Skutečně privátní a bezpečná komunikace?

Budoucnost nemusí být pouze v Cloudu…

babelnet

Babelnet

- Současný stav ve světě elektronické komunikace
- Co je to Babelnet? Představení platformy
- Co plánujeme do budoucna

babelnet

OKsystem a.s.

- Ředitelství v Praze
  - Pobočky v Brně a v Ostravě
- Přes 25 let na trhu
- Roční obrat přes 600 mil. Kč
- Zaměření
  - Vývoj aplikací na míru
  - Mobilní aplikace
  - Datová bezpečnost
  - Školící a testovací středisko
  - Oceňované aplikace OKbase, OKsmart, OKdox, Babelnet

babelnet

OKsystem

Současný stav světa elektornické komunikace

babelnet

Co je běžné (a nemělo by být)

- používání nezabezpečeného e-mailu pro komunikaci
- používání veřejné e-mailové služby (Seznam, Gmail…)
- používání populárních komunikačních služeb (IM), které „jsou zdarma“ (Viber, WhatsApp, Telegram, Threema…)
- přesvědčení, že když nedělám nic protiprávního, nemám co tajit
- pocit, že nikdo mé e-maily již roky nečte…
- nedocenění hodnoty kontaktů v mém mobilu
- představa, že firemní správce IT je dobře placený a loajální (a moje PC vypnuté)

babelnet

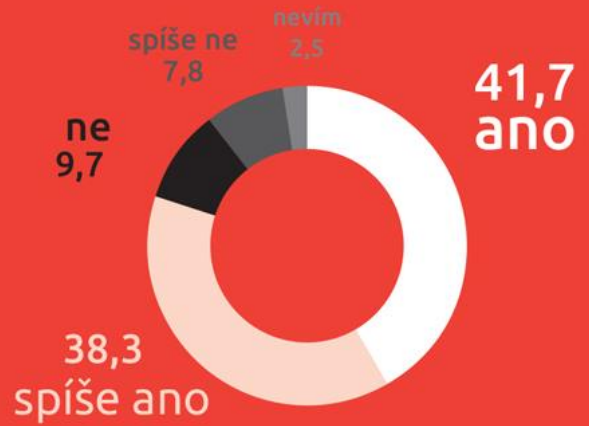
Datová bezpečnost

Průzkum agentury SANEP, zpracovaný pro značku Babelnet

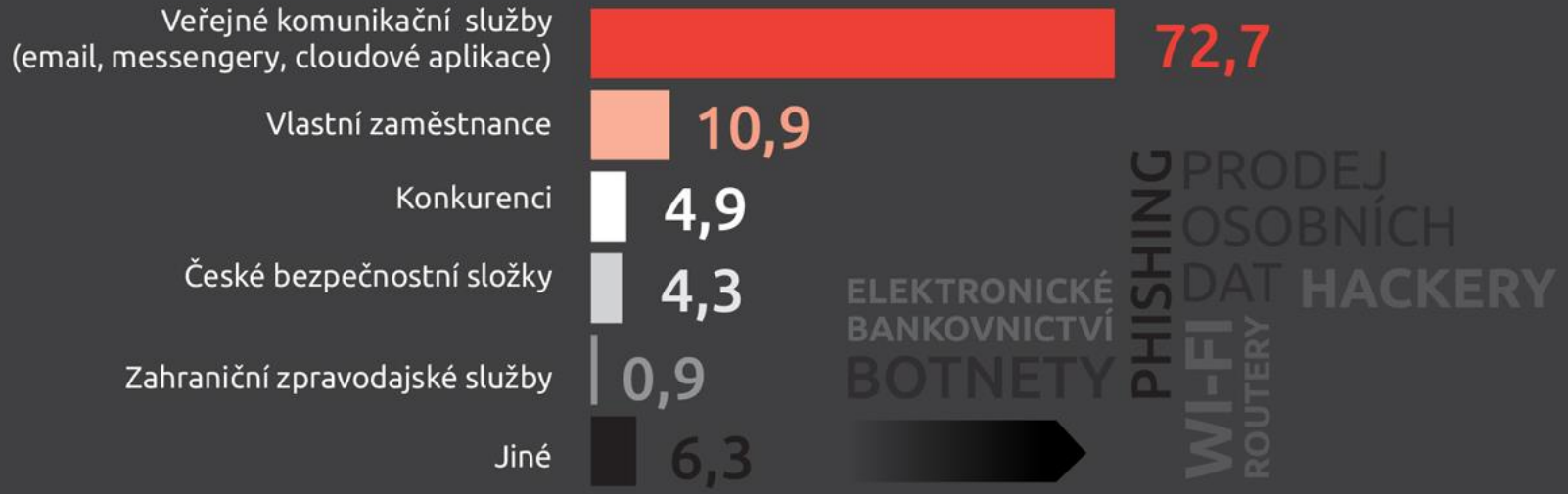
Velikost respondentního vzorku N=2.137
Termín realizace: 12.–16. 9. 2016 | In %

babelnet

Domníváte se, že má někdo zájem (osobní, obchodní apod.) získávat informace z Vaší pracovní, osobní nebo firemní komunikace?



