

of strict timeouts in contactless transactions. Timeouts could also be based on a history of measured command-response delays from previous transactions to detect significant deviations in comparison to previous transactions. A third possibility would be the explicit activation of card emulation by user interaction (e.g. by pressing a button on the mobile phone that is directly connected to the SE.) However, this would significantly complicate over-the-air card management.

References

1. Clark, S.: RIM releases BlackBerry NFC APIs. Near Field Communications World (May 2011), <http://www.nfcworld.com/2011/05/31/37778/rim-releases-blackberry-nfc-apis/>
2. Desmedt, Y., Goutier, C., Bengio, S.: Special Uses and Abuses of the Fiat-Shamir Passport Protocol (extended abstract). In: Advances in Cryptology — CRYPTO '87, LNCS, vol. 293/2006, pp. 21–39. Springer Berlin Heidelberg (1988)
3. EMVCo: EMV Contactless Specifications for Payment Systems – Book A: Architecture and General Requirements, Version 2.1 (Mar 2011)
4. Francis, L., Hancke, G.P., Mayes, K.E., Markantonakis, K.: Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones. In: Radio Frequency Identification: Security and Privacy Issues, LNCS, vol. 6370/2010, pp. 35–49. Springer Berlin Heidelberg (2010)
5. Gostev, A.: Monthly Malware Statistics: August 2011 (Sep 2011), <http://www.securelist.com/analysis/204792190>
6. Hancke, G.P.: A Practical Relay Attack on ISO 14443 Proximity Cards (Jan 2005), <http://www.rfidblog.org.uk/hancke-rfidrelay.pdf>, (retrieved: 20 Sep 2011)
7. Hancke, G.P., Mayes, K.E., Markantonakis, K.: Confidence in smart token proximity: Relay attacks revisited. *Computers & Security* 28(7), 615–627 (2009)
8. Höbarth, S., Mayrhofer, R.: A framework for on-device privilege escalation exploit execution on Android. In: Proceedings of IWSSI/SPMU (Jun 2011)
9. Jeon, W., Kim, J., Lee, Y., Won, D.: A Practical Analysis of Smartphone Security. In: Human Interface and the Management of Information. Interacting with Information. LNCS, vol. 6771/2011, pp. 311–320. Springer Berlin Heidelberg (2011)
10. Kfir, Z., Wool, A.: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). pp. 47–58 (Sep 2005)
11. McLean, H.: Nokia: No mobile wallet support in current NFC phones. Near Field Communications World (Jul 2011), <http://www.nfcworld.com/2011/07/21/38715/nokia-no-mobile-wallet-support-in-current-nfc-phones/>
12. RIM: Blackberry API 7.0.0: Package net.rim.device.api.io.nfc.emulation (2011), <http://www.blackberry.com/developers/docs/7.0.0api/net/rim/device/api/io/nfc/emulation/package-summary.html>
13. Roland, M., Langer, J., Scharinger, J.: Practical Attack Scenarios on Secure Element-enabled Mobile Devices. In: Proceedings of the Fourth International Workshop on Near Field Communication (NFC 2012). p. 6. Helsinki, Finland (Mar 2012)
14. Smart Card Alliance: Transit and Contactless Open Payments: An Emerging Approach for Fare Collection (Nov 2011), http://www.smartcardalliance.org/resources/pdf/Open_Payments_WP_110811.pdf