Near Field Communication
Research Lab
Hagenberg

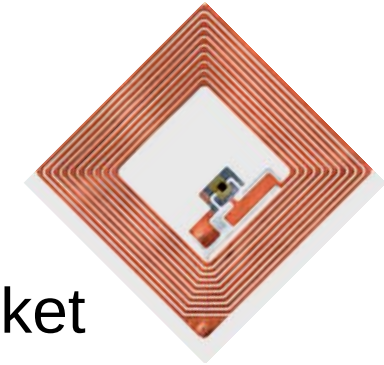
OBERÖSTERREICH
University of Applied Sciences

NFC Devices: Security & Privacy

Gerald Madlmayr

March, 7th 2008

NFC - What is it all about …

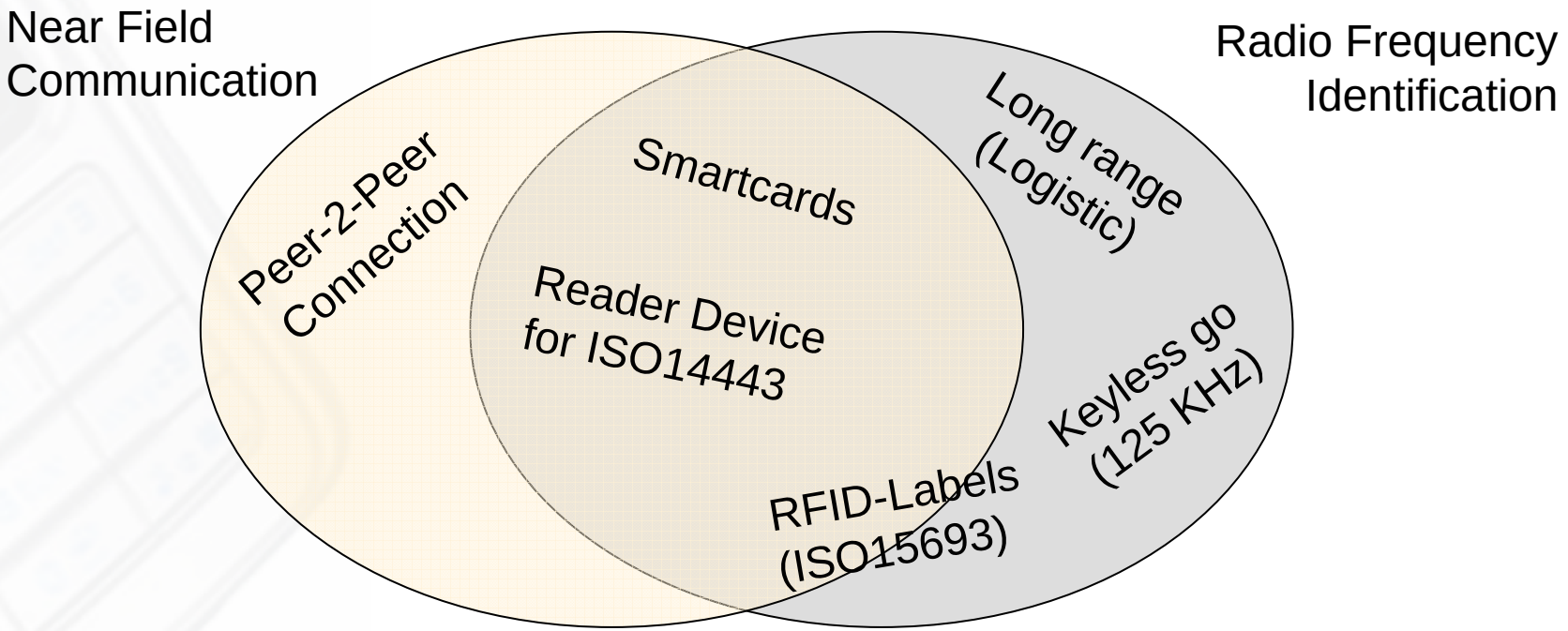


- RFID Derivate 13,56 Mhz
- Integrated in mobile devices for consumer market

- Operating Modes
  - Tag Emulation (PICC)
  - Reader/Writer (PCD)
  - Peer (NFC)

- Range: 0 – 10 cm (proximity Technology)

NFC vs. RFID


Near Field Communication
Radio Frequency Identification
Peer-2-Peer Connection
Smartcards
Reader Device for ISO14443
Long range (Logistic)
Keyless go (125 KHz)
RFID-Labels (ISO15693)

