RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

NFC, Contactless, and Mobile: A Security Analysis

Speaker：Hadi Nahari

Job Title：Principal Mobile &Security Architect

Company Name：PayPal

Intro

- **Devices have changed… just a little bit**

1956, a 5 MB HDD by IBM

2011, Kindle Fire by Amazon

Hadi’s Background

- **Author of “Web Commerce Security: Design and Development” book, published by John Wiley & Sons.**
- **Security, Cryptography, Complex System Analysis Identity Management, Asset Protection, Information Assurance Schemes**
- **Massively Scalable Systems design, implementation, and governance Vulnerability Assessment, Threat Analysis (VATA)**
- **Theory of Programming Languages, Formal Languages, Functional Languages, Semantics of Security**
- **Enterprise & Embedded (Netscape, Sun Microsystems, United States Government, Motorola, eBay, PayPal,…)**

Agenda

- **NFC**
- **Mobile**
- **Mobile + NFC**
- **Conclusion, Q&A**

Contactless & NFC

- **NFC: Near Field Communication**
- **NFC is a short-range wireless technology that allows devices to exchange information when *tapped* together**
- **NFC is a subset of *Contactless***
  - **Bluetooth, Wi-Fi, & ZigBee are other examples**

NFC modes

- **Tag/Sticker (or read/write)**
  - **Non-secure, reading smart tags**

- **Peer-To-Peer**
  - **Non-secure, device to device**

- **Card Emulation**
  - **Secure via “Secure Element”**

Secure Element

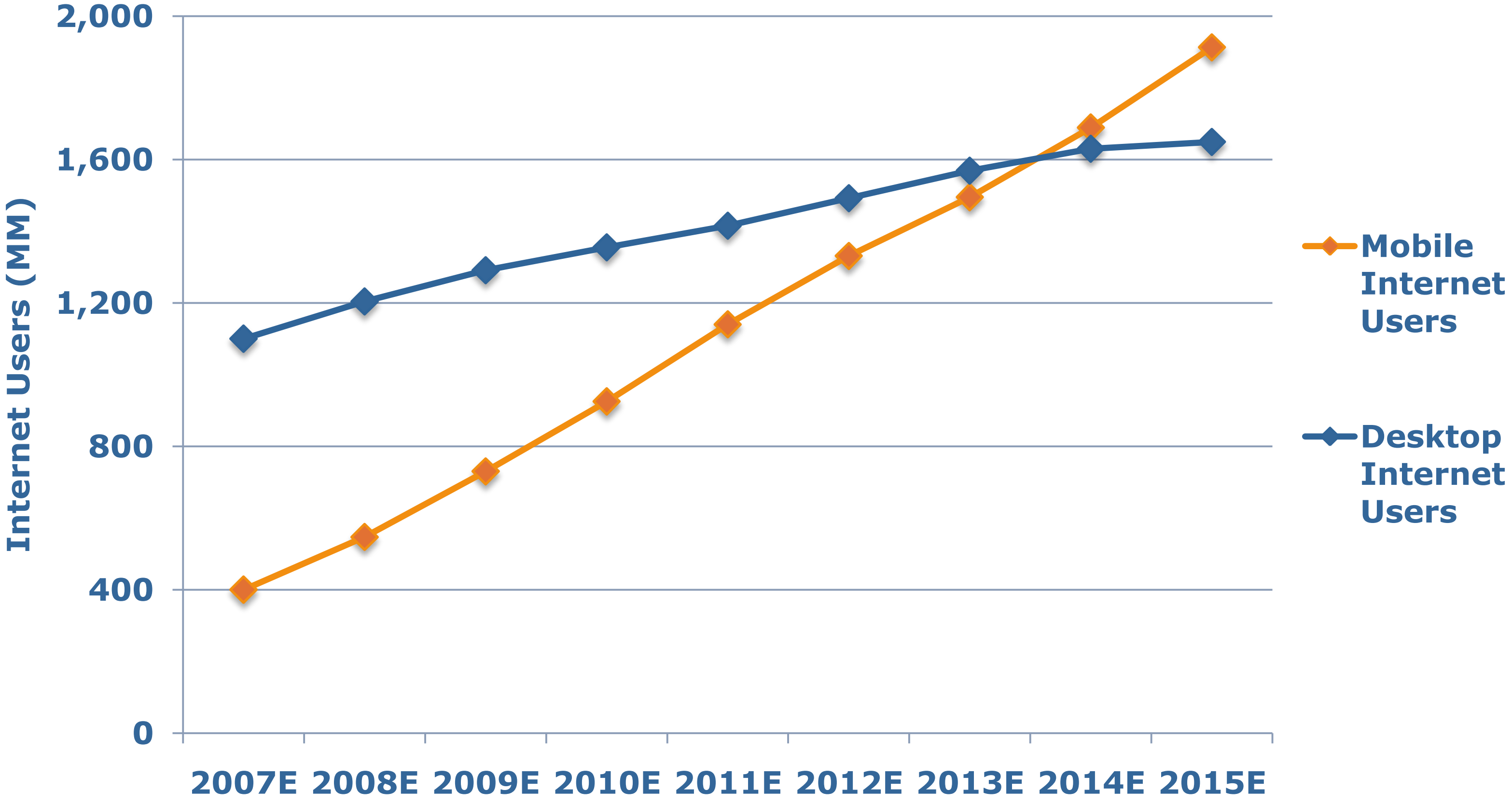
- **Secure Element (SE) is a hardware device that protects key material**
- **May or may not include crypto engine**
- **Different SE types:**
  - **USIM/UICC**
  - **Embedded SE (eSE)**
  - **microSD**
  - **TPM**
  - **MTM**

