NFC Malicious Content Sharing

Roel Verdult[1] and François Kooman[2]

[1] Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands.
rverdult@cs.ru.nl

[2] SURFnet B.V., The Netherlands.
Francois.Kooman@surfnet.nl

1 Talk at BruCON Security Conference 2010

The security features of Near Field Communication (NFC) compatible mobile phones needs to be seriously revised. NFC mobile phones can communicate with other NFC mobile phones, NFC readers, or RFID tags in so-called smart posters, for instance to exchange of small files with photos or contact details. To exchange files, two devices should be within the proximity coupling distance of 5 cm, besides this phisical constraint there is no user interaction required. We show that feature interaction between NFC and bluetooth, where an NFC connection starts a bluetooth connection without any request for permission, can be abused to surreptiously install software on an NFC phone [1]. This results in a serious vulnerability, when, for instance smart posters start acting smarter and install malicious applications instead of providing some harmless information. We verified this vulnerability on the recently released Nokia 6212 Clasic phones.

2 About the author

Roel Verdult is scientific researcher at the Radboud University Nijmegen. He played an important role in the research that uncovered the serious security vulnerabilities in the widely deployed MIFARE Classic RFID tag [2–4]. This is a contactless smartcard that is sold more than a billion times and used in several public transport systems around the world [5,6]. The impact is even more catastropic for MIFARE Classic access control systems of highly secured facilities like ministries, military bases, banks, nuclear power plants and prisons. Furtermore, he demonstrated how to recover the secret cryptographic keys of vehicle immobilizers which are used by most car makes [7].

Roel is currently a member of the Digital Security group at the Radboud University Nijmegen. His research covers a variety of security topics which include (but are not limited to) the electronic passports, contactless smartcards, Radio Frequency Identification (RFID) [8], Near Field Communication (NFC) [9], secure storage [10,11], access control systems [12,13], authentication protocols and other types of transmission security. His research work and publications are honored with several national and international awards.

3 About the conference

BruCON is an annual security and hacker conference providing two days of an interesting atmosphere for open discussions of critical infosec issues, privacy, information technology and its cultural/technical implications on society. Organized in Brussels, BruCON offers a high quality line up of speakers, security challenges and interesting workshops. BruCON is a conference by and for the security and hacker community.

References

1. Roel Verdult and François Kooman. Practical attacks on NFC enabled cell phones. In *3rd International Workshop on Near Field Communication (NFC 2011)*, pages 77–82. IEEE Computer Society, 2011.
2. Ronny Wichers Schreur, Peter van Rossum, Flavio D. Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. Security flaw in MIFARE Classic. *Press release, Digital Security group, Radboud University Nijmegen, The Netherlands*, March 2008.
3. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling MIFARE Classic. In *13th European Symposium on Research in Computer Security (ESORICS 2008)*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114. Springer-Verlag, 2008.
4. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a MIFARE Classic card. In *30th IEEE Symposium on Security and Privacy (S&P 2009)*, pages 3–15. IEEE Computer Society, 2009.
5. Roel Verdult. Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen, 2008.
6. Roel Verdult. Security analysis of RFID tags. Master's thesis, Radboud University Nijmegen, 2008.
7. Roel Verdult, Flavio D. Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with Hitag2. In *21st USENIX Security Symposium (USENIX Security 2012)*, pages 237–252. USENIX Association, 2012.
8. Roel Verdult, Gerhard de Koning Gans, and Flavio D. Garcia. A toolbox for RFID protocol analysis. In *4th International EURASIP Workshop on RFID Technology (EURASIP RFID 2012)*. IEEE Computer Society, 2012.
9. Gergely Alpár, Lejla Batina, and Roel Verdult. Using NFC phones for proving credentials. In *16th Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance (MMB&DFT 2012)*, volume 7201 of *Lecture Notes in Computer Science*, pages 317–330. Springer-Verlag, 2012.
10. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling SecureMemory, CryptoMemory and CryptoRF. In *17th ACM Conference on Computer and Communications Security (CCS 2010)*, pages 250–259. ACM, 2010.
11. Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede. Power analysis of Atmel CryptoMemory - recovering keys from secure EEPROMs. In *12th Cryptographers' Track at the RSA Conference (CT-RSA 2012)*, volume 7178 of *Lecture Notes in Computer Science*, pages 19–34. Springer-Verlag, 2012.
12. Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Exposing iClass key diversification. In *5th USENIX Workshop on Offensive Technologies (WOOT 2011)*, pages 128–136. USENIX Association, 2011.
13. Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac. Dismantling iClass and iClass Elite. In *17th European Symposium on Research in Computer Security (ESORICS 2012)*, Lecture Notes in Computer Science. Springer-Verlag, 2012.