Wireless Attacks on Automotive Remote Keyless Entry Systems
Oswald, David

DOI:
10.1145/2995289.2995297

License:
None: All rights reserved

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):

Link to publication on Research at Birmingham portal

Publisher Rights Statement:
Checked 20/10/16

General rights
Unless a licence is specified above, all rights (including copyright and moral rights) in this document are retained by the authors and/or the copyright holders. The express permission of the copyright holder must be obtained for any use of this material other than for purposes permitted by law.

• Users may freely distribute the URL that is used to identify this publication.
• Users may download and/or print one copy of the publication from the University of Birmingham research portal for the purpose of private study or non-commercial research.
• Users may use extracts from the document in line with the concept of ‘fair dealing’ under the Copyright, Designs and Patents Act 1988 (?
• Users may not further distribute the material nor use it for the purposes of commercial gain.

Where a licence is displayed above, please note the terms and conditions of the licence govern your use of this document.

When citing, please reference the published version.

Take down policy
While the University of Birmingham exercises care and attention in making items available there are rare occasions when an item has been uploaded in error or has been deemed to be commercially or otherwise sensitive.

If you believe that this is the case for this document, please contact UBIRA@lists.bham.ac.uk providing details and we will remove access to the work immediately and investigate.
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 authorize 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.

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, Skoda, Audi) based the security of their RKE system on a few global cryptographic keys, potentially affecting hundreds of million vehicles worldwide. 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 vehicles worldwide. 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.

2. REFERENCES


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, Skoda, Audi) based the security of their RKE system on a few global cryptographic keys, potentially affecting hundreds of million vehicles worldwide. 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 worldwide. 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.

2. REFERENCES


