DOI: 10.15199/ELE-2014-218

Silent Circle – zaklęty krąg nowoczesnej kryptografii dla wszystkich

dr inż. WOJCIECH NOWAKOWSKI, prof. ndzw.

Instytut Maszyn Matematycznych

W 2011 roku Phil Zimmermann, twórca powszechnie stosowanego w internecie protokołu **PGP** (ang. *Pretty Good Privacy,* całkiem niezła prywatność) zapewniającego poufność poczty elektronicznej oraz Mike Janke, były specjalista od zabezpieczeń US Navy SEAL a także Jon Callas, twórca oprogramowania szyfrującego zawartość dysków twardych (*Whole Disk Encryption Apple*), powołali firmę *Silent Circle* dla stworzenia pierwszej na świecie prywatnej bezpiecznej łączności cyfrowej, zarówno głosowej, tekstowej jak i wideo, a także transmisji plików. *Silent Circle* jest obecnie uznaną firmą zapewniającą rzeczywiście bezpieczną komunikację cyfrową dzięki wykorzystaniu technologii kryptograficznych oferując w ponad 130 krajach tani i jednocześnie zaawansowany system szyfrowanych usług komunikacyjnych na bazie protokół ZRTP [1].

Pierwszym na świecie operatorem telekomunikacyjnym oferującym usługi szyfrowanych połączeń mobilnych firmy Silent Circle jest holenderski **KPN** (**Koninklijke KPN NV**, wcześniej **Koninklijke PTT Nederland**). KPN informuje [2], że aplikacje Silent Circle są dostępne dla klientów biznesowych poprzez kpn.com/cloud. Aplikacje te dostępne są poprzez smartfony i tablety z systemem iOS lub Android.

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.

Warto podkreślić, że matematyczne instrumentarium stosowane we współczesnej kryptografii klucza publicznego, w tym także w *Silent Network*, nie jest jeszcze do końca zbadane i domknięte. Zarówno normatywne algorytmy zatwierdzone przez instytucje standaryzacyjne jak i właściwości funkcji matematycznych stosowanych w aplikacjach nie są do końca zbadane, a prace wciąż trwają. Bezpieczeństwo stosowanych algorytmów jest wciąż dyskutowane, testowana jest też ich odporność na ataki cybernetyczne. Uznanie bowiem jakiejkolwiek funkcji za bezpieczną do zastosowań kryptograficznych opiera się wciąż na **domniemaniu** odporności na **znane** ataki kryptoanalityczne, nie zaś na matematycznych dowodach gwarantujących niemożność jej złamania [4–7].

Na przykład Istnienie jednokierunkowych funkcji nie zostało dotychczas dowiedzione. Poważne słabości znaleziono w wielu funkcjach skrótu, które historycznie uchodziły za bezpieczne. Funkcje skrótu (haszujące) używane obecnie w kryptografii to MD5, SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), RIPEMD-160. Jedną z najbardziej popularnych rodzin funkcji skrótu jest rodzina MD (*Message Digest*) Ronalda Rivesta, współtwórcy RSA. MD5 (*Message-Digest algorithm 5*), piata wersja funkcji została opracowana w 1991 roku, która z dowolnego ciągu danych generuje 128-bitowy skrót. W 2004 znaleziono sposób na generowanie kolizji w MD5, co spowodowało, że nie jest już ona polecana do zastosowań wymagających wysokiego poziomu bezpieczeństwa. Jest jednak w dalszym ciągu powszechnie stosowana w internecie jako suma kontrolna przesyłanych plików.

