GROŹNE KOMUNIKATORY. „NA CZYM ZARABIAJĄ DOSTAWCY BEZPŁATNYCH USŁUG”?

W zawrotnym tempie rośnie liczba polskich użytkowników darmowych aplikacji szyfrowanej komunikacji. – Swoista moda wyłączyła racjonalne myślenie, zagrożenia są bardzo poważne – podkreślą eksperci.

W marcu ubiegłego roku firma Check Point Software opublikowała raport dotyczący dziur w Telegram oraz WhatsApp umożliwiających hakerom dostęp do 1,1mld kont użytkowników. Co więc powoduje, że uważane tak powszechnie za „w pełni szyfrowane” rozwiązania są w rzeczywistości bardzo groźne.

> *Komunikatory mają powszechną opinię „bezpiecznych”, ale to złudne przekonanie. Używanie zagranicznego oprogramowania - szczególnie w takich obszarach jak administracja państwowa czy strategiczne obszary gospodarki niesie wiele zagrożeń*
>
> Pułkownik Grzegorz Małecki - były szef Agencji Wywiadu

Informacje ujawnione przez Edwarda Snowdena o masowej inwigilacji prowadzonej przez NSA wraz ze zwiększającą się liczbą różnego rodzaju ustaw ułatwiających podsłuchiwanie i przechwytywanie danych doprowadziły do wzrostu zainteresowania szyfrowaną komunikacją, mającą gwarantować prywatność i odpowiednią ochronę przesyłanych informacji. W Polsce lawinowo rośnie liczba użytkowników tego typu oprogramowania, tajemnicą poliszynela jest, że takich komunikatorów używają nie tylko dziennikarze, politycy ale także menedżerowie, adwokaci…do przesyłania często wrażliwych dokumentów.

> *W celu posiadania pełnego obrazu zagrożeń musimy odpowiedzieć sobie na pytanie na czym zarabiają dostawcy darmowych usług. Na czym polega patent komunikatora. Bezpłatne komunikatory muszą dostarczyć swoim twórcom jakieś konkretne zyski. Dobrze byłoby gdybyśmy wiedzieli jakie i znali ich model biznesowy*
>
> Pułkownik Grzegorz Małecki - były szef Agencji Wywiadu

Bezpieczeństwo urządzenia, którym się posługujemy

Żaden komunikator oferujący szyfrowane połączenia nie zapewni bezpieczeństwa jeżeli skompromitowany jest telefon. Przejęcie kontroli nad kamerą czy mikrofonem przez nieuprawnioną do tego trzecią stronę daje olbrzymie możliwości podsłuchiwania rozmów prowadzonych przez użytkownika, nawet jeżeli rozmawia z wykorzystaniem zaszyfrowanych komunikatorów. Ponadto umożliwia to monitorowanie otoczenia, w którym znajduje się skompromitowany aparat. Dodatkowo nieuprawniona osoba może również eskalować uprawnienia administratora przejmując praktycznie kontrolę nad urządzeniem czy w przypadku modeli Apple usunąć ograniczenia narzucone przez tą firmę. Jedynym komunikatorem, który umożliwia sprawdzenie czy aparat jest skompromitowany jest UseCrypt, co pozwala stwierdzić jeszcze przed nawiązaniem komunikacji, czy na pewno nasz telefon nie został zainfekowany złośliwym oprogramowaniem. Żaden z innych komunikatorów (Signal, Telegram, Viber czy WhatsUpp) tego nie umożliwia, przez co ich stosowanie może okazać się nieskuteczne już na samym początku.

Wykorzystywanie danych użytkownika

Powszechnie uważane za zapewniające prywatność komunikatory zbierają dane użytkowników, które następnie wykorzystywane są w celach marketingowych. Dlatego początkowo płatne aplikacje jak np. WhatsApp stały się darmowe. W 2016 roku burzę w mediach wywołała informacja dotycząca przekazania ponad miliarda numerów telefonów Facebook'owi przez WhatsApp w celach marketingowych.

