Cryptology ePrint Archive: Report 2011/492

Rational distance-bounding protocols over noisy channels

Long H. Nguyen

Abstract: We use ideas from game theory to define a new notion for an optimal threshold for the number of erroneous responses that occur during the rapid-bit exchange over noisy channels in a distance-bounding protocol. The optimal threshold will ensure that even if an intruder attempts to cause incorrect authentication, the expected loss the verifier suffers will still be lower than when the intruder does not attack. Any rational intruder, who always tries to maximise the verifier's loss, will not therefore have any incentive to attack the protocol. We then demonstrate how statistical analysis and binary search can be used to locate such a unique and optimal threshold accurately.

Category / Keywords: cryptographic protocols / distance-bounding protocols, RFID protocols, game theory

Publication Info: In Proceedings of the 4th International Conference on Security of Information and Networks -- SIN2011

Date: received 11 Sep 2011, last revised 7 Oct 2011

Contact author: Long Nguyen at cs ox ac uk

Available formats: PDF | BibTeX Citation

Note: As explained above, this is the extended version of a paper which has been accepted to appear in the 4th International Conference on Security of Information and Networks SIN in November 2011.

This version contains a number of formal proofs and some new materials that cannot be put into the published version due to page limit.

Version: 20111007:153523 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]