Near Field Communication
Research Lab
Hagenberg

© Michael Roland
www.mroland.at

Applying Relay Attacks to Google Wallet

Michael Roland
NFC Research Lab Hagenberg
University of Applied Sciences Upper Austria

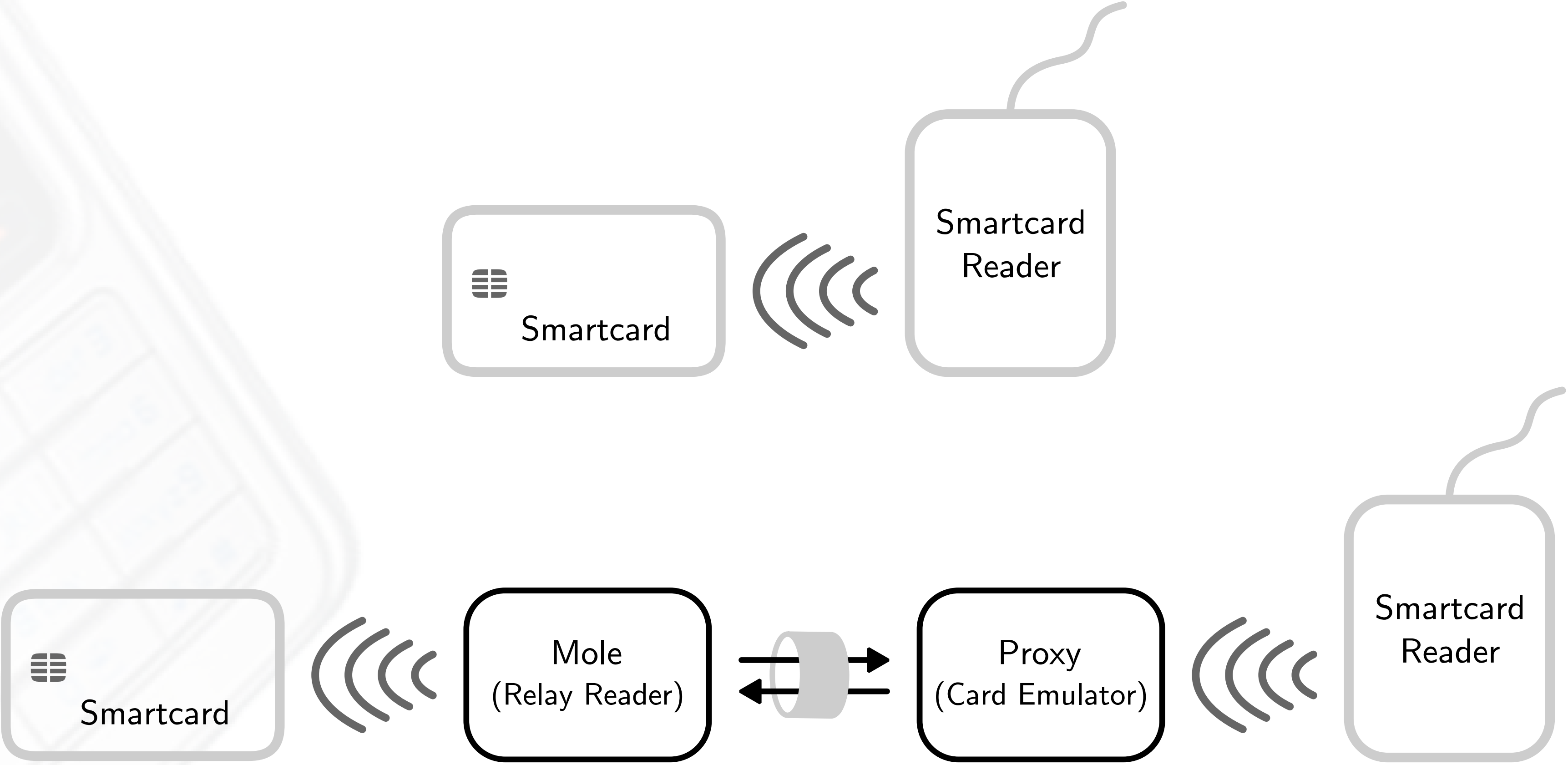
5th International Workshop on Near Field Communication
5 February 2013, Zurich, Switzerland

