Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones

Collin Mulliner
Fraunhofer SIT (Darmstadt, Germany)

1st International Workshop on Sensor Security
March 2009
Fukuoka, Japan

Near Field Communication (NFC)

- Bidirectional proximity coupling technology
  - Based on 13,56Mhz RFID ISO14443 and FeliCa
- NFC devices support three modes of operation
  - PCD (read/write), PICC (card emu), peer-to-peer
- Standardized data formats on tags
  - NFC Data Exchange Format (NDEF)

Introduction

- NFC phones and services are just being introduced into the public (outside of Japan!)
- NFC is designed for payment and ticketing
  - Security is essential
- Current devices and services use passive tags
  - Large scale use in the future because of low price
  - Our work focused on interaction with passive tags

Contributions

- Methods for vulnerability analysis of NFC-enabled mobile phones
- Developed tools for security testing of NFC mobile phones and NFC-services
- Multiple novel attacks against NFC mobile phones and services

An NFC Mobile Phone

- Mobile phone that also integrates NFC-chip and -antenna and possible a smart card
- NFC-system constantly scans for and reads tags
  - Tag data is processed by either OS functionality or third party application
- Third party application can take control of NFC functionality for arbitrary use

An NFC Mobile Phone

Nokia 6131 NFC

Analyzing an NFC Mobile Phone

- Interaction with passive tags (NDEF format)
  - What formats are supported, what can be attacked?
- J2ME NFC API (JSR-257)
  - Can the API be abused for attacks?
- System components that can be controlled through NFC
  - Do these components have issues that can be abused through the NFC interface?

NDEF Security Toolkit

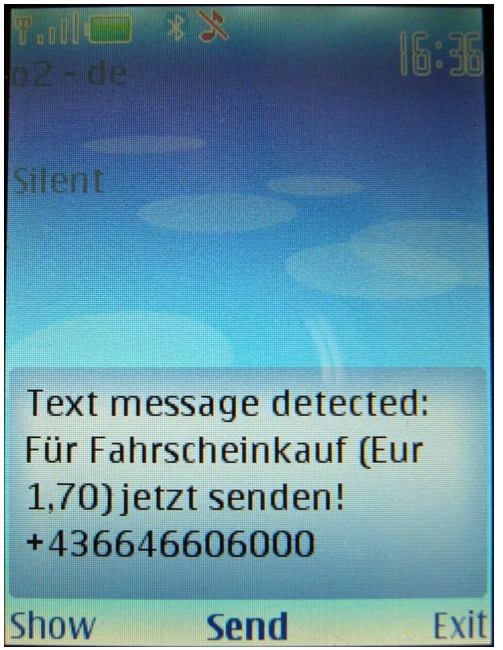
- Flexible implementation of the NDEF standard
  - Arbitrary modification of format and data
- Tag reading/writing, dumping tools
  - Immune against malformed data
  - Test lab version (use with desktop computer)
  - Mobile phone version for analyzing services

NDEF Fuzzing

- Fuzzing is a good choice when testing without access to source code
- Fuzzing procedure required a human operator
  - Manually moved tag between writer and phone
- Found multiple vulnerabilities
  - Tested phone crashes and resets

NDEF Smart Poster

- URIs are technical and not suited for the user
- Smart Poster allows to display information in addition to URI
  - Human readable text
  - Image (optional)



URI: **sms:+436646606000?body=Fahrschein**
Title: **Für Fahrscheinkauf (Eur 1,70) jetzt senden!**

