Analiza bezpieczeństwa komunikatorów szyfrowanych

21 lipca 2024

W dobie, kiedy jest ogólny problem z brakiem demokracji na świecie i zamiast ludzi rządzą firmy technologiczne, ważne jest, aby sprawdzać zapewnienia producentów oprogramowania, które używamy. Mozilla zapewniała nas, że „Firefox" dba o prywatność użytkowników, a tymczasem po zmianie CEO w brutalny niedemokratyczny sposób z użyciem podstępu w czerwcu 2024 – Mozilla Firefox zawiera instrukcje przekazujące dane o sposobie używania Firefoxa firmie reklamowej.

Wydarzenie to spowodowało konsternację wśród użytkowników „Firefoxa". Nigdy więcej nie polecam używania „Firefoxa" jako przeglądarki zapewniającej prywatność. Na ten moment polecam jej odgałęzienie (tzw. fork) o nazwie „Tor Browser". Myślę, że nie jest przesadnym uruchamianie „Tor Browsera" do każdej aktywności, gdy firmy po prostu kradną nasze dane osobowe, nie pytając nas o zdanie i gwałcąc w ten sposób RODO/GDPR. Nie polecam również żadnej przeglądarki opartej na silniku Blink, ponieważ instrukcje śledzące znajdują się już w samym silniku. Bazując na ostatnim silniku Gecko z maja 2024, nie powinniśmy trafić na instrukcje śledzące umieszczone wprost w silniku Gecko.

Niestety nie inaczej wygląda sytuacja wśród markowych komunikatorów, reklamowanych jako komunikatory E2E (end-to-end) rzekomo szyfrujące od jednego końca do drugiego tak, że nie jest możliwe podsłuchiwanie komunikacji. Niestety nic bardziej mylnego. Wszystkie bardziej znane komunikatory udało się złamać poprzez podmianę serwera pośredniczącego w

komunikacji. Dowód: wiersz „Directory service could be modified to enable a MITM attack?” („Czy serwis katalogowy może być zmodyfikowany tak, aby umożliwić atak MITM”) cały wypełniony opisem „Tak” na stronie „Secure Messaging Apps”. Nie wygląda to dobrze. To wygląda wręcz tragicznie, jakby ktoś celowo się postarał o brak podstawowego bezpieczeństwa i prywatności.

Na początek wyjaśnię, na czym polega atak MITM. Atak MITM (Man In The Middle – człowiek pośrodku) polega na tym, że osoby (nazwijmy je Alicja i Bob) próbują wymienić między sobą klucze publiczne tak, aby nikt nie mógł podsłuchiwać połączenia. Problem polega w tym, że trzecia osoba (nazwijmy ją Ewą) może te klucze tak zmanipulować, by być w stanie czytać korespondencję. Ewa odbiera klucze od Alicji i podstawia swoje w komunikacji do Boba. Bob odbiera więc klucz Ewy, a nie Alicji, błędnie będąc przekonanym, że ma klucz Alicji. W drugą stronę odbywa się to identycznie. Ewa przekazuje Alicji klucz swój zamiast klucz Boba. Dalej komunikacja toczy się drogą Alicja → Ewa → Bob i Bob → Ewa → Alicja zamiast bezpośrednio. Ewa cały ruch rozszyfrowuje i szyfruje, ponownie wysyłając dalej. Komunikacja mimo szyfrowania End-To-End jest czytana i w całości automatycznie rejestrowana (nagrywana) przez Ewę.

W rzeczywistości Ewą będą zazwyczaj: ISP, rząd, trzyliterowe służby, Google, Microsoft. Dostawca internetu (ISP) jest w stanie zmienić cały ruch. Jeżeli nie wierzysz, zastanów się ile razy u swojego operatora zamiast strony, którą wywołasz, widzisz treść „Doładuj swoje konto” u swojego dostawcy internetu. Treść może podmienić rząd. Uzyskać dostęp do serwera i umieścić tam oprogramowanie takie, jakie chce.

Każdy komunikator powinien być na to odporny, a nie jest. W końcu Google i Microsoft na swoich systemach operacyjnych mogą podmieniać zawartość stron wraz z certyfikatami. Nic nie stoi na przeszkodzie, by Windows podmienił certyfikat stronie twojego Banku. Nie będzie to jednak certyfikat wystawiony przez Bank, ale przez kogoś innego. Np. anonimowy certyfikat Let's Encrypt. Przeglądarka „Google Chrome" (oraz „Chromium") czy „Firefox" nie ostrzeże o niebezpieczeństwie.

Twórcy markowych komunikatorów nie zapewniając podstawowego bezpieczeństwa – odporności przeciwko Man In The Middle – jednocześnie potrafią się chwalić, że niektóre umieją szyfrować szyfrem Kyber-1024, rzekomo odpornym na ataki kwantowe. Tyle że co z tego, skoro każdy, kto zmodyfikuje ruch przez serwis katalogowy (Directory Service), jest w stanie już teraz rozszyfrować ruch. Poza tym w roku 2022 złamano na zwykłym komputerze szyfr postkwantowy SIDH, który miał być bezpieczny w czasach post-kwantowych. Niestety nie wytrzymał próby 5 lat i nie dotrwał tego czasu. Szyfry Rabin, RSA i El Gamal były testowane długo i udowodnione jest, że gdy są poprawnie zaimplementowane, są bezpieczne przy kluczach 2048-bitowych i dłuższych.

