A Hybrid Mutual Authentication Protocol for RFID

Harinda Fernando and Jemal Abawajy

School of Information Technology, Deakin University, Geelong, Australia
{hsf,jemal.abawajy}@deakin.edu.au

Abstract. Out of the large number of RFID security protocols proposed in recent years none have proven to be truly secure and the creation of a truly secure security protocol for systems employing low cost RFID tags remains an open problem. In this paper we develop and present a RFID security protocol which not only allows mutual authentication and secure transmission of data between the reader and tag but is also secure against a number of common attacks.

1 Introduction and Related Work

RFID is a tagging technology that allows an object, place, or person to be automatically identified from a distance without visual or physical contact. Recently a number of RFID security protocols employing cryptographic hashes, public key encryption and PRNG on tag side have been proposed [1]. But these protocols proved to be too resource intensive to me implemented on low cost tags. Therefore protocols using ultra-light-weight cryptography was developed. Some of the more notable protocols in this area are the UMAP family and Gossamer [2]. Unfortunately these protocols were compromised soon after their publication. In this paper we present a mutual authentication protocol for networked RFID system. By using a hybrid of simple one way hash functions, reader side PRNG and bitwise operations we have developed a provably secure protocol whose resource requirements are compatible with low cost RFID tags.

2 Proposed Protocol

Both the tag and the backend system store the EPC and an associated IDS, K1 and K2 for each tag. On coming into contact with the radio wave field of a RFID reader the tag responds with its current IDS. If the received IDS is not recognized the protocol is terminated.

Once the reader has received the IDS it selects the matching EPC, K1 and K2 and generates the PRNG R. It then calculates M1 = H(EPC+K1) and M2 = (K1+R) and M1||M2 is transmitted to the tag. On receiving M1||M2 the tag uses the K1 and EPC it has on its memory to calculate C1= H(EPC+K1) and compares it to the received M1. If the two values match the reader is authenticated by the tag. If the values don't match the protocol terminates. Then the tag uses the K1 saved on its memory retrieves R from M2 and calculates M3 = H(EPC+K2+R) and transmits it to the reader. On receiving M3 the reader uses the EPC and K2 it received from the backend

P. Sénac, M. Ott, and A. Seneviratne (Eds.): MobiQuitous 2010, LNICST 73, pp. 310–311, 2012.

database to calculate C2 = H(EPC+K2+R) and compares it to M3. If they match the reader authenticates the tag else the protocol terminates.

Then the reader generates PRNG R2 and calculates M4 = (K1+R2) and M5 = H(EPC+R2) and broadcasts M4||M5. On receiving M4||M5 the tag retrieves R2 and calculates C2= H(EPC+R2). If C2 == M5 then the tag accepts the R2 else it discards and requests a new R2. Once a secure R2 is received the tag starts its key updating. To do this it updates its IDS. K1 and K2 as IDS = IDS + R2, K1 = (K1Right||K2Left) + R2 and K2 = (K2Right||K1left) + R2. Simultaneously the reader does the same calculations and transmits the IDSnew, K1new and K2new along with the EPC to the back end database which updates those values for that EPC.

3 Protocol Evaluation

Our protocol does not contain any of the common weaknesses from other protocols:

- Most protocols use multiple weakly encrypted messages containing the secret keys during authentication which can be leveraged by the attacker using crypto attacks. Our protocol transmits only one message which holds the secret values.
- Most RFID protocols broadcast the EPC of the tag allowing for data leakage attacks. Our protocol only broadcasts the EPC in one way hashed form.
- Some of the protocols employ bitwise AND and OR which have poor statistical properties. Our protocol only employs the XOR function which does not have a biased output eliminating this weakness.

The security analysis of the protocol further showed that the hybrid protocol successfully implements the core security concepts of mutual authentication, transmission confidentiality and integrity, anonymity and availability. It is also secure against a large number of common attacks including main-in-the middle attacks, eavesdropping attacks, replay attacks, tag cloning and spoofing, reader impersonation and de-synch attacks.

We also compared the performance of our protocol against a number of protocols. The analysis showed that our protocol compared favorable to both the ultra-light-weight protocols and the traditional protocols on the metrics of storage and required and overhead bandwidth. Under the metric of number of operations it was definitely less resource intensive than traditional protocols. While it required a hash function on the tag it also required significantly less boolean operations to be carried out when compared to the only currently unbroken ultra-light-weight protocol: Gossamer [2]

References

1. Lim, J., Oh, H., Kim, S.: A New Hash-Based RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection. In: Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 278–289. Springer, Heidelberg (2008)
2. Peris-Lopez, P., Hernandez-Castro, J.C., Tapiador, J.M.E., Ribagorda, A.: Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol. In: Chung, K.-I., Sohn, K., Yung, M. (eds.) WISA 2008. LNCS, vol. 5379, pp. 56–68. Springer, Heidelberg (2009)