JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 15 (2020) 121-125
Received: 26 October 2019
Accepted: 4 November 2019

Comparison of the NFC authentication method with the methods available in Android

Porównanie metody uwierzytelniania NFC z metodami dostępnymi w Android

Dmytro Malenko*

Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract
Most multi-user applications need an access system so that users can log in from different devices. To identify a user, at least one authentication method must be used. The article presents a comparison of the authentication method using NFC technology with other methods that are available for Android devices and differ in both implementation and specific usage.

Keywords: android; nfc; safety

Streszczenie
Większość aplikacji przeznaczonych dla wielu użytkowników powinno korzystać z systemu autoryzacji, aby użytkownicy mogli logować się z różnych urządzeń. Aby zidentyfikować użytkownika, należy użyć co najmniej jednej metody uwierzytelnienia. W artykule przedstawiono porównanie metody uwierzytelniania wykorzystującej technologię NFC z innymi metodami dostępnymi dla urządzeń z Androidem, różniącymi się zarówno implementacją, jak i określonym zastosowaniem.

Słowa kluczowe: android; nfc; bezpieczeństwo

*Corresponding author
Email address: dimon95me@gmail.com (D. Malenko)

1. Wstęp

Technologia NFC (ang. Near Field Communication) została opublikowana w 2004 r. [1]. Od tego czasu stopniowo zdobywała popularność. W tej chwili prawie każdy telefon jest wykonany z wykorzystaniem tej technologii. Jednak technologia wciąż zyskuje na popularności. Jest stosowana w systemach płatności jako środek rozpowszechniania informacji (tag NFC), jako klucz dostępu. Wykorzystanie tej technologii jest ograniczone tylko wyobraźnią. Można śmiało powiedzieć, że technologia ta nie osiągnęła jeszcze swojego szczytu technicznego i stale się rozwija. Urządzenia do noszenia z obsługą tej technologii są już produkowane.

Jedną z ważnych cech jest niewielki rozmiar części technologicznej i niskie zużycie energii. W przypadku z tagami NFC zapewnienie zasilania jest konieczne tylko po stronie odbiorczej. Obecnie rozmiary części technologicznej pozwalają osadzić tę technologię niemal wszędzie. Od elektronicznych zegarków i bransoletek fitness po tkanki miękkie w ludzkim ciele [2].

W tej chwili dla programistów nie ma natychmiastowych i wygodnych rozwiązań. Poszukiwanie bibliotek dla najwygodniejszego zarządzania NFC za pomocą kodu wykazało, że obecnie najlepszym rozwiązaniem jest standardowa biblioteka NfcHelper. Jednocześnie, szukając oficjalnej dokumentacji, można dowiedzieć się, jak odczytywać i zapisywać informacje na poziomie urządzenia [3].

Z czasem potrzebne są nowe metody uwierzytelniania. Zbadanie nowej metody autoryzacji użytkownika za pomocą taga NFC pomoże dostrzec zalety i wady tego podejścia. Pomoże również zrozumieć, które warunki są najbardziej odpowiednie dla szybkiego, bezpiecznego i poprawnego odczytu danych z taga.

2. Analiza literatury

Peter Konrad Tysowski w artykule „Near-field communication (NFC) system providing NFC tag geographic position authentication and related methods" przedstawił alternatywną metodę autoryzacji za pomocą tagów zawierających geodane [4]. System sugeruje obecność telefonu, który może pobierać informacje o lokalizacji nie tylko z GPS. Podejście to dotyczy dużych i małych miast o niewystarczającym zasięgu sieci.

Artykuł „Wearable Authentication Device" Jamesa A Van Boscha i Pavla A. Shostaka przedstawia koncepcję noszonego urządzenia, które ma ulepszone połączenie z czytnikiem NFC [5]. Jego zwartość pozwala na dopasowanie projektu do wymiarów pierścienia. Zasada działania polega na lokalizacji dwóch anten zamiast jednej. Dzięki temu możliwe jest szybkie nawiązanie kontaktu zamiast wybierania domniemanej lokalizacji anteny.

