Active attack against HB$^+$: a provably secure lightweight authentication protocol

H. Gilbert, M. Robshaw and H. Sibert

Much research has focused on providing RFID tags with lightweight cryptographic functionality. The HB$^+$ authentication protocol was recently proposed and claimed to be secure against both passive and active attacks. A linear-time active attack against HB$^+$ is proposed.

Introduction: Much research has focused on providing RFID tags with lightweight cryptographic functionality. Particular interest has been paid to the issue of authentication, in order to both prevent counterfeiting and enhance privacy. In this Letter, we focus on an authentication protocol by Juels and Weis [1], which is to be presented at Crypto'05. This protocol, called HB$^+$, provides a symmetric authentication scheme that is claimed to be well-suited to low-cost devices such as RFID tags. In [1], HB$^+$ is presented as an enhanced variant of a protocol due to Hopper and Blum [2] (and known as the HB protocol). While HB was proven secure against passive attacks under the 'learning parity with noise' (LPN) hardness assumption, HB$^+$ is claimed to be secure against both passive and active attacks and a security proof is provided [1]. In this Letter, we show that HB$^+$ is vulnerable to an efficient active attack with linear computational and communication complexity. In this Letter, we first provide an outline of the LPN problem and the HB and HB$^+$ protocols; we then describe the attack and assess its cost; finally, we consider the implications of our observations.

LPN problem and HB and HB$^+$ protocols: In this Section we briefly review the HB and HB$^+$ protocols. It is interesting to note that they have much in common with a scheme first presented in [3]. Roughly speaking, the LPN problem requires an adversary to recover a k-bit secret x after being given several equations of the form $b_i = a_i \cdot x \oplus v_i$, with unknowns x and the v_is. Here v_i is a (noise) bit equal to 1 with a probability $\eta \in [0, 1/2]$. Throughout we denote the Hamming weight of a vector x by $|x|$.

Definition 1: The LPN problem with security parameters q, k, η, with $\eta \in [0, 1/2]$ is defined as follows: given a random $q \times k$ binary matrix A, a random k-bit vector x, a vector v such that $|v| \leq \eta q$, and the product $z = A \cdot x \oplus v$, find a k-bit vector x' such that $|A \cdot x' \oplus z| \leq \eta q$.

The HB scheme is a symmetric-key authentication protocol that is directly related to the LPN problem. The round described in Fig. 1 is repeated r times. The tag is authenticated if the checking procedure fails at most ηr times.

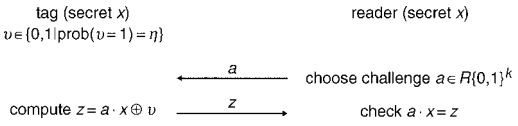

Fig. 1 *One round of HB protocol*

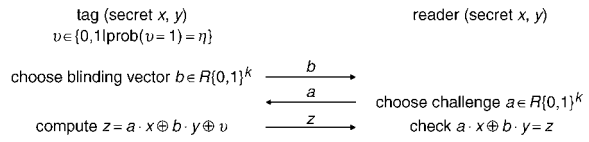

Fig. 2 *One round of HB$^+$ protocol*

Note that the HB scheme is not secure against active attacks. Since v is strictly less than $1/2$, by challenging the tag with some chosen a several times the value $a \cdot x$ will be revealed. Gaussian elimination will therefore give x once k equations with linearly independent as have been retrieved. The HB$^+$ protocol is an augmented version of the basic HB scheme. The aim of the HB$^+$ protocol [1] is to prevent the extraction of tag secrets by corrupt readers using such chosen challenges. The symmetric key now consists of two k-bit vectors x and y, and a blinding vector is first sent by the tag. The HB$^+$ round described in Fig. 2 is repeated r times and the tag successfully authenticated if the check fails at most ηr times (note 1).

Active attack against HB$^+$: Here we show a simple active attack against the HB$^+$ protocol. The attack requires that the adversary is capable of manipulating challenges sent by a legitimate reader to a legitimate tag during the authentication exchanges, and to check whether this manipulation results (or not) in an authentication failure. In detail, the attack consists of choosing a constant k-bit vector δ and using it to perturb the challenges sent by a legitimate reader to the tag: δ is XOR'ed to each authentication challenge for each of the r rounds of authentication. If the authentication process is successful, then we must have that $\delta \cdot x = 0$ with overwhelming probability. If authentication does not succeed then $\delta \cdot x = 1$ with overwhelming probability.

The attack is illustrated in Fig. 3 for one round of the HB$^+$ protocol. We use the same δ in all r rounds of the protocol. Acceptance or rejection by the reader would thereby reveal one bit of secret information. To retrieve the k-bit secret x, it is sufficient to repeat the full protocol k times for linearly independent δs, and to solve the resulting system. Conveniently, one can choose δs with a single nonzero bit. Once x has been derived, the attacker can either immediately impersonate the tag using commitment values $b = 0$, or the attacker can then derive (see note 2) the k-bit secret y using linearly independent linear combinations $b \cdot y$. Another side-effect of the disclosure of x is that the privacy of the tag's identity is also compromised.

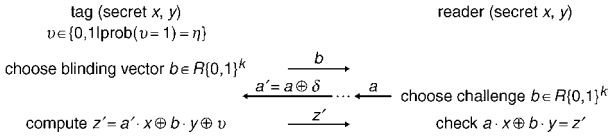

Fig. 3 *Attack on one round of HB$^+$ protocol*

Discussion: We have described an active attack against the HB$^+$ protocol [1] that has a complexity linear in the length of the keys and number of rounds. It is interesting to consider how such an attack evades the proof of security that accompanies the HB$^+$ protocol [1]. The main problem is that the security model in [1] does not take account of the potential leak of information by a legitimate verifier as well as a legitimate prover. In the attack, each 'accept' or 'reject' outcome from a legitimate verifier provides one bit of information about the shared secret key x. Moreover, an attacker is not restricted to attacking the tag only, and then the reader only, as the proof of security demands. Instead the adversary interacts with both at the same time to gain an advantage.

From a practical point of view, the most obvious way to mount the attack is to use a false reader to communicate with the legitimate tag and a false tag to communicate with the legitimate reader. Note that the false reader and tag need not be in the same physical place, they need only communicate with each other. However, such a man-in-the-middle configuration is not really required. Instead an adversary need only cause controlled perturbations to the challenges sent from the reader to the tag.

It is worth noting that, while the attacker interacts with both the tag and the reader, this is done in an unintrusive manner. From the point of view of the reader, either authentication with a legitimate tag has been successful or it has been unsuccessful (due, for instance, to a noisy transmission). In both cases the attacker gains information and the reader is unlikely to be aware that an attack has taken place.

Conclusion: While protocols with a proof of security are to be welcomed, caution demands that the security model be sufficiently robust. Given the practical nature of the attack outlined here, it is fair to conclude that the security model considered in [1] is too restrictive and that the HB$^+$ protocol is vulnerable to a realistic active attack.

Notes: 1. A straightforward generalisation of HB$^+$ consists in replacing the authentication acceptance threshold ηr by $\eta' r$, where η' is a constant which may differ from η. It is easy to see that the attack described in this Letter is also applicable to this slight variant of HB$^+$.

2. These can be obtained by using, for instance, a false tag that sends a chosen blinding factor b to a legitimate reader during a complete execution of the protocol, and returns $a \cdot x$ to each authentication

challenge a. If the authentication is successful then $b \cdot y = 0$ with overwhelming probability. If authentication does not succeed then $b \cdot y = 1$ with overwhelming probability.

19 July 2005
Electronics Letters online no: 20052622
doi: 10.1049/el:20052622

H. Gilbert and M. Robshaw (*France Télécom, R&D Division, 38–40, rue du Général Leclerc, 92794 Issy les Moulineaux, Cedex 9, France*)

E-mail: matt.robshaw@francetelecom.com

H. Sibert (*France Télécom, R&D Division, 42, rue des Coutures, BP 6243, 14066 Caen, Cedex 4, France*)

References

1 Juels, A., and Weis, S.A.: 'Authenticating pervasive devices with human protocols' *in* Shoup, V. (Ed.): Advances in Cryptology – Crypto 05, *Lect. Notes Comput. Sci.* (Springer-Verlag) (to appear 2005). Also available via http://www.rsasecurity.com/rsalabs/

2 Hopper, N.J., and Blum, M.: 'Secure human identification protocols' *in* Boyd, C. (Ed.): 'Advances in cryptology – Asiacrypt'01, *Lect. Notes Comput. Sci.*, 2001, **2248**, pp. 52–66

3 Gilbert, H.: 'Techniques for low cost authentication and message authentication' *in* Quisquater, J.J. (Ed.): 'Smart card research applications', Proc. CARDIS'98, Louvain-la-Neuve, Belgium, September 1998, *Lect. Notes Comput. Sci.*, 2000, **1820**, pp. 183–192