Poster: Gone in 360 seconds: Hijacking with Hitag2

Roel Verdult Flavio D. Garcia
Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands.
{rverdult,flaviog}@cs.ru.nl

Josep Balasch
KU Leuven ESAT/COSIC and IBBT
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
josep.balasch@esat.kuleuven.be

I. Introduction

An electronic vehicle immobilizer is an anti-theft device which prevents the engine of the vehicle from starting unless the corresponding transponder is present. Such a transponder is a passive RFID tag which is embedded in the car key and wirelessly authenticates to the vehicle. It prevents a perpetrator from hot-wiring the vehicle or starting the car by forcing the mechanical lock. Having such an immobilizer is required by law in several countries. Hitag2, introduced in 1996, is currently the most widely used transponder in the car immobilizer industry. It is used by at least 34 car makes and fitted in more than 200 different car models. Hitag2 uses a proprietary stream cipher with 48-bit keys for authentication and confidentiality. This article reveals several weaknesses in the design of the cipher and presents three practical attacks that recover the secret key using only wireless communication. The most serious attack recovers the secret key from a car in less than six minutes using ordinary hardware. This attack allows an adversary to bypass the cryptographic authentication, leaving only the mechanical key as safeguard. This is even more sensitive on vehicles where the physical key has been replaced by a keyless entry system based on Hitag2. During our experiments we managed to recover the secret key and start the engine of many vehicles from various makes using our transponder emulating device. These experiments also revealed several implementation weaknesses in the immobilizer units.

Fig. 1: Car keys with a Hitag2 transponder/chip

In the past, most cars relied only on mechanical keys to prevent a hijacker from stealing the vehicle. Since the '90s most car manufacturers incorporated an electronic car immobilizer as an extra security mechanism in their vehicles. From 1995 it is mandatory that all cars sold in the EU are fitted with such an immobilizer device, according to European directive 95/56/EC. Similar regulations apply to other countries like Australia, New Zealand (AS/NZS 4601:1999) and Canada (CAN/ULC S338-98). An electronic car immobilizer consists of two main components: a small transponder chip which is embedded in (the plastic part of) the car key, see Figure 1; and a reader which is located somewhere in the dashboard of the vehicle and has an antenna coil around the ignition, see Figure 2.

The transponder is a passive RFID tag that operates at a low frequency (LF) wave of 125 kHz. It is powered up when it comes in proximity range of the electronic field of the reader. When the transponder is absent, the immobilizer unit prevents the vehicle from starting the engine.

A distinction needs to be made with remotely operated central locking system, which opens the doors, is battery powered, operates at a ultra-high frequency (UHF) of 433 MHz, and only activates when the user pushes a button on the remote key. More recent car keys are often deployed with a hybrid chip that supports the battery powered ultra-high frequency as well as the passive low frequency communication interface.

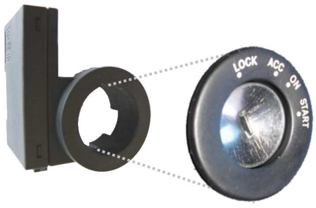

Fig. 2: Immobilizer unit around the ignition barrel

With the Hitag2 family of transponders, its manufacturer NXP Semiconductors (formerly Philips Semiconductors) leads the immobilizer market [1]. Even though NXP boosts "Unbreakable security levels using mutual authentication, challenge-response and encrypted data communication", it uses a shared key of only 48 bits.

Since 1988, the automotive industry has moved towards the so-called keyless ignition or keyless entry in their high-end vehicles [2]. In such a vehicle the mechanical key is no longer present. The only anti-theft mechanism left in these vehicles is the immobilizer. Startlingly, many keyless ignition or entry vehicles sold nowadays are still based on the Hitag2 cipher.

Background The history of the NXP Hitag2 family of transponders overlaps with that of other security products designed and deployed in the late nineties, such as Keeloq [3]–[6], MIFARE Classic [7]–[12], CryptoMemory [13]–[15] or iClass [16], [17]. Originally, information on Hitag2 transponders was limited to data sheets with high level descriptions of the chip's functionality [18], while details on the proprietary cryptographic algorithms were kept secret by the manufacturer. This phase, in which security was strongly based on obscurity, lasted until in 2007 when the Hitag2 inner workings were reverse engineered [19]. Similarly to its predecessor Crypto1 (used in MIFARE Classic), the Hitag2 cipher consists of a 48 bit Linear Feedback Shift Register (LFSR) and a non-linear filter function used to output keystream. The publication of the Hitag2 cipher attracted the interest of the scientific community.

