UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
OBERÖSTERREICH

KONFERENZEN
SEMINARE
IIR
Wissen, das bewegt

Host Card Emulation

Wie sicher ist das Bezahlen ohne Secure Element?

Dr. Michael Roland

IIR Jahresforum Cashless Payments • Wien
28. September 2016

u'smile

This work is funded by the Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH.

Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) • www.usmile.at
A research group of the University of Applied Sciences Upper Austria, Hagenberg Campus

Was leistet NFC im Smartphone?

Reader/Writer Mode

Peer-to-Peer Mode

Card Emulation Mode

Was leistet NFC im Smartphone?

Reader/Writer Mode

Peer-to-Peer Mode

Card Emulation Mode

Bezahlen mit NFC

Transaktionsdaten
- Betrag
- Datum/Uhrzeit
- …

Freigabe

Transaktionsdaten
- Kartendaten

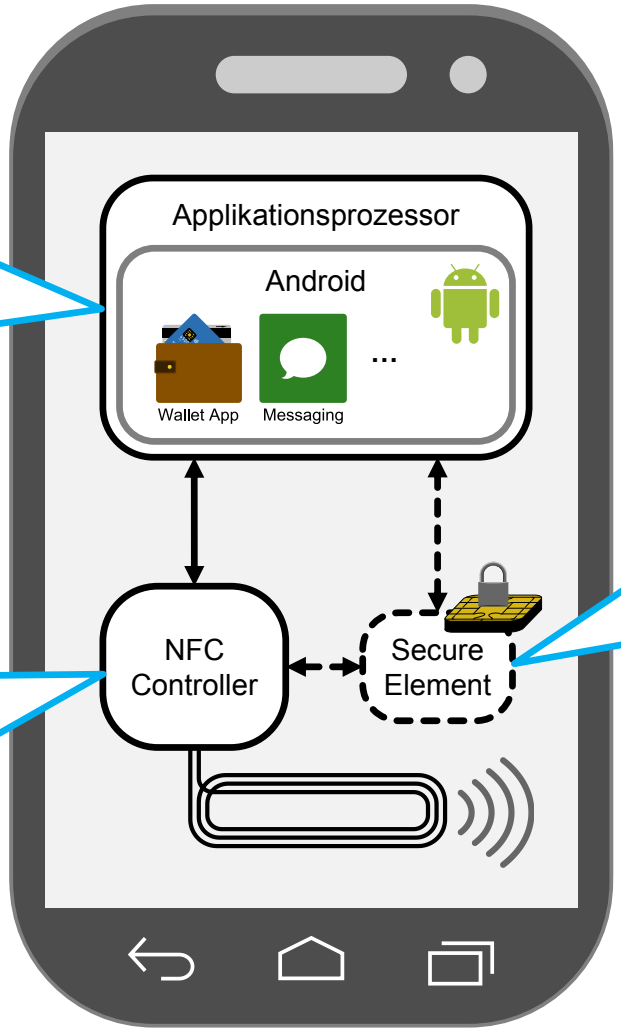
- Signatur

Enthält:

- Kartendaten
  - PAN
  - Ablaufdatum
  - …
- geheimen Schlüssel

Komponenten im Smartphone

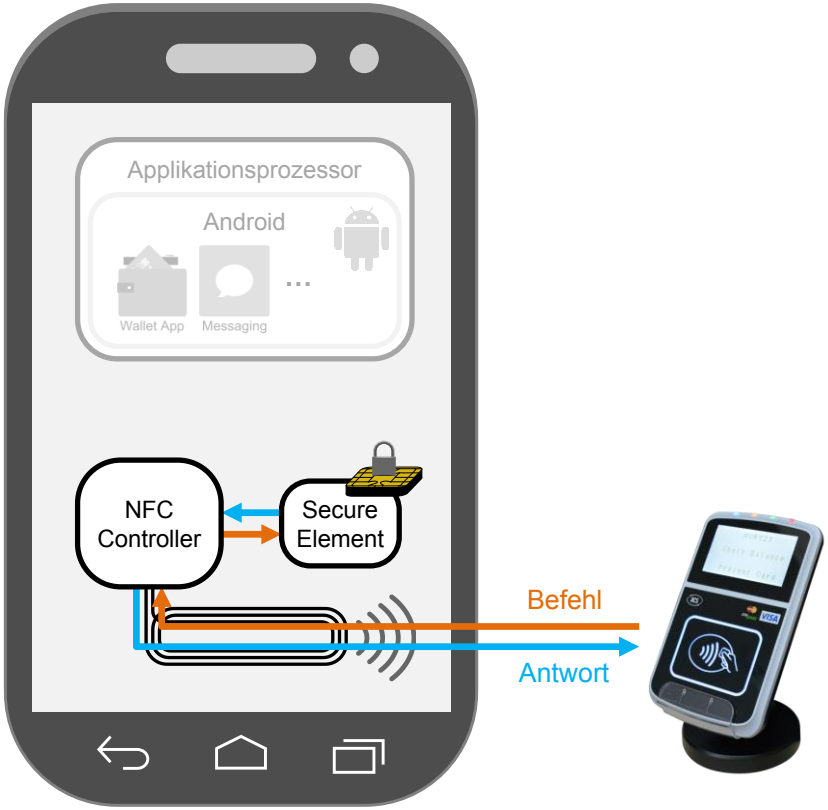
Applikationsprozessor
- Smartphone-OS (z.B. Android)
- Apps



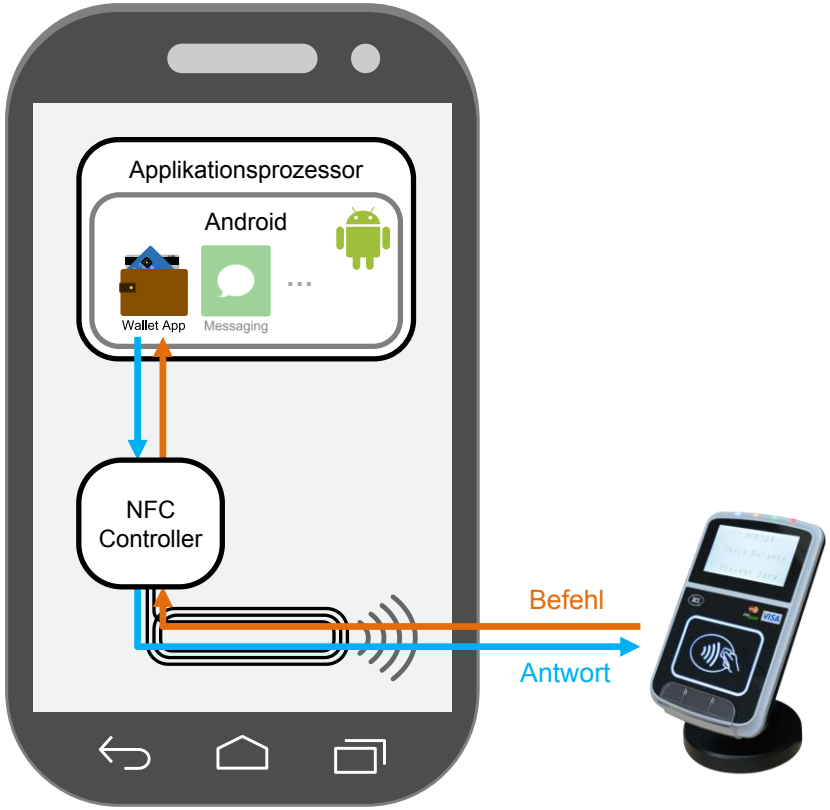
Secure Element
- Smartcard-Chip
- Prozessor und Speicher für sicherheitskritische Applikationen und Daten

NFC-Controller
- Analoges Front-End
- NFC-Modem

Secure Element vs. Host



Secure Element

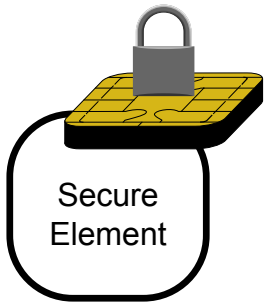


Host Card Emulation

Secure Element

Vorteile

- Geschlossene und streng kontrollierte Umgebung
- Sicheres Betriebssystem
- Sicherer Prozessor und Speicher
- Zertifizierung der Hardware und Software



