Relaying contactless EMV transactions with off-the-shelf hardware
Something about me

- Jordi van den Breekel (NL)
- Graduation project (2014)
- Security consultant

KPMG the Netherlands

Dr. Nicola Zannone
Dr. Erik Poll
Dr. Joeri de Ruiter

Msc. Stan Hegt
Msc. Thijs Timmerman
Contents

• What is EMV?
• EMV Contactless transactions
• Relay attacks
• Performance
• Limits
• Conclusions
What is EMV?
Europay
Mastercard
Visa
From Section 5.5.4.3: If the card responds to GPO with SW1 SW2 = x'9000' and AIP byte 2 bit 8 set to b'0', and if the reader supports qVSDC and contactless VSDC, then if the Application Cryptogram (Tag '9F26') is present in the GPO response, then the reader shall process the transaction as qVSDC, and if Tag '9F26' is not present, then the reader shall process the transaction as VSDC.
EMV Contactless transaction
Relay attack scenario
Relay attack demonstration
Developments of relay attacks on EMV

- Relay attacks are not new
  - On EMV Contact (2005)
  - On NFC
    - Special hardware
    - Unlocked SE (e.g.
    - Modified Android

![Image of relay attack setup](image.png)
There's an app for that.
Android 4.4

- Host Card Emulation
- Adoption rate 2015: 41.3%+
## Performance

- **Typical Dutch transactions**: 330ms – 637ms
- **Basic relay transactions**: 1152ms – 1336ms
- **Max allowed transaction time**: 52 seconds

### Graph

<table>
<thead>
<tr>
<th></th>
<th>ING</th>
<th>Triodos</th>
<th>ABN new</th>
<th>ABN old</th>
<th>Knab</th>
<th>VF Card</th>
<th>VF Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>1.161</td>
<td>1.152</td>
<td>1.161</td>
<td>1.336</td>
<td>1.029</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maestro</td>
<td>462</td>
<td>453</td>
<td>462</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa</td>
<td>147</td>
<td>409</td>
<td>176</td>
<td>438</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EMV Contactless transaction
Select Payment Environment

Card

Terminal

<table>
<thead>
<tr>
<th>Application ID</th>
<th>Application name</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0000032010</td>
<td>Visa Electron</td>
<td>1</td>
</tr>
<tr>
<td>A0000032020</td>
<td>Visa V Pay</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application ID</th>
<th>Application name</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0000004306</td>
<td>Maestro</td>
</tr>
<tr>
<td>A0000032020</td>
<td>Visa V Pay</td>
</tr>
<tr>
<td>A0000002501</td>
<td>American Express</td>
</tr>
</tbody>
</table>
Android’s power savings function

• Network adapter
  • After 100ms of inactivity
  • Adds + 40ms additional delay
• Implement ‘keep-alive’ function

```java
public class Send extends AsyncTask<String, Void, String> {
    protected String doInBackground(String... commandApdu) {
        try {
            while (true) {
                MainActivity.writer.write("Stay Alive");
                MainActivity.writer.newLine();
                MainActivity.writer.flush();
                Thread.sleep(80);
            }
        } catch (Exception e) {
            return null;
        }
    }
}
```
Select Payment Environment

Return Application ID

Select Application ID

"Application selected"

Get Processing Options

4 Record Locations

Repeat four times

Request Record

Return Record

Generate Cryptogram

Return Cryptogram

Reduction: + 160ms
Performance results

<table>
<thead>
<tr>
<th>ING</th>
<th>Triodos</th>
<th>ABN new</th>
<th>ABN old</th>
<th>Knab</th>
<th>VF Card</th>
<th>VF Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>623</td>
<td>453</td>
<td>462</td>
<td>637</td>
<td>330</td>
<td>147</td>
<td>334</td>
</tr>
<tr>
<td>1.161</td>
<td>1.152</td>
<td>1.161</td>
<td>1.336</td>
<td>627</td>
<td>438</td>
<td>305</td>
</tr>
<tr>
<td>462</td>
<td>462</td>
<td>485</td>
<td>409</td>
<td>500</td>
<td>176</td>
<td>409</td>
</tr>
</tbody>
</table>

Relayed transaction with slowest card is faster than normal transaction
Amounts limits

• No PIN for < €25/$25
• Pin needed for > €25/$25
  • Cameras
  • PIN pad
  • Shoulder surfing
  • Infrared pictures (?)
Infrared pictures

iPhone ATM PIN code hack - HOW TO PREVENT

Mark Rober

183,012 subscribers

13,974,110 views

36,804 likes

2,810 dislikes
Infrared in practice

PIN entered: 1-2-3-4-5

PIN entered: 6-7-8-9-0
Infrared pictures

iPhone ATM PIN code hack - HOW TO PREVENT

Mark Rober
Abonnieren

183,012

13,974,110

36,804
2,810
## Amounts overview

<table>
<thead>
<tr>
<th>Limit</th>
<th>Without PIN</th>
<th>With PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV Contact</td>
<td>-</td>
<td>€2500-€5000</td>
</tr>
<tr>
<td>EMV Contactless</td>
<td>€25</td>
<td>€2500-€5000</td>
</tr>
</tbody>
</table>

- 1€ contact transactions protected with PIN worth up to €5000
- Contactless transactions up to €5000 allowed
Conclusion

• Relay setup possible with 2 OTS Android devices
• Simple application needed (± 2 days developing)
• No effective countermeasures existent
  • Probably difficult to realize
• Payment limits should be optimized
Thank you!

Contact: vandenBreekel.Jordi@KPMG.nl