This work is part of the projects “4EMOBILITY” and “High Speed RFID” within the EU program “Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)” funded by the European Regional Development Fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

Outline

- Introduction
  - Relay Attack
  - Software-based Relay Attack
- Google Wallet
- Google Wallet Relay Attack
  - Test Setup
  - Limitations & Improvements
  - Workarounds
- Google‘s Response

Relay Attack



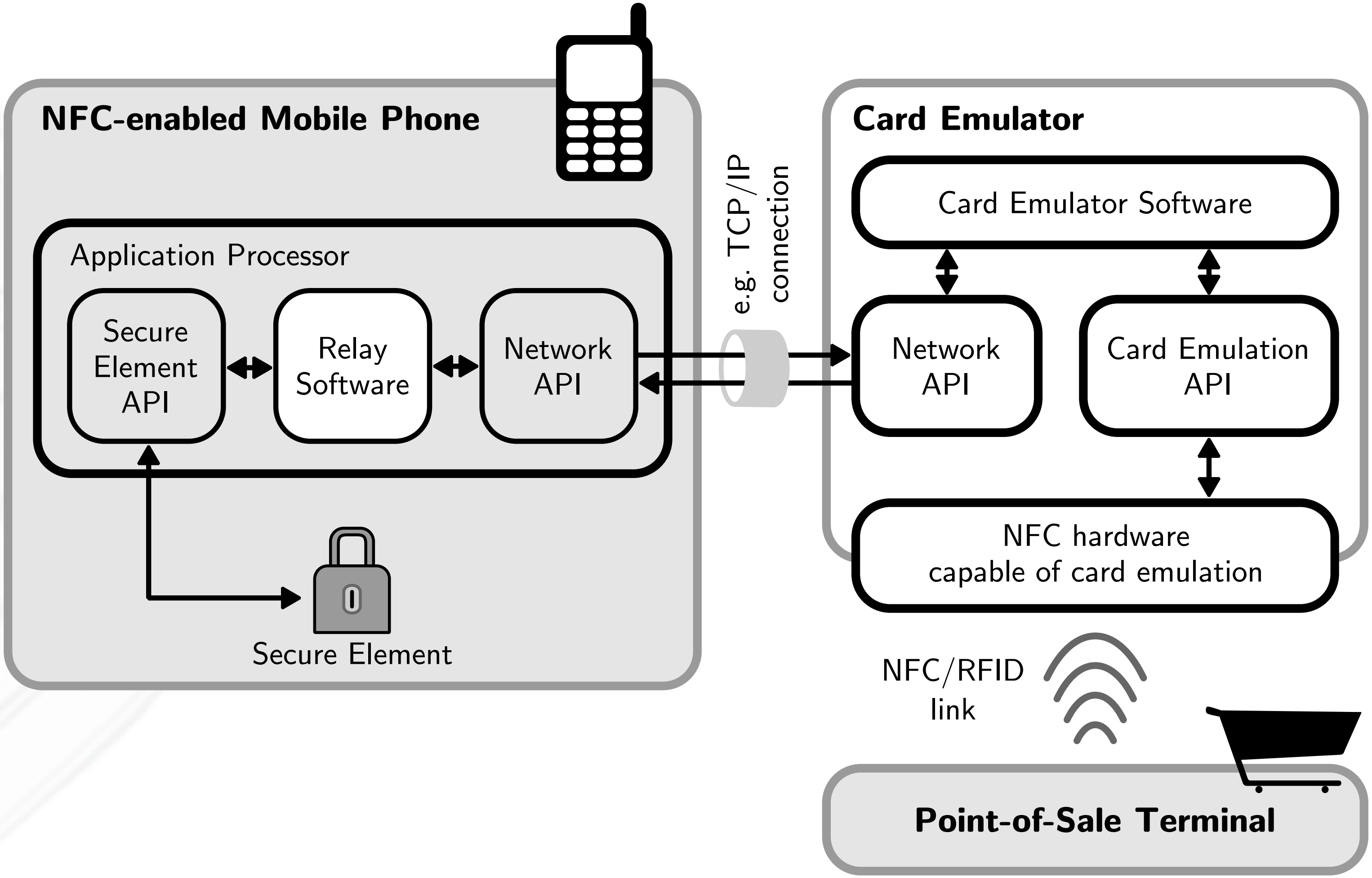
Relay Attack

- Cannot be prevented by application layer cryptography
  - Simple range extension of contactless communication channel
- Typical countermeasures:
  - Shielding of contactless interface with Faraday cage
  - Physical activation and deactivation
  - Two-factor authentication (e.g. PIN/password in addition to card)
  - Distance bounding protocols

