PRIVACY-PRESERVING INSTANT MESSAGING APPLICATION

Štefan Krajanec
Master, FEKT BUT
E-mail: xkraja00@feec.vutbr.cz

Supervised by: Petr Dzuenda
E-mail: dzurenda@vutbr.cz

Abstract: Instant messaging applications noted significant grow especially in the last decade. In fact, the Internet communication is cheap and convenient way how to communicate with distant people. However, this grow of user communication and data exchange through the online world impacts user security and privacy, as it was also shown recently by WhatsApp privacy issues. Firstly this article evaluates security and privacy issues of current mobile messaging applications. Secondly, we design our basic open source solution with the focus on security, privacy, and user centric features. Furthermore, we provide proof-of-concept implementation of our system.

Keywords: Privacy, Security, Instant Messaging, Android, Metadata

1 ÚVOD

Mobilné aplikácie sú neodmyslitelnou súčasťou života ľudí po celom svete. Pred pár rokmi bol odštartovaný trend IM (Instant Messaging) aplikácii, ktoré sú v súčastnosti masovo používané. Avšak, dodnes sa nekladie dostatočný dôraz na súkromie ich užívateľov. Súkromie ale nie je prioritou, spoločnosti hromadia a spracúvajú užívateľské dáta skôr za účelom vytvorenia profitu. Napríklad Facebook, dokáže na každom aktívnom užívateľovi zarobiť každý štvrťrok minimálne 10 $ na cielených reklamách a táto suma sa zväčšuje každým štvrťtrokom o 10 % [1].

Väčšina IM aplikácii v skutočnosti nejakým spôsobom šifruje správy užívateľov (často ale nie End-to-End), ale aktívne pracuje s ich metádatami. Tie sú často odosielané buď s obsahom správy alebo v pravidelných intervaloch [3]. Treba brať na vedomie fakt, že hoci v metadátach nie je prenášaný samotný obsah správy, ale ich vystavenie môže mať značný vplyv na súkromie užívateľa [4]. Napríklad, ak zamestnanec väčšiej organizácie (vláda, veľká spoločnosť) komunikuje s novinárom za účelom odhalenia určitej pofidérnej činnosti, je možné, na základe metadát túto komunikáciu odhaliť.

Tento článok predstavuje návrh IM systému zameraný na zaistenie ochrany súkromia jeho uživatelov a nemožnosti profilovania či sledovania. Navrhnutý systém je uživatelsky centralizovaný, uživatel má všetky svoje dáta pod kontrolou, tj. môže mazať svoje správy, nastavovať ich životnosť či obmedziť množstvo informácii odhalovaných posktovatelom služby. Celý projekt je cielený na open source riešenie, to znamená, že IM systém môže byť prevádzkovaný samotnými uživatelmi, ktorí sa nemusia spoliehať na nadkorporátne společnosti. Napríklad nie je tak dávno, kedy sa zaktualizovali podmienky používania služby Whatsapp od Facebooku a užívatelia v miliónoch túto sociálnu sieť začali opúšťať [2].

1.1 BEZPEČNOSTNÉ POŽIADAVKY NA IM APLIKACE

Porovnanie bezpečnosti našej aplikace Grobardo s najpoužívanejšou konkurenciou je prehladne naznačané v tabuľke 1. Navrhnutý systém podporuje mnoho ďalších vlastností, ktoré umožňujú dosiahnuť vyššieho súkromia užívateľov a dávaju užívateľom väčšiu kontolu nad ich dátami, napríklad:

1) nastavenie životnosti správ po ktorej sa úplne odstránia zo systému aj keď je kľúč platný, 2) limitovanie informácii poskytnutých oponentovi (napr. komunikovanie pod dočasným pseudonymom), 3) žiadosť o povolenie vykonať screenshot obrazovky, 4) nastavenie životnosti všetkým typom správ (počet otvorení, možnosť otvorenia na celú obrazovku), 5) odoslanie informácie o prečítaní správy oponentom. Navrhnuté riešenie umožňuje užívateľom využívať vlastný server so správami a réžiou miestnosti, na ktorý sa aplikácia pripojí len jednoduchou zmenou endpointov. Všetky servery okrem autorizačného je možné naklonovať a rozbehnúť vlastný server aplikácie. Vďaka tomu je možné pri prvom spustení aplikácie určiť, ku ktorému serveru sa bude zariadenie pripájať, de facto na ktorom serveri budú uložené užívateľove kľúče. Ten, kto si stiahne, nakonfiguruje a spustí servre vytvorené v tejto práci, si po prihlásení do aplikácie vpíše cestu k svojim servrom.

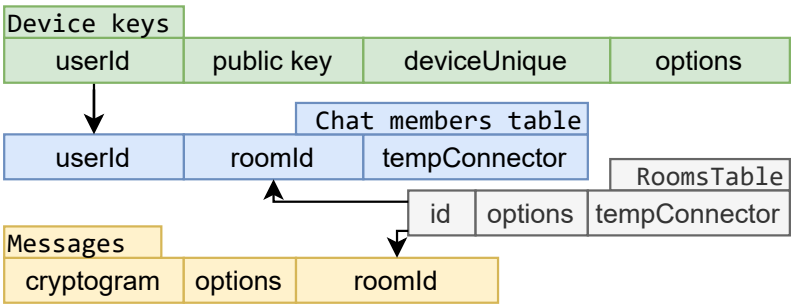
Tabulka 1: Porovnanie bezpečnosti aktuálne najvýznamnejších IM app.

	Whatsapp	Threema	Facebook	Signal	Telegram	Grobardo
Poskytovanie dát tretím stranám	ano	nie	ano	nie	ano	nie
Uchovávanie a zber užívateľských dát	ano	nie	ano	nie	ano	nie
Zálohovanie dešifrovacieho kľúča na serveri	áno	nie	áno	nie	áno	nie
Logovanie času a IP	nie	nie	áno	áno	nie	nie
Samozničujúce správy	áno	nie	áno	áno	áno	áno
Užívateľská réžia kľúčov	nie	nie	nie	ano	nie	ano
Úplné odstránenie odoslaných správ	nie	nie	nie	ano	nie	ano
Zneprístupnenie zariadení	áno	nie	áno	ano	nie	ano
Réžia práv oponenta	nie	nie	nie	nie	nie	áno
Open source	nie	nie	nie	ano	ano	ano
Klonovateľný kód serverov s plnou réžiou	nie	nie	nie	nie	nie	ano

2 ARCHITEKTURA NAVRHNUTÉHO SYSTÉMU

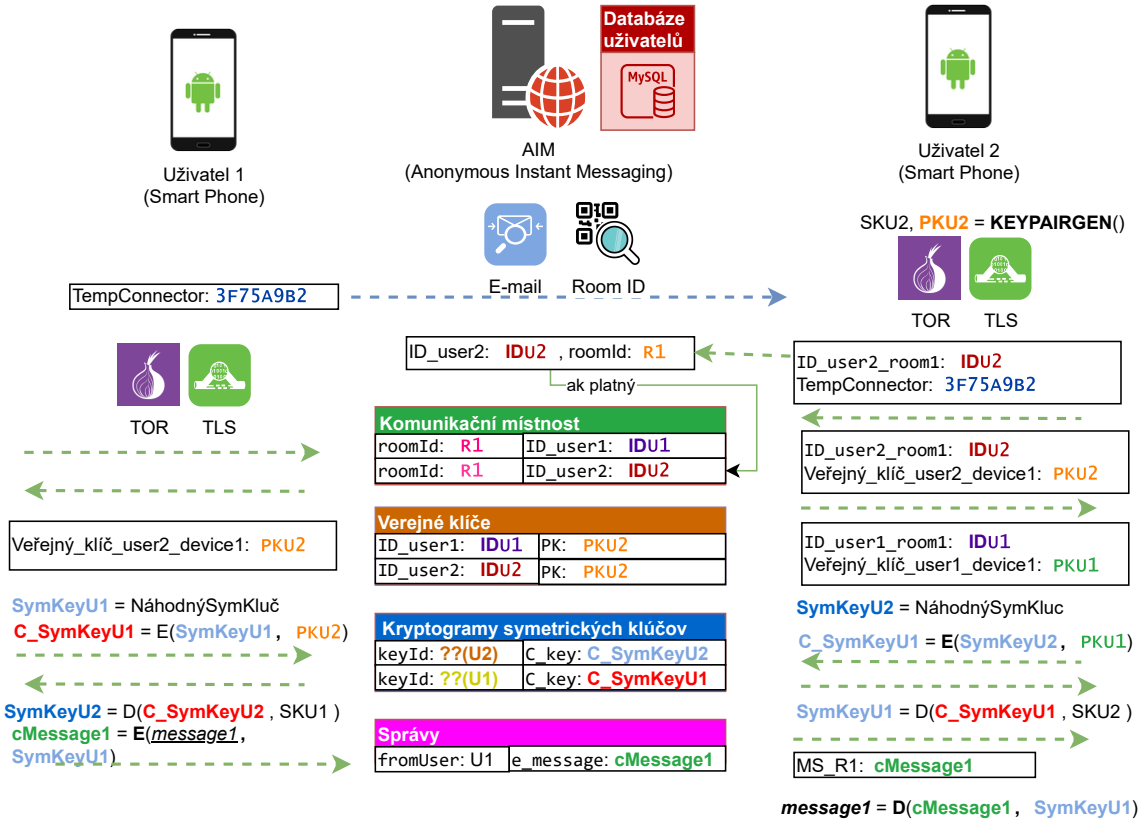
Navrhnutý IM systém je založený na inovatívnom návrhu databázových tabuliek. Základom je tabuľka miestností, v ktorej je najdôležitejším identifikátorom ID miestnosti a dalšie konfiguračné dáta. Ďalšia tabuľka obsahuje informáciu, aký užívateľ (`userId`) sa nachádza v ktorej miestosti (`roomId`). Posledná najdôležitejšia tabuľka obsahuje správy, kde každý riadok obsahuje šifrovanú správu, identifikátor miestností do ktorej správa patrí a ID užívateľa, ktorý správu odoslal plus ďalšie konfiguračné dáta. Základná architektúra tabuľkového systému a ich závisostí je zobrazená na obrázku 1. Návrh je multifunkčný, ale aktuálne je implementovaný len na android OS.

Systém je implementovaný pomocou troch klonovatelných open source serverov, ktoré zastrešujú správnu distribúciu kľúčov a ukladanie správ (kryptogramov). Medzi neklonovatelné servery patria tie, ktoré zabezpečujú autentizáciu užívateľa a autorizáciu zariadení. Momentálne je používaný jeden volitelný server, vďaka ktorému sú na zariadenia správne doručované notifikácie v prípade novej správy alebo nového člena v miestnosti, rozširovaním funkcionalit v aplikácii bude narastať počet volitelných serverov.



Obrázek 1: Základná architekrúra tabuľkového systému.

Vďaka návrhu distribúcie kľúčov, je každá správa šifrovaná symetrickým kľúčom a uložená na server do už spomínanej tabuľky. Správny kľúč k danej správe majú len jej adresáti a odosielateľ. A do miestnosti sa nedostane užívateľ, ktorý do nej nebol pozvaný a ak by sa tam nejakým spôsobom dostal alebo by nejakým spôsobom dokázal zistiť, ktoré správy patria do miestnosti na ktorú útočí, tak bude vidieť len kryptogramy správ ku ktorým nemá kľúč. Kľúč má len zariadenie, ktoré bolo do miestnosti pozvané z vnútra. Princíp komunikácie medzi dvoma zariadeniami v miestnosti je zobrazený na obrázku 2.

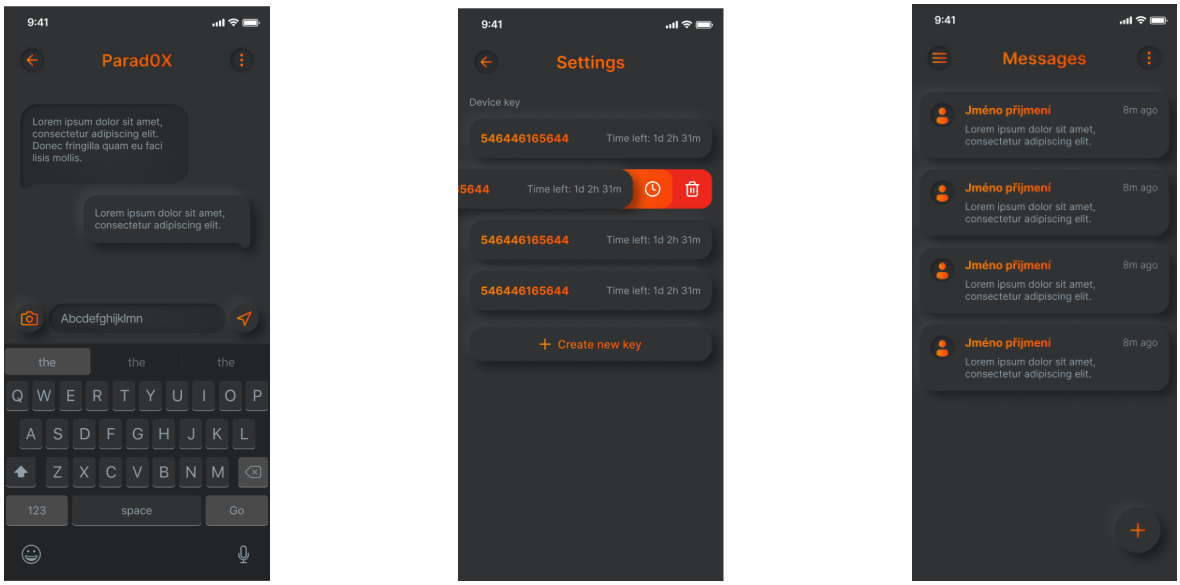


Obrázek 2: Princip konvrzácie pomocou miestnosti.

2.1 Implementácia systému

Technológie, pomocou ktorých bol implementovaný proof-of-concept systém, ktorý obsahuje: Vývoj len na operačný systém `Android` s programovacím jazykom Kotlin Android 5.+, programovací jazyk na serveri `Golang` a príležitostne `Python` používajúc technológie `GRPC` - diaľkové

volanie procedúr od Googlu, umožňuje reaktívny prístup komunikácie serveru s aplikáciou spolu s `PostgreSQL` - voľne šíriteľný objektovo-relačný databázový systém, komunikácia zariadení so serverom cez `TOR` sieť a kryptotechnologie: 1.) hashovacia funkcia - `SHA-256` pre integritu dát, 2.) symetrická šifra - `AES-256` pre šifrovanie dát pred serverom a 3.) `RSA-2048` - asymetrická šifra - na distribúciu symetrických kľúčov. Obrázok 3 zobrazuje snímky obrazovky vytvorenej aplikácie pre instant messaging.



Obrázek 3: Screeny IM aplikácie (zľava): správy v miestnosti, správa kľúčov a dostupné chaty

3 ZÁVER

V článku sme predstavili návrh IM systému zvyšujúci ochranu súkromia užívateľov a ich kontrolu nad ich dátami. Podarilo se overiť funkčnosť teoretického návrhu systému a implementovať základnú funkcionalitu distribúcie kľúčov, odosielanie a prijímanie správ, vytvorenie a pripojenie do miestnosti, zobrazovanie a aktualizovanie správ, miestností a kľúčov. Aplikácia ešte neobsahuje všetky požadované funkcionality. Keď sa uzatvorí vývoj distribúcie kľúčov a šifrovania bude čas maximálne zredukovať citlivé dáta (id) v prepojených tabuľkách na šifrovanú prípadne zahashovanú podobu, tak aby nebolo možné bez kľúčových znalostí dopátrať adresátov správ. Ďalšími plánovanými krokmi je doimplementovať zvyšnú funkcionaitu ako odosielanie obrázkov, konfigurácia jednotlivých správ, miestností a užívateľov, a integrovanie ToR technológie pre anonymnú komunikáciu cez internet.

REFERENCE

[1] *Facebook Q4 and full Y2020* https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx

[2] *Is it time to leave WhatsApp* https://www.theguardian.com/technology/2021/jan/24/is-it-time-to-leave-whatsapp-and-is-signal-the-answer

[3] *26th Symposium on Operating Systems Principles: A Distributed Metadata-Private Messaging System*. s. 440. ISBN 978-1-4503-5085-3. https://dl.acm.org/citation.cfm?id=3132783

[4] Stefan Schiffner. Privacy and Data Protection by Design - from policy to engineering. *CoRR*. 2015, 79. Dostupné také z: http://arxiv.org/abs/1501.03726