© Michael Roland
www.mroland.at

Applying Relay Attacks to Google Wallet

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

7th WIMA NFC – Research Track
10 April 2013, Monaco

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).

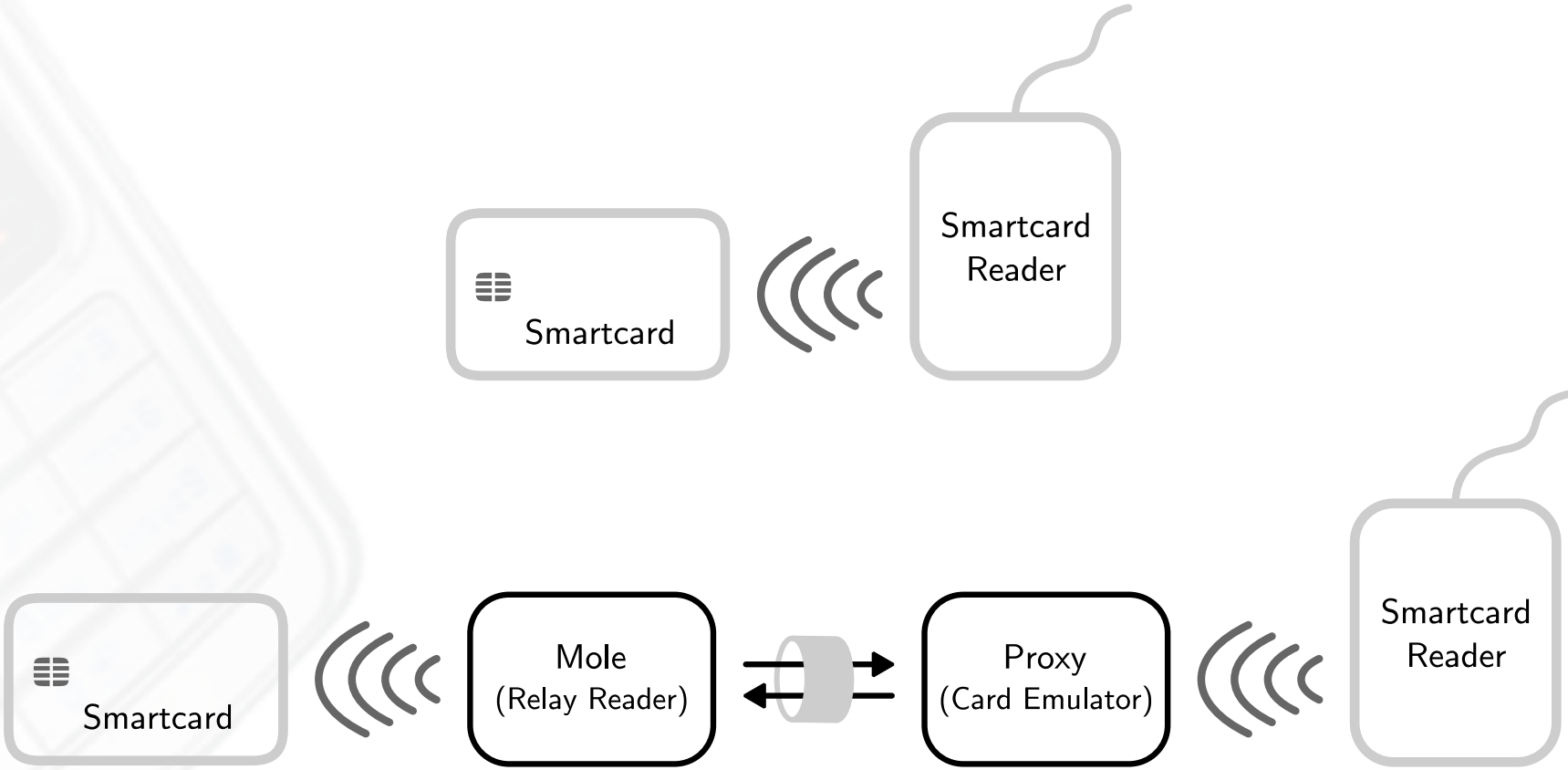
© Michael Roland
www.mroland.at

Outline

- Introduction
  - Relay Attack
  - Software-based Relay Attack
- Google Wallet
- Google Wallet Relay Attack
- Google‘s Response

