Konference Security 2015

Zabezpečení mobilních bankovnictví

Petr Dvořák
CEO, Lime - HighTech Solutions s.r.o.
petr@lime-company.eu

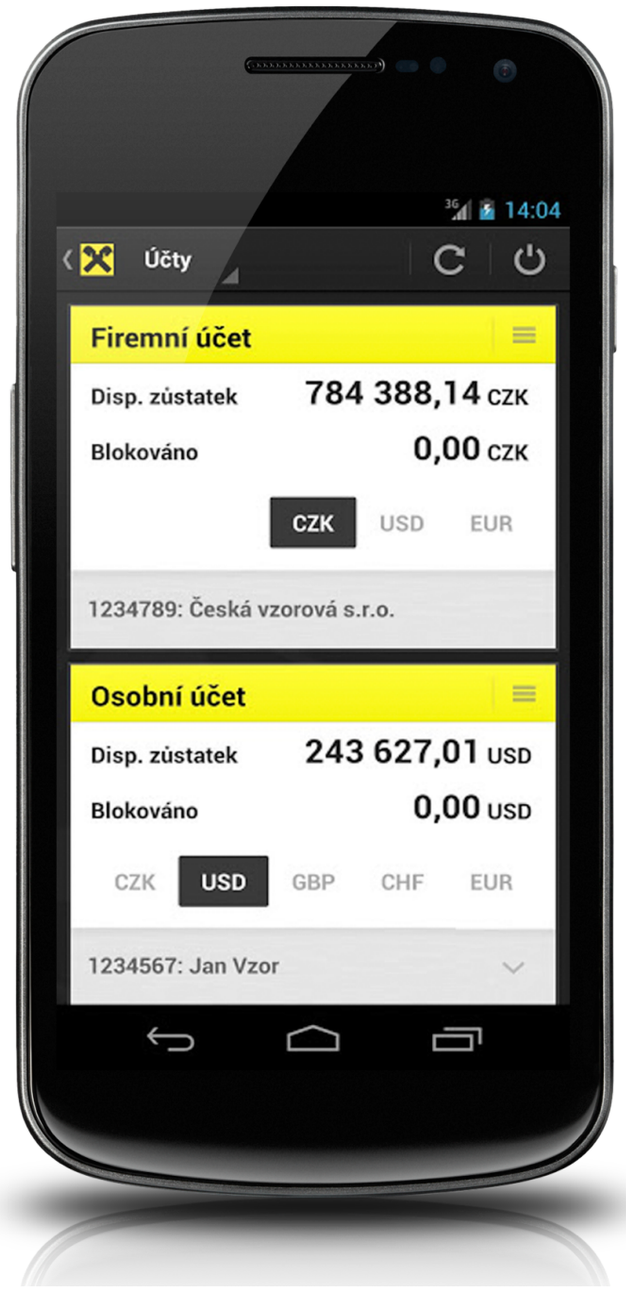
Obsah

- Vlastnosti mobilních zařízení.
- Architektura mobilního bankovnictví.
- Popis současného stavu zabezpečení.
- Témata roku 2015.

Vlastnosti mobilních zařízení

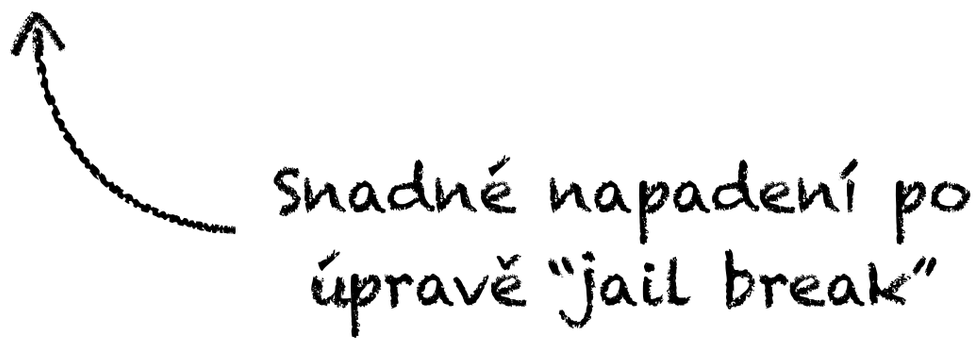
Mobilní zařízení

- Chytré telefony a tablety.
- Zcela běžně dostupná.
- Vysoce přenosná, osobní.
- Vždy on-line (GSM i Wi-Fi).
- Vybavená senzory.



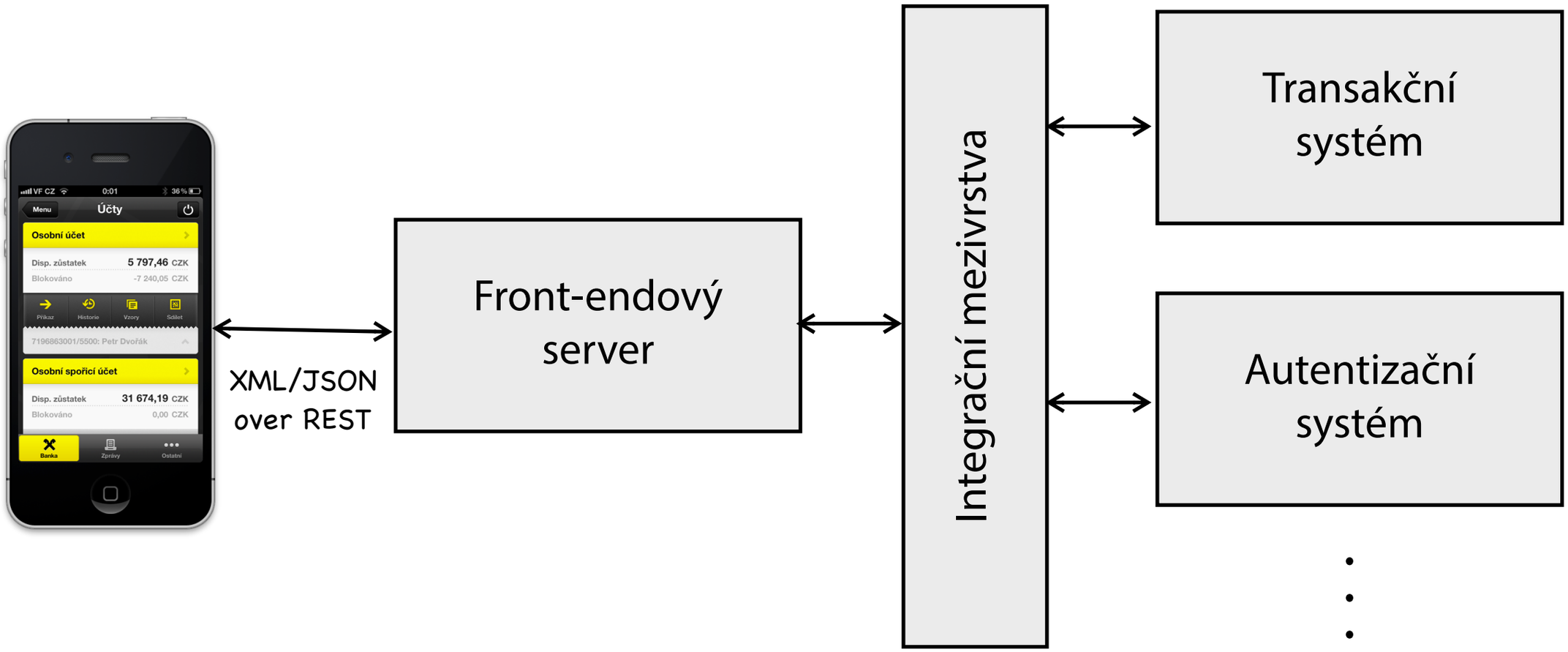
Mobilní operační systémy

- iOS: Mac OS X, Objective-C / Cocoa.
- Android: Linux, Java (Dalvik).
- Relativně snadné zásahy v runtime.
- Benevolentní management paměti.

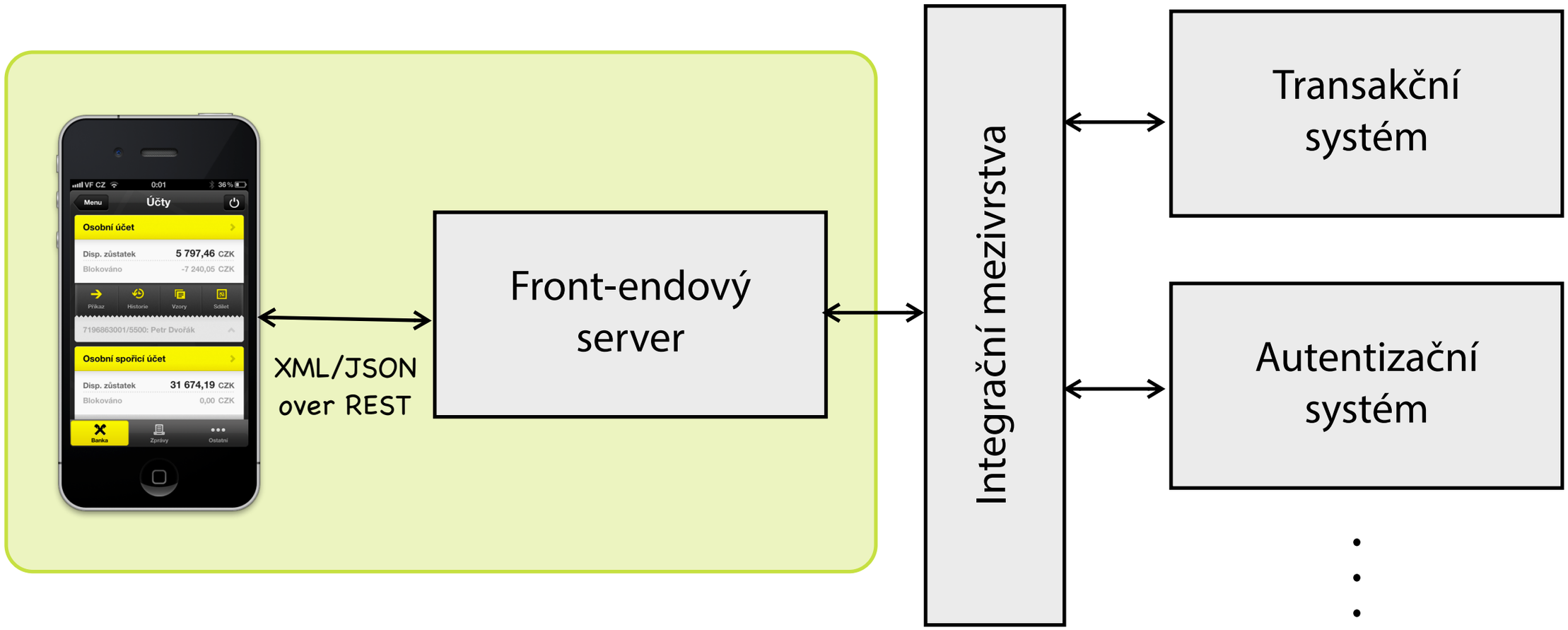


Architektura mobilních bankovnictví

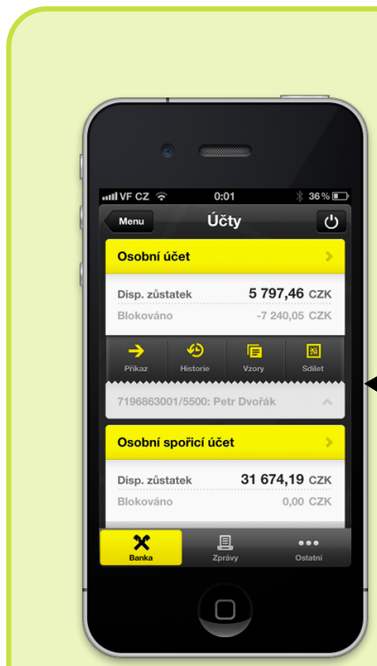
Celkový pohled shora



Celkový pohled shora



Celkový pohled shora



XML/JSON over REST

Front-endový server

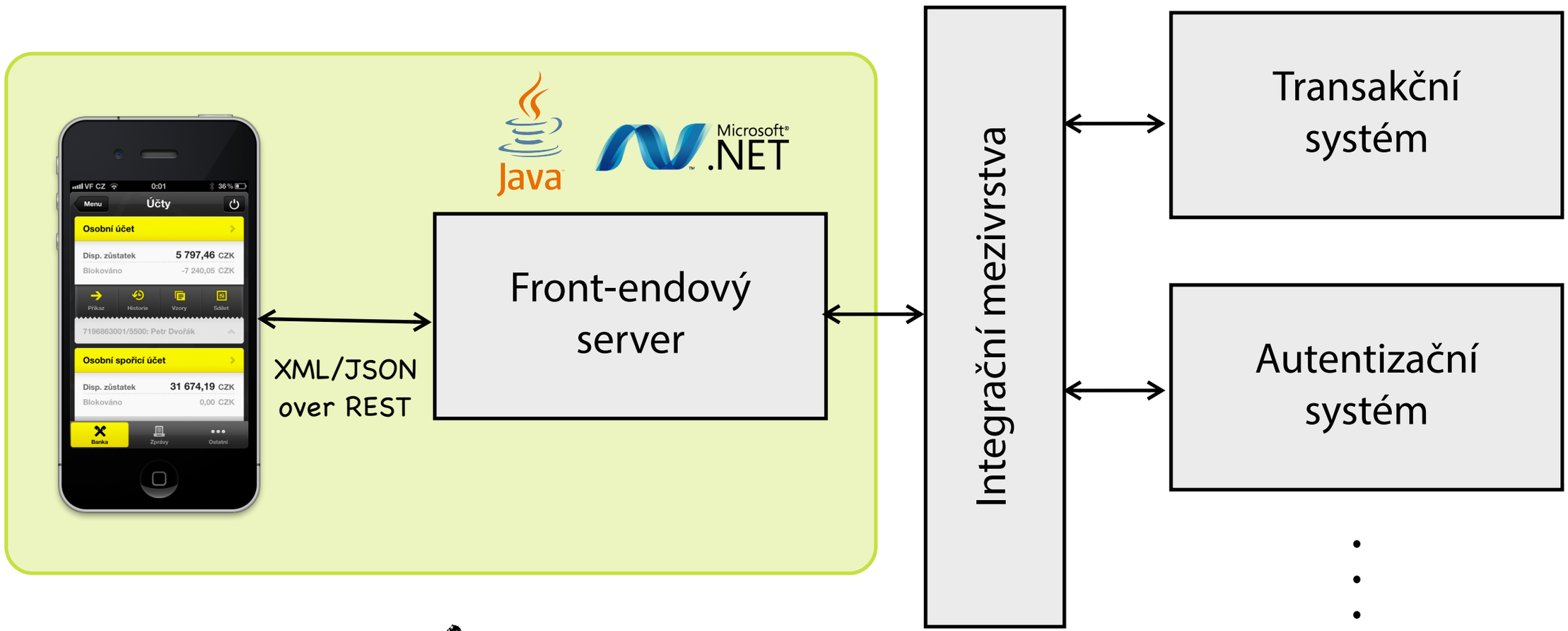
Integrační mezivrstva

Transakční systém

Autentizační systém

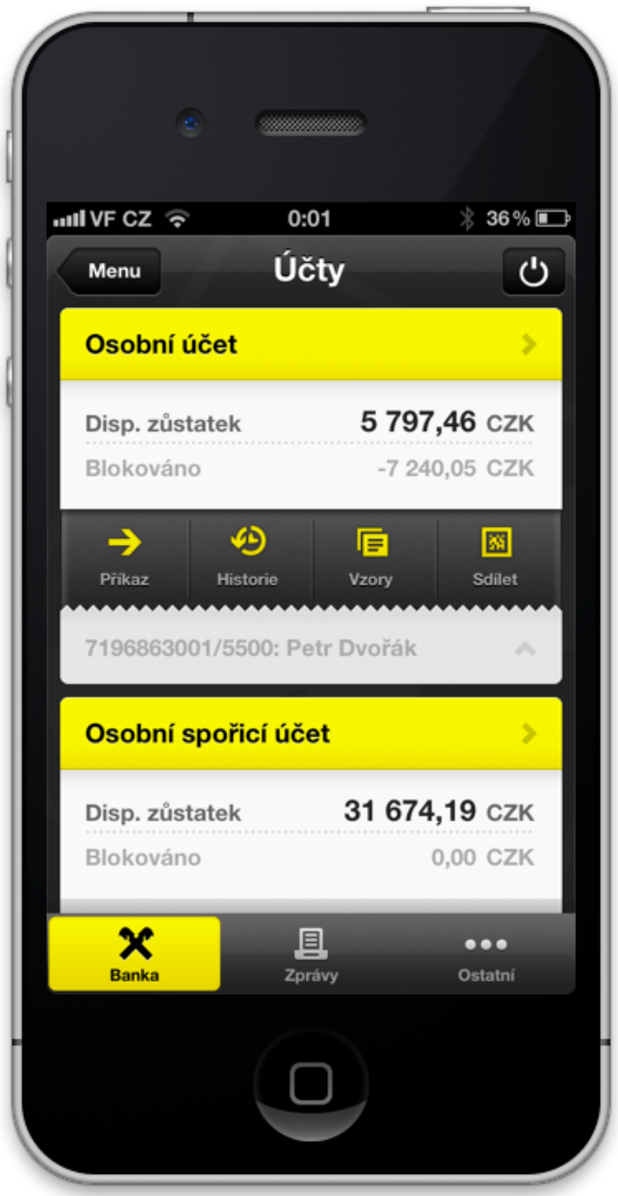
Penetrační testy vždy před "většími" release

Celkový pohled shora



Penetrační testy vždy před "většími" release

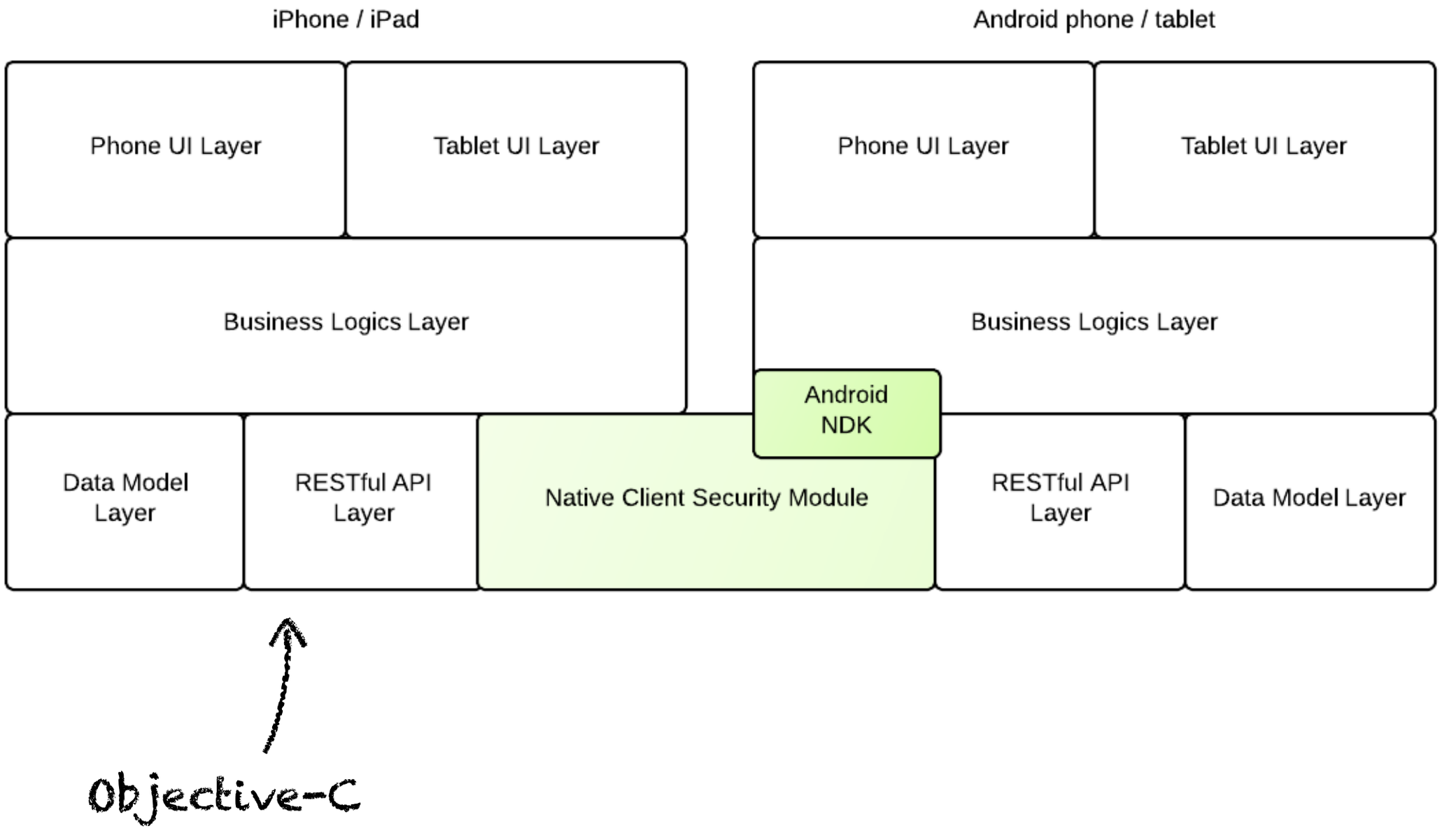
Mobilní bankovnictví



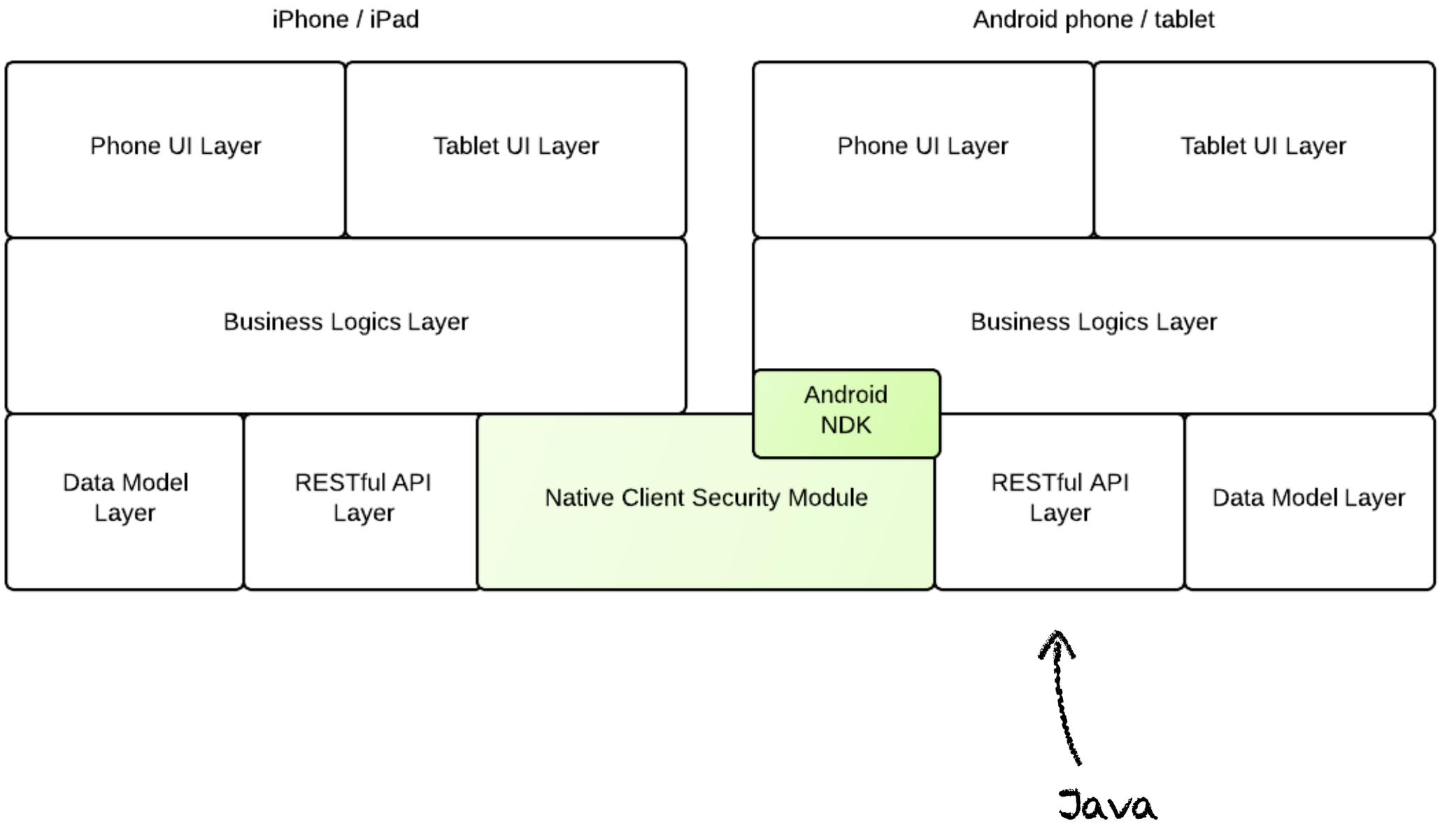
Nativní aplikace.

Různé operační systémy

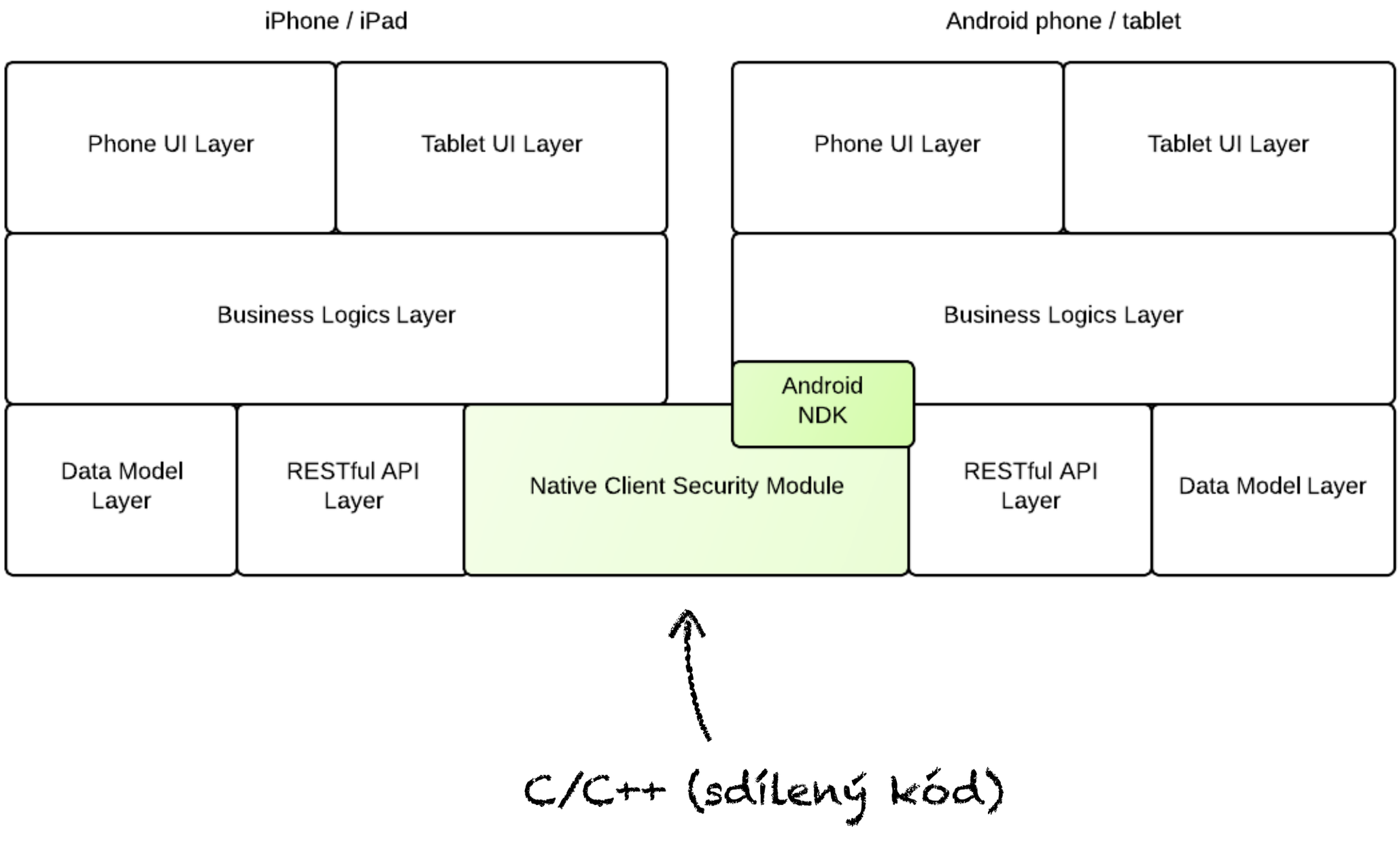
Mobilní bankovnictví



Mobilní bankovnictví



Mobilní bankovnictví



Popis súčasného stavu zabezpečení

Současný stav zabezpečení

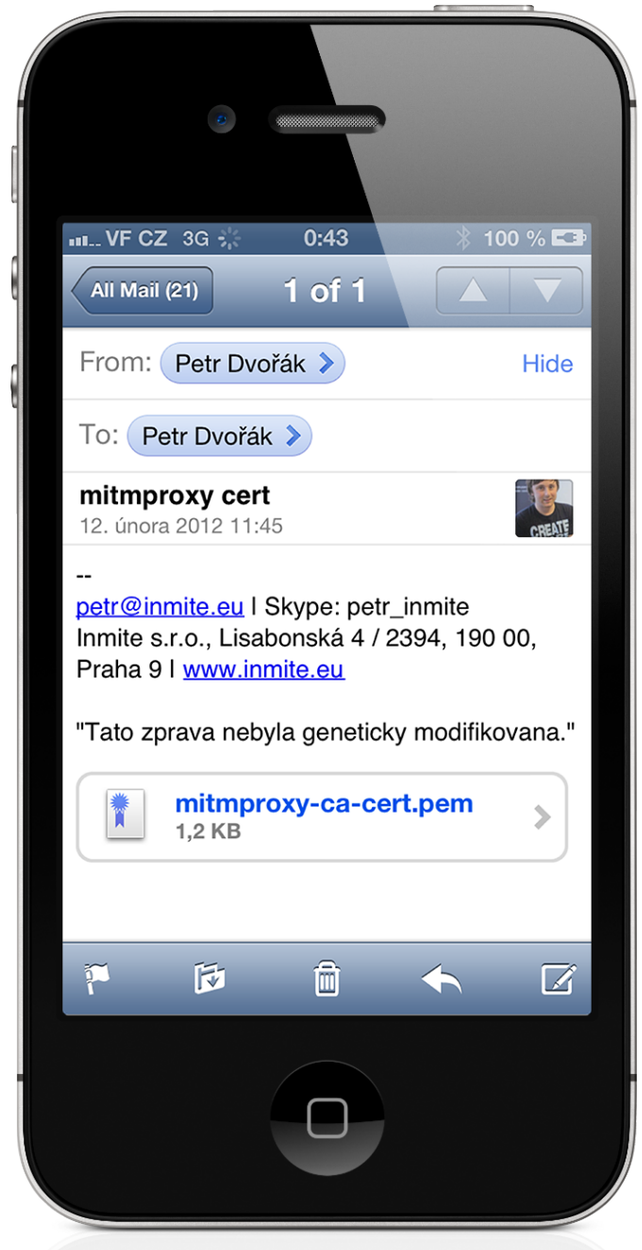
- Bezpečnost MB - vyšší než bezpečnost IB.
- Konsenzus: Aktivace skrze IB + jiné kanály.
- Kompromis UX vs. bezpečnost “vyřešený”.
- Řeší se už především “vychytávky”.

Staré dobré útoky

- Útok MITM.
- Podvržená aplikace.
- Útok po ukradení.
- Reverzní inženýrství.

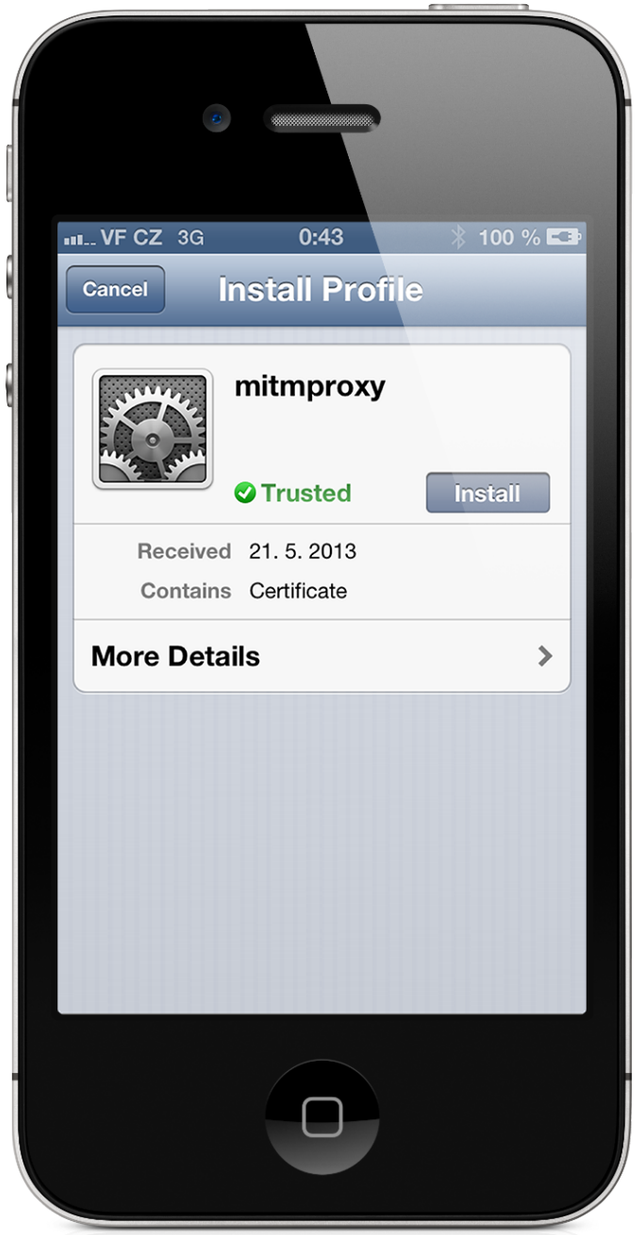
Útok MITM

- iOS - Snadné (Wi-Fi, e-mail).
- Android - Méně snadné (SD karta).
- Podepisování na aplikační vrstvě.
- Striktní validace SSL certifikátu.



Útok MITM

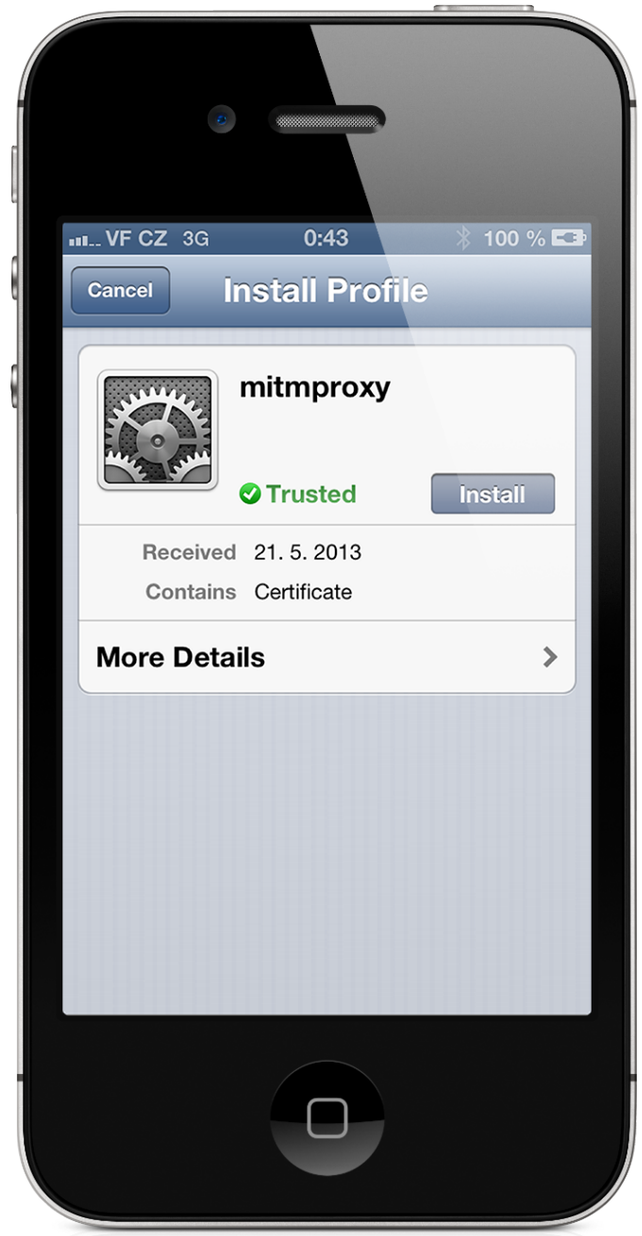
- iOS - Snadné (Wi-Fi, e-mail).
- Android - Méně snadné (SD karta).
- Podepisování na aplikační vrstvě.
- Striktní validace SSL certifikátu.



Útok MITM

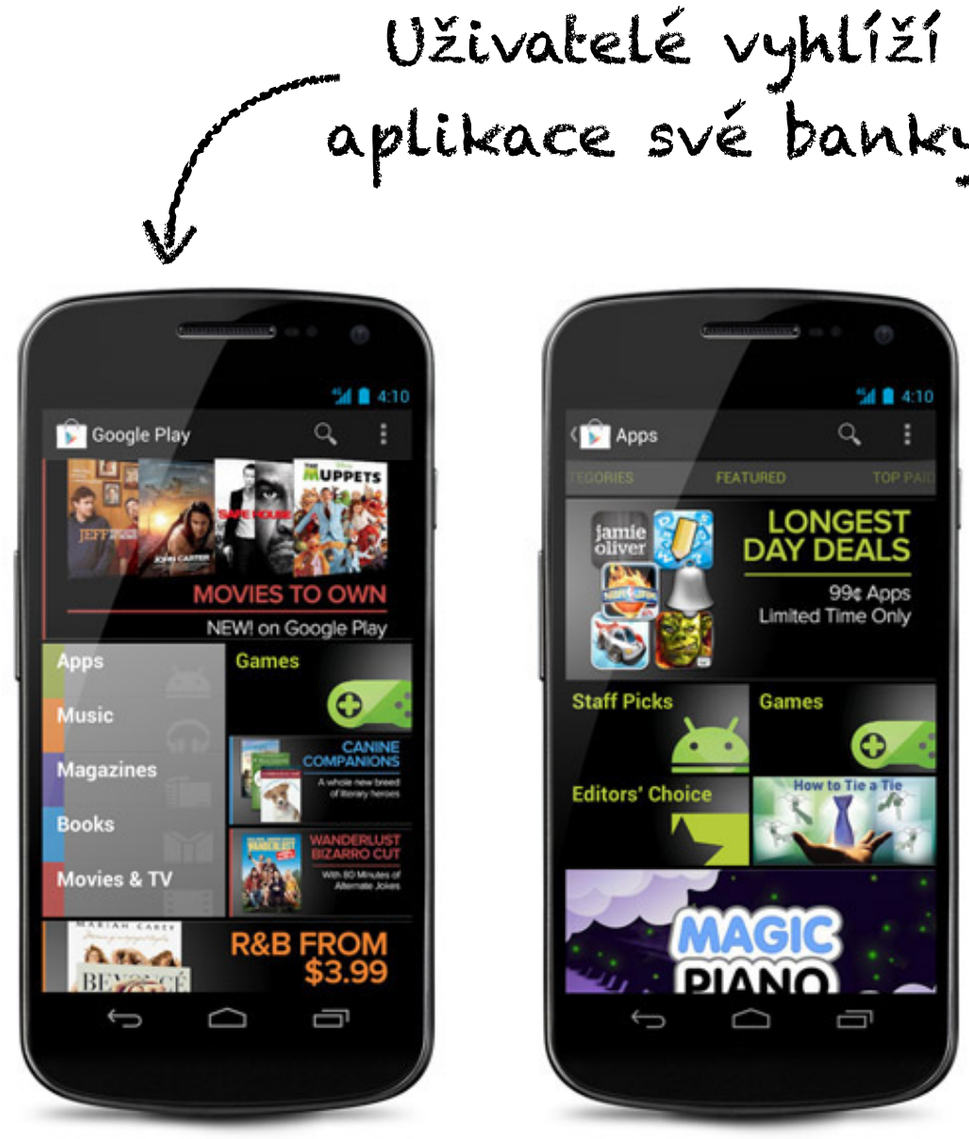
- iOS - Snadné (Wi-Fi, e-mail).
- Android - Méně snadné (SD karta).
- Podepisování na aplikační vrstvě.
- Striktní validace SSL certifikátu.

Problém při vypršení platnosti.



Podvržená aplikace

- iOS - “Nemožné” (review).
- Android - Snadné (otevřenost).
- Manuální kontrola Google Play (a App Store).
- Uživatelská hodnocení.



Podvržená aplikace

- iOS - “Nemožné” (review).
- Android - Snadné (otevřenost).
- Manuální kontrola Google Play (a App Store).
- Uživatelská hodnocení.

Nejlepší obrana: vydejte aplikaci včas a komunikujte ji! ☺

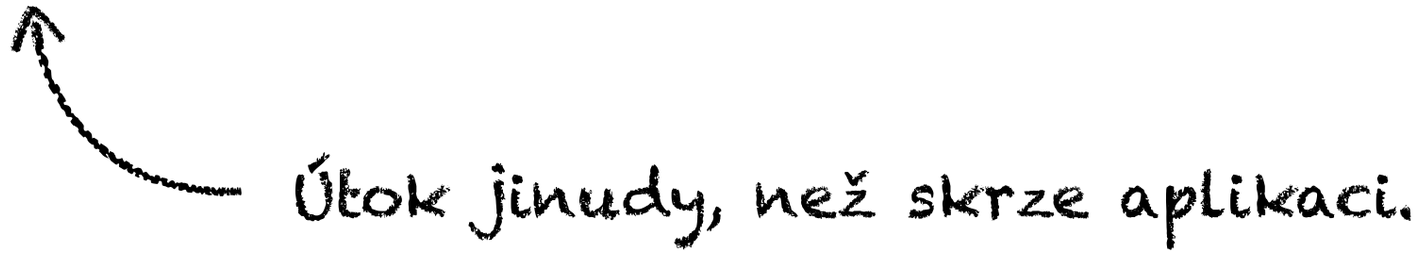
Podvržená aplikace

- Cross-platform útoky na desktop i smartphone.
- Častější aplikace, které útočí na IB.
- Instalace z externích zdrojů
- Stále sofistikovanější realizace.

Útok po ukradení

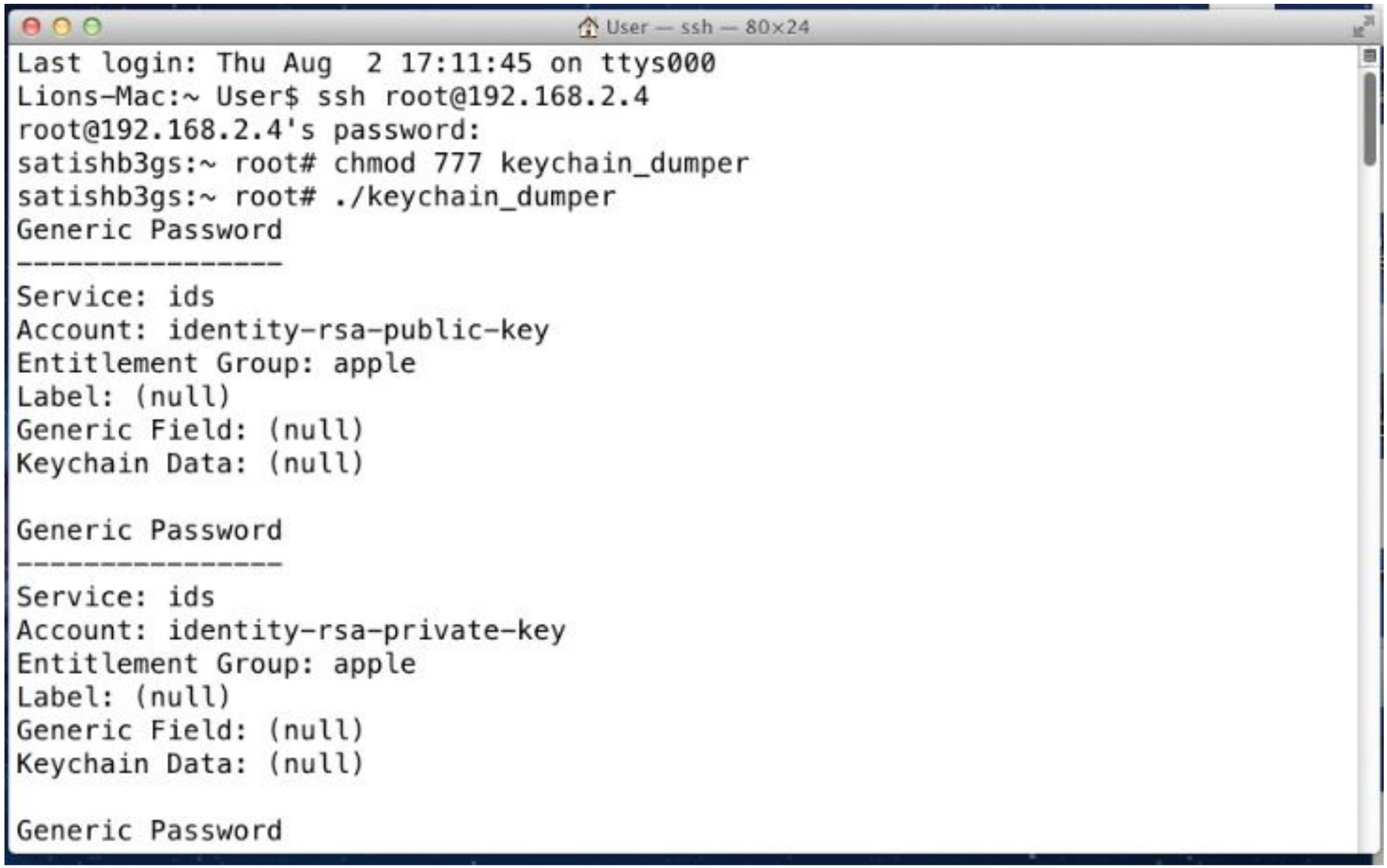
- Krádež či ztráta zařízení.
- Malý dopad reálně, velké obavy uživatelů.
- Typy útoků:
  - Postranní kanály.
  - Hádání hesla.
  - Dolování hesla.

Postranní kanály



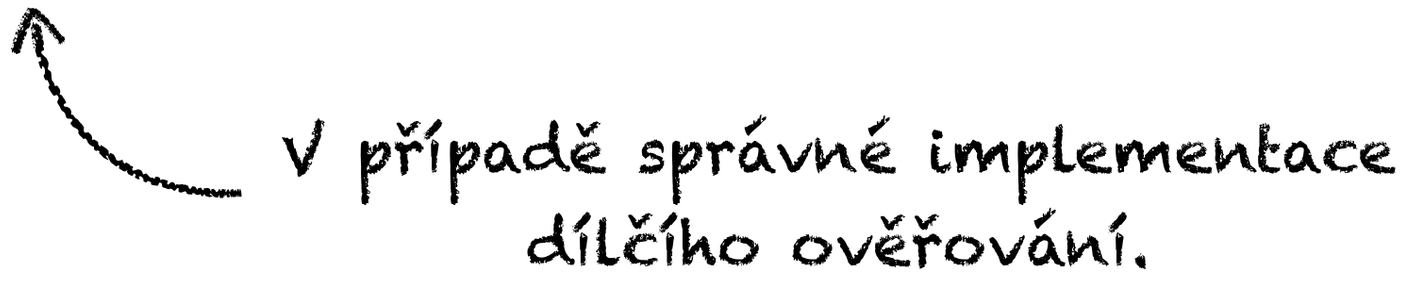
- Použití stejného hesla napříč aplikacemi s různým zabezpečením.
- Slabá úložiště hesel.
- Otisky prstů na displeji.

Postranní kanály

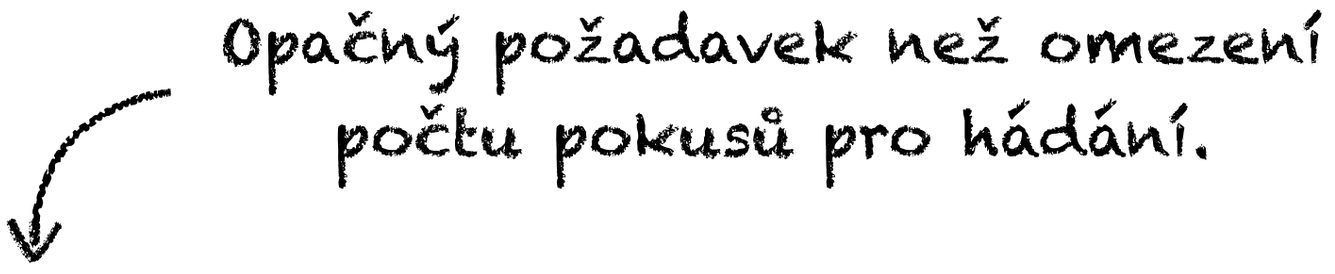


Hádání hesla

- Nutné efektivně omezit počet pokusů.
- Sdílený náhodný klíč (symetrická šifra).
- Sekvenčnost.
- Heslo odemykající klíč nemusí být složité.

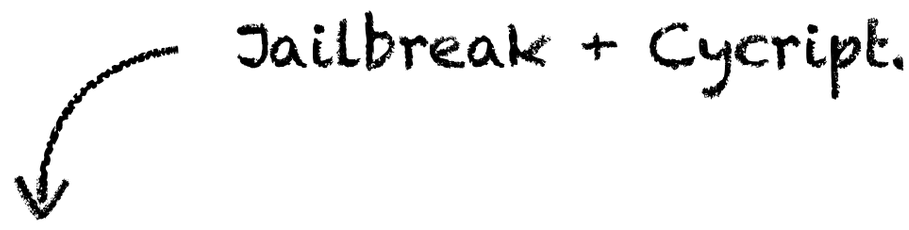


Hádání hesla



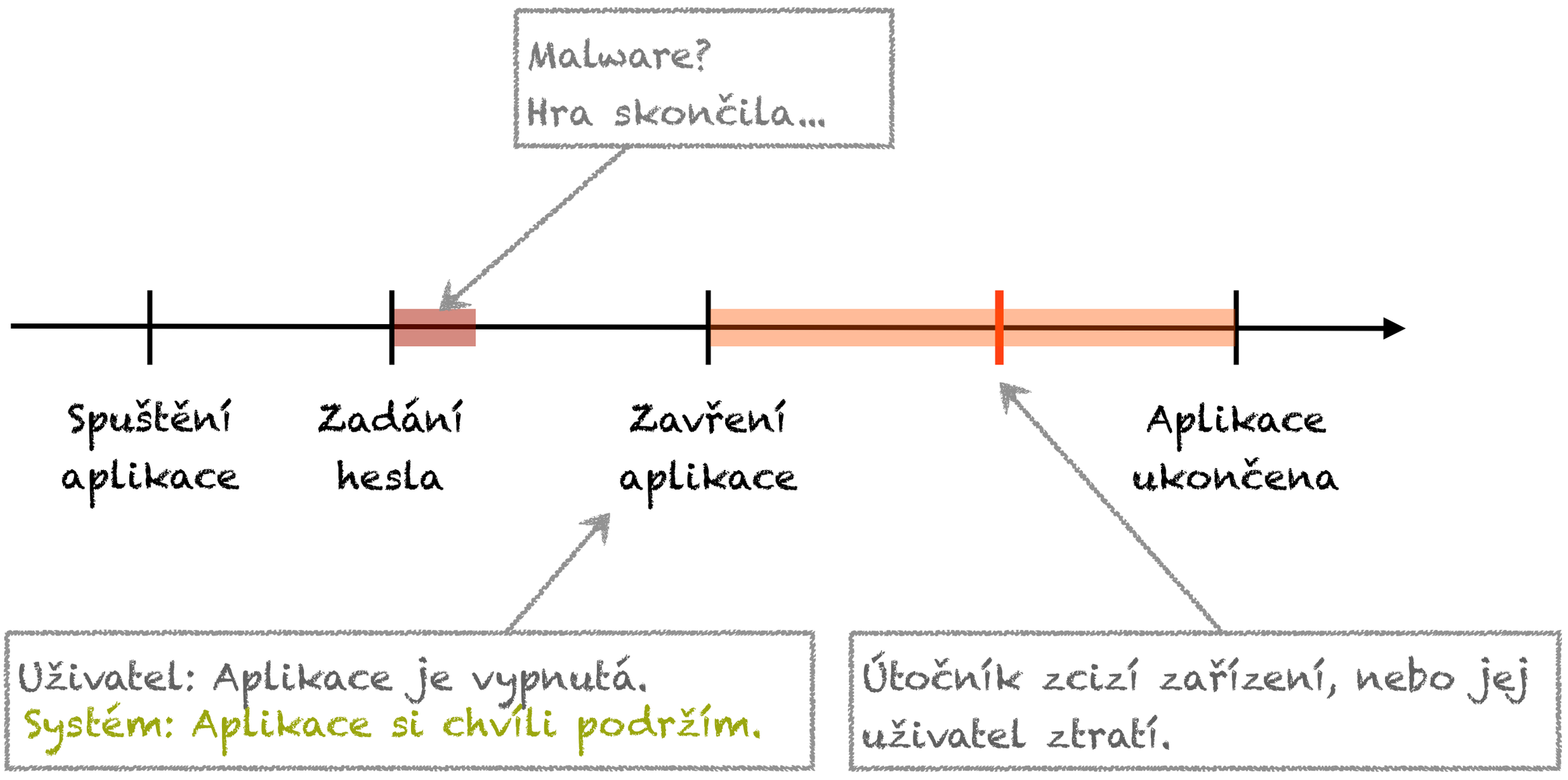
- Nutné omezení možnosti blokování účtu.
- Rozpoznání situace, kdy útočník vlastní zařízení uživatele.
- Dvou-faktorová autentizace.

Dolování hesla



- Výpis paměti nebo útok na run-time.
- Nutné zajistit striktní práci s pamětí.
- Low-level implementace (C/C++ modul).
- Android NDK.

Dolování hesla



Dolování hesla

- Přemazávání klíčů a dočasných hodnot.
- Složitější dekompilace algoritmů.
- Speciální klávesnice.
- Zabezpečení zadávání hesla do textových polí.

Reverzní inženýrství

- Přílišné odkrývání implementačních detailů láká zvědavce.
- Diskuze, které se nemusí vést = reputační riziko.
- Možnost nalezení slabších míst implementace.

Témata 2015

Silnější autorizace

- Současné mobilní banky směřují na “retail”.
- Chybí řešení pro SME a větší podniky.
- Jak z pohledu funkčnosti, tak bezpečnosti.

HW token, ARM TrustZone, ...

Možností je mnoho ...

TrustZone®
System Security by ARM

HW token, ARM TrustZone, …

2 - 10 m radius

Inovativní funkčnosti

- Otisky prstů - TouchID
- Hlasová biometrie - Nuance
- Kontext-aware bezpečnost - iBeacon

Děkuji.

Petr Dvořák
CEO, Lime - HighTech Solutions s.r.o.
petr@lime-company.eu

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Panelová diskuse

Bezpečnost mobilních zařízení

16. února 2011