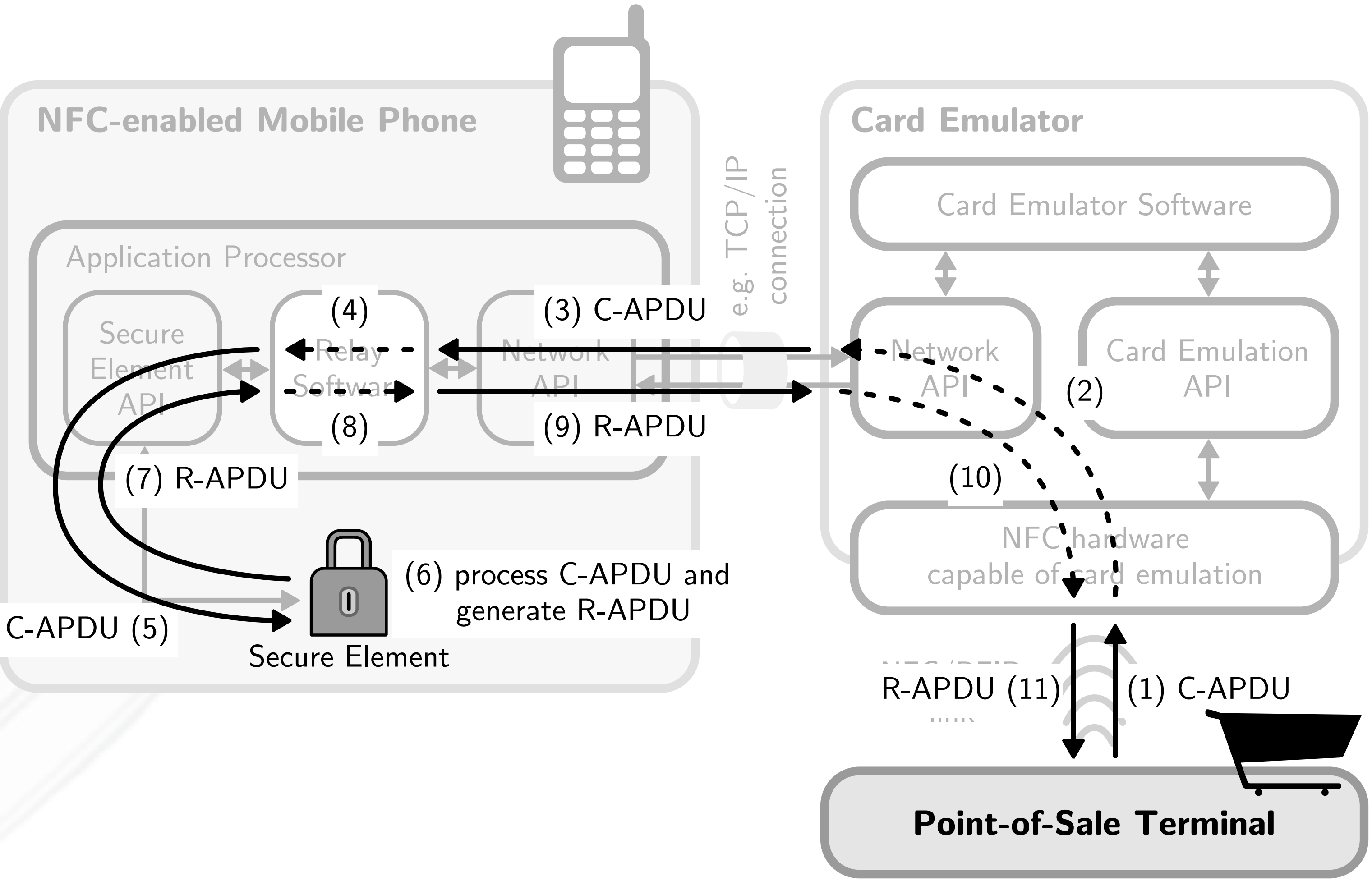
Software-based Relay Attack

- Relay attack: Mole requires **close physical proximity** to device-under-attack
- Software-based Relay Attack:
  - Secure element access through application processor
  - App (software) replaces physical mole
  - App needs access to secure element and network interface(s)
  - Secure element access typically through privilege escalation