SHA (*Secure Hash Algorithm*) to rodzina kryptograficznych funkcji skrótu zaprojektowanych przez NSA (*National Security Agency*) i publikowanych przez NIST (*National Institute of Standards and Technology*). Pierwsza z tych funkcji, opublikowana w 1993 roku, została wycofana ze względu na oficjalnie nieujawnione wady. W 1995 roku została ona zastąpiona przez algorytm SHA-1. Algorytm ten generuje 160-bitowy skrót z wiadomości o maksymalnym rozmiarze 264 bitów. W budowie jest on podobny do MD5. Grupa funkcji SHA-2, a więc i stosowana w Silent Network funkcja SHA-256 jest wciąż przedmiotem badań matematyków. Dlatego NIST prowadzi publiczny konkurs na następcę dotychczasowych funkcji skrótu.

RIPEMD to funkcja skrótu opracowana w ramach projektu Unii Europejskiej o nazwie RIPE (RACE Integrity Primitives Evaluation) realizowanego w la-tach 1988–1992. W 1996 roku powstała wersja generująca skrót 160-bitowy nazwana RIPEMD-160. W 2004 roku Xiaoyun Wang, Dengguo Feng, Xuejia Lai oraz Hongbo Yu opublikowali dokument w którym podano dwie pary wiadomości produkujących te same skróty. Algorytm RIPEMD-160 jest więc stosunkowo mało popularny gdyż jest słabo zbadany z punktu widzenia bezpieczeństwa stosowania.

Również szeroko stosowane w praktyce systemy kryptograficzne jak RSA, ElGamal, DSA (Digital Signature Algorithm), ECDSA (krzywe eliptyczne DSA), algorytm Rabina, podpisy Schnorra, czy w końcu klasa podpisów Nyberg-Rüppel'a nie są jeszcze do końca zbadane, choć niektóre z nich zostały już zestandaryzowane (IEEE P1363). Dowodzi tego analiza prostego schematu Nyberg-Rüppel'a tzw. *schematu bez odzysku wiadomości* [8], w której przeanalizowano i oceniono prawdopodobieństwo ingerencji w tym systemie i zaproponowano proste metody kontroli prawdopodobieństwa fałszerstwa transmisji.

Sieć *Silent Network* jest siecią równorzędną typu każdy z każdym (ang. *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 [1]. Po zakończeniu każdego połączenia klucze i tekst, np. rozmowy, są niszczone co uniemożliwia jakiekolwiek odtworzenie przesyłanej informacji.

Serwery sieci *Silent Network* zlokalizowane są w Montrealu i Toronto. Są one skalowalne i przystosowane do redundancji geograficznej – wkrótce ma zostać uruchomiony kolejny serwer w szwajcarskiej siedzibie firmy. W sieć wbudowano mechanizmy *Interactive Voice Authentication* oraz *Visual Encryption Verification* [3], aby zabezpieczyć sieć przed tzw. atakiem MITM (ang. *man in the middle*), czyli włączenia się w połączenie osoby trzeciej w celu np. podmiany kluczy. W sieci *Silent Network* wykorzystywane są 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).

Podstawowe aplikacje Silent Circle na smartfony i tablety

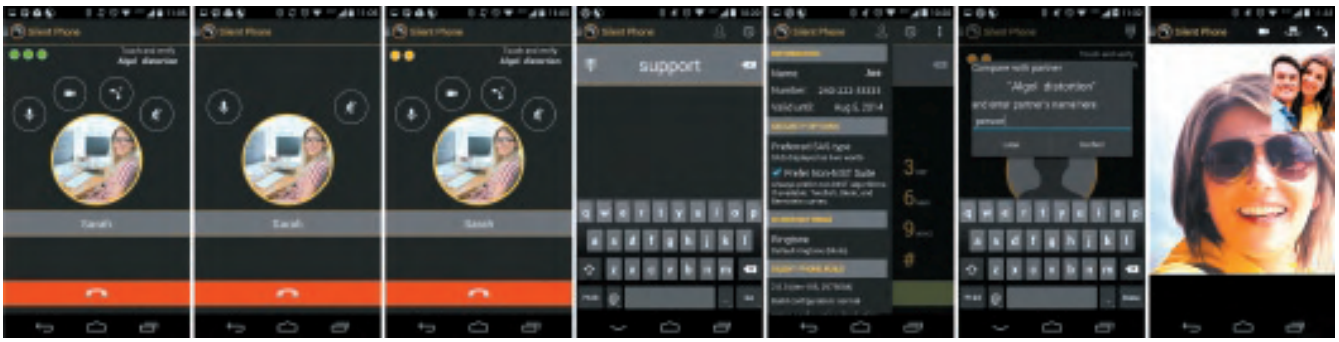
Po zbudowaniu niezbędnej infrastruktury, czyli *Silent Network*, i opracowaniu koniecznego software'u firma *Silent Circle* zaoferowała kilka aplikacji na istniejące urządzenia mobilne. Instalacja tych aplikacji jest darmowa (przez Apple App Store lub Google Play), ale korzystanie z nich – płatne w postaci abonamentu na minuty, podobnie jak w telefonii komórkowej. e te są udostępniane w za miesięczną opłatą. Dwie najważniejsze aplikacje to *Silent Phone* i *Silent Text.*

