Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Security of RFID-based technology

Tommi Hakamäki
Seinäjoki University of Applied Sciences
School of Technology
Seinäjoki, Finland
tommitapanihakamaki@gmail.com

Heikki Palomäki
Seinäjoki University of Applied Sciences
School of Technology
Seinäjoki, Finland
heikki.palomaki@seamk.fi

AmiEs-2015, 24-26 September, 2015, Oostende, Belgium

Index

- Introduction
- State of the art
- Function of RFID/NFC
- Used data security
- Unauthorized use cases
- Conclusion

Introduction

- RFID access control
- NFC payment cards
- Manufacturer & service providers:
  - “Very security technology”
- Practical tests:
  - “Copying and hacking are possible”

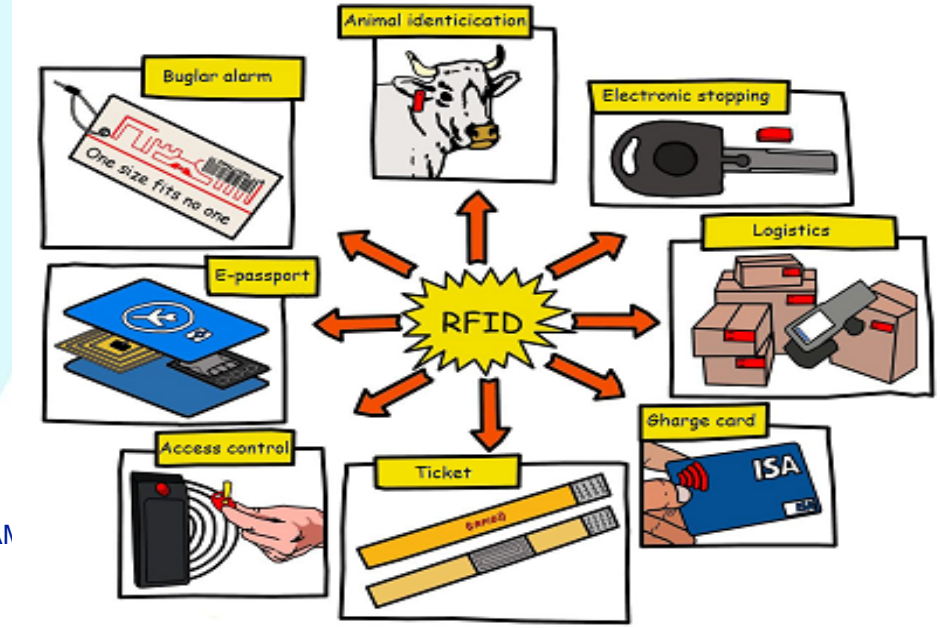
State of the art

- History
  - 2'th world war➔ Primary & secondary radars
  - 1950➔EAS anti-theft system for shops
  - 1973➔Active & passive RFID
  - 1990➔0.3-3 GHz systems
  - 2003➔sponsored by over 100 companies

Features

- Identifier (=tag), reader and control system

Frequency bands	Most used frequencies
LF (low frequency)	125 – 134 kHz
HF (high frequency)	13.56 MHz
UHF (ultra high frequency)	860-960 MHz



- New applications
- Old technology

Standards

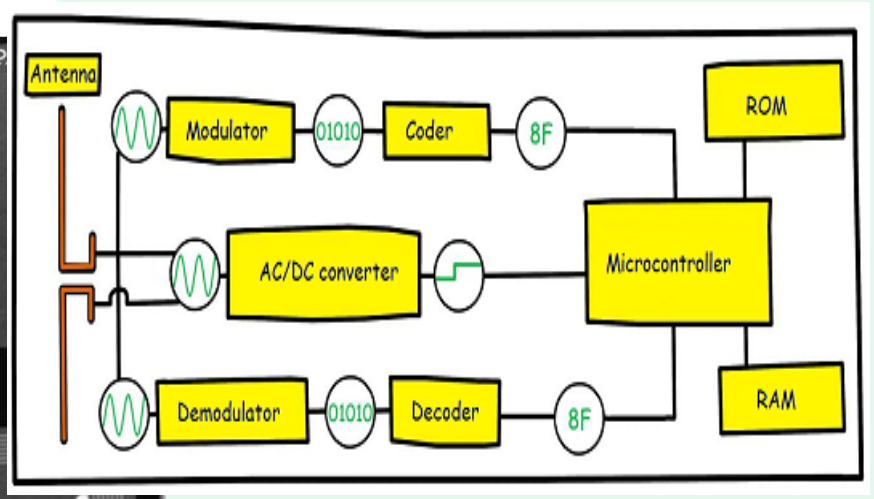
Standard	Definition
ISO 11784 **ISO 11785** **ISO 14223**	Data content, communication and air interface of identifiers for animals
ISO 10536	Identifiers using 4.9152 MHz frequency and maximum 1 cm reading distance
ISO 14443	Identifiers using 0–10 cm reading distance
ISO 15693	Identifiers using 13.56 MHz frequency and 0–1m reading distance
ISO 18000	Air interface and obligatory commands of identifiers using separate frequencies