Artykuł napisany przez Jurisa Klonovsa, Christoffera Kjeldgaarda Petersena, Henninga Olesena, Allana Hammershoj z tytułem „ ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System" mówi o zastosowaniu elektroencefalografu i tagów NFC [6]. Główny nacisk położony jest na podpis elektroencefalograficzny. System sugeruje biome-

tryczne rozpoznanie osoby na podstawie aktywności jego mózgu. Zgodnie z artykułem aktywność mózgu każdej osoby jest wyjątkowa. Aby uniknąć przypadkowej autoryzacji klienta, postanowili dodać technologię NFC i technologię rozpoznawania twarzy do schematu uwierzytelniania. System jest w początkowej fazie rozwoju i został zaprojektowany z myślą o postępie technologicznym, kiedy części systemu można będzie wykonać z bardziej kompaktowych urządzeń.

Ciekawe podejście zostało zastosowane w artykule Muhammada Qasima Saeeda i Colina D. Waltera „Offline NFC Tag Authentication". Najważniejsze jest użycie tagów NFC, gdy nie masz połączenia z Internetem. Integralność danych w tagach zapewniają podpisy cyfrowe. Konwencjonalne protokoły nie zapewniają ochrony przed użyciem kopii takich tagów. W tym artykule zaproponowano opcję zapobiegania stosowaniu kopii tagów. Rozwiązanie oparte jest na protokole protokół żądanie-odpowiedź z wykorzystaniem kryptografii klucza publicznego i PKI [7]. Proponowana opcja różni się bardzo od oryginalnego podejścia. Te podejście się odnosi do uwierzytelniania tagiem NDEF.

Artykuł „Mobile wireless communications device providing near field communication (NFC) unlock and tag data change features and related methods" mówi o odblokowaniu urządzenia za pomocą znacznika NFC. Ta metoda odblokowania urządzenia obejmuje dwie opcje odczytu. Pierwsza opcja to prosty odczyt i odblokowanie. Druga opcja polega na odblokowaniu urządzenia poprzez przepisanie klucza zgodnie z harmonogramem [8].

Artykuł „Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks" omawia sposoby uniknięcia przechwytywania informacji przez zewnętrznych słuchaczy. Rozważane są również wady tych metod. Główną ideą tego artykułu jest zmiana temperatury powierzchni tagu, co wpływa na sygnał i upośledza zdolność do przechwytywania sygnału. Z tego powodu czas transmisji danych na odległość zmienia się, a sygnał jest zniekształcony [9].

Artykuł „Two-factor user authentication using near field communication" autorstwa Philipa Hewinsona opisuje dwukierunkową weryfikację tożsamości. Unikalny klucz jest przechowywany w pamięci telefonu. Przy pierwszym podłączeniu taga do czytnika uwierzytelnienie zakończy się sukcesem, do tagu zapisywany jest oddzielny klucz, który identyfikuje tag. Przy następnym połączeniu z tagiem porównywany jest klucz identyfikujący telefon i klucz identyfikujący taga. Posiadanie dwóch kluczy do sprawdzania zwiększa bezpieczeństwo odblokowywania. Niezawodność staje się jeszcze większa dzięki dynamicznej zmianie klucza taga [11].

Standardowym protokołem przesyłania danych do znacznika NFC jest NDEF. Artykuł „Secure and Lightweight Authentication Protocol for NFC Tag Based Services" opisuje możliwości uszkodzenia danych na tagu z podanym protokołem i ich konsekwencje. Jako rozwiązanie zaproponowano dodatkowe protokoły, które są bardziej korzystne, gdy stosuje się niedrogie tagi z mniejszą pamięcią. Dodatkowymi zaletami dostarczonych protokołów są bezpieczniejsze rejestrowanie i przechowywanie danych, które zapobiegają fałszowaniu, DoS, modyfikacji danych i atakowi typu phishing[12].