Smart Poster URI Spoofing

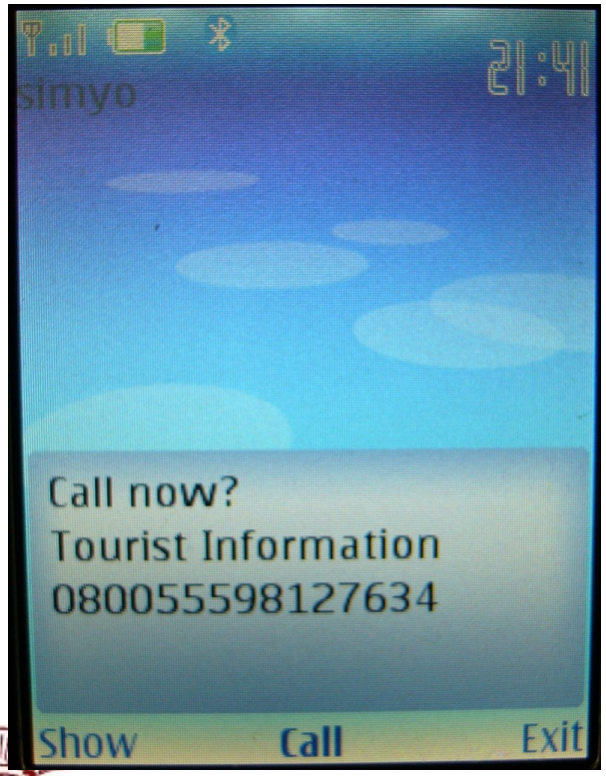
- Smart Poster display problem
  - Informational text can be used to prevent the URI from being displayed
  - Text can be used to spoof the URI
  - Smart Poster details-view can also be manipulated
- Show innocent looking URI to trick user into opening it!

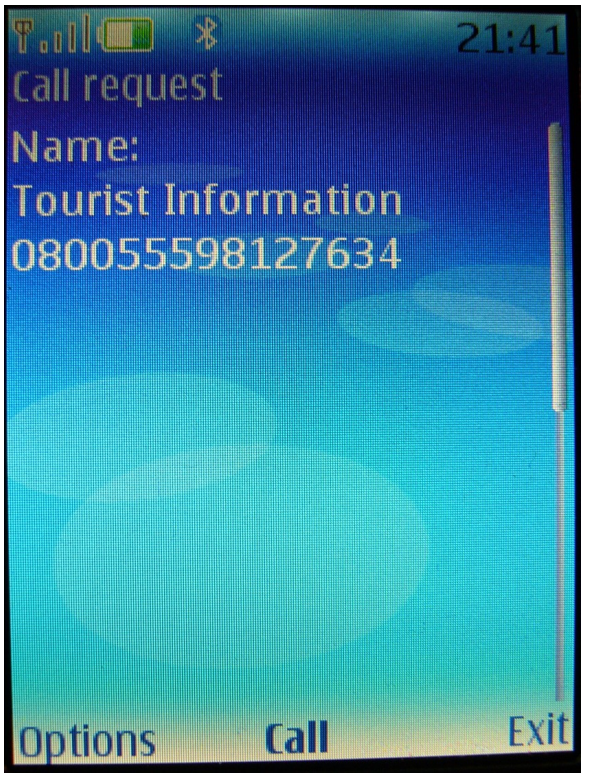
Smart Poster URI Spoofing Attacks

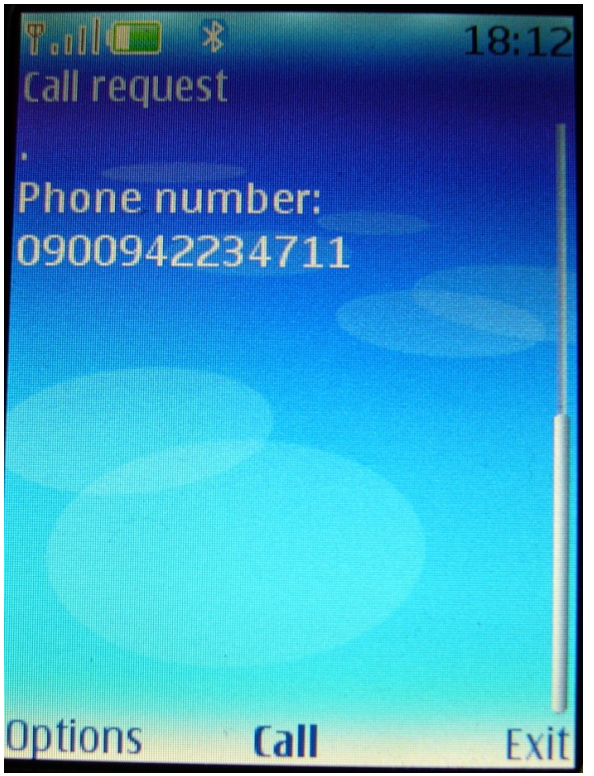
- Web Browser
  - Load malicious site (URL not displayed on phones)
  - Web-based Man-in-the-Middle attack
    - Steal credentials or inject malicious content
- Mobile Telephony Service
  - Premium rate phone call or SMS

Example: Attacking the Mobile Telephony Service

Title: **Tourist Information\r0800559812763 4\r\r\r\r\r.**
URI: **tel:0900942234711**







Proof-of-Concept NFC Worm

- Push registry allows registration for plain URI
  - App can intercept all tag read events for URI tags
- Basic idea: writable tags as transport for worm
  - Use URI spoofing to hide the worm-install-URL
  - Exploit phone's web browser vulnerabilities
    - Silent/automatic install + ask user to run application
  - Spreads by writing URL pointing to itself to tag
  - Worm is activated by phone reading plain URI tag

Denial-of-Service Attacks

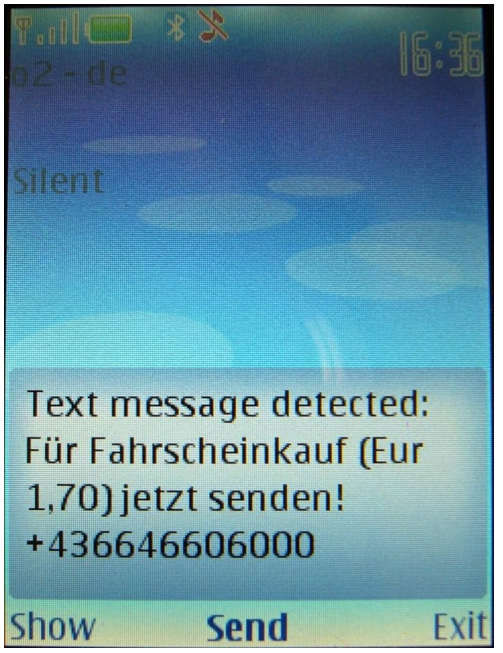
- Destroy trust relationship between customer and the service provider
  - Competitor or prankster
- Sticky paper tag on top of service provider tag
  - Data on tag causes the NFC-phone to crash
  - Paper tag cannot be linked to crash since it looks just like a sticker
- Attacks found through fuzzing

Security of NFC-based Services

- Survey to verify that attacks are practical today
  - Three services surveyed in Vienna, Austria
- All services only use built-in functionality
  - No additional software is installed onto user phones
- Survey was conducted using a NFC-phone running our security toolkit applications

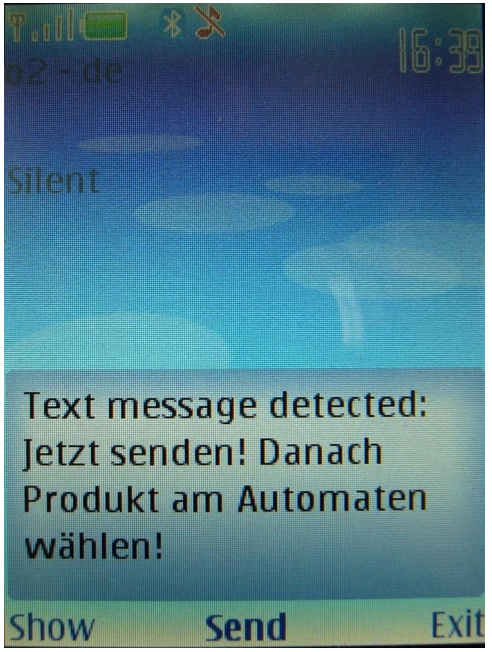
Wiener Linien

- SMS-based ticketing (NDEF Smart Poster)
- Phone number can be spoofed
  - Victim sends SMS to premium rate number



Selecta Vending Machines

- Mobile phone payment via SMS
- Phone number can be spoofed
  - Payment can be redirect to another machine



Vienna ÖBB Handy-Ticket

- Link to online ticket shop
- URL spoofed for Man-in-the-Middle attack
  - Steal credentials or inject malware

Conclusions

- We showed how NFC mobile phones and services can be analyzed for security
  - Non-NFC-components also need to be taken into account
- We introduced a new set of attacks
  - Attacks target both phones and services
  - Attacks can be utilized for fraud, worms, phishing, and Denial-of-Service

Future Work

- Improve fuzzing process through automation
- Follow development of NFC
  - New devices and features
  - More complex services

Questions?

Thank you for your attention!