CZUJNIK ŚWIATŁA MOŻE STAĆ SIĘ ZAGROŻENIEM DLA PRYWATNOŚCI UŻYTKOWNIKÓW

Obecnie większość popularnych urządzeń mobilnych takich jak smartfony czy tablety korzysta z czujników światła dopasowując jasność ekranu do otoczenia w którym się znajdujemy. Jednak jak udało się zbadać dr Łukaszowi Olejnikowi, może on zostać wykorzystany do profilowania czy nawet określenia rozmiarów miejsca w którym korzystamy z urządzenia.

Nowe technologie nie zawsze są bezpieczne

Większość urządzeń, z których korzystamy obecnie jest wyposażona w czujnik światła, ułatwia on nam korzystanie z telefonu dopasowując jasność ekranu do poziomu światła jaki znajduje się w otoczeniu. Powoduje, że w nocy kiedy korzystamy z urządzenia nie świeci ono zbyt mocno, lub odwrotnie w dzień pozwala nam na swobodne korzystanie i pracowanie np. na naszym laptopie. Oprócz tego przeglądarki zaczynają implementować mechanizmy pozwalające każdej stronie internetowej odczytanie danych właśnie z tych sensorów światła. Według dr Łukasza Olejnika to właśnie kod obecny w przeglądarkach oraz informacje jakie są zbierane przez sam czujnik może przyczynić się do wycieku informacji. Choćby możliwość potencjalnego stwierdzenia, że dwie osoby znajdują się w tym samym pomieszczeniu. I być może wyda się to to być przydatnym niektórym osobom/organizacjom.

Czujnik zagrożeniem dla naszego bezpieczeństwa

Na pierwszy rzut oka informacje, które zbiera sam czujnik wydają się nie mieć większego znaczenia dla naszej prywatności oraz bezpieczeństwa. Jednak przy odpowiednio długim pobieraniu takich informacji można stwierdzić, np. w jakich porach dniach korzystamy z naszych elektronicznych narzędzi, jak duże jest pomieszczenie w którym przebywamy czy po której stronie mamy okna. Problem wydaje się z początku trywialny, potencjalna strona zainteresowana złym wykorzystaniem, może dokonać podobnego rekonesansu obserwując nasze mieszkanie przez kilka dni. Jednak nie trudno sobie wyobrazić scenariusza w którym, haker obserwując setki takich domów, będzie wstanie stworzyć odpowiednią bazę, którą potem sprzeda. Baza może zostać wykorzystana do zwykłego włamania lub nawet przeprowadzenia kampanii ransomware. Oczywiście jeżeli uznamy, że im większy dom, tym więcej pieniędzy ktoś będzie wstanie zapłacić za sam okup swoich zaszyfrowanych plików. Bardziej prawdopodobnym scenariuszem, który Łukasz Olejnik przedstawia w swojej analizie jest wykorzystanie tych informacji w systemach śledzących czy reklamowych.

Jak podkreśla Łukasz Olejnik w swojej analizie, dzięki czujnikom można także w pewnym stopniu sprofilować samą potencjalną ofiare. Bazując tylko na prostych informacjach jakie sam czujnik dostarcza, w jakich porach dania pracuje, przy jakim świetle, jak często zmienia miejsce i inne. Wśród potencjalnych zagrożeń Olejnik wymienia także rozwój Internetu Rzeczy, który może spowodować np. możliwość dokładnego zmierzenia rozkładu pokojów bazując np. tylko na kilku czujnikach obecnych w domu.

Zbyt dokładne dane szkodzą prywatności

Jednak realny problem pojawia się w przypadku smartfonów, które posiadają czujniki światła i korzystają z przeglądarek, które posiadają odpowiednie oprogramowanie pozwalające na odczytywanie danych z samego sensora. Ujawni się on zbyt dokładnym odczytywaniem danych przez Ambient Light Sensors API, ponieważ realnie nie ma większych różnic pomiędzy naświetleniem o wartości 1 i 1.33 luxów, zbyt dokładny odczyt ewentualnie może pozwolić na dokładniejsze śledzenie ludzi. To pierwszy krok, jaki według Olejnika, powinien zostać uczyniony jeżeli chodzi o samo oprogramowanie. W dodatku twórcy przeglądarek powinni skupić się nad tym aby samo mechanizm odpowiedzialny za dopasowanie jasności ekranu posiadał odpowiednie pozwolenia od użytkowników oraz innych aplikacji na urządzeniu. Łukasz Olejnik poinformował dostawców przeglądarek o istniejącym problemie, obecnie pracują nad poprawą swoich rozwiązań.

Łukasz Olejnik jest konsultantem bezpieczeństwa i prywatności i badaczem na University College London. Jest także ekspertem World Wide Web Consortium (W3C).

Sam autor prosi o odwiedzenie jego obecnie trwającego projektu badawczego pod nazwą Sensors Privacy, który służy do zbadania oraz szerszego omówienia kwestii związanych z zagadnieniem prywatności sensorów w ramach działalności w W3C.

Czytaj też: Edward Snowden chce chronić smartfony przed podsłuchami za pomocą etui