Cryptology ePrint Archive: Report 2011/651

CHECKER: On-site checking in RFID-based supply chains

Kaoutar Elkhiyaoui and Erik-Oliver Blass and Refik Molva

Abstract: Counterfeit detection in RFID-based supply chains aims at preventing adversaries from injecting fake products that do not meet quality standards. This paper introduces CHECKER, a new protocol for counterfeit detection in RFID-based supply chains through on-site checking. While RFID-equipped products travel through the supply chain, RFID readers can verify product genuineness by checking the validity of the product's path. CHECKER uses a polynomialbased encoding to represent paths in the supply chain. Each tag T in CHECKER stores an IND-CCA encryption of T's identifier ID and a signature of ID using the polynomial encoding of T's path as secret key. CHECKER is provably secure and privacy preserving. An adversary can neither inject fake products into the supply chain nor trace products. Moreover, RFID tags in CHECKER can be cheap read/write only tags that are not required to perform any computation. Storage requirements for a tag are low with only 120 Bytes.

Category / Keywords: RFID, counterfeit detection, privacy

Date: received 2 Dec 2011

Contact author: kaoutar elkhiyaoui at eurecom fr