Breaking automotive remote keyless entry systems

or: why your car is not a safe box

David Oswald$^1$

joint work with: Flavio D. Garcia$^1$, Timo Kasper$^2$ and Pierre Pavlidès$^1$

1. University of Birmingham, UK
2. Kasper & Oswald GmbH, Germany
Remote Keyless Entry (RKE)
- Active UHF transmitter (315 / 433 / 868 MHz)
- Unidirectional
- Sometimes integrated with immobilizer chip ("hybrid"), sometimes separate

Im mobilizer (Immo)
- Passive RFID at 125 kHz
- Many broken systems (DST40, Hitag2, Megamos)

Wireless attacks?
Fix codes

Eavesdropping and replay from 10 ... 100 m
More examples for fix code systems
Rolling codes

\[ \text{uid, enc}_K(\text{ctr}', \text{btn}) \]

\[ \text{uid, enc}_K(\text{ctr}' + 1, \text{btn}) \]

\[ \text{uid, enc}_K(\text{ctr}' + 2, \text{btn}) \]

Decrypt \( \text{ctr}' \)

if \( \text{ctr} < \text{ctr}' < \text{ctr} + \Delta \)

\[ \text{ctr} := \text{ctr}' \]

open / close

"validity window"
Rolling codes

uid, $\text{enc}_K(\text{ctr'}, \text{btn})$

Note: there are some devices (medical) that use rolling codes w/o crypto

ctr' incremented on each button press, replay fails
Previous attacks on RKE

• 2007: Cryptanalysis of KeeLoq garage door openers ($2^{16}$ plaintext/ciphertext pairs) by Biham et al.
• 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
Side-channel attacks on KeeLoq

• Key derivation based on manufacturer key $k_M$: 
  $k_{device} = f(uid, k_M)$

• Recover $k_{device}$ with 10 power traces

• But: $k_M$ used in every receiver of manufacturer

• Recover $k_M$ with single power trace

• Single point of failure
Previous attacks on RKE

- 2007: Cryptanalysis of KeeLoq garage door openers ($2^{16}$ plaintext/ciphertext pairs) by Biham et al.
- 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
- 2010: Relay attacks on passive keyless entry systems (Francillon et al.)
Passive keyless entry systems (PKES)

Car to key: 125 kHz, short range
Key to car: 433 MHz, long range
Relay attacks on PKES

wakeup, nonce c

Long-range RF link

uid, $\text{enc}_K(c)$

Car to key: 125 kHz, short range

Key to car: 433 MHz, long range
Montag, den 10.10.2016, 9:00 Uhr, Landgericht Detmold (Strafkammer I)

Strafsache gegen M. aus Litauen, Verteidigerin: Rechtsanwältin Grohmann aus Münster

wegen schweren Bandendiebstahls in 21 Fällen
Staatsanwaltschaft Detmold 31 Js 199/16

Die Staatsanwaltschaft Detmold legt dem 28 Jahre alten Angeklagten folgendes zur Last:

Der Angeklagte soll Mitglied einer organisierte agierenden Gruppe litauischer Autoscheiber sein, die in Deutschland Fahrzeuge der Oberklasse mit einem Wert zwischen 33.000,00 und 130.000,00 € entwendet haben sollen, welche mit einem Keyless-Go-System ausgestattet sind.

Derartige Fahrzeuge lassen sich starten, ohne dass ein Zündschlüssel in ein Zündschloss eingeführt wird. Vielmehr ist es für das Starten des Fahrzeugs ausreichend, dass sich der zugehörige Fahrzeugschlüssel oder die zugehörige Chipkarte im Fahrzeug befindet. Zudem lassen sich die verschlossenen Fahrzeuge öffnen, wenn sich der Schlüssel im unmittelbaren Umfeld des Fahrzeugs befindet.

Die hier agierende Tätersgruppe, zu der auch der Angeklagte zählen soll, habe sogenannte „Mobi-Finder“ als Repeater verwendet, mit welchen das Funksignal der in der Wohnung der Geschädigten befindlichen Fahrzeugschlüssel aufgegriffen und weitergeleitet wurde.
Previous attacks on RKE

• 2007: Cryptanalysis of KeeLoq garage door openers (2^{16} plaintext/ciphertext pairs) by Biham et al.
• 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
• 2010: Relay attacks on passive keyless entry systems (Francillon et al.)
• 2015: “RollJam” by Spencerwhyte / Kamkar (had been proposed before)
“Intelligent jamming”

uid, $\text{enc}_K(\text{ctr}', \text{btn}), \text{crc}$
“Intelligent jamming”

Attacker now has another valid rolling code \((\text{ctr}' + 1)\)
However, cannot change \(\text{btn}\)!
Question:
State of RKE security in 2016
(or: have we learnt from KeeLoq?)
**Cryptographic** attack surface

uid, $\text{enc}_K(\text{ctr'}, \text{btn})$

Option 1: Attack key management
Option 2: Attack crypto
The VW Group System
VW Group RKE

