DOI: 10.15199/13.2017.5.3

Kryptograficzne technologie zabezpieczania poufności transmisji. Stan obecny

(Cryptographic technologies protect the confidentiality of the transmission. State-of-the-art)

dr inż. WOJCIECH NOWAKOWSKI, prof.

Instytut Maszyn Matematycznych, Warszawa

Streszczenie

Opisano stan wiedzy dotyczący kryptograficznego zabezpieczania wymiany informacji głosowych i tekstowych

Słowa kluczowe: ChatSecure, CryptoCat, Signal, Redphone, TextSecure, Silent Circle, ZRTP

Abstract

The state of cryptographic protection of information exchange, voice and text, is described

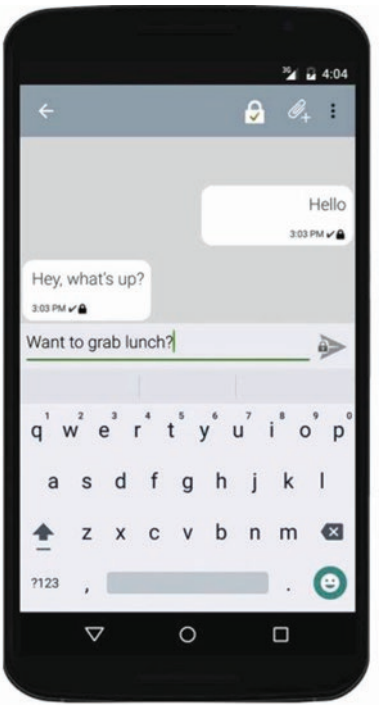
Keywords: ChatSecure, CryptoCat, Signal, Redphone, TextSecure, Silent Circle, ZRTP

W obliczu powszechnego nadzoru i śledzenia sieci bardzo ważne dla wielu internautów jest zabezpieczenie ich telefonów i komputerów przed posłuchem i ingerencją obcych w ich prywatne treści. Do niedawna nieźle zabezpieczona przed ingerencją osób trzecich była jedynie usługa e-mail dzięki leciwemu, choć stale uwspółcześnianemu protokołowi PGP Phila Zimmermanna. O tajność informacji w sieciach publicznych, a zwłaszcza w telefonii komórkowej dbały przede wszystkim administracje centralne i wielki biznes.

Od kilku ostatnich lat jednak infiltracja ruchu informatycznego, również prywatnego, przez służby, wynajmowanych hakerów czy konkurencyjnego biznesu stała się powszechna. Odpowiedzią rynku na ten proces była płatna usługa *Silent Phone* (SP) opisana w dalszej części artykułu. Może nieco później, ale również w związku z opublikowaniem przez wspomnianego autora PGP zmodyfikowanego protokołu ZRTP potrzebnego do wspomnianej usługi SP nastąpił żywiołowy rozwój oprogramowania utajniającego prywatna wymianę informacji w internecie. Już opublikowano ponad 100 różnych aplikacji typu *Secure Messaging*, wykorzystujących algorytmy kryptograficzne, których celem jest zapewnienie bezpieczeństwa kontaktów w sieci. Co wiecej, powstały niezależne serwisy internetowe, zajmujące się badaniem tych aplikacji i stopnia bezpieczeństwa, jaki one zapewniają [4]. Okazuje się, że naprawdę bezpiecznych narzędzi do utajniania korespondenci cyfrowej, zarówno głosowej jak i tekstowej, jest zaledwie kilka. Poniżej zostały one przedstawione. Należy przy tym zauważyć, że wypracowanie choćby listy kryteriów przeprowadzanej oceny jest trudne i jednocześnie, jak to zostanie pokazane dalej, odkrywcze. Oto krótkie przedstawienie aplikacji, które zostały ocenione jako bezpieczne.

- ***ChatSecure*** [5] jest darmowym i typu *open source* tzw. klientem IRC czyli oprogramowaniem korzystającym z serwerów sieci IRC (*Internet Relay Chat*) dla iPhone i Android, które obsługuje szyfrowanie OTR (*Off-the-Record Messaging*) z zastosowaniem szyfrów *SQLCipher* do zabezpieczenia dzienników rozmowy. OTR to protokół kryptograficzny, zapewniający silne szyfrowanie dla tzw. konwersacji błyskawicznych, czyli *instant messaging*. OTR używa kombinacji algorytmu klucza symetrycznego AES, protokołu Diffiego-Hellmana i funkcji skrótu SHA-1 na XMPP. XMPP, czyli *Extensible Messaging and Presence Protocol* (dawniej *Jabber*), to protokół na bazie języka XML zapewniajacy przesyłanie w czasie rzeczywistym wiadomości oraz kodów statusu. Głównym zastosowaniem protokołu XMPP jest wymiana wiadomości w komunikatorach internetowych. Protokół XMPP jest publicznie dostępny i podlega swobodnej modyfikacji. Klienty, serwery oraz biblioteki są często udostępniane jako Oprogramowanie Wolne i Otwarte. Serwery XMPP mogą współpracować z innymi protokołami oraz obsługiwać pocztę elektroniczną.