Software-based Relay Attack

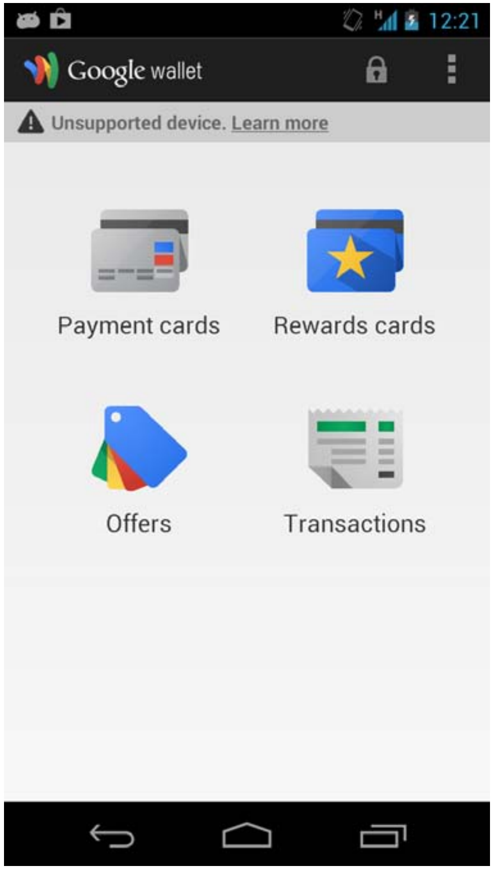


Software-based Relay Attack



Google Wallet

- Container for
  - Payment cards
  - Gift cards
  - Reward cards
  - Special offers
- Android app
  - User interface
- Java Card applets on secure element
  - Secure data storage
  - Interface with POS terminals

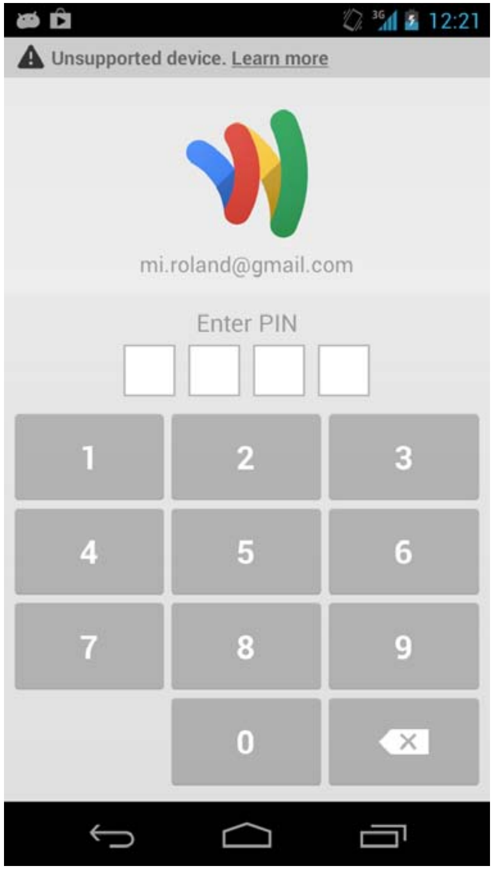


Analysis of Google Wallet

- Focus on communication between
  - Android app and secure element
  - POS terminal and secure element
- Secure element contains
  - Google Wallet on-card component
    - Manages access to payment cards, …
  - Google MIFARE access applet
    - Provides access to secure element’s MIFARE 4K memory
  - EMV-compliant proximity payment application