- > 10% worldwide market share
- Immobilizer (Megamos) and RKE separate for most vehicles
- Proprietary RKE system, mostly 434.4 MHz
- We analyzed vehicles between ~2000 and today
- Four main schemes (VW-1 ... VW-4) studied
VW Group RKE: signals

Step 1: Eavesdropping & decoding
VW Group RKE: signals

Step 1: Eavesdropping & decoding

• VW-1:

• VW-2 ... 4:
Analyzing ECUs

Step 2: Obtain ECUs for analysis (eBay) ...
Reverse engineering

Step 3: Reverse-engineering ECUs
Example: VW-3

- AUT64\_{K_3}(\text{uid, ctr}', \text{btn}'), \text{btn}

- AUT64 is a proprietary block cipher, no trivial attacks known
- ... but key \( K_3 \) is \textbf{the same} in all VW-3 vehicles
- VW-2: Same cipher, different key
- VW-1: Weak crypto (LFSR)
Example: VW-3

- AUT64 is a proprietary block cipher, no trivial Aacks known
- ... but key $K_3$ is the same in all VW-3 vehicles
- VW-2: Same cipher, different key
- VW-1: Weak crypto (LFSR)

Byte permutation $\sigma$

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 \\
\end{array}
\]
Example: VW-4

- Used from ~ 2010 onwards
- Secure standard cipher: XTEA
- ... but again one worldwide key $K_4$
- Adversary can clone remote by eavesdropping a single rolling code
Affected vehicles

• **Audi**: A1, Q3, R8, S3, TT, other types of Audi cars (e.g. remote control 4D0 837 231)

• **VW**: Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, Golf 5, Golf 6, Golf Plus, Jetta, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran, Up

• **Seat**: Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII, Toledo

• **Škoda**: City Go, Roomster, Fabia 1, Fabia 2, Octavia, Superb, Yeti

• **In summary**: probably most VW group vehicles between 2000 and today not using Golf 7 (MQB) platform
VW RKE demo
Intermezzo

- Cryptographic algorithms improving over time, but: Secure crypto ≠ secure system
- Reverse engineering ECU firmware yields a few worldwide keys
- Attack highly practical and scalable
- MQB allegedly protected
- Seems worse compared to KeeLoq (’08), actually quite similar though
The Hitag2 System
Previous work on Hitag2

• At Usenix Security ’12, Verdult et al. presented a secret key recovery attack against Hitag2 immobilizer requiring:
  – Immobilizer transponder uid
  – 136 authentication attempts from the car
  – 5 minutes computation

• Note: This attack is not car-only due to the first requirement
Hitag2 RKE: Our contribution

• Step 1: Black-box reverse engineering of RKE protocol
  – Known cipher and inputs
  – Trial-and-error, guessing probable implementations

• Step 2: 136 traces is not practical in a RKE context; need for improved attack
RKE protocol (simplified)

Diversified keys

<table>
<thead>
<tr>
<th>id</th>
<th>k</th>
<th>ctr</th>
</tr>
</thead>
<tbody>
<tr>
<td>id₁</td>
<td>k₁</td>
<td>ctr₁</td>
</tr>
<tr>
<td>id₂</td>
<td>k₂</td>
<td>ctr₂</td>
</tr>
<tr>
<td>id₃</td>
<td>k₃</td>
<td>ctr₃</td>
</tr>
</tbody>
</table>

MACₖ is 32 bits of keystream

uid, btn, ctr, MACₖ, crc

If (ctr₁ < ctr'₁ < ctr₁ + Δ) then ctr₁ := ctr'₁; open
A few observations

• Put uid, btn, ctr, key into Hitag2, MAC is 32 bit of keystream
• Only a few bit difference in input for subsequent protocol runs (ctr and btn change)
• Hybrid chip (Immo + RKE) uses a different secret key but the same uid (can be eavesdropped from 100 m)
• Hitag2 systems have diversified keys
Our novel attack requires:

- ≈ 4 to 8 traces (key presses)
- $40 Arduino board can collect them
- Speeding up trace collection: Device also implements reactive jamming:

uid, btn, ctr, MAC_k, crc
Hitag2 cipher

48 bit internal state (LFSR stream $a_0a_1...$)

$$a_0...a_{31} = id_0...id_{31}$$
$$a_{32}...a_{47} = k_0...k_{15}$$
$$a_{48+i} = k_{16+i} \oplus \{\text{data}\}_i \oplus f(a_i...a_{47+i})$$

Initialized LFSR = $a_{32}...a_{79}$
Hitag2 cipher

48 bit internal state (LFSR stream $a_0a_1...$)

$\begin{align*}
a_0...a_{31} &= id_0...id_{31} \\
a_{32}...a_{47} &= k_0...k_{15} \\
a_{48+i} &= k_{16+i} \oplus iv_i \oplus f(a_i...a_{47+i})
\end{align*}$

Initialized LFSR = $a_{32}...a_{79}$
A fast correlation attack on Hitag2 (simplified)

- Guess a 16-bit window value
A fast correlation attack on Hitag2 (simplified)

Score guess as ratio of unknown input bits with correct output
A fast correlation attack on Hitag2 (simplified)

Score guess as ratio of unknown input bits with correct output
A fast correlation attack on Hitag2 (simplified)

Score guess as ratio of unknown input bits with correct output
A fast correlation attack on Hitag2 (simplified)

• Discard overall low scoring guesses
• Increase window size by one
• Repeat
• Takes ~1 minute on a laptop to recover the key
Practical limitations

- Only the 10 LSBs of the counter are sent over the air, but all 28 bits are used
  - we need to guess 18 MSBs -> surprisingly easy as they start from zero
- Attack works with 4 traces for Immo, as it uses a random challenge. RKE traces give out less information so we need more, usually 8.

