APPLICATION PROGRAMMING: MOBILE COMPUTING [INEA00112W]

Marek Piasecki PhD

Mobile Security (W13/2013)

Choose yourself and new technologies

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

Wrocław University of Technology

EUROPEAN SOCIAL FUND

Project co-financed from the EU European Social Fund

Security for Mobile Computing

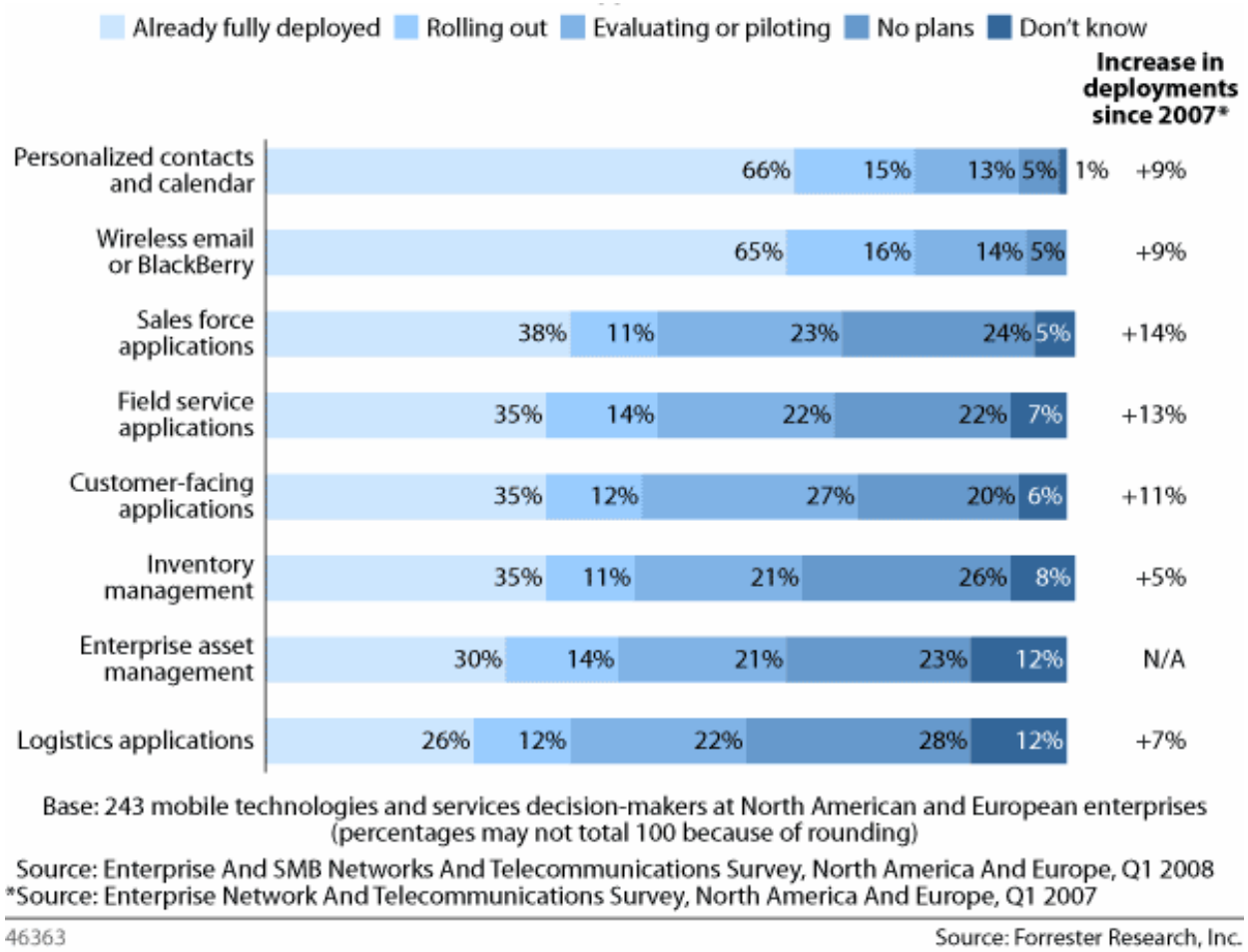
- Security is an important concern over mobile applications where devices are **used in more open environments**.
- Desktop solutions for authentication and authorization, that require **complex interaction** with remote services, usually cause a **critical overhead** to mobile users.
- Standard security techniques: **doors/guards/locks** adequate for workstations,
  are **unsuitable** for mobile/pocket devices
- Real possibility of Data/**Device loss or theft** !

