

Stan baterii może służyć do śledzenia w sieci

10 sierpnia 2015

Informacja o stanie baterii okazuje się kolejnym szczegółem, który może zagrozić Twojej prywatności. W jaki sposób? Wystarczy, że strona, z której korzystasz, otrzymuje informacje na ten temat.

Prywatność online to trudna sprawa. Wszędzie są ciasteczka, a do tego powstają nowe technologie śledzenia takie jak canvas fingerprinting. Poza tym różne informacje o naszym urządzeniu mogą być zbierane nawet w celach innych niż śledzenie, ale ostatecznie mogą i tak służyć do śledzenia. Taką informacją może być... status baterii.

Nie każdy wie, że strony, z jakimi się łączymy, mogą mieć dostęp do informacji o stanie baterii urządzenia mobilnego lub laptopa. Jest to możliwe dzięki specjalnemu API w HTML5, które zostało wprowadzone dawno temu. Już w roku 2012 niektórzy deweloperzy zwracali uwagę na potencjalnie zagrożenia dla prywatności. Mimo to API jest wspierane przez Firefoksa, Operę i Chrome, bez zastosowania szczególnych rozwiązań chroniących prywatność.

Po co informacja o stanie baterii? Może ona pozwalać na przełączenie strony lub aplikacji w tryb bardziej energooszczędny, jeśli bateria jest na wyczerpaniu. To ma sens. Naukowcy z Francji i Belgii ustalili jednak, że informacje uzyskiwane przez strony internetowe mogą być na tyle dokładne, by identyfikować użytkownika. Te informacje obejmują szacowany czas do wyczerpania baterii oraz stan baterii wyrażony w procentach. Ta para liczb może tworzyć specyficzny identyfikator.

Najkrótszy zaobserwowany przez badaczy czas do wyczerpania baterii wynosił 355 sekund. Najdłuższy sięgał 40 277 sekund. W

tym zakresie mamy ponad 39 tysięcy możliwych numerów. Do tego mamy 90 możliwych stanów baterii wyrażonych procentowo (jeśli założymy, że ludzie podłączają baterię do ładowania, gdy jej poziom spadnie poniżej 10%).

Oczywiście taki identyfikator nie może pozwalać na wieczne śledzenie danej osoby, ale śledzenie w krótkim okresie czasu jest możliwe. Istnieje względnie małe prawdopodobieństwo wystąpienia tych samych identyfikatorów u dwóch osób.

Dane o stanie baterii są aktualizowane co pół minuty, ale ten tymczasowy identyfikator jest niezależny od takich rzeczy jak ciasteczka. Załóżmy więc, że ktoś wchodzi na stronę, a potem przełącza się na przeglądarkę w trybie „prywatnym” (incognito) i znów wchodzi na stronę. Istnieje możliwość połączenia tych dwóch wizyt z jedną osobą.

Badacze ustalili również, że istnieje możliwość identyfikowania ludzi przez dłuższy czas, jeśli uda się ocenić maksymalne wartości pojemności baterii. Ta metoda jest o wiele trudniejsza i nie zawsze da się jej użyć.

Czy w tym przypadku dałoby się zapobiec zagrożeniom dla prywatności? Sam dostęp do statusu baterii nie musi być zły, ale zdaniem badaczy użytkownik powinien wyrażać zgodę na ten dostęp. Ta uwaga dotyczy wielu innych „zagrożeń dla prywatności”. One nie będą „zagrożeniami”, jeśli będą opcjonalne, a ludzie będą świadomie się zgadzać na używanie tych rozwiązań.

Autorstwo: Marcin Maj

Na podstawie: ePrint.iacr.org

Źródło: DI.com.pl