Wydział elektroniki i Technik Informacyjnych

Near Field Communication

Podatności na ataki

Albert Sitek

Seminarium z Kryptografii i Ochrony Informacji
Warszawa, 07.12.2011

Plan prezentacji

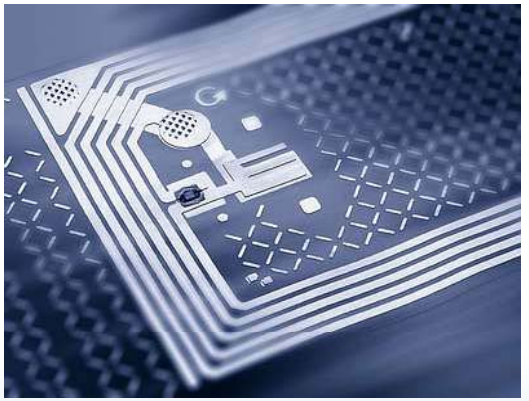
- Opis interfejsu NFC
- Przykładowe zastosowania
- NFC – nowy wymiar płatności zbliżeniowych
- Przegląd ataków na NFC
- Podsumowanie

Czym jest NFC?

- ISO/IEC 18092 oraz ISO/IEC 21481
- Rozwinięcie ISO/IEC 14443
- Pasmo ISM – 13,56 MHz
- Zasięg - kilka centymetrów
- Obsługiwane prędkości transmisji:
  - ✓106 kbit/s, 212 kbit/s, 424 kbit/s

Rodzaje tagów NFC

- Tag 1 Type – ISO14443A, 96B-2kB, 106 kbit/s
- Tag 2 Type – ISO14443A, 48B-2kB, 106 kbit/s
- Tag 3 Type – Sony FeliCa, 2kB, 212kbit/s
- Tag 4 Type – ISO14443A i B, 106 kbit/s lub 424 kbit/s, pre-configured

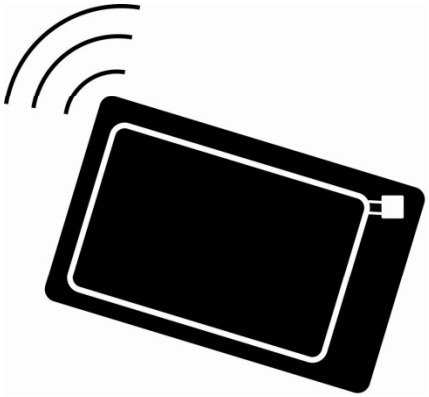


NDEF – NFC Data Exchange Format

- Zdefiniowane przez NFC FORUM
- Kontener dla danych zapisanych w Tagach
  - URI Record – HTTP, TEL, SMS
  - Text Record
  - SmartPoster – URI + Text

Tryby działania urządzeń NFC

- RFID Reader – Writer
  TAG Emulation



- Card Emulation

- NFCIP the Peer-t e (ISO 18092)