© Michael Roland
www.mroland.at

Relay Attack



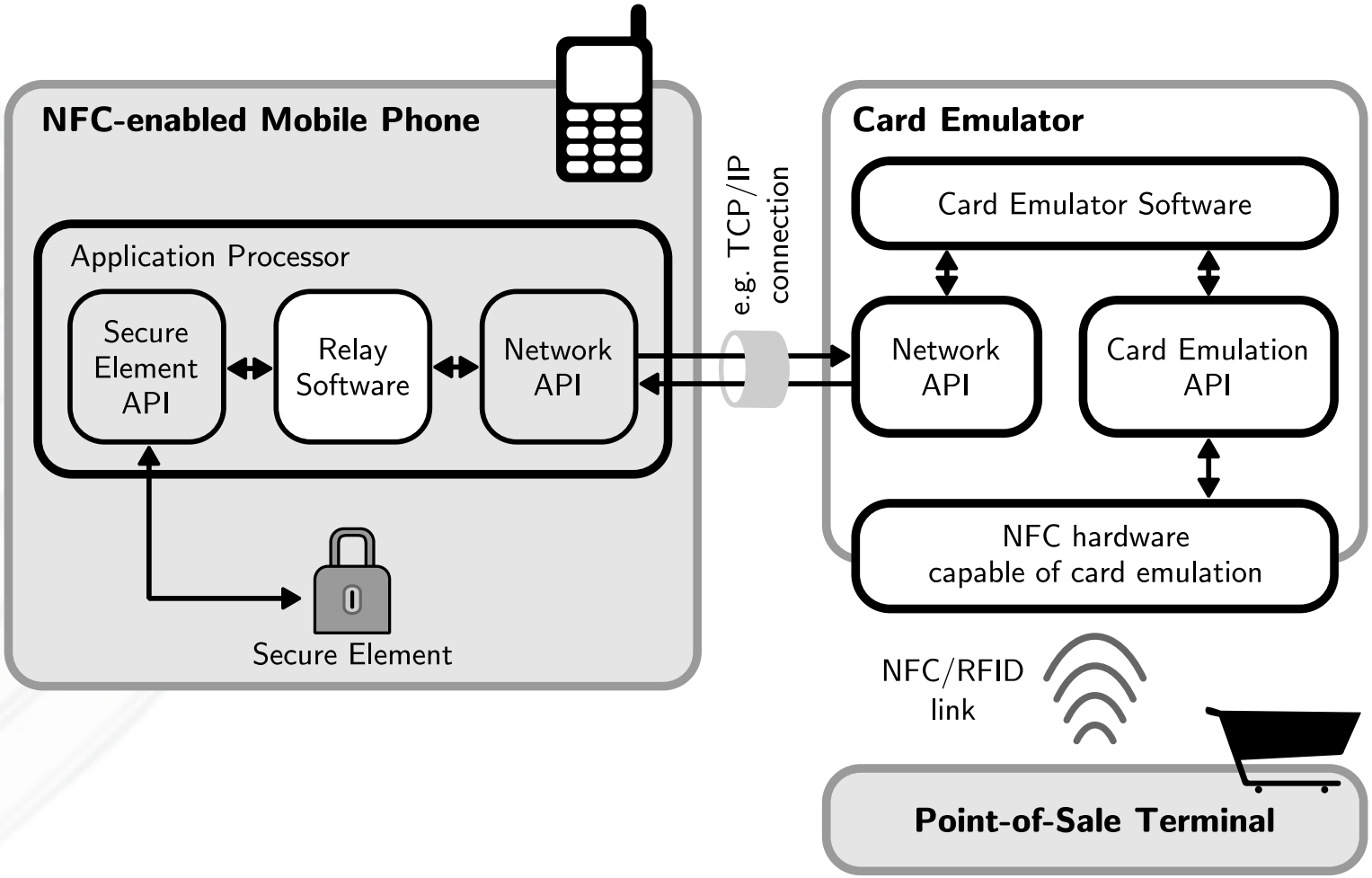
© Michael Roland
www.mroland.at

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

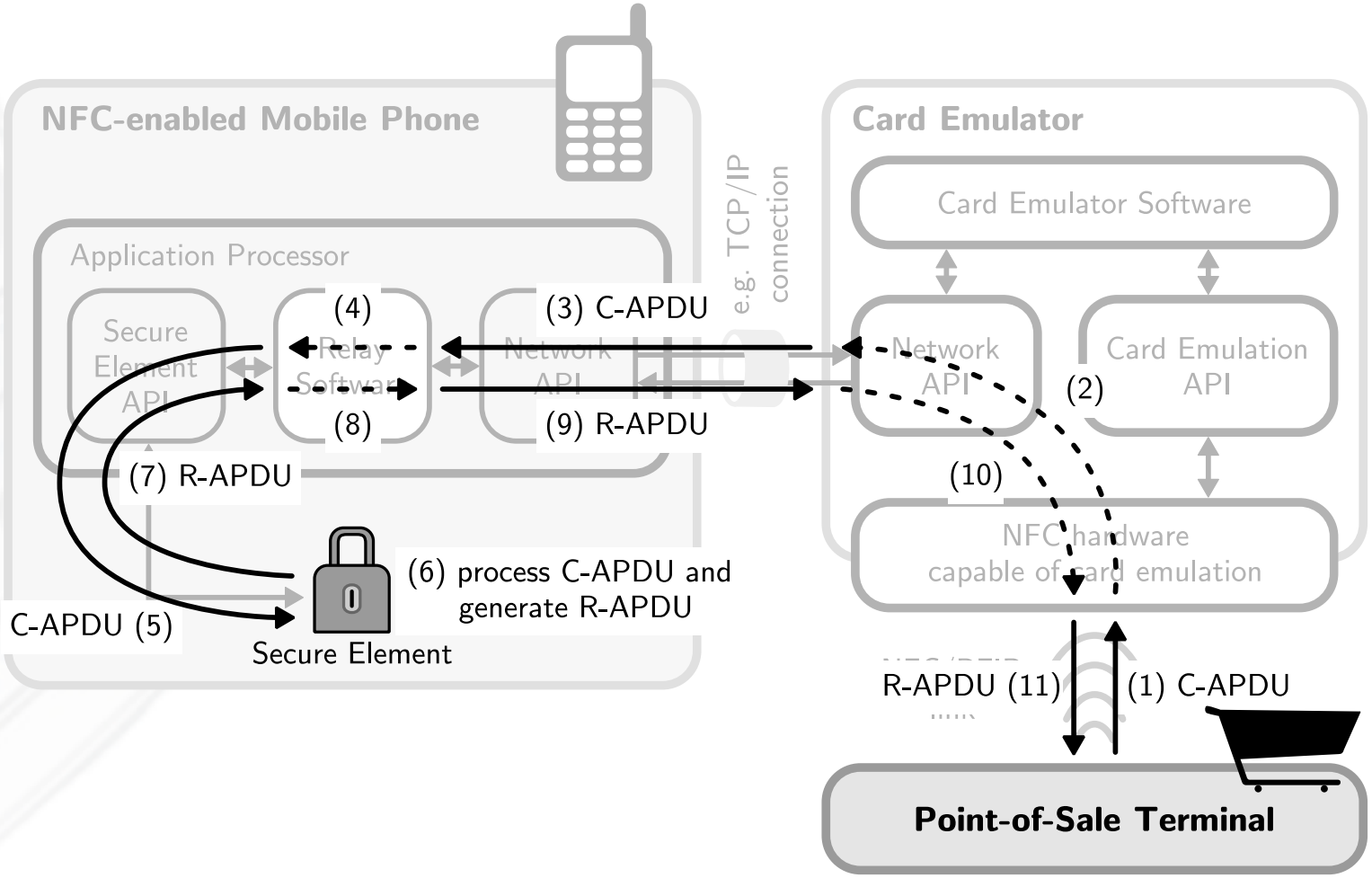
© Michael Roland
www.mroland.at

Software-based Relay Attack



© Michael Roland
www.mroland.at

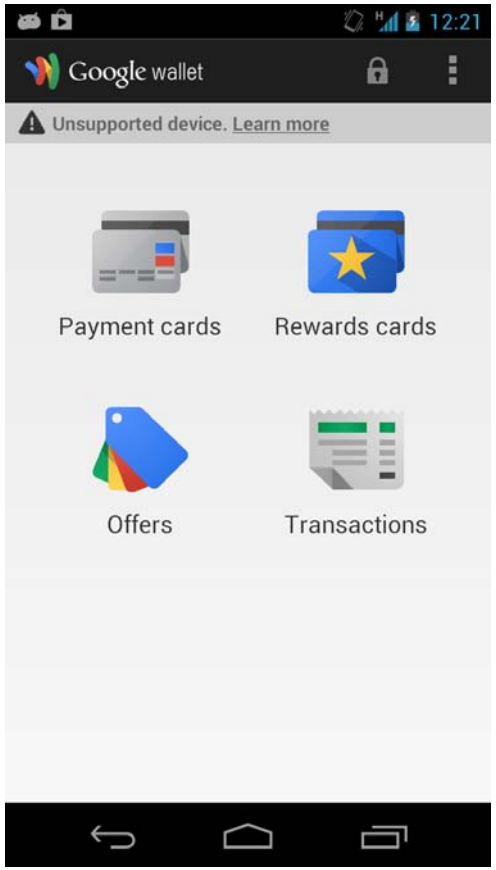
Software-based Relay Attack



© Michael Roland
www.mroland.at

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



© Michael Roland
www.mroland.at

