AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS

Porównanie mobilnych komunikatorów w prawdziwych scenariuszach ataków

Listopad 2019

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Kradzież urządzenia: urządzenie zostało przejęte przez nieznaną osobę i nie ma (nawet pośredniego) sposobu na interakcję z aplikacją. Posiadacz urządzenia próbuje uzyskać dostęp do danych przechowywanych w aplikacji.
Signal	C I Domyślnie Signal nie zmusza użytkownika do odblokowania aplikacji za pomocą hasła (lub Touch ID / FaceID). Ze względu na integrację z systemem, odbieranie połączenia nie wymaga od użytkownika wprowadzania kodu dostępu lub wykonywania uwierzytelniania biometrycznego (ta funkcja nie może być wyłączona). Aplikacja wykorzystuje systemowy kod PIN / dane biometryczne, więc jeśli atakujący znajdzie sposób na ominięcie blokady ekranu (przy użyciu skradzionego kodu PIN lub wymuszenia uwierzytelnienia biometrycznego) — dostęp do aplikacji może zostać przyznany. Signal używa ustawień systemowych do odblokowania (w systemie Android) — istnieje ryzyko nadpisania ustawień plików systemowych przez atakującego i uzyskania dostępu do aplikacji.
Wire	C I Domyślnie Wire synchronizuje się z systemem iOS, dzięki czemu historia połączeń rejestrów połączeń jest dostępna na zablokowanym ekranie (opcja Udostępnij w systemie iOS). Domyślne ustawienia pozwalają przeglądać wiadomości (powiadomienia i wiadomości na zablokowanym ekranie). Domyślnie Wire nie wymusza zablokowania aplikacji hasłem (lub Touch ID / Face ID). Aplikacja wykorzystuje systemowy kod PIN / dane biometryczne, więc jeśli atakujący znajdzie sposób na ominięcie blokady ekranu (przy użyciu skradzionego kodu PIN lub wymuszenia uwierzytelnienia biometrycznego) — dostęp do aplikacji może zostać przyznany.
Telegram	C I Domyślnie Telegram nie zmusza użytkownika do zablokowania aplikacji hasłem (np. Touch ID / Face ID). W przypadku kodu dostępu użytkownika przypisywany jest dedykowany kod (opcjonalnie Touch ID / FaceID). Aplikacja wykorzystuje systemowy kod PIN / dane biometryczne, więc jeśli atakujący znajdzie sposób na ominięcie blokady ekranu (przy użyciu skradzionego kodu PIN lub wymuszenia uwierzytelnienia biometrycznego) — dostęp do aplikacji może zostać przyznany. Lokalna baza danych Telegramu nie jest szyfrowana na niektórych platformach (stosowane jest tylko podstawowe zaciemnianie).
Usecrypt (wersja do wdrożeń zamkniętych)	C I Domyślnie Usecrypt zmusza użytkownika do skonfigurowania kodu, aby odblokować aplikację. Po 10 nieudanych próbach baza danych aplikacji jest wymazywana i zastępowana losowymi danymi. Aplikacja nie rejestruje otwarcia / zamknięcia aplikacji. Usecrypt nie korzysta z preferencji systemowych do odblokowania urządzenia (wzór / PIN / dane biometryczne).
Threema	C I Domyślnie Threema nie zmusza użytkownika do ustawienia blokady hasła. Istnieje jednak możliwość ustawienia kodu / biometrycznego (FaceID / Touch ID). Dodatkowa warstwa zapewnia ochronę danych — opcja usuwania po 10 nieudanych uwierzytelnieniach. Użytkownik ma możliwość wyboru pomiędzy PIN i FaceID / TouchID. Dziennik walidacji nie jest domyślnie rejestrowany. Entropia szyfrowania danych jest zapewniona przez zapewnienie losowego ruchu odcisków palców na ekranie konfiguracji, który oblicza klucz szyfrowania i identyfikator użytkownika. Threema dostarcza odbiorcy wiadomości zwrotnej na temat poziomu bezpieczeństwa wybranego przez wybranego użytkownika (skala 3 punktów)
WhatsApp	C I Domyślnie WhatsApp nie wymusza zablokowania aplikacji hasłem (lub Touch ID / Face ID). Aplikacja wykorzystuje systemowy kod PIN / dane biometryczne, więc jeśli atakujący znajdzie sposób na ominięcie blokady ekranu (przy użyciu skradzionego kodu PIN lub wymuszenia uwierzytelnienia biometrycznego) — dostęp do aplikacji może zostać przyznany.

