Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

ÚJ SZÉCHENYI TERV

RFID RELAY ATTACK

Átjátszásos támadás az RFID technológiában

2013.06.17 Workshop Eger, EKF TTK MatInf

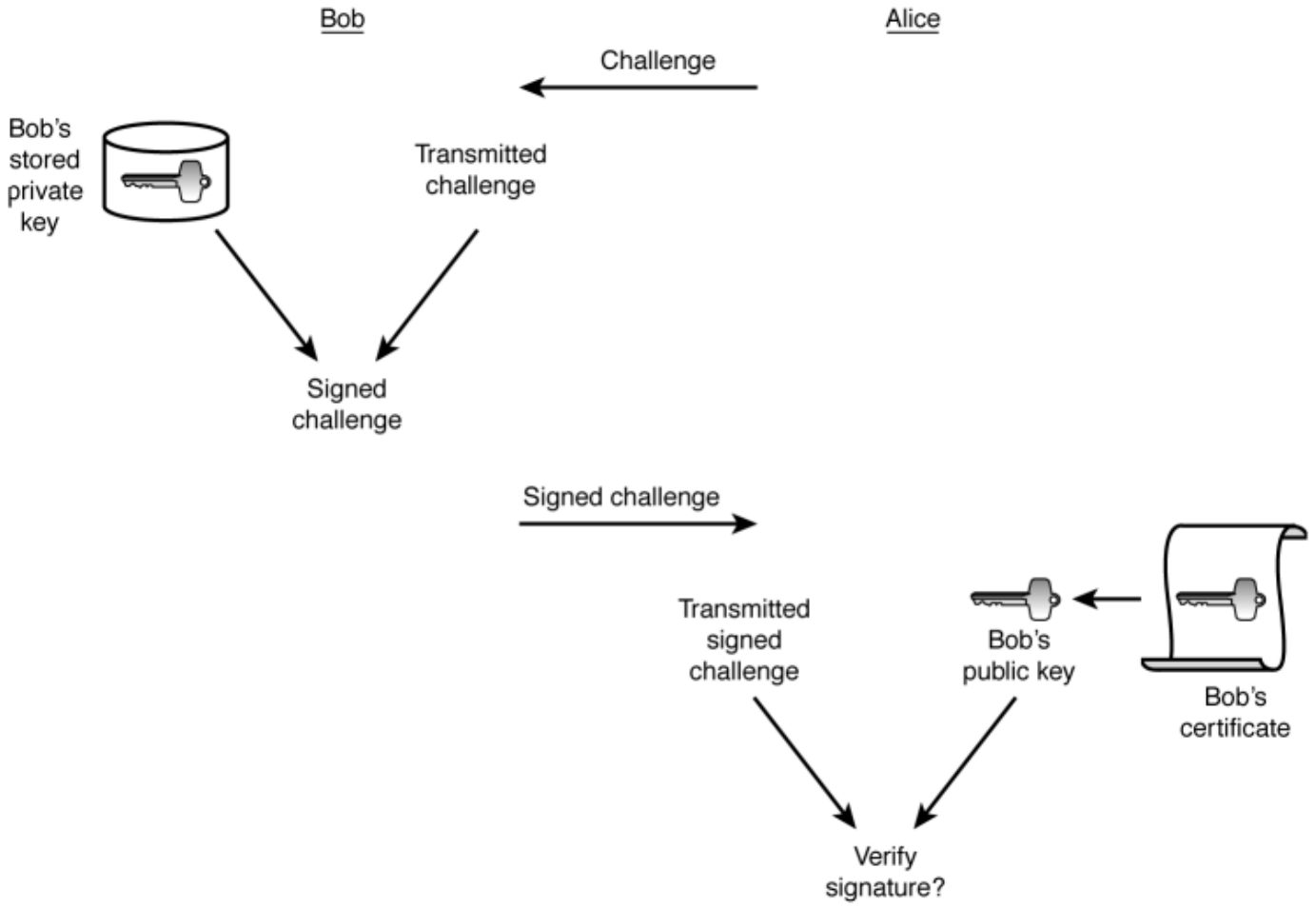
Tartalom

- Secure NFC
- A kommunikációt célzó Támadási formák
- A relay attack
- Védekezési javaslatok

Near Field Communication

- Tulajdonságok
  - Kis mennyiségű adatcsere
  - Távolság <10cm
  - A hatótávon belül leolvasás lehet automatikus
  - Gyakran hitelesítésre
- Megvalósítás
  - Secure Smart Card + NFC = Secure NFC
  - App + NFC képes Okos telefon

