Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?

Michael Roland
University of Applied Sciences Upper Austria, Hagenberg, Austria

IWSSI**SPMU**2012 – International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use
18 June 2012, Newcastle, UK

This work is part of the project “4EMOBILITY” 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
  - Near Field Communication
  - Secure Element-based Card Emulation
  - Software Card Emulation
- Software Card Emulation
  - Advantages
  - Disadvantages
- Conclusion

Near Field Communication

- Advancement of proximity RFID and smartcard technology
- Idea: Touch an object to trigger an action
- 3 operating modes
  - Peer-to-peer mode
  - Reader/writer mode
  - Card emulation mode

NFC in a Mobile Phone

(1)

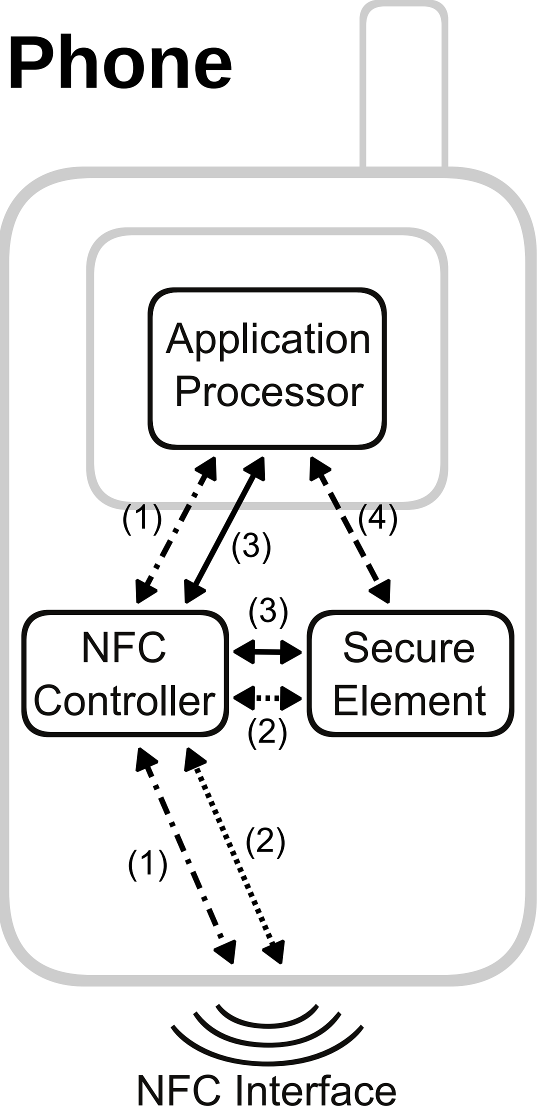
Application processor – NFC interface

Peer-to-peer mode,
Reader/writer mode,
Software card emulation

(2)

Secure element – NFC interface

Secure card emulation



(3)

Application processor – Secure element (via NFC controller)

Secure card emulation (internal access to secure element)

(4)

Application processor – Secure element (direct)

Secure card emulation (internal access to secure element)

Card Emulation

- NFC device emulates a contactless smartcard
  - Access control token
  - Credit card
  - …
- Compatibility to existing proximity smartcard infrastructure
- Emulation by
  - Smartcard chip (secure element)
  - Software on application processor