ChatSecure wykorzystuje do szyfrowania tylko dobrze znane biblioteki kryptograficzne typu *open source*. Jakkolwiek inne aplikacje reklamują często „militarny” stopień bezpieczeństwa, jednak bez publicznej kontroli i weryfikacji kodu źró-



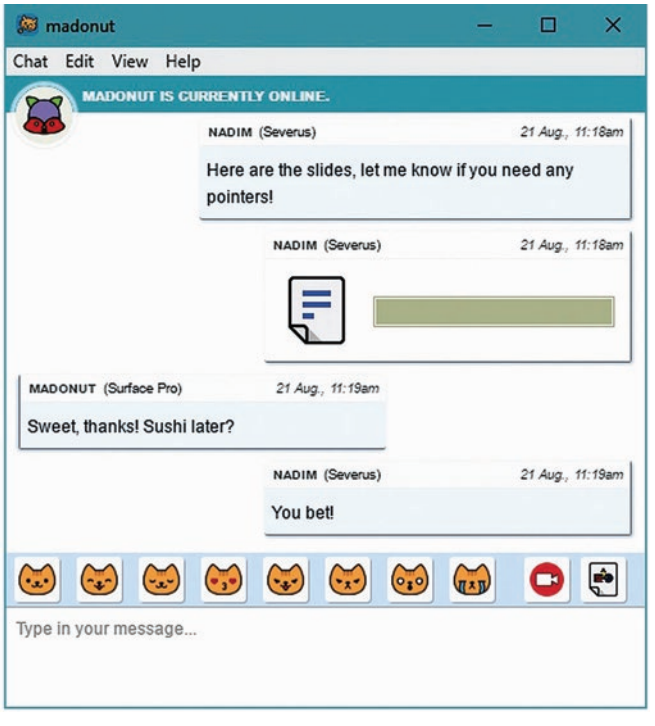
Rys. 1. *ChatSecure* w Android [5]
Fig. 1. *ChatSecure* Android screenshot [5]

dłowego nie można być pewnym, że szyfrowanie jest pewne. *ChatSecure* szyfruje czatowanie. Spełnia wszystkie kryteria EFF (*Electronic Frontier Foundation* [6]), ale tylko wtedy, gdy jest używana wspólnie z wtyczką prywatności *Orbot* [7], obsługiwaną przez sieć *Tor*. Jest to aplikacja, która dzięki serwerom *proxy* daje możliwość anonimowego przeglądania sieci. Niestety samo zainstalowanie odpowiedniej aplikacji nie zapewnia bezpieczeństwa sukcesu. Większość mobilnych klientów sieci Tor można łatwo zmusić do wyjawienia prawdziwego adresu IP [9].

- ***CryptoCat*** [10] jest usługą komunikacji szyfrowanej w kodzie otwartym (*open source*) napisanym przez Nadima Kobeissi w 2011 roku. Jest on dostępny na platformach Windows, Linux and Mac, do przeglądarek Chrome, Firefox, Safari i Opera, systemu operacyjnego OS X i smartfonów iPhone. Spodziewana jest wersja dla Androida oraz szyfrowany czat wideo. Oprogramowanie *CryptoCat* jest wspierane przez *Electron* [11], *Prosody* [12], *Red Hat Enterprise Linux* [13], *Fedora* [14], *Microsoft Azure* [15] i *Node.js* [6].

Każda wiadomość przesyłana przez *CryptoCat* jest szyfrowana. Czaty są bezpieczne, nawet jeśli klucze zostały skradzione. *CryptoCat* wykorzystuje bowiem algorytm *Double Ratchet* (ratchet to po polsku mechanizm zapadkowy, grzechotka), opracowany przez Trevora Perrina i Moxie Marlinspike'a w roku 2013. Po wstępnej wymianie kluczy mechanizm ten zarządza odnowę i wykorzystanie krótkotrwałych kluczy sesyjnych w protokole Diffie-Hellmana (DH) z wydłużaniem klucza (KDF, *key derivation function*), np. za pomocą funkcji *hash* [17] (dlatego jest też nazywany podwójnym mechanizmem zapadkowym). W warstwie transportowej *CryptoCat* wykorzystuje protokoły XMPP otaz TLS (*Transport Layer Security* – standard stanowiący rozwinięcie protokołu *Secure Socket Layer*, SSL) oraz *WebSocket* – technologię zapewniającą dwukierunkowy kanał komunikacji za pośrednictwem jednego gniazda TCP.