Nachteile

- Sicherheit hat hohen Preis
- SE ist nicht in jedem Gerät verfügbar

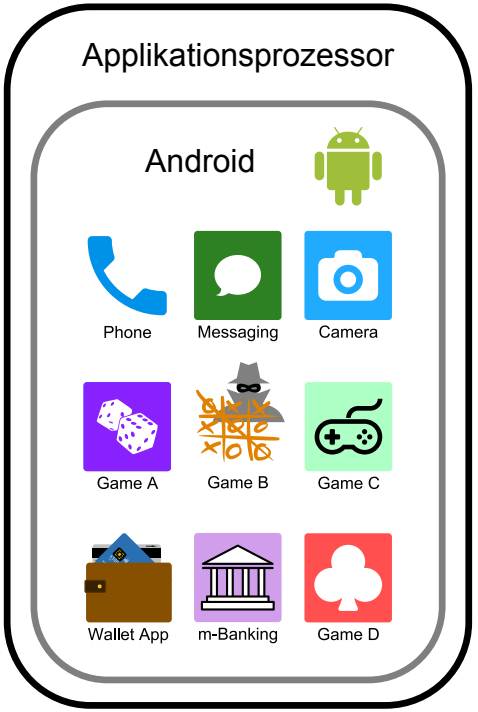
Host Card Emulation

Vorteile

- Offene Umgebung
- Praktisch in jedem aktuellen Android-Gerät verfügbar (wenn NFC vorhanden)

Nachteile

- Offene Umgebung (!)
- Bewusstes Außerkraftsetzen von Schutzmechanismen durch Benutzer
- Komplexes Betriebssystem
- Hardware kaum gegen physische Angriffe geschützt



„Pure“ HCE

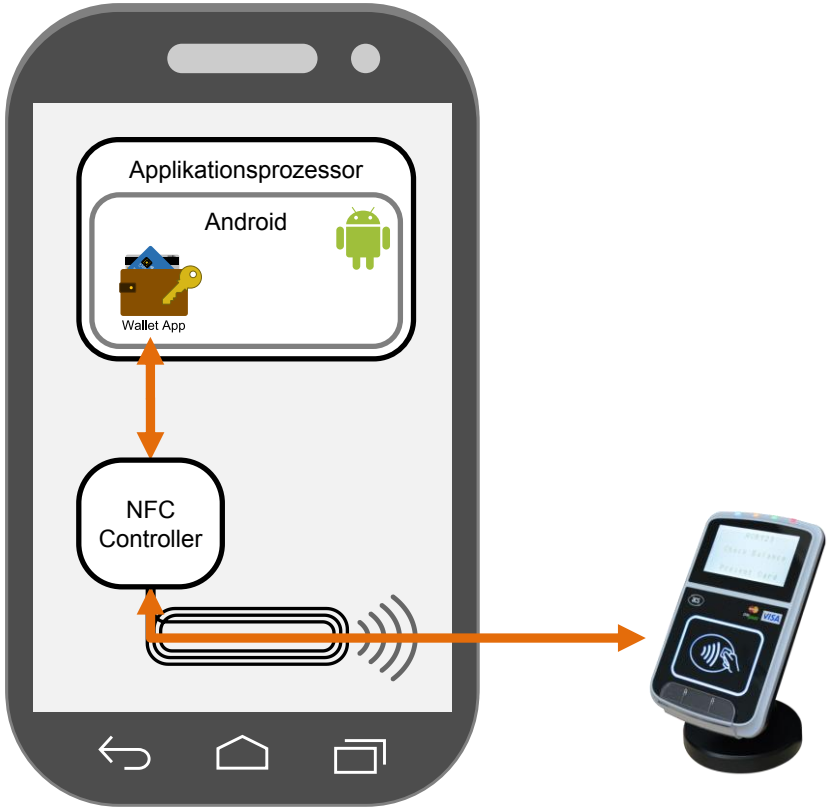
- Smartcard-Applikation 1:1 als HCE-App umgesetzt