RFID identifiers

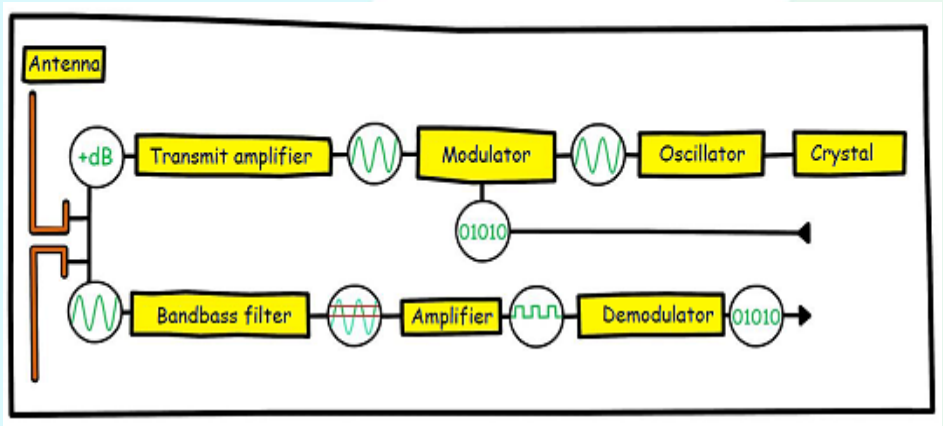
- Antenna
- Controller
- (Memory)
- (Power supply)