NFC Phone ←→ POS

- **Point Of Sale (POS) devices operate in CE mode***
- **In CE, NFC device and POS mutually authenticate each other**
- **SE is *required* in an NFC-mobile phone**
- **Solutions with no SE:**
  - **Higher risk**
  - **Increased fraud**
- **Why does Mobile+NFC matter?**

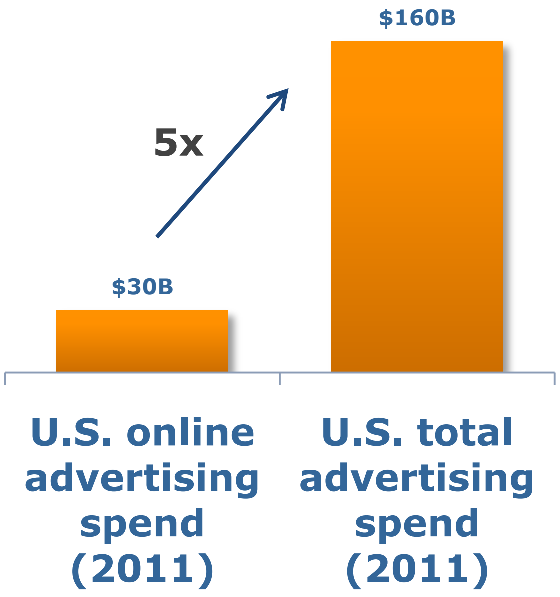
Mobile: Usage

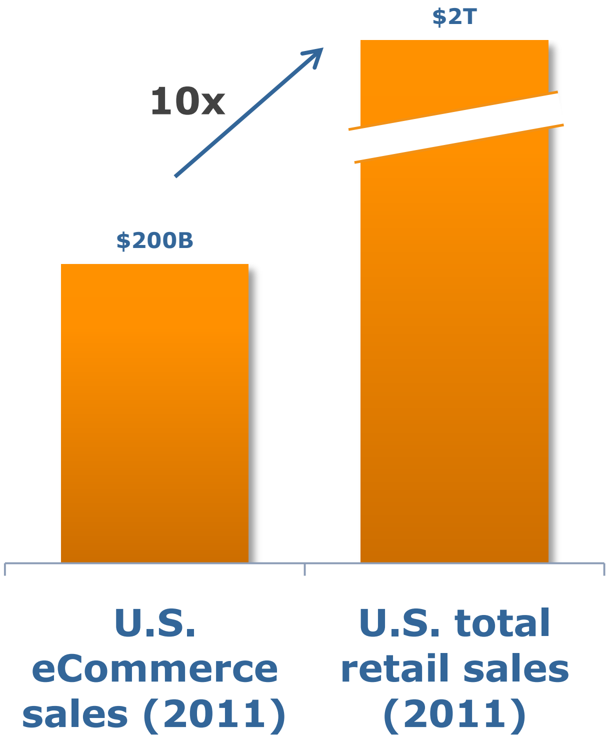
Global Mobile vs. Desktop Internet User Projection, 2007 – 2015E



