

Elektroniczne odciski palców

30 kwietnia 2014

Profesor Romit Roy Choudhury i studenci Sanorita Dey oraz Nirupam Roy z University of Illinois wykazali, że podzespoły znajdujące się w smartfonach są na tyle unikatowe, iż pozwalają na jednoznaczne zidentyfikowanie urządzenia i jego śledzenie. Są podobne do odcisków palców, ale jednocześnie dają ewentualnemu śledzącemu znacznie większą wiedzę, gdyż pozwalają określić, gdzie użytkownik urządzenia przebywał w danej chwili oraz – często – co robił.

Badacze skupili się na akcelerometrach. To czujniki śledzące ruchy smartfona w trzech wymiarach. Są one wykorzystywane przez liczne aplikacje, od gier po programy służące do liczenia kroków. Aplikacje takie otrzymują dane z akcelerometrów, ale wykorzystują niewielką część z nich. Tymczasem szczegółowa analiza takich danych pozwala na jednoznaczne zidentyfikowanie urządzenia. „Fabryki produkujące sprzęt nie są w stanie wytworzyć milionów identycznych urządzeń. W każde z nich wkradają się jakieś niedoskonałości. I te właśnie niedoskonałości stają się unikatowymi odciskami” – stwierdził Roy.

Naukowcy przetestowali ponad 100 akcelerometrów: 80 osobnych chipów przeznaczonych dla smartfonów, 25 smartfonów z Androidem oraz 2 tablety. Wybrano urządzenia różnych producentów, by upewnić się, że występujące w akcelerometrach błędy nie są specyficzne dla jednej linii produkcyjnej. Szczegółowe badania ujawniły, że na podstawie dogłębnej analizy danych przekazywanych przez akcelerometry można zidentyfikować konkretne urządzenie z 96-procentową dokładnością. „Nie potrzebujemy żadnych innych informacji o telefonie, ani jego numeru, ani numeru karty SIM. Patrząc tylko i wyłącznie na dane z akcelerometra możemy stwierdzić, z którego urządzenia pochodzą. Są jak każdy inny identyfikator” – mówi Dey.

Okazuje się zatem, że nawet jeśli nie wyraziliśmy zgody na zbieranie informacji o naszej aktywności, dane takie i tak są zbierane. Nie ma bowiem żadnych wymagań dotyczących wyrażenia przez użytkownika zgody na wykorzystywanie przez aplikację akcelerometru.

Do śledzenia konkretnego urządzenia konieczne jest zebranie próbki danych z akcelerometru. W tym celu uczeni poddawali urządzenie dwusekundowym wibracjom, podobnym do tych informujących o nadejściu SMS-a. Akcelerometr odczytywał te wibracje i przesyłał sygnał, który należało przechwycić. „Nawet jeśli wykasowałeś daną aplikację z telefonu czy usunąłeś i przeinstalowałeś całe oprogramowanie, to urządzenie nadal ma ten sam charakterystycznych 'odcisk'. To poważne zagrożenie prywatności” – stwierdzili uczeni.

Obecnie nie istnieje żaden środek zaradczy, który chroniłby naszą prywatność przed osobą, chcącą śledzić nas za pomocą akcelerometra. Obudowy telefonów nie blokują sygnału, a celowe wprowadzenie szumu mającego ukryć sygnał mogłoby doprowadzić do błędów w pracy aplikacji wykorzystujących akcelerometr.

Naukowcy przypuszczają, że także inne podzespoły w smartfonach – żyroskopy, mikrofony, kamery itp. – również posiadają niedoskonałości pozwalające na zidentyfikowanie urządzenia. Zatem nawet jeśli przy próbach masowego śledzenia użytkowników smartfonów odsetek prawidłowej identyfikacji pojedynczego podzespołu się zmniejsza, to jednoczesne śledzenie kilku podzespołów pozwoli na jednoznaczne zidentyfikowanie urządzenia. „Wyobraźmy sobie, że jakimś cudem odciski palców twojej prawej ręki są identyczne z odciskami palców mojej prawej ręki. Ale prawdopodobieństwo, że i odciski palców naszych lewych dłoni będą identyczne jest bardzo małe. Zatem jeśli nawet w grupie milionów akcelerometrów będą takie o identycznych niedoskonałościach, to gdy połączymy śledzenie akcelerometra z np. śledzeniem żyroskopu, będziemy mogli nadzorować konkretne urządzenie w czasie i przestrzeni” – wyjaśnia profesor Choudhury.

Autor: Mariusz Błoński

Na podstawie: PhysOrg

Źródło: [Kopalnia Wiedzy](#)