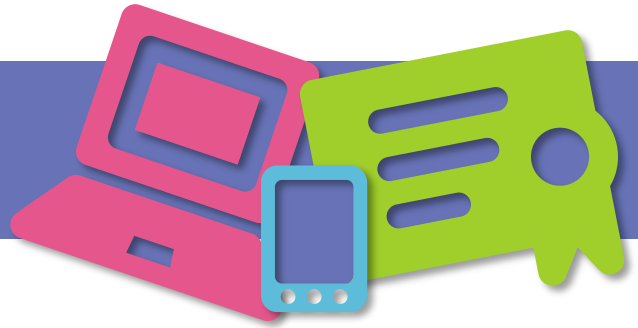
SECURITY 2014
22. ročník konference o bezpečnosti v ICT



Bezpečnost platebních systémů založených na čipových kartách

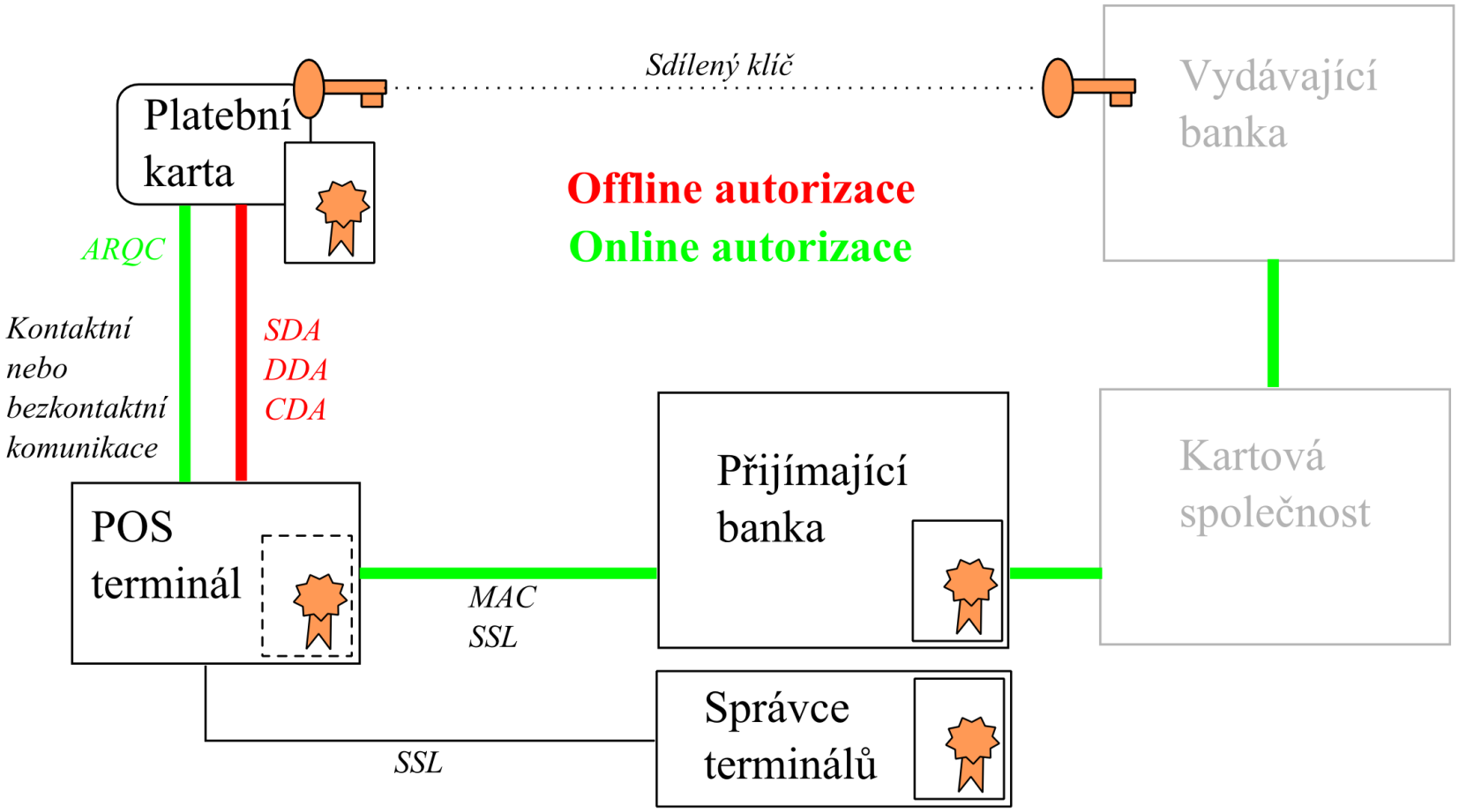
Martin Henzl

Vysoké učení technické v Brně

Platební systémy

- EMV
  - Europay, MasterCard, VISA
  - „Chip and PIN“
  - Standard definující komunikaci mezi terminálem POS a platební kartou
  - Zabezpečuje:
    - Risk management
    - On-line autentizaci
    - Off-line autentizaci
    - Ověření držitele karty (CVM)
    - Offline autorizaci
- Banka zajišťuje
  - Implementaci EMV
  - Komunikaci mezi terminálem a autorizačním centrem
  - SW v terminálech a bankomatech

Schéma platebního systému

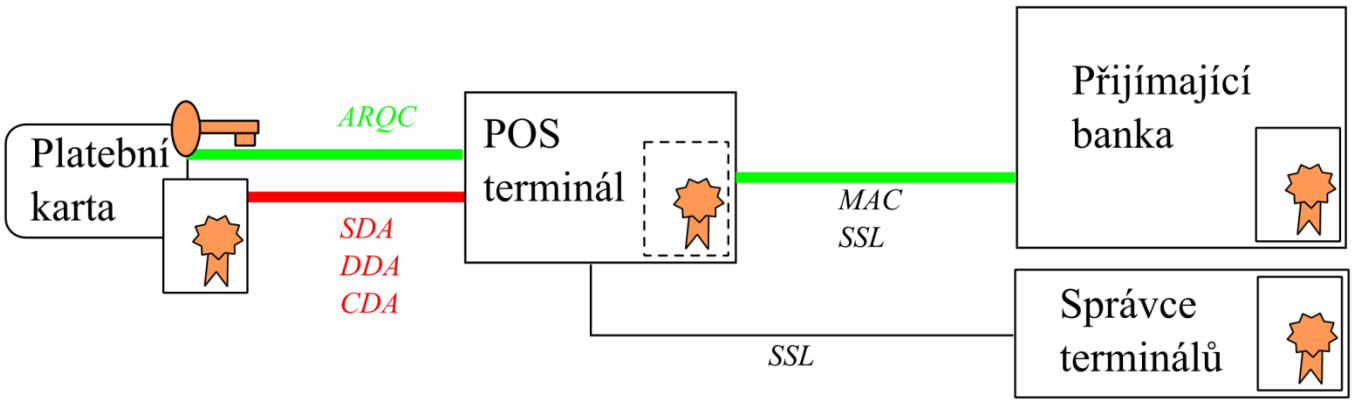


Platební transakce

- EMV transakce má 3 fáze:
  - Autentizace karty (CAM)
    - SDA – statická autentizace
    - DDA – dynamická autentizace
    - CDA – kombinovaná autentizace
  - Ověření identity držitele karty (CVM)
    - PIN (online, offline)
    - Podpis
    - žádné ověření
  - Autorizace transakce bankou

Zranitelná místa

- Komunikace banka – terminál
  - Není součástí EMV
  - SSL není povinné
  - Integrita zpráv chráněna pomocí MAC
- Komunikace terminál – karta
  - U bezkontaktních karet bezdrátový přenos



Útok „No PIN“

- Man-in-the-middle
- Útočník odpoví terminálu, že PIN je OK (0x9000)
- Před kartou útočník předstírá, že PIN je verifikován jiným způsobem
- Útok využívá toho, že odpověď karty není při offline ověřování PINu autentizována
- Zdroj: Murdoch, Drimer, Anderson, Bond. *Chip and PIN is broken*. In IEEE Symposium on Security and Privacy, 2010.

Pre-play útok

- Nahrání odpovědí ARQC karty na náhodné výzvy terminálu předem
- Pozdější přehrání odpovědi na náhodnou výzvu, kterou útočník očekával a předem si nahrál
- Téměř stejně účinné jako naklonování karty
- Omezení
  - Datum musí být zvoleno předem
  - Musí být předem znám stát, kde bude útok proveden
  - Suma musí být zvolena předem
- K provedení útoku pomůže:
  - Malware
  - Obchodník spolupracující s útočníky
  - Spolupracovník v dodavatelském řetězci
  - Man-in-the-middle mezi POS a bankou
  - Slabý generátor náhodných čísel
- Zdroj: Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson. *Chip and Skim: Cloning EMV cards with the pre-play attack*. 2012.

Slabý generátor náhodných čísel

- Velmi slabé generátory
  - Čítače
  - Hodiny
  - Amatérské algoritmy
- Jednoduché generátory
  - Rand()
- Generátory, které je možné uvést do předvídatelného stavu
  - Slabý zdroj náhodnosti
  - Data z předchozích transakcí
  - Zdroj náhodnosti se restartuje při každém spuštění

Útoky na čipové karty

- Fyzické útoky
- Logické útoky
  - Útoky pomocí postranních kanálů
    - Odběrová analýza
    - Časová analýza
    - Chybová analýza
    - Elektromagnetická analýza
  - Útoky na API

Bezkontaktní čipové karty

- Komunikace pomocí modulace elektromagnetických vln
- Vzájemná indukčnost
- Amplitudová modulace, zátěžová modulace
- ISO/IEC 14443, Mifare, ISO 15693, FeliCa
- 13,56 MHz
- 106-848 kbit/s

Zabezpečení bezkontaktních plateb

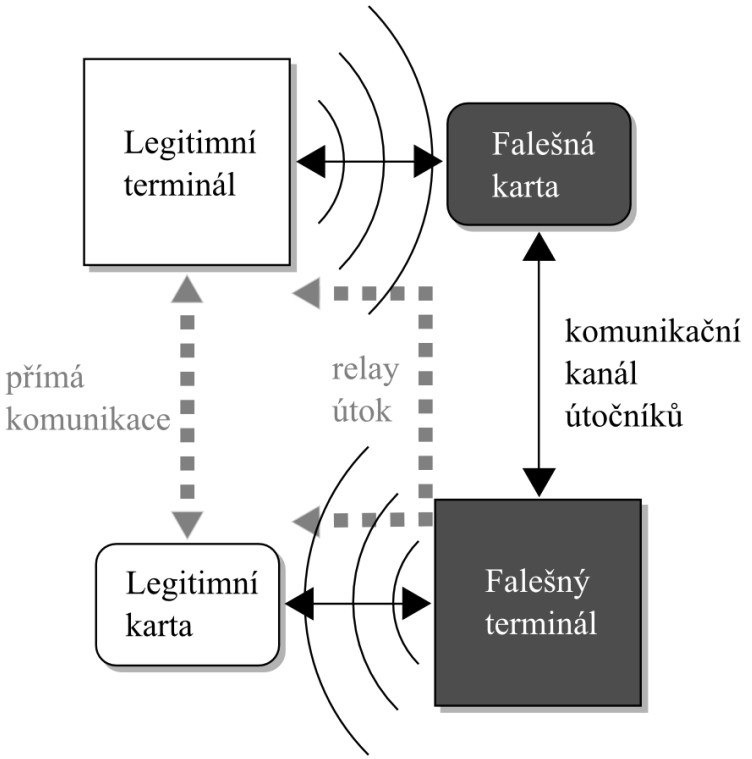
- Offline
  - Bez zadání PINu
  - DDA
    - Chrání před klonováním karty
  - V případě překročení některého z limitů na kartě se provede transakce online
    - Limit na jednu transakci
    - Kumulativní limit všech transakcí
- Online
  - Při překročení některého limitu
  - Téměř stejné jako u kontaktních karet
  - Se zadáním PINu
  - Bez zadání PINu

Zranitelnosti bezkontaktní kom.

- Odposlech
  - Šifrování
- Detekce a čtení bez vědomí uživatele
  - Faradayova klec
- Útok Relay
  - Distance bounding protocol
- Útok DoS
  - Faradayova klec
  - Zničení čipu
- Útok Man-in-the-middle
  - Téměř neproveditelný
- Přerušení operace
  - Backup, backtracking
- Utajené transakce
  - Silná obousměrná autentizace, interakce uživatele

Relay útok

- Terminál komunikuje s kartou přes 2 útočníky
  - Jeden útočník má falešný terminál a komunikuje s legitimní kartou
  - Druhý útočník má falešnou kartu a komunikuje s legitimním terminálem
  - Veškerou komunikaci si přeposílají
- Terminál ani karta nemohou útok zjistit
- Útočníci mohou provést man-in-the-middle
- Ochrana: Distance bounding protokoly



SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Martin Henzl

VUT Brno

ihenzl@fit.vutbr.cz