Interesującą implementację anteny NFC do telefonów zaproponowano w artykule „NFC Antenna Design for Low-Permeability Ferromagnetic Material", napisanym przez Byungje Lee, Byeongkwan Kim, Frances J. Harackiewicz, Byeonggwi Mun, Hyunwoo Lee. W artykule opisano nową konstrukcję anteny opartą na zmianie struktury wewnętrznej pętli i uzwojenia. Zastosowanym materiałem jest kompozyt ferrytowo-polimerowy, który jest lepszy i bardziej skuteczny niż drogie elementy ferrytowe. Proponowana antena ma większy o 23% zasięg odczytu, i o 65% lepszą modulację obciążenia w porównaniu z rozwiązaniami obecnymi odpowiednikami na rynku [13].

Artykuł „Automated antenna impedance adjustment for Near Field Communication (NFC)" proponuje nowe podejście do odczytu różnych typów urządzeń. W telefonie moduł NFC jest ułożony inaczej niż na karcie bankowej lub w tagu NFC. Aby zapewnić pełną zgodność, urządzenie, które odczytuje, musi zawierać kilka rodzajów anten. Jako rozwiązanie zaproponowano jedną antenę z automatyczną regulacją anteny w oparciu o cyfrowe strojenie kondensatorów. W takim przypadku antena dostosowuje się do urządzenia nadawczego, skutecznie go identyfikuje i wymienia informacje[14].

3. Technologie badawcze

W artykule zbadano kilka różnych metod autoryzacji. Każda metoda ma swoje zalety i wady. Każda metoda została wybrana z uwzględnieniem bezpieczeństwa, wygody, dostępności rozwoju, wszechstronności i popularności wykorzystania.

Początkowo proponowane metody autoryzacji:

1. Biometryczne rozpoznawanie twarzy
2. Rozpoznawanie odcisków palców
3. Klasyczne hasło
4. Maskowane hasło
5. Odblokowanie za pomocą kodu QR
6. Odblokowanie za pomocą technologii NFC
7. Graficzny wzór

Wdrożenie autoryzacji przy użyciu biometrycznego rozpoznawania twarzy nie jest obecnie dostępne przy użyciu gotowych bibliotek do implementacji w aplikacjach innych firm. Rozwiązaniem do wprowadzenia metody autoryzacji wykorzystującej biometryczne rozpoznawanie twarzy jest jedynie samodzielne opracowanie i dostosowanie tej metody.

Rozpoznawanie odcisków palców jest obecnie bardzo popularne i niedrogie pod względem rozwoju. Niestety urządzenie wykorzystane w próbach przedstawionych poniżej nie posiadało czytnika odcisków palców dlatego nie uwzględniono tej metody odblokowywania w testach praktycznych.

Klasyczne hasło jest bardzo popularne i jest używane na prawie wszystkich systemach. Ta metoda autory-

zacji zostanie wykorzystana w badaniu i porównana z innymi metodami autoryzacji.

Maskowane hasło składa się z kilku pól, w których wpisany jest jeden znak. Każde pole odpowiada za określony znak hasła. Niektóre pola są nieaktywne i odpowiednio ponumerowane. Numeracja służy jako wskazówka, aby nie pomylić się podczas wprowadzania poszczególnych znaków hasła. Ta metoda autoryzacji nie jest najpopularniejsza i najwygodniejsza, a jednocześnie zapewnia wysoki poziom bezpieczeństwa i jest stosowana głównie w aplikacjach bankowych. Ta metoda jest bardzo dobra do badań ze względu na łatwość rozwoju i wysoki poziom bezpieczeństwa.

Odblokowanie za pomocą kodu QR wykorzystuje moduł kamery. Kamera jest skierowana na zakodowany obraz, a informacje zakodowane na obrazie są konwertowane przez urządzenie na dane cyfrowe. Ta metoda charakteryzuje się niskim poziomem bezpieczeństwa, ponieważ zakodowany obraz można sfotografować, a następnie wydrukować lub zapisać w pamięci innego urządzenia. Ta metoda nie nadaje się do autoryzacji i jest lepsza do udostępniania informacji w otwartej formie. Ta metoda nie nadaje się do badań ze względu na niskie bezpieczeństwo.

