Cryptology ePrint Archive: Report 2011/618

Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones

Lishoy Francis and Gerhard Hancke and Keith Mayes and Konstantinos Markantonakis

Abstract: Contactless technology is widely used in security sensitive applications, including identification, payment and access-control systems. Near Field Communication (NFC) is a short-range contactless technology allowing mobile devices to act primarily as either a reader or a token. Relay attacks exploit the assumption that a contactless token within communication range is in close proximity, by placing a proxy-token in range of a contactless reader and relaying communication over a greater distance to a proxy-reader communicating with the authentic token. It has been theorised that NFC-enabled mobile phones could be used as a generic relay attack platform without any additional hardware, but this has not been successfully demonstrated in practice. We present a practical implementation of an NFC-enabled relay attack, requiring only suitable mobile software applications. This implementation reduces the complexity of relay attacks and therefore has potential security implications for current contactless systems. We also discuss countermeasures to mitigate the attack.

Category / Keywords: Implementation/relay, practical relay, RFID, Near Field Communication (NFC), mobile phone, contactless, smart card, ISO 14443, payments, identification, access control, transactions, proximity, practical implementation, security attack, countermeasure.

Publication Info: in submission

Date: received 17 Nov 2011, last revised 24 Feb 2012

Contact author: lishoy at gmail com

Available formats: PDF | BibTeX Citation

Note: An improved version.

Version: 20120224:103814 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]