Hitelesítés Smart Carddal



Támadási formák

- Jól védhető
  - Adat manipuláció
  - Lehallgatás
  - Men In The Middle
- Problémás
  - DoS
- Veszélyes
  - Relay Attack

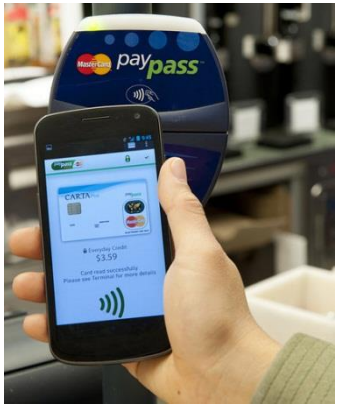
Relay Attack

- Cél
  - A leolvasási távolság megnövelése
- Nem cél
  - A lehallgatás
  - Az adatok módosítása

NFC megvalósításai

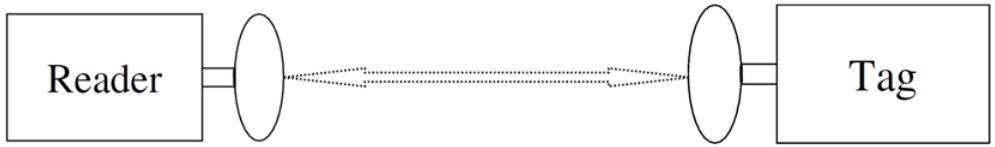
Secure NFC

NFC képes Okostelefon

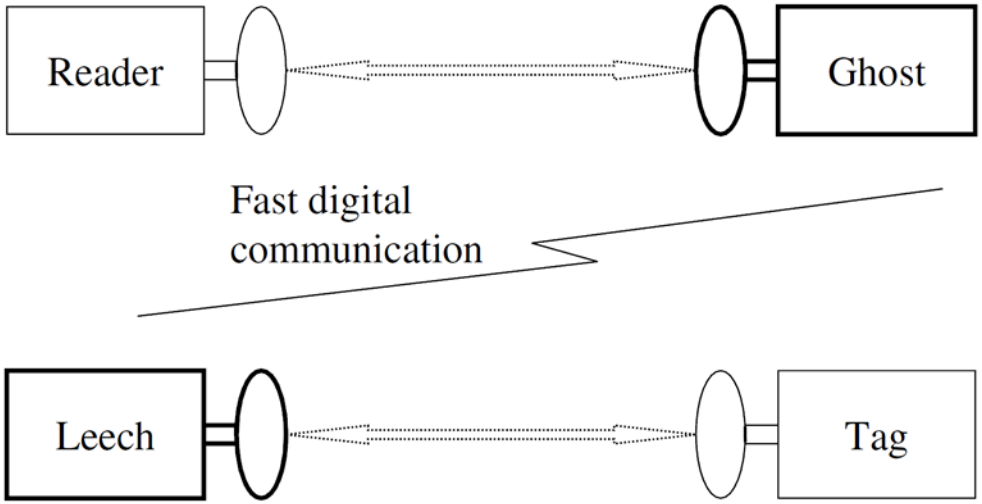


Relay Attack – NFC -n keresztül

Normál leolvasás:



Relay Attack:



Relay Attack a gyakorlatban

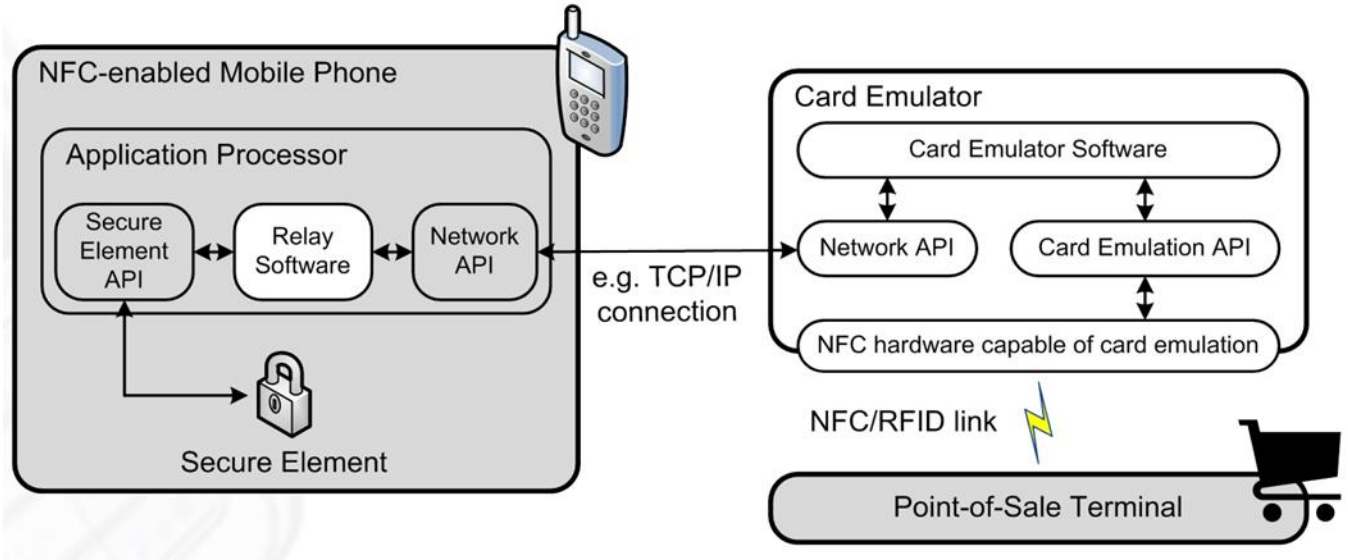
Reader + Ghost

Leach + Tag

A Leach szerepét saját feltört mobiltelefonunk is játszhatja!

Relay Attack - Okostelefonon

- A telefonon nem történik RFID olvasás
- A szoftvernek elég a telefon biztonsági rendszerét kijátszani



Megvalósítási különbségek

Secure NFC

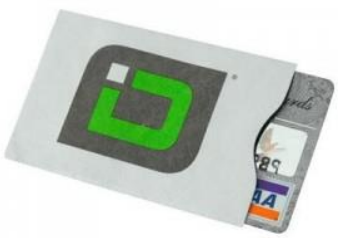
- A chip közelében kell lenni
- A leolvasási távolság megnövelhető kb 1m
- Két támadó

NFC képes Okostelefon

- Nem szükséges a közelség
- Telepített szoftver + jogosultság
- Egy támadó

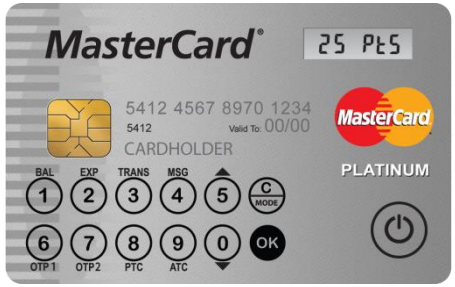
Védelem – Secure NFC

Speciális tároló



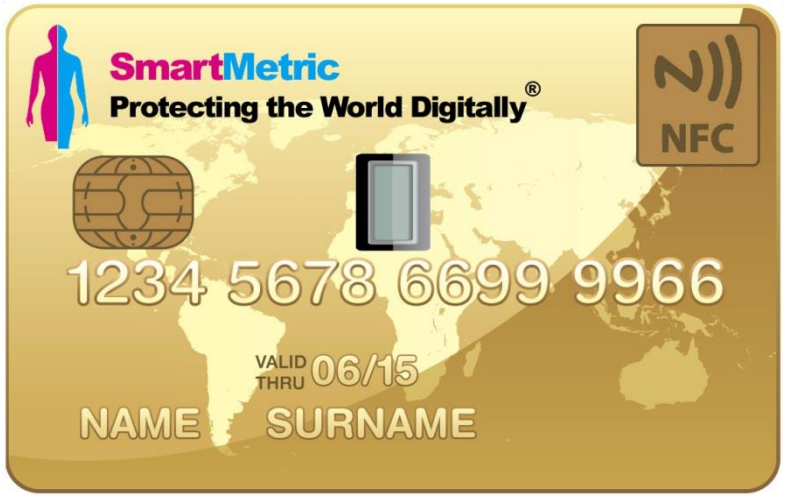
Interakció

Blockoló Tag



Védelem – Secure NFC

Lehetséges irány: Biometrikus azonosítás hozzáadása



Mobil védelem

- Interakció: Pin kód
- Biztonsági frissítések
- Vírusírtó
- Tűzfal

Mobil védelem

- Lehetséges irány: Védett tároló
- Külső kártyaolvasóhoz hasonlóan működhetne
- Kívülről csak írható tároló
- Olvasni, csak a külön hardwerben lévő szoftver tudná
- A leolvasás újlenyomat ellenőrzéssel történhet

Köszönöm a figyelmet!