Vorteile

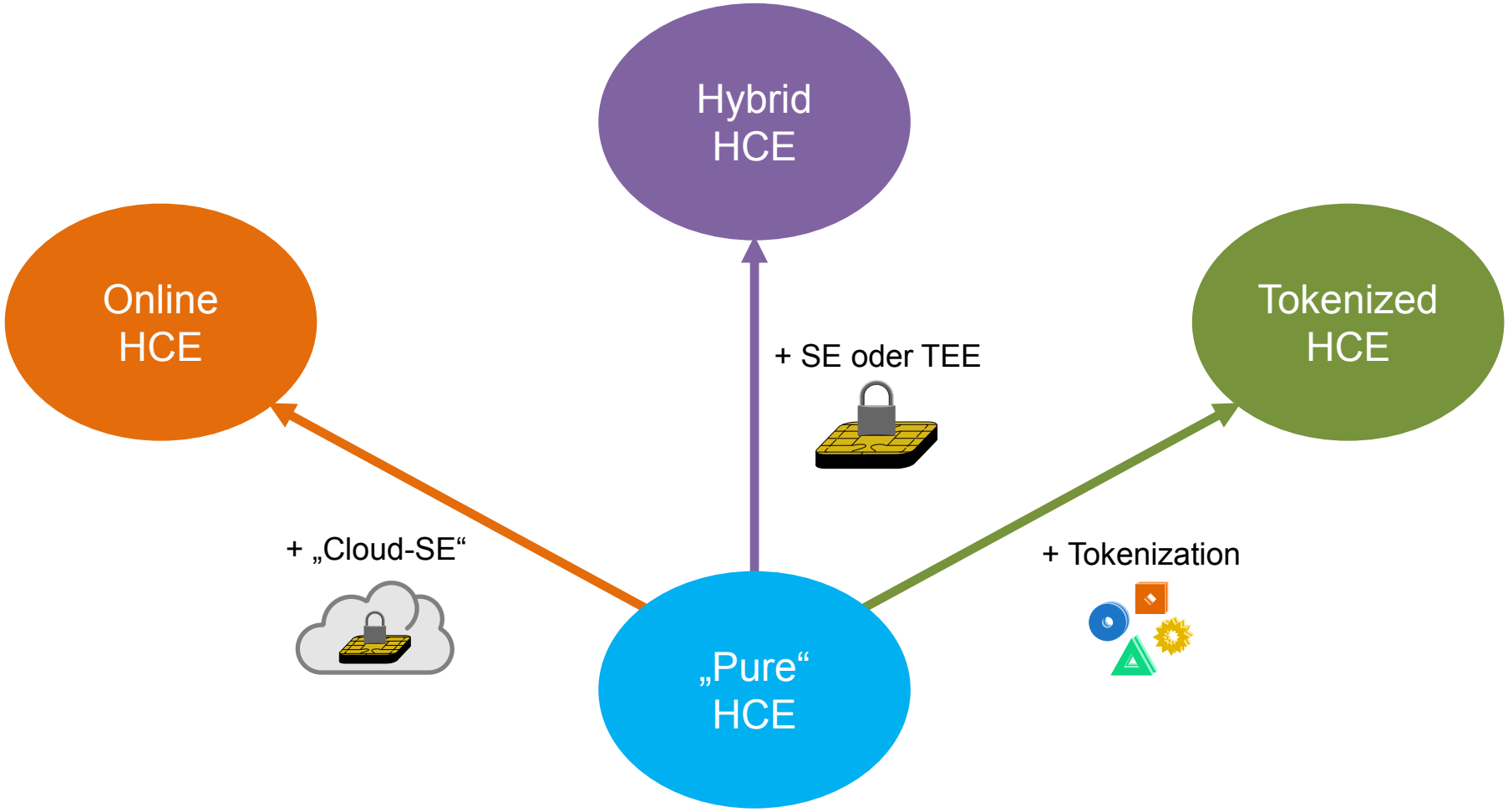
- Offline verwendbar
- Einfach zu implementieren

