Securing HB+ against Man-in-the-middle Attacks

Dang Nguyen Duc* and Kwangjo Kim*

E-mail: {nguyenduc, kkj}@icu.ac.kr

*International Research Center for Information Security (IRIS)

Information and Communications University (ICU)

Abstract

In Crypto'05, Juels and Weis proposed an efficient and provably secure authentication protocol for RFID devices, namely HB+. The protocol is adapted from a human authentication protocol called HB which was proposed earlier by Hopper and Blum. Although HB+ is more secure than HB, it still suffers from an inherent weakness of HB. That is, HB+ is not shown to be provably secure against the strongest type of attack, *e.g.,* man-in-the-middle attack. This problem was quickly demonstrated by Gilbert *et al.* They presented a man-in-the-middle-attack with linear complexity which can discover a secret information shared by a RFID tag and a RFID reader. Till then, an efficient variant (e.g., without using any additional primitive) of HB+ which is secure against active adversaries remains an open question. In this paper, our goal is to solve this open question. We propose an augmented version of HB+ and show that the new protocol is secure against man-in-the-middle attacks. Comparing to HB+, our improved protocol requires only one more secret and minimal additional computation at tag and reader's side. And therefore HB* is still usable for RFID devices.

I. Introduction

Research on lightweight cryptographic protocols has attracted significant attention in the cryptologic community. A lightweight cryptographic protocol can be informally defined as an extremely efficient one yet obtain a reasonable level of security comparing to the conventional protocols. The main motivation behind this trend is the blossom of various kinds of pervasive devices as we enter the so-called ubiquitous computing era. Pervasive devices like mobile phones, personal assistance devices (PDA), sensors, smart cards and RFID tags, *etc.* share a common characteristic that its computational ability is very limited, sometimes even extremely basic as in the case of passive RFID tags. As a result, it is inappropriate to use most of conventional security protocols, which have been designed for fully functional computers, in these devices.

RFID security is one of the hottest subjects in the cryptologic community in recent years. RFID system is a promising technology to replace with Barcode-based recognition system and provide much more powerful applications. By tagging each and every object with a unique identification which can be read by RFID readers using radio communication, people can virtually identify and keep track of everything.

And this potential results in limitless applications, most notably automated supply chain management, smart home appliances, library management, *etc.* However, besides its prospective usefulness, RFID technology also brings a long security threat to personal and business sectors. The security concern is two-fold: Fake RFID tags results in impersonation and counterfeiting products; The availability of unique identification results in the disclosure of personal belongings, preferences and movements. Many protocols for RFID devices have been proposed to address the above security issues [9,10,11,12,13,18]. Among these protocols, HB+ protocol by Juels and Weis is considered to be the most interesting one because their protocol is very efficient to implement on extremely low-cost hardware and bases its security on a well-studied hard problem called *Learning Parity in the Presence of Noise* (LPN for short). The LPN problem is relatively new to the cryptologic applications but better known in the machine learning area and has been shown to be NP-hard. The origin of HB+ can be traced back to the work of Hopper and Blum's Asiacrypt'01 paper [7]. Hopper and Blum [7] presented two provably secure human authentication protocols, one of which depends on the hardness of the LPN problem (and usually referred to as HB protocol). Because HB protocol can be carried out by a human, it is conceivable that HB is also suitable for computationally limited devices. Note that, in case of human authentication, a person authenticates to a machine and we can assume that the machine is trusted. However, it is different in RFID environment because RFID tags and readers communicate in an automated manner so neither tags nor readers need to be trustful. As a consequence, Juels and Weis designed HB+ from HB in a way that a malicious reader has little chance of violating security of the protocol, *e.g.,* extracting secret information stored in a tag. HB+ as well as HB protocols are shown to achieve its intended security features assuming that LPN problem is hard.

Unfortunately, HB+ is only secure against active adversaries (also known as secure in *detection model*). Resistant against more advanced attacks like man-in-the-middle attack was not achieved in [14]. This drawback was quickly shown by Gilbert *et al* (GRS attack for short) in [15]. By presenting a man-in-the-middle attack with linear complexity, they proved that tag's secret can be recovered with high probability.

Our contribution. In this paper, we present an augmented version of HB+ protocol to thwart the man-in-the-middle attack like GRS attack. Our proposed protocol introduces reasonable computational and communication overhead comparing to HB+ protocol.

