Cryptology ePrint Archive: Report 2011/061

Cryptanalysis of Some Protocols for RFID Systems

Masoumeh Safkhani, Majid Naderi, Nasour Bagheri and Somitra Kumar Sanadhya

Abstract: In this paper we analyze the security of the mutual authentication and ownership transfer protocols which have been recently proposed by Kulseng \textit{et al.} Our analysis demonstrates a variety of attacks against these protocols. We present a secret parameters disclosure attack which discloses any secret parameter between the tag and the reader. Our disclosure attack can be easily used as an impersonation attack against the mutual authentication protocol. In addition, we present an attack that retrieves the PIN-value in the ownership transfer protocol, where the PIN-value is a parameter that must be kept secret from any party including the owner of the tag.

All the attacks presented in this work are passive, have low complexity and have the success probability of 1.

Category / Keywords: cryptographic protocols /

Publication Info: RFID, Lightweight Mutual Authentication, Ownership Transfer Protocol, PUF, LFSR.

Date: received 1 Feb 2011, last revised 9 Feb 2011

Contact author: nbagheri at srttu edu, na bagheri@gmail com

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20110209:083808 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]