Our contribution In our paper [20], we show a number of vulnerabilities in the Hitag2 transponders that enable an adversary to retrieve the secret key. We propose three attacks that extract the secret key under different scenarios. We have implemented and successfully executed these attacks in practice on more than 20 vehicles of various make and model. On all these vehicles we were able to use an emulating device to bypass the immobilizer

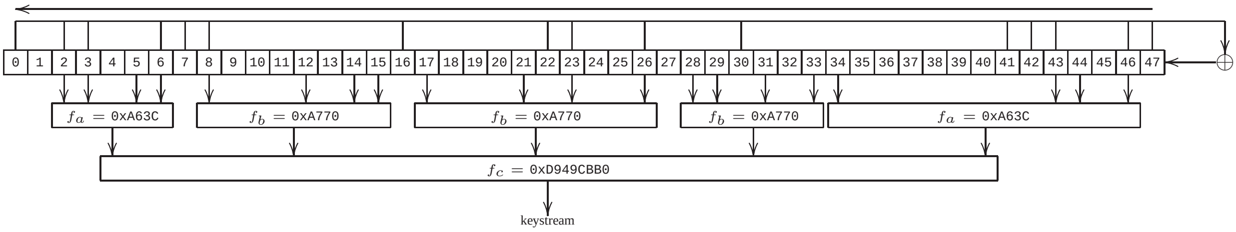

Fig. 3: Structure of the Hitag2 stream cipher, based on [19]

and start the vehicle. Fooling a car with a portable tag-emulating device has been demonstrated many times in the literature [21]–[25]. For eavesdropping and card emulation we used the Proxmark III [26], [27]. This is an FPGA-based RFID research tool that costs approximately 200 USD.

Fig. 4: Successful authentication using a Proxmark III

We have executed all our attacks in practice within the claimed attack times. We have experimented with more than 20 vehicles of various makes and models and found also several implementation weaknesses. In line with the principle of responsible disclosure, we have notified the manufacturer NXP six months before disclosure. We have constructively collaborated with NXP, discussing mitigating measures and giving them feedback to help improve the security of their products.

References

[1] Karsten Nohl. Immobilizer security. In *8th International Conference on Embedded Security in Cars (ESCAR 2010)*, 2010.

[2] Motoki Hirano, Mikio Takeuchi, Takahisa Tomoda, and Kin-Ichiro Nakano. Keyless entry system with radio card transponder. *IEEE Transactions on Industrial Electronics*, 35:208–216, 1988.

[3] Andrey Bogdanov. Linear slide attacks on the KeeLoq block cipher. In *Information Security and Cryptology (INSCRYPT 2007)*, volume 4990 of *Lecture Notes in Computer Science*, pages 66–80. Springer, 2007.

[4] Sebastiaan Indesteege, Nathan Keller, Orr Dunkelmann, Eli Biham, and Bart Preneel. A practical attack on KeeLoq. In *27th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 2008)*, volume 4965 of *Lecture Notes in Computer Science*, pages 1–8. Springer-Verlag, 2008.

[5] Nicolas T. Courtois, Gregory V. Bard, and David Wagner. Algebraic and slide attacks on KeeLoq. In *15th International Workshop on Fast Software Encryption (FSE 2000)*, volume 5086 of *Lecture Notes in Computer Science*, pages 97–115. Springer-Verlag, 2008.

[6] Markus Kasper, Timo Kasper, Amir Moradi, and Christof Paar. Breaking KeeLoq in a flash: on extracting keys at lightning speed. In *2nd International Conference on Cryptology in Africa, Progress in Cryptology (AFRICACRYPT 2009)*, volume 5580 of *Lecture Notes in Computer Science*, pages 403–420. Springer-Verlag, 2009.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[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] 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.

[15] 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.

[16] 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.

[17] 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.

[18] Transponder IC, Hitag2. Product Data Sheet, Nov 2010. NXP Semiconductors.

[19] I.C. Wiener. Philips/NXP Hitag2 PCF7936/46/47/52 stream cipher reference implementation. http://cryptolib.com/ciphers/hitag2/, 2007.

[20] 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.

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

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

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

[24] 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.

[25] 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.

[26] 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.

[27] 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.