Probleme

- Kartendaten und Schlüssel in unsicherem Speicher
- Daten einfach kopierbar
- Kartenduplikate uneingeschränkt nutzbar



Strategien für mehr Sicherheit



Online HCE

- HCE-App leitet Kommunikation direkt in die Cloud weiter

Vorteile

- Kartendaten und Schlüssel nicht am Smartphone gespeichert (kein Zugriff durch andere Apps)

Probleme

- Nur online verwendbar
- Ev. lange NFC-Interaktion
- Verbindung zwischen HCE-App und Cloud-SE: Absicherung problematisch

Hybrid HCE

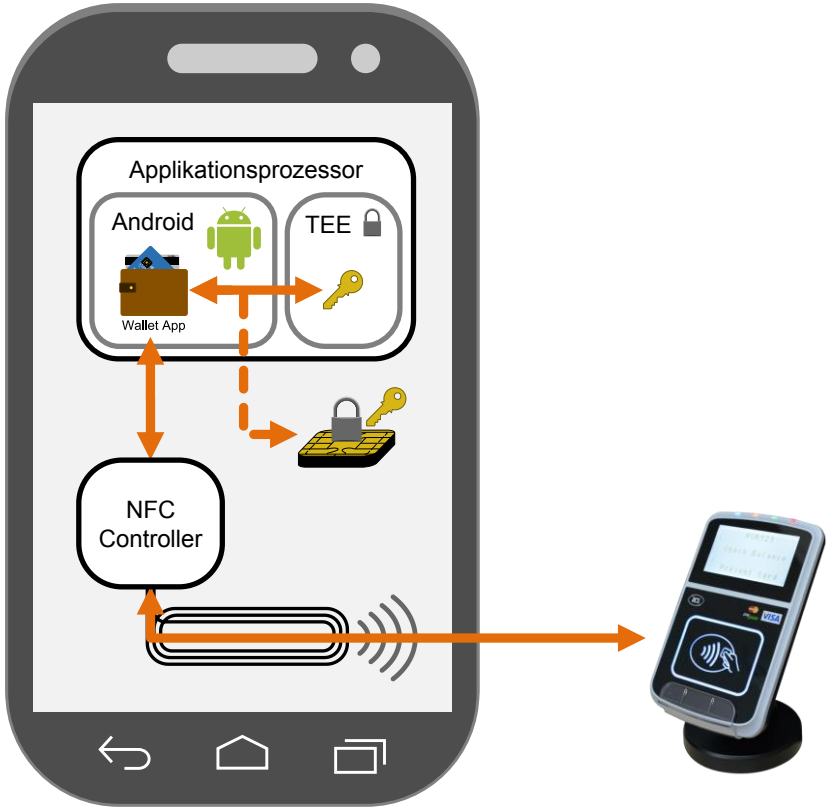
- HCE-App nutzt sicheren Schlüsselspeicher am Smartphone

Vorteile

- Offline verwendbar
- Schlüssel nicht durch andere Apps kopierbar

Probleme

- Geeigneter Schlüsselspeicher notwendig
- SE: Komplexität, Verfügbarkeit
- TEE: geringeres Schutzniveau
- Verwendung von Schlüsselspeicher durch andere Apps



Tokenized HCE

- Kurzlebige Token statt regulärer Kartendaten/Schlüssel
- Online-Phasen: HCE-App lädt begrenzte Anzahl an Token

Vorteile

- (begrenzt) offline verwendbar
- Sehr begrenzte Gültigkeit der Schlüssel im unsicheren Speicher