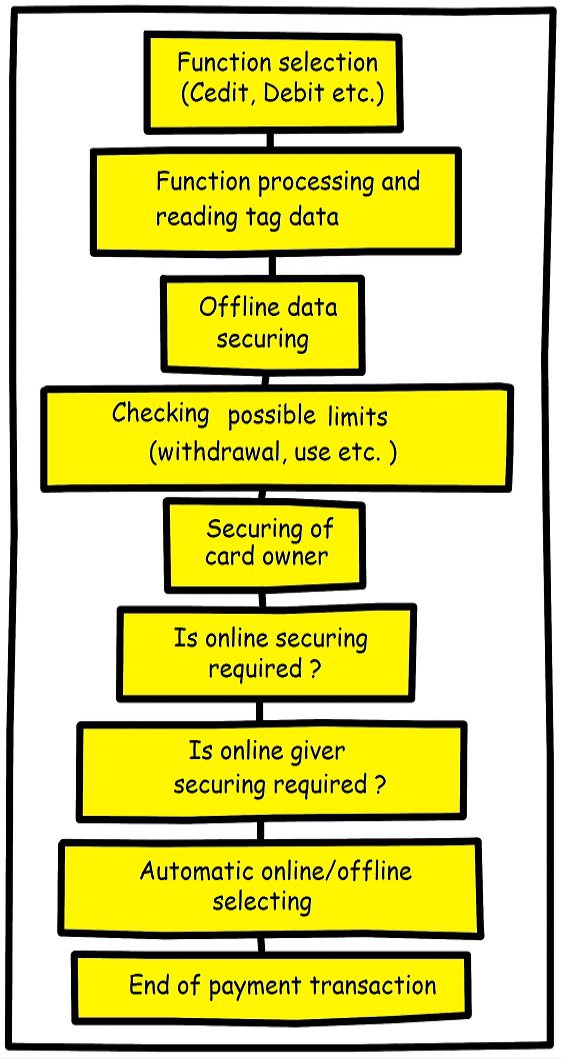
- Passive
- Half-passive
- Active

NFC payment cards

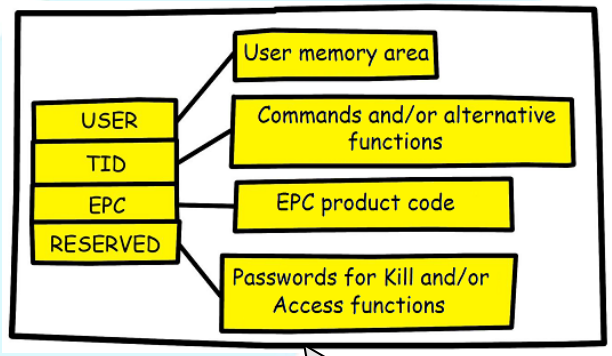


RFID reader

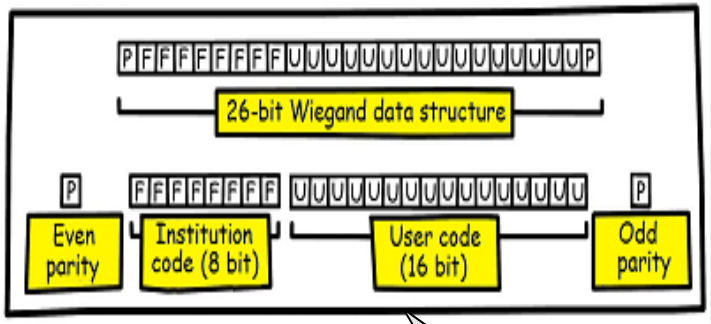

Antenna
+dB
Transmit amplifier
Modulator
Oscillator
Crystal
01010
Bandbass filter
Amplifier
Demodulator
01010


Function selection (Cedit, Debit etc.)
Function processing and reading tag data
Offline data securing
Checking possible limits (withdrawal, use etc.)
Securing of card owner
Is online securing required ?
Is online giver securing required ?
Automatic online/offline selecting
End of payment transaction

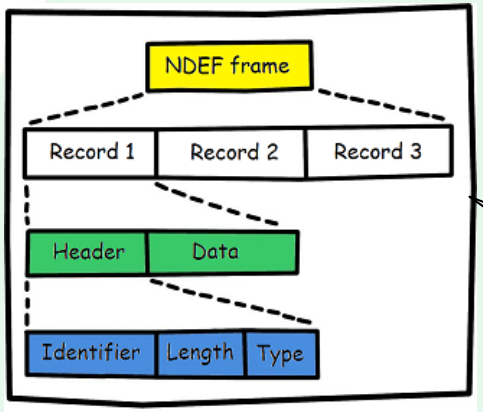
Data structures



EPC
Class-1 Gen-2



Wiegand



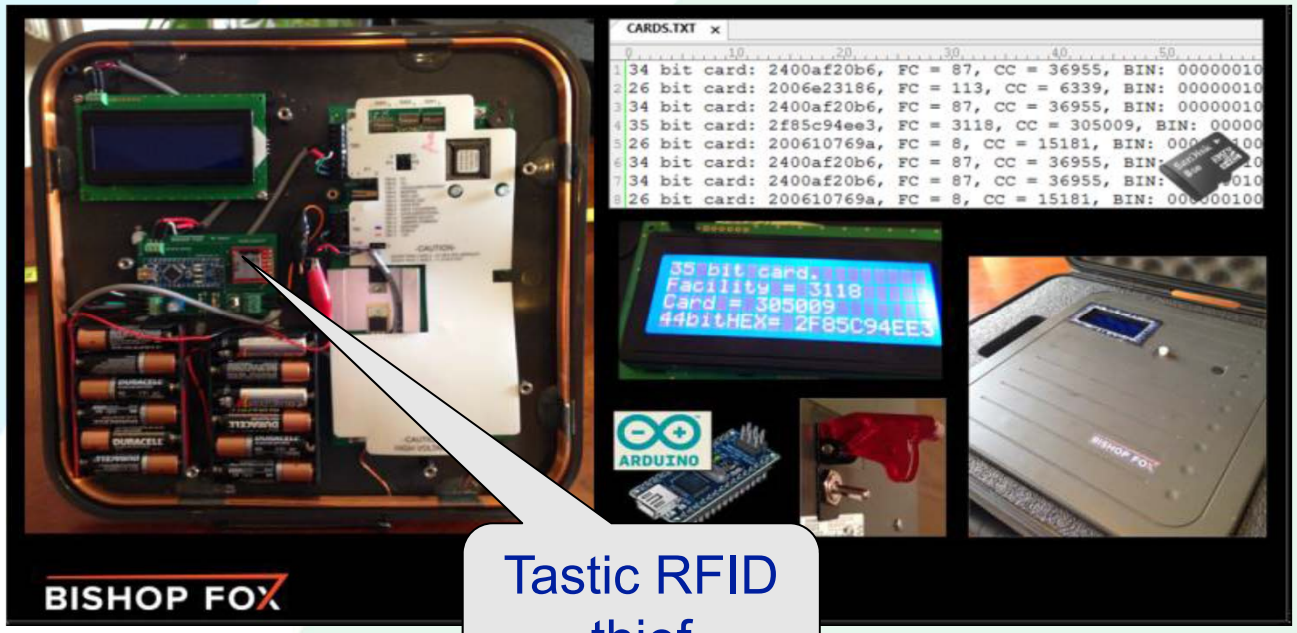
NDEF

Encryption

- Encryption key
  - 2008➔ copying is possible
- Better encryption is possible
  - More processing power
  - More cost ?
  - Compatibility ?

Unauthorized RFID reader

- Access control:
  - Often no encryption – readable data



Tastic RFID thief

Hacking

- Encryption of 48 bit is developed at 1994 ➔Too old !!
- All devices are hacked at 2013 (HID Global)

Skipping the reader

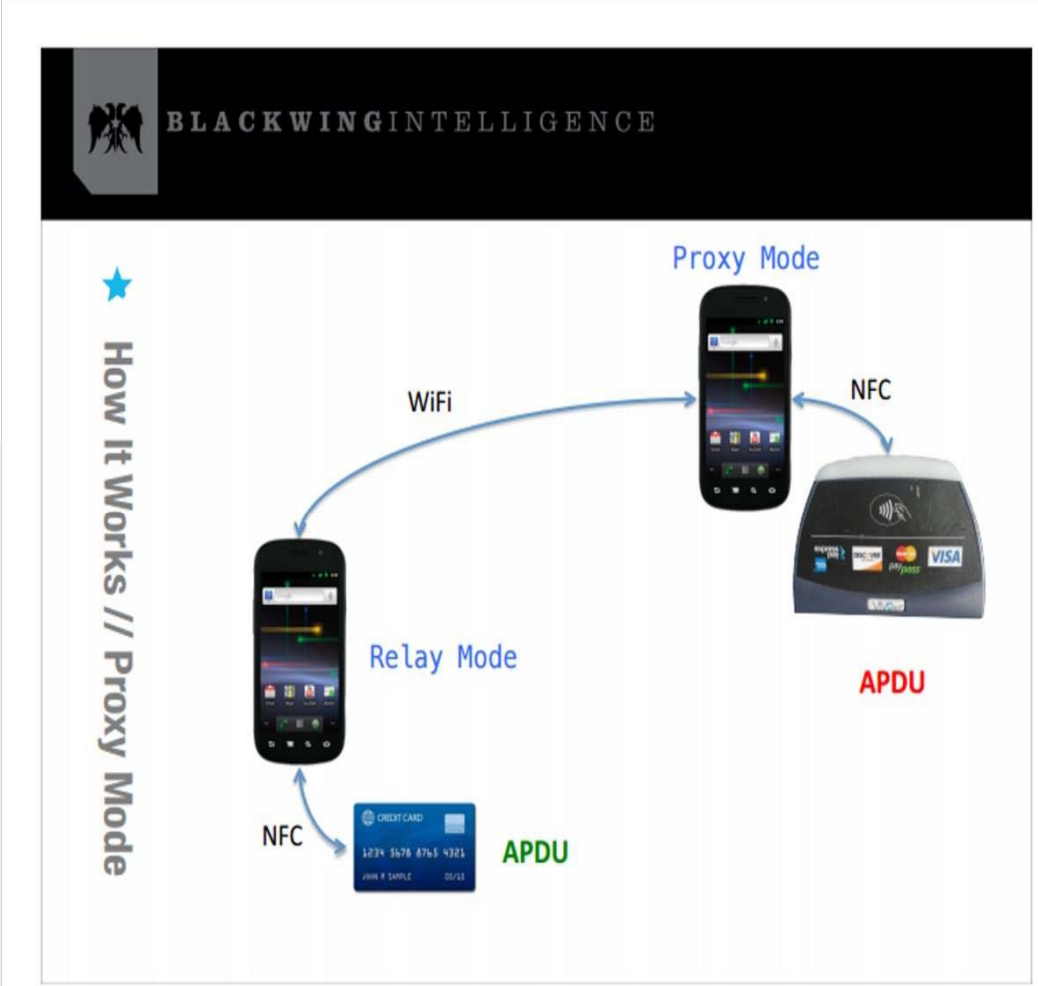
1. Contac to data cable
2. Read data flow in the real case
3. Replay data without RFID when needed

Exploitation case of payment card 1

- Nixu.com test 2013:
  1. Buy a NFC reader (about 20€)
  2. Read from neighbours card in 1 second:
     - Card number
     - Validation date
     - The owner name
  3. Use data in online shop without limits

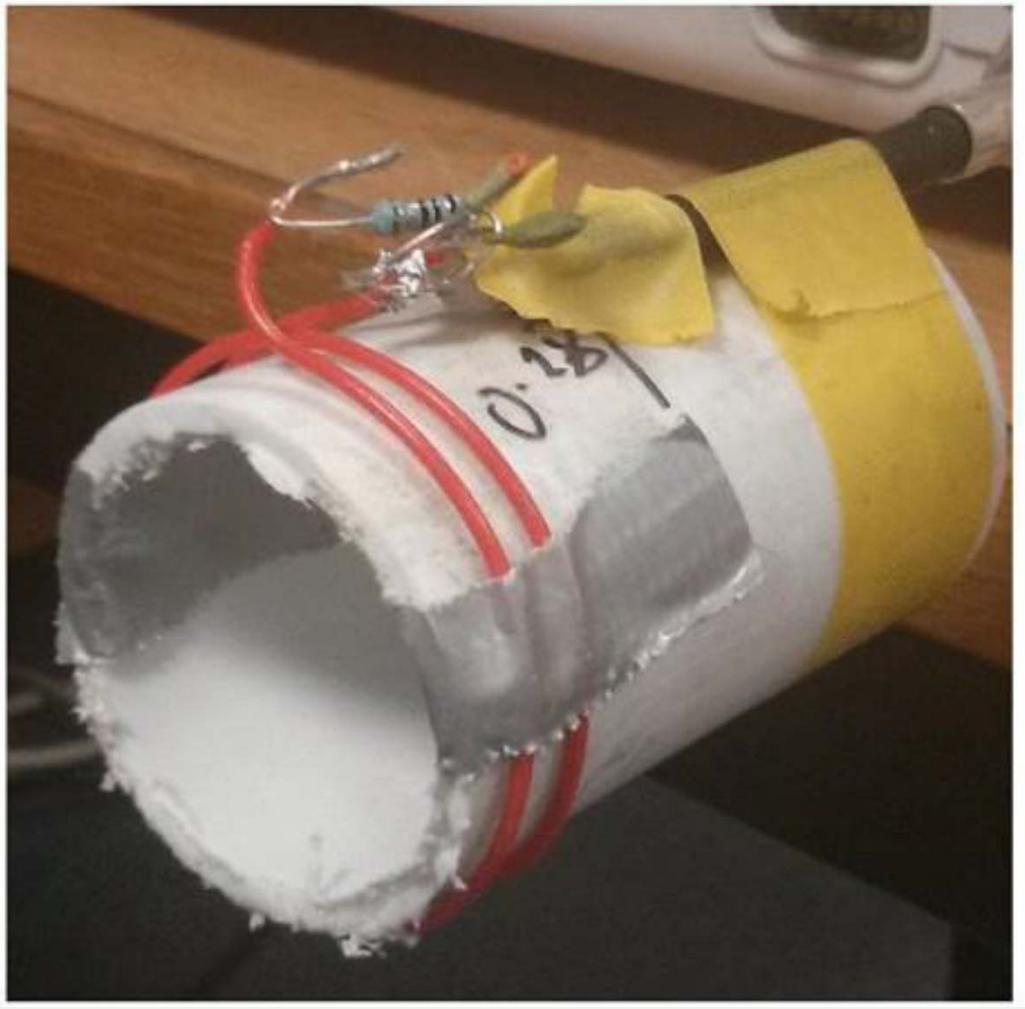
Exploitation case of payment card 2

- Eddie Lee 2014:
  1. Use 2 mobile phones with NFC feature
  2. Create a virtual link between payment card and NFC reader

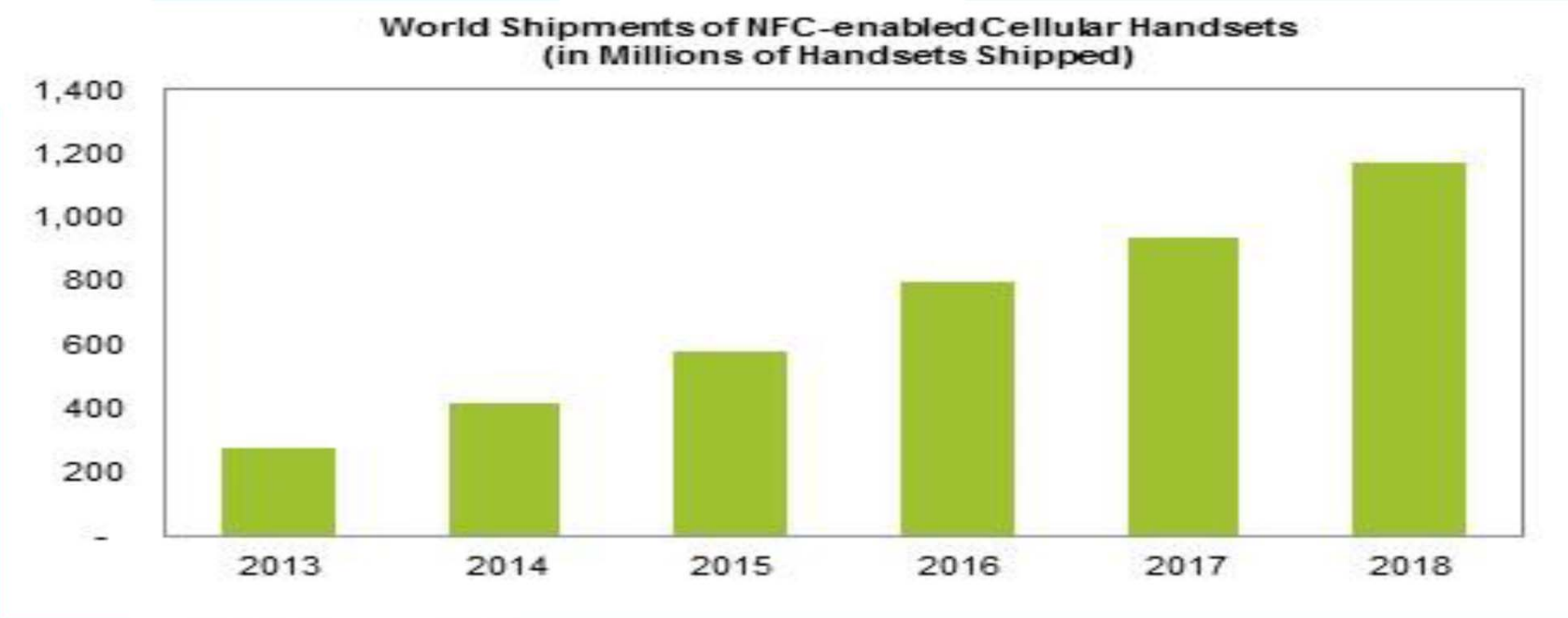


Long distance reading of payment card

- Surrey university:
  - Long distance antenna layout
  - Range 45-80 cm



Estimated use of NFC payment cards



- A good market for hackers ?

Conclusion

- Problem: the old low-cost, unsecure and compatible standards
- Solution: the new, better, higher-cost, incompatible protocols.
- Mobile phones makes NFC technology more unsecure
- Opposite information from two sources: Banks and practical test
- New market area for unstandardized technology