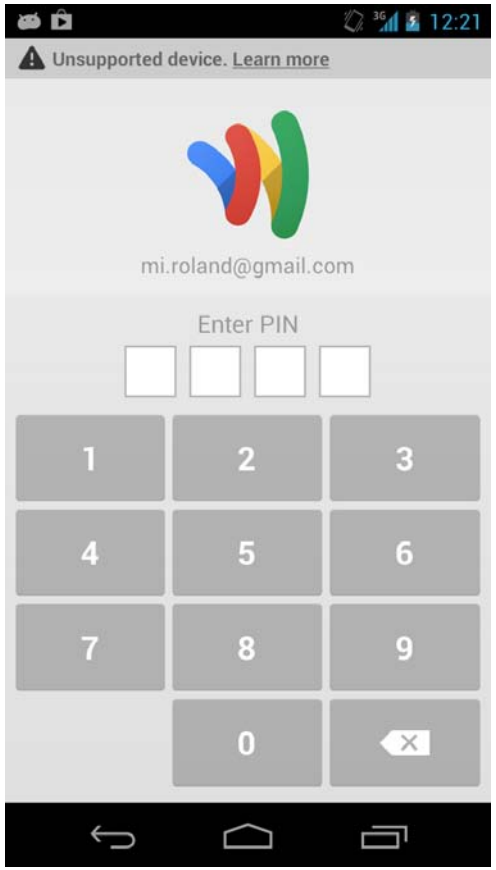
Analysis of Google Wallet

- 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

© Michael Roland
www.mroland.at

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!



© Michael Roland
www.mroland.at

Google Prepaid Card

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

© Michael Roland
www.mroland.at

Relay Attack on Google Wallet

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

Relayed payment transaction **successful**

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