NFC – Przykładowe zastosowania

Automaty vendingowe

Sprzedaż biletów

Systemy informacji

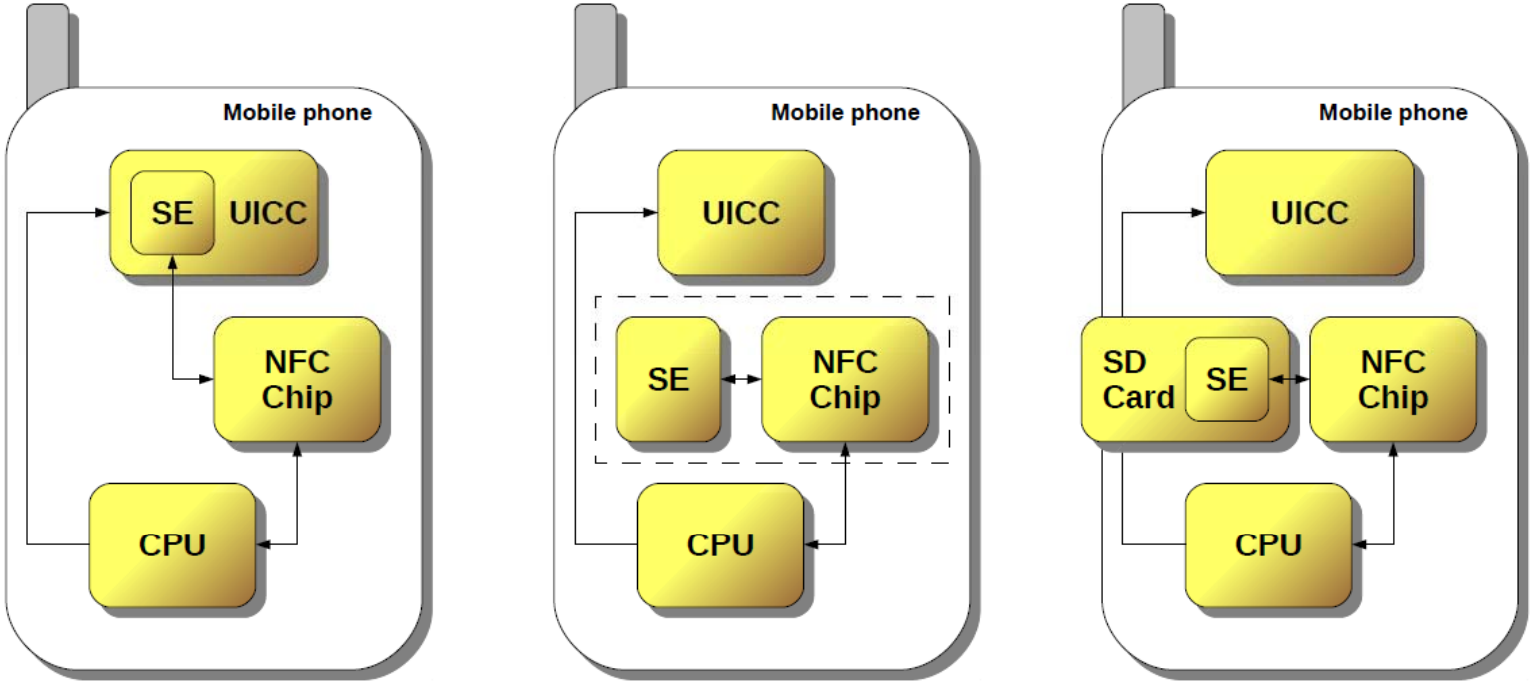
NFC – Przykładowe zastosowania 2

Wymiana wizytówek

Parowanie z routerem WiFi

NFC – Nowy wymiar płatności zbliżeniowych

Ale żeby to było możliwe…



(a) UICC as secure element (b) directly embedded in mobile phone (c) embedded in additional SD card

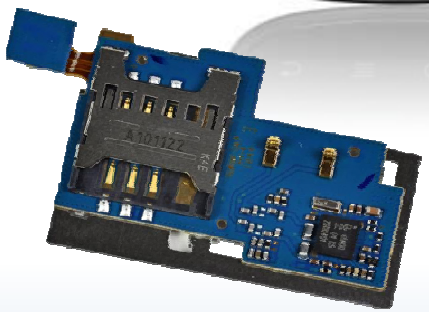
NFC – Płatności „od drugiej strony”?

NFC

Square

ERPLY

Telefony z NFC



Cele ataków…

- … na telefony:
  - Crash telefonu bądź aplikacji
  - Instalacja złośliwego oprogramowania
  - Błędne działanie aplikacji
- … na świadczone usługi:
  - Atak na tagi i infrastrukturę usługową
  - Ukierunkowane na ochronę usługodawców, a nie klientów

Czynniki sprzyjające

- Brak szyfrowania komunikacji:
  - Podsłuch
  - Atak Man-in-the-middle
  - Manipulacja transmitowanymi danymi
- Łatwa manipulacja przy tagach NFC/RFID
  - Modyfikacja
  - Podmiana oryginalnego taga
- Integralność tagów pierwotnie niezabezpieczona

Jak przeprowadzić atak z użyciem taga?