Dzieje się tak, bowiem model biznesowy wielu aplikacji mobilnych wprost zakłada zbieranie i przechowywanie danych, które często dotyczą nie tylko samych użytkowników aplikacji, ale również danych osób trzecich znajdujących się na urządzeniu mobilnym.

W polityce prywatności Viber możemy przeczytać, że dane z książki telefonicznej trafiają na serwer Viber i dotyczą wszystkich posiadanych przez danego użytkownika kontaktów, nawet osób które nie korzystają z tego komunikatora. Przykładowo oznacza to, że np. polityk rejestrujący się do usługi Viber udostępnia właścicielowi oprogramowania wszystkie numery telefonów, które posiada w swojej książce kontaktowej"

> *Nie ulega wątpliwości, że wykorzystywanie zagranicznych komunikatorów daje zewnętrznym podmiotom, w wielu przypadkach rządowym (służbom) możliwość monitorowania naszej przestrzeni informacyjnej. Nie chodzi o samą treść (teoretycznie nie powinien mieć do niej dostępu nikt), ale wiedzy na temat ruchu, metadanych czy kontaktów. Jest to niewątpliwie utrata części suwerenności informacyjnej*
>
> Pułkownik Grzegorz Małecki - były szef Agencji Wywiadu

Telegram w swojej polityce prywatności nie informuje jakie konkretnie dane pozyskuje. Ogranicza się do lakonicznego stwierdzenia, że przetwarza minimum niezbędnych danych. Sformułowanie to powinno wywoływać niepokój wśród użytkowników.

Signal z kolei zachowuje sobie prawo do udostępniania informacji o użytkowniku jeżeli wynika to z obowiązku spełnienia obowiązujących wymogów prawa i regulacji, procedury sądowej lub

prawomocnego żądania instytucji państwowej. Może to doprowadzić do przekazania danych amerykańskiej administracji. To samo tyczy się aplikacji WhatsApp, należącej do Facebook'a, na którego stronach możemy przeczytać, że liczba zapytań organów ścigania z Polski dotycząca danych użytkowników liczona jest w tysiącach rocznie, a Facebook pozytywnie weryfikuje ponad 50% zapytań udostępniając dane użytkowników. Z kolei polityka prywatności WhatsApp zakłada pełną wymianę wiadomości z „rodziną Facebook'a".

Powyżej opisane przykłady wcale nie oznaczają, że tak musi być. W przypadku Usecrypt Messenger, w momencie rejestracji użytkownika porównywane są jedynie skróty kryptograficzne (zaciemniony ciąg, z którego nie da się odtworzyć numeru telefonu), tzw. funkcja jednokierunkowa, która pozwala poinformować użytkownika, który z jego kontaktów używa usługi.

Przechowywanie danych na serwerze usługodawcy

Polityki prywatności większości komunikatorów są lakoniczne i pozostawiają usługodawcy wiele furtek. Z łatwością możemy znaleźć w ich treści stwierdzenia informujące nas użytkowników iż w „pewnych" przypadkach zachowuje sobie prawo do przechowania oraz przekazywania wszystkich informacji.

Jeżeli chodzi o dostęp oraz przechowywanie danych, producenci aplikacji ograniczają się do stwierdzeń, że dane przechowywane są „jak najkrócej jest to możliwe", że „pozostają kilka sekund" lub są „przechowywane nie dłużej niż daną liczbę dni". Oznacza to jednak, że w rzeczywistości nie gwarantują żadnej poufności. Sam fakt obecności danych użytkownika na serwerze usługodawcy w pełni kompromituje te rozwiązanie.

