Poster: Dismantling iClass and iClass Elite

Flavio D. Garcia   Gerhard de Koning Gans   Roel Verdult
Radboud University Nijmegen, The Netherlands
{flaviog,gkoningg,rverdult}@cs.ru.nl

Milosch Meriac
Bitmanufaktur GmbH
milosch.meriac@bitmanufaktur.de

I. Introduction

With more than 300 million cards sold, HID iClass is one of the most popular contactless smart cards on the market. It is widely used for access control, secure login and payment systems. The card uses 64-bit keys to provide authenticity and integrity. The cipher and key diversification algorithms are proprietary and little information about them is publicly available. iClass is an ISO/IEC 15693 compatible contactless smart card manufactured by HID Global. It was introduced in the market back in 2002 as a secure replacement of the HID Prox card which did not have any cryptographic capabilities. According to the manufacturer, more than 300 million iClass cards have been sold. These cards are widely used in access control of secured buildings such as The Bank of America Merrill Lynch, the International Airport of Mexico City and the United States Navy base of Pearl Harbor among many others. Other applications include secure user authentication such as in the naviGO system included in Dell's Latitude and Precision laptops; e-payment like in the FreedomPay and SmartCentric systems; and billing of electric vehicle charging such as in the Liberty PlugIns system. iClass has also been incorporated into the new BlackBerry phones which support Near Field Communication (NFC).

iClass uses a proprietary cipher to provide data integrity and mutual authentication between card and reader. The cipher uses a 64-bit diversified key which is derived from a 56-bit master key and the serial number of the card. This key diversification algorithm is built into all iClass readers. The technology used in the card is covered by US Patent 6058481 and EP 0890157. The precise description of both the cipher and the key diversification algorithms are kept secret by the manufacturer following the principles of security by obscurity. Remarkably, all iClass Standard cards worldwide share the same master key for the iClass application. This master key is stored in the EEPROM memory of every iClass reader. It is possible though to let HID generate and manage a custom key for your system if you are willing to pay a higher price. The iClass Elite Program (a.k.a., High Security) uses an additional key diversification algorithm and a custom master key per system which according to HID provides "the highest level of security".

Over the last few years, much attention has been paid to the (in)security of the cryptographic mechanisms used in contactless smart cards [8], [13], [17], [22]. Experience has shown that the secrecy of proprietary ciphers does not contribute to its cryptographic strength. Most notably the MIFARE Classic, which has widespread application in public transport ticketing and access control systems, has been thoroughly broken in the last few years [3], [6], [12], [16], [23]. Other prominent examples include Hitag2 [4], [18], [22] used in car keys and CryptoRF [1], [2], [13] used in access control and payment systems. HID proposes iClass as a migration option for systems using Mifare Classic, boosting that iClass provides "improved security, performance and data integrity". For almost one decade after its introduction to the market, the details of the security mechanisms of iClass remained unknown.

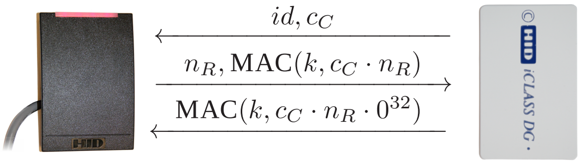
id, c_C
$n_R, \mathrm{MAC}(k, c_C \cdot n_R)$
$\mathrm{MAC}(k, c_C \cdot n_R \cdot 0^{32})$
HID
HID iCLASS DG

Fig. I.1: Authentication protocol between an iClass card and reader.

Our contribution In this paper [11] we have fully reverse engineered iClass's proprietary cipher and authentication protocol which we publish in full detail. This task is not trivial since it was first necessary to bypass the read protection mechanisms of the microcontroller used in the readers in order to retrieve its firmware.

Furthermore we have found serious vulnerabilities in the cipher that enable an attacker to recover the secret key from the card by just wirelessly communicating with it. The potential impact of this attack is vast since other vulnerabilities in the key diversification algorithm allow an adversary to use this secret key to recover the master key, provided that he has mild computational power. Additionally, we have reverse engineered the iClass Elite key diversification algorithm which we describe in full detail. We show that this algorithm has even more serious vulnerabilities than the standard key diversification algorithm, allowing an attacker to directly recover the *master key* by simply communicating with a legitimate iClass reader. Concretely, we propose two attacks: one against iClass Standard and one against iClass Elite. Both attacks allow an adversary to recover the master key.

- The first attack exploits a total of *four* weaknesses in the cipher, key diversification algorithm and implementation. In order to execute this attack the adversary first needs to eavesdrop one legitimate authentication session between card and reader. Then it runs 2^{19} key updates and 2^{22} authentication attempts with the card. This takes less than six hours to accomplish when using a Proxmark III as a reader and recovers 24 bits of the card key. Finally, off-line, the attacker needs to search for the remaining 40 bits of the key. Having recovered the card key, the adversary gains full control over the card. Furthermore, computing the master key from the card key is as hard as breaking single DES [9].