Polskim komunikatorem nieuwzględnionym w tych badaniach jest komunikator „Valkyria Besiada", który można pobrać TUTAJ.

Komunikator ten jest tworzony przez osobę prywatną nie prowadzącą żadnej firmy (przynajmniej jawnie). Brak firmy stojącej za produktem zazwyczaj oznacza, że nie ma nikogo, kto byłby łasy na dane osobowe użytkowników. Komunikator ten jest tak pomyślany przez autorkę, że już samo zaproszenie zawiera klucz publiczny algorytmu szyfrowania Rabin 6144-bit. Kryptosystem Rabina opiera się na problemie faktoryzacji liczb złożonych utworzonych z 2 dużych liczb pierwszych. Ponieważ konto jest wskazywane przez identyfikator będący kluczem publicznym, nie jest już możliwe na żadnym etapie podmiana tego klucza. Chyba że w sposób wulgarny – jawnie w otwartym tekście zaproszenia wstawionego np. na forum, które widzi użytkownik i inni.

Tak zaprojektowany system jest bezpieczny w tym sensie, że jeżeli 2 osoby wymienią się swoimi identyfikatorami, na przykład na kartach SD, nie ma możliwości podsłuchiwania i modyfikacji komunikacji do czasu skonstruowania stabilnego komputera kwantowego, którego do tej pory nie stworzono. W 2001 roku dokonano faktoryzacji 15=3×5 z użyciem komputera kwantowego. W roku 2019 niemożliwa była faktoryzacja 35=5×7 oryginalnym algorytmem Shora. Algorytm musiał być upraszczany, a i tak wystąpiły błędy wynikające z kwantowej metody. Myślę, że do roku 2030 nikt nie opracuje stabilnego komputera kwantowego przeprowadzającego algorytm Shora dla liczb złożonych z 2 liczb pierwszych 3072-bitowych.

Komunikator „Valkyria Besiada” jest więc odporny na atak MITM polegający na przeprowadzeniu podmiany serwera serwisu katalogowego. Serwer DMTP tego komunikatora opiera się na najprostszym rozwiązaniu – przekładaniu wiadomości z jednej kupki na drugą wg zapewnień autorki oprogramowania. Wg zapewnień wkrótce kod serwera będzie jawny (aplikacja już teraz posiada otwarty kod źródłowy). Komunikator nie wymaga logowania, rejestracji, podawania jakichkolwiek danych osobowych typu adres e-mail czy numer telefonu. Aplikacja możliwa jest do uruchomienia na każdym systemie operacyjnym

posiadającym współczesną przeglądarkę internetową.

Aplikacja, według treści zamieszczonych na stronie, jest rozwijana wyłącznie z darowizn. Zarobek serwisu nie odbywa się na zbieraniu danych osobowych. Dodatkowo konstrukcja programu wskazuje, że aplikacja sama dba o to, aby rozmówcy, gdy to potrzebne, dokonali wzajemnych obowiązków informacyjnych wynikających z RODO, czego nie można uświadczyć w innych komunikatorach tego typu.

Innym problemem, na który należy zwrócić uwagę, jest to, że większość komunikatorów dostarcza otwarty kod, jednak gdy spróbowano go skompilować, nie dawał on docelowego kodu maszynowego. Dowód: analiza Security Messaging Apps, wiersz „Are reproducible builds used to verify apps against source code?”. Oznacza to, że to, co użytkownik uruchamia, może działać inaczej, niż opisano w otwartej części kodu, o ile nie podjął próby kompilacji oprogramowania. Komunikator „Besiada” posiada kod napisany w języku JavaScript, którego nie trzeba kompilować. Przechodzi więc również ten test bez negatywnych uwag.

Osobom, którym realnie zależy na prywatności, a nie tylko na ułudnym poczuciu prywatności i poczuciu bezpieczeństwa, odradzam komunikatory takie jak „Session”, „MS Teams”, „Apple iMessage”, „Whats App”, ponieważ ryzyko udanego ataku MITM jest nieakceptowalne w świecie, gdzie ważna jest prywatność. Komunikator „Besiada”, mimo że znajduje się dopiero w fazie rozwojowej (brak jest rozmów grupowych, rozmów przez kamerkę) nadaje się do prowadzenia zwykłych rozmów w 4 oczy z wykorzystaniem komunikacji tekstowej, transferu obrazków i plików oraz rozmów głosowych. Rozmowy głosowe działają nie najlepiej i są dostępne tylko w trybie P2P, czyli wtedy, gdy obie osoby się zgodzą na bezpośrednie połączenie i na ujawnienie adresu IP.

Autorstwo: RisaA
Źródło: WolneMedia.net