Biorąc pod uwagę lokalizację serwerów na terenie USA (Signal), Telegram (Rosja), Viber (producent nie podaje takiej informacji) oraz liczne doniesienia prasowe na temat back-door'ów, które posiadają agencje rządowe oznacza to, że komunikowana przez producentów poufność jest pozorna. Wystarczy bowiem ułamek sekundy, aby dane użytkownika, które trafiają na serwer usługodawcy, zostały skopiowane i przekazane osobie trzeciej.

Zestawianie połączeń

W UseCrypt Messenger połączenia zestawiane są poprzez serwer pośredniczący, który jednak nie uczestniczy w komunikacji jak i w żadnych operacjach kryptograficznych, co gwarantuje pełną anonimowość użytkownikowi. Poufność danych zapewnia też fakt, że usługodawca nie przechowuje na serwerze danych użytkownika. Konkurencyjny Signal szyfruje wiadomości i przesyła je przez serwer pośredniczący do odbiorcy. Podczas tego procesu uzyskuje informacje na temat czasu ostatniego połączenia do serwera. Jeszcze gorzej sytuacja wygląda w przypadku WhatsApa, który tworzy backupu wiadomości w chmurze, co naraża je na ryzyko przejęcia przez nieuprawnioną trzecią stronę.

UseCrypt wprowadza mechanizm wykrywania ataków man-in-the-middle w postaci dodatkowej warstwy ochrony – short authentication string – krótkiego wyrażenia pozwalają na porównanie wynegocjowanie parametrów z drugą stroną połączenia. Po zestawieniu połączenia na ekranie pokazywane są dwa wyrazy. Takie same dwa wyrazy są wyświetlane na ekranie drugiej osoby. Dla pełnego bezpieczeństwa należałoby rozpocząć rozmowę od porównania tych ciągów. Jeżeli są takie same – połączenie jest bezpieczne (nikt nie przechwytuje komunikacji pomiędzy punktami). Inne komunikatory internetowe jak Viber, WhatsApp czy Telegram nie oferują takiej możliwości.

Do szyfrowania komunikacji jest wykorzystywany algorytm szyfrujący AES. W konkurencyjnym Signalu, do szyfrowania komunikacji wykorzystywany jest algorytm z podwójną „grzechotką" (double ratchet). Wykorzystuje on Curve25519, AES-256 oraz HMAC-SHA256 jako algorytmy pierwotne. Podobnie sytuacja wygląda w WhatsUppie, gdzie zaimplementowano mechanizm Signala. W Viberze

zastosowano również algorytm z podwójną „grzechotką”, który został jednak rozwinięty niezależnie od Signala.

Telegram wykorzystuje symetryczne, autorskie szyfrowanie MTProto nawiązujące do 256 bitowego symetrycznego szyfrowania AES, 2048 bitowego RSA oraz protokołu Diffiego-Hellmana. Tym samym program ten łamie podstawową zasadę kryptografii by oprzeć się na sprawdzonych rozwiązaniach, jak krzywa eliptyczna Diffiego-Hellmana. W tym wypadku użytkownik nie może być pewny nie tylko implementacji wybranego przez producenta rozwiązania kryptograficznego, ale nawet skuteczności samej kryptografii.

Dobór wszystkich parametrów operacyjnych dla algorytmów kryptograficznych UseCrypt Messenger został przeprowadzony przez specjalistów odpowiedzialnych za wytwarzanie wojskowych systemów łączności. Dzięki temu UseCrypt Messenger jest wolny od kleptograficznych dodatków (celowe osłabianie systemu kryptograficznego), umożliwiających łatwiejsze złamanie wykorzystanych prymitywów kryptograficznych. Istotność powyższego może być potwierdzona odnalezionymi w innych komunikatorach przejawami wykorzystania właśnie tak źle dobranych parametrów.