CryptoCat jest oprogramowaniem bezpłatnym, tworzonym by umożliwić wszystkim wymianę informacji zabezpieczoną przed ingerencją prywatną.



Rys. 2. Ekran komunikatora *CryptoCat* w Android [10]
Fig. 2. *CryptoCat* screenshot [10]

Signal, Redphone, TextSecure [18]

Signal, *RedPhone* i *Textsecure* są produktami Open Whisper Systems. *Signal* to bezpieczna platforma komunikacji dla iOS. *RedPhone* i *Textsecure* to bezpieczne platformy wykonywania połączeń oraz przesyłania wiadomości tekstowych dla Androida.

Signal jest szyfrowanym komunikatorem tekstowo-graficzno-głosowym dla telefonów komórkowych z systemami operacyjnymi Android i iOS. Umożliwia przesyłanie informacji w internecie zarówno indywidualnych (1:1) jak i grupowych. Do identyfikacji *Signal* wykorzystuje standardowe numery telefonów komórkowych i szyfruje end-to-end zabezpieczając całą komunikację - rozmowy głosowe i video. Aplikacja zawiera mechanizmy, dzięki którym użytkownicy mogą samodzielnie zweryfikować tożsamość swoich korespondentów oraz i integralność kanału danych. Aplikacja Chrome, które mogą łączyć się z klientem sygnału jest także w rozwoju. Klienci korzystają z bezpłatnego i otwartego oprogramowania klienckiego na licencji GPLv3. Kod serwera jest publikowany częściowo na licencji AGPLv3, choć jest częściowo zastrzeżony.

Signal jest następcą szyfrowanej aplikacji głosowej o nazwie *RedPhone* i szyfrowanego programu tekstowego *TextSecure*. Wersje beta obu aplikacji ogłoszono w maju 2010 roku przez Whisper Systems, start-up współfinansowany przez badacza bezpieczeństwa Moxie Marlinspike i Stuarta Andersona. Whisper Systems wyprodukował także *firewall* i narzędzia do szyfrowania innych form danych. Wszystkie te aplikacje były zastrzeżone dla przedsiębiorstw opracowujących mobilne oprogramowanie zabezpieczające i dostępne tylko na platformie Android.

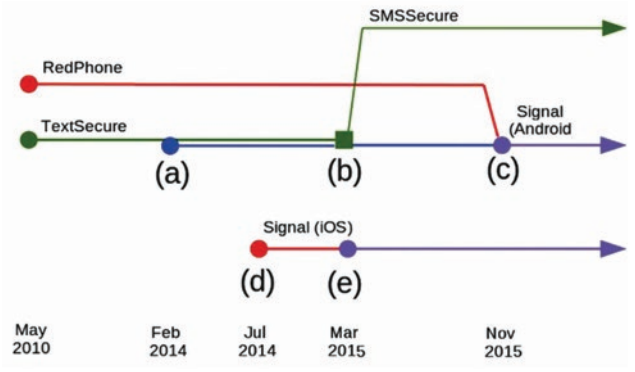
W listopadzie 2011 r. Whisper Systems ogłosiła, że została przejęta przez Twittera. Twitter wydał *TextSecure* jak oprogramowanie wolne i otwarte na licencji GPLv3 w grudniu 2011 roku . *RedPhone* został wydany na podstawie tej samej licencji w lipcu 2012 roku. Moxie Marlinspike wkrótce opuścił Twittera i założył firmę *Open Whisper Systems* celem dalszego rozwoju TextSecure i RedPhone. Otwarte Whisper Systems (2013-obecnie).

Kalendarium rozwoju *Signal*

W lutym 2014 roku Open Whisper Systems opublikował drugą wersję protokołu przesyłania wiadomości dodając do szyfrowania *end-to-end* czatu grupowego i innych funkcji komunikatora. Pod koniec tego roku firma ogłosiła plany ujednolicenia jej aplikacji *RedPhone, TextSecure* i *Signal*. Zapowiedziała także wersję dla systemu iOS i uruchomić klienta WWW. *Signal* był pierwszą darmową aplikacją na iOS. TextSecure dodano do iOS w 2015 r.

