Cryptology ePrint Archive: Report 2011/194

Cryptanalysis of Chen \textit{et al.}'s RFID Access Control Protocol

Masoumeh Safkhani, Nasour Bagheri and Majid Naderi

Abstract: Recently Chen \textit{et al.} have proposed a RFID access control protocol based on the strategy of indefinite-index and challenge-response. They have claimed that their protocol provides optimal location privacy and resists against man in the middle, spoofed tag and spoofed reader attacks. However, in this paper we show that Chen \textit{ et al.} protocol does not provide the claimed security. More precisely, we present the following attacks on the protocol:

\begin{enumerate} \item Tag impersonation attack. \item Reader impersonation attack. \item Location traceability attack. \end {enumerate} All attacks presented in this paper have the success probability of '1' on the cost of only one or two runs of protocol.

Category / Keywords: cryptographic protocols / RFID, Access Control, Spoofed Reader Attack, Authentication, Desynchronization Attack.

Date: received 15 Apr 2011, last revised 15 Apr 2011

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