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Wymuszanie dostępu do danych: Właściciel urządzenia jest zmuszony do wykonywania poleceń stron trzeciej, której celem jest uzyskanie dostępu do poufnych danych przechowywanych w aplikacji.
Signal	 Domyślnie Signal nie zmusza użytkownika do odblokowania aplikacji za pomocą hasła (lub Touch ID / FaceID). Ze względu na integrację z systemem, odbieranie połączenia nie wymaga od użytkownika wprowadzania kodu dostępu lub wykonywania uwierzytelniania biometrycznego (ta funkcja nie może być wyłączona). W przypadku zmuszenia do podania kodu PIN lub użycia danych biometrycznych nie ma żadnych możliwości ochrony dostępu do danych.
Wire	 Domyślnie Wire nie zmusza użytkownika do zablokowania aplikacji hasłem (lub Touch ID / FaceID). W przypadku zmuszenia do podania kodu dostępu nie ma możliwości ochrony dostępu do danych.
Telegram	 Domyślnie Telegram nie zmusza użytkownika do zablokowania aplikacji hasłem (lub Touch ID / FaceID). W przypadku zmuszenia do podania kodu dostępu nie ma możliwości ochrony dostępu do danych.
Usecrypt (wersja do wdrożeń zamkniętych)	 Usecrypt ma funkcję "paniccode" — użytkownik ustawia alternatywny kod odblokowujący dla aplikacji. Po wprowadzeniu w miejscu ważnego kodu odblokowującego aplikację, aplikacja usuwa i nadpisuje historię korespondencji. PANIC CODE – ten numer wprowadza się w tym samym momencie, co normalnie przy odblokowywaniu aplikacji.
Threema	Domyślnie Threeme nie zmusza użytkownika do zablokowania aplikacji hasłem (lub Touch ID / FaceID). W przypadku zmuszenia do podania kodu dostępu i wcześniejszym skonfigurowaniu tej opcji, baza danych zastanie wyczyszczona po 10 nieudanych próbach uwierzytelnienia.
WhatsApp	 Domyślnie WhatsApp nie zmusza użytkownika do zablokowania aplikacji hasłem (lub Touch ID / FaceID). W przypadku zmuszenia do podania kodu dostępu nie ma możliwości ochrony dostępu do danych.