Aby odblokować za pomocą technologii NFC, należy użyć urządzenia, które odczytuje informacje oraz urządzenia, które przechowuje informacje. Urządzeniem przechowującym informacje może być telefon lub znacznik NFC. Zaletą tagów NFC jest to, że nie trzeba zużywać energii elektrycznej do interakcji z urządzeniami odczytującymi informacje. Metoda autoryzacji z wykorzystaniem technologii NFC jest świetna do badań, ponieważ hasło jest przechowywane w pamięci przenośnej i jest obowiązkowe, aby obsługiwać technologię NFC za pomocą urządzenia odczytującego informacje, co zapewnia dodatkowy poziom bezpieczeństwa.

Odblokowanie za pomocą wzoru jest zbiorem macierzą punktów. Przesuwanie palcem od punktu do punktu tworzy wzór, który tłumaczy się na obiekt. Cechy metody odblokowania z wzorem to szybkie wprowadzanie hasła i łatwość użycia. Podczas korzystania ze złożonej kombinacji hasło jest trudne do podejrzenia za pierwszym razem. Ponieważ metoda odblokowywania za pomocą hasła graficznego ma średni poziom bezpieczeństwa, wysoki poziom wygody i jest popularna wśród nowoczesnych metod odblokowywania, będzie stosowana w badaniach porównaniu z innymi wybranymi metodami autoryzacji. W rezultacie wybrano następujące metody autoryzacji:

1. Klasyczne hasło
2. Maskowane hasło
3. Autoryzacja za pomocą technologii NFC
4. Logowanie za pomocą wzoru

4. Środowisko testowe

Do przeprowadzenia testów używany jest telefon Motorola Droid Turbo XT1254 z systemem operacyjnym Android 6.0.1. Ta wersja dobrze nadaje się do testowania, ponieważ obsługuje aktualizację 28 wersji biblioteki SupportLibrary. Biblioteka SupportLibrary zawiera funkcje kolejnych systemów operacyjnych Android, częściowo zastępując potrzebę aktualizacji systemu operacyjnego urządzenia [15]. Zaletą tego modelu telefonu jest obsługa technologii NFC.

Jako przetestowane oprogramowanie stworzono aplikację mobilną dla systemu Android, począwszy od Android API 10. Aplikacja imituje działanie aplikacji bankowej, skupiając się na bezpieczeństwie i użyteczności oraz zawiera wszystkie zaimplementowane wybrane metody autoryzacji.

5. Procedura testowa

W testowaniu metod autoryzacji wzięło udział 9 osób. Podczas testowania dla każdej metody autoryzacji było zastosowano osobne hasło. Każdy użytkownik logował się co najmniej 10 razy w każdej z metod autoryzacji.

Każda próba autoryzacji obejmuje wejście do aplikacji i podanie odpowiedniego loginu. Po wprowadzeniu loginu i naciśnięciu przycisku potwierdzenia aplikacja komunikuje się z serwerem, skąd otrzymuje informacje o metodzie dołączonej do tego loginu. Jeśli w bazie danych nie ma takiego loginu, wyświetlane jest powiadomienie o braku użytkownika o tej nazwie. Następnie dane są wprowadzane zgodnie z wyświetlaną metodą, a login i hasło są sprawdzane na serwerze. Jeśli test się powiedzie, nastąpi przejście do nowego okna użytkownika. Jeśli test się nie powiedzie, zostanie wyświetlone powiadomienie z informacją, że weryfikacja nie została zakończona przy użyciu nazwy użytkownika i hasła.

Wygoda każdej metody autoryzacji została oceniona przez użytkowników na podstawie kryteriów szybkości autoryzacji, łatwości pracy z metodą autoryzacji i liczby udanych prób autoryzacji.

6. Analiza prezentowanych metod uwierzytelnienia

Analiza przedstawionych metod autoryzacji została przetestowana przez kilku użytkowników na tym samym urządzeniu. Przy każdej autoryzacji śledzono czas. Odwołanie do zapisu czasu rozpoczęło się natychmiast po przejściu do metody autoryzacji użytkownika docelowego. Koniec zliczania był wskazywany przez pomyślne zwrócenie odpowiedzi serwera do użytkownika. W wyniku praktycznych testów metod autoryzacji uzyskane wartości zostały wyświetlone w tabeli 1 i tabeli 2.

