exploit the unsigned fields. Such attacks can be countered if the length fields of the NDEF header are also signed. We proposed a solution that requires modification to the Signature RTD in which, amongst others, the *TNF, Type-Length, Payload-Length* and *ID-Length* fields are included. We presented a security analysis of the proposed scheme, and verified that it was no longer possible to exploit the NDEF header in attacks of the type discussed, thus successfully countering Record Composition and Decomposition Attacks in particular. Inclusion of the *TNF* field accounted for some remaining semantic issues. Because of their impracticality, we discarded alternative solutions involving updating the NDEF specification.

13. References

[1] NFC Forum, "NFC Data Exchange Format (NDEF): Technical Specification", *http://www.nfc-forum.org/specs/spec_list/*, July 2006.

[2] NFC Forum, "Signature Record Type Definition: Technical Specification", *http://www.nfc-forum.org/specs/spec_list/*, November 2010.

[3] Michael Roland and Josef Langer and Josef Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type", *Third International Workshop on Near Field Communication,* Hagenberg, Austria, February 22-23, 2011. IEEE Computer Society, 2011, pp. 65–70.

[4] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones", *The Forth International Conference on Availability, Reliability and Security,* Fukuoka, Japan, March 16-19, 2009. IEEE Computer Society, 2009, pp. 695–700.

[5] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy", *Third International Conference on Availability, Reliability and Security,* Technical University of Catalonia, Barcelona, Spain, March 4-7, 2008. IEEE Computer Society, 2008, pp. 642–647.

[6] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "On the security issues of NFC enabled mobile phones", *International Journal of Internet Technology and Secured Transactions,* vol. 2*, Number 3-4*, *2010.* Inderscience Enterprises Ltd, 2010, pp. 336–356.

[7] NFC Forum, "NFC Forum Home Page", *http://www.nfcforum.org/home/*, 2004.

[8] NFC Forum, "Smart Poster Record Type Definition: Technical Specification", *http://www.nfc-forum.org/specs/spec_list/*, July 2006.

[9] E. Haselsteiner and K. Breitfuß, "Security in Near Field communication (NFC): Strengths and Weaknesses", *Workshop on RFID Security (RFIDSec)*, Graz, Austria, July 12-14, 2006.

[10] M. Roland and J. Langer, "Digital Signature Records for the NFC Data Exchange Format", *Second International Workshop on Near Field Communication,* Monaco, April 20-22, 2010. IEEE Computer Society, 2010, pp. 71–76.

[11] R. Verdult and F. Kooman, "Practical attacks on NFC enabled cell phones", *Third International Workshop on Near Field Communication,* Hagenberg, Austria, February 22-23, 2011. IEEE Computer Society, 2011, pp. 77–82.

[12] M. Q. Saeed and C. D. Walter, " A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition, *6th International Conference on Internet Technology and Secured Transactions,* Abu Dhabi, UAE, December 11-14, 2011. IEEE Computer Society, 2011, pp 284-287.

Copyright © 2013, Infonomics Society