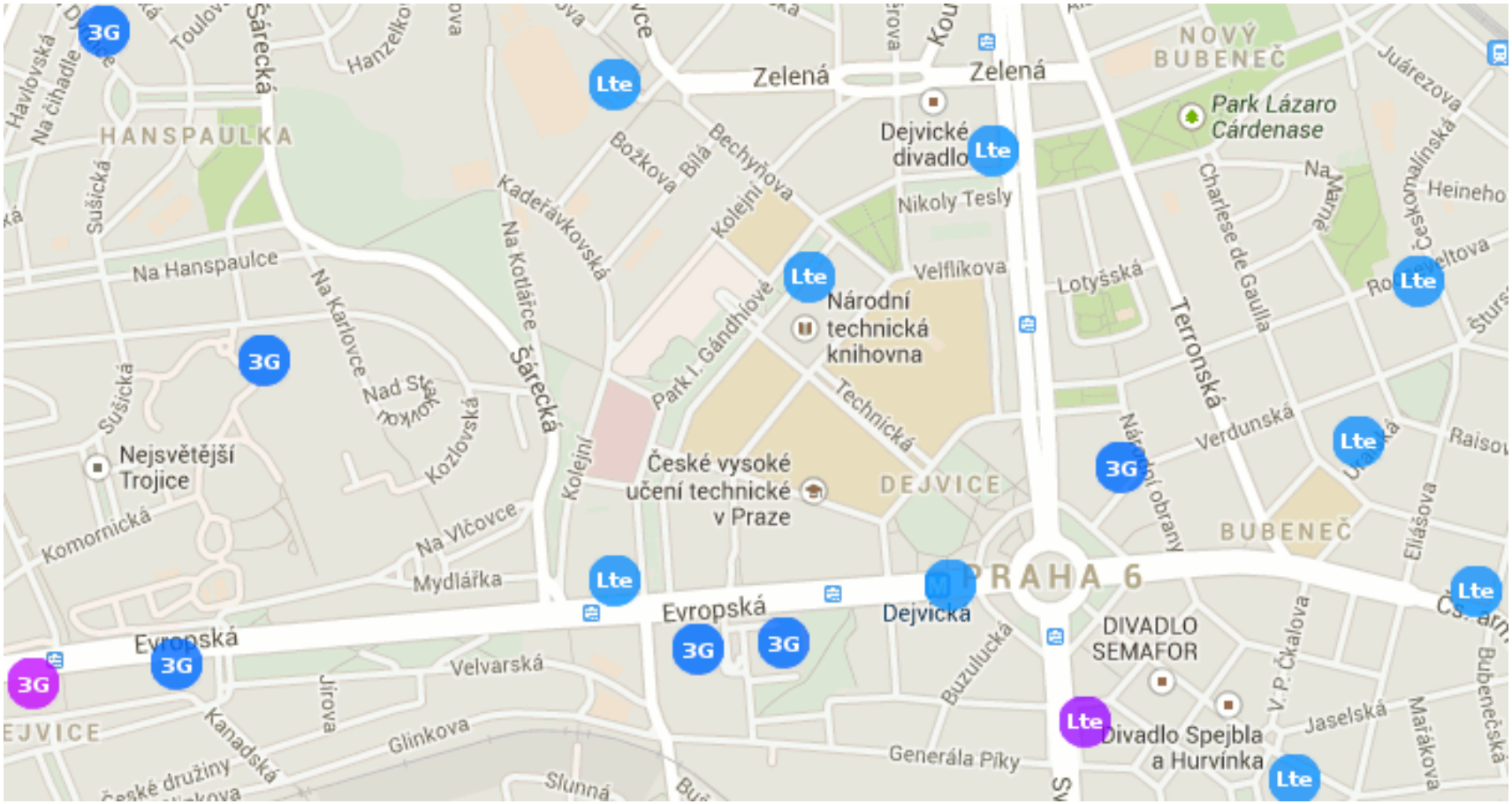
Mobilní zranitelnosti

Ondřej Caletka

27. března 2014

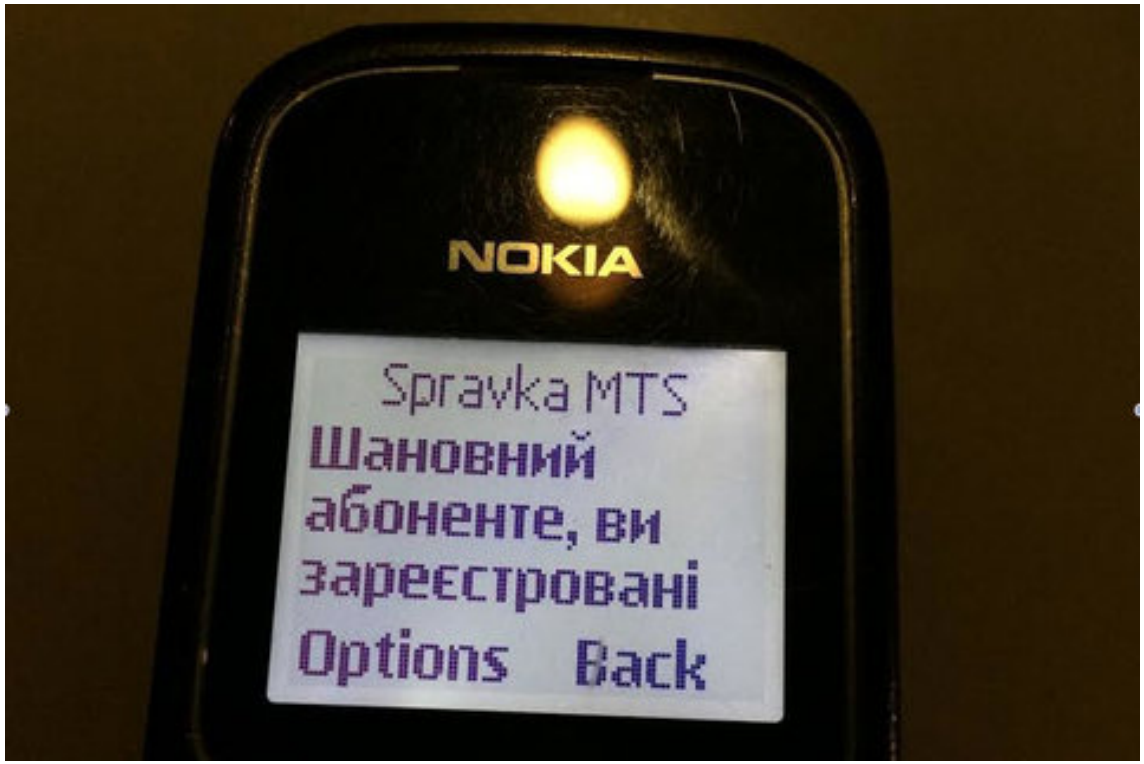
Geolokace mobilních zařízení



Zdroj: gsmweb.cz

Kijev, leden 2014

Vážený zákazníku, zaregistrovali jsme vás jako účastníka nepovolené demonstrace. Váš operátор.



Zdroj: thelede.blogs.nytimes.com

CLIP (Identifikace volajícího)

