Cryptology ePrint Archive: Report 2011/667

An Efficient and Private RFID Authentication Protocol Supporting Ownership Transfer

Suleyman Kardas and Atakan Arslan and Serkan Celik and Albert Levi

Abstract: Radio Frequency IDentification based systems, which are the most famous example of ubiquitous networks, are getting pervasively deployed in many daily life applications where privacy sensitivity is entrusted to tag or server. In some applications, ownership transfer of RFID labels is another significant requirement. Specifically, the owner of RFID tags could be required to change several times during its lifetime. During the transfer, new owner first obtains necessary private information from the old owner, with these information he then takes over tag identification and authorization so as to have secure communication with tags. Security and privacy are major issue in the presence of malicious adversary. Therefore, the protocol used to identify tag should not only allow a legitimate reader to authenticate a tag but it should also protect the privacy of the tag against unauthorized tracing. Besides, after ownership transfer, the authentication protocol should also prevent the old owner to trace the tags and disallow the new owner to trace old transactions of the tags. On the other hand, while achieving privacy and security on tag and server side, the computation complexity is also very important.

In order to resolve these security and privacy problems, numerous authentication protocols have been proposed in the literature. Many of them are failed to provide security and privacy and the computation on the server side is also very high. Motivated by this need, in this paper, we first analyze an existing RFID authentication protocol and show that it does not resist against tag tracking attack. Then, we propose an RFID mutual authentication protocol which is also used to realize ownership transfer. In our protocol, the server needs only a constant-time complexity for identification when the tag and server are synchronized. In case of ownership transfer, our protocol preserves both old owner and new owner privacy. Our protocol also achieves backward untraceability against a strong adversary who compromise tag, and forward untraceability under the assumption that the adversary misses at least one subsequent successful session between the tag and the reader.

Category / Keywords: RFID, Privacy, Security, Ownership Transfer Protocol

Date: received 9 Dec 2011, last revised 18 Dec 2011

Contact author: skardas at gmail com