Cała komunikacja z innymi użytkownikami jest w *Signal* automatycznie szyfrowana *end-to-end* . Klucze wykorzystywane do szyfrowania komunikacji użytkownika są generowane i przechowywane przez użytkowników, a nie przez serwery. *Signal* posiada również wbudowane mechanizmy weryfikacji przeciwko atakom *man-in-the-middle*.

Połączenia głosowe są szyfrowane protokołami znanymi nam już z Silent Circle (SRTP, ZRTP) opracowanymi przez Phila Zimmermanna [1]. *Signal instant messages* są szyfrowane za pomocą protokołu *Signal* (dawniej znanego jako protokół Axolotl), który zawiera w sobie wspomniany już algorytm z podwójną „grzechotką". Wykorzystuje on Curve25519, AES-256 oraz HMAC-SHA256 jako algorytmy pierwotne. Protokół ten zapewnia poufność, integralność, uwierzytelnianie, spójność walidację docelowego uczestnika, *forward secrecy, backward secrecy* i asynchroniczność. Nie zachowuje anonimowości i wymaga serwerów do przekazywania komunikatów i przechowywania materiału klucza publicznego



Rys. 3. Kalendarium rozwoju *Signal*. a) Dodanie szyfrowanego czatu grupowego oraz możliwości przesyłania *Instant Messaging* do *TextSecure* b) Koniec szyfrowania wiadomości SMS / MMS w TextSecure, co przyczyniło się do stworzenia odgałęzienia c) Wersja Signal dla Androida została uruchomiona zaraz po włączeniu *RedPhone* do *TextSecure*. d) *Signal* dla iOS został uruchomiony jako część *RedPhone* dla iOS. e) Dodanie szyfrowanego czatu grupowego i *instant messaging* do wersji iOS Signal
Fig. 3. A timeline of the development of *Signal*. a) Addition of encrypted group chat and instant messaging capabilities to TextSecure. b) End of encrypted SMS/MMS messaging in TextSecure, which prompted the creation of a fork. c) The Android version of Signal was launched after RedPhone was merged into TextSecure. d) Signal for iOS was launched as a RedPhone counterpart for iOS. e) Addition of encrypted group chat and instant messaging capabilities to the iOS version of Signal

Signal dziś

Obecnie kompletne kody źródłowe Signal dla Android, iOS i Google Chrome dostępne są na GitHub na wolnej licencji. To umożliwia zainteresowanym stronom analizowanie kodu oraz pomaga programistom sprawdzenie ich działania. Pozwala również zaawansowanym użytkownikom skompilowanie własnych kopii aplikacji i porównanie ich z wersjami dystrybuowane przez Open Whisper Systems. Oprogramowanie *Signal*, które obsługuje routing komunikatów czyli TextSecure-Server i jest również open source. *Signal* jest oficjalnie rozprowadzany wyłącznie za pośrednictwem Google Play, App Store firmy Apple i Chrome Web Store.

Były pracownik NSA Edward Snowden potwierdzał wielokrotnie wysoką jakość narzędzia *Signal*. We wrześniu 2015 roku, amerykańska Unia Swobód Obywatelskich zaleciła używanie oprogramowania kryptograficznego *Signal*, pisząc:

„...Jedno z najbardziej powszechnie szanowanych szyfrowanych aplikacji komunikacyjnych, Signal, od Open Whisper Systems, otrzymała znaczną pomoc finansową od rządu USA, została zbadana przez niezależnych ekspertów od bezpieczeństwa i jest obecnie powszechnie stosowana przez specjalistów od bezpieczeństwa komputerowego...".

Po 2016 roku Krajowy Komitet Partii Demokratycznej, po przecieku korespondencji Hillary Clinton, polecił prawnikom korzystać wyłącznie z komunikatora *Signal* , który jest obecnie rozwijany przez grupę non-profit Open Whisper Systems. Grupa ta jest finansowany poprzez skomasowanie dotacji i grantów, a wszystkie jej produkty są publikowane jako oprogramowanie wolne i otwarte [10].

