Kraków, 23 sierpnia 2017 r.

Sprawdzamy, która metoda blokady ekranu jest najbezpieczniejsza

Wydaje się, że zablokowany ekran jest barierą nie do przejścia. Jednak jak się okazuje, chętnie wybierana blokada z wykorzystaniem wzoru może zostać złamana w zaledwie 90 sekund, a do obejścia zabezpieczenia za pomocą odcisku palca wystarczy niedrogi kompozyt dentystyczny i odrobina plasteliny.

Hasło i PIN

Ten sposób wydaje się być najskuteczniejszym zabezpieczeniem – możemy stworzyć kod PIN o długości minimum 4 cyfr lub hasło, składające się z małych i wielkich liter, znaków specjalnych oraz cyfr. Niełatwo będzie je odgadnąć, o ile nie postawimy na najpopularniejsze kombinacje, takie jak qwerty, asdf, 1234 czy 1111 lub schematy związane z datami, imionami lub nazwami własnymi.

Jednak pomimo wysokiej skuteczności takiego hasła, sprytny użytkownik odkrył lukę, która pozwalała uzyskać dostęp do smartfona z Androidem w wersji 5.x, zabezpieczonego hasłem – wystarczyło uruchomić aplikację Aparat i następnie na ekranie połączenia alarmowego wpisać bardzo długi ciąg znaków. Skutkowało to chwilowym zawieszeniem się urządzenia, a następnie uzyskaniem pełnego dostępu. Luka ta została usunięta w aktualizacji systemu, jednak co jakiś czas pojawiają się nowe sposoby na obejście blokady hasłem lub PIN-em.

Blokada za pomocą wzoru

W przypadku tej metody odblokowanie urządzenia wymaga narysowania palcem na ekranie ustalonego wcześniej wzoru na polu, składającym się z dziewięciu punktów. Wzór musi mieć długość od 4 do 9 punktów. Daje to około 150 milionów możliwych kombinacji. Jednak w praktyce użytkownicy wykorzystują zaledwie ułamek z tej liczby, przez co sama metoda w gruncie rzeczy nie jest tak bezpieczna, jak by się mogło wydawać.

Według anonimowych badań ekspertów od zabezpieczeń urządzeń mobilnych co czwarty smartfon jest chroniony jednym z 15 najpopularniejszych wzorów. Pozwala to w teorii przyjąć, że złamanie zabezpieczeń statystycznego urządzenia może zająć odpowiednio przygotowanej

osobie maksymalnie 90 sekund – ponieważ po pięciu nieudanych próbach należy odczekać 30 sekund.

Skanowanie tęczówki oka

Cechami charakterystycznymi tęczówki oka każdego człowieka są unikalny układ oraz jego niezmienność w czasie. Dzięki temu można wykorzystać tęczówkę, podobnie jak odcisk palca, jako zabezpieczenie biometryczne. Do skanowania tęczówki oka jest wykorzystywany specjalny moduł oraz dioda doświetlająca twarz światłem podczerwonym. Proces skanowania jest bardzo szybki – odblokowanie smartfona tym sposobem trwa niecałą sekundę.

Niestety mimo pozornie wysokiego poziomu bezpieczeństwa, metoda ta została bardzo szybko złamana. Hakerowi ukrywającemu się pod pseudonimem Starbug wystarczyło odpowiednio spreparowane zdjęcie oka oraz nałożona na nie soczewka kontaktowa. Najnowszy Samsung Galaxy S8, wyposażony w skaner IRIS, został bezproblemowo odblokowany już przy pierwszym podejściu.

Odcisk palca

Skaner odcisków palców nie jest niczym nowym w świecie technologii, jednak dopiero w ostatnich latach zdobył popularność na rynku konsumenckim. Rolą czytnika linii papilarnych jest identyfikacja użytkownika po unikalnym układzie bruzd i grzbietów na opuszku palca. Każdy człowiek na świecie ma swój własny i niepowtarzalny układ linii — nawet bliźnięta jednojajowe.

Jednak czytnik linii papilarnych, tak jak każde inne zabezpieczenie, nie zapewnia 100% bezpieczeństwa. Do jego złamania wystarczy kompozyt dentystyczny i plastelina oraz oczywiście dostęp do dłoni użytkownika konkretnego urządzenia. W 2014 roku hakerom udało się wydrukować działający odcisk palca niemieckiego ministra obrony na podstawie zdjęcia, opublikowanego w internecie.

Zabezpieczenie bez kodu

Jako ciekawostkę można wymienić metodę, która zabezpiecza smartfona i nie wymaga wprowadzania kodu PIN lub rysowania wzoru za każdym razem, gdy chcemy z niego skorzystać. Użytkownicy smartfonów z Androidem mogą skorzystać z opcji, która nazywa się Smart Lock. Umożliwia ona automatyczne odblokowywanie urządzenia w określonych sytuacjach.

Smartfon pozostanie odblokowany, gdy wykryje, że jest w pobliżu ciała, kiedy znajdzie się w konkretnym miejscu, jeśli będzie w zasięgu określonego urządzenia Bluetooth oraz gdy wykryje

twarz użytkownika. Funkcje te działają dzięki akcelerometrowi, modułowi Bluetooth oraz GPS i przedniej kamerce. Dodatkowym zabezpieczeniem jest automatyczne włączenie blokady ekranu po 4 godzinach bezczynności.

Jak zrobić to dobrze?

„Nie korzystajmy zatem z prostych kształtów przy blokadzie ekranu wzorem. Unikajmy odniesień do imion, dat oraz potocznych wyrazów przy korzystaniu z PIN-ów i haseł” – powiedział Piotr Pachota z serwisu GoRepair. *„Wyłączmy także wszelkie funkcje i mechanizmy, które mogą ułatwić uzyskanie dostępu do naszego smartfona osobom postronnym. A najlepiej wykorzystajmy podwójne zabezpieczenia i ograniczmy do minimum liczbę możliwych nieudanych prób odblokowania”* – dodał.

Jak widać żaden z wymienionych sposobów na blokadę ekranu nie zapewnia pełnego bezpieczeństwa naszych danych. Aby nie być łatwym celem, trzeba zastosować się do najważniejszej reguły: bezpieczeństwo jest ważniejsze od komfortu.

O firmie GoRepair

GoRepair to pogwarancyjny serwis naprawiający smartfony, tablety i laptopy najpopularniejszych marek. Wygodne narzędzie dostępne na stronie internetowej umożliwia łatwe i szybkie zgłoszenie usterki oraz wybór terminu, w którym kurier odbierze urządzenie od klienta. Dla większości napraw dostępna jest natychmiastowa wycena kosztów. Typowe uszkodzenia są naprawiane od ręki, a w bardziej skomplikowanych przypadkach czas naprawy jest ustalany indywidualnie. Gwarancja udzielana na usługi wykonane przez GoRepair to 12 miesięcy.

Więcej informacji: www.gorepair.pl

Kontakt dla mediów

Agencja WĘC Public Relations

Tomasz Węc / PR Director
E-Mail: tomasz@wec24.pl
Telefon: 667 954 282

Łukasz Warchoł / Senior PR Executive
E-Mail: lwarchol@wec24.pl
Telefon: 535 954 212