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Anonimowość komunikacji IP: Została naruszona przez dostawcę usług internetowych, który próbuje uzyskać dostęp do wymienianych wiadomości i metadanych.
Signal	C I Aplikacja komunikuje się z serwerem, a ruch jest szyfrowany, przy założeniu, że zabezpieczenia systemu nie zostały naruszone.Aplikacja wykrywa i powiadamia użytkownika o zmianach w certyfikacie SSL (tj. kiedy ISP odszyfrowuje ruch do celów monitorowania).Domyślnie aplikacja korzysta z połączenia peer-to-peer, dlatego adresy IP zarówno wywołującego, jak i wywoływanego, mogą być rejestrowane przez ISP.
Wire	C I Aplikacja komunikuje się z serwerem, a ruch jest szyfrowany, przy założeniu, że zabezpieczenia systemu nie zostały naruszone.Aplikacja wykrywa i powiadamia użytkownika o zmianach w certyfikacie SSL (tj. kiedy ISP odszyfrowuje ruch do celów monitorowania).Domyślnie aplikacja korzysta z połączenia peer-to-peer, dlatego adresy IP zarówno wywołującego, jak i wywoływanego, mogą być rejestrowane przez ISP.
Telegram	C I Domyślnie szyfrowanie end-to-end nie jest włączone i użytkownik musi użyć funkcji Secret Chat, aby upewnić się, że kanał komunikacji jest zabezpieczony. W przypadku braku zastosowania tego wariantu nie ma gwarancji poufności wymienianych komunikatów.Aplikacja komunikuje się z serwerem, a ruch jest szyfrowany, przy założeniu, że zabezpieczenia systemu nie zostały naruszone. Aplikacja wykrywa i powiadamia użytkownika o zmianach w certyfikacie SSL (tj. kiedy ISP odszyfrowuje ruch do celów monitorowania). Domyślnie aplikacja korzysta z połączenia peer-to-peer, dlatego adresy IP zarówno wywołującego, jak i wywoływanego, mogą być rejestrowane przez ISP.
Usecrypt (wersja do wdrożeń zamkniętych)	C I Aplikacja komunikuje się z serwerem, a ruch jest szyfrowany, przy założeniu, że zabezpieczenia systemu nie zostały naruszone. Aplikacja wykrywa i powiadamia użytkownika o zmianach w certyfikacie SSL (tj. kiedy ISP odszyfrowuje ruch do celów monitorowania). Organizacja może wdrożyć własną infrastrukturę serwerową w celu zapewnienia komunikacjidla członków organizacji. Dostawca Internetu widzi tylko transfer danych do serwera Usecrypt (i tylko IP serwera proxy).
Threema	C I Aplikacja komunikuje się z serwerem, a ruch jest szyfrowany, przy założeniu, że zabezpieczenia systemu nie zostały naruszone. Threema używa dwóch różnych warstw szyfrowania w celu ochrony wiadomości między nadawcą a odbiorcą. Warstwy szyfrowanie end-to-end na podstawie kryptografii krzywej eliptycznej oraz warstwy transportowej - każda zaszyfrowana wiadomość od końca do końca jest ponownie szyfrowana w celu transportu między klient i serwer, w celu ochrony informacji nagłówka. Domyślnie Threema łączy się z IPv6 na serwerze. Przy przesyłaniu danych są przesyłane przez serwer. W przypadku połączeń, jeśli to możliwe, nawiązywane jest bezpośrednie połączenie między dzwoniącym a wywołanym (peer to peer) po skonfigurowaniu połączenia.
WhatsApp	C I Cała komunikacja między klientami WhatsApp, a serwerami WhatsApp jest osadzona w oddzielnym zaszyfrowanym kanale. Do szyfrowania wykorzystuje się mechanizm NoisePipes razem z algorytmami Curve25519, AES-GCM i SHA256 z Noise Framework Protocol dla długich połączeń interaktywnych. Domyślnie WhatsApp łączy się z serwerem, a nie bezpośrednio z użytkownikami.

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia; są pewne braki w zabezpieczeniach; nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Zabezpieczenia infrastruktury: Aplikacja po stronie operatora została naruszona, a atakujący uzyskał dostęp do danych przechowywanych na serwerach.
Signal	C I Zakres danych przechowywanych na serwerze nie jest precyzyjnie opisany i nie ma możliwości precyzyjnej oceny związanych z tym ryzyk.
Wire	C I Wire przechowuje wiele informacji na serwerze / w tym wszystkie kontakty i listę dzienników połączeń. Utrata / przekazanie kontroli nad serwerem przez operatora powoduje wyciek istotnych danych na temat użytkowników.
Telegram	C I Zakres danych przechowywanych na serwerze nie jest precyzyjnie opisany i nie ma możliwości precyzyjnej oceny związanych z tym ryzyk.
Usecrypt (wersja do wdrożeń zamkniętych)	C I Przejęcie serwera nie rodzi ryzyka wycieku wrażliwych danych, ponieważ żadne dane nie są przechowywane na serwerze.
Threema	C I Zakres danych przechowywanych na serwerze nie jest precyzyjnie opisany i nie ma możliwości precyzyjnej oceny związanych z tym ryzyk.
WhatsApp	C I Serwery WhatsApp nie mają dostępu do kluczy prywatnych użytkowników. Na serwerach przechowywane są zaszyfrowane wiadomości użytkowników (aż do momentu dostarczenia - do 30 dni) oraz metadane na temat przesyłanych wszystkich wiadomości (bez treści).

