Cryptology ePrint Archive: Report 2013/187

Enhanced Ownership Transfer Protocol for RFID in an Extended Communication Model

Jorge Munilla, Alberto Peinado, Guoming Yang and Willy Susilo

Abstract: Ownership Transfer Protocols for RFID allow transferring the rights over a tag from a current owner to a new owner in a secure and private way. Recently, Kapoor and Piramuthu have proposed two schemes which overcome most of the security weaknesses detected in previously published protocols. Still, this paper reviews that work and points out that such schemes still present some practical and security issues. In particular, they do not manage to guarantee the privacy of the new owner without the presence of a Trusted Third Party, and we find that the assumed communication model is not suitable for many practical scenarios. We then propose here a lightweight protocol that can be used in a wider range of applications, and which incorporates recently defined security properties such as Tag Assurance, Undeniable Ownership Transfer, Current Ownership Proof and Owner Initiation. Finally, this protocol is complemented with a proposed Key Change Protocol, based on noisy tags, which provides privacy to the new owner without either resorting to a Trusted Third Party or assuming an Isolated Environment.

Category / Keywords: cryptographic protocols / RFID, Ownership Transfer Protocols, Privacy, Key Change Protocol

Date: received 2 Apr 2013

Contact author: munilla at ic uma es