II. The Previous Works

1. HB Human Authentication Protocol and LPN Problem

The HB protocol involves the computation of binary inner product of two k-bit numbers. The operation is defined as follows: given two k-bit number $a = (a_0 a_1 ... a_{k-1})_2$ and $x = (x_0 x_1 ... x_{k-1})_2$, the binary inner product of a and x, denoted as $a \cdot x$ is computed as follows: $a \cdot x = (a_0 \wedge x_0) \oplus (a_1 \wedge x_1) \oplus ... \oplus (a_{k-1} \wedge x_{k-1})$.

This binary inner product operation can be carried out relatively easy by a human as well as by low-cost devices (like RFID tag). It is easy to show that binary inner product operation follows distributive law: $(a \oplus b) \cdot x = (a \cdot x) \oplus (b \cdot x)$.

In the HB protocol, the human (denoted as H, also called the prover) and a machine (denoted as C, also called the verifier) share a secret x of k-bit long. The protocol consists of several executions of a basic challenge-response protocol which is described in Fig. 1.

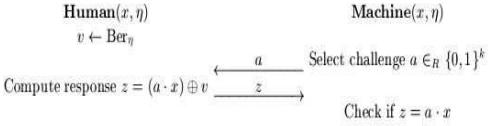

Fig. 1. HB Protocol

Ber_η denotes Bernoulli distribution with expected value η (that is the bit v - known as noise bit - is generated independently for each protocol round with probability η). The purpose of v is to prevent adversaries from extracting the secret x by eavesdropping k pairs (a, z). The machine accepts the human after say r rounds of the above protocol if and only if human produces roughly $r\eta$ incorrect responses (usually we can enforce the threshold to be strictly less than $r\eta$).

It is quite straightforward that HB protocol is secure only if an eavesdropper observing messages exchanged between H and C has a negligible chance of impersonating H. More specifically, an eavesdropper A obtains r pairs (a, z) and tries to deduce a k-bit number x' such that using x' to carry out HB protocol, A would get accepted by C. The problem of finding such x' is called *Learning Parity in the Presence of Noise problem* (LPN). However, as noted by Katz and Shin in [17], finding x' is essentially equivalent to finding x itself.

The LPN problem has been extensively studied in several research works including [4,5,6]. Those results show that LPN problem is very likely an intractable problem. To solve LPN problem as mentioned before, the best known algorithm by Blum *et al.* has sub-exponential complexity of $2^{O(k/\log k)}$. Hopper and Blum even conjectured that there is no polynomial algorithm to solve LPN problem given that with an instance of the problem is randomly chosen.. The latest result related to the LPN problem is due to Regev [16], and Katz and Shin [17]. They showed that if LPN problem is hard, a $(k+1)$-bit string $(a, (a \cdot x) \oplus v)$ is indistinguishable from a true random $(k+1)$-bit string. In fact, Katz and Shin used this result to give more elegant security proofs of HB protocol family than ones provided by Juels and Weis. We are going to use their technique in the analysis of our proposed protocol.

2.HB+ Authentication Protocol

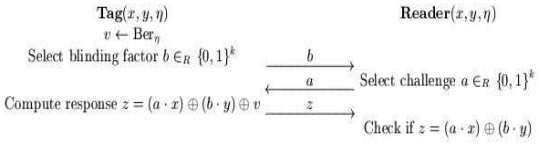

Fig. 2. HB+ Protocol

HB+ protocol is an augmented version of the HB protocol and it was proposed by Juels and Weis in [14]. HB+ preserves the efficiency nature of its ancestor while offers better security strength for RFID environment. In the HB+ protocol, a RFID tag (denoted as T) plays a role as a human and a RFID reader (denoted as R) plays a role as a machine. Comparing to the HB protocol, T and R share an additional k-bit secret y. To prevent a malicious reader from extracting the secrets stored in tag's memory, T first selects a random k-bit blinding factor and sends it to R. This blinding factor can effectively eliminate the threat of losing tag's secret to malicious readers. The detail of HB+ protocol is given in Fig. 2.

3.Man-in-the-middle Attack on HB+

In [17], Gilbert *et al.* presented a very effective man-in-the-middle attack which could allow an attacker to discover the secret x and y. The attack requires an attacker to intercept the challenge a sent by R and replace it with $a' = a \oplus \delta$. T then innocently computes the response z using a'. We have, $z = (a' \cdot x) \oplus (b \cdot y) \oplus v = ((a \oplus \delta) \cdot x) \oplus (b \cdot y) \oplus v = (\delta \cdot x) \oplus (a \cdot x) \oplus (b \cdot y) \oplus v$.