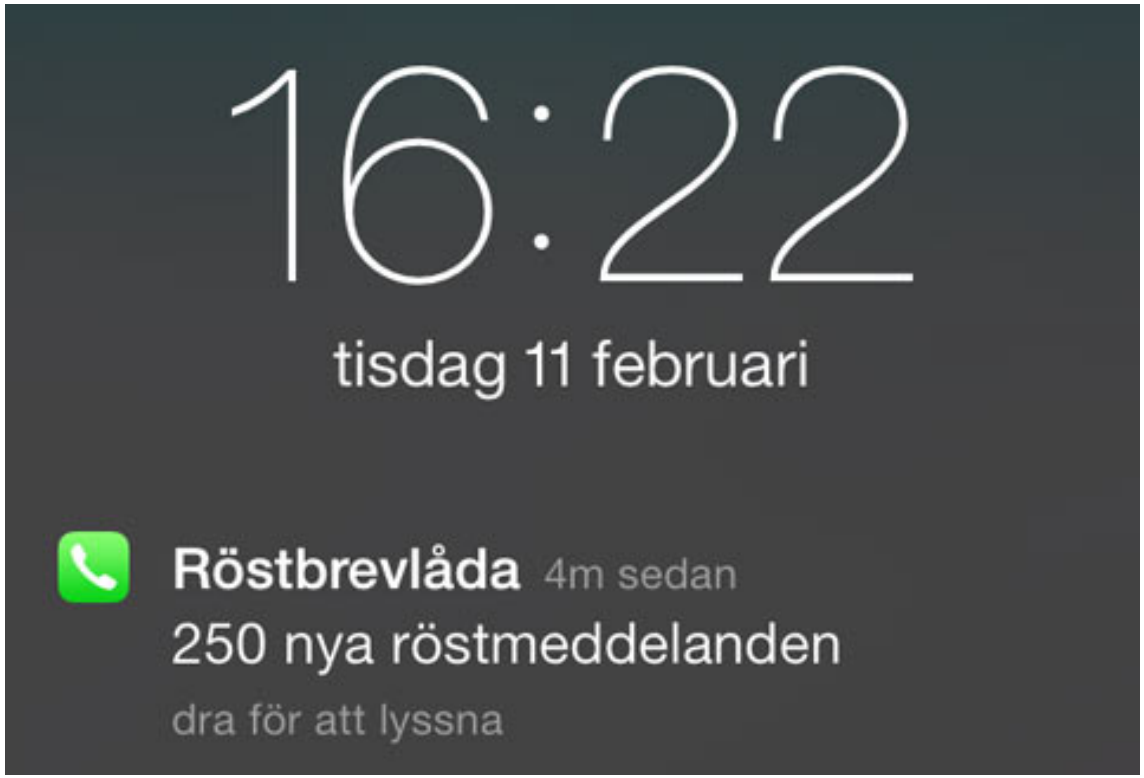
- doplňková služba inteligentní sítě
- za validitu dat odpovídá originující operátor
- v rámci mezinárodního styku dobrovolné

Prozváněcí podvody

- Útočník provede krátký hovor z čísla například +2431230292
- Oběť volá zpět v domnění, že jde o místní hovor
- Útočník (*spolu s místním operátorem*) profituje z astronomické ceny mezinárodního hovoru