<table>
<thead>
<tr>
<th>UID</th>
<th>btn</th>
<th>ctr</th>
<th>challenge</th>
<th>MAC</th>
<th>crc</th>
</tr>
</thead>
<tbody>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>0294</td>
<td>0000e948</td>
<td>27ee2032</td>
<td>1e</td>
</tr>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>0295</td>
<td>0000e958</td>
<td>2dee2f1e</td>
<td>be</td>
</tr>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>02a9</td>
<td>0000ea98</td>
<td>220d918e</td>
<td>45</td>
</tr>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>02ab</td>
<td>0000eab8</td>
<td>2a0f91e8</td>
<td>fc</td>
</tr>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>0338</td>
<td>0000f388</td>
<td>08f405c9</td>
<td>07</td>
</tr>
<tr>
<td>5ad40e29</td>
<td>08</td>
<td>033a</td>
<td>0000f3a8</td>
<td>08f48d8a</td>
<td>20</td>
</tr>
</tbody>
</table>
Hitag2 RKE attack demo
## Hitag2 RKE vehicles

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfa Romeo</td>
<td>Giulietta</td>
<td>2010</td>
</tr>
<tr>
<td>Chevrolet</td>
<td>Cruze Hatchback</td>
<td>2012</td>
</tr>
<tr>
<td>Citroen</td>
<td>Nemo</td>
<td>2009</td>
</tr>
<tr>
<td>Dacia</td>
<td>Logan II</td>
<td>2012</td>
</tr>
<tr>
<td>Fiat</td>
<td>Punto</td>
<td>2016</td>
</tr>
<tr>
<td>Ford</td>
<td>Ka</td>
<td>2009, 2016</td>
</tr>
<tr>
<td>Lancia</td>
<td>Delta</td>
<td>2009</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>Colt</td>
<td>2004</td>
</tr>
<tr>
<td>Nissan</td>
<td>Micra</td>
<td>2006</td>
</tr>
<tr>
<td>Opel</td>
<td>Vectra</td>
<td>2008</td>
</tr>
<tr>
<td>Opel</td>
<td>Combo</td>
<td>2016</td>
</tr>
<tr>
<td>Peugeot</td>
<td>207</td>
<td>2010</td>
</tr>
<tr>
<td>Peugeot</td>
<td>Boxer</td>
<td>2016</td>
</tr>
<tr>
<td>Renault</td>
<td>Clio</td>
<td>2011</td>
</tr>
<tr>
<td>Renault</td>
<td>Master</td>
<td>2011</td>
</tr>
<tr>
<td>Opel</td>
<td>Astra H</td>
<td>2008</td>
</tr>
<tr>
<td>Opel</td>
<td>Corsa D</td>
<td>2009</td>
</tr>
<tr>
<td>Fiat</td>
<td>Grande Punto</td>
<td>2009</td>
</tr>
</tbody>
</table>
RKE system in some cars...

State:

<table>
<thead>
<tr>
<th>id</th>
<th>k</th>
<th>ctr</th>
</tr>
</thead>
<tbody>
<tr>
<td>id₁</td>
<td>k₁</td>
<td>ctr₁</td>
</tr>
<tr>
<td>id₂</td>
<td>k₂</td>
<td>ctr₂</td>
</tr>
<tr>
<td>id₃</td>
<td>k₃</td>
<td>ctr₃</td>
</tr>
</tbody>
</table>

If \((\text{ctr₁} - \Delta < \text{ctr'}₁ < \text{ctr₁} + \Delta)\)
then \(\text{ctr₁} := \text{ctr'}₁; \text{open}\)
Have we learnt from KeeLoq?

Not really
Countermeasures:
What to do?
Countermeasures

For owners of affected vehicles:
- Stop using RKE
- Hope for vendor upgrade

For manufacturers:
- Use secure key distribution and good crypto
- E.g. exchange keys via LF (immo) once and use AES for RKE

Responsible disclosure

• We contacted VW Group in Dec 2015 and NXP Semiconductors in Jan 2016

• In general: good cooperation/communication

• VW Group claims that MQB has diversified keys

• NXP has AES-based products
Conclusions

• Poor crypto is bad ...
• Poor key management is worse.
• Finding widespread examples was rather surprising in 2016.
• This research may explain mysterious theft cases without forced entry.

Your car is not a safe box.
Thanks for your attention!
Questions?