Cryptology ePrint Archive: Report 2011/321

A Formal Approach to Distance-Bounding RFID Protocols

Ulrich Duerholz and Marc Fischlin and Michael Kasper and Cristina Onete

Abstract: Distance-Bounding identification protocols aim at impeding man-in-the-middle attacks by measuring response times. There are three kinds of attacks such protocols could address: (1) Mafia attacks where the adversary relays communication between honest prover and honest verifier in different sessions; (2) Terrorist attacks where the adversary gets limited active support from the prover to impersonate. (3) Distance attacks where a malicious prover claims to be closer to the verifier than it actually is. Many protocols in the literature address one or two such threats, but no rigorous cryptographic security models ---nor clean security proofs--- exist so far. For resource-constrained RFID tags, distance-bounding is more difficult to achieve. Our contribution here is to formally define security against the above-mentioned attacks and to relate the properties. We thus refute previous beliefs about relations between the notions, showing instead that they are independent. Finally we use our new framework to assess the security of the RFID distance-bounding scheme due to Kim and Avoine, and enhance it to include impersonation security and allow for errors due to noisy channel transmissions.

Category / Keywords: foundations / RFID distance-bounding protocols, formal models, provable security

Date: received 16 Jun 2011

Contact author: cristina onete at gmail com