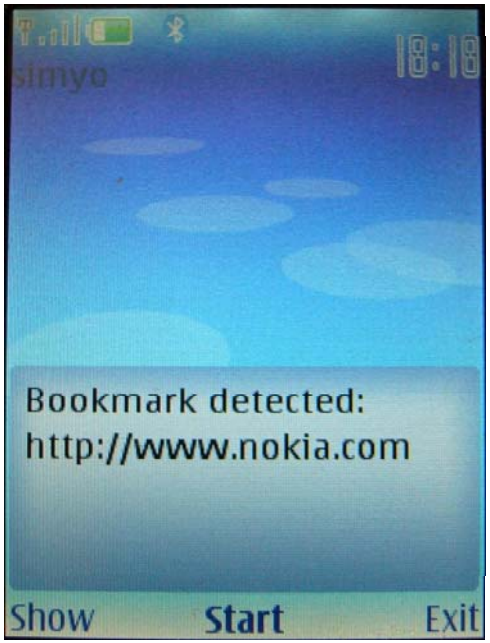
- Przykleić fałszywy tag na wierzch oryginalnego
  - Użyć RFID-Zapper
  - Odizolować folią aluminiową
- Podmienić oryginalny tag

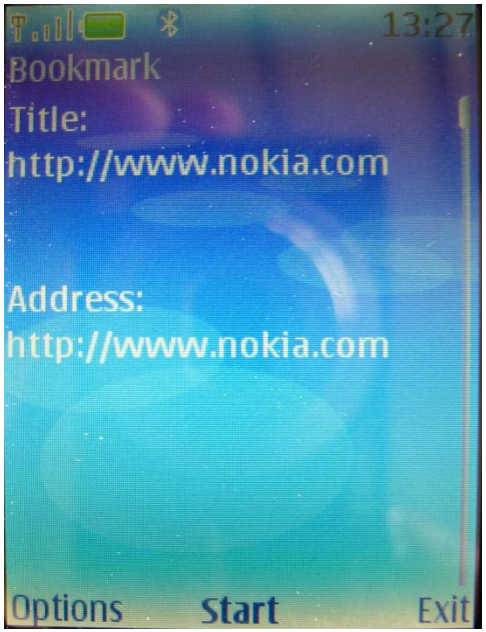
Koszt ~5 zł

- Złamać klucz zabezpieczający

Atak na przeglądarkę

- URI = „http://mulliner.org/blog/”
- Title = „http://www.nokia.com\r\r\rAddress:\rhttp://www.nokia.com\r**...**\r.”





Collin Mulliner: http://mulliner.org/nfc/

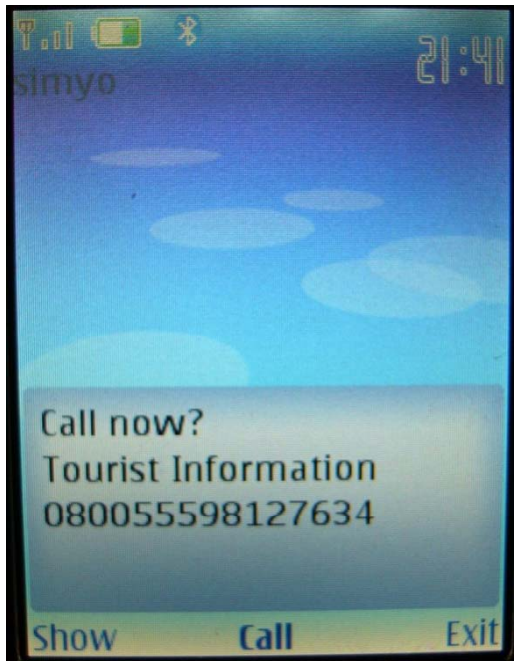
Atak na przeglądarkę 2

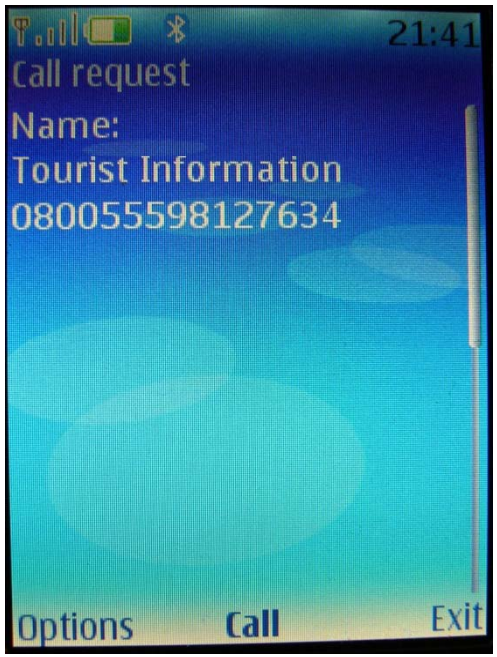
- Man-in-the-middle Proxy przy użyciu CGIProxy.
- Przykład:
  - Title = „https://mshop.store.com/”
  - URI = „http://attacker.com/proxy.cgi/https/mshop.store.com/”
- Działa jeśli przeglądarka nie wyświetla adresu docelowego
- Możliwa kradzież danych poufnych, dołączanie złośliwych treści

Collin Mulliner: http://mulliner.org/nfc/

Fałszywy numer połączenia

- URI = „tel:0900942234711”
- Title = „Tourist Information\r080055598127634\r\r\r\r\r\r\r.”

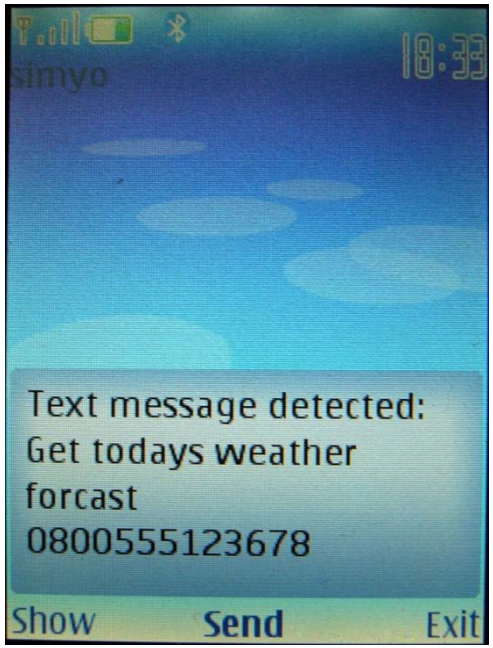


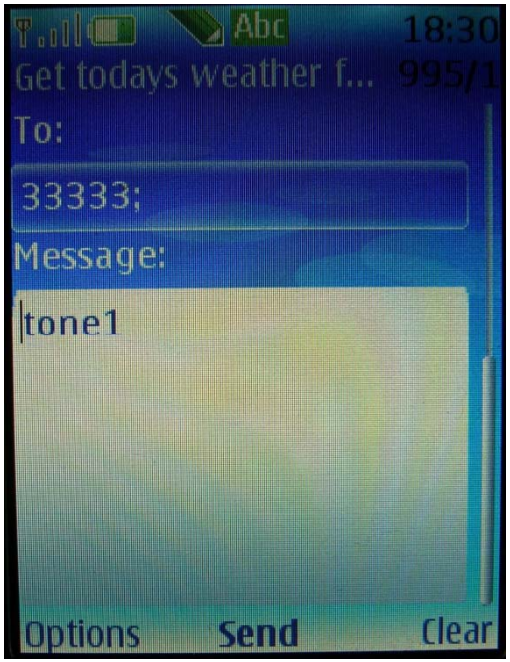


Collin Mulliner: http://mulliner.org/nfc/

Fałszywe dane SMS

- URI = „sms:33333?body=tone1”
- Title is:"Get todays weather forecast\r0800555123678"

