Smartfony przekazują dane o użytkownikach

22 listopada 2015

Pod pretekstem walki z terroryzmem służby specjalne różnych krajów próbują zdobyć bezpośredni dostęp do popularnych serwisów internetowych urządzeń mobilnych, co pozwoli im na inwigilowanie wszystkich użytkowników.[SN]

Współczesne smartfony i tablety mogą wiele powiedzieć o swoich właścicielach, którzy czasami nawet tego nie podejrzewają. Podczas pierwszego uruchomienia urządzenia użytkownik może nie zauważyć odznaczenia funkcji geolokalizacji i zacznie zapisywać geograficzne położenie. Ponadto współczesne smartfony podczas pierwszego uruchomienia proponują, by włączyć opcję wyszukiwania urządzenia w przypadku jego utraty. Pozwoli to je znaleźć lub nawet wyśledzić złodzieja w przypadku kradzieży, ale jeśli jest dla was ważne, by postronni nie znali każdego waszego kroku, należy wyłączyć geolokalizację. Niestety, teraz w zasadzie każda aplikacja zapisuje dane o miejscu pobytu.[SN]

Niepożądane jest także to, by w ręce osób trzecich trafiła prywatna korespondencja. Stuprocentowej gwarancji jej bezpieczeństwa nie może dać nawet najbardziej pewne hasło, jednak znacznie zostanie utrudniony dostęp do Messengera z szyfrowanym przesyłaniem danych. W Rosji jest coraz bardziej popularny stworzony przez Pawła Durowa Telegram, już oskarżany o wykorzystywanie przez terrorystów, oraz Signal – osobisty wybór Edwarda Snowdena.[SN]

Kolejnymi narzędziami umożliwiającymi gromadzenie informacji o użytkownikach mogą się stać „inteligentni” asystenci „Siri”, „Google Now” i „Cortana”. Jeśli dla „Siri” możliwość przewidywania pytania użytkownika na podstawie poprzednich zapytań pojawiła się jedynie w nowym iOS 9, to „Google Now”

już posiada rozszerzone możliwości „inteligentnej” selekcji danych (zarówno przychodzących wiadomościom jak i działań). Aby pomóc użytkownikowi, asystent uwzględnia harmonogram dnia, najczęściej uczęszczane trasy, zapytania w wyszukiwarce, a nawet listę zakupów w internecie. To samo można powiedzieć o nowym mobilnym asystencie Microsoftu „Cortana” – aktywnie zgromadzi dane o użytkowniku, by wygenerować najbardziej relatywne odpowiedzi na zapytania.[SN]

Należy zachowywać ostrożność nawet podczas zwykłego korzystania z sieci. W Rosji wiele publicznych punków dostępu do Wi-Fi już podlega regulacji rządowej numer 758. Dokument przewiduje, że operator telekomunikacyjny przed udostępnieniem internetu musi zażądać podania numeru telefonu komórkowego, na który wysyłany jest kod potwierdzający. Oznacza to, że podczas łączenia się z siecią automatycznie dokonuje się również autoryzacja, a ponieważ karta SIM wydana została na konkretne nazwisko, provider internetowy poznaje tożsamość klienta. Ponadto większość operatorów może też ustalić czas i miejsce podłączenia się do sieci.[SN]

Głównym problemem osób, które chcą uniknąć inwigilacji, pozostaje sama architektura internetu: każde łączące się z siecią urządzenie ma swój unikalny identyfikator, czyli adres IP. Jest on niezbędny do prawidłowego przekierowywania danych i dzięki niemu można określić, gdzie fizycznie znajduje się urządzenia i, oczywiście, jego właściciel.[SN]

Choć nowoczesna elektronika pozwala na wyłączenie geolokalizacji, a programy – szyfrować dane, to zastosowanie technologii anonimizacji powoduję utratę funkcjonalności. Na przykład, nie wiedząc, gdzie się znajdujecie, GPS nie będzie mógł wytyczyć trasy. Dlatego trzeba wybierać: owoce cywilizacji z ryzykiem przekształcenia prywatnych danych w publiczne, czy wolność bez typowych konsumenckich udogodnień.[SN]

Okazuje się też, że połowa połączeń nawiązywanych przez 500

najpopularniejszych aplikacji na Androida nie ma nic wspólnego z potrzebami użytkownika. Naukowcy z MIT-u odkryli, że aż 50% połączeń z i do aplikacji jest inicjalizowanych przez moduły analizy danych, które służą nie użytkownikom, a twórcom oprogramowania. „Może istnieć bardzo ważna przyczyna, dla której te ukryte przed użytkownikiem połączenia są rozpoczynane. Nie twierdzimy, że należy z tym skończyć. Uważamy jednak, że użytkownicy powinni o tym wiedzieć" – mówi doktor Julia Rubin z Computer Science and Artificial Intelligence Laboratory (CSAIL) MIT-u. W pracach zespołu Rubin brali udział profesor Martin Rinard, doktor Michael Gordon oraz Nguyen Nguyen z firmy UWin Software.[KW]

Specjaliści zauważyli, że różne działania podejmowane przez konkretną aplikację mogą wymagać nawiązania łączności na zewnątrz. Aplikacje otwierają wówczas nowe kanały połączenia dla każdej operacji. Uczeni przeanalizowali kanały otwierane przez 500 najpopularniejszych aplikacji i odkryli, że połowa z nich nie ma związku z tym, czego potrzebuje użytkownik. Nie musi to jednak oznaczać, że w każdej chwili połowa wysyłanych danych to informacje, o których użytkownik nie ma pojęcia. Jeśli mamy otwartą długą sesję wysyłania danych, na przykład transferujemy jakiś duży plik, to stosunek danych wysyłanych przez aplikację do danych, które wysyłamy świadomie, jest bardzo mały. Z czasem aplikacja przestaje wysyłać swoje dane, ale kanał komunikacji pozostaje otwarty.[KW]

Co prawda większość oprogramowania ma zamknięty kod i nie można go swobodnie analizować, jednak muszą one korzystać ze standardowych interfejsów umożliwiających współpracę z systemem operacyjnym. To właśnie dzięki temu specjaliści są w stanie stwierdzić, jaka część aplikacji zajmuje się np. wyświetlaniem użytkownikowi informacji, o jakie prosił, jaka odtwarza pożądany przez użytkownika dźwięk, a jaka zajmuje się przesyłaniem danych, o których użytkownik nie ma pojęcia. Szczegółowa analiza przepływu danych pozwala na stwierdzenie, z jak wielu informacji korzysta użytkownik, a z ilu – twórca

aplikacji.[KW]

Specjaliści z MIT-u przeprowadzili tez interesujący eksperyment. Zmodyfikowali 47 ze 100 najpopularniejszych aplikacji tak, by nie wysyłały one żadnych informacji, które nie służą użytkownikowi. Następnie przetestowali te programy pod kątem ich użyteczności oraz wydajności i porównali z niezmodyfikowanymi wersjami programów. Okazało się, że w przypadku 30 z 47 aplikacji nie było żadnej różnicy w działaniu pomiędzy wersją zmodyfikowaną a niezmodyfikowaną. W dziewięciu przypadkach z programów zniknęły reklamy, ale aplikacje działały bez zarzutu. W trzech przypadkach zauważono niewielkie różnice, na przykład ze zmodyfikowanej wersji zniknęła ikona aktualizacji programu. W kolei w pięciu przypadkach aplikacje w ogóle przestały działać, z tym, że jeden z tych przypadków był związany z zabezpieczeniami przed odsprzedażą oprogramowania stronie trzecieć. Nie ustalono, dlaczego w pozostałych czterech przypadkach programy nie działały.[KW]

Naukowcy przeanalizowali też dane z niektórych aplikacji, starając się ustalić, do jakich celów ich autorzy wykorzystują otrzymywane informacje. Dowiedzieli się, na przykład, że aplikacja pozwalająca skanować kody paskowe i poznać ceny produktów w Wal-Marcie wysyła na firmowy serwer informacje, które wydają się powiązane z serwisem eBay. Zablokowanie wysyłania tych informacji nie wpłynęło na pracę programu. Z kolei gra Candy Crush Saga, którą przed kilku laty oskarżano o naruszenia prywatności, nie wysyłała nigdzie żadnych danych.[KW]

Narzędzia analityczne wykorzystane przez uczonych z MIT-u bazowały na wcześniejszym projekcie grupy Rinard, która brała udział w zawodach zorganizowanych przez DARPA. W ramach czteroletnich badań dziewięć uczelni rozwijało techniki wykrywania złośliwego kodu w programach tworzonych przez firmy trzecie na zlecenie Pentagonu.[KW]

Autorstwo: Sputnik [SN], Mariusz Błoński [KW]
Źródła: pl.SputnikNews.com [SN], KopalniaWiedzy.pl [KW]
Kompilacja 2 wiadomości: WolneMedia.net