Reality [2009/2010]

- More than **250,000** handheld devices are **left** at U.S. airports every year
- About **100,000** devices are **found** each year in the London Underground
- **30%** of mobile devices are **lost** every year
- At least **25%** of all mobile devices in an organization carry **mission-critical information**
- The number of enterprise **mobile users** will increase to over **269 million** by 2010

Mobile Application Adoption

(North American & European Enterprises 2007/08)



Threats to Mobile Devices

- Device loss or theft
- Data theft
- Mobile malware
- SMS spam

An Irresistible Temptation

- Widely used, lots of users
  (increasing number of potential victims)
- Increasingly used for payments
- Store private/confidential data
- Broad interconnectivity
- Low user-awareness of mobile threats

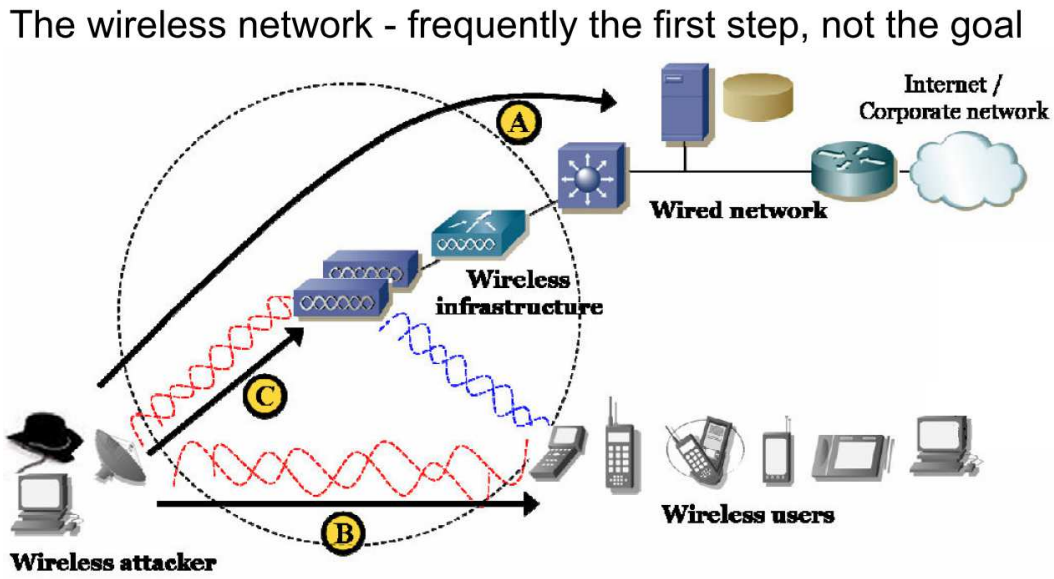
Wireless Attack Scenario

Attack at:

A. wired network using the wireless network as a medium

B. wireless users using the wireless network as a medium; the user may or may not be connected

C. wireless network infrastructure using rogue access point or wireless controllers



Classical Wireless Vulnerabilities

- Password-guessing
  (e.g. user name: Admin; password: Password)
- Wireless Network Encryption: WEP (under 3 min to crack)
- Media access control (MAC) address spoofing
- Threats & attack sophistication is evolving
- Bluesnarfing - the theft of information through a Bluetooth connection.
- Attacker can leave no evidence when accessing a mobile device
- Device drivers - a primary source of security holes in modern OS

New Security Challenges

- Wireless networks are more susceptible to hackers/crackers
- RF signals allow for more attempts at unauthorized access
- New viruses can throw off antivirus software
- Massive increase in bandwidth from data services
- Signaling protocols for wireless networks - key communications target for attacks
- Need for a rich ecosystem of technologies and vendors with 4G
- Attacks include rogue access points

Increase of Mobile Threat

Year	Spam	Threats	Solutions
2005	<1%	Mass texting	Closed network
2006	5-10%	Contest scams Toll calls Premium rate numbers	Protocol filter Handset policies Internet gateway
2007	10-20%	SMS Spoofing SMS Faking SMS Flooding Increase in MMS Viruses	Anti-Spoofing Anti-Faking Anti-Flooding Handset Security
2008	30-50%	On Network Attacks Stock Scams	Fingerprinting Content analysis Distributed network intelligence
Future	>75%	Zombies & Bots Spyware	Fingerprinting Content analysis Distributed network intelligence