Source: http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/

Mobile: Growth





Source: Forrester Research; eMarketer

Mobile matters to NFC

- **Ok, mobile+NFC is important**
- **How to integrate NFC into mobile?**
  - **Where should the surgery be made?**
- **Which stack matters the most?**

Mobile: Which Stack?

- **3 month average ending in July 2011**
- **Mobile subscribers age 13+**

Smartphone Platform	**Share (%) of EU5 Smartphone Users**		
	Jul-10	**Jul-11**	**Point Change**
Total Smartphone Users	*100.00%*	*100.0%*	*0.0*
Symbian	53.9%	37.8%	-16.1
Google	6.0%	22.3%	16.2
Apple	19.0%	20.3%	1.2
RIM	8.0%	9.4%	1.5
Microsoft	11.5%	6.7%	-4.8

**MobiLens measures users above the age of 13 and reports on only primary handset usage*

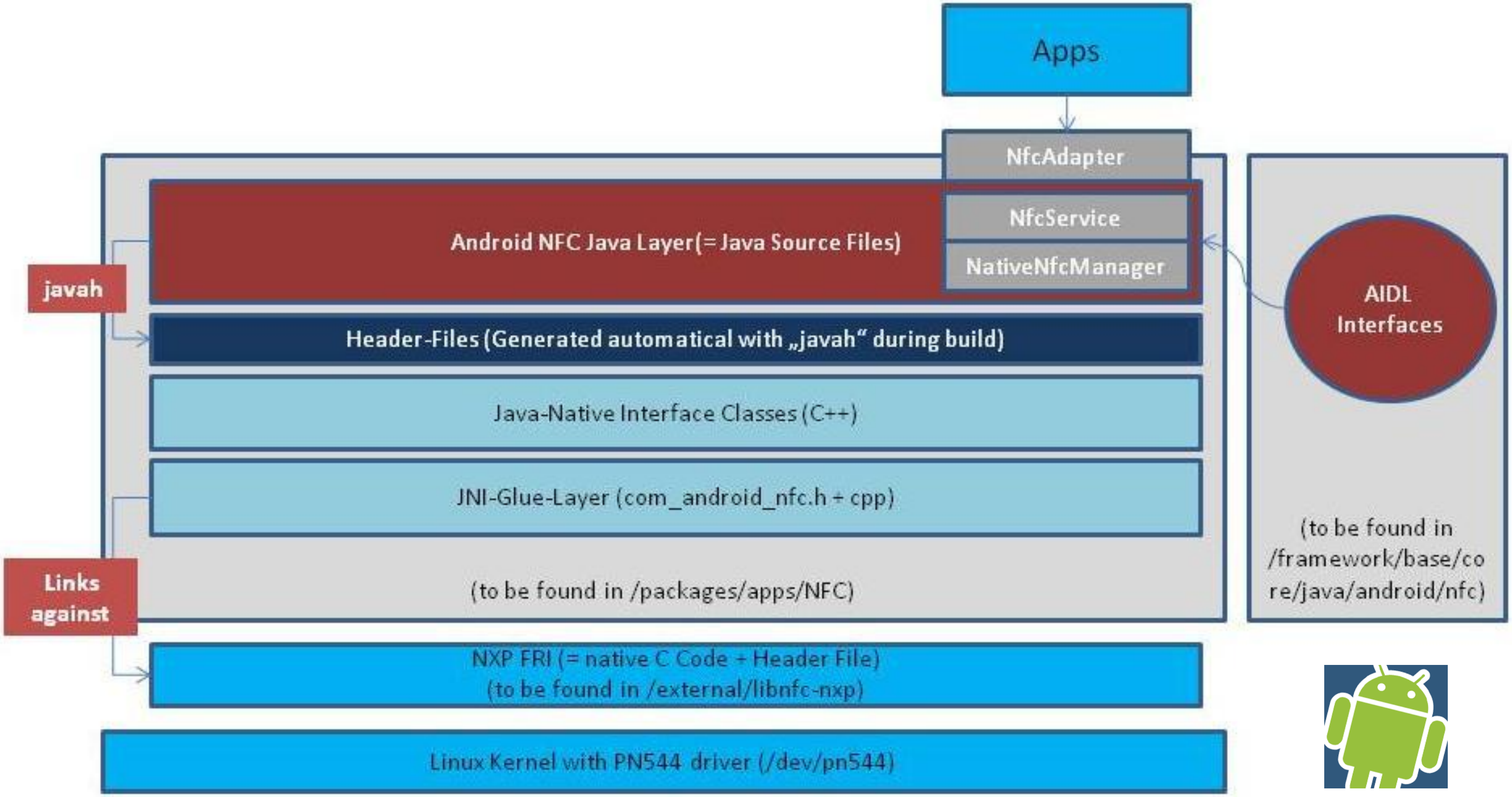
Source: comScore Mobile

Android + NFC

- **Well, Android is not *exactly* the most secure OS**
  - **In fact, Android is hackers' heaven…**
  - **…and our job-security**
- **Thus exposing NFC functionality to Android should be done carefully**
  - **"CIA agent in KGB domain" paradox**
- **Some integration *glue* is needed**
  - **Both in Java & native layers**

Stack Integration