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Przekazanie urządzenia: Tymczasowe użyczenie telefonu np. w celu pokazania zdjęcia. W tym scenariuszu osoba tymczasowo korzysta z urządzenia i spróbuje uzyskać dostęp do poufnych danych przechowywanych w aplikacji.
Signal	C I Domyślnie Signal nie zmusza użytkownika do zablokowania aplikacji za pomocą hasła (lub Touch ID / FaceID). Ze względu na integrację z systemem, odbieranie połączeń nie wymaga uwierzytelniania użytkownika w aplikacji (tej funkcji nie można wyłączyć). Zrzuty ekranu z rozmów mogą być wykonywane. Signal nie wymaga wprowadzania hasła podczas przełączania między otwartymi aplikacjami. Aplikacja nie wymusza ponownego wprowadzenia hasła / weryfikacji danych biometrycznych.
Wire	C I Domyślnie ustawienia pozwalają przeglądać wiadomości na zablokowanym ekranie (powiadomienia i wiadomości). Aplikacja pozwala wyświetlić ostatni status w aplikacji paska menu. Zrzuty ekranu mogą być wykonywane.
Telegram	C I Domyślnie Telegram nie zmusza użytkownika do zablokowania aplikacji hasłem lub danymi biometrycznymi. Aplikacja nie rejestruje otwarcia / zamknięcia aplikacji. Zrzuty ekranu mogą być wykonywane.
Usecrypt (wersja do wdrożeń zamkniętych)	C I Domyślnie Usecrypt zmusza użytkownika do skonfigurowania kodu odblokowania aplikacji. Po przywróceniu w systemie aplikacji, użytkownik musi wprowadzić kod odblokowujący. Zrzuty ekranu mogą być wykonywane tylko na urządzeniach z systemem iOS. Domyślnie podczas przełączania między uruchomionymi aplikacjami zawartość aplikacji jest zaciemniona.
Threema	C I Domyślnie Threema nie zmusza użytkownika do zablokowania aplikacji hasłem lub danymi biometrycznymi. Aplikacja nie rejestruje otwarcia / zamknięcia aplikacji. Zrzuty ekranu mogą być wykonywane.
WhatsApp	C I Domyślnie Threema nie zmusza użytkownika do zablokowania aplikacji hasłem lub danymi biometrycznymi. Aplikacja nie rejestruje otwarcia / zamknięcia aplikacji. Zrzuty ekranu mogą być wykonywane.

Analiza została przeprowadzona w kontekście prawdopodobnych scenariuszy, w których komunikator jest atakowany przez zdeterminowanego napastnika, który próbuje ominąć zabezpieczenia, aby złamać poufność danych (C - confidentiality) lub integralność (I) aplikacji.

Ocena aplikacji w każdym scenariuszu: dostateczne zabezpieczenia | są pewne braki w zabezpieczeniach | nieefektywne zabezpieczenia lub ich brak

Komunikator	SCENARIUSZ ATAKU: Uruchamianie aplikacji: Na urządzeniu z root / jailbreak
Signal	C I Brak informacji o osłabieniu zabezpieczeń systemu — aplikacja działa bez przerwy.
Wire	C I Brak informacji o osłabieniu zabezpieczeń systemu — aplikacja działa bez przerwy.
Telegram	C I Brak informacji o osłabieniu zabezpieczeń systemu — aplikacja działa bez przerwy.
Usecrypt (wersja do wdrożeń zamkniętych)	C I Aplikacja informuje użytkownika o osłabieniu zabezpieczeń systemu. Aplikacja nie będzie działać na urządzeniu z root / jailbreak.
Threema	C I Brak informacji o osłabieniu zabezpieczeń systemu — aplikacja działa bez przerwy.
WhatsApp	C I Brak informacji o osłabieniu zabezpieczeń systemu — aplikacja działa bez przerwy.

AV LAB

THE INDEPENDENT ANTIVIRUS TESTS

Jako niezależna organizacja stojąca na straży bezpieczeństwa w Internecie, zajmujemy się dostarczaniem informacji z branży poprzez artykuły, relacje ze szkoleń oraz konferencji. Naszą dominantą są profesjonalne recenzje oraz testy bezpieczeństwa, które przeprowadzamy w warunkach zbliżonych do rzeczywistości. W testach wykorzystujemy szkodliwe oprogramowanie narzędzia oraz techniki obchodzenia zabezpieczeń, które są używane w prawdziwych atakach.