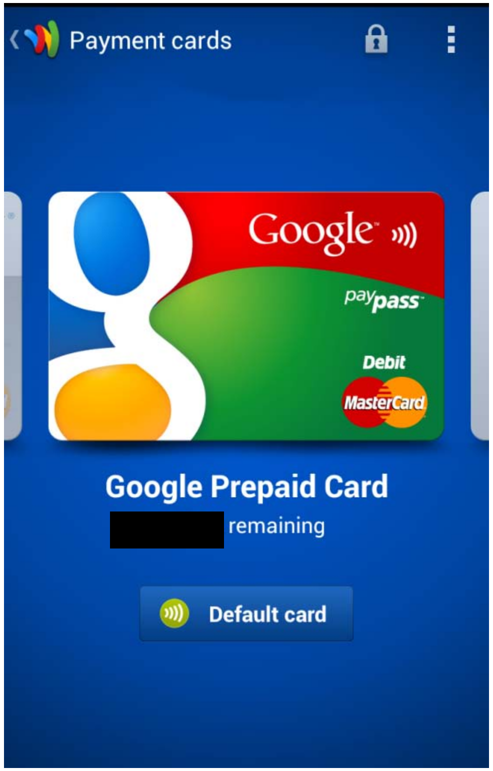
Google Wallet's PIN

- Unlocks access to
  - User interface (Google Wallet app)
  - EMV payment cards
- Issues
  - PIN is verified by Google Wallet app
    - Known attack on PIN hash exists!
  - On-card component does not verify the PIN
    - Unlock command: **`80 E2 00 AA 00`**
    - PIN is not necessary to unlock Google Wallet → Send unlock command instead!



Google Prepaid Card

- EMV-compliant
- MasterCard PayPass
- EMV Mag-Stripe protocol
  - with dynamic CVC3

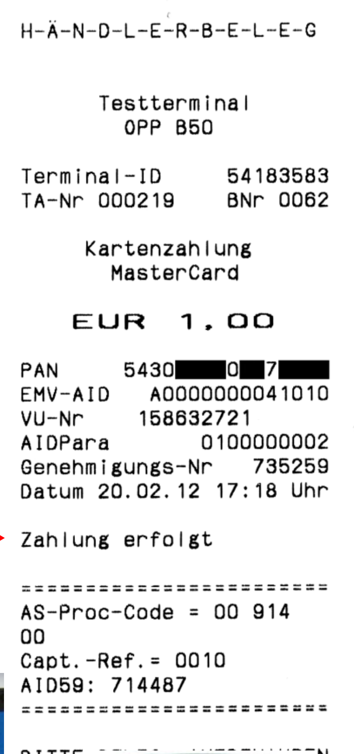


EMV Mag-Stripe Transaction

- *POS:* Select Proximity Payment System Environment (PPSE)
  - *SE:* Confirm and return list of available EMV payment applications
- *POS:* Select MasterCard Google prepaid card
  - *SE:* Confirm selection and return application details
- *POS:* Request processing options of the payment system
  - *SE:* Return processing options (Mag-Stripe mode only, online transactions only, no cardholder verification, etc.)
- *POS:* Request Mag-Stripe data file
  - *SE:* Return Mag-Stripe data of track 1 and track 2
- *POS:* Request computation of cryptographic checksum (CVC3) for a given random number
  - *SE:* Return transaction counter and dynamic CVC3 for track 1 and track 2