Silent Circle

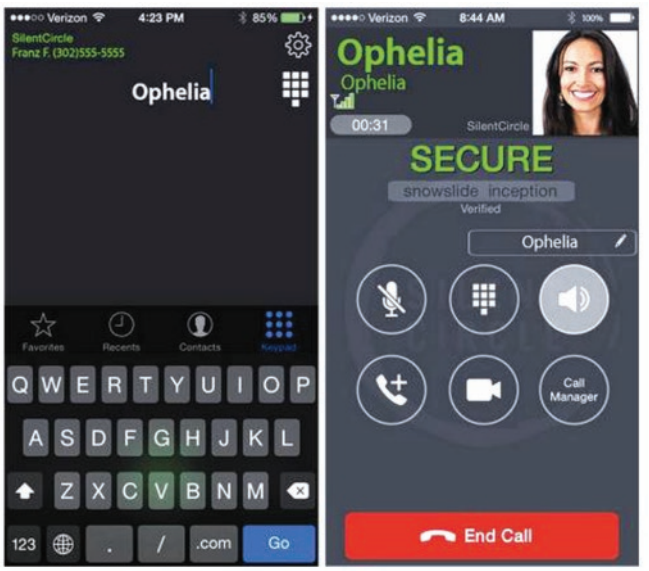
Silent Phone i Silent Text należą do firmy Silent Circle i są to bezpieczne usługi wykonywania połączeń i pisania. Wprawdzie są płatne, ale są kompatybilne z systemem iOS i Android, a także działają na tradycyjnych komputerach. Silent Circle stworzył także swój własny bezpieczny dedykowany smartfon o nazwie Blackphone, na którym znajduje się zmodyfikowany kryptograficznie system operacyjny Android. Firma zapewnia przede wszyskim wsparcie dla klientów korporacyjnych.

Twórcami projektu **Silent Circle** byli: Phil Zimmermann, autor powszechnie stosowanego w internecie protokołu **PGP** (ang. *Pretty Good Privacy,* całkiem niezła prywatność) zapewniającego poufność poczty elektronicznej, Mike Janke, były specjalista od zabezpieczeń US Navy SEAL oraz Jon Callas, współautor oprogramowania szyfrującego zawartość dysków twardych (*Whole Disk Encryption Apple*). Oni właśnie w 2011 roku powołali firmę *Silent Circle* dla stworzenia pierwszej na świecie prywatnej bezpiecznej łączności cyfrowej, zarówno głosowej, tekstowej jak i wideo, a także transmisji plików. Obecnie *Silent Circle* jest uznaną firmą zapewniającą rzeczywiście bezpieczną komunikację cyfrową dzięki wykorzystaniu technologii kryptograficznych mając miliony użytkowników w ponad 130 krajach świata [2].

Silent Network. Podstawą działania cyfrowej łączności szyfrowanej firmy *Silent Circle* jest *Silent Network*, czyli zamknięta, nie współdzielona sieć prywatna. Składa się ona z dedykowanych serwerów, kodeków, szeregu urządzeń specjalnych i oprogramowania, specjalnie zaprojektowanych dla zapewnienia bezpieczeństwa informacji (ang. *security integrated through design*), w czym twórcy firmy są uznanymi autorytetami. Sieć *Silent Network* jest siecią równorzędną typu każdy z każdym (*peer-to-peer*, P2P), której architektura zapewnia równoważność wszystkich jej węzłów. W sieci P2P każdy komputer dysponuje podobnymi możliwościami oraz może inicjować połączenia. Nie ma ustalonej hierarchii ani centralnego serwera. Ten sam komputer może równocześnie pełnić rolę serwera i klienta, czyli pobierać dane z innych komputerów i udostępniać swoje zasoby wszystkim pozostałym komputerom.

Każda sesja łączności, a wiec np. każde połączenie telefoniczne, jest w sieci *Silent Network* poprzedzone fazą negocjacji klucza [2]. Po zakończeniu każdego połączenia klucze i tekst, np. rozmowy, są kasowane co uniemożliwia jakiekolwiek odtworzenie przesyłanej informacji.

Serwery sieci *Silent Network* są skalowalne i przystosowane do redundancji geograficznej. W sieć wbudowano mechanizmy *Interactive Voice Authentication* oraz *Visual Encryption Verification* [3] aby zabezpieczyć sieć przed tzw. atakiem (*man in the middle*), czyli włączenia się w połączenie osoby



Rys. 4. Aplikacja *Silent Phone* dla systemu operacyjnego iOS
Fig. 4. Application *Silent Phone* for iOS system *(https://support.silentcircle.com/)*

Tab. 1. Porównanie opublikowanych dotąd aplikacji szyfrowania komunikacji cyfrowej [8]