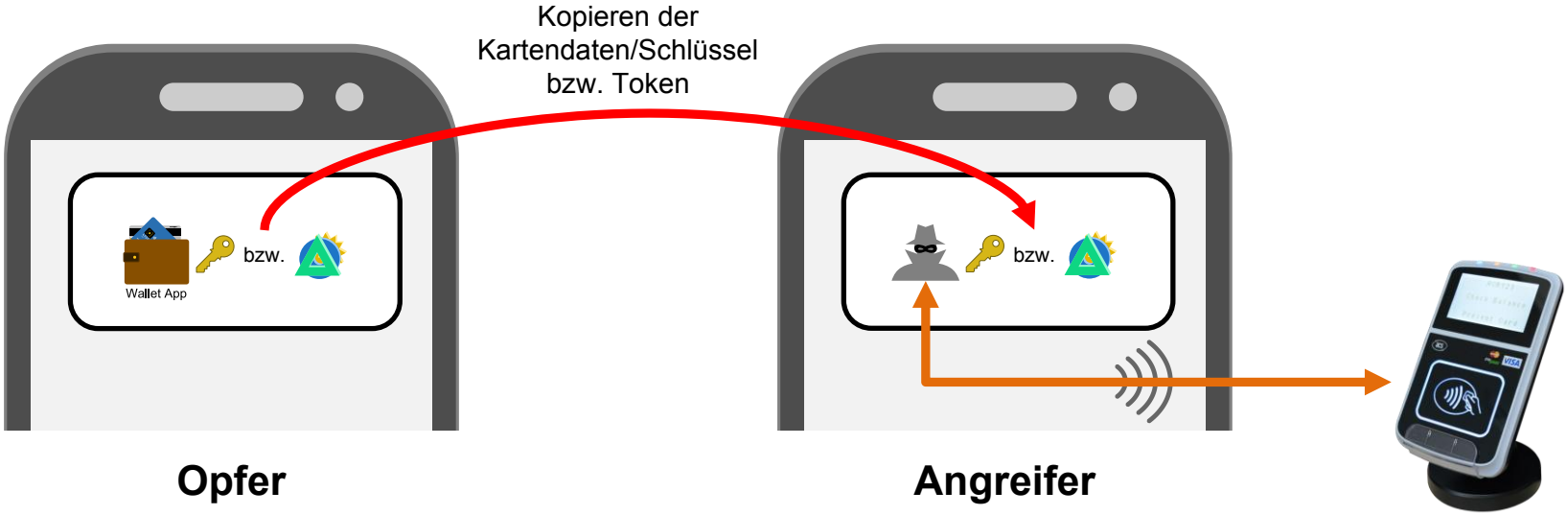
Probleme

- Verbrauch/Ablauf der Token
- Token in unsicherem Speicher
- Verbindung zwischen HCE-App und Token Provider: Absicherung problematisch

Angriffsszenario
Skimming

- Kopieren der für den Bezahlvorgang relevanten Daten auf ein anderes Gerät (oder eine Smartcard)
- Zugriff auf Daten des Wallet notwendig
  - Lokaler Angreifer (ev. auch Benutzer selbst)
  - Entfernter Angreifer mittels App (& Privilege Escalation)
- Bei Tokenization:
  - Kopierte Daten nur sehr begrenzt nutzbar

	Risiko	Nutzen
„Pure“ HCE	♦♦♦♦	♦♦♦♦♦
Online HCE	*nicht anwendbar*	
Hybrid HCE	♦♦	♦♦♦♦♦
Tokenized HCE	♦♦♦♦	♦♦♦
Secure Element	♦	♦♦♦♦♦

