Analyses of Lightweight Privacy and Authentication Protocol for Passive RFID Tags

김정태
목원대학교

수동 RFID 태그를 위한 경량화된 보안 및 인증 프로토콜 분석

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

Radio frequency identification (RFID) tags are cheap, simple devices that can store unique identification information and perform simple computation to keep better inventory of packages. Because of this, they are intended to replace the barcodes for supply chain management in the near future. However, unlike barcodes, these tags have a longer range in which they are allowed to be scanned, subjecting them to unauthorized scanning by malicious readers and to various attacks. Therefore, a security protocol for RFID tags is needed to ensure privacy and authentication between each tag and their reader. In order to accomplish this, in this paper, we proposed a lightweight privacy and authentication protocol for passive RFID tags.

Ⅰ. Introduction

RFID is increasingly becoming more popular and is expected to replace the current barcode technology in the near future. But this breakthrough comes with its own caveats. There is a growing concern among people about consumer privacy protection and other security loopholes that make RFID tags an easy target for malicious attacks. Passive RFID tags in their current form are vulnerable to various types of attacks and thus there is a pressing need to make this technology more secure before it is viable for mass deployment. Privacy and authentication are the two main security issues that need to be addressed for the RFID technology.[1]

II. Related Wok

To reduce the gate count on a tag to accommodate security functions, there are a number of lightweight authentication protocols being proposed without assumptions on conventional cryptographic primitives. The HB family of RFID Authentication Protocols. Weis introduced the Hopper and Blum Protocol (HB) under the RFID setting. Subsequently, Juels and Weis proposed a lightweight authentication protocol(HB+) in Reference. The security of both the HB and HB+ protocols are based on the Learning Parity with Noise problem, whose hardness over random instances remains as an open question. However, Gilbert etal. showed that HB+ isnot secure against a simple MITM attack. To defend against such active attacks, Bringer et al. extended the protocols to HB++ protocol. In Ultra-Lightweight RFID Authentication Protocols, Vajda and Buttyan presented a set of extremely lightweight challenge response authentication protocols that are suitable for authenticating tags, but their protocols can be broken by a powerful adversary. So far, almost all those lightweight protocols are being attacked in some way, their practical deployment might be at risk unless strict security analysis is conducted. Recently, Peris-Lopez etal. proposed a family of ultra-lightweight mutual authentication protocols for low-cost RFID tags: LMAP, M2AP, and EMAP, in which only simple bitwise operations are used. The protocols have some merits on its innovative design of using only ultra-lightweight primitives, but this also induces higher risk. As such, their schemes suffer from serious attacks in which all secrets on a tag can be disclosed to an attacker either by active attacks or by passive attacks.[2]

III. Lightweight Mutual Authentication

There have been several hash based solutions that create authentication for systems. These solutions are not practical for low-cost tags due to the complexity of hash functions. Furthermore, most of these solutions do not authenticate the tag, and is vulnerable to man-in-the-middle attacks. Some lightweight solutions to securing RFID systems have also been proposed, including the HB family and the MAP family of protocols, however, they have been shown to have serious security flaws. TRMA and TRMA+ tried to adhere strictly to the EPC Class 1 Gen 2 standard of tags, however, they were broken. Some protocols based on PUF have been explored. These solutions require that the back-end is preloaded with a very large amount of challenge response pairs for the reader to use to verify the authenticity of the tag. Moreover, the HB-PUF solution does not provide mutual authentication. There exist fewer solutions to the ownership transfer problem than to mutual authentication for RFID. Some of them rely on hash functions or symmetric encryption functions. A similar solution to our two-party ownership transfer protocol is mentioned, which uses similar assumptions about the security of the backwards channel. The solution depends on the tags ability to execute a cryptographic function.[3]

IV. Conclusion

RFID is a promising technology that can revolutionize the way we lead our lives. However, before this becomes a reality, certain security issues like consumer privacy protection and fraud prevention and detection must be addressed and solved.

References

[1] Juels A. Rfid security and privacy: a research survey. IEEE Journal on Selected Areas in Communications 2006; 24(2): pp.381 394.

[2] Tieyan Li, "The security and improvement of an ultra-lightweight RFID authentication protocolThe security and improvement of an ultra-lightweight RFID authentication protocol", Security Comm. Networks. 2008; 1:135 146

[3] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, in Security in Pervasive Computing, LNCS 2802, pp. 201-212, 2003.

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:2010-0024133)