Secure and Efficient Mobile RFID Authentication Protocol

Hung-Min Sun[1,*], Shuai-Min Chen[1], Chen-En Lu[1], and Cheng-Ta Yang[2]

[1] Department of Information Engineering and Computer Science

National TsingHua University

HsinChu 300, Taiwan, ROC

{hmsun, sean, viva}@cs.nthu.edu.tw

[2] Department of Multimedia and Entertainment Science

Southern Taiwan University

Taiwan, ROC

zl8@mail.stut.edu.tw

Received 1 8 May 2009; Revised 1 July 2009; Accepted 8 July 2009

Abstract. There are varies of RFID authentication schemes have been proposed. Most of them address on privacy issues over the tag and the user, however, they are still vulnerable to different attacks and with some weaknesses. In addition, the readers and the back-end server are considered as a single entity for these typical RFID schemes, hence, the communication channel is assumed to be secure. Recently, a concept of mobile reader has been proposed in which the reader is possessed by the user and is equipped inside a mobile device. The mobile RFID reader possessor can extract the information about the tagged objects by communicating with the back-end server through an insecure channel; consequently, a secure RFID authentication is needed.

In this paper, two RFID authentication schemes are proposed for the reader-portable RFID environment. These schemes not only provide a novel usage of RFID system, but resolve privacy threats while a mobile reader is not authorized to acquire every tag's information.

Keywords: anonymity, authentication, privacy, mobile RFID, user-portable reader

References

[1] A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags," *International Conference on Security in Communication Networks – SCN'*04, LNCS 3352, pp. 149–164, September 2004.

[2] Auto-ID Center, "860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0," Technical Report MIT-AUTOID-TR-007, November 2002.

[3] G. Avoine and P. Oechslin, "RFID Traceability: A Multilayer Problem," *Financial Cryptography – FC'*05, LNCS 3570, pp. 125–140, 2005.

[4] D. Eastlake and P. Jones, US Secure Hash Algorithm 1 (SHA1), Internet RFC 3174, September 2001.

[5] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communication*, Vol. 24, pp. 381–394, February 2006.

[6] J. Kim and H. Kim, "A Wireless Service for Product Authentication in Mobile RFID Environment," *International Symposium on Wireless Pervasive Computing – ISWPC'*06, pp. 1–5, January 2006.

[7] T. Dimitriou, "A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks," *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm'05*, pp. 59-66, IEEE Computer Society Press, September 2005.

[8] S. Sarma, S. Weis, D. Engels, "RFID Systems and Security and Privacy Implication," *Workshop on Cryptographic Hardware and Embedded Systems – CHES'*02, LNCS vol. 2523, pp. 454-469, August 2002.

[9] R. L. Rivest, "The MD5 Message Digest Algorithm," Technical Report RFC 1321, MIT Lab for Computer Science and RSA Laboratories, April 1992.

[10] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Workshop on Cryptographic Hardware and Embedded Systems – CHES'04*, LNCS 3156, pp. 357–370, August 2004.

[11] M. Ohkubo, K. Suzuki, S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," *RFID Privacy Workshop* 2003, MIT, November 2003.

[12] S. L. Garfinkel, A. Juels, R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Transactions on Security and Privacy*, Vol.3, pp. 33–34, May/June 2005.

[13] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *International Conference on Security in Pervasive Computing – SPC'*03, LNCS 2802, pp. 454–469, March 2003.

[14] G. Avoine and P. Oechslin, "A Scalable and Provably Secure Hash Based RFID Protocol," *International Workshop on Pervasive*

* Correspondence author

*Computing and Communication Security – PerSec'*05, pp. 110–114, March 2005.
[15] A. Juels, R. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *ACM Conference on Computer and Communications Security – CCS'03*, pp. 103–111, October 2003.
[16] K. Fishkin, S. Roy, B. Jiang. "Some Methods for Privacy in RFID Communication"," *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS'*04, LNCS 3313, pp. 42–53, August 2005.
[17] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, "Mutual Authentication Protocol for Low-Cost RFID," Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
[18] D. Henrici and P. Muller, "Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," *Workshop on Pervasive Computing and Communications Security*, pp. 149–153, March 2004.
[19] A. J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
[20] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," *ACM Conference on Computer and Communications Security – CCS'04*, pp. 210–219, October 2004.
[21] G. Avoine, E. Dysli, P. Oechslin, "Reducing Time Complexity in RFID Systems," *Selected Area in Cryptography – SAC'*05, LNCS 3897, pp. 291–306, August 2005.
[22] S. M. Lee, Y. J. Hwang, D. H. Lee, J. I. Lim, "Efficient Authentication for Low-Cost RFID Systems," *International Conference on Computational Science and its Applications*, LNCS 3480, pp. 619–629, May 2005.
[23] K. Rhee, J. Kwak, S. Kim, D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," *International Conference on Security in Pervasive Computing – SPC'05*, LNCS 3450, pp. 70–84, April 2005.
[24] D. Morikawa, M. Honjo, A. Yamaguchi, S. Nishiyama, M. Ohashi, "Cell-Phone Based User Activity Recognition, Management and Utilization," *International Conference on Mobile Data Management – MDM'06*, pp. 51, May 2006.
[25] J. Bringer, H. Chabanne, E. Dottax, "HB^{++}: A Lightweight Authentication Protocol Secure against Some Attacks," *International workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SerPerU'06*, pp. 28–33, June 2006.
[26] Nokia unveils RFID phone reader. http://www.rfidjournal.com/article/view/834/
[27] Electronic Product Code Global Inc. http://www.epcglobalinc.org/
[28] H. Gilbert, M. Robshaw, H. Sibert, "Active Attack against HB^{+}: A Provably Secure Lightweight Authentication Protocol," *IEE Electronics Letters*, Vol. 41, pp. 1169–1170, October 2005.
[29] N. Hopper and M. Blum, "Secure Human Identification Protocols," *Advances in Cryptography – ASIACRYPT'*01, LNCS 2248, pp. 52–66, December 2001.
[30] S. Weis, "Security Parallels between People and Pervasive Devices," *International Workshop on Pervasive Computing and Communication Security – PerSec'05*, pp. 105–109, March 2005.
[31] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptography – CRYPTO'*05, LNCS 3621, pp. 293-308, August 2005.
[32] H. Y. Chien, "SASI: A New Ultra-Lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 4, pp. 337–340, 2007.