- **How NFC is *Glued* into Android**



Apps

NfcAdapter

NfcService

NativeNfcManager

Android NFC Java Layer(=Java Source Files)

javah

Header-Files (Generated automatical with „javah“ during build)

Java-Native Interface Classes (C++)

JNI-Glue-Layer (com_android_nfc.h + cpp)

Links against

(to be found in /packages/apps/NFC)

AIDL Interfaces

(to be found in /framework/base/core/java/android/nfc)

NXP FRI (= native C Code + Header File)
(to be found in /external/libnfc-nxp)

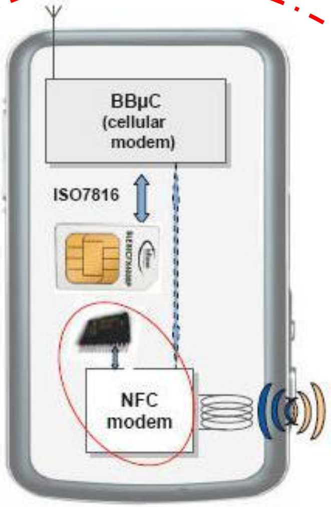
Linux Kernel with PN544 driver (/dev/pn544)

What about SE??

- **Don’t worry: we still need SE**
- **Two* main SE use cases**
  - **Embedded SE (eSE)**
  - **UICC/SIM as SE**
  - ***the other use cases are less prevalent**

Two* Main Cases

GOOGLE WALLET APPROACH



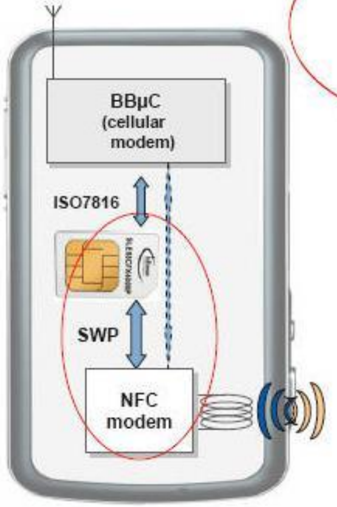
Handset Manufacturer - Centric Approach

– Secure Element = a device in the handset so called "**SE-NFC** "

– Security: in the SE (device-oriented)

EMBEDDED SE

NFC device
=
Secure Element
+
NFC modem



Mobile Network Operator – Centric Approach

– Secure Element = SIM so called "**SIM-NFC**"

– Download of credentials via the network (from MNO or 3rd party)

