Security Taken for Granted

Roel Verdult

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

1 Talk at 6th Bits&Chips Hardware Conference

In its everyday life an average person is surrounded by RFID devices. For example when using the access control at your office building, when travelling with a public transport card, when authenticating to a vehicle immobiliser that is embedded in your car key, when paying for lunch with your mobile phone and when reading out your pacemaker at the doctor. We often use such devices without giving its security much attention, let alone the actual strength of the provided security. It just works great and often feels even a bit magical, opening a door from a distance using (batteryless) wireless devices. This concept tends to give a false feeling of confidence about its security. It looks very complicated, so it is probably pretty hard to abuse.

The opposite seems to be true when we inspect the products around us. This talk shows several examples where it went wrong and we, the general public, ended up with weak security using easy to break ciphers and protocols [1–15] with off-the-shelf hardware. We end up with such weak security when we let the industry sell us all kinds of incompetent products. It is no wonder that people start to feel like "everything is hackable". The problem is not the availability of decent ciphers and protocols [16–21], but the choices we let the industry make for us.

2 About the conference

Over the past five years the Bits&Chips Hardware Conference has grown into a high-quality, mature and influential event. The Bits&Chips Hardware Conference traditionally attracts the best and the brightest from the Benelux high-tech electronics sector. Since 2012 it has opened up internationally, attracting many of the top developers, decision makers, professionals, technical managers and buyers in the high-end electronics, advanced systems and IC development industry.

The Bits&Chips Hardware Conference gives visitors a comprehensive and multidisciplinary view at the world of electronics. A focused industry trade fair programme and a high-quality peer-reviewed lecture programme are integral to the Bits&Chips Hardware Conference. The event is a must for every engineer or decision maker in the industry.

Bits&Chips Hardware Conference is an open invitation for suppliers to partner in the high tech Benelux/International market. The Dutch market alone has a healthy growth and is expected to double by 2020. There is business to be done at the Bits&Chips Hardware Conferenceand expertise to be shared.

References

1. 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.
2. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the MIFARE Classic. In *8th Smart Card Research and Advanced Applications Conference (CARDIS 2008)*, volume 5189 of *Lecture Notes in Computer Science*, pages 267–282. Springer-Verlag, 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. 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.
6. 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.
7. 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.
8. 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)*, volume 7459 of *Lecture Notes in Computer Science*, pages 697–715. Springer-Verlag, 2012.
9. Roel Verdult. Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen, 2008.
10. Roel Verdult. Security analysis of RFID tags. Master's thesis, Radboud University Nijmegen, 2008.
11. Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OV-chipkaart project. Master's thesis, Radboud University Nijmegen, 2008.
12. 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.
13. Roel Verdult, Flavio D. Garcia, and Barış Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *22nd USENIX Security Symposium (USENIX Security 2013)*. USENIX Association, 2013.
14. 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.
15. Arjan Blom, Gerhard de Koning Gans, Erik Poll, Joeri de Ruiter, and Roel Verdult. Designed to fail: A USB-connected reader for online banking. In *17th Nordic Conference on Secure IT Systems (NordSec 2012)*, volume 7617 of *Lecture Notes in Computer Science*, pages 1–16. Springer-Verlag, 2012.
16. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.
17. David Galindo and Flavio D. Garcia. A Schnorr-like lightweight identity-based signature scheme. In *2nd International Conference on Cryptology in Africa, Progress in Cryptology (AFRICACRYPT 2009)*, volume 5580 of *Lecture Notes in Computer Science*, pages 135–148. Springer-Verlag, 2009.
18. Flavio D. Garcia and Peter van Rossum. Modeling privacy for off-line RFID systems. In *9th Smart Card Research and Advanced Applications (CARDIS 2010)*, volume 6035 of *Lecture Notes in Computer Science*, pages 194–208. Springer-Verlag, 2010.
19. Gerhard de Koning Gans and Flavio D. Garcia. Towards a practical solution to the RFID desynchronization problem. In *6th Workshop on RFID Security (RFIDSec 2010)*, volume 6370 of *Lecture Notes in Computer Science*, pages 203–219. Springer-Verlag, 2010.
20. 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.
21. Willem Burgers, Roel Verdult, and Marko van Eekelen. Prevent session hijacking by binding the session to the cryptographic network credentials. In *18th Nordic Conference on Secure IT Systems (NordSec 2013)*, volume 8208 of *Lecture Notes in Computer Science*, pages 33–50. Springer-Verlag, 2013.