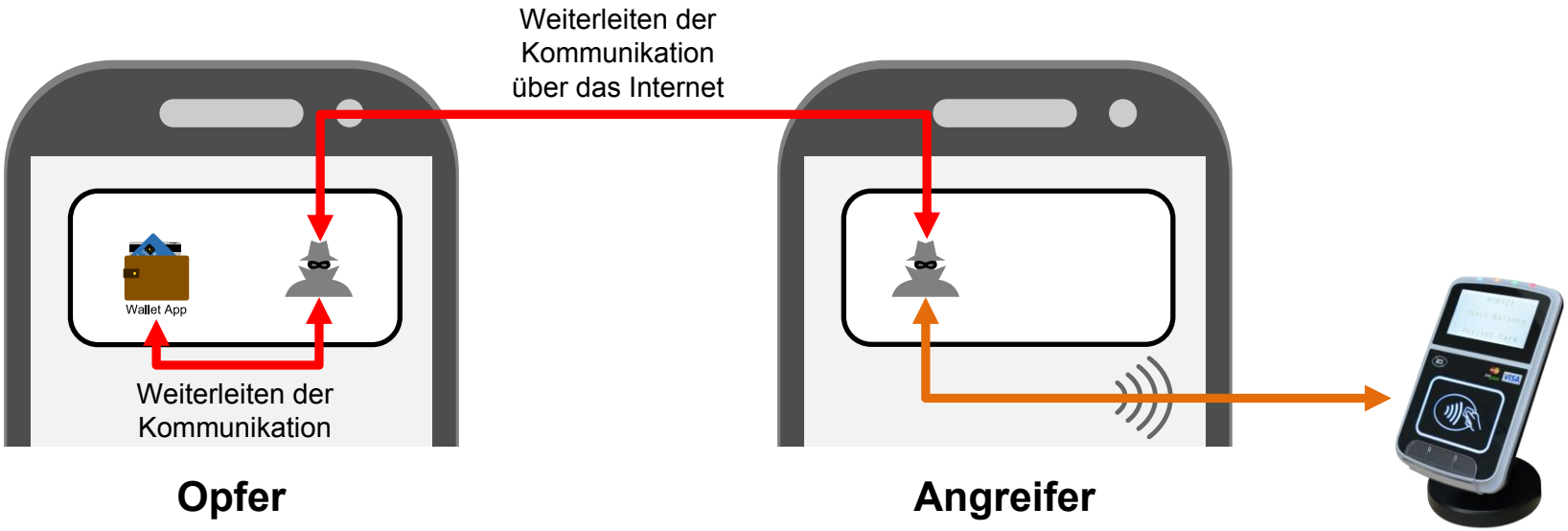


Angriffsszenario

Software-based Relay zu Wallet-App

- Weiterleiten der NFC-Kommunikation zur Wallet-App am Gerät des Opfers
- App am Gerät des Opfers notwendig
- Während Bezahlvorgang: Verbindung zwischen Angreifer- und Opfer-Gerät notwendig
- Android schützt HCE-Apps gegen diesen Angriff
  - Privilege Escalation könnte Schutz aushebeln

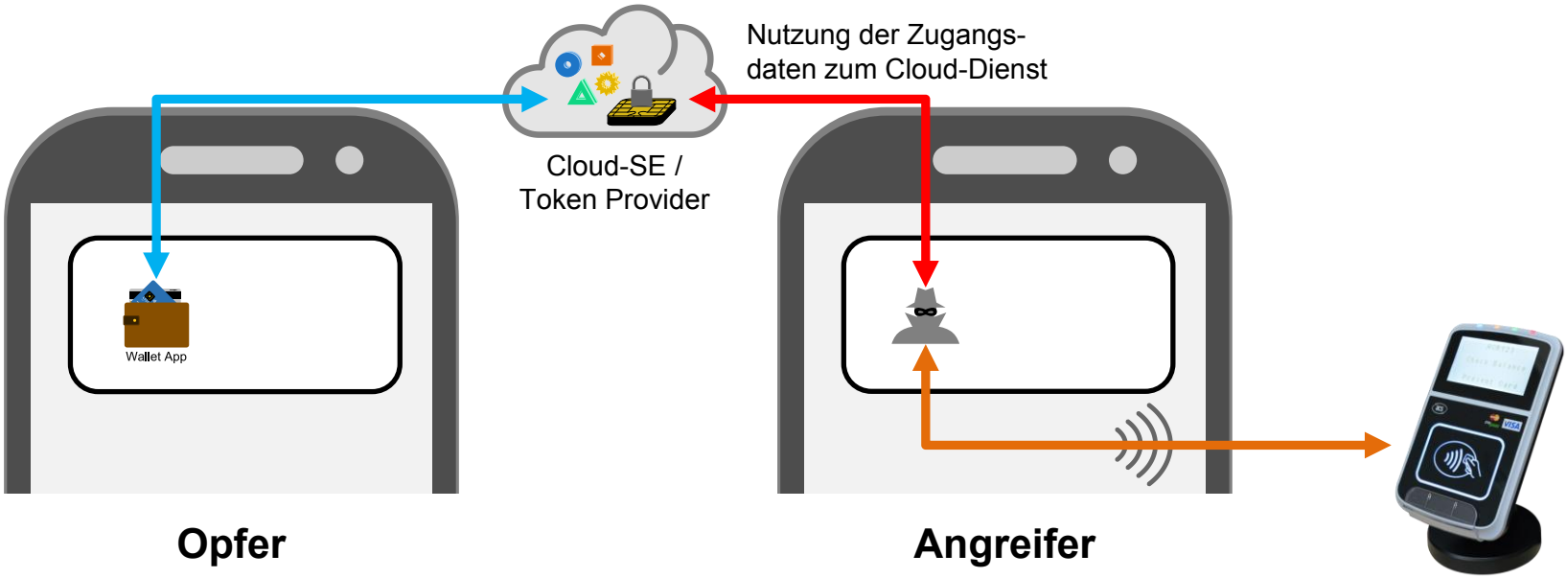
	Risiko	Nutzen
„Pure“ HCE	♦♦♦♦	♦♦♦
Online HCE	♦♦♦♦	♦♦♦
Hybrid HCE	♦♦♦♦	♦♦♦
Tokenized HCE	♦♦♦♦	♦♦♦
Secure Element (direkt zum SE statt zur App)	♦♦♦♦	–