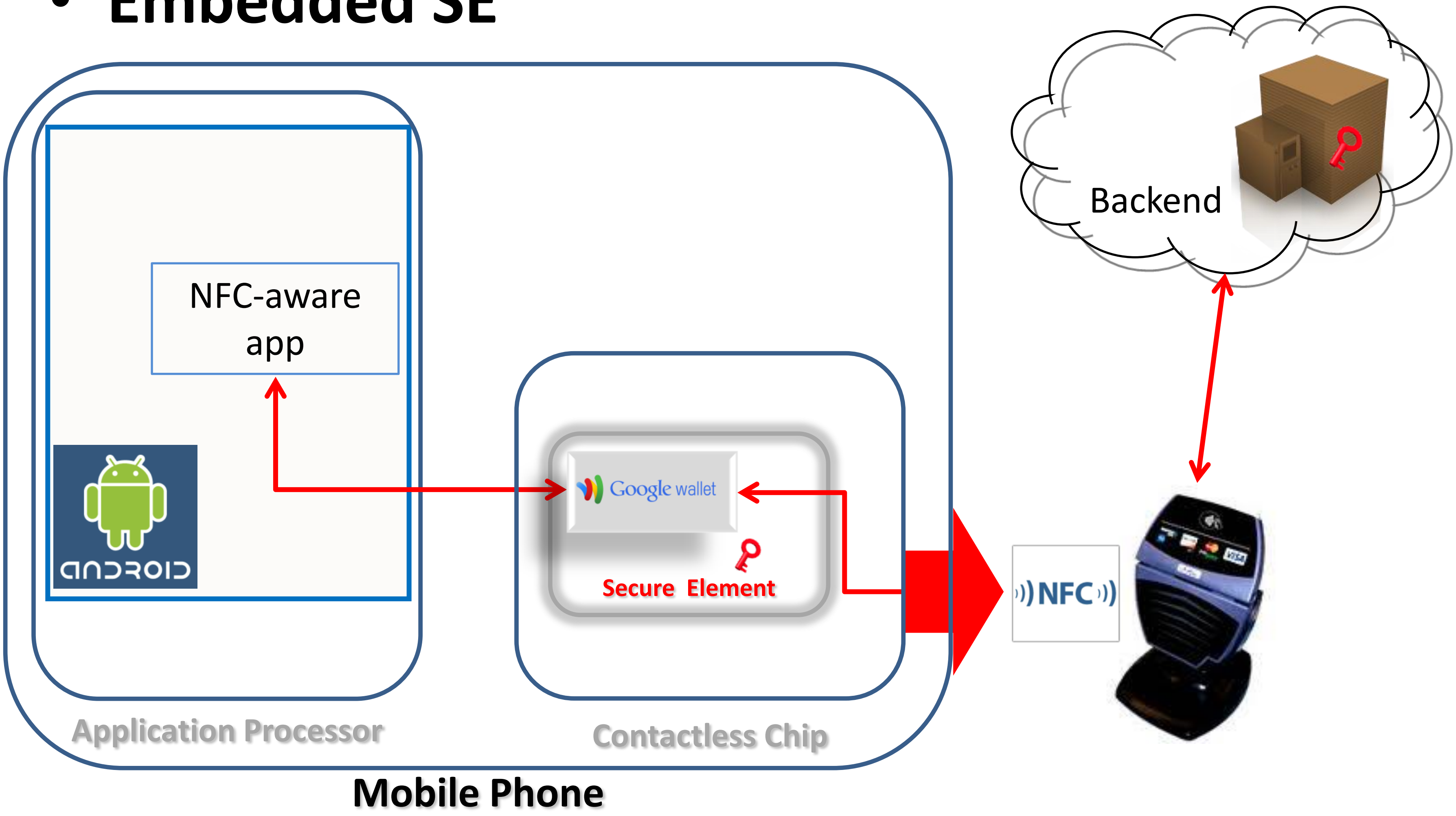
– Security: in the SIM (user-oriented, removable)