Tabela 1: Dane analityczne

	Minimalny czas autoryzacji [ms]	**Średni czas autoryzacji [ms]**	**Maksymalny czas autoryzacji [ms]**
Klasyczne hasło	5456	6804	8785
Autoryzacja przy użyciu technologii NFC	2017	3511	5575
Autoryzacja	1372	2746	3891

przy użyciu graficznego klucza			
Maskowane hasło	2746	10065	19715

Tabela 2: Dane statystyczne

	Liczba błędów podczas wprowadzania hasła [%]	**Łączna liczba prób logowania**	**Ocena użytkowników**
Klasyczne hasło	9	35	6/10
Autoryzacja przy użyciu technologii NFC	0	51	9/10
Autoryzacja przy użyciu graficznego klucza	7,6	64	8/10
Maskowane hasło	31,2	55	5/10

Warto zauważyć, że przy planowaniu autoryzacji nie zauważono skrócenia czasu autoryzacji. Wynika to z faktu, że użytkownik musi powtórzyć autoryzację setki razy, aby zmniejszyć szybkość korzystania z tej metody.

Klasyczne hasło w szybkości autoryzacji jest gorsze niż wszystkie metody autoryzacji, z wyjątkiem złożonego hasła. Czas potrzebny do autoryzacji wynosi od 5,5 do 8,5 sekundy. Użytkownicy logowali się średnio przez prawie 7 sekund. Jednocześnie trudno jest podejrzeć hasło, ponieważ nowowprowadzone znaki są wyświetlane przy wprowadzaniu tylko przez krótki czas. Ponadto znaki są natychmiast ukryte po wprowadzeniu nowego znaku. Z punktu widzenia wygody pozostaje zwykłą i najpopularniejszą metodą autoryzacji, ponieważ można ją łatwo wdrożyć w większości projektów. Wsparcie i rozwój nie wymagają dużego wysiłku ze strony programistów. Tej metody autoryzacji można łatwo wdrożyć w większości środowisk programistycznych. Błędy podczas wprowadzania hasła wynikały z natychmiastowego ukrycia poprzedniego znaku. Z drugiej strony takie podejście zwiększa bezpieczeństwo podczas korzystania z klasycznej metody wprowadzania hasła.

Korzystanie z metody autoryzacji z wykorzystaniem technologii NFC ma dodatkowe wymagania. Aby ta metoda działała, urządzenie musi obsługiwać technologię NFC. Przechowywanie klucza w pamięci zewnętrznej pozwala wydajniej i szybciej używać złożonych haseł, których nie trzeba zapamiętywać. Badanie wykazało, że metoda autoryzacji wykorzystująca technologię NFC zajmuje drugie miejsce pod względem szybkości autoryzacji. Czas autoryzacji przy użyciu technologii NFC trwał średnio 3,5 sekundy. A maksymalna i minimalna autoryzacja zajęła odpowiednio 5,5 i 2 sekundy. Ponadto ta metoda okazała się najbardziej skuteczna w obliczaniu liczby nieważnych autoryzacji. Ponieważ hasło znajduje się na oddzielnym urządzeniu, użytkownik musi tylko podnieść telefon do urządzenia, na którym hasło jest przechowywane. Użytkownicy docenili wygodę autoryzacji przy użyciu technologii NFC.

Autoryzacja za pomocą wzoru wzbudziła największe zainteresowanie użytkowników, ponieważ jest ona najbardziej znana dzięki możliwości odblokowania ekranu w ten sam sposób. Wyróżniającymi pozytywnymi cechami metody autoryzacji przy użyciu klucza graficznego są łatwość i szybkość użytkowania. Szybkość odblokowania pokazała najlepsze wyniki ze wszystkich badanych metod autoryzacji. Średni czas autoryzacji nie przekraczał 3 sekund, a minimalny i maksymalny czas autoryzacji trwał odpowiednio 1,3 i 3,8 sekundy. Jednocześnie ta metoda ma największą szansę na podejrzenie klucza. Pomimo łatwości i szybkości metody autoryzacji za pomocą hasła graficznego, nie jest zalecane korzystanie z tej metody w celu ochrony ważnych informacji.

