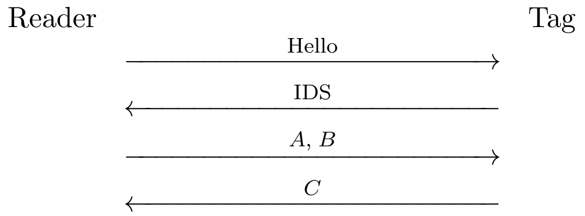

Figure 1: Eghdamian and Samsudin's Protocol

$$A = K \oplus N \tag{1}$$
$$B = \mathrm{Rot}(K, N) \wedge \mathrm{Rot}(N, K) \wedge \mathrm{Rot}(N, N) \tag{2}$$
$$C = \mathrm{Rot}((K + \mathrm{Rot}(N, N)), (\mathrm{Rot}(K, K) \vee N)) \tag{3}$$

where $\mathrm{Rot}(X, Y)$ means that X is rotated of $\mathcal{H}(Y)$ bits to the left, where $\mathcal{H}(Y)$ denotes the Hamming weight of Y. The symbol N represents a random value. After a successful authentication, the tag updates its key and session identifier as follows:

$$K^{next} = \mathrm{Rot}(N + \mathrm{Rot}(K, K), \mathrm{Rot}(N, N) \wedge K) \tag{4}$$
$$\mathrm{IDS}^{next} = K \wedge \mathrm{Rot}(N, K \vee N) \tag{5}$$

Let L denote the length of all the variables (recommended to be 96 in [3]):

$$|K| = |N| = |A| = |B| = |C| = |IDS| = L.$$

3. Attack

We introduce in this section a key-recovery attack that allows an adversary to recover the key K shared by the reader and the tag. The attack requires a passive adversary to eavesdrop one authentication session where a property on the Hamming weight of N is ensured, as detailed below. If the adversary is active and knows the current IDS of her target, she can perform her attack without the presence of the targeted tag.

3.1. Discovering the Hamming weight of N

The first step of the attack aims to recover $\mathcal{H}(N)$. Below B_i denotes the bit at index i of B, with B_0 being the least significant bit of B. From Eq (2), we know that:

$$\forall i, 0 \leq i < L, (B_i = 1) \Rightarrow (K_{i-\mathcal{H}(N) \bmod L} = N_{i-\mathcal{H}(N) \bmod L} = 1).$$

Using Eq (1), we deduce:

$$\forall i, 0 \leq i < L, (B_i = 1) \Rightarrow (A_{i-\mathcal{H}(N) \bmod L} = 0). \tag{6}$$

Consequently, a candidate r for $\mathcal{H}(N)$ is discarded if Eq (6) is not satisfied. If only one candidate r among the n possible ones remains, then $\mathcal{H}(N) = r$. Experimentally, we observed that this case occurs with a probability close to 0.9 when $L = 96$. When more that one candidate remain, the adversary can keep the few candidates and discard the wrong ones later in the attack, or she can simply eavesdrop another authentication session in order to be luckier and obtain a single candidate.
We consider from now on that the adversary knows $\mathcal{H}(N)$.

3.2. Recovering half of the secret bits

The adversary assumes that $\mathcal{H}(K) = \mathcal{H}(N)$. This assumption will be denoted H_1 in the following. Whenever H_1 is true, Eq (2) yields:

$$B = \mathrm{Rot}(K, N) \wedge \mathrm{Rot}(N, N),$$

and so:

$$\mathrm{Rot}^{-1}(B, N) = K \wedge N. \tag{7}$$

where Rot^{-1} means the right-rotation. We will denote below:

$$\widetilde{B} := \mathrm{Rot}^{-1}(B, N).$$

From Eq (1), we know that $A_i = 0$ implies that either $K_i = N_i = 0$ or $K_i = N_i = 1$. Consequently:

$$\forall i, 0 \leq i < L, (A_i = 0) \Rightarrow (K_i = \widetilde{B}_i).$$

This technique allows the adversary to recover half of the secret bits on average. Given that $\mathcal{H}$ follows a binomial distribution, Vandermonde's identity allows to demonstrate that the assumption H_1 actually occurs with probability $\binom{2L}{L}/2^{2L}$. When $L = 96$, this value is close to 0.058, which implies that the adversary should eavesdrop about 18 authentication sessions on average in order to observe one where the property $\mathcal{H}(N) = \mathcal{H}(K)$ is satisfied.

3.3. Recovering more secret bits

The adversary can increase the number of revealed bits of the secret key by exploiting the IDS following the session where H_1 is satisfied. Indeed, we know from Eq (5) that:

$$\mathrm{IDS}^{next} = K \wedge \mathrm{Rot}(N, K \vee N).$$

We conclude that

$$\forall i, 0 \le i < L, \left(\mathrm{IDS}_i^{next} = 1\right) \Rightarrow (K_i = 1)\,. \tag{8}$$

3.4. Recovering still more secret bits

Once some bits of K and N are known, the adversary can exploit them to recover more bits of K. For that, we can first trivially notice that:

$$K \vee N = (K \wedge N) \vee (K \oplus N). \tag{9}$$

When H_1 holds, we deduce, by inserting Eq (1) and Eq (7) in Eq (9):

$$K \vee N = A \vee \widetilde{B}. \tag{10}$$

Therefore, Eq (5) can be rewritten using Eq (10) as:

$$\mathrm{IDS}^{next} = K \wedge \mathrm{Rot}(N, A \vee \widetilde{B}). \tag{11}$$

If the adversary already knows i such that $K_i = 1$ then using Eq (1) and Eq (11), we deduce:

$$K_{i-\mathcal{H}(A\vee\widetilde{B})} = A_{i-\mathcal{H}(A\vee\widetilde{B})} \oplus \mathrm{IDS}_i^{next}. \tag{12}$$

Likewise, if the adversary already knows i such that $K_{i-\mathcal{H}(A\vee\widetilde{B})} \oplus A_{i-\mathcal{H}(A\vee\widetilde{B})} = 1$ then using Eq (1) and Eq (11), we deduce:

$$K_i = \mathrm{IDS}_i^{next}. \tag{13}$$

These two last steps can further be iterated a few times, until no more information can be gathered. At that point, most of the bits of K are known. We have observed experimentally that an average of 73 bits of K are discovered.

3.5. Recovering the remaining secret bits with a passive adversary

If the adversary is passive, she can recover the remaining secret bits performing a reasonable exhaustive search on the 23 unknown bits (on average). Candidates can be tested on C and B. If no suitable candidate is found in the exhaustive search, then the hypothesis $\mathcal{H}(K) = \mathcal{H}(N)$ was wrong, and another authentication attempt must be eavesdropped on.

3.6. Recovering the remaining secret bits with an active adversary

An active adversary can block the message C in order to cancel the update on the reader side, and thus force the tag to use the same IDS and K in the following session. This allows her to collect A, B, C messages for the same K, but different N, and therefore guess all the bits of K, with no exhaustive search required.

4. Conclusion

We have showed in this paper that Eghdamian and Samsudin's ultralightweight protocol is not secure, since a passive adversary can recover the key of a tag in an average of 20 authentication sessions. Although this number depends on L, the attack remains very efficient, even for bigger values of L than the recommended 96. This attack is an additional example of the lack of security of ultralightweight protocols, and it questions about the relevance of this approach to design authentication protocols.

References

[1] Gildas Avoine, Xavier Carpent, and Benjamin Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Applications*, 2011.

[2] Carl Bosley, Kristiyan Haralambiev, and Antonio Nicolosi. HB^N: An HB-like protocol secure against man-in-the-middle attacks. Cryptology ePrint Archive, Report 2011/350, 2011.

[3] Aras Eghdamian and Azman Samsudin. A secure protocol for ultralightweight radio frequency identification (RFID) tags. In *Informatics Engineering and Information Science – ICIEIS 2011*, volume 251 of *Communications in Computer and Information Science*, pages 200–213, Kuala Lumpur, Malaysia, November 2011. Springer.

[4] Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.