Silent Phone (Cichy Telefon) to aplikacja na smartfony i tablety, zarówno z systemem operacyjnym iOS jak i Android, zapewniająca prywatną szyfrowaną komunikacji głosową i wideo. Jest to aplikacja łatwa w użyciu umożliwiająca połączenia w jakości HD, w sieciach 3G/4G i Wi-Fi, szyfrowane protokołem ZRTP [1]. Protokół ten wykrywa kiedy zaczyna się rozmowa, inicjuje wymianę kluczy kryptograficznych między dwoma rozmówcami, a następnie szyfruje i rozszyfrowuje *on-line* transmisję głosu i danych. Uzgadnianie kluczy odbywa się bezpośrednio *peer-to-peer*, w strumieniu danych. Klucze są niszczone z końcem rozmowy. *Silent Phone* umożliwia szyfrowane połączenia głosowe, bezpieczny wideo-czat i bezpieczne połączenia konferencyjne.

Silent Phone

Rys. 1. Kod QR trailer reklamowego aplikacji Silent Phone
Fig. 1. Trailer QR-code Silent Phone application

Rys. 2. Aplikacja *Silent Phone* dla systemu operacyjnego iOS
Fig. 2. Application *Silent Phone* for iOS system
(https://support.silentcircle.com/)



Rys. 3. Aplikacja *Silent Phone* dla systemu operacyjnego Android
Fig. 3. Application *Silent Phone* for Android system
(https://play.google.com/store/apps/details?id=com.silentcircle.silentphone)

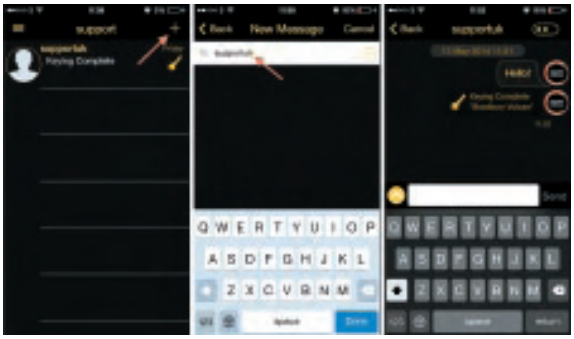
Silent Text

Silent Text (Cichy Tekst) 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.

Zastosowanie aplikacji *Silent Text* w sposób kolokwialny a jednocześnie celny wyraża na swojej stronie internetowej twórcy systemu:

„...jest to system bezpiecznego przesyłania informacji tekstowych i obrazków dla działaczy, żołnierzy, biznesmenów w podróży, zakochanych, bojowników o wolność, prawników, lekarzy, dyrektorów i prezesów, tzn. tych, którzy potrzebują uchronić swoje poufne informacje przed wścibskimi. Silent Text zapewnia najsilniejsze szyfrowanie, bez wymagania żadnej wiedzy technicznej. Twórcy nowoczesnej kryptografii i weterani operacji specjalnych stworzyli produkt, zapewniający bezpieczeństwo i prywatność w sposób prosty i dostępny wszystkim, a jednocześnie najlepszy w swojej klasie.