– The SIM can also support DRM, Mobile TV access rights

UICC-BASED SE

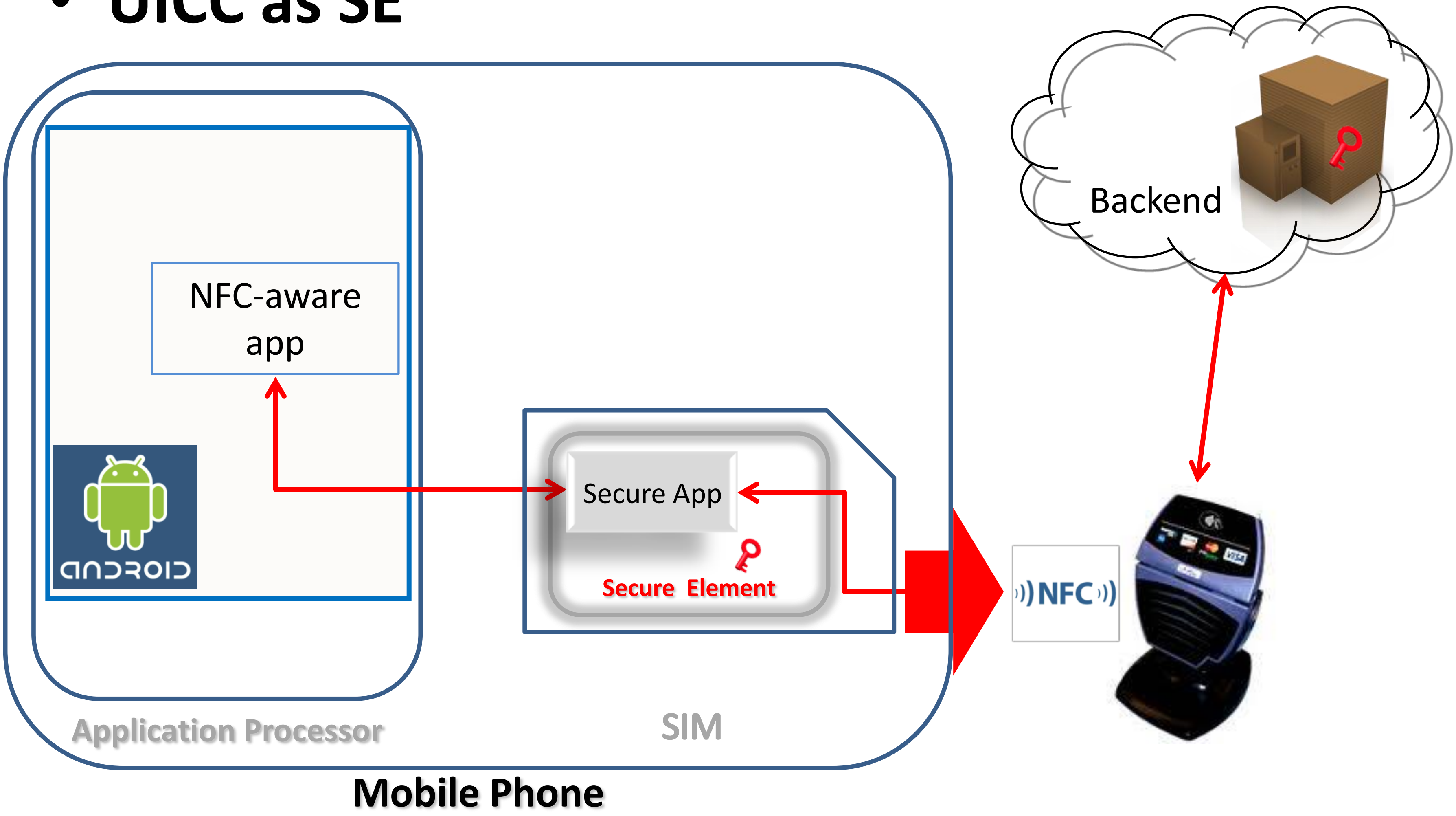
Mobile+NFC: Case I

- **Embedded SE**



Mobile+NFC: Case II

- **UICC as SE**

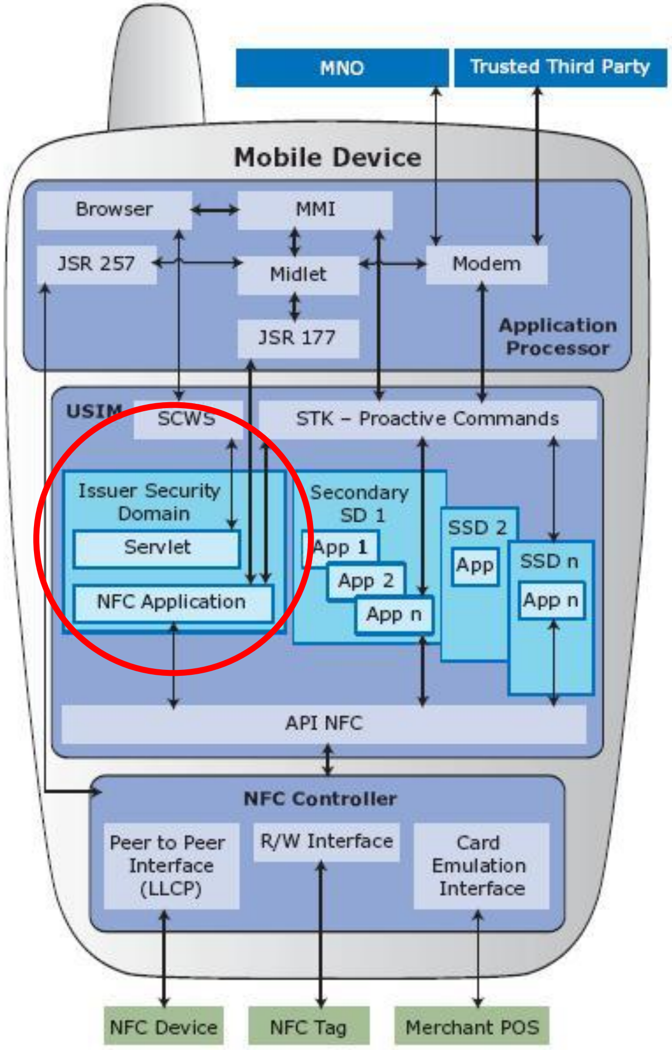


Who does what

- **Android holds the high-level app**
- **SE holds the secure app**
  - **establishes secure NFC channel**
- **Isolation at hardware layer**
- **There is more within SE and its apps**
  - **ISD: Issuer Security Domain**
  - **SSD: Secondary Security Domain**
  - **…**

Inside SE

- **Issuer Security Domain (ISD)**
  - **ISD has the highest privilege**
  - **Can enable/disable other SDs**
  - **Is invoked first in CE mode**
  - **All this is outside "Android"**