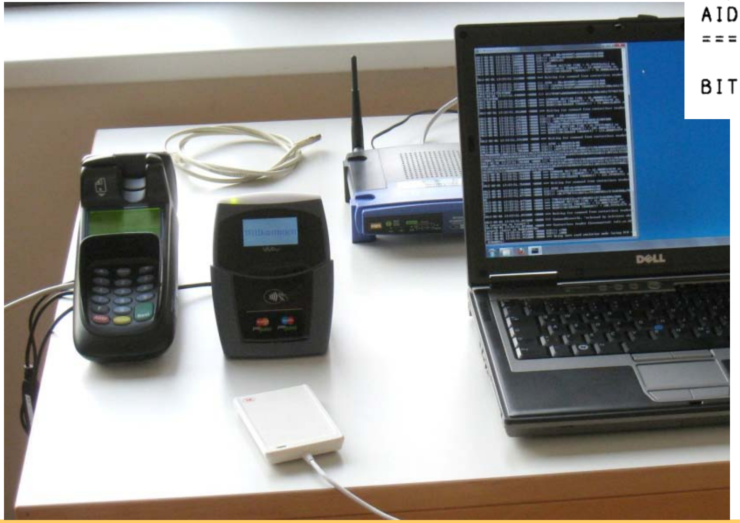
Relay Attack on Google Wallet

- Relay app
  - Android app
  - Unlock/lock Google Wallet on-card component
  - Forward APDUs to secure element
- Card emulator
  - Python application
  - ACR 122U
  - Notebook computer
- POS terminal
  - Hypercom Artema Hybrid
    ViVOtech ViVOpay 5000



```
H-Ä-N-D-L-E-R-B-E-L-E-G


    Testterminal
      OPP B50

Terminal-ID      54183583
TA-Nr 000219     BNr 0062

    Kartenzahlung
     MasterCard

    EUR   1,00

PAN      5430[redacted]0[redacted]7[redacted]
EMV-AID    A0000000041010
VU-Nr     158632721
AIDPara        0100000002
Genehmigungs-Nr    735259
Datum 20.02.12 17:18 Uhr

Zahlung erfolgt

========================
AS-Proc-Code = 00 914
00
Capt.-Ref.= 0010
AID59: 714487
========================

BITTE
```

Relayed payment
transaction **successful**



Limitations & Improvements

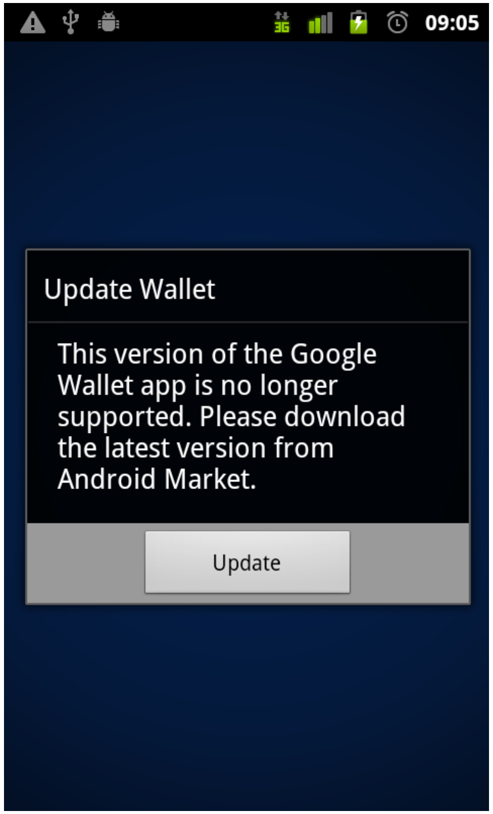
- Relay app needs access to secure element
  - Root privileges
  - Privilege escalation exploits
- Transaction limits
  - In Austria: € 25 for contactless transactions
  - Google Wallet: $ 100 possible according to user reports
  - Build “bot network” of wallets
    → Distribute payments to many wallets
- Slow relay communication (5 commands + 5 responses)
  - Only checksum computation contains dynamic data
    → 1 command + 1 response

Workarounds

- Timeouts of POS terminals
  - Now: 20 seconds with many POS terminals
  - Benchmark target of EMV specification: 500 ms
  - Problem: Cloud-based EMV applications use same principle as relay attack
- PIN verification
  - Now: PIN is only verified by Google Wallet app
  - PIN could be verified by on-card component
  - PIN could be verified at POS terminal
- Disable internal mode for payment applets
  - Modern secure elements can distinguish between external and internal mode communication
  - Rules can be setup on per-applet or per-APDU basis
  - Problem: Payment applets cannot be used for future on-device payment applications (e.g. payment in mobile phone's web browser)

Google's Response

- April 2012: Reported to Google
- June 2012: New installations no longer vulnerable
- September 2012: Existing users are forced to install update
- New version:
  - Blocks all access to payment applet from application processor (internal mode disabled)
  - PIN is still only verified by Wallet app



Update Wallet

This version of the Google Wallet app is no longer supported. Please download the latest version from Android Market.

© Michael Roland
www.mroland.at

Demo available at

http://youtu.be/hx5nbkDy6tc

http://youtu.be/_R2JVPJzufg

Michael Roland
Research Associate, NFC Research Lab Hagenberg
University of Applied Sciences Upper Austria

michael.roland (at) fh-hagenberg.at
www.mroland.at

This work is part of the projects “4EMOBILITY” and “High Speed RFID” within the EU program “Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)” funded by the European Regional Development Fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).