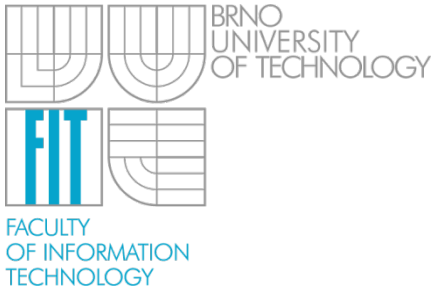
Čipové karty

Martin Henzl

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 2, 612 66 Brno
ihenzl@fit.vutbr.cz



12.11.2014

Obsah

- Úvod
- Čipové karty
  - Architektura
  - Komunikace
  - Bezkontaktní rozhraní
- Útoky
  - Fyzické, logické
  - Postranní kanály
  - Útoky na API
- Elektronické pasy
- Near Field Communication

Úvod

- Co jsou čipové karty a k čemu je potřebujeme?
- Cíle
  - Autentizace
  - Důvěrnost
  - Integrita
- Aplikace
  - Bankovnictví
  - Telekomunikace
  - Přístupové systémy
  - Bezpečné uchování kryptografických klíčů
  - Kryptografické operace

Fyzická bezpečnost

- Tamper evidence
  - Mechanismy, které zanechávají důkazy
- Tamper resistance
  - Odolné materiály, ochranné kryty
- Tamper detection
  - Speciální senzory
- Tamper response
  - Zničení paměti

Standardy

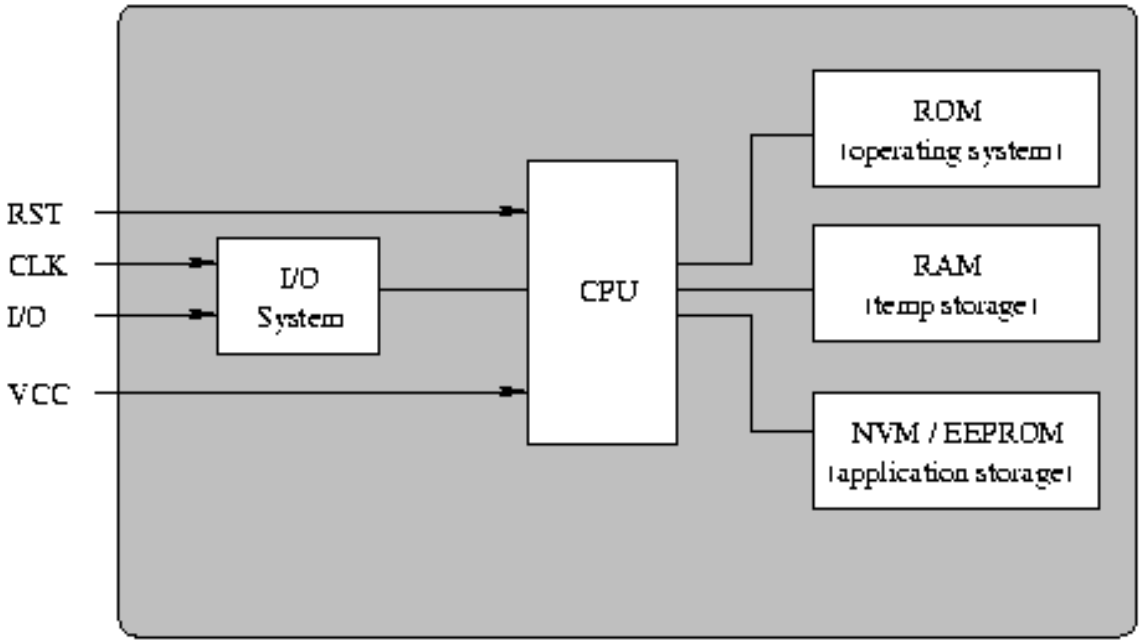
- **FIPS 140-1/2/3**
  - Kryptografické moduly
    - Specifikace
    - Porty a rozhraní
    - Role, služby, autentizace
    - Stavový model
    - Fyzická bezpečnost
    - Operační prostředí
    - Správa klíčů
    - Elektromagnetická kompatibilita
    - Atd.
- **ISO/IEC 7810**
  - Fyzická charakteristika, 4 typy
  - Platební karty, identifikační karty, SIM karty
- **ISO/IEC 7816-1/2/3/4**
  - Fyzická charakteristika
  - Rozměry a umístění kontaktů

  - Komunikační protokoly
    - T=0 – bytově orientovaný protokol
    - T=1 – blokově orientovaný, asynchronní, half-duplex
  - Organizace, bezpečnost, příkazy a odpovědi

Typy čipových karet

- Dle integrovaných obvodů:
  - Paměťové karty
    - Straight Memory Cards
    - Protected Memory Cards
    - Stored Value Memory Cards
  - Mikroprocesorové karty
    - Operační systém
    - Kryptografické funkce
    - Virtual Machine (Java Card)
- Dle komunikačního rozhraní:
  - Kontaktní
  - Bezkontaktní
  - Hybridní
  - Dual-Interface
  - Multi-component
- Form Factor
  - ISO 7810 (Platební karty, Občanské průkazy, SIM karty, …)
  - SD a Micro SD karty
  - USB Token