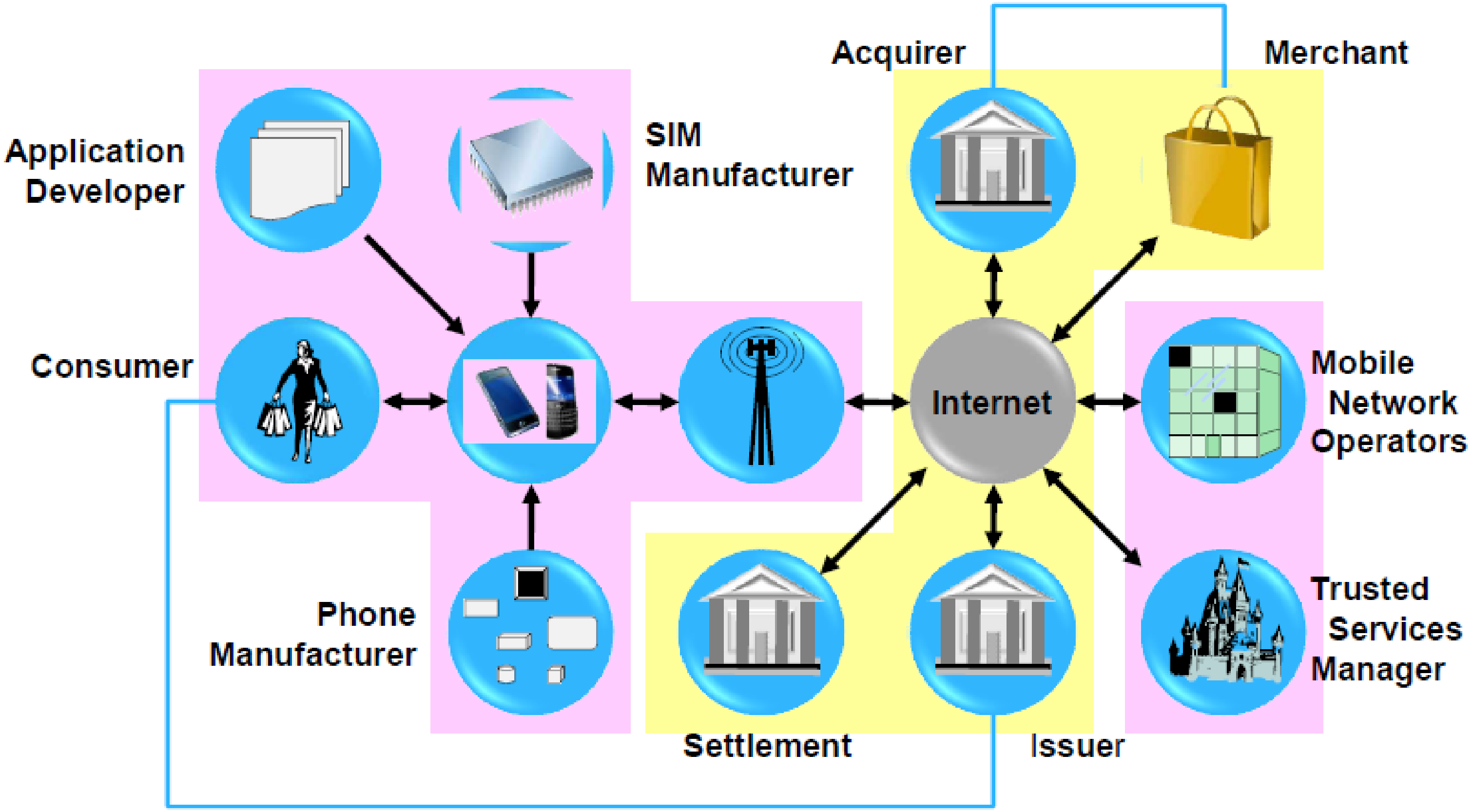


The rest of *Mobile*

- **There’s more to mobile+NFC than just the handheld device**
- **Very complex, busy ecosystem**
- **Many, many players from cradle to grave**
- **Ecosystem still undergoing changes**

Ecosystem

- **Complexity = security's worst enemy**



🟪 Mobile Fraud Risk: new environments & entities

🟨 Financial Fraud Risk: legacy environments & entities

▬ Legacy payments relationships

Source: Federal Reserve, "The Case for Mobile Payments in the US", April 2011

Observation #1

- **Without a footprint in SE, even a privileged access to Android core won’t help, because:**
  - **Card Emulation mode cannot be enabled (readers/POS require this mode)**
- **Therefore Android apps are left with P2P or tag/sticker modes:**
  - **neither is suitable for security-sensitive ops**

Observation #2

- **It is very likely that Android applications will remain un-secure, because:**
  - **It’s unlikely that Android will ever give applications any access to Secure Element**

Observation #3

- **UICC/SIM is still the most prevalent SE**
- **But this is quickly changing:**
  - **eSE, µSD, TrustZone, TEE, TPM, MTM, Secure µKernel, …**

Observation #4

- **Unsolved or unclear use cases:**
  - **Multiple SE in the same device**
  - **Multiple Trusted Service Manager (TSM)**
  - **Device-to-human identity binding**
  - **Roles of ecosystem participants**

Final thoughts

- **It’s no longer sufficient to rely *only* on the device: Backend risk mitigation, fraud detection and prevention is necessary**
- **Adaptive, extensible risk mitigation infrastructure that works with device-based security is required**
- **Collaboration among ecosystem participants is critical: the most effective and efficient risk mitigation and fraud prevention models are collaborative**

Thank You

- **Q&A**

- Standard Rates:
  - Answers: $1
  - Correct answers: $3
  - Correct answers requiring thought: $5

- **Contact:**
  - **www.linkedin.com/in/hadinahari**