Co považujete za největší hrozby pro bezpečnost Vaší komunikace?



Úvod – co je BabelNet?

…to nejlepší z e-mailu, instant messagingu a bezpečnosti

Babelnet je platforma pro efektivní a bezpečnou komunikaci mezi uživateli, mobilními zařízeními, stolními počítači a firemními aplikacemi.

Chrání telefonní hovory, zprávy a dokumenty nejen při komunikaci, ale i při uložení prostřednictvím silné kryptografie.

babelnet

Platforma pro šifrovanou komunikaci

- **Bezpečné zasílání zpráv**
  - Zprávy, konverzace, předmět zpráv
  - Více příjemců
  - Doručenky, přečtenky
  - Vzdálené mazání zpráv (automatické, manuální)
  - A další.
- **Posílání dokumentů**
  - Dokumenty mohou mít velikost až 2GB
- **Telefonování**
- **API**
- **Klienti**
  - Android
  - iOS
  - BlackBerry
  - Windows Desktop
  - macOS

babelnet

Babelnet – Výhody

- End to end šifrování
  - Komunikace je šifrována mezi koncovými zařízeními a využívá firemní servery pro zprostředkování komunikace

- Komunikace probíhá přes vlastní server
  - Přístup k serveru určujete vy
  - Nikdo cizí nesleduje ani provoz na serveru
  - Server slouží k distribuci klíčů a doručování zpráv
  - Revokace klíčů

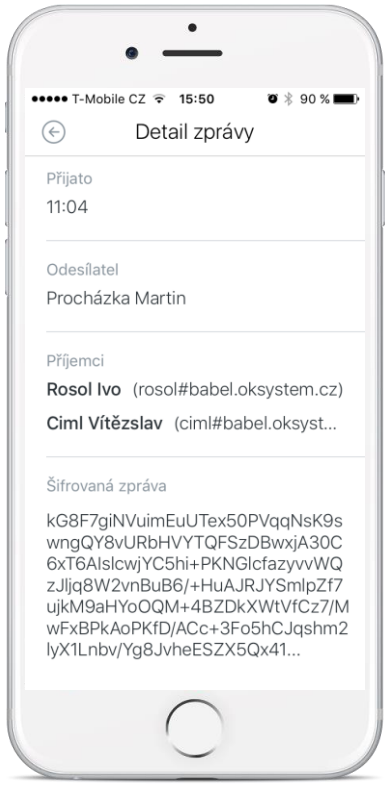
babelnet

Proč Babelnet?

- **Jednoduchá instalace**
  - Plná instalace v řádu hodin
- **Propojení serveru s firemními aplikacemi a zařízeními**
  - LDAP, CRM, DMS, Canon…
- **Použití v MDM, EMM**
  - MobileIron, AirWatch
- **Znáte vývojáře**
  - Možnost reagovat na nové požadavky

