Analyses of Enhanced Security Protocol for HB Family RFID Mutual Authentication

양지수·김승민·김정태
목원대학교

HB 형의 RFID 상호 인증을 위한 향상된 보안 프로토콜의 해석

Ji-Su Yang, Seung-Min Kim, Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

RFID security protocol is widely discussed as an important issue, while the mutual authentication with the security agreement is mostly discussed enthusiastically. In this paper we improve HB family to achieve the property of mutual authentication, so that the user privacy can be protected. The future direction is to adapt the protocol for cloud computing.

Ⅰ. Introduction

RFID is a popular technology, and RFID system is composed of tags, a reader, and a back-end application system. RFID mainly transmits information stored in tags to a reader which is connected to the back end system by wireless technology,

RFID technology has received much attention in industry and academia in recent years. Previous research in this area has investigated the rigorous definition and modelling of privacy in RFID systems. The previous research differs in how they treat the adversary's ability to corrupt tags and their different privacy notions for corrupted tags. Much research have been carried out into lightweight protocols based on the learning parity with noise (LPN) problem, such as HB, HB+ and its variants etc [1]. The operations in the LPN problem involve the calculation of inner products of binary vectors and Bernoulli noise bit generation. Computing the binary inner product only requires bitwise AND and OR operations that can be computed on the fly. Therefore the LPN problem is a hardware-friendly primitive, and very attractive to low-cost RFID security. Like nost communication technologies, RFID has some security problems fir us to overcome, Some proposals about cryptographic algorithms and protocols for RFID systems have been proposed. With deep insight into HB protocol family, only dot product operation of binary vectors is needed while its security relies on the computational hardness of Learning Parity with Noise(LPN) problem, which has been proven as an NP complete problem.

II. Related Work

In 2001, Hopper and Blum proposed HB

protocol for RFID. HB protocol's security is based on difficulty of LPN(Learning Parity with Noise). In 2005, Juels and Weis mentioned HB protocol weakness, and pointed out that HB protocol can only protect against passive attacks, but cannot resist the reader's disguise malicious attacks. In 2007 Gilber successful used the man-in-the-middle attack to get the secret key x taken out from the HB+ protocol to prove that HB+ protocol still has room for improvement. Then in 2007, Munilla and Peinado proposed HB-MP protocol. HB-MP protocol only transmitted a random value. Compared with HB+, HB-MP is faster with fewer transfer processes. However, HB-MP protocol also cannot resist the man-in-the-middle attack because the value during transmission is changed so that tag will receives value that is not initiated by the value of the original reader [2].

III. Comparison of Security Mechanism

Security and communication analysis is shown in figure 1 [2]. Since HB-MP+ is based on the LPN, a passive attacker has to solve the LPN problem to reveal the secret key of x. As the protocol is also designated to have rounds keys which are rotated a random the security is updated in each round and synchronization problem is able to intensify security with the ultra simple 4 step function, XOR, LFSR, Rotate and Truncate [3].

	HB	HB+	HB-MP	HB-MP+
Resistant man-in-the-middle attack	No	No	No	No
Resistance disclosure	No	No	Yes	Yes
Privacy	No	No	No	No
Data integrity	No	No	No	Yes
Mutual authentication	No	No	No	No
Total messages for one way authentication	3L	3L	2L	2L
Memory size on tag	1L	2L	2L	1L
Memory size for each tag on database	1L	2L	2L	1L

IV. Conclusion

In this paper, we surveyed an improved RFID mutual authentication protocol, which added only two operators and extra five steps to achieve mutual authentication. Furthermore, the protocol had more comprehensive protection mechanism, but also retained the HB-MP+ protocol security for the HB series of RFID identification.

References

[1] Xiaolin Cao, "F-HB: An Efficient Forward Private Protocol", 2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications, pp.53-60

[2] Chia-Min Lin, "HB family RFID mutual authentication protocol", 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.230-235

[3] J. Munilla, A. Peinado, HB-MP牯 A Further Step in the HB Family of Light-weight Authentication Protocols, Computer Network, Vol. 51,2007, pp. 2262-2267.

[4] X, Leng, K. Mayes, K, Markantonakis, HB-MP+ Protocol An Improvement on the HB-MP Protocol, Proceedings of IEEE International Conference on RFID, April, 2008.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: 2012-0007896)