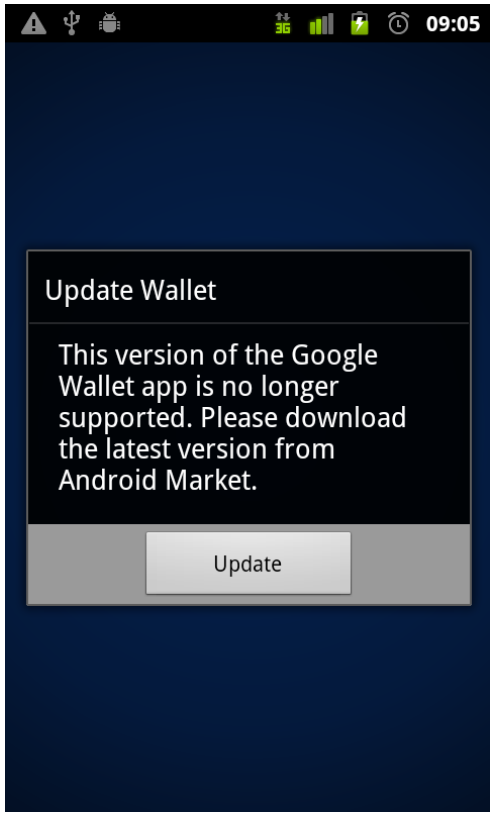
==========
AS-Proc-Code = 00 914
00
Capt.-Ref.= 0010
AID59: 714487
==========

BITTE [redacted]N

© Michael Roland
www.mroland.at

Google's Response

- April 2012: Reported to Google
- End of April 2012: New installations no longer vulnerable
- June 2012: New secure element applet
- September 2012: Existing users are forced to install update
- October 2012: PIN verification on secure element



© 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).