Securing Wireless Network

- Encrypt your communication over the network
- Install anti-virus, and firewall software
- Stop identifier broadcasting mechanism
- Change the router's identifier from the default
- Change the router's default password
- Deny all, permit only some approach
- Don't assume that public hot-spots are safe

Radio Frequency Fingerprinting

Radio frequency fingerprinting (RFF)
for wireless intrusion detection systems (IDS)

- **Anomaly-based** intrusion detection approach with RFF
- Uniquely identifies a transceiver based on the **transceiverprint** (set of features) of the signal it generates.
- MAC address can be spoofed, but the transceiverprints from the illegitimate device would **not match the profile** of the legitimate device.

Anti-theft Solutions

- SMS-Block and SMS-Clean
- SMS-Find
- SIM Watch
- Encrypted safe folder

SPAM in SMS

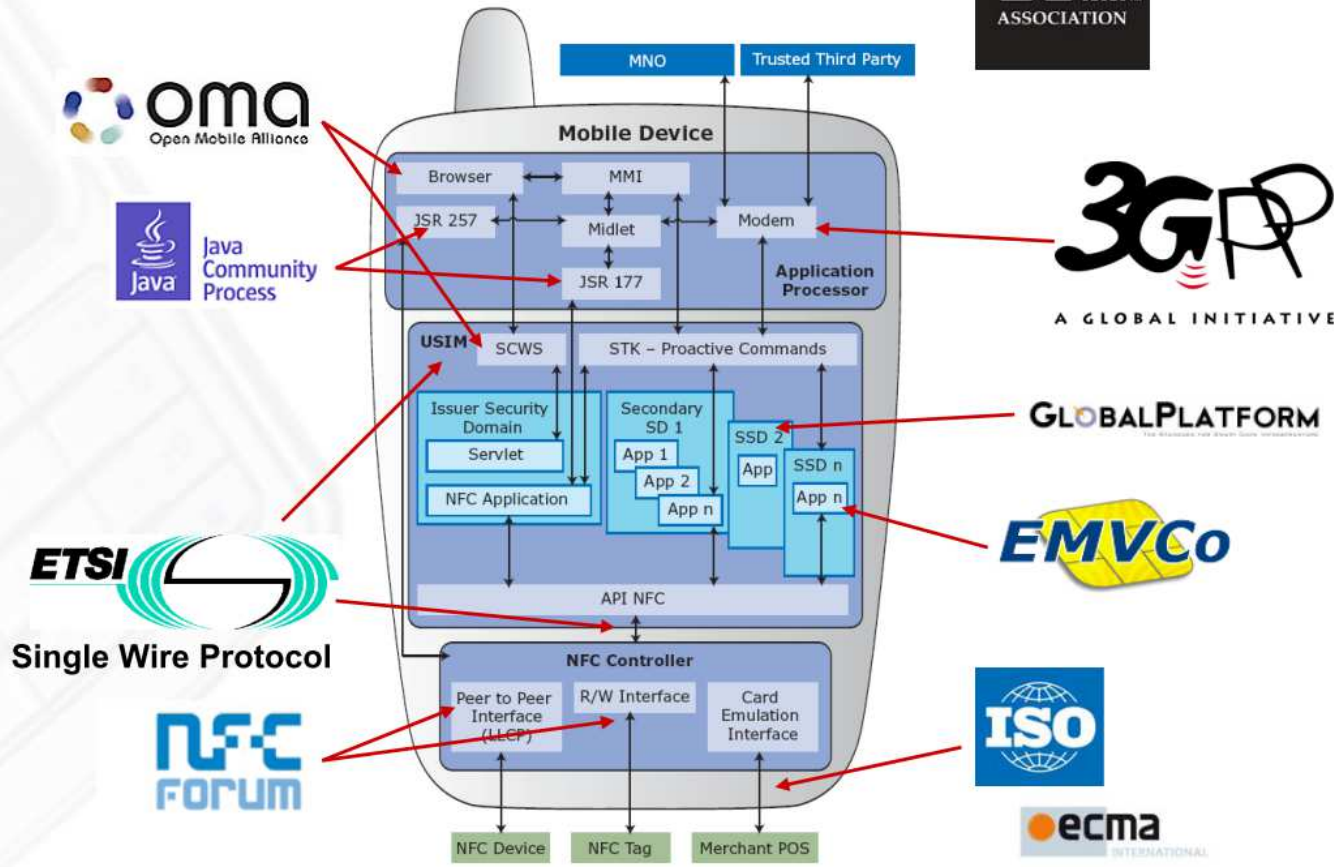
- In 2008 the amount of SMS spam was expected to grow by almost 50% to 1.5 million in the U.S.
- In China, the average subscriber receives 6-10 mobile spam messages every day

Mobile Secure Element

- Secure storage in your NFC device
- Current Secure Element Implementations
  - Embedded in Mobile Phone
  - SIM Based
  - Removeable SD Card

Different secure element solutions

NFC Device Standards



Popular Solution - SmartCard

- It is an Embedded System
- No Monitor, no keyboard
- Only a simple communication interface
  - Single Wire Protocol
  - USB
  - T0/T1 protocol
- Contact-based: Plastic Card ID1, UICC, USB token,
- Contactless: Mastercard, embedded in jewelry or watches

Application Domains of Smartcards

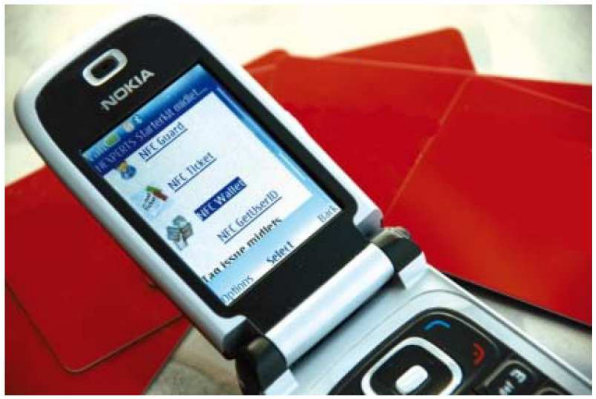
- Secure Storage
- Payment
- Authentication
- Signing
- E-Pass
- E-Health
- Ticketing,…

Security of SmartCards

- Crypto Co-Processors:
  - special math. co-processors that are optimized for the calculation of Crypto algorithms
- True Random Generator:
  - Special hardware block, which is responsible for the generation of random numbers
  - Random numbers are often required for the generation of keys in smart cards
- Memory Management Unit (MMU)
  - A hardware memory management unit is used to control memory accesses
  - Configuration of the MMU via the smart card operating system
  - The MMU secures access to ROM, RAM and EEPROM

