Classic Mistakes

Roel Verdult

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

1 Talk at Hacking at Random 2009

The MIFARE Classic tag is a contactless smart card that is used extensively in access control for office buildings, payment systems for public transport and other security related applications. The security mechanisms of this chip were reversed engineered in 2008 by independent researchers [1–3]. Using the knowledge of the CRYPTO1 cipher, multiple cryptographic attacks were proposed [4–9]. The Chaos Computer Club, University of Virginia and the Radboud University Nijmegen released several scientific papers and seminars covering this topic. The attacks all differ in speed, requirements, costs and impact.

This lecture gives a broad overview of the vulnerabilities that exists in MIFARE Classic products and the way they are used by system integrators. During this presentation the publicly available documentation, hardware and source-code is combined into an impressive overview of security vulnerabilities. Furthermore, a real life demonstration will recover the keys from a genuine MIFARE Classic tag within seconds using just an inexpensive stock commercial NFC reader (30 USD). This lecture summarizes the classic mistakes that were made in 1994, the year that MIFARE was born.

2 About the conference

From the ancient days long before the first wayback-machine snapshot, hackers have a track record for appropriating technology that was meant for something completely different and putting it to alternative uses. And every four years since 1989, the international hacker community has descended upon The Netherlands in great numbers for a conference that focuses on contemporary and future issues surrounding technology and its social and political consequences. One reason that these conferences have been successful is the wide range of participants: from students, amateurs and aficionados to researchers, scientists and entrepreneurs who are recognized as some of the best in their respective fields.

The atmosphere is open, friendly and relaxed, the scope of subjects insanely wide, the average level of knowledge high. The venue is always buzzing with energy, ideas and projects. The New York Times described the 1997 edition as ‘Woodstock for Hackers’. We will gladly honor that legacy. This year we celebrate the 20th anniversary of this event with a new installment: ’Hacking at Random’. HAR wants to offer presentations that feature the joy of hacking. That means hardcore hacking and science for its own sake. HAR is soliciting abstracts from anybody who is interested in giving a talk, in doing a workshop or in otherwise presenting their work.

When this series of conferences started twenty years ago, the net was new and unexplored terrain where only the bold dared to tread, and where legislation and regulation were absent. That has changed. Today, virtually every household in the Western world has access and many analogue services are being relocated to the internet, reinventing themselves while doing so, and thereby simultaneously making internet even more of a commodity and an

indispensable part of our daily lives. Internet has become ubiquitous, all pervasive, huge and crowded. Because of this, new questions are becoming increasingly important: questions about governance, sustainability, dying analogue media, ownership of data and content, shortage of IP space and energy, censorship, filtering, data trails, data breaches, security, surveillance to mention but a few.

As the world is more and more defined in terms of the technology of the internet, the once obscure political freedom-fights that hackers were involved in, have truly reached center stage. The next few years are about defending fundamental freedoms, and we better step to it, because nobody is going to do it for us.

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. Karsten Nohl, David Evans, Starbug, and Henryk Plötz. Reverse engineering a cryptographic RFID tag. In *17th USENIX Security Symposium (USENIX Security 2008)*, pages 185–193. USENIX Association, 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. 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.
5. 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.
6. Nicolas T. Courtois. The dark side of security by obscurity - and cloning MIFARE Classic rail and building passes, anywhere, anytime. In *4th International Conference on Security and Cryptography (SECRYPT 2009)*, pages 331–338. INSTICC Press, 2009.
7. Roel Verdult. Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen, 2008.
8. Roel Verdult. Security analysis of RFID tags. Master's thesis, Radboud University Nijmegen, 2008.
9. Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OV-chipkaart project. Master's thesis, Radboud University Nijmegen, 2008.