Przykładowo, komunikator Signal wykorzystuje w procesie negocjacji klucza protokół Diffie-Hellman, dla którego grupy multiplikatywnej modulo p przyjęto generator grupy o wartości 2. W rzeczywistości generatorem tej grupy jest liczba 5. W efekcie zastosowania złej wartości, protokół operuje jedynie na podgrupie wskazanej grupy multiplikatywnej, co w sposób znaczący zmniejsza bezpieczeństwo całego protokołu, a w konsekwencji prowadzonej z jego zastosowaniem komunikacji.

Ponadto ostatnie badania przeprowadzone przez naukowców z politechniki Rurh-Universität Bochum wykazały możliwość podsłuchiwania grupowych rozmów w aplikacjach Signal i WhatsApp. Jest to przełomowe odkrycie, ponieważ do tego czasu Signal był uznawany za gwarantujące bezpieczeństwo i prywatność. Naukowcy odkryli, że administrator serwera Signal czy WhatsAppa, który udostępnia grupową rozmowę, jest w stanie skrycie dodać niewidocznego człowieka do grupy. Umożliwia to podsłuchiwanie rozmów grupy osób, które myślą, że są bezpieczne przed ingerencją osób trzecich.

Podsumowanie

Czytaj więcej: Co sprawia, że polski komunikator UseCrypt Messenger jest tak bezpieczny?

Z proponowanych rozwiązań, najpełniejsze bezpieczeństwo zapewnia UseCrypt. Jako jedyny już na poziomie urządzenia sprawdza bezpieczeństwo aparatu i czy nie został on skompromitowany. Ponadto, w przeciwieństwie do rozwiązań konkurencji, polski produkt nie pozyskuje ani nie przechowuje żadnych informacji na temat użytkowników, zapewniając im całkowitą anonimowość. Dodatkowo z punktu widzenia polskiego klienta, w szczególności z administracji państwowej, wojska i biznesu ważne jest używanie rozwiązań stosowanych w Polsce, co zabezpiecza przed atakami kleptograficznymi.

> *Komunikatory mają powszechną opinie „bezpiecznych”, ale to złudne przekonanie. Używanie darmowego oprogramowania - szczególnie w takich obszarach jak administracja państwowa czy strategiczne obszary gospodarki niesie wiele zagrożeń. Nie ulega wątpliwości, że wykorzystywanie zagranicznych komunikatorów daje zewnętrznym*

> *podmiotom, w wielu przypadkach rządowym (służbom) możliwość monitorowania naszej przestrzeni informacyjnej. Nie chodzi o samą treść (teoretycznie nie powinien mieć do niej dostępu nikt), ale wiedzy na temat ruchu, metadanych czy kontaktów. Jest to niewątpliwie utrata pewnej części suwerenności informacyjnej. W celu posiadania pełnego obrazu zagrożeń musimy odpowiedzieć sobie na pytanie na czym zarabiają dostawcy darmowych usług. Na czym polega patent komunikatora. Bezpłatne komunikatory muszą dostarczyć swoim twórcom jakieś konkretne zyski. Dobrze byłoby gdybyśmy wiedzieli jakie i znali ich model biznesowy. Jednym z zagrożeń może być pozyskanie listy kontaktów z telefonów. Często wielu ludziom wydaje się, że informacje te nie są ważne i nie wymagają należytej ochrony. Z perspektywy wywiadu taka wiedza jest jednak bezcenna. Umożliwia to m.in. stworzenie siatki kontaktów danych polityków czy nawet przy wykorzystaniu zdolności współczesnego SIGINTU podsłuchiwanie niezaszyfrowanych rozmów. Komunikatory, które zaciągają takie listy, nie należy uznać za bezpieczne. Polska administracja powinna używać komunikatorów szyfrujących i to nie tylko w rozmowach dotyczących tajemnic państwowych. Polskie rozwiązania muszą być w pełni funkcjonalne i zapewniać wysoką ochronę. Ich stosowanie pozwoli na zwiększenie suwerenności informacyjnej w tym newralgicznym obszarze*
>
> Pułkownik Grzegorz Małecki - były szefa Agencji Wywiadu