Metoda autoryzacji wykorzystująca maskowane hasło znajduje się obecnie tylko w bardzo bezpiecznych systemach, na przykład w systemach bankowych. Ta metoda pokazuje najlepsze wyniki bezpieczeństwa. Nawet jeśli wprowadzono litery hasła jeden raz, niektóre z nich nadal będą nieznane. Badanie metody autoryzacji za pomocą złożonego hasła wykazało, że stosowanie tej metody potrzebuje największej ilości czasu od wszystkich przedstawionych metod autoryzacji. Maksymalny czas autoryzacji wynosił prawie 20 sekund. Najszybsza autoryzacja zajęła 3 sekundy. A średni czas autoryzacji wynosił 10 sekund. Zaleca się stosowanie go w celu zapewnienia maksymalnej ochrony danych lub autoryzacji, co nie musi być wykonywane zbyt często. Użytkownicy ocenili tą metodę jako raczej niski wynik z powodu trudności z wprowadzeniem hasła i ilości czasu spędzonego na wprowadzaniu hasła. Chociaż ta metoda nie jest najbardziej rozpoznawalna wśród użytkowników, jest najbezpieczniejsza ze wszystkich badanych metod w tym artykule.

7. Wnioski

Autoryzacja za pomocą NFC ma wiele zalet i kilka wad. Atutami tej technologii są szybkość, dokładność i mnogość zastosowań. Ze słabości można zauważyć, że technologia nie jest nowa i dla programistów nie została jeszcze szybko opanowana. Technologia NFC może również utrudniać niektóre niuanse bezpieczeństwa. Jednocześnie technologia NFC aktywnie się rozwija i zyskuje na popularności. Technologia jest bardziej odpowiednia do autoryzacji w aplikacjach. Podczas praktycznej analizy podanych metod wykazano, że każda z prezentowanych metod ma swoje zalety i wady, które czynią te technologie wyjątkowymi.

Przy odpowiedzialnym podejściu można stworzyć doskonały klucz ze zwykłego tagu NFC. Dane tego klucza będą trudne do przechwycenia, zastąpienia lub uszkodzenia. Potwierdzają to artykuły i patenty omówione w podanym artykule.

Badanie wykazało zalety technologii NFC tylko w odniesieniu do technologii uwierzytelnienia. W rzeczywistości technologia NFC ma wiele sposobów użycia w innych obszarach, takich jak autoryzacja w systemach różnych aplikacji, płatności zbliżeniowe, transfer danych między urządzeniami i inne. Wszystkie powyższe sposoby użycia są również uzupełnione o dodatkowy poziom bezpieczeństwa.

Literatura

[1] www.androidauthority.com/what-is-nfc-270730/ [30.06.2019]

[2] www.arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/oggle.it [01.03.2018]

[3] www.medium.com/@ssaurel/create-a-nfc-reader-application-for-android-74cf24f38a6f74cf24f38a6f&usg=AOvVaw00OJumUuBVTM1fhpfM6Rk0 [09.11.2017]

[4] www.patents.google.com/patent/US8831514B2/en [09.09.2014]

[5] www.patents.google.com/patent/US20140266624A1/en [18.09.2014]

[6] www.ieeexplore.ieee.org/abstract/document/6449282 [04.02.2013]

[7] www.ieeexplore.ieee.org/abstract/document/6470914 [11.03.2013]

[8] www.patents.google.com/patent/US9276643B2/en [01.03.2016]

[9] www.www.sciencedirect.com/science/article/pii/S0167923613002509 [01.03.2014]

[10] www.patents.google.com/patent/US8478196B1/en [02.07.2013]

[11] www.ieeexplore.ieee.org/abstract/document/7568941 [15.09.2016]

[12] www.ieeexplore.ieee.org/abstract/document/7153937 [13.07.2015]

[13] www.ieeexplore.ieee.org/abstract/document/6698315 [06.01.2014]

[14] www.ieeexplore.ieee.org/abstract/document/6578295 [16.08.2013]

[15] www.medium.com/google-developer-experts/exploring-the-v28-android-design-support-library-2c96c6031ae8 [19.03.2018]