https://plblog.kaspersky.com/czy-platnosci-zblizeniowe-sa-bezpieczne/3387/

Czy płatności zbliżeniowe są bezpieczne?

04/08/2015 Vladislav Biryukov Bezpieczeństwo, Informacje, Post dnia 0 komentarzy

"Należy się 12,95 zł"- mówi kasjer w osiedlowym supermarkecie. Biorę swój portfel, dotykam nim terminala, czekam sekundę, słyszę piknięcie i – voila! – zapłacone!

Bankowe karty zbliżeniowe są bardzo wygodne. Nie musisz przeciągać swojej karty, wprowadzać PIN-u, podpisywać rachunku, wyjmować jej z portfela, szukać gotówki czy łowić monet w czeluści kieszeni. Po prostu przybliżasz – i już.

Kasjerzy także mają powody do zadowolenia: zakup obywa się o wiele szybciej, więc i efektywność kasjera jest większa.

Chociaż ta prostota użycia sprawia, że zastanawiasz się, czy można tak łatwo ukraść też Twoje pieniądze. Czy przestępca może zwyczajnie dotknąć Twojej kieszeni ukrytym czytnikiem i całkowicie pozbawić Cię ciężko zarobionych pieniędzy?

Aby się tego dowiedzieć, przestudiowałem wiele raportów z konferencji poświęconych włamaniom oraz rozmawiałem z wieloma przedstawicielami banku. Ogólnie wnioski są pozytywne, choć jest też kilka drobnych wad.

Zasięg

Karty bezdotykowe używają technologii komunikacji krótkiego zasięgu (NFC). Karta łączy czip oraz antenę, która odpowiada na żądania terminala POS na częstotliwości 13,56 MHz. I chociaż każdy system płatności używa swojego standardu (np. Visa payWave, MasterCard PayPass, American Express ExpressPay, etc.), to wszystkie stosują to samo podejście i tę samą technologię.

Zasięg transmisji NFC jest mały i wynosi nie więcej niż 4 cm. Zatem pierwsza linia obrony jest fizyczna – czytnik powinien znajdować się w bezpośredniej bliskości karty, co trudno byłoby wykonać niepostrzeżenie.

Chociaż ktoś mógłby stworzyć niestandardowy czytnik zdolny do działania na większej odległości. Na przykład, badacze z uniwersytetu w Surrey zademonstrowali kompaktowy skaner potrafiący czytać dane NFC na odległości 80 cm.

Urządzenie takie może wysyłać żądania do karty zbliżeniowej w transporcie publicznym, w centrach handlowych, na lotniskach i innych obszarach, w których znajduje się wielu ludzi. W wielu krajach karty kompatybilne z NFC znajdują się w co drugim portfelu, więc w przeludnionych miejscach przestępcy mogą znaleźć całkiem sporo ofiar.

Ostatecznie można poradzić sobie bez standardowego skanera czy fizycznej bliskości. Hiszpańscy hakerzy Ricardo Rodrigues i Jose Villa wymyślili elegancki sposób na wyeliminowanie dystansu i pokazali go podczas konferencji Hack in the Box.

Większość dzisiejszych smartfonów jest wyposażona w moduł NFC. Urządzenia te często znajdują się blisko portfela – na przykład w torebce czy kieszeni. Rodrigues i Villa opracowali trojana na Androida, który zmienia wybranego smartfona w urządzenie działające jak trandponder NFC.

Gdy zhakowany smartfon znajdzie się blisko karty bankowej, sygnalizuje atakującym możliwość przeprowadzenia transakcji. Wtedy oszuści aktywują zwykły terminal POS i umieszczają blisko niego swojego smartfona z funkcją NFC. Można powiedzieć, że pomiędzy kartą NFC a terminalem NFC powstaje niewidzialny pomost przez internet, niezależny od zasięgu.

Trojan może być dystrybuowany standardowymi metodami, np. poprzez pakiety szkodliwego oprogramowania czy zhakowane płatne aplikacje. Jedynym warunkiem jest to, aby system Android był w wersji 4.4 lub nowszy. Nie jest nawet konieczny dostęp do poziomu administratora, chociaż jest to pożądana opcja, aby trojan mógł działać nawet po zablokowaniu ekranu smartfona.

Szyfrowanie

Umieszczenie danej karty w obrębie spreparowanego czytnika to tylko połowa sukcesu. Jest jeszcze druga, poważniejsza linia obrony – szyfrowanie.

Transakcje bezprzewodowe są chronione tym samym standardem EMV, który zabezpiecza zwykłe plastikowe karty wyposażone w czip EMV. Podczas gdy pasek magnetyczny można z łatwością sklonować, w przypadku czipa nie jest to takie proste. Po odebraniu żądania z terminala POS jego układ scalony generował klucz jednorazowy. Można było go przechwycić, jednak nie byłby ważny dla kolejnej transakcji.

Badacze wiele razy wyrazili swoje obawy na temat bezpieczeństwa standardu EMV; chociaż nie słyszy się o prawdziwych przypadkach hakowania kart, które go wykorzystują.

Czy płatności zbliżeniowe są bezpieczne?

Jest jeszcze jedna kwestia, o której należy wspomnieć. W standardowym zastosowaniu koncepcja bezpieczeństwa kart EMV opiera się na kombinacji kluczy szyfrowania i wprowadzanego przez użytkownika kodu PIN. W przypadku transakcji bezstykowych kod PIN nie jest wymagany, więc w tym przypadku środki bezpieczeństwa są ograniczone do kluczy szyfrujących generowanych przez kartę i terminal.