Architektura



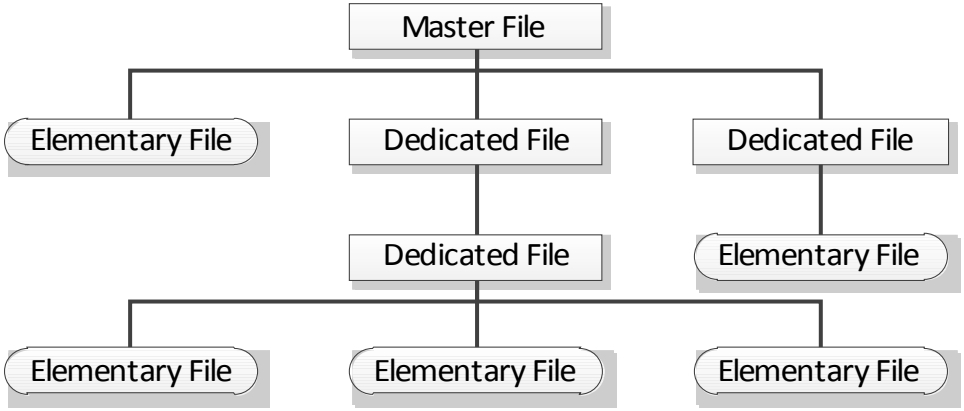
- Kryptografické čipové karty jsou vybaveny kryptografickým koprocesorem

Čip a operační systém

- Čip
  - Podpora kryptografických operací
    - Symetrická kryptografie
    - Asymetrická kryptografie
  - Tamper-resistance
    - Ochranný kovový kryt
    - Nepravidelné rozmístění obvodů
- Operační systém
  - Pevná souborová struktura
  - Dynamická struktura – systém aplikací

Operační systém

- Operační systémy většiny čipových karet podporují množinu standardních příkazů (20-30)
- Filesystem
  - Stromová struktura
  - Autorizace (u každého souboru zvláštní seznam oprávnění)
  - Typy souborů: Linear, Cyclic, Transparent, SIM
  - Operace: Create, Delete, Read, Write, Update
  - PIN

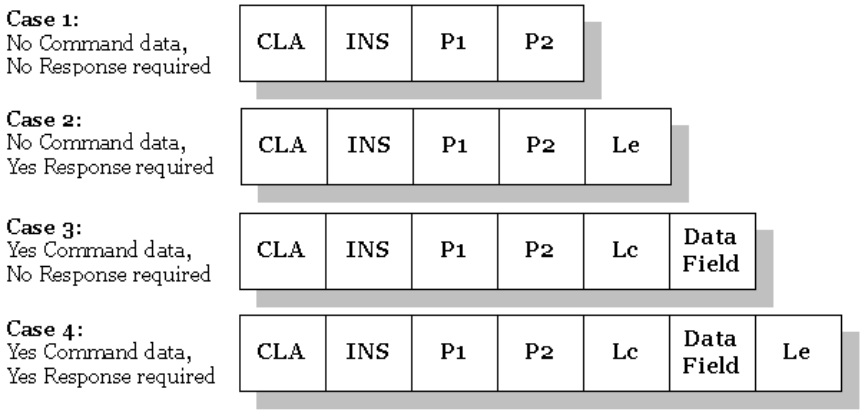


- Java Cards
  - Java applety
  - SIM karty, platební karty

APDU

- Application Protocol Data Unit
- Komunikační datagram
- Až 255 bytů dat ve směru od čtečky ke kartě
- Až 256 bytů dat z karty

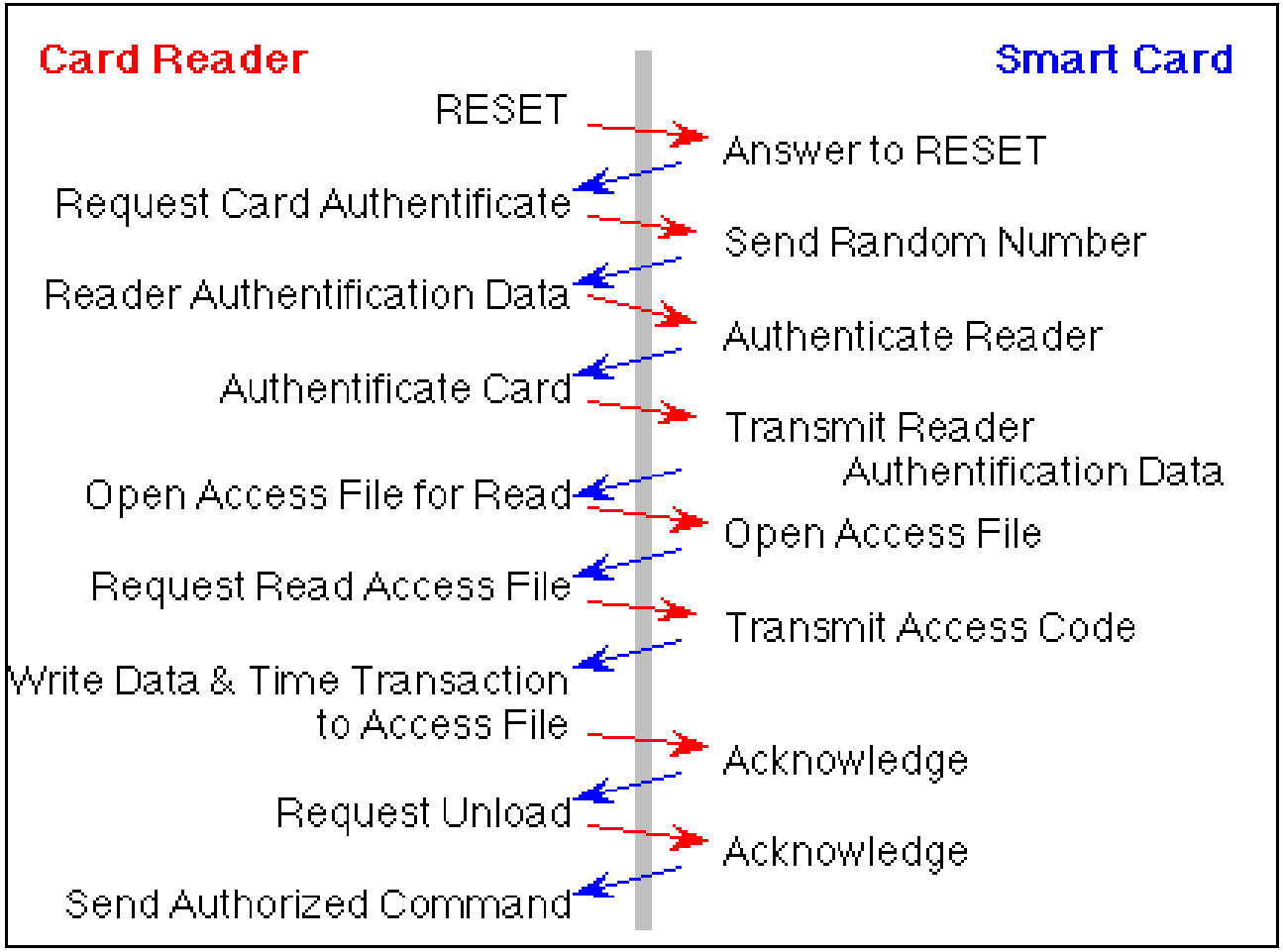
- APDU příkaz:
  - CLA – třída instrukce
  - INS – číslo instrukce
  - P1, P2 – volitelná data
  - Lc – délka dat
  - Le – očekávaná délka dat