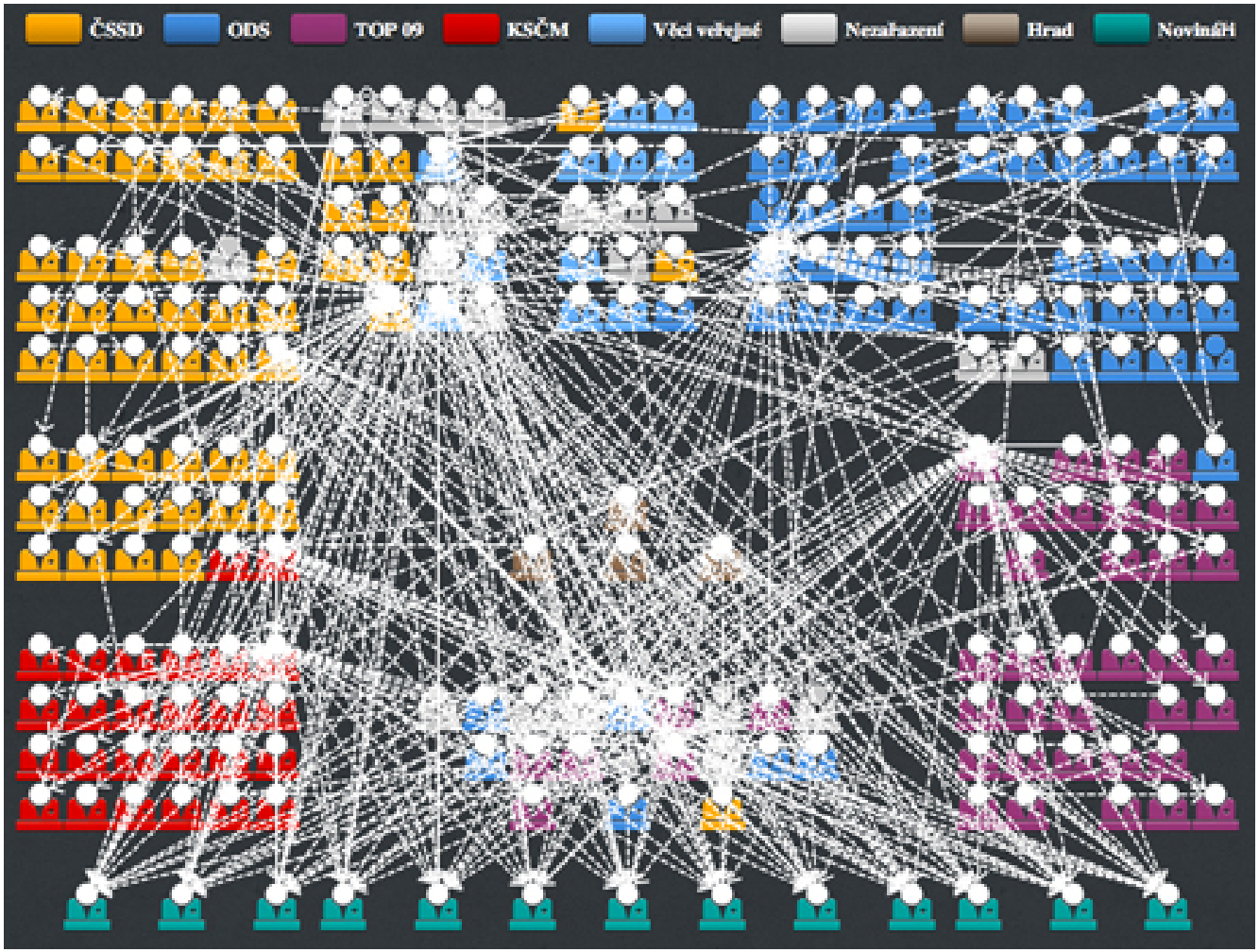
SMS zprávy

- původně jen servisní zprávy sítě
- nenesou jen text
- lidé jim mají tendenci důvěřovat