NFC Device *Operating Modes*

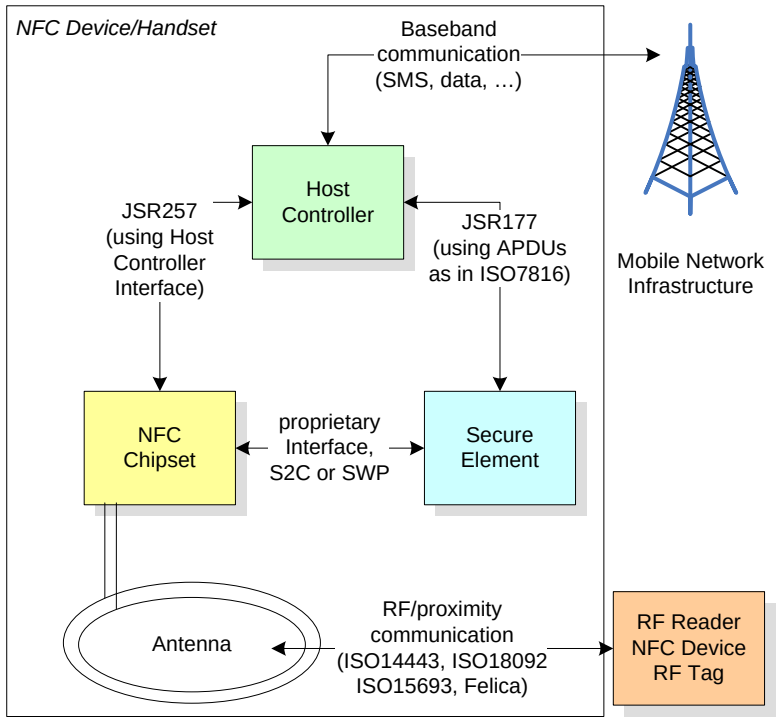
- Data exchange (P2P – NFC peer-to-peer)
  - Bidirectional connection to exchange data between devices
  - WiFi, BT, P2P Payment, Contacts, vCards, …
- Reader/Writer mode (PCD – Proximity Coupling Device)
  - Mobile Device is able to read external tags/smartcards
  - SmartPoster, WiFi Config, Ring-Tones, …
- Tag emulation (PICC – Proximity Card)
  - Reader can't distinguish between smartcard & tag emulation
  - Handset could contain multiple smartcards (smartcard chips)

Goal of Paper: NFC Threat Model

- Define Setup/Architecture
- Define Use cases
- Derive Assumptions
- Look at Interfaces to be attacked
- Clarify Trust Level of Components
- Assets to be protected
- Compose Threat Model
- Conclusion: Propose Counter Measures

Setup/Architecture & Use cases

- Platform: Handset
- Modes
  - Identification Mode
  - Tag Emulation (SE extern)
  - Wired Mode (SE intern)
  - P2P Mode
  - R/W Mode

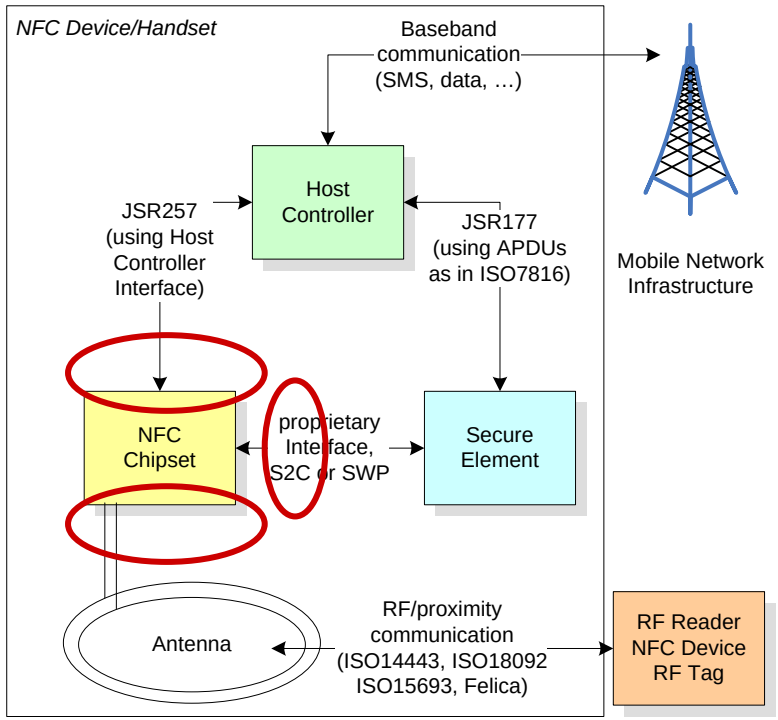


Use Cases

Communication Flow	*Operation Mode*	*Communication Interface*	*Use case*
(1) Use of unique ID Handset providing data Reader collecting data	– Tag Emulation Read/Write	ISO14443	Access Loyalty
(2) External mode of secure element Handset providing data Reader collecting data	– Tag Emulation Read/Write	ISO14443	Access Loyalty Payment
(3) Handset reads external tag Tag holding data Handset reading tag/target	– tag (emulation) Read/Write	ISO14443	BT/WiFi-Config VCard transfer SmartPoster
(4) Data exchange using NFC NFC target providing data Handset collecting data	– Peer (Target) Peer (Init)	ISO18092	BT/WiFi-Config VCard transfer data exchange
(5) Internal mode of secure element Secure elements in the handset Host Controller Application	– Internal mode Comm. channel to SE	ISO7816	OTA provisioning Ticket upload Money top up

Assumptions & Interfaces to be attacked

- Handset allows baseband connection
- Firmware in NFC chip can't be modified
- Secure Element is secure (attacking of interaces possible)
- Multiple Secure Elements possible



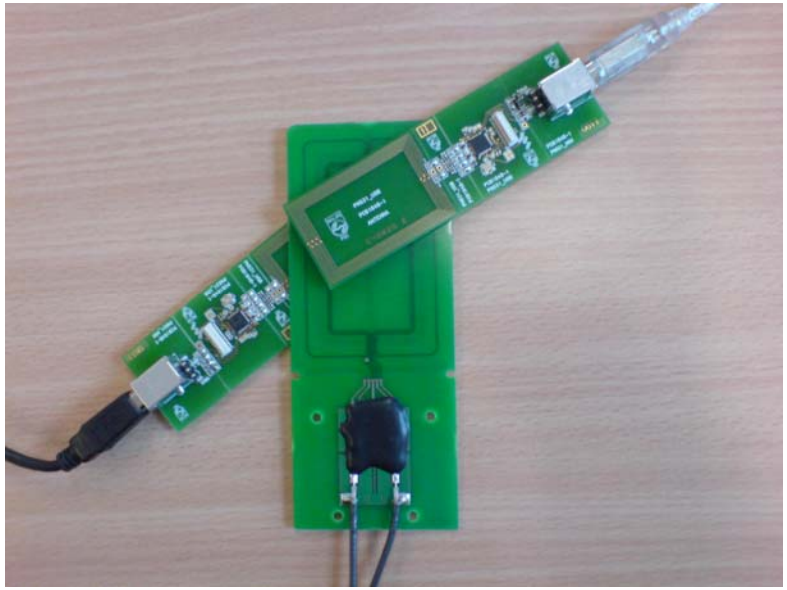
Trust Level & Assests

- Host Controller: untrusted
- RF interface: untrusted
- SE: trusted, but interface itself not. (SWP, S2C)

1. user's privacy
2. handset functionality causing cost (e.g. air time)
3. data stored in the mobile device (e.g. bluetooth address, contacts, short messages)
4. applications (and linked functionality; e.g. payment) and data stored in the secure elements/tags
5. NFC/RFID functionality of the handset

NFC Threat Model Matrix

- Use cases
- Attack Scenarios
  - Eavesdropping
  - Man-in-the Middle
  - Relay/Replay
  - Skimming
  - Phishing
  - Brute Force
- Components
- Assets to be protected



Proposed Counter Measures

- No ID based Services
- Button for NFC (on/off)
- No battery off mode (but NFC flight mode)
- No application index in SE without (mutual) authentication
- Managing in-device security (certificate based)
- Integrate Security Layer in NFC IP1

Near Field Communication
Research Lab
Hagenberg

OBERÖSTERREICH
University of Applied Sciences

Happy to answer any questions

Gerald Madlmayr

Gerald.Madlmayr@fh-hagenberg.at

NFC Threat Model Matrix

		ID Based Systems	PICC Case		PCD Case			NFC Case		OTA Case	
Use case Components		(1) *ID*	(2) *SE*	*RF*[4]	(3) *Device*	*Tag*	*RF*	(4) *Device*	*RF*	(5) *SE*	*OTA*
Spoofing	Man-in-the-Middle	1					2, 3		2, 3		4
	Skimming	1					1		1	1	1
	Relay	1		4			2, 3		2, 3		1
	Replay	1					2, 3		2, 3		4
	Eavesdropping	1					2, 3		2, 3	4	4
Tampering	Brute Force		4			4		3		4	
Repudiation	Application driven		4							4	
Information disclosure	Tracking/Tracing	1	1			1				1	
	Eavesdropping	1					3		3		4
	Phishing				2			2			
DoS	(Blocker) Tags		4, 5		5			5			
	Application driven		4, 5		5			5		4, 5	
Elevaltion of Privilege	Application driven				5			5		4, 5	