The attacker can use the same δ for all challenges in one session of the protocol. And if R accepts T, with high probability, $\delta \cdot x = 0$ since δ does not change the value of the correct response $z = (a \cdot x) \oplus (b \cdot y) \oplus v$. Otherwise, it is likely that $\delta \cdot x = 1$. By collecting k linear independent such δ, the attacker can discover x using Gaussian elimination. The attack is illustrated in Fig. 3.

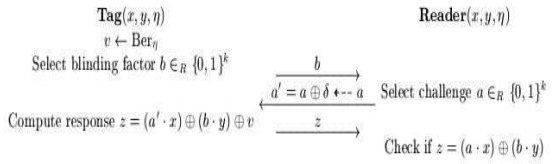

Fig.3. GRS Attack on HB+

III.HB* Protocol Secure against GRS Attack

We now present our variant of HB+ protocol which is secure against GRS attack and name our protocol HB*. We observe that in the HB+ protocol, the response z is always computed by associating the secret x with the challenge a and the secret y with the blinding factor b. This partly helps the GRS attack because an attacker knows that his modified challenge a' will be counted with respect to x. Note that, in term of security, there is no distinction between the role of x and y. Therefore, we think that it is possible to eliminate GRS attack by randomly swapping the role the x and y when computing the response z. The source of randomization should be de-randomized by R so that it can verify the response. In addition, any attacker neither de-randomizes this process nor tricks T into doing so. We propose an addition of one instance of the HB protocol into the HB+ protocol to achieve the goal.

In the HB* protocol, T and R share three k-bit secret x, y and s. There is one more noise parameter $\eta' \in (0, 1/2)$ which is not necessarily to be public. The other parameters are the same as in HB+ protocol. One round of the HB* protocol starts with T choosing a random k-bit blinding factor b and computing $w = (b \cdot s) \oplus \gamma$ where $\gamma \in \{0,1 \mid \text{Prob}(\gamma = 1) = \eta'\}$. Reader R then replies with a random k-bit challenge a. After receiving a, if $\gamma = 0$, T computes the response $z = (a \cdot x) \oplus (b \cdot y) \oplus v$. Otherwise, the response z is computed as $z = (a \cdot y) \oplus (b \cdot x) \oplus v$. Once collecting T's response z, R checks if $w = b \cdot s$, it verifies whether $z = (a \cdot x) \oplus (b \cdot y)$. Otherwise, it verifies $z = (a \cdot y) \oplus (b \cdot x)$. The protocol is described in Fig. 4.

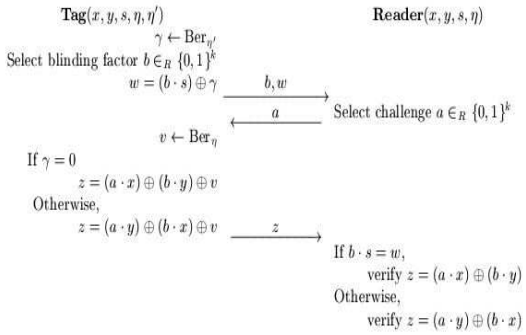

Fig.4. HB* Protocol

Similar to HB and HB+ protocols, after r rounds of the above basic protocol, R accepts T if less than $r\eta$ responses z from T are incorrect.

Regarding overhead introduced by our augmented computation, communication and storage, we think that our proposed solution causes only minimal increase comparing with the HB+ protocol. More specifically, our HB* protocol requires only one more k-bit secret, one more bit exchanged and two more binary inner product evaluations. Therefore, we can conclude that HB* is still suitable for very computationally limited devices.

IV.Security of HB* Protocol

In this section, we briefly summarize our security analysis of the HB* protocol. Full security proof of the protocol is available in the full version of this paper.

First of all, we can see that a direct application of the GRS attack does not work for HB* protocol. It is because an attacker who intercepts R's challenge a and changes it to $a' = a \oplus \delta$ cannot know which secret (either x or y) is associated with δ. Therefore, he cannot recover any secret. On the other hand, the pair (b, w) which is used to determine which secret is associated with a comes from only T. Therefore, having access to R does not help attacker discover the secret s which in turn means the possibility of the GRS attack.

Last but not least, an instance of the LPN problem formed by the pair (b, w) can be harder than the original LPN instance defined in [7]. It is because the noise factor η' needs not to be public or fixed and therefore it can be a secret to T. Current algorithms to solve LPN problem require noise factor as an input. As a consequence, the lack of knowledge of noise factor will likely increase the complexity of the algorithms.