Zdroj: www.idg.se/2.1085/1.546628/sa-enkelt-hackar-han-iphone

Morální reforma



Zdroj: ccc.de: Hacking the Czech Parliament via SMS

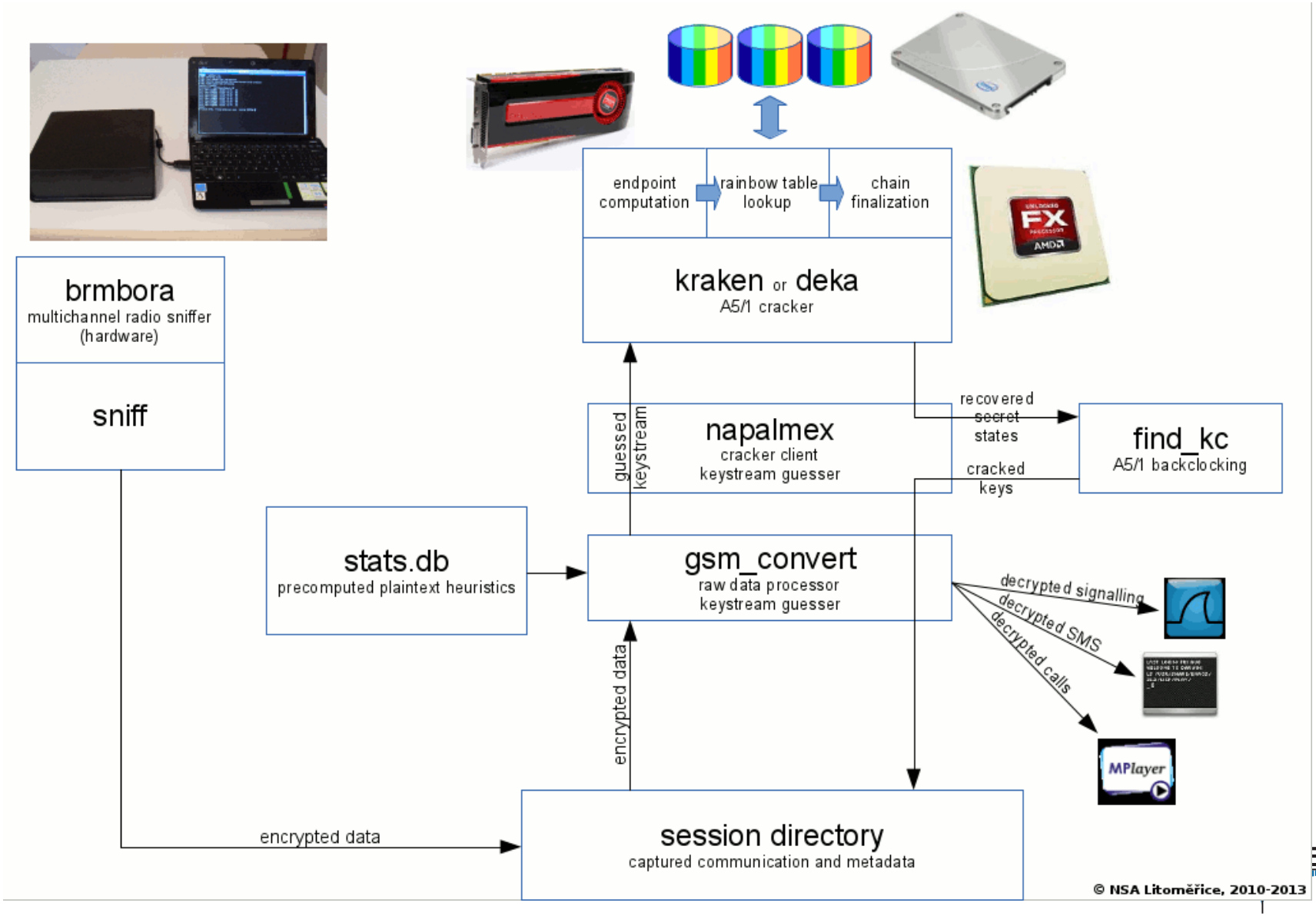
Sociální inženýrství

příchozí hovor

Dobrý den, nabízím vám speciální tarif pouze pro vás,
Nejprve mi ale prosím sdělte heslo pro komunikaci
s operátorem...

- identifikaci volajícího lze poměrně snadno podvrhnout
- autentizace by měla být vzájemná
- autentizace by neměla umožnit převzetí identity protistrany (nesdělovat celé heslo, jen vybrané znaky)

