AUTHENTICATION USING MOBILE PHONES

Zdeněk Fusek
Master Degree Programme (2), FEEC BUT
E-mail: xfusek07@email.feec.vutbr.cz

Supervised by: Jan Hajný
E-mail: hajny@feec.vutbr.cz

Abstract: This project deals with authentication by a mobile device. The mobile device with the operating system Android 5.0 was chosen as authentication device. The user can perform authentication with emulation of contactless chip cards by using Host-based Card Emulation, which runs via Near Field Communication, where cryptographic keys are stored in a secure environment KeyStore. The project continues with implementation of authentication via Bluetooth LE and describes application for authentization by using the protocol