Wireless Attacks on Automotive Remote Keyless Entry Systems

Oswald, David

DOI:
10.1145/2995289.2995297

Wireless Attacks on Automotive Remote Keyless Entry Systems

[Invited Keynote Talk Abstract]

David Oswald
School of Computer Science
The University of Birmingham
Birmingham, UK
d.f.oswald@bham.ac.uk

Keywords

remote keyless entry; automotive security; wireless attacks; embedded systems

1. ABSTRACT

Modern vehicles rely on a variety of electronic systems and components. One of those components is the vehicle key. Today, a key typically implements at least three functions: mechanical locking with a key blade, the electronic immobilizer to autorise the start of the engine, and the remote keyless entry (RKE) system that allows to wirelessly (un)lock the doors and disable the alarm system. These main components of a vehicle key are shown in Figure 1.

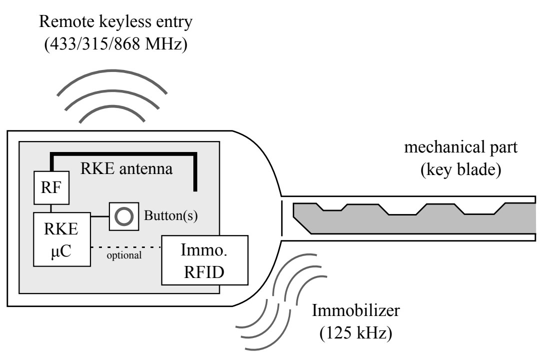

Figure 1: Main components of a vehicle key: mechanics, immobilizer, RKE

For the mechanical part of the vehicle key, it is well known that the key blade can be easily copied and that the locking cylinder can be bypassed with other means (using so-called "decoders" or simply a screwdriver). In contrast, immobilizer and RKE rely on wireless protocols to cryptographically authenticate the vehicle key to the car. Immobilizers employ radio frequency identification (RFID) transponders to carry out a challenge-response protocol over a low-range bidirectional link at a frequency of 125 kHz. In the past, researchers have revealed severe flaws in the cryptography and protocols used by immobilizers, leading to the break of the major systems Megamos, Hitag2, and DST40 [7, 6, 1].

In contrast to the immobilizer, the RKE part uses unidirectional communication (the vehicle only receives, the key fob only transmits) over a high-range wireless link with operating distances of tens to one hundred meters. These systems are based on rolling codes, which essentially transmit a counter (that is incremented on each button press) in a cryptographically authenticated manner.

Until recently, the security of automotive RKE had been scrutinized to a lesser degree than that of immobilizers, even though vulnerabilities in similar systems have been known since 2008 with the attacks on KeeLoq [3]. Other results reported in the literature include an analytical attack on a single, outdated vehicle [2] and the so-called "RollJam" technique [5], which is based on a combination of replay and selective jamming.

In 2016, it was shown that severe flaws exist in the RKE systems of major automotive manufacturers [4]. On the one hand, the VW group (Volkswagen, Seat, Škoda, Audi) based the security of their RKE system on a few global cryptographic keys, potentially affecting hundreds of million vehicles world-wide. By extracting these global keys from the firmware of electronic controls units (ECUs) once, an adversary is able to create a duplicate of the owner's RKE fob by eavesdropping a single rolling code.

The second case study in [4] exposes new cryptographic weaknesses in the Hitag2 cipher when used for RKE. Applying a correlation-based attack, an adversary can recover the 48-bit cryptographic key by eavesdropping four to eight rolling codes and performing a one-minute computation on a standard laptop. Again, this attack affects millions of vehicle world-wide. Manufacturers that used Hitag2 in their RKE system include Alfa Romeo, Peugeot, Lancia, Opel, Renault, and Ford among others.

In this keynote talk, we will present the results of [4] and put them in into a broader context by revisiting the history of attacks on RKE systems and automotive electronics.

TrustED'16 October 28 2016, Vienna, Austria

ACM ISBN 978-1-4503-4567-5/16/10.
DOI: http://dx.doi.org/10.1145/2995289.2995297

2. REFERENCES

[1] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo. Security analysis of a

cryptographically-enabled RFID device. In *14th USENIX Security Symposium (USENIX Security 2005)*, pages 1–16. USENIX Association, 2005.

[2] S. Cesare. Breaking the security of physical devices. Presentation at Blackhat'14, August 2014.

[3] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology – CRYPTO'08*, volume 5157 of *LNCS*, pages 203–220. Springer, 2008.

[4] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès. Lock it and still lose it – on the (in)security of automotive remote keyless entry systems. In *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, 2016. USENIX Association.

[5] S. Kamkar. Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars. Presentation at DEFCON 23, August 2015.

[6] R. Verdult, F. D. Garcia, and J. Balasch. Gone in 360 seconds: Hijacking with Hitag2. In *USENIX Security Symposium*, pages 237–252. USENIX Association, August 2012. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf.

[7] R. Verdult, F. D. Garcia, and B. Ege. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In *22nd USENIX Security Symposium (USENIX Security 2013)*, pages 703–718. USENIX Association, 2015.