"W teorii możliwe jest wyprodukowanie terminala, który odczytywałby dane NFC karty, będąc na przykład w kieszeni. Terminal taki powinien używać kluczy szyfrujących uzyskanych z banku przejmującego i systemu płatności. Klucze są wydawane przez bank przejmujący, co oznacza, że oszustwo byłoby łatwe do wyśledzenia", wyjaśnił Alexander Taratorin, dyrektor wsparcia aplikacji w Raiffeisenbank.

Wartość transakcji

Jest jeszcze jedna linia obrony: ograniczenie wartości transakcji dla płatności zbliżeniowych. Ograniczenie to jest zakodowane w ustawieniach terminala POS i o jego wysokości decyduje bank przejmujący na podstawie poleceń uzyskanych z systemów płatności. W Polsce maksymalna wartość transakcji zbliżeniowej wynosi 50 zł, w Stanach Zjednoczonych 25 dolarów, w Wielkiej Brytanii 20 funtów (wkrótce zostanie podniesiona do 30 funtów).

Jeśli wartość przewyższy ograniczenie, transakcja zostanie odrzucona lub trzeba będzie podać dodatkowy element potwierdzający, np. PIN czy podpis (w zależności od ustawień banku wydającego). Aby zapobiegać częstym obciążeniom na mniejsze kwoty, w sytuacji takiej także zostanie wywołany dodatkowy mechanizm bezpieczeństwa.

Chociaż i tu znalazła się luka. Prawie rok temu inny zespół badaczy z Uniwersytetu w Newcastle (Wielka Brytania) wykrył lukę w systemie bezpieczeństwie kart zbliżeniowych typu Visa. Po wybraniu dokonania płatności w walucie obcej (innej niż funty brytyjskie) badaczom udało się ominąć wspomniane ograniczenie. W przypadku gdy terminal POS jest w trybie offline, maksymalna wartość transakcji może osiągnąć nawet 1 milion euro.

Firma Visa informuje, że prawdopodobieństwo takiego ataku w prawdziwym życiu zmniejsza się, twierdząc, że tak ogromna transakcja zostałaby odrzucona przez bankowe systemy bezpieczeństwa.

Według Taratorina z Raiffeisenbank terminal POS kontroluje maksymalną wartość transakcji, bez względu na walutę.

Wybierzemy inną drogę

Czy wszystko zatem sprowadza się do tego, że praktycznie niemożliwa jest taka awaria systemu płatności banku, przez którą można by przeprowadzić podejrzane transakcje bezstykowe? Prawdopodobnie odpowiedź jest twierdząca, pod warunkiem że oszuści nie pracują dla danego banku.

Tymczasem są jeszcze inne wnioski: jeśli nie można przechwycić samej transakcji, technologia NFC może ułatwić kradzież danych uwierzytelniających karty płatności.

Standard EMV zakłada, że niektóre dane są przechowywane w pamięci czipu w postaci niezaszyfrowanej. W zależności od polityki banku wydającego lub systemu płatności mogą one zawierać numer karty, ostatnie transakcje itp. Dane mogą zostać odczytane za pośrednictwem smartfona z włączoną funkcją NFC, na którym zainstalowana jest oryginalna aplikacja (np. czytnik kart bankowych NFC).

Do niedawna uważano, że nie można złamać zabezpieczeń karty. Chociaż, wybitny brytyjski outlet mediów konsumenckich Which? niespodziewanie obalił stary mit.

Eksperci z Which? przetestowali kilka różnych kart bezprzewodowych emitowanych przez banki w Wielkiej Brytanii. Używając czytnika NFC oraz darmowego oprogramowania, odkodowali numery wszystkich kart i ich daty ważności.

Niby nie było się czym martwić. W końcu aby kupić coś w internecie, potrzebny jest numer CVV, prawda?

Niestety prawda jest taka, że wiele sklepów online nie wymaga numeru CVV. Eksperci z firmy Which? z powodzeniem zamówili telewizor za 3 tysiące funtów w jednym z największych sklepów internetowych.

Konkluzja

Chociaż technologia płatności bezprzewodowych zakłada stosowanie kilku warstw ochrony, nie oznacza to, że Twoje pieniądze są w stu procentach bezpieczne. Wiele elementów kart bankowych opiera się na przestarzałych technologiach, np. pasek magnetyczny czy możliwość płacenia w internecie kartą bez dodatkowej autoryzacji.

W wielu aspektach bezpieczeństwo zależy od ustawień używanych przez instytucje finansowe i sprzedawców. Ci ostatni, dążąc do przyspieszenia procesu zakupu i zmniejszenia liczby "porzuconych wózków", wolą czasami poświęcić bezpieczeństwo płatności na rzecz większego zarobku.

Poniżej znajdziesz ogólne podstawowe zasady bezpieczeństwa:

- zwracaj uwagę, aby podczas wprowadzania kodu PIN nikt obcy go nie widział,
- nie pokazuj karty publicznie,
- zachowaj ostrożność podczas pobierania aplikacji na swojego smartfona,
- zainstaluj antywirusa,
- włącz powiadomienia SMS-owe z banku,
- niezwłocznie informuj bank, jeśli zauważysz podejrzaną aktywność.

Jeśli chcesz być całkowicie pewny, że nikt nie odczyta Twojej karty NFC, rozważ zakup portfela ekranowanego. Nikt nie oszuka praw fizyki.