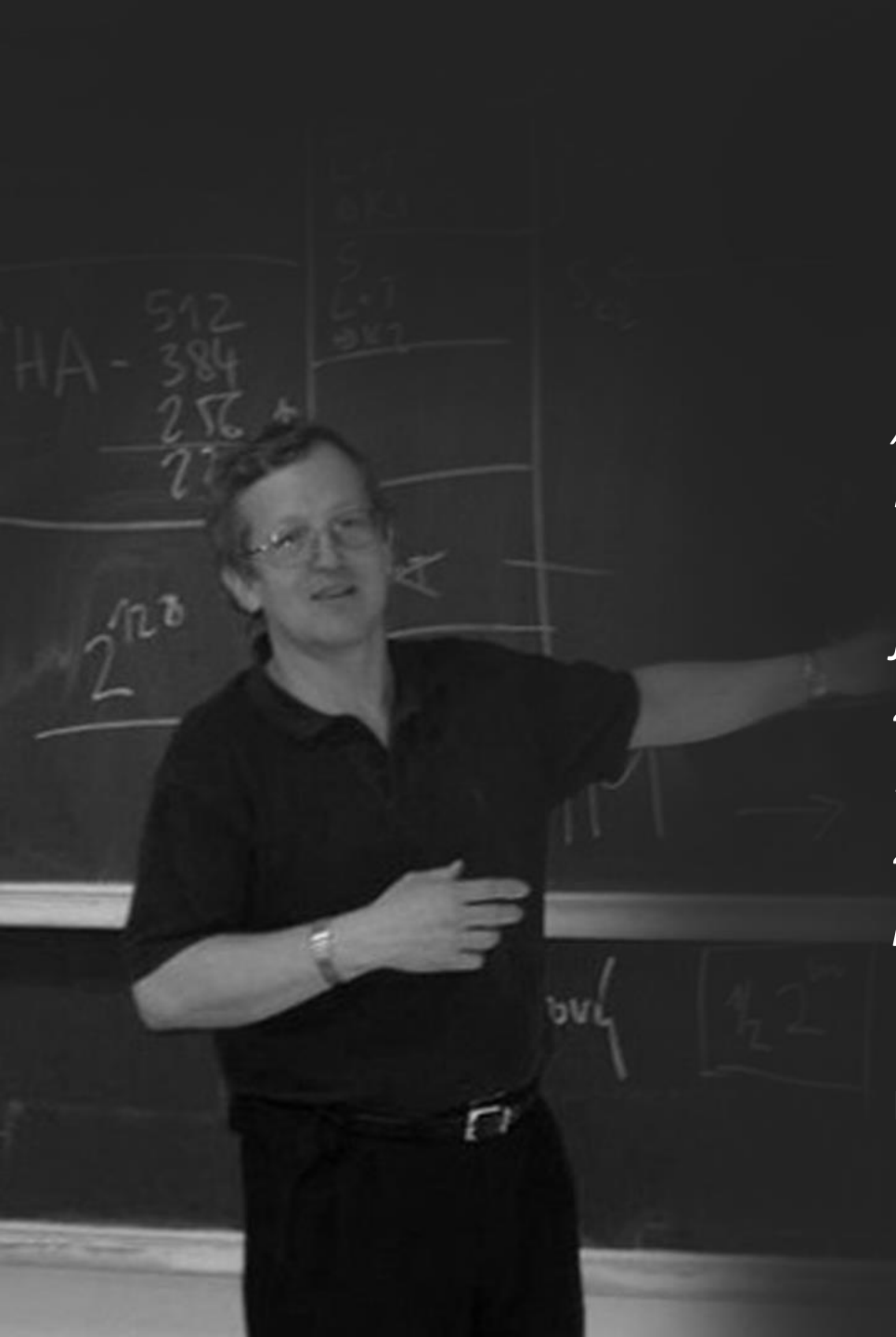
babelnet

Bezpečnost „by design & by default“



Babelnet byl od počátku navržen primárně jako bezpečnostní řešení za účelem ochrany dat a komunikace.

- kryptografie je základem produktu, nikoli doplňkem
- šifrování je použito vždy při komunikaci i uložení
- integrované prohlížeče pro bezpečné zobrazení nejčastěji používaných formátů příloh
- jsou implementovány mechanismy ochrany proti pasivním a aktivním útokům
- nastavení pravidel pro komunikaci mezi servery, zprávy doručuje výhradně server odesilatele
- vaše kontakty zůstanou vaše – Babelnet nestahuje vaše kontakty (= osobní údaje jiných subjektů!)



babelnet

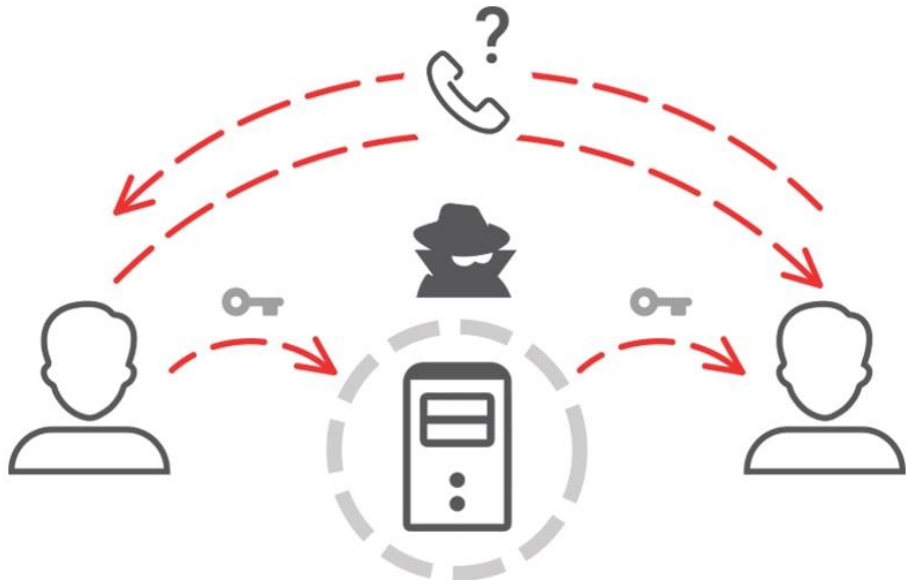
„Systém Babelnet používá moderní know-how z oblasti kryptografie a aplikuje správně silné kryptografické techniky. Při kontrole kryptografického designu jsem nenašel žádné slabiny ani pochybení z kryptografického hlediska. U vývojářů systému Babelnet jsem se setkal se snahou aplikovat to nejlepší z existujících prostředků a know-how. Nebál bych se přenášet svá tajemství tímto systémem."

RNDr. Vlastimil Klíma
přední český kryptolog

Nedaleká budoucnost

babelnet

Babelnet & Bitcoin / Blockchain – proč?



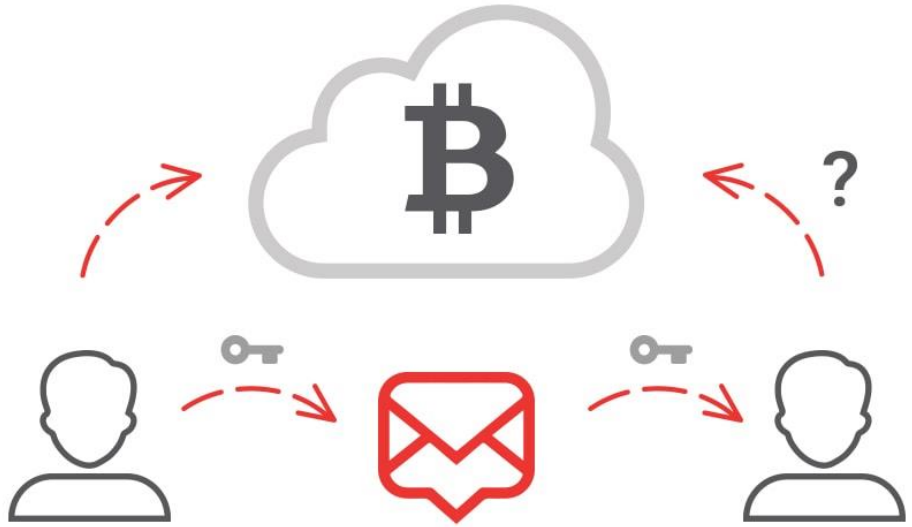
- **Ostatní aplikace**
  Pro bezpečnost komunikace musíte manuálně ověřovat klíče (QR kody, volání, osobní kontrola, apod.)

- Při end to end šifrované komunikaci je **potřeba získat veřejný klíč** druhé strany. Tento klíč vám poskytne server, ke kterému jste připojeni. **Pokud je server napaden, klíč vám může dát záměrně špatně**, aby mohl vaši komunikaci odposlouchávat (takovýto útok se nazývá **Man In The Middle - MITM**).

- Chceme-li tomuto útoku zabránit, **je potřeba si přímo s daným kontaktem klíče ověřit** (například si zavolat a přečíst si ověřovací kódy). Jedině tak si můžeme být jisti, že pro šifrování používáme správné klíče.

babelnet

Babelnet - Automatické ověření klíčů pomocí Blockchainové databáze



- Naše aplikace **využívá pro ověřování klíčů unikátní mechanismus**, který pracuje s moderním bezpečným úložištěm, **kde není možné**, aby již jednou vložená **data kdokoliv jakkoli modifikoval**. Takovéto úložiště se nazývá blockchainová databáze.
- Veřejné **blockchainové DB jsou v současné době využívány výhradně pro kryptoměny**. Největší a nejbezpečnější z nich je DB, kterou používá **Bitcoin**. Kromě toho, že je tato DB využívána k zápisu jednotlivých Bitcoinových transakcí, je možné do ní zapisovat i jiné údaje. V našem případě koncové zařízení s aplikací Babelnet zapíše do této databáze informace potřebné pro ověření veřejného klíče, které si mohou kdykoli přečíst ostatní účastníci komunikace.
- Díky tomu tedy může kdokoli s vámi **komunikovat bez obav z útoku MITM**, aniž byste si před komunikací museli volat a ověřovat veřejné klíče.

babelnet

Babelnet

Děkujeme za pozornost

OKsystem

Filip Filipović

OKsystem a.s. / Na Pankráci 125 / 140 21 Praha 4
tel.: +420 734 525 017 / filipovic@oksystem.cz

www.babelnet.com / www.okdox.cz / www.okbase.cz / www.oksystem.cz

babelnet