AIM	Tak	Nie	Nie	Nie	Nie	Nie	Nie
BlackBerry Messenger	Tak	Nie	Nie	Nie	Nie	Nie	Nie
BlackBerry Protected	Tak	Tak	Tak	Nie	Nie	Tak	Tak
ChatSecure + Orbot	Tak	Tak	Tak	Tak	Tak	Tak	Tak
CryptoCat	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Ebuddy XMS	Tak	Nie	Nie	Nie	Nie	Nie	Nie
Facebook chat	Tak	Nie	Nie	Nie	Nie	Nie	Tak
FaceTime	Tak	Tak	Nie	Tak	Nie	Tak	Tak
Google Hangouts/Chat „off the record”	Tak	Nie	Nie	Nie	Nie	Nie	Tak
Hushmail	Tak	Nie	Nie	Nie	Nie	Nie	Nie
iMessage	Tak	Tak	Nie	Tak	Nie	Tak	Tak
iPGMail	Tak	Tak	Tak	Nie	Nie	Tak	Nie
Jitsi + Ostel	Tak	Tak	Tak	Tak	Tak	Tak	Nie
Kik Messenger	Tak	Nie	Nie	Nie	Nie	Nie	Nie
Mailvelope	Tak	Tak	Tak	Nie	Tak	Tak	Tak
Mxit	Nie	Nie	Nie	Nie	Nie	Nie	Nie
Off-The-Record Messaging for Mac (Adium)	Tak	Tak	Tak	Tak	Tak	Tak	Nie
Off-The-Record Messaging for Windows (Pidgin)	Tak	Tak	Tak	Tak	Tak	Tak	Tak
PGP for Mac (GPGTools)	Tak	Tak	Tak	Nie	Tak	Tak	Nie
PGP for Windows Gpg4win	Tak	Tak	Tak	Nie	Tak	Tak	Nie
QQ	Tak	Nie	Nie	Nie	Nie	Nie	Tak
RetroShare	Tak	Tak	Tak	Tak	Tak	Tak	Nie
Signal/RedPhone/Textsecure	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Silent Phone/Silent Text	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Skype	Tak	Nie	Nie	Nie	Nie	Nie	Nie
SnapChat	Tak	Nie	Nie	Nie	Nie	Nie	Tak
StartMail	Tak	Nie	Tak	Nie	Nie	Tak	Nie
SureSpot	Tak	Tak	Tak	Nie	Tak	Tak	Nie
Telegram	Tak	Nie	Nie	Nie	Tak	Tak	Tak
Telegram (secret chats)	Tak	Tak	Tak	Tak	Tak	Tak	Tak
TextSecure	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Threema	Tak	Tak	Tak	Tak	Nie	Tak	Tak
Viber	Tak	Nie	Nie	Nie	Nie	Nie	Tak
Virtru	Tak	Nie	Nie	Nie	Nie	Tak	Tak
WhatsApp	Tak	Tak	Tak	Tak	Nie	Tak	Tak
Wickr	Tak	Tak	Tak	Tak	Nie	Nie	Tak
Yahoo! Messenger	Tak	Nie	Nie	Nie	Nie	Nie	Nie

trzeciej w celu np. podmiany kluczy. W sieci *Silent Network* wykorzystywane są (podobnie jak w wielu innych rozwiązaniach, m. in. opisanych wyżej) procedury SAS (ang. *short authentication string*), algorytmy *Peer Reviewed Encryption* i *Hashing Algorithms*, *Elliptic Curve Cryptography* (P-384), *Advanced Encryption Standard* (AES-256) oraz *Secure Hash Algorithm* (SHA-256).

Silent Text to aplikacja pozwalająca na przesyłanie automatyczne zaszyfrowanych wiadomości tekstowych – plików, SMS-ów, obrazów, linków i wielu innych obiektów. Aplikacja ta wyposażona jest w funkcję niszczenia wiadomości po przeczytaniu. Podobnie jak *Silent Phone*, aplikację tę można instalować bezpłatnie z *Apple App Store* lub *Google Play* i używać w ramach płatnych planów taryfowych. Silent text oparty jest na protokole SCIMP [1], który zapewnia szyfrowanie, zabezpieczenie treści i proces negocjacji kluczy.

Obok opisanych wyżej aplikacji firma *Silent Circle* oferuje jeszcze szereg usług o charakterze bardziej profesjonalnym:

Reinventing Privacy. Dedykowane zastosowania platformy bezpiecznych prywatnych usług łączności *peer-to-peer* we własnej zastrzeżonej sieci.

Silent Phone For Desktop czyli Silent Phone w wersji *desktop*.