- APDU odpověď karty:
  - Le bytů dat
  - 2 status bytes (0x90 0x00 = OK)

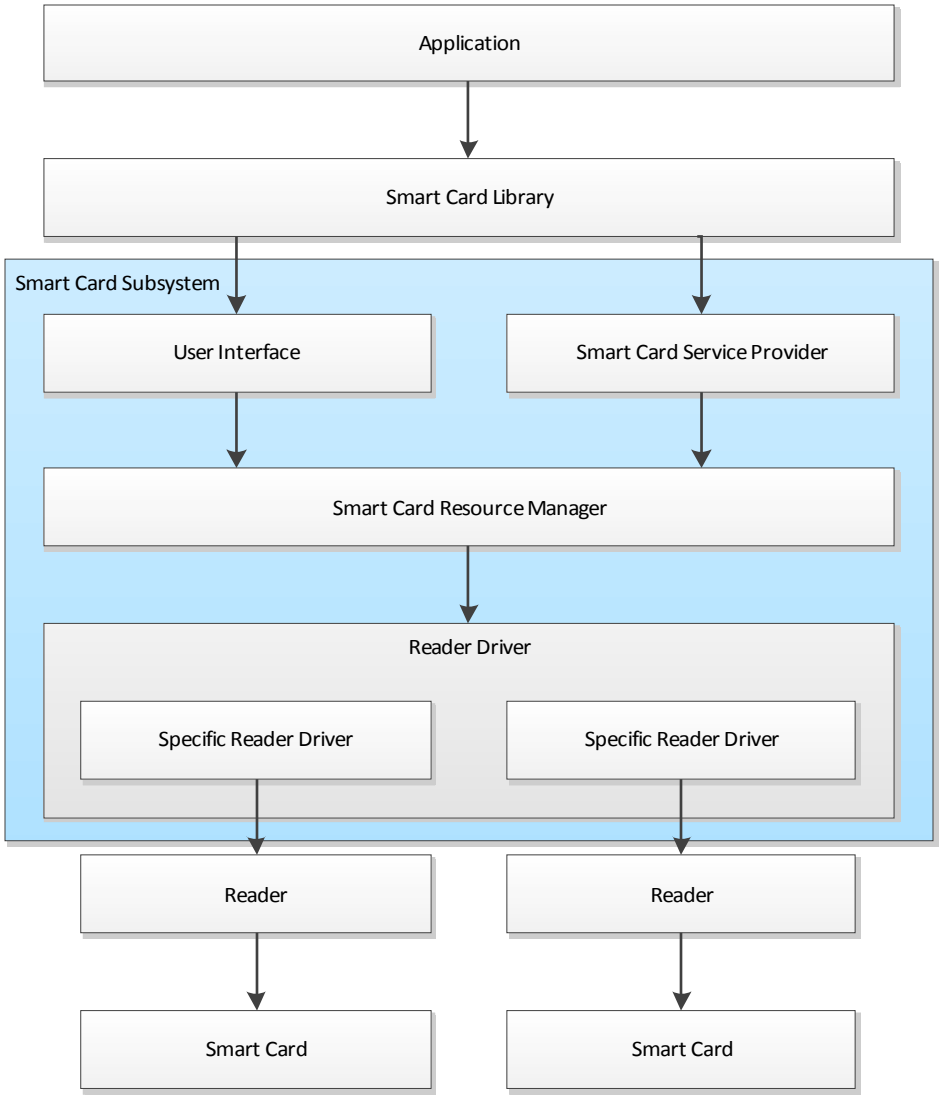
Příklad komunikace

- Handshaking protocol



Komunikace s čipovou kartou

- Rozhraní
  - Proprietární SDK
  - PC/SC – Personal Computer/Smart Card
    - Specifikace integrace čipové karty do systému



API

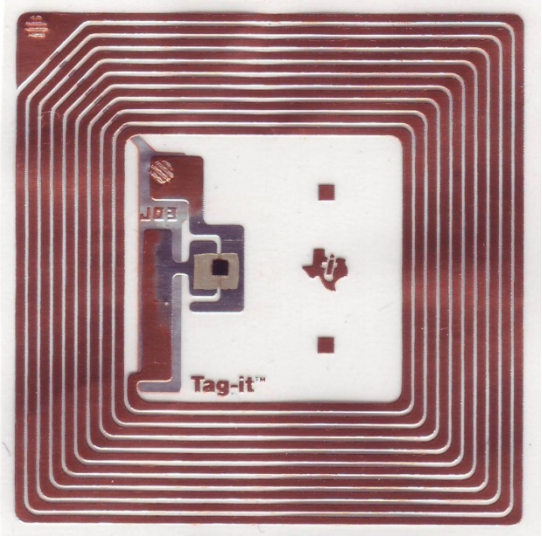
- **Public Key Cryptographic Standard #11 (PKCS #11)**
  - Abstraktní vrstva pro obecný kryptografický hardware
  - API nezávislé na platformě
    - Čipové karty
    - Kryptografické tokeny
    - Hardware security module (HSM)
  - Nejčastěji používané typy kryptografických objektů
    - RSA klíče
    - X.509 certifikáty
  - Funce:
    - Vytvořit, změnit, smazat objekty
    - Šifrovat/dešifrovat
    - Podepsat/ověřit
- **Microsoft CryptoAPI (MS-CAPI)**
  - Cryptographic Service Provider (CSP) – softwarová knihovna
  - CSP vybráno na základě analýzy Answer to Reset (ATR)

Čipové karty v PKI

- PKI entity
  - Certifikační autorita (CA)
  - Registrační autorita (RA)
  - Koncový uživatel (nebo zařízení)
- Čipová karta
  - Bezpečné úložiště citlivých dat
  - Čipová karta je použita koncovým uživatelem pro:
    - Vygenerování páru klíčů
      - Soukromý klíč nemůže opustit kartu
    - Podepsání Certificate Signing Request (CSR)
    - Uložení certifikátů
      - Certifikát kořenové certifikační autority (read-only)
      - Vlastní certifikát
    - Autentizaci
    - Podepisování
    - Šifrování/dešifrování

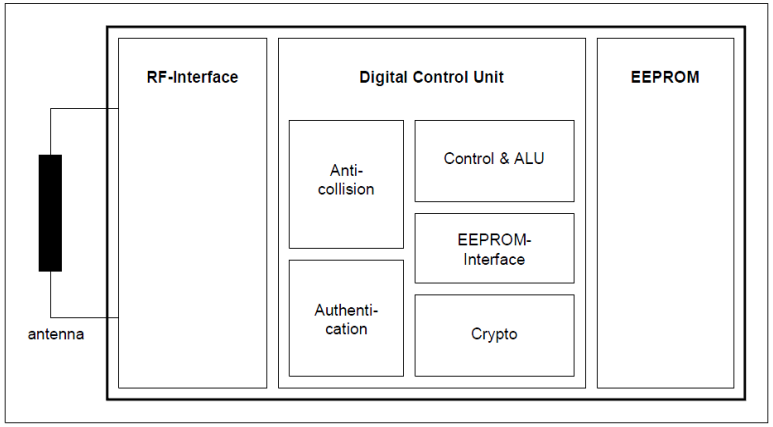
RFID

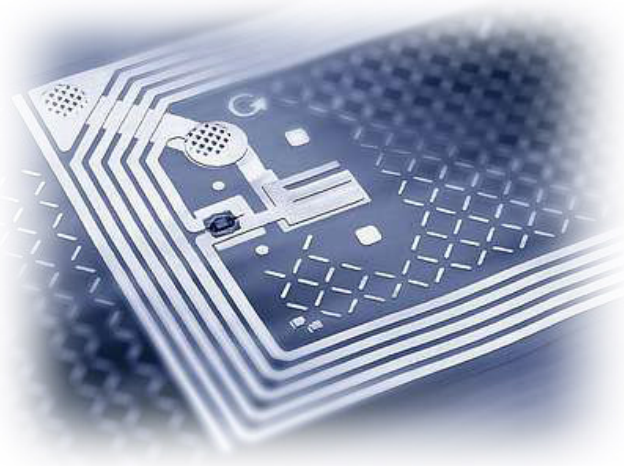
- Radio-frequency identification
- Komunikace pomocí modulace elektromagnetických vln
- Vzájemná indukčnost
- Amplitudová modulace, zátěžová modulace



Bezkontaktní čipové karty

- ISO/IEC 14443, Mifare, ISO 15693, FeliCa
- 13,56 MHz
- 106-848 kbit/s
- Antikolizní procedura
- Aplikace
  - Platební karty, elektronické pasy, identifikační karty, hromadná doprava, vstupenky





Mifare Classic

- Nejrozšířenější bezkontaktní čipová karta
- Proprietární šifrovací algoritmus Crypto-1
  - 48 bitový šifrovací klíč
  - Je možné ho prolomit během několika vteřin
- Slabý PRNG
- 2007 – úspěšně proveden útok založený na reverzním inženýrství
- Dva módy:
  - Unikátní UID
  - Kryptografický (s obousměrnou autentizací)

Mifare DESFire

Bezkontaktní paměťová karta, nást. Mifare Classic

Šifrovací algoritmy DES, 3DES, AES

Až 32 aplikací, každá aplikace až 14 klíčů

UID, vzájemná trojcestná autentizace

Komunikace probíhá na třech úrovních bezpečnosti

- prostý text
- prostý text s MAC
- šifrovaný text

Java Card

Bezkontaktní procesorová karta

Umožňuje běh vlastních aplikací – Java Applet

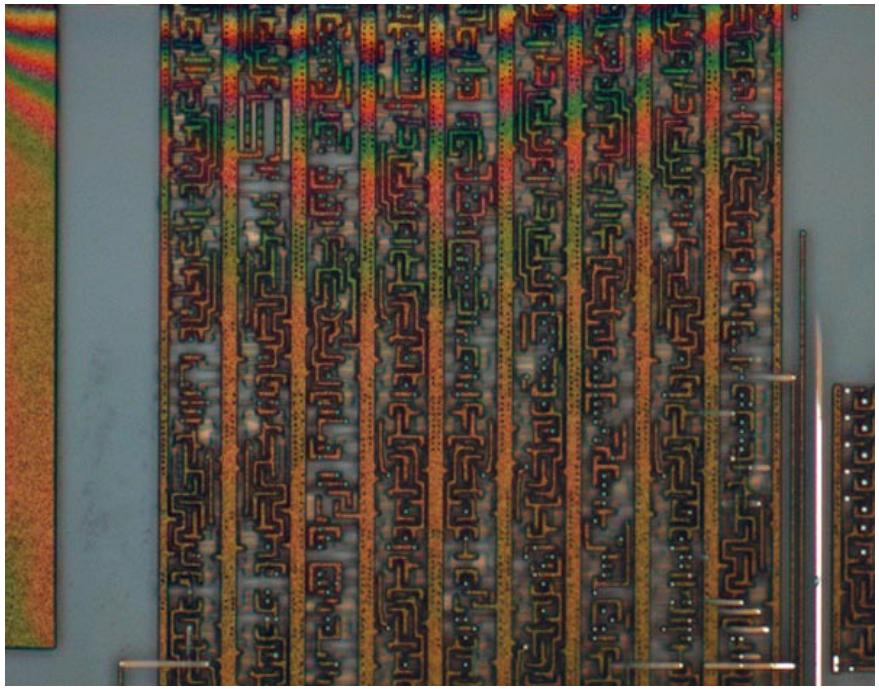
Složitější, potenciálně více chyb v aplikacích

Útoky na čipové karty

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

Fyzické útoky

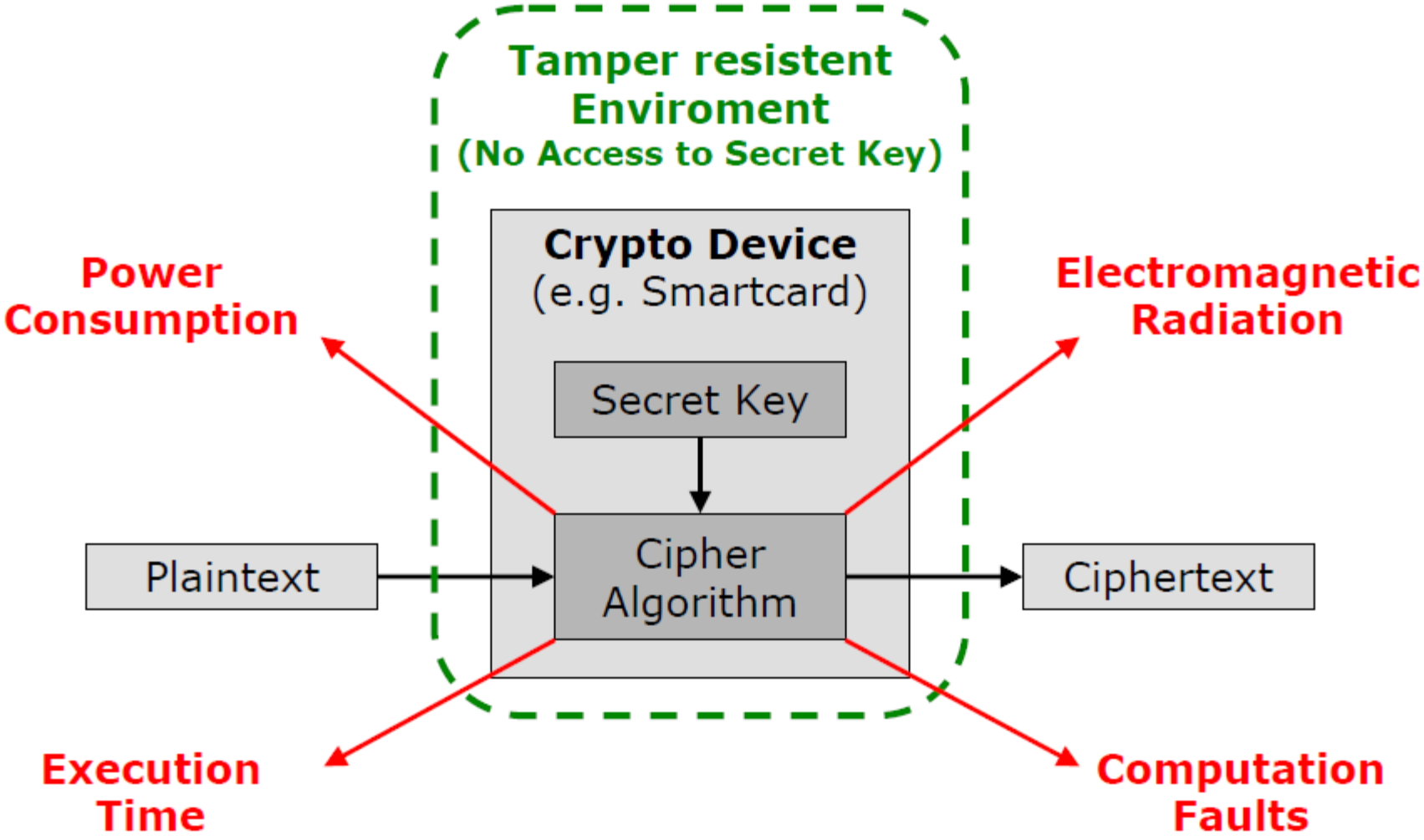
- Mikrosonda
- Reverzní inženýrství
- Rozebrání čipu



Logické útoky

- Bez fyzického poškození zařízení
- Monitorování
- Útoky využívající postranních kanálů
  - Časová analýza
  - Odběrová analýza
  - Chybová analýza
  - Elektromagnetická analýza
- Útoky na API

Postranní kanály



Bezpečnostní API

- Bezpečný HW obsahující citlivá data musí komunikovat s nedůvěryhodným okolím
- Citlivá data nesmí opustit bezpečné prostředí
- Musí poskytovat služby nezabezpečenému okolí
- Bezpečnostní API je rozhraní pro komunikaci bezpečného HW s okolím, které musí splňovat další bezpečnostní cíle
- Navrženy tak, aby mohly komunikovat s potenciálním útočníkem

Útoky na bezpečnostní API čipových karet

- Původně analyzovány ručně
- Automatická analýza
- Současné útoky nevyužívají jeden příkaz na zjištění celé tajné informace naráz, ale využívají úniku informace z nějaké odpovědi
- Po aplikaci několika takových příkazů s různými parametry získá útočník dostatečně mnoho informací o tajných datech
- Problémy kryptografických API:
  - Nedostatečné zajištění integrity klíčů
  - Nedostatečná kontrola parametrů funkcí
  - Nedostatečné prosazování bezpečnostní politiky

Příklad útoku na bezpečnostní API

PIN Verifikace v HSM

Útok pomocí decimalizační tabulky

PIN je spočítán z čísla účtu

první čtyři hex. číslice se decimalizují pomocí převodní tabulky, která se předává jako parametr:

0123456789ABCDEF

0123456789012345 6

Útočník zadá PIN 0000 a decimalizační tabulku 0100000000000000

Pokud verifikace proběhne úspěšně, útočník ví, že PIN neobsahuje číslici 1

Příklad útoku - EMV

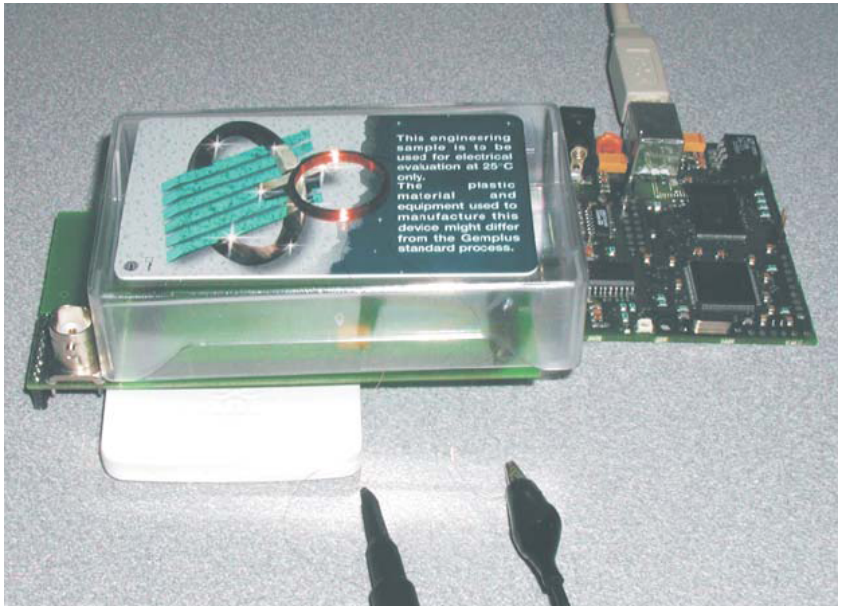
- EMV – Europay, MasterCard, VISA
- „Chip and PIN“
- 3 fáze:
  - Autentizace karty
  - Ověření identity držitele karty
    - PIN (online, offline)
    - Podpis
    - žádné ověření
  - Autorizace transakce bankou
- Útok využívá toho, že odpověď karty není při offline ověřování PINu autentizována
- Man-in-the-middle: Útočník odpoví čtečce, že PIN je OK (0x9000), před kartou předstírá, že PIN je verifikován jiným způsobem

Hrozby specifické pro bezkontaktní technologii

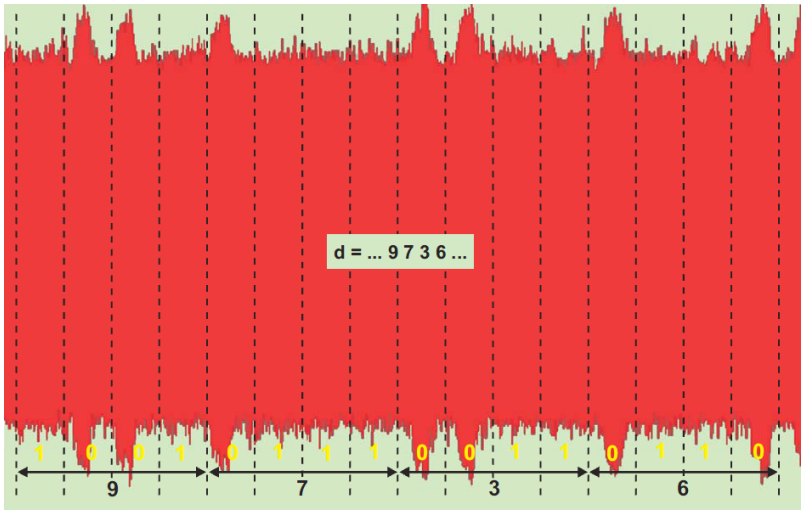
- Odposlech
  - Šifrování
- Detekce a čtení bez vědomí uživatele
  - Faradayova klec
- Útok Relay
  - Distance bounding protocol
- Útok DoS
  - Faradayova klec
  - Zničení čipu
- Útok Man-in-the-middle
  - Téměř neproveditelný
- Přerušení operace
  - Backup, backtracking
- Utajené transakce
  - Silná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

Příklad útoku (postranní kanál)

- Ananlýza elektromagnetického pole
  - Měření elektromagnetického pole obklopujícího čip
  - Magnetické pole se mění v závislosti na aktuálním odběru karty

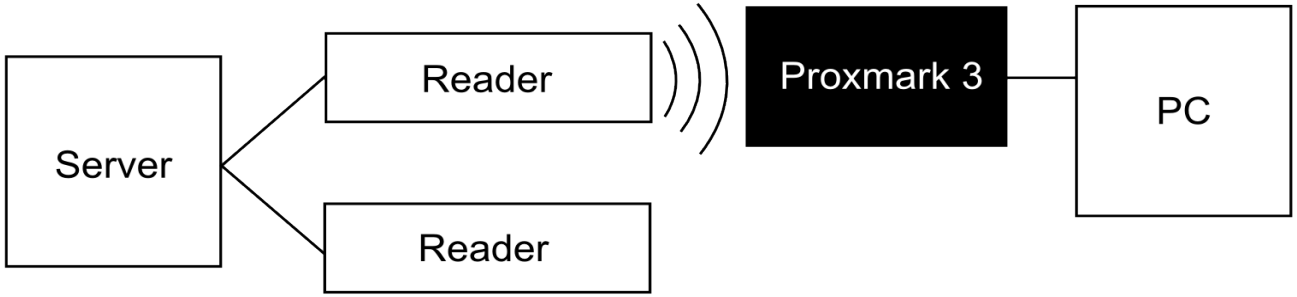



```
Input:    message m to be signed
          public RSA modulus n
          secret RSA exponent d of size k bits

Let s = m
For i = k-2 down to 0
    Let s = s^2 mod n                 /* SQUARE */
    If (bit i of d is 1)
        Then s = s x m mod n          /* MULTIPLY */
        Else s' = s x m mod n         /* DUMMY MULTIPLY */
    End if
End for

Output:   public RSA signature s = m^d mod n
```



Příklad útoku na přístupový systém

- Proxmark 3



- Přehrání antikolizní procedury

RDR: 26	REQA (7bits)
TAG: 04 00	ATQA
RDR: 93 20	SEL cascade 1
TAG: 08 ab cd ef 81	CT (1B), UID (4B), BCC (1B)
RDR: 93 70 08 ab cd ef 81 a1 ebSEL	
TAG: 09 3f cc	SAK

Elektronické pasy

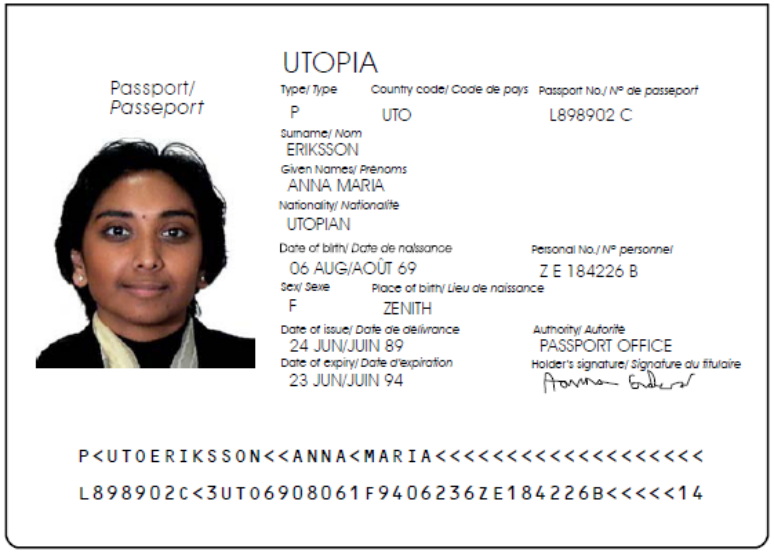
- ICAO 9303
- ISO 14443
- Asymetrická kryptografie
- Bezpečnost
  - Pasivní autentizace
  - Základní řízení přístupu
  - Aktivní autentizace

Pasivní autentizace

- Digitální podepsání všech údajů vydávající institucí
  - Bez soukromého klíče se nedá pas padělat
  - Nezabrání klonování
- Každý stát má svou národní CA
  - Podepisuje klíče CA vydávajících dokumenty
- CRL maximálně jednou za 90 dnů
  - V případě kompromitace do 48 hodin
- Povinná u všech elektronických pasů

Základní řízení přístupu

- Basic Access Control (BAC)
- Autentizace a ustavení společného šifrovacího klíče
- Klíč se získá ze strojově čitelné zóny (MRZ)
  - Číslo pasu, datum narození a datum expirace se hashuje funkcí SHA-1 (získají se dva 3DES klíče)
- Malá entropie dat z MRZ
- Povinné u pasů všech evropských zemí

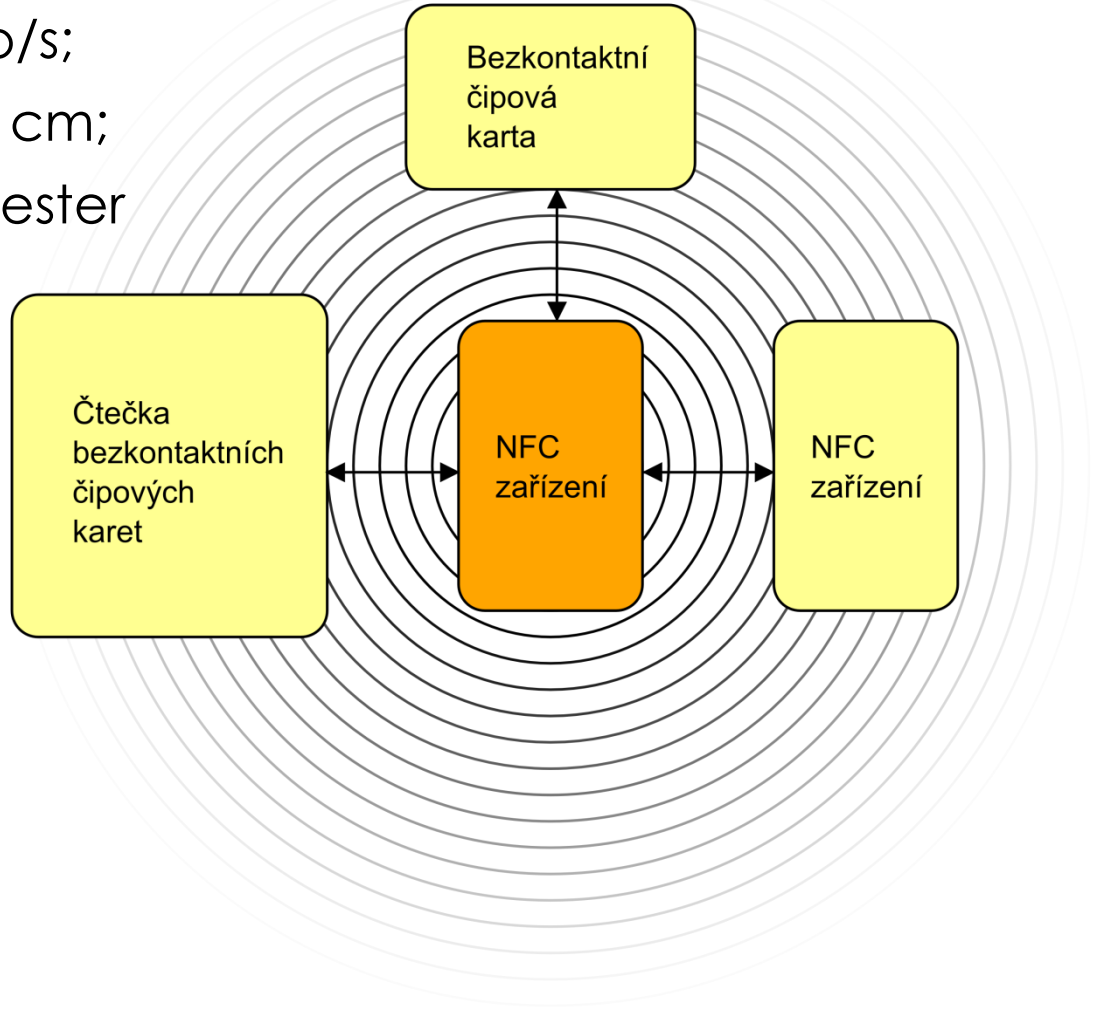


Aktivní autentizace

- Ochrana proti klonování
- Soukromý asymetrický klíč, který nikdy neopustí kartu (nelze přečíst)
- Součástí dat podepsaných CA je veřejný klíč pasu
- Protokol výzva-odpověď (challenge-response)
  - Čtečka pošle náhodné číslo, které pas dohromady s vlastním náhodným číslem digitálně podepíše
- Nepovinná, v ČR je však implementována
- Možnost relay útoku

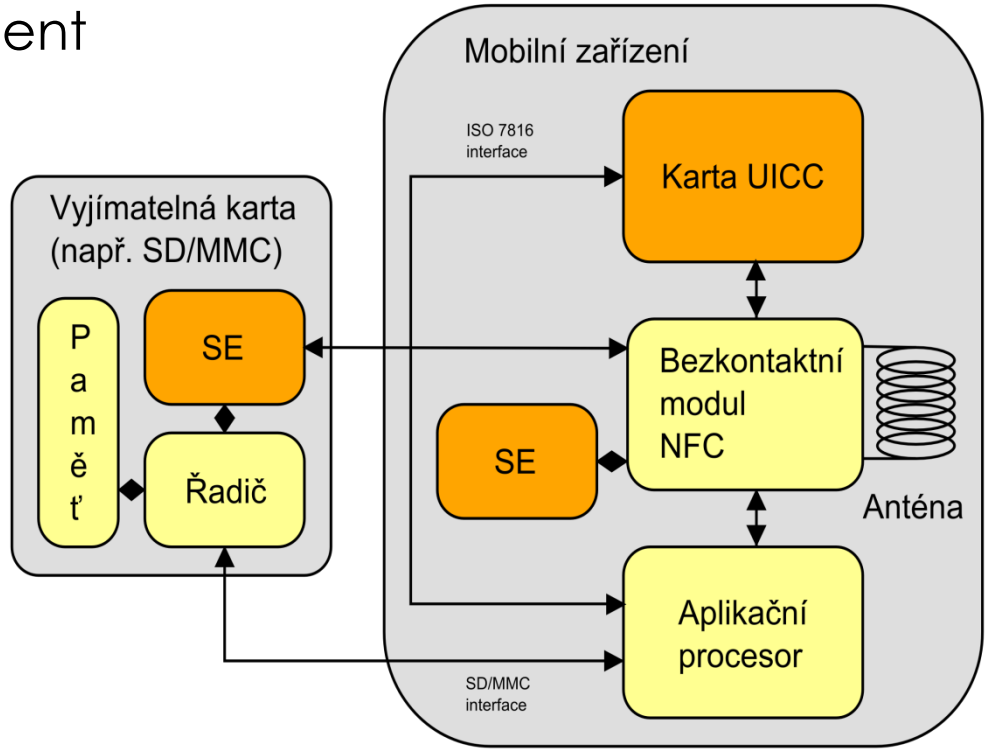
Near Field Communication

- ISO/IES 18092 a ISO/IEC 21481
- Pracovní frekvence: 13,56 MHz;
- Bitová rychlost: 106-424 kb/s;
- Pracovní vzdálenost: < 10 cm;
- Kódování: Miller a Manchester



Near Field Communication

- Secure element



- Dva pohledy na bezpečnost NFC:
  - Útoky na NFC
  - NFC zařízení jako nástroj k útoku

Otázky?

Děkuji za pozornost!