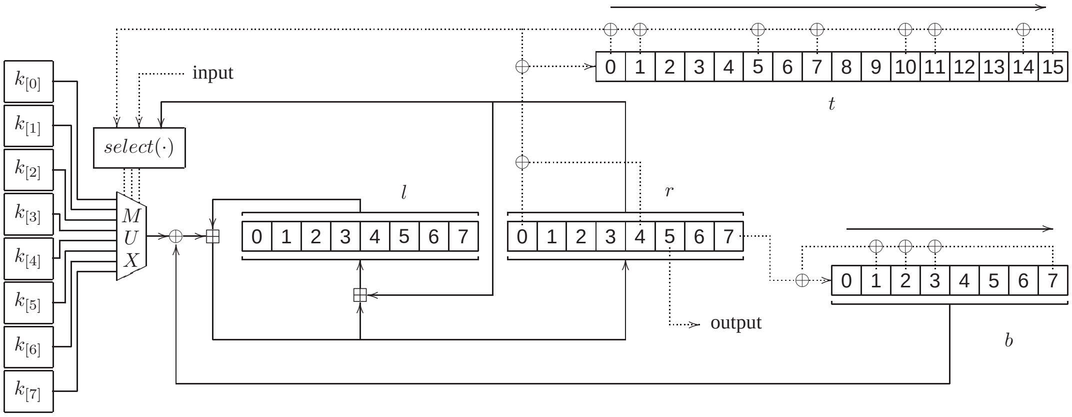

Fig. I.2: The iClass cipher. Solid lines represent byte operations while dotted lines represent bit operations.

- The second attack concerning iClass Elite exploits *two* weaknesses in the key diversification algorithm and recovers the master key directly. In order to run this attack the adversary only needs to run 15 authentication attempts with a legitimate reader. Afterwards, off-line, the adversary needs to compute only 2^{25} DES encryptions in order to recover the master key. This attack, from beginning to end runs within 5 seconds on ordinary hardware.

We have executed both attacks in practice and verified these claims and attack times. The attack on iClass Elite requires tag-emulation of several chosen card serial numbers. Fooling a genuine reader with a portable tag-emulating device has been demonstrated many times in the literature [5], [7], [14], [15], [19], [20]. For eavesdropping and card emulation we used the Proxmark III [10], [21]. This is an FPGA-based RFID research tool that costs approximately 200 USD.

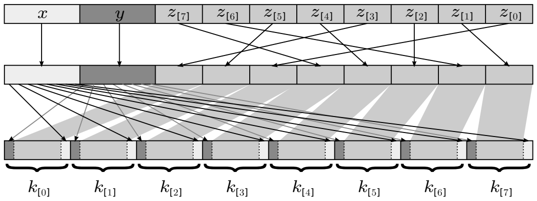

Fig. I.3: Schematic representation of the function *hash0*, used in iClass and iClass Elite key diversification.

References

[1] 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.

[2] Alex Biryukov, Ilya Kizhvatov, and Bin Zhang. Cryptanalysis of the Atmel cipher in SecureMemory, CryptoMemory and CryptoRF. In *9th Applied Cryptography and Network Security (ACNS 2011)*, volume 6715 of *Lecture Notes in Computer Science*, pages 91–109. Springer-Verlag, 2011.

[3] 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.

[4] Nicolas T. Courtois, Sean O'Neil, and Jean-Jacques Quisquater. Practical algebraic attacks on the Hitag2 stream cipher. In *12th Information Security Conference (ISC 2009)*, volume 5735 of *Lecture Notes in Computer Science*, pages 167–176. Springer-Verlag, 2009.

[5] Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OV-chipkaart project. Master's thesis, Radboud University Nijmegen, 2008.

[6] 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.

[7] Martin Feldhofer, Manfred Josef Aigner, Michael Hutter, Thomas Plos, Erich Wenger, and Thomas Baier. Semi-passive RFID development platform for implementing and attacking security tags. In *2nd International Workshop on RFID/USN Security and Cryptography (RISC 2010)*, pages 1–6. IEEE Computer Society, 2010.

[8] 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.

[9] Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Exposing iClass key diversification. In *5th USENIX Workshop on Offensive Technologies (USENIX WOOT 2011)*, pages 128–136. USENIX Association, 2011.

[10] Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Tutorial: Proxmark, the swiss army knife for RFID security research. Technical report, Radboud University Nijmegen, 2012.

[11] 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.

[12] 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.

[13] 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/SIGSAC, 2010.

[14] Timo Kasper, Michael Silbermann, and Christof Paar. All you can eat or breaking a real-world contactless payment system. In *14th International Conference on Financial Cryptography and Data Security (FC 2010)*, volume 6052 of *Lecture Notes in Computer Science*, pages 343–350. Springer-Verlag, 2010.

[15] M. Ayoub Khan, Manoj Sharma, and Prabhu R. Brahmanandha. FSM based manchester encoder for UHF RFID tag emulator. In *17th International Conference on Computing, Communication and Networking (ICCCn 2008)*, pages 1–6. IEEE Computer Society, 2008.

[16] 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.

[17] Henryk Plötz and Karsten Nohl. Peeling away layers of an RFID security system. In *16th International Conference on Financial Cryptography and Data Security (FC 2012)*, volume 7035 of *Lecture Notes in Computer Science*, pages 205–219. Springer-Verlag, 2012.

[18] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT solvers to cryptographic problems. In *12th International Conference on Theory and Applications of Satisfiability Testing (SAT 2009)*, volume 5584 of *Lecture Notes in Computer Science*, pages 244–257. Springer-Verlag, 2009.

[19] Roel Verdult. Proof of concept, cloning the OV-chip card. Technical report, Radboud University Nijmegen, 2008.

[20] Roel Verdult. Security analysis of RFID tags. Master's thesis, Radboud University Nijmegen, 2008.

[21] 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.

[22] Roel Verdult, Flavio D. Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with Hitag2. In *21st USENIX Security Symposium (USENIX Security 2012)*. USENIX Association, 2012.

[23] 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.