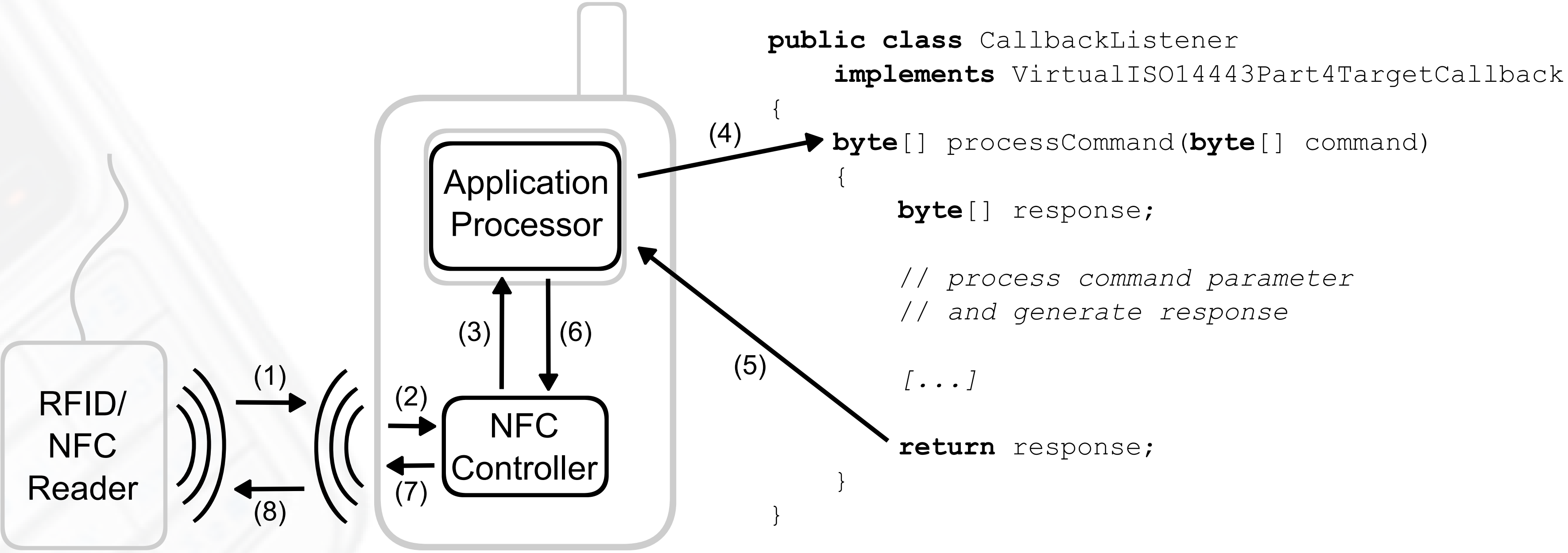
Secure Element-based Card Emulation

- Secure Element
  - Dedicated secure element chip
  - UICC (“SIM card”)
  - SD memory card
- Same high security level as other smartcards
  - Secure storage
  - Secure execution environment
  - Hardware-based cryptographic operations

Attacks on Card Emulation and Smartcards

- Example: Relay Attack
  - Communication between smartcard and reader can be relayed over longer distances
  - Proxy reader in proximity of the smartcard
  - Proxy card emulator in proximity of the actual reader
  - Proxy card emulator and proxy reader communicate over an alternative channel (e.g. Bluetooth)

Software card emulation



```
public class CallbackListener
  implements VirtualISO14443Part4TargetCallback
{
  byte[] processCommand(byte[] command)
  {
    byte[] response;

    // process command parameter
    // and generate response

    [...]

    return response;
  }
}
```

- No secure element
- Smartcard commands handled by software on the application processor

Availability of Software Card Emulation

- All BlackBerry NFC mobile phones
- CyanogenMod 9 after-market firmware for Android devices
- Dedicated NFC reader devices (e.g. ACR 122U)
- Dedicated card emulators (Proxmark, …)

Advantages of Software Card Emulation

- Card emulation is often associated with high revenue applications (payment, ticketing, access control)
  - Everyone wants to develop these applications
- BUT:
  - Secure element is under tight control of handset manufacturer/trusted service manager/mobile network operator
  - Competing applications not likely to be allowed to coexist on one secure element
  - High cost to get applications onto a secure element (due to limited space and expensive certification)

