Cryptology ePrint Archive: Report 2011/129

Distance Hijacking Attacks on Distance Bounding Protocols

Cas Cremers and Kasper Bonne Rasmussen and Srdjan Capkun

Abstract: Distance bounding protocols are typically analyzed with respect to three types of attacks: Distance Fraud, Mafia Fraud, and Terrorist Fraud. We define and analyze a fourth main type of attack on distance bounding protocols, called Distance Hijacking. We show that many proposed distance bounding protocols are vulnerable to this type of attack, and we propose solutions to make these protocols resilient to Distance Hijacking. We further show that verifying distance bounding protocols using existing informal and formal frameworks does not guarantee the absence of Distance Hijacking attacks.

Category / Keywords: applications / Distance bounding, location verification, position verification, attacks, hijacking, multi-prover environment

Date: received 14 Mar 2011, last revised 24 Aug 2011

Contact author: cas cremers at inf ethz ch

Available formats: PDF | BibTeX Citation

Version: 20110824:080005 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]