Silent Circle Management Consol. Konsola internetowa do zarządzania w swojej własnej sieci usługami *Silent Phone* i *Silent Text.*

Ostatnią i koronną propozycją firmy jest *Blackphone* czyli smartfon opracowany przez specjalnie powołana firmę SGP Technologies (joint venture *GeeksPhone* i *Silent Circle*), który zapewnia szyfrowanie rozmów telefonicznych, e-maili, tekstów i przeglądania Internetu w sposób wbudowany, a nie za pomocą instalowanej aplikacji. Telefon ma nowy system operacyjny *PrivatOS,* który jest rozszerzonej wersją Android 4.4.2 o pakiet narzędzi kryptograficznych.

Warto zauważyć, że wszystkie dane w systemach *Silent Circle* płyną przez łącza, kodeki i serwery sieci dedykowanej *Silent Network*. A więc jest jednak jakaś Centrala. Jak jest w innych przedstawionych aplikacjach nie wiadomo.

Tab. 2. Przegląd i porównanie aplikacji komunikacyjnych z wbudowanym szyfrowaniem *end-to-end* [19]

Client name	Development status	Open source client	Servers: Decentralized	Servers: Open source	Servers: Distributed	Servers: Federated	Contact verification	Encryption ciphers: Symmetric	Encryption ciphers: Asymmetric: RSA	DSA	ECC	NTRU	El Gamal	Asym. key size: Default	Asym. key size: Max.	Forward secrecy	Multiple encryption	Encrypted group-chat	Encrypted file transfer	Public key and IP unrelated	Transport: Proxy /Tor	TCP	UDP	SCTP	Asynchronous encryp. communication	Encrypted client data	Screenshot protection	Self-destructing messages
Briar	Active, private beta	Yes	Yes	N/A	N/A	N/A	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Cryptocat	Active	Yes	No	?	?	No	Yes	?	?	?	?	?	?	?	?	Yes	Yes	No group-chat	Yes	?	?	?	?	?	?	?	?	?	?
FireChat	Active	No	Yes	N/A	N/A	N/A	?	?	?	?	?	?	?	?	?	?	?	No	?	?	No	?	?	?	Yes	?	?	No
Line	Active	No	No	No	?	No	No	?	?	?	Yes	?	?	256 bit ECC	N/A	No	?	Yes	?	?	No	?	?	?	Yes	No	No	No
RetroShare	Active	Yes	Yes	N/A	N/A	N/A	Yes	Yes	Yes	?	?	No	No	?	?	Yes	Yes	Yes	Yes	Optional	Optional	Yes	Yes	No	Yes	Yes	?	?
Ricochet	Active	Yes	Yes	N/A	N/A	N/A	No	?	?	?	?	?	?	?	?	Yes	No	No group-chat	No	Yes	Yes	?	?	?	No	No	No	No
Sicher	Active	No[ed]	No	No	?	No	?	Yes	Yes	?	?	No	No	2048 bit RSA	N/A	No	No	Yes	Yes	No	No	Yes	No	No	?	Yes	?	Yes
Signal	Active	Yes	No	Partially	Yes	No	Yes	Yes	?	No	Yes	No	No	256 bit ECC	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes	No
Silent Phone	Active	Viewable source[f]	No	No	?	No	Yes	?	?	?	?	?	?	?	?	Yes	?	?	Yes	?	?	?	?	?	?	?	?	Yes
Surespot	Active	Yes	No	No	?	No	Yes	Yes	No	?	Yes	No	No	521 bit ECC	N/A	Yes	No	No group-chat	No	No	?	Yes	No	No	?	?	?	No
TextSecure	Discontinued	Yes	Partially	Yes	Yes	Yes, briefly	Yes	Yes	?	No	Yes	No	No	256 bit ECC	N/A	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes	No
Threema	Active	Partially	No	No	?	No	Yes	?	?	?	?	?	?	?	?	No	?	Yes	Yes	?	?	?	?	?	Yes	Yes	?	No
Tox	Active	Yes	Yes	N/A	N/A	N/A	No	Yes	Yes	?	?	No	No	?	?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
WASTE	Discontinued	Yes	Yes	N/A	N/A	N/A	No	Yes	?	?	No	No	?	?	No	No	No	Yes	No	No	Yes	No	No	?	?	?	?	
WhatsApp	Active	Partially	No	No	Yes	No	Yes	Yes	?	?	Yes	?	?	256 bit ECC	N/A	Yes	Yes	Yes	Yes	Yes	No	?	?	?	Yes	No	No	No
Wickr	Active	No	No	No	?	No	Yes	Yes	Yes	Yes	Yes	No	No	256 bit ECC	N/A	Yes	Yes	?	?	?	No	Yes	?	?	Yes	Yes	?	Yes
Wire	Active	Yes	No	No	?	No	Yes	Yes	?	?	Yes	?	?	256 bit ECC	N/A	Yes	Yes	Yes	?	?	No	Yes	Yes	?	Yes	Yes	No	No

Porównanie aplikacji szyfrowania komunikacji cyfrowej

Kilka omówionych wyżej aplikacji służących bezpieczeństwu komunikacji głosowej lub tekstowej w publicznej i niekodowanej sieci internetu to zaledwie niewielki fragment podobnego oprogramowania, którego celem jest zapewnienie prywatności informacji w morzu sieci powszechnej. Istniejące aplikacje są ciągle ulepszane. Również stały jest proces powstawania nowych. Jest to proces podobny do do tego, którego skutkiem jest generacja nowych kryptowalut. Stale implementowane są zarówno starsze jak nowo publikowane procedury kryptograficzne, ktore umożliwiają lepsze lub gorsze zapewnienie poufności transmisji cyfrowej w sieciach publicznych. Świadczy to o przedtem niedostrzeganej lub niedocenianej potrzebie utajnienia prywatnych przekazów, która ujawniła się bardzo wyraźnie dzięki publikacjom związanym z Edwardem Snowdenem lub Wikileaks.

Aplikacji szyfrowania komunikacji cyfrowej w sieciach publicznych jest wiele, a stale publikowane sa nowe. Większość z tych aplikacji jest słaba, lub, inaczej mówiąc, mało skuteczna. Najlepsze pokrótce omówiono w uprzednio. W *tabeli 1* ich nazwy zaznaczono kolorem czerwonym. Niektóre pozostałe są „prawie dobre". Wiele innych w zasadzie stwarza jedynie pozory bezpieczeństwa.

W lewej rubryce tabeli podano nazwy aplikacji szyfrujących komunikację cyfrową: głosową, tekstową lub graficzną. Z prawej strony podano odpowiedź na siedem poniższych pytań, dla każdej aplikacji oddzielnie.

Czy dane są szyfrowane in flow?
Czy szyfrowanie utajnia dane nawet dla dostawcy usługi?
Czy użytkownik może zidentyfikować tożsamość kontaktu?
Czy dostawca zapewnia, że skradziony klucz nie odszyfruje transmisji?
Czy kod oprogramowania jest otwarty i publicznie dostępny?
Czy procedury i procesy szyfrowania są udokumentowane?
Czy usługa był niezależnie audytowana?

W *tabeli 2* przedstawiono większość opisanych w literaturze kryptograficznie zabezpieczanych aplikacji komunikacyjnych. Zwraca uwagę ich różnorodność (wszystkie powstały w ostatnich 3 latach) i bardzo różny stopień wykorzystania narzędzi kryptograficznych.

Konkluzja: Nowoczesne technologie dały rządzącym nowe możliwości podsłuchiwania i zbierania prywatnych danych o wszystkich ludziach świata. Internet na to odpowiada samoobroną.

Literatura

[1] Wojciech Nowakowski, Tomasz Adamski: (2014) Protokół ZRTP – telekomunikacja wspomagana kryptografią. DOI 10.15199/ELE-2014-178, Elektronika nr 10/2014, s. 80–87.
[2] Wojciech Nowakowski (2014) Silent Circle – zaklęty krąg nowoczesnej kryptografii dla wszystkich DOI: 10.15199/ELE-2014-218, Elektronika 12/2014, str. 38-40.
[3] http://en.wikipedia.org/wiki/Visual_cryptography
[4] https://www.eff.org/secure-messaging-scorecard
[5] https://chatsecure.org
[6] https://www.eff.org
[7] [8] https://www.eff.org/pl/node/82654
[9] https://zaufanatrzeciastrona.pl/post/korzystasz-z-sieci-tor-na-telefonie-lepiej-uwazaj
[10] https://crypto.cat
[11] http://electron.atom.io
[12] http://prosody.im
[13] https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux
[14] https://getfedora.org
[15] https://azure.microsoft.com/en-us/
[16] https://nodejs.org
[17] Wojciech Nowakowski, (2014) Kryptografia współczesna. Monografia IMM 2014, ISBN 978-83-927542-4-4
[18] https://en.wikipedia.org/wiki/Signal_(software)
[19] https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients