Mobilní aplikace – BABEL – Šifrované SMS

BABEL encrypted text messaging

Smart Cards & Devices Forum 2013

Available on the App Store

ANDROID APP ON Google play

Mgr. Filip Filipović
Obchodní manažer

Praha, 23.5.2013

OKsystem

Obsah prezentace

Proč šifrované SMS ?

- SMS je masivně využívaná služba, registrujeme zájem uživatelů mobilních zařízení o ochranu soukromí a tajemství.
- Nedostatek podobných produktů dostupných pro širokou veřejnost na našem i světovém trhu – spojení nízké ceny a kvalitní implementace použité kryptografie.
- Spojení tradičního know-how v oblasti šifrování s vývojem mobilních aplikací.

Současný stav na trhu aplikací pro psaní textových zpráv (messenger)

Nejrozšířenější aplikace:

- Nativní SMS aplikace – nezabezpečené zprávy odesílány v „plain textu“ – potenciální riziko v případě odposlouchávání nebo pokusu o útok na takovou zprávu
- Nejpoužívanější aplikace třetích stran pro textovou a jinou komunikaci:
  - WhatsApp
  - Viber
  - BlackBerry Messenger
  - Wickr (šifrovaná komunikace)
  - TextSecure (šifrované zprávy)

→ **V čem spočívají hlavní slabiny těchto produktů ?**

Nedostatky a slabiny populárních aplikací 1/5

- Nejpopulárnější „messengery“ mají několik společných rysů:
  - Tvrzení, že zprávy jsou šifrované
  - Naději, že vaše zprávy neukládají na serverech
  - Pocit, že zaručují ochranu přenášených údajů

ALE

- Fungují na principu:
  - klient-server-klient, tedy „důvěřuj serveru“
  - Využívají datové přenosy pro zasílání zpráv (ne vždy, všude a každému dostupné)
  - Přistupují k vaším datům (adresář kontaktů), a hlavně je přemisťují na své servery – ochrana osobních údajů?

Nedostatky a slabiny populárních aplikací 2/5

- WhatsApp:
  - Využívá data a svůj server
  - Šifrování – do 8/2012 ŽÁDNÉ šifrování (zprávy chodily v plain textu), nyní „prý“ šifrují ale nikde nebylo zveřejněno jakým kryptografickým standardem
  - uploaduje VŠECHNY Vaše kontakty na svůj server (včetně těch, které nemají nainstalovaný WhatsApp) a uloží je tam
  - Spousta možností a návodů, jak aplikaci „hacknout“ (naposledy z 4/2013)

Zdroje: http://androidweeds.com/some-whatsapp-hack/, http://en.wikipedia.org/wiki/WhatsApp

Nedostatky a slabiny populárních aplikací 3/5

- Viber:
  - Aplikace od ex-člena Izraelských obranných sil (Talmon Marco), který je tvůrcem aplikaci iMesh (sdílení souborů) a Bandoo (Facebook plugin) – u obou je potvrzena skrytá instalace spywaru a podezřelé aktivity na PC uživatelů
  - Umí: číst a přijímat SMS, non-Viber zprávy a další informace z Vaší SIM karty
  - Kontakty: viz WhatsApp
  - Dále umí číst vaší polohu, nahrávat audio, video a fotit a další.
  - Žádný „Revenue/Business Model“ – společnost nevydělává, je podporována individuálními investory (sídlo na Kypru)

Zdroje: http://thehayden.org/i-refuse-to-sign-up-for-viber-heres-why/, http://viberphoneapp.wordpress.com/

Nedostatky a slabiny populárních aplikací 4/5

- BlackBerry Messenger
  - Datová služba
  - Komunikace pouze mezi BlackBerry zařízeními
  - Nutnost mít aktivovaný BlackBerry Service u operátora – dodatečné náklady (nestačí pouze data v mobilu)
  - BlackBerry PIN messages NEJSOU doslova šifrovány – jsou pouze „zakódovány“ (scrambled) univerzálním klíčem, který je stejný pro KAŽDÉ BlackBerry na světě → tzn. že jakékoliv BB zařízení dokáže přečíst zprávu z jiného BB zařízení
  - Občasné výpadky serverů v Kanadě:
    - 2011 – zasáhnuta Evropa, Střední Východ, Afrika, Indie a Severní Amerika
    - 2012 – zasáhnuta Asie

Zdroj: http://www.berryreview.com/2010/08/06/faq-blackberry-messenger-pin-messages-are-not-encrypted/

Nedostatky a slabiny populárních aplikací 5/5

- Wickr – aplikace pro šifrovanou komunikaci
  - Vyžaduje datové spojení
  - Nutnost věřit třetí straně – zprávy chodí přes server
  - JEN iOS verze

- TextSecure – aplikace pro šifrovanou komunikaci
  - Kompatibilní pouze s operačním systémem Android

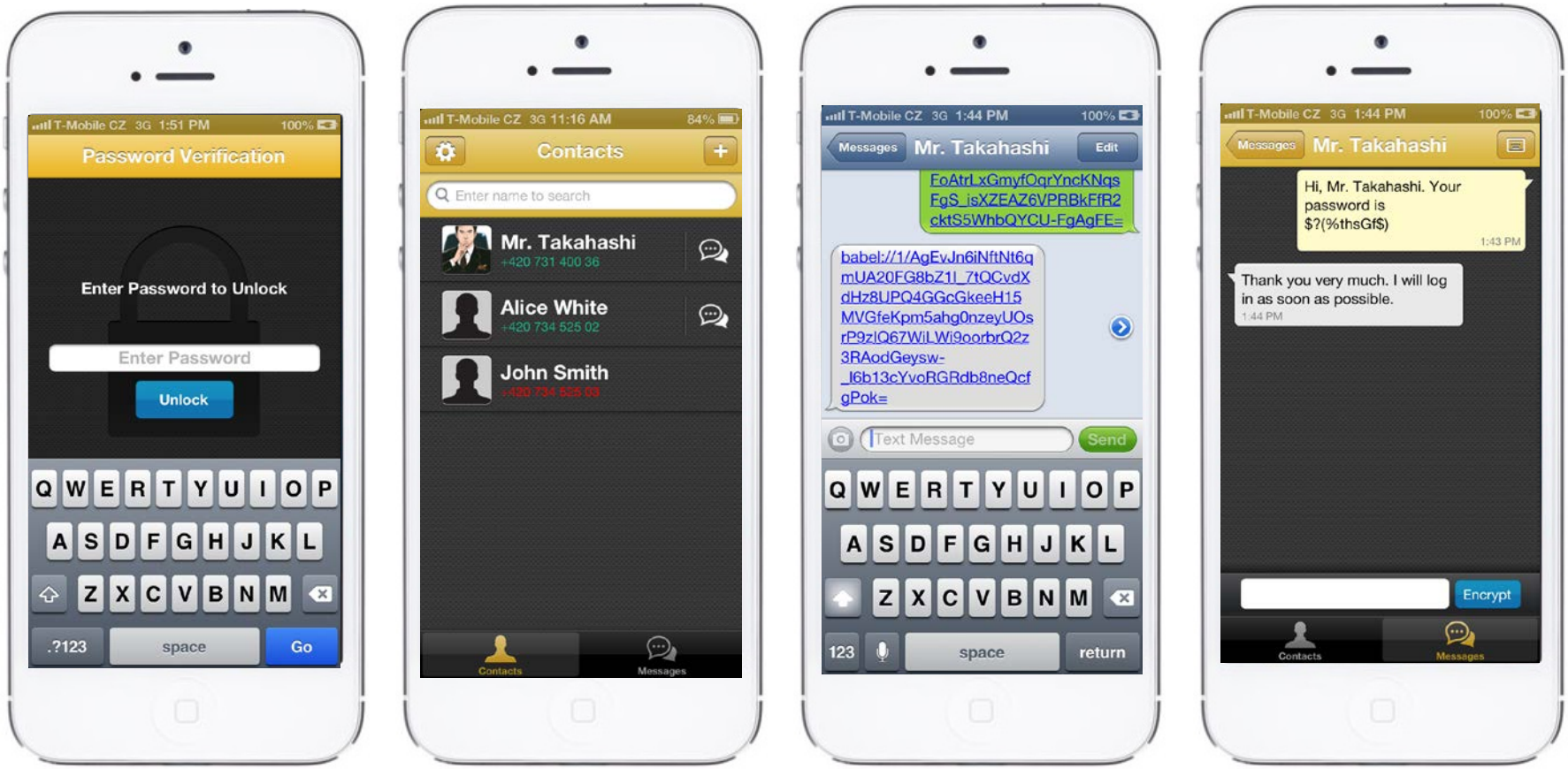
Představení aplikace BABEL

- Maximálně jednoduché, avšak profesionální řešení zasílání BEZPEČNĚ šifrovaných textových zpráv bez využití třetí strany – serveru a bez nutnosti datového spojení.
- Vytvořili jsme tedy platformu, díky které si uživatele naší aplikace mohou bezpečně posílat šifrované zprávy s principem End-to-End encryption – tzn. šifruje se na straně koncových uživatelů (na jejich zařízeních) a ne „někde“ v cloudu, na serveru, po cestě…
- Proč název „BABEL“ ?

Pro více informací navštivte www.getbabel.com

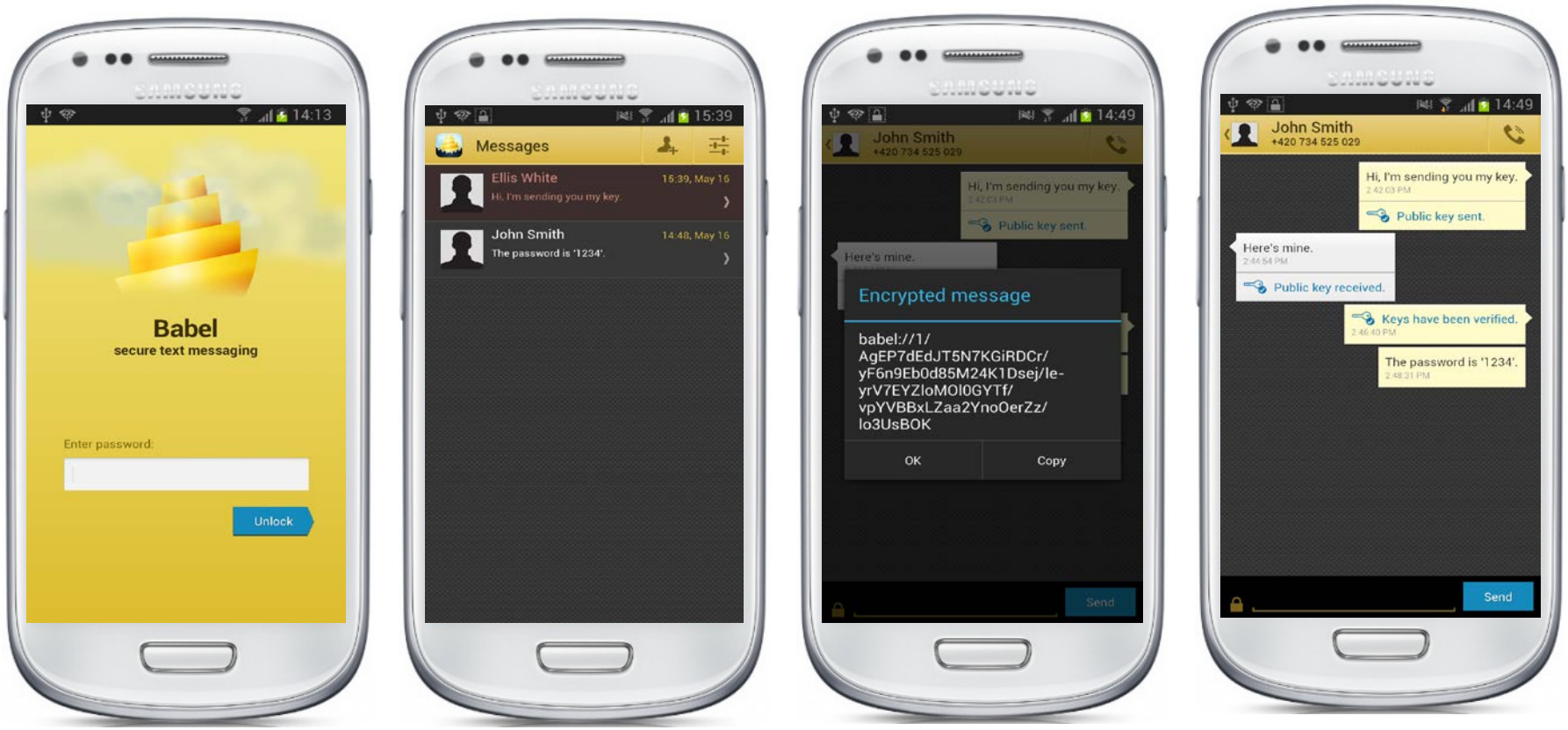
Uživatelské prostředí – iOS verze 1/2

BABEL na Apple iPhone 5:



Uživatelské prostředí – Android verze 2/2

BABEL na Samsung S3 (Android v 4.1.2):



Hlavní vlastnosti aplikace BABEL

- Výhody a rozdíly oproti existujícím řešením:
  - Cross-platform řešení – možnost komunikace na platformách Apple iOS a Google Android
  - Žádná třetí strana, nebo centrální server – jediný komu musíte věřit je Vaše protistrana
  - Datové spojení není vyžadováno, BABEL využívá standardní SMS protokol (pro iOS na obou stranách komunikace automaticky využije iMessage pro přenos šifrované zprávy, pokud je k dispozici datové spojení)
  - Aplikace a použité šifrovací algoritmy jsou klasifikovány a prostřednictvím procesu SNAP-R registrovány pro povolení exportu silné kryptografie z USA (nutná podmínka pro nahrání na AppStore)
  - BABEL používá prověřené a standardní algoritmy se silnou kryptografií – AES pro šifrování textových zpráv a Diffie-Hellman pro prvotní výměnu klíčů
  - Zprávy zůstávají šifrované nejen při odesílání, ale i v samotném zařízení
  - Jednoduché a přívětivé uživatelské rozhraní

Cíl aplikace BABEL - příklady využití

- Hlavním a nejpodstatnějším cílem aplikace BABEL je chránit soukromí uživatelů a jejich textové komunikace před možnými útoky
- Příklady využití:
  - Důvěrná komunikace mezi obchodními partnery prostřednictvím smartphonu, kdykoliv a kdekoliv (SMS na rozdíl od datové nebo hlasové komunikace „odejde“ téměř vždy a všude, odpadá nutnost nosit notebook a pořizovat certifikáty kvůli šifrování)
  - Posílání citlivých údajů (přihlašovací hesla, různé PINy, přístupy k emailům, atd.)
  - Běžná komunikace s nejvyšší úrovní bezpečnosti (náhrada za SMS klient, nebo jiný messenger)

Kryptografie – algoritmy, klíče

- Použité kryptografické algoritmy
  - Diffie-Hellman (RFC 2631, NIST SP 800-56A) pro nalezení shody na hodnotě pro odvození klíče
  - AES (FIPS PUB 197) pro šifrování klíčů a zpráv
  - PBKDF2 (PKCS#5) pro odvození klíčů z hesla
  - KDF (RFC 2631) pro odvození klíče z hodnoty nalezené pomocí D-H.
- Kryptografické klíče
  - Klíč uživatele (AES) – odvozen z hesla uživatele. Šifruje klíč zařízení
  - Klíč zařízení (AES) – náhodně generován při instalaci BABEL. Šifruje klíče kontaktů
  - Klíče kontaktů (AES) – odvozeny z hodnoty nalezené pomocí výměny D_H. Šifrují klíče zpráv vyměňované s daným kontaktem
  - klíče zpráv (AES) – náhodně generovány pro každou zprávu. Šifrují odesílané zprávy.
- Heslo uživatele
  - Základní bezpečnostní prvek, který chrání zprávy uložené ve smartphonu
  - Z hesla je odvozen klíč uživatele
  - Heslo odemyká obrazovku aplikace
  - Heslo lze měnit.

Jak BABEL funguje ?

- Ukázka na projektoru – iOS a Android:
  - Spuštění aplikace
  - Výměna klíčů
  - Ověření autentizačních kódů
  - Odeslání a příjem SMS
  - Zamknutí obrazovky (BABEL lock)

BABEL download – dnes ZDARMA!

BABEL encrypted text messaging

- Stahujte “BABEL – Encrypted Messaging” pro Apple iPhone z App Store (iTunes) – dnes a zítra pro návštěvníky SmartCard fóra ZDARMA! (jindy 1,99$)
- Stahujte “BABEL – Encrypted Messaging” pro smartphony s Androidem z Google Play (39 Kč)
- Nebo navštivte www.getbabel.com pro více informací

OKsystem

Mgr. Filip Filipović
filipovic@oksystem.cz

OKsystem s.r.o.
Na Pankráci 125
140 21 Praha 4
tel: +420 236 072 112
Mob: +420 734 525 017
www.oksystem.cz

Otázky?

Děkujeme za pozornost