Software-based Relay zu Cloud-Dienst

- Nutzung des Cloud-Dienstes über anderes Gerät
- Zugangsdaten zum Cloud-Dienst notwendig
  - z.B. aus Datenspeicher der Wallet-App
  - Lokaler Angreifer (ev. auch Benutzer selbst)
  - Entfernter Angreifer mittels App (Privilege Escalation)
- Schutzmaßnahmen beim Cloud-Dienst möglich
  - z.B. Erkennung mehrerer gleichzeitiger Verbindungen

	Risiko	Nutzen
„Pure“ HCE	*nicht anwendbar*	
Online HCE	♦♦♦	♦♦♦♦
Hybrid HCE	*nicht anwendbar*	
Tokenized HCE	♦♦♦	♦♦♦
Secure Element	*nicht anwendbar*	



Strategien für noch mehr Sicherheit?

Verschleierung der Funktionsweise des Programmcodes

- Problem:
  - Android-Apps relativ einfach in Java-Code rückübersetzbar
  - statische Code-Analyse und Reverse Engineering
- Techniken:
  - **Code Obfuscation / Code „Encryption“**
  - Ausweichen auf **Native Code**
    - Werkzeuge und Bedienung einfach nur teurer und komplexer
    - Verlust impliziter Sicherheitsmaßnahmen bei Speicherzugriffen von Java
  - **White-Box Cryptography**
    - Eigentlich: nicht „Kryptographie“ sondern Steganographie (bzw. Verschleierung)
- Aber:
  - Nur Verschleierung, kein wirklich wirksamer Schutz

Strategien für noch mehr Sicherheit?

Erkennung unerwünschter Geräteeigenschaften

- Probleme:
  - Bekannte Bedrohungen
  - Bewusstes Aushebeln von Sicherheitsmechanismen durch Benutzer
  - Kopieren von Daten auf andere Geräte
- Techniken:
  - **Device Fingerprinting**
  - **Root Detection**
  - **Debug Detection**
- Aber:
  - Nur bekannte(!) Muster können auch erkannt werden
  - Wer das gesamte System kontrolliert kann auch verhindern, dass er erkannt wird

Dr. Michael Roland

Research Associate
Josef Ressel Center u'smile and Research Group Embedded Systems
University of Applied Sciences Upper Austria

michael.roland (at) fh-hagenberg.at

u'smile

Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile) • www.usmile.at
A research group of the University of Applied Sciences Upper Austria, Hagenberg Campus