Příliš děravé GSM



Zdroj: brmlab.cz

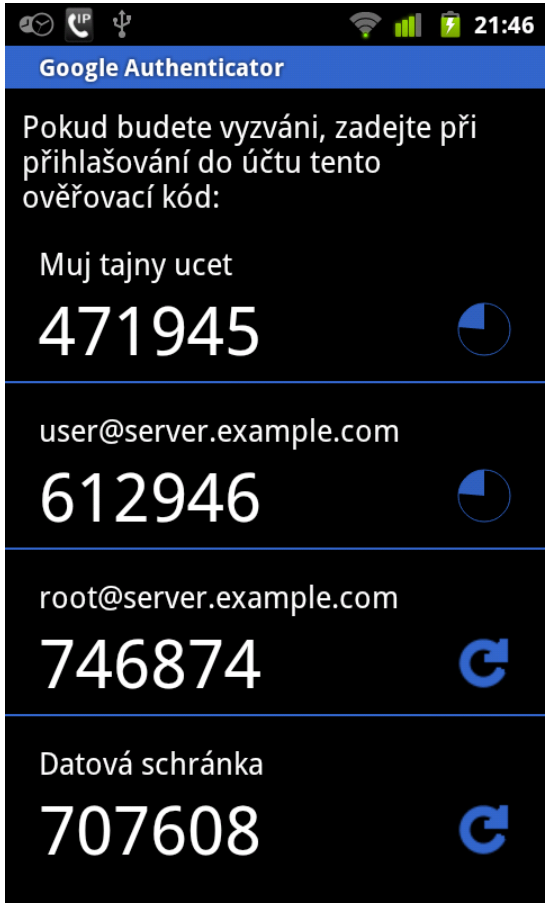
Příliš děravé GSM

- odposlech SMS zpráv k uživateli je realizovatelný v amatérských podmínkách
- ceny profesionálních zařízení stále klesají
- lze postavit falešnou BTS s vypnutým šifrováním
- moderní telefony nešifrovaný provoz nedokáží signalizovat
- částečným řešením je přechod na UMTS

Dvoufaktorová autentizace s mobilním telefonem

Autentizační kalkulátor v mobilu

- Aplikace drží sdílené tajemství se serverem
- Z tajného klíče jsou podle aktuálního času odvozovány jednorázová hesla
- Standardizováno v RFC 6238, široká podpora v aplikacích:
  - Google
  - GitHub
  - MojeID
  - Datové schránky



Problém roku ~2004

- lidé začali ve velké míře využívat e-banking
- jejich počítače byly prolezlé malwarem
- ukradení jména a hesla (případně X.509 souboru z disku) bylo příliš lákavé

Přidání jednorázového SMS hesla

- kompromitace počítače nestačí
- kompromitace mobilního telefonu těžko realizovatelná
- obtížné propojení dat z kompromitovaných zařízení

Post-PC era ~2012

- lidé přestávají konzumovat obsah z PC
- banky se předhánějí, která nabídne lepší aplikaci pro smartphone
- lidé zadávají přihlašovací údaje *do téhož zařízení*, do kterého následně přichází ověřovací zpráva
- kompromitace mobilního zařízení nás vrací k problémům z roku 2004
  …ale útočník musí být schopen zneužití v reálném čase

Rizika mobilních aplikací

Mobilní aplikace

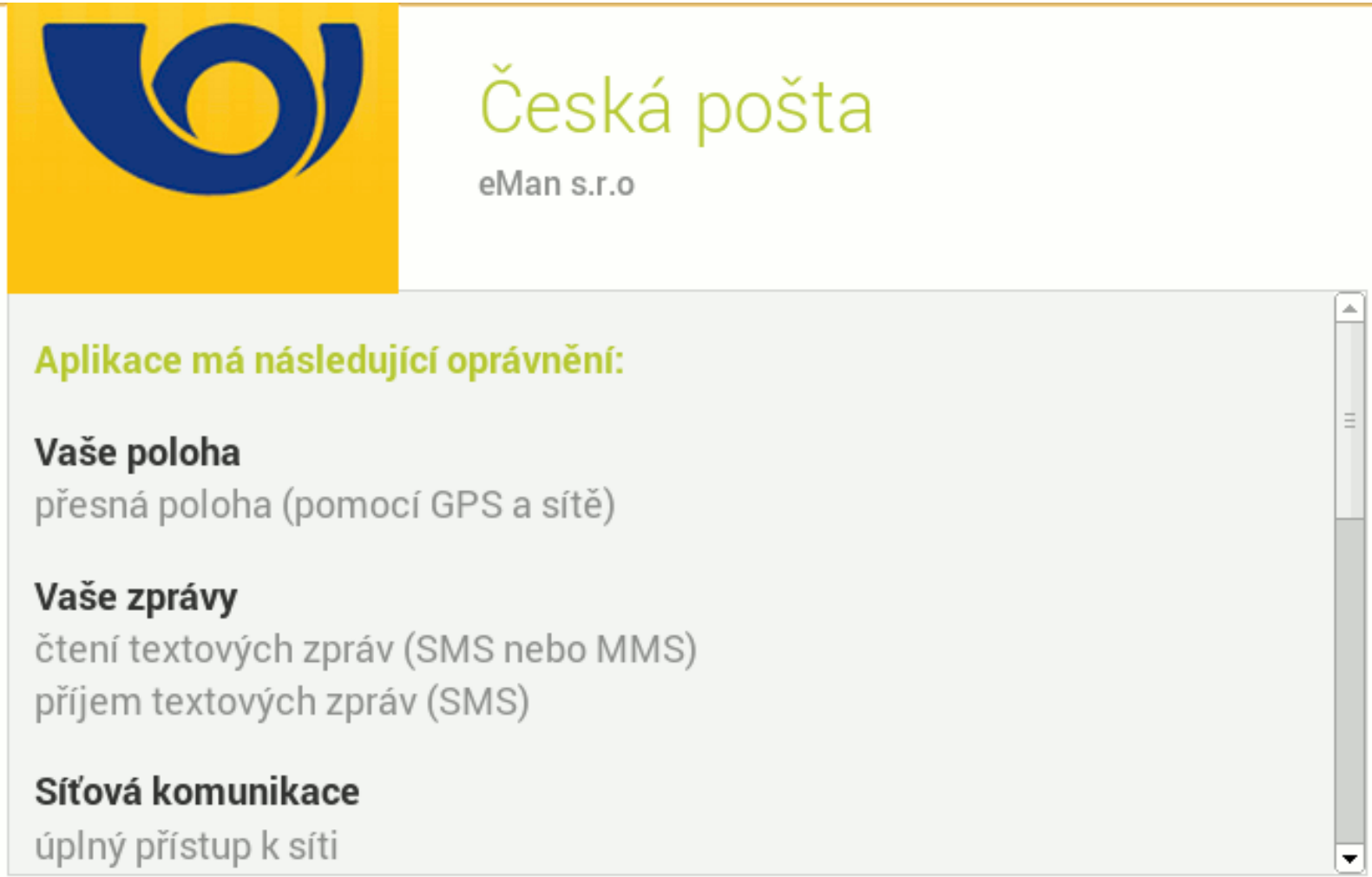
iPhone

- licence pro vývojáře
- přísné podmínky nabízení aplikací v App Store
- možnost nastavení oprávnění aplikací uživatelem

Android

- vývojář může být každý
- velmi otevřený Google Play Store
- oprávnění aplikací určuje vývojář

Pozor na oprávnění



Pozor na oprávnění

- odebírání oprávnění aplikaci uživatelem není na Androidu podporováno
- lze spoléhat jen na dobrou reputaci autora aplikace
- klíče k podepisování aplikace mohou být autorovi ukradeny

Root oprávnění

- aplikace s root oprávněním mohou *úplně všechno*
  - vstupovat do šifrovaných spojení
  - krást privátní klíče a hesla
  - maskovat se
- ani zařízení bez root nejsou v bezpečí

Rady na závěr

- nezkoušet všechny aplikace za každou cenu
- používat dvoufaktorovou autentizaci, kde je to možné, využívat hesla pro konkrétní zařízení
- omezit používání e-bankingu, řešitele a podobně kritických aplikací na mobilních zařízeních
- **nastavit zamykání obrazovky**

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz