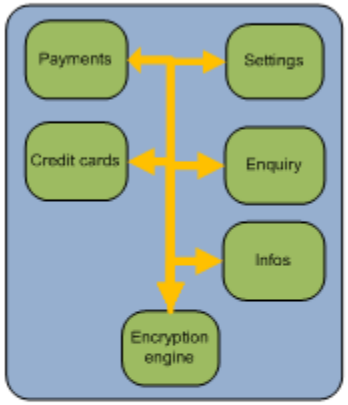
# Bezpečnosť mobilných bankových aplikácií

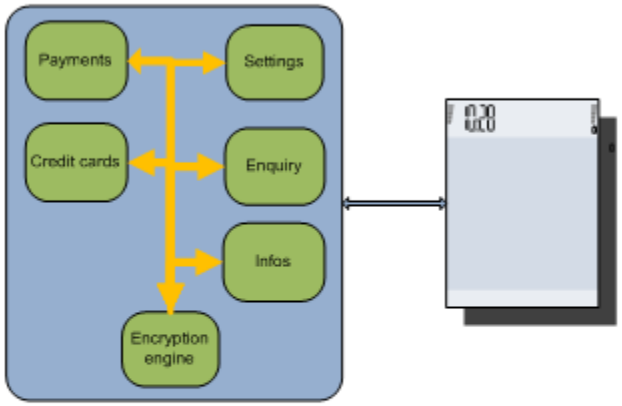

# Bezpečnosť mobilných bankových aplikácií

Ing. Peter Kopriva, Tatra banka, a.s.

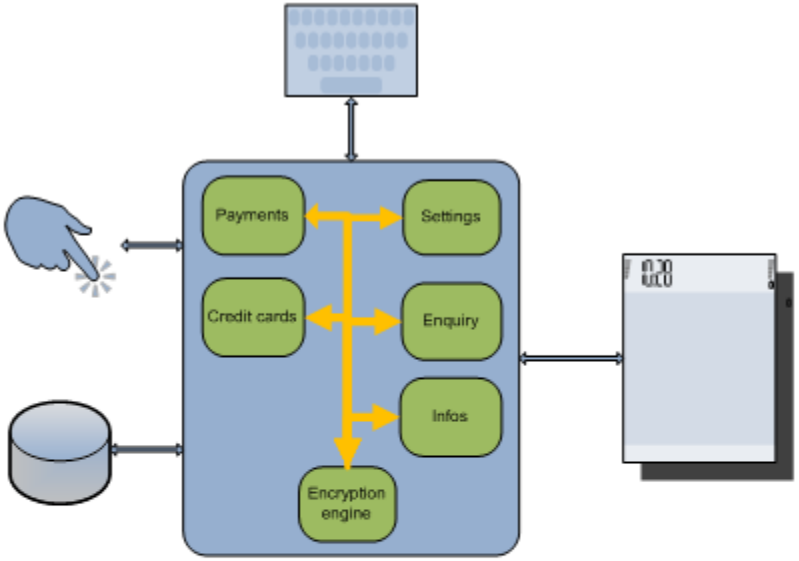
# Štandardný model



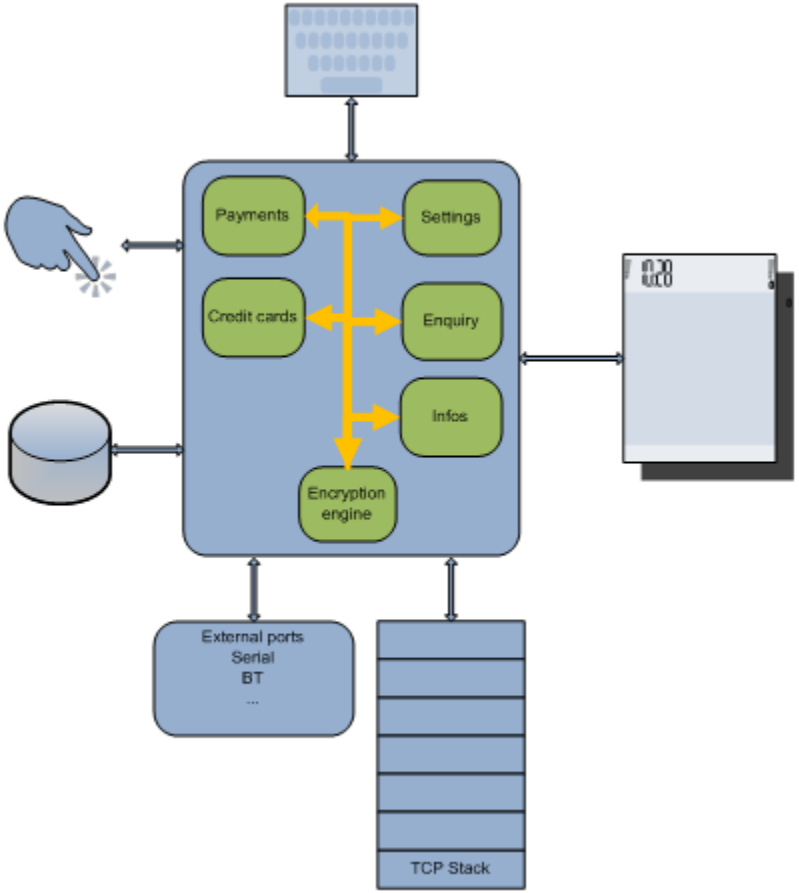
# Štandardný model



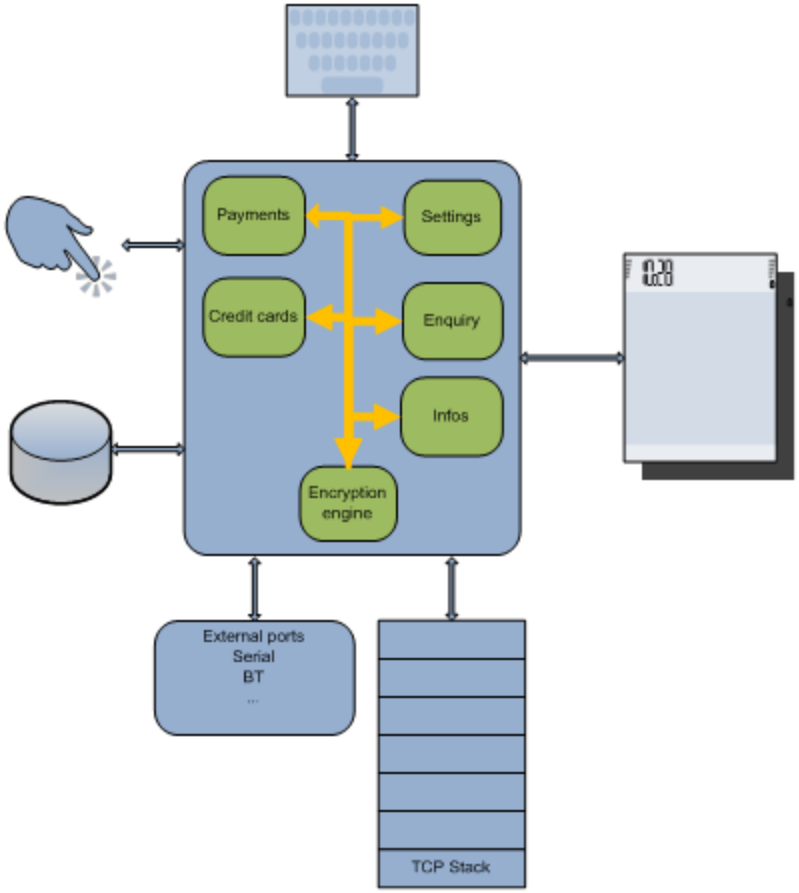
# Štandardný model

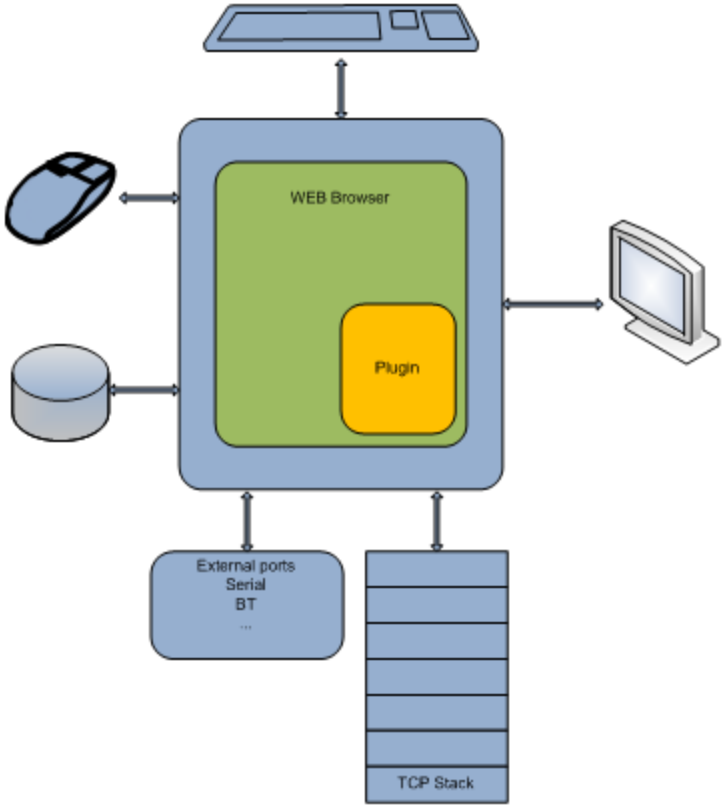


# Štandardný model



# Mobilný vs PC model



# Mobilný vs PC model

- Mobilné zariadenia sa môžu sa stratiť
  - Shared secret, ukradnuté citlivé údaje
- Stálen „ON“
  - Timeout session
- Dostupné odkiaľkoľvek
  - Risk analýza
- Rozdielna funkcionalita
  - Optimalizácia ponuky, nové možnosti (ATM lokalizácia)
- Rozdielnosť platforiem
  - Android, iOS, Windows Phone 7, Java based
- Bezpečnosť !?!
  - Autentizácia, autorizácia

# Mobilný vs PC  model

- zložitosť integrovaných obvodov sa zdvojnásobuje každých 24 mesiacov, pričom cena ostáva konštantná

  (1965 Gordon E. Moore)

- 90 roky – meno/heslo prípadne SSL
- OOB
  - GRID karty
  - SMS kód
  - TAN kód

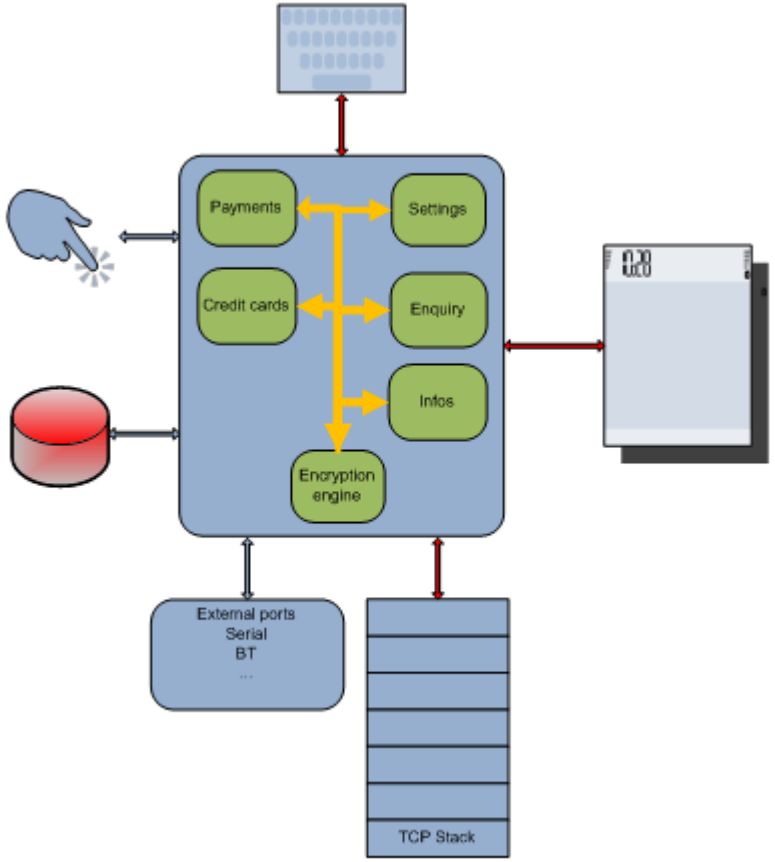
} 20 rokov

- Mobilný svet => 3 roky "NotCompatible"

# Security

- **Akákoľvek diskusia o počítačovej bezpečnosti nutne vychádza z definície požiadaviek (tj čo to naozaj znamená volať počítačový systém "bezpečný"). Všeobecne platí, že bezpečný systém riadi, vďaka použitiu osobitných bezpečnostných čŕt, prístup k informáciám tak, že iba riadne oprávnené osoby, alebo procesy pôsobiace v ich mene, budú mať prístup na čítanie, zápis, vytvorenie alebo odstránenie informácií.**
  - **Trusted Computer System Evaluation Criteria (the “Orange Book”)**

# Hrozby




- OA - Online Attack
  - Session hijacking
  - Keyboard hijacking / keylogger
  - Bluejacking, bluesnarfing
- TA – Theft Attack – plný HW prístup
- CA – Clone Attack - skopírovanie úložiska, klonovanie

# OA - Session hijacking

- Získa obsah komunikácie
- Údaje posiela na kontrolný server
- Údaje môže modifikovať

Zneužitie:

- Legálnou aplikáciu aplikuje ukradnuté údaje
- Modifikáciou údajov ovplyvní vykonávanie programu

Ochrana:

- Šifrovanie komunikácie / integrita/ redundancia údajov
- Tokenizácia
- Počítadlá
- Timeouty

# OA - Keyboard hijacking / logger

- Zaznamenáva citlivé údaje vložené prostredníctvom štandardného vstupu
- Údaje odosiela na kontrolný server
- Údaje môže modifikovať

**Zneužitie:**

- Legálnou aplikáciu aplikuje ukradnuté údaje
- V súčinnosti s klonovaním získa citlivé údaje v chránemom priestore

**Ochrana:**

- Virtuálna klávesnica

# TA – HW Access

- Získa obsah chráneného súboru z snapshotu zariadenia
- Získa citlivé údaje z snapshotu volatile pamäte
- Údaje môže modifikovať

**Zneužitie:**

- Legálnou aplikáciu aplikuje ukradnuté údaje
- Zneužije legitímne, spárované HW

**Ochrana:**

- Šifrované úložisko
- Integrita/ redundancia údajov

# CA - Storage thefts / cloning

- Získa obsah chráného súboru
- Údaje posiela na kontrolný server
- Údaje môže modifikovať

Zneužitie:

- Legálnou aplikáciu aplikuje ukradnuté údaje
- Modifikáciou údajov ovplyvní vykonávanie programu

Ochrana:

- Šifrované úložisko
- Integrita/ redundancia údajov

# Zásady bezpečného vývoja

- Zásady bezpečného kódovania /programovania
  - Obfuskácia kódu, formálna správnosť CryptoVerif, ProVerif
- Podmienený dočasný prístup – session timeout
  - permissions
- Šifrovanie citlivých údajov
  - PKCS#7, AES, SHA256, PKCS#5
- Dôkladný test
  - + QA testy, business testy
- Penetračný test
  - Nezávislou osobou/spoločnosťou
- Spôsob autentizácie
  - oob => OTP token,  ZKA-TAN-Generator, CAP/DPA, optické čítačky, NFC, BT

# Najčastejšie chyby

- **Dátova redundancia**

```
RSAPrivateKey ::= SEQUENCE {
    version Version,
    modulus INTEGER, -- n
    publicExponent INTEGER, -- e
    privateExponent INTEGER, --
    prime1 INTEGER, --p
    prime2 INTEGER, -- q
    exponent1 INTEGER, -- d
    mod (p-1)
    exponent2 INTEGER, -- d mod (q-1)
    coefficient INTEGER, -- (inverse of q) mod p
    otherPrimeInfos OtherPrimeInfos OPTIONAL
}
```

- **PKCS7 padding**

```
... | DD DD DD DD DD DD DD DD | DD DD DD DD 04 04 04 04 |
```

# Najčastejšie chyby

- **Pamäťový model**

```
paddByte=BLOCK_LENGTH – PIN.length();
while(PIN.lenth() < BLOCK_LENGTH)
{
     PIN = PIN + String.format(“%02d”,paddByte);
}
```

```
byte code = (byte)(in.length - inOff);

        while (inOff < in.length)
        {
             in[inOff] = code;
             inOff++;
        }
```

# Autentifikácia/Autorizácia

- **Dvojfaktorová autentifikácia (2FA) vyžaduje použitie dvoch zo štyroch!! autentifikačných faktorov. Tieto faktory sú:**
  - **Niečo čo užívateľ vie (napr. heslo, PIN, ...)**
  - **Niečo co užívateľ má (napr. ATM karta, „chytrá karta“...)**
  - **Niečo čím užívateľ je (biometrická charakteristika, ako je napríklad odtlačok prsta)**
  - **Niečo čím sa užívateľ prejavuje (behaviorálna chrakteristika, ako je napríklad „vlastnoručný“ podpis)**

- **OOB – out of band – nezávislý kanál**
  - **CAP/DPA**
  - **HHD**
  - **Optická čítačka**

# Ďakujeme za pozornosť

TATRA BANKA
Member of Raiffeisen Bank International

eFOCUS