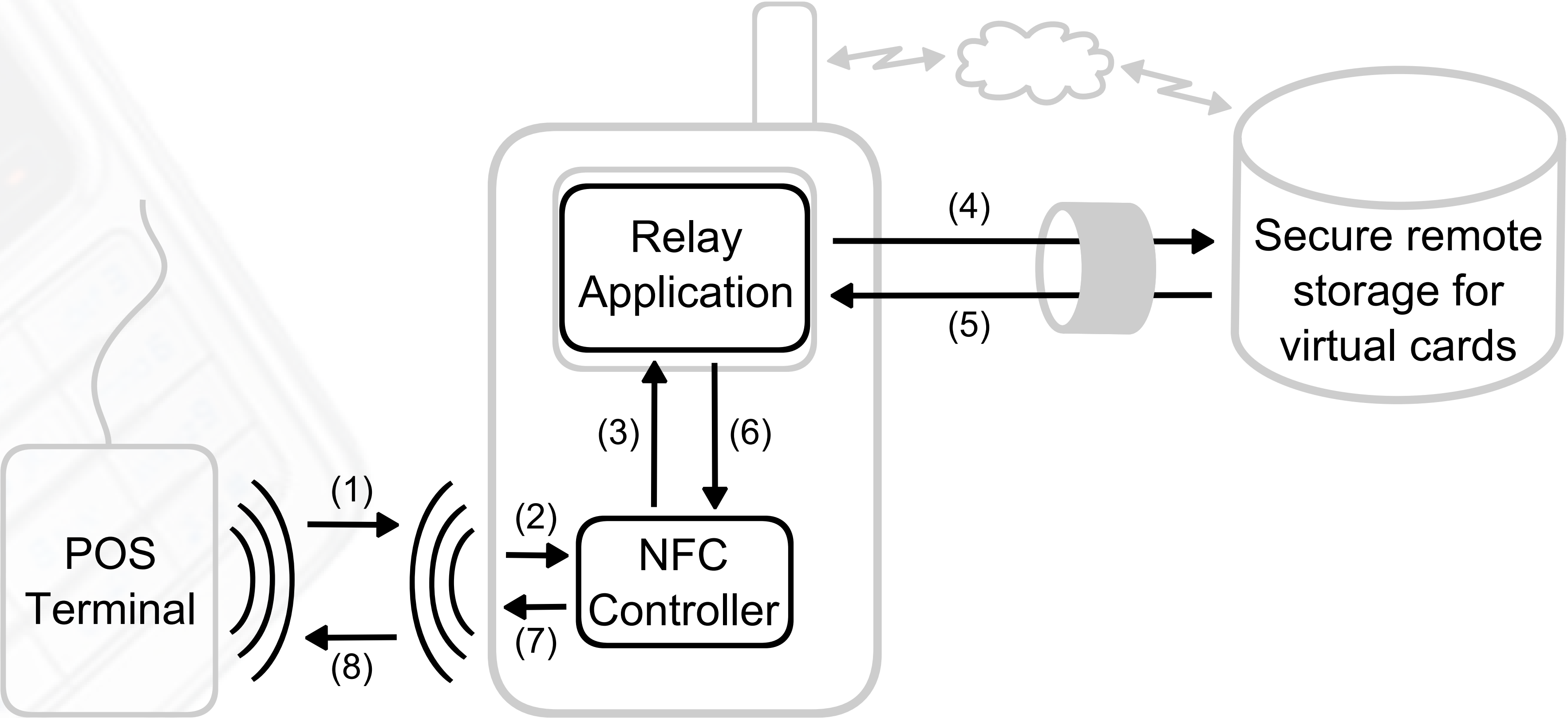
Advantages of Software Card Emulation

- Software card emulation opens card emulation applications to average developers
  - Complex secure element is not needed
- Anybody can develop applications based on existing reader infrastructure
- Software card emulation can be used as an alternative to peer-to-peer mode
  - Peer-to-peer mode is still not (fully) supported by many NFC devices
  - Many smartcard readers for PCs do not support peer-to-peer mode
  - Reader/writer mode is well supported on the PC platform through PC/SC (peer-to-peer mode is not!)
  - Software stack for reader/writer mode is less complex than that of peer-to-peer mode
- Great chance for others than the “big players” to create innovative NFC applications

Disadvantages of Software Card Emulation

- Application processor is less secure than secure element (no secure storage, no trusted execution environment)
  - Difficult to store sensitive data
  - Possible interference by other applications
  - Maybe okay for some applications (e.g. ticketing)
  - Problematic with other applications (e.g. payment, access control)
- Software card emulation devices as attack platform
  - Card emulator for relay attacks
  - Mobile phones have form factor expected for NFC/contactless transactions
  - Mobile phones have network connectivity for the relay channel

Cloud-based Secure Element



Conclusion

- Software card emulation is a great opportunity for developers
  - Breaks the barrier of secure element-based solutions
  - Easy integration into existing contactless smartcard systems
  - Easier to use than peer-to-peer mode
- Significant risk
  - Developers may be lazy with securing their applications and data
  - Devices may be used as platform for relay attacks

NFC
Congress 2012
Hagenberg

September 11th – 12th, 2012
Hagenberg, Austria

http://congress.nfc-research.at/

Thank You!

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

michael.roland (at) fh-hagenberg.at

This work is part of the project “4EMOBILITY” 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).