Testing the Security of Embedded Systems: Side-Channel Attacks, Reverse Engineering, and more

David Oswald

Stuttgart, 7. Mai 2019
Vector Testing Symposium
Classical IT security
/software, interfaces/
Embedded security
(hardware, firmware, interfaces)

CC-BY-SA-3.0
Albert Belchers
Research Question:

**Security of Embedded Devices?**

<table>
<thead>
<tr>
<th>12:45pm</th>
<th>Lunch Break &amp; Trade Exhibition</th>
</tr>
</thead>
</table>
| 02:00pm | Testing the Security of Embedded Systems  
Side-Channel Attacks, Reverse Engineering, and more |

- Presentation of test methods for **safety analysis** on the basis of practical case studies
- Firmware extraction

Dr. David Oswald, KAOS
An implementation attack ...
Principle of Side-Channel Analysis
(here: listen to Sound)

A Bank Robbery
The world is changing...
Principle of Side-Channel Analysis
(Monitor the power consumption / run-time)

The world is changing...

...the tools are, too.
Case Study: Remote Keyless Entry
Remote Keyless Entry (1)

Uni-directional

First systems: **Fixed code**
Remote Keyless Entry (2)
Uni-directional with Crypto

Industry reacts: **Rolling code**
Remote Keyless Entry (2)
Uni-directional with Crypto

Industry reacts: **Rolling code**

Option 1: Attack **key management**

Option 2: Attack **crypto**

**Cipher**

encrypt(124)
encrypt(125)
...

**BUT** there are attacks ...
Side-Channel Attacks on KeeLoq (Crypto 2008)
Power analysis attack (with physical access):
→ clone a remote control from 10 power measurements
→ obtain manufacturer key from 1 power measurement

Flaw of KeeLoq system:
Key derivation from manufacturer key $k_M$

- $k_{\text{remote\_control}} = f(#\text{ser}, k_M)$
- $k_M$ used in every receiver of manufacturer $M$
- Single point-of-failure
Case Study: KeeLoq Rollcode
German TV (3Sat NANO, 2008)
Automotive RKE
(Usenix 2016)
Santa’s Problem
So how did Santa do it?
VW Group RKE

Step 1: Eavesdropping & decoding
Step 2: Obtain ECUs for analysis (eBay) ...
Reverse engineering

Step 3: Reverse-engineering ECUs

```assembly
sub_F5CA:
pshd
pshx
lea \%r6, $t0, SP
and $t0, $t0, $t0
clr
add $t0, $t0, $t0
add $8000, $t0
bce loc_F5D2
inx
```

```assembly
loc_F5D2:
std $a0, $t0
lrd $11, $t0
ldr $12, $t0
subd $E, $t0
sbex $C, $t0
```
Management Summary

*VW Group*: secure crypto ≠ secure system

- extract a few **worldwide keys**

→ **instantly copy** a remote control from **1 signal**

- RF attack highly practical and scalable
VW Group: 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**: most VW group vehicles between 1995 and 2016/17 except the new Golf 7 (MQB) platform
Hitag2 RKE Attack Demo
<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>
Management Summary

**VW Group**: secure crypto ≠ secure system
- extract a few **worldwide keys**
  - instantly copy a remote control from **1 signal**
- RF attack highly practical and scalable

**Hitag2**: diversified keys but bad crypto
- eavesdrop ≈ **4 to 8 signals** (key presses)
  - copy remote control with **some computations**

Poor crypto is bad, but poor key management is worse.
Case Study: RFID Cards
Examples for RFID cards w/ crypto

Broken crypto
• 125 kHz: Hitag 1/2/S, Megamos, ...
• 13.56 MHz: Mifare Classic, HID iClass, Legic Prime, ...

→ Cloning possible with medium efforts

Secure crypto
• 13.56 MHz: Mifare DESfire EV1/2, NXP SmartMX, Infineon SLE XX, JCOP, ...

→ Cloning „impossible“

Unknown: Legic Advant
Analysis of the ID-Card 1/2

Extracting Keys

• test our key-recovery on ID-Card → extraction of all secret keys

... 

• surprising discovery:

All ID-Cards have **identical keys**!
Real-World Tests

• **clone** ID-Cards (copy to blank card)
  → payments with clones accepted ?

• **modify** credit balances
  → payments with “counterfeit money” possible ?

• **production** of “new” cards (new card number)
  → pay with arbitrarily generated cards ?

No effective countermeasures in the back-end!
new issued cards are Mifare DESfire (EV1)
old Mifare Classic cards are still working
improved backend: shadow accounts are used (...and still manually checked...)
ChameleonMini as a Virtual Wallet
ChameleonMini
A Versatile NFC Emulator and more
2006: Kaffeeetassen Transponder (Coffee Cup Tag)
ChameleonMini
Rev.E

- 8 card slots
- Integrated antenna
- Improved USB command set
- Widespread

open source project: https://github.com/emsec/ChameleonMini
ChameleonMini Rev.E visits the University of Aveiro, Portugal, Part 1: Barriers
ChameleonMini Rev.G

- (Basic) RFID Reader
- ATX Mega 128 + FRAM
- Li-Ion Battery

- 8 virtual card slots
- ISO 14443/ ISO 15693
- Log Mode
ChameleonMini and E-Mobility
(“Ladekarten” used all over Europe)

Identify with UID of Mifare Classic ...

Source:
https://github.com/emsec/ChameleonMini/issues/140
ChameleonMini and E-Mobility
What to do?
A system designer’s perspective
Secure Against Cyber Attacks
A System Designer’s Perspective: How to Secure The Internet of Things?

- Use **standard crypto** and **standard protocols**
- Test the security of your system!
- Implementation attacks: Practical threat, but:
  - Use certified devices (**secure hardware**)
  - Algorithmic countermeasures (**secure software**)
- System level: Second line of defense!
  - Shadow accounts / Logging (detect fraud)
  - Key diversification (minimize impact)
  - Fallback plan (update, notify, ...)


Expect the unexpected.
Thank you!
Questions? Comments?

Contact: info@kasper-oswald.de