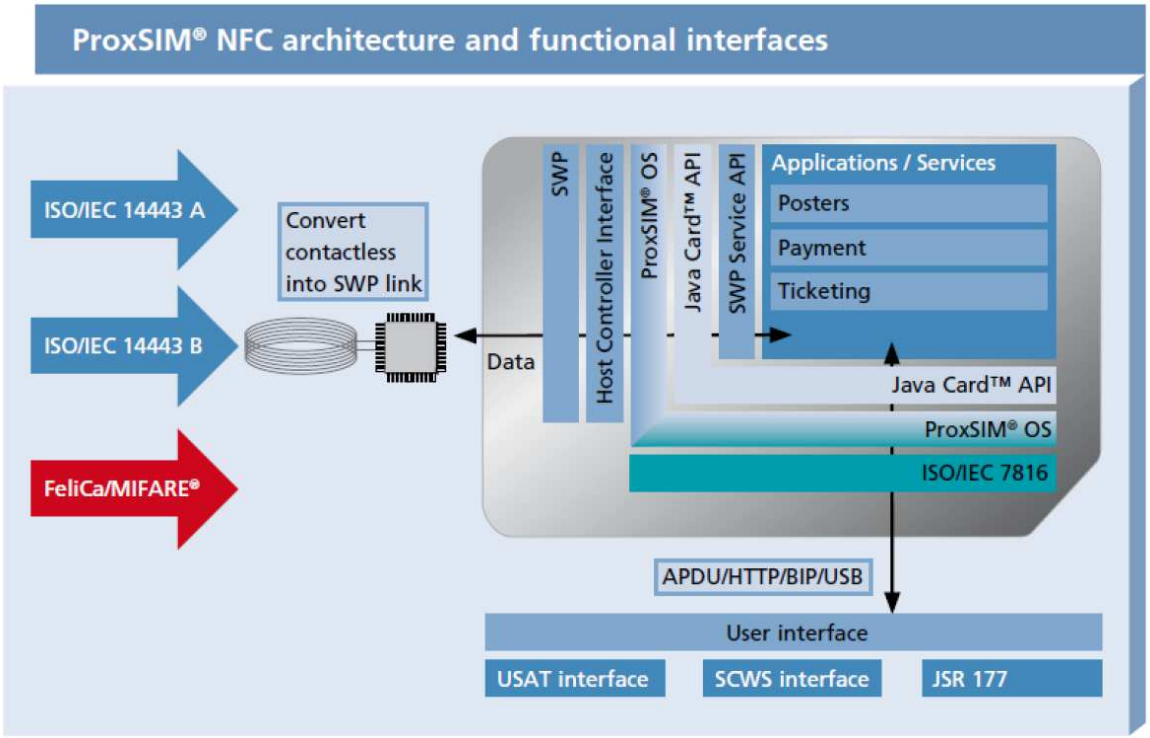
Future - NFC Phone Handset

- Contactless Smartcard
  - Payment
  - Ticketing
  - Loyalty
- Benefits of NFC Handset
  - Display to view Card Content
  - OTA Transactions
- J2ME - JSR 177:
  Secure Applications and Trust Services API



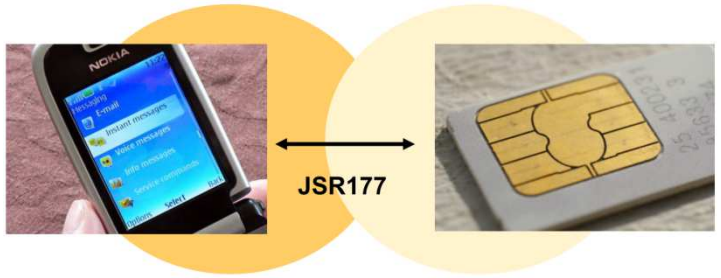
NFC Wallet

Example: ProxSIM from G&D



NFC Handset Secure Applications

- Handset Acts as a reader of Secure Element
- Two Applications needed:
  - J2ME as „GUI“ and „Reader“
  - JavaCard as application in Secure Element
- JSR177
  acts as interface between J2ME
  and internal JavaCard



J2ME - JSR177

(Security and Trust Services API)

- Defines an API to support communication with smart card applications using the APDU protocol
- Defines a Java Card RMI client API (allows a J2ME application to invoke a method of a remote Java Card object)
- Supports application level digital signature signing
- Allows basic user credential management
- Defines a subset of the J2SE cryptography API (support message digest, signature verification, encryption, and decryption)

Mobile Security Best Practices (1)

1. Enable device diversity (less susceptible to cyber-attack, different devices better suit different workers/users)
2. Enforce a strong password policy
3. Remotely lock or wipe all lost or stolen devices
4. Automate remote device wipe after 10 unsuccessful authentication attempts
5. Encrypt the data: consider file-level, application-level, or full-disk/memory card encryption

Mobile Security Best Practices (2)

6. Enable support for dual-usage models
   (professional and personal profiles on a single device)
7. Try to manage remotely all devices
   and limit the data stored on unmanaged devices
   (e.g. use a document management portal; and encourage people
   to only send links to the files and not the files themselves)
8. Avoid a company logo on the device (they encourage thieves)
   and display a contact phone number on the locked state
9. Utilize a single Web-based console for all management
   and security operations (e.g. 24/7 remote lock or wipe center)
10. Timely notification of lost or stolen mobile devices is the key
    (educate, how important it is to report these incidents immediately)

Privacy Concerns

e.g. Yahoo! oneConnect:

- **Draws information from social-networking sites** such as MySpace, AOL Instant Messenger, and e-mail to build a picture of the mood, location, and activities of friends and colleagues.
- **Status** - view the contacts by their most recent status updates on popular social networks and **automatically broadcast it** to their friends.
- **Pulse** - see a **dynamic overview** of what friends are up to, including recent photos, their status, profile updates, and recommendations based on their most recent actions on popular social networks.
- . . . **?**