V.Concluding Remarks

In this paper, we have presented HB* protocol, an augmented version of HB+ protocol which can prevent the man-in-the-middle attack described in [15]. Our protocol can be seen as a combination of two instances of the HB and HB+ protocols. Comparing with the HB+ protocol, our protocol requires one more additional secret, two more binary inner product computation and one more bit to transfer by the reader. Therefore, HB* can still be useful for tightly resource-constrained devices like RFID tags and sensor nodes.

References

[1] E. R. Berlekamp, R. J. McEliece and H. C. A Van Tilborg, ''On the Inherent Intractability of Certain Coding Problems'', IEEE Transactions on Information Theory, Vol. 24, pp. 384--386, 1978.

[2] Amos Fiat and Adi Shamir, ''How to Prove Yourself: Practical Solutions to Identification and Signature Problems'', Proceedings of CRYPTO'86, A. M. Odlyzko (Ed.), Springer-Verlag, LNCS 263, pp. 186 - -194, 1987.

[3] Oded Goldreich and L.A. Levin, ''Hard-core Predicates for Any One-Way Function'', 21st ACM Symposium on Theory of Computation, pages 25--32, 1989.

[4] Johan Hastad, ''Some Optimal Inapproximability Results'', Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, ACM Press, pp. 1--10, May, 1997.

[5] Michael Kearns, ''Efficient noise-tolerant learning from statistical queries'', Journal of ACM Volume 45, Issue 6, ACM Press, pp. 983--1006, November, 1998.

[6] Avir Blum, Adam Kalai and Hal

Wasserman, ''Noise-tolerant Learning, the Parity Problem, and the Statistical Query Model'', Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, ACM Press, pp. 435--440, 2000.

[7] Nicholas Hopper and Manuel Blum, ''A Secure Human-Computer Authentication Scheme'', Proceedings of ASIACRYPT'01, Bart Preneel (Ed.), Springer-Verlag, LNCS 2248, pp. 149 - -153, 2001.

[8] Stephen Weis, ''Security and Privacy in Radio Frequency Identification Devices'', Master Thesis, Available at http://theory.lcs.mit.edu/~sweis/masters.pdf, May 2003.

[9] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, ''Efficient Hash-Chain Based RFID Privacy Protection Scheme'', Proceedings of International Conference on Ubiquitous Computing, Workshop Privacy, September 2004.

[10] Gildas Avoine and Philippe Oechslin, ''A Scalable and Provably Secure Hash-Based RFID Protocol'', Proceedings of Workshop on Pervasive Computing and Communications Security - PerSec'05, March 2005.

[11] Gildas Avoine, Etienne Dysli, and Philippe Oechslin, ''Reducing Time Complexity in RFID System'', Proceedings of Selected Areas in Cryptography (SAC)'05, Bart Preneel and Stafford Tavares (Ed.), Springer-Verlad, LNCS 3897, pp. 291--306, 2005.

[12] D. Molnar, A. Soppera and D. Wagner, ''A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of a RFID Tag'', Proceedings of Selected Areas in Cryptography (SAC)'05, Bart Preneel and Stafford Tavares (Ed.), Springer-Verlad, LNCS 3897, pp. 276--290, 2005.

[13] Tassos Dimitriou, ''A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks'', Proceedings of SecureComm'05, September 2005.

[14] Ari Juels and Stephen Weis, ''Authenticating Pervasive Devices with Human Protocols'', Proceedings of CRYPTO'05, Victor Shoup (Ed.), Springer-Verlag, LNCS 3261, pp. 293 - -308, 2005.

[15] Henri Gilbert, Matthew Robshaw and Herv\'e Silbert, ''An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol'', Available at http://eprint.iacr.org/2005/237.pdf.

[16] Oded Regev, ''On Lattices, Learning with Errors, Random Linear Codes, and Cryptography'', Proceedings of 37th ACM Symposium on Theory of Computing, ACM, pp. 84--93, 2005.

[17] Jonathan Katz and Ji Sun Shin, ''Parrallel and Concurrent Security of the HB and HB+ Protocols'', Available at http://eprint.iacr.org/2005/461.pdf.

[18] Ari Juels, ''Strenthening EPC Tag against Cloning'', ACM Workshop on Wireless Security (WiSe), M. Jakobsson and R. Poovendran (Ed.), pp.67-76. 2005.