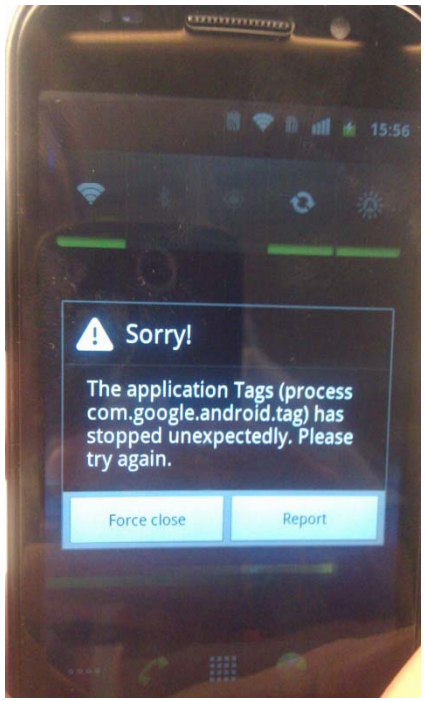


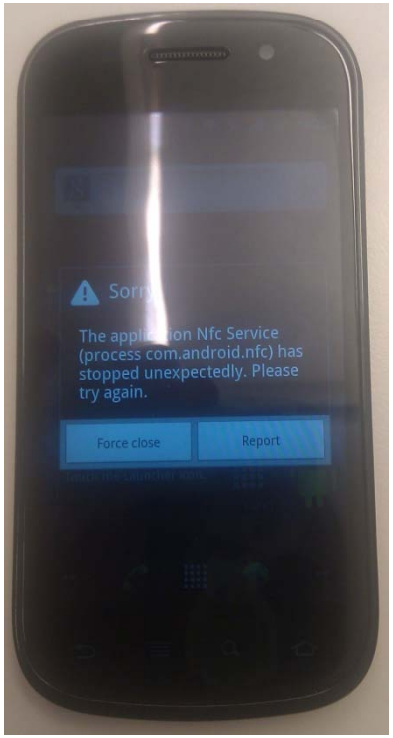


Collin Mulliner: http://mulliner.org/nfc/

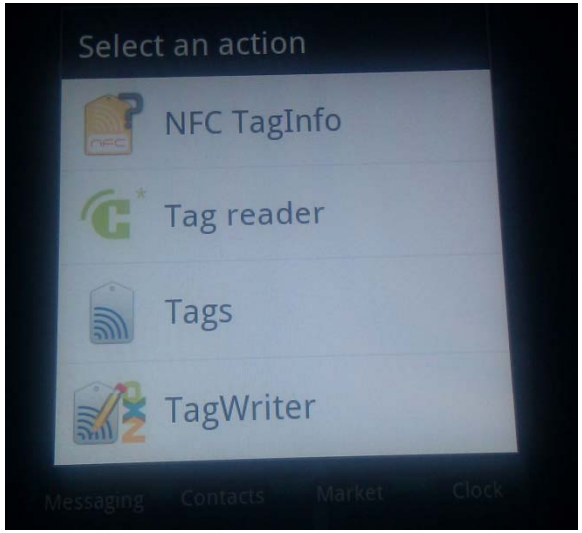
Błędy w tagach NFC

- Długość taga NFC = 0xFFFFFFFF
- Długość Rekordu = 0x0F i brak zawartości





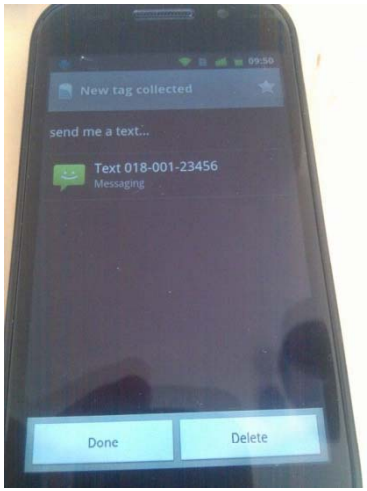
Ale istnieje wiele aplikacji do odczytu tagów…

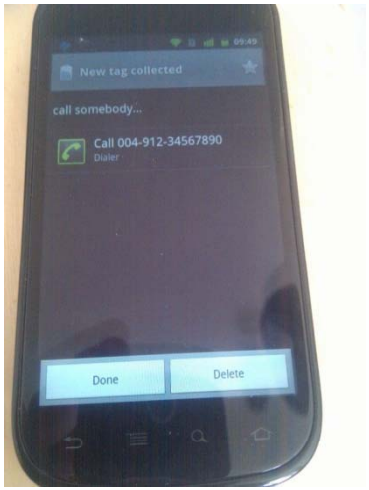


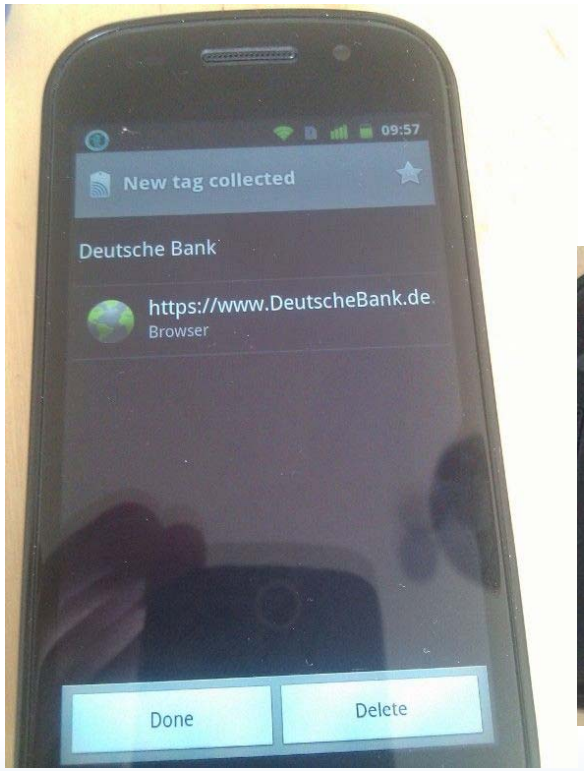
Collin Mulliner: http://mulliner.org/nfc/

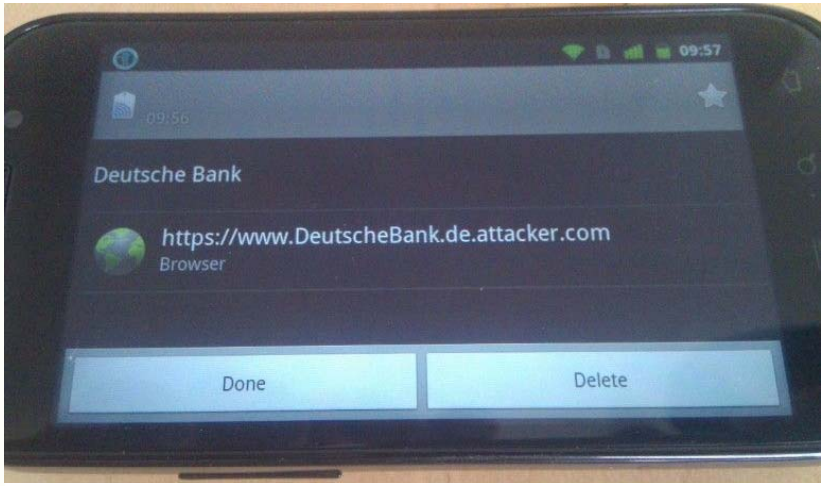
Pozostałe ataki na Nexus S

- Tel i SMS nie działa
- HTTP…









… „prawie” działa

Collin Mulliner: http://mulliner.org/nfc/

Atak na maszyny vendingowe

Tagi wskazujące na jedną maszynę mogą być naklejone na wielu automatach.

Przykładowy scenariusz ataku DoS

- Przypuszczalny cel:
  - Chęć przekonania użytkowników o niebezpieczeństwie użytkowania NFC
- Przeprowadzenie ataku:
  - Przyklejenie tagów z błędogenną/złośliwą zawartością na oryginalne tagi
- Rezultat:
  - Klient przestaje korzystać z usługi

Ataki typu RELAY

„*Practical NFC Peer-to-Peer Relay Attack using Mobile Phones*” - Lishoy Francis, Gerhard Hancke, Keith Mayes, Konstantinos Markantonakis

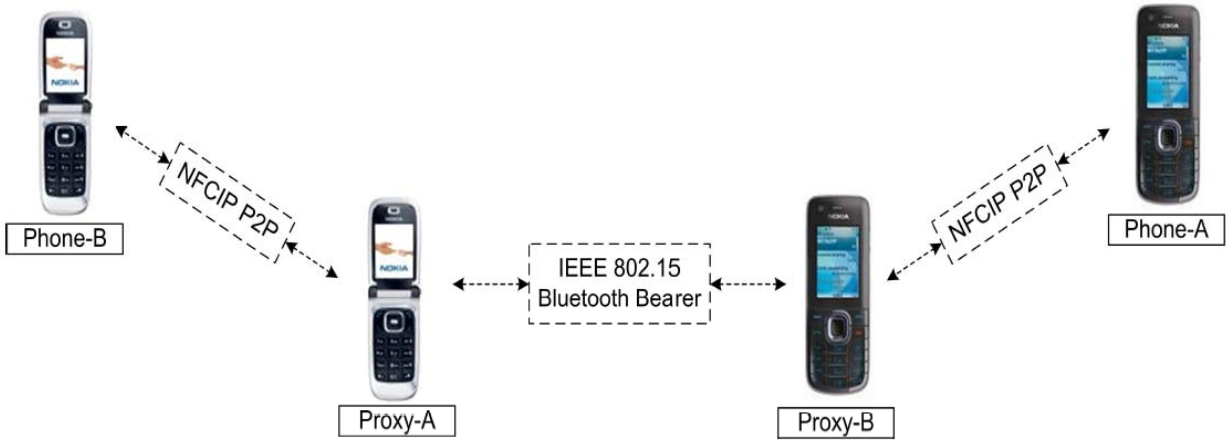
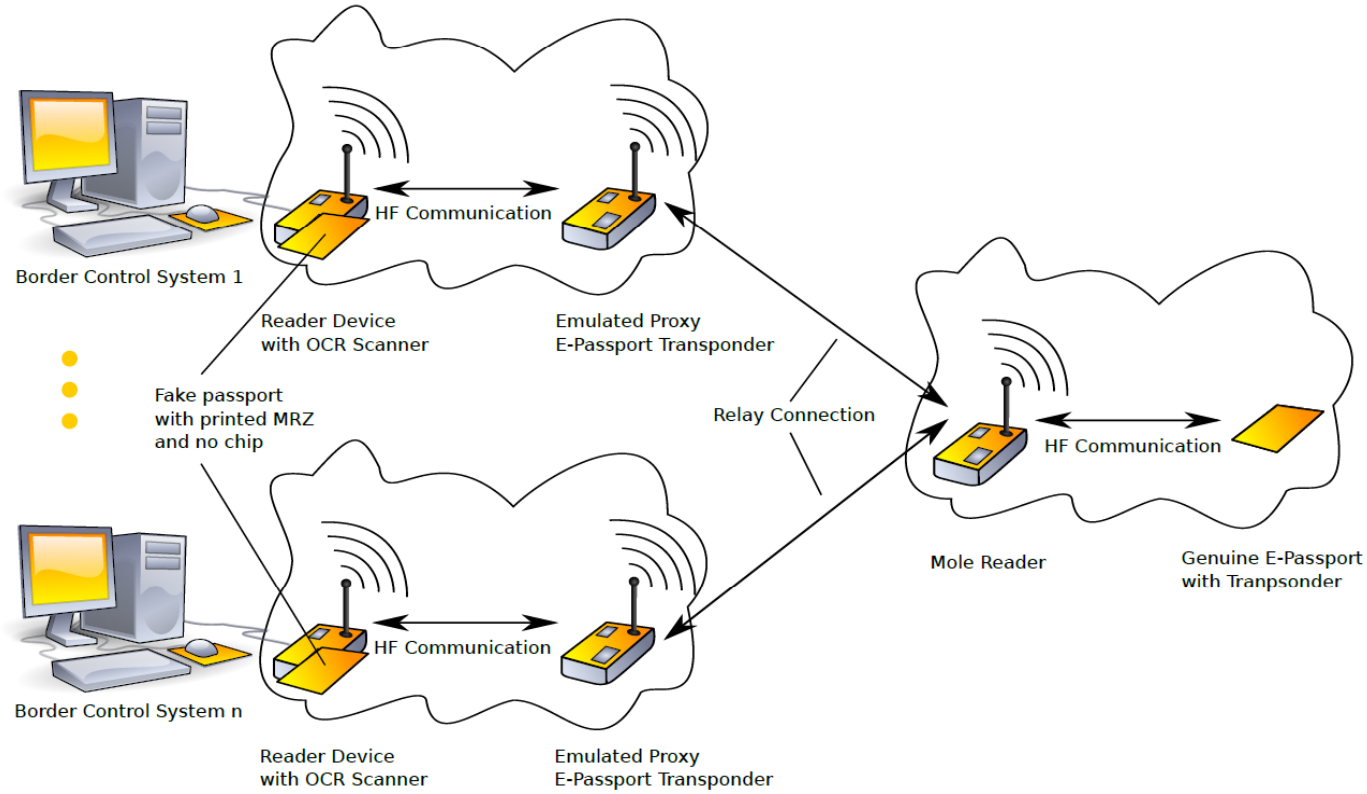


Fig. 1. P2P Relay Setup using Bluetooth.

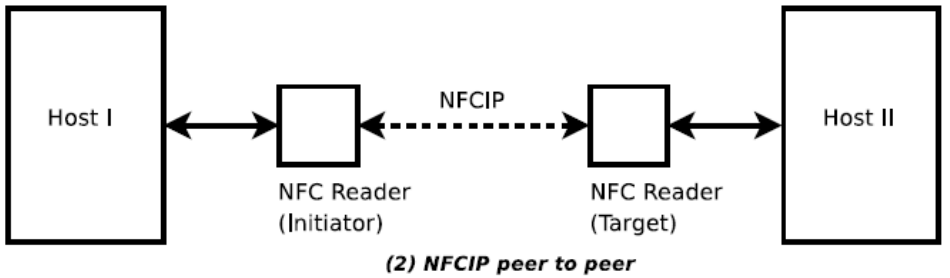
Ataki typu RELAY 2

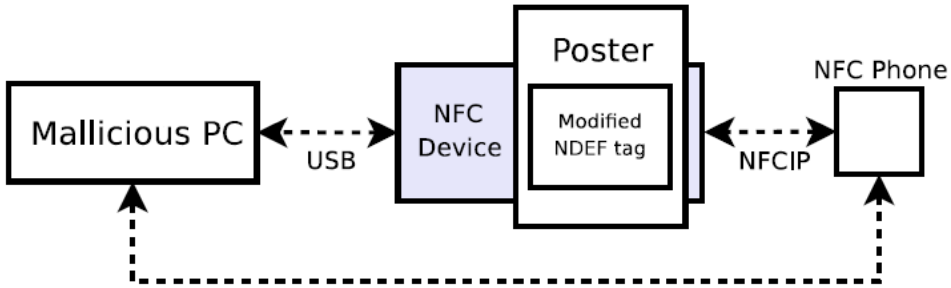
„Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment” - Michael Weiß



Atak najciekawszy - kombinowany

„*Practical attacks on NFC enabled cell phones*” - Roel Verdult, François Kooman





- Dostęp do całej pamięci telefonu
- Nadawanie uprawnień aplikacjom

Podsumowanie

- NFC – nowy, wszechstronny, rewolucyjny
- Nadal mało telefonów
- Ataki związane z:
  - Interfejsem użytkownika
  - Błędami logicznymi w oprogramowaniu
  - Wszechstronnością ataków RELAY
- Nowy standard umożliwiający podpisywanie tagów

Pytania?