Silent Text to narzędzie, które sprzedajemy. Ty jesteś naszym klientem, którego zapewniamy, że jego dane są bezpieczne. Stworzyliśmy najlepsze w swojej klasie szyfrowane usługi komunikacyjne. Stworzyliśmy system, który nie może być naruszony nawet przez nas. Ty i twoi korespondenci są jedynymi opiekunami tajnych kluczy. Jednak nie można nam w pełni ufać, gdyż istnieją przecież wymuszenia, łapówki, korupcja, zaniedbania lub po prostu niewłaściwe korzystanie z urzadzeń...



Rys. 4. Aplikacja *Silent Text* dla systemu operacyjnego iOS
Fig. 4. Application *Silent Text* for iOS system
(https://support.silentcircle.com/customer/portal/articles/1645084-how-do-i-initiate-a-new-text-message-conversation-)

Rys. 5. Aplikacja *Silent Phone* dla systemu operacyjnego Android
Fig. 5. Application *Silent Phone* for Android system
(https://https://support.silentcircle.com/customer/portal/articles/1645084-how-do-i-initiate-a-new-text-message-conversation-)

Inne produkty firmy *Silent Circle*

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. Ale to już następny temat.

Zakończenie

Technologie *Silent Circle* mają rzeczywiście charakter rewolucyjny: w sposób łatwy, przyjemny. skuteczny i tani udostępniają wszystkim chętnym trudne i skomplikowane technologie kryptograficzne, które sprawiają, że kontrola oferowanej przez nich komunikacji staje się bardzo trudna. Natychmiast pojawiają się wątpliwości, czy technologie te nie mogą zostać wykorzystane przez przestępców i terrorystów. Sam twórca protokołu ZRTP Phil Zimmermann zapewniał, żа jak dotąd nie zaimplementował „tylnych drzwi" w algorytmie, np. dla NSA. A bez tego zabezpieczanie danych może być śmiertelnie niebezpieczne dla innych. Na ten temat nic jak dotąd nie wiadomo.

Jednak pewną nadzieję na możliwość kontroli stanowi jednak fakt, że wszystkie dane w systemach *Silent Circle* płyną przez łącza, kodeki i serwery sieci dedykowanej *Silent Network*. A więc jest Centrala, która być może coś może. Pokaże to najbliższa przyszłość.

Literatura

[1] Wojciech Nowakowski, Tomasz Adamski: Protokół ZRTP – telekomunikacja wspomagana kryptografią. Elektronika nr 10/2014, s. 80–87.
[2] http://corporate.kpn.com/pers/persberichten/silent-circle-vanaf-nu-beschikbaar-bij-kpn.htm
[3] http://en.wikipedia.org/wiki/Visual_cryptography
[4] Wojciech Nowakowski, Kryptografia współczesna. Monografia, wyd. IMM 2014, ISBN 978-83-927542-4-4.
[5] Wojcieh Nowakowski, Robert Poznański: Podpis elektroniczny – zasady działania. Elektronika nr 7/2010, str. 265–267.
[6] Wojciech Nowakowski: O bezpieczeństwie algorytmu RSA., Elektronika nr 2/2012, str. 80–82.
[7] Wojciech Nowakowski: Kryptograficzne aspekty technologii wirtualnej waluty BitCoin. Elektronika nr 5/2013, str. 58–62.
[8] Tomasz Adamski, Wojciech Nowakowski: Security of Nyberg-Rueppel digital signatures without message recovery. Bulletin of the Polish Academy of Sciences – Technical Sciences, Vol. 62, No. 4/2014, DOI: 10.2478/bpasts-2014-0090, str. 817–825.