Cryptology ePrint Archive: Report 2011/426

Cryptanalysis of improved Yeh \textit{et al. }'s authentication Protocol: An EPC Class-1 Generation-2 standard compliant protocol

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

Abstract: EPC class 1 Generation 2(or in short term EPC-C1 G2) is one of the most important standards for RFID passive tags. However, the original protocol known to be insecure. To improve the security of this standard, several protocols have been proposed compliant to this standard. In this paper we analyze the improved Yeh \textit{et al. }'s protocol by Yoon which is conforming to EPC-C1 G2 standard and is one of the most recent proposed protocol in this field. We present several efficient attacks against this protocol. Our first attack is a passive attack that can retrieve all secret parameters of the tag on the cost of eavesdropping only one session of protocol between the tag and a legitimate reader (connected to the back-end database) and $O(2^{16})$ evaluations of $PRNG$-function in off-line . Although the extracted information are enough to mount other relevant attacks (e. g. such as traceability, tag impersonation, reader impersonation, and desynchronization attacks) and would be enough to rule out any security claim for this protocol, to highlight other weaknesses of the protocol we present another tag impersonation attack with the complexity of two runs of protocol and the success probability of ``1''. In addition, we show a straight forward way to trace the tag as long as it has not updated its secret values.

Category / Keywords: cryptographic protocols / RFID, EPC-C1 G2, Mutual Authentication, Secret Disclosure, Tag/Reader Impersonation, Traceability

Date: received 8 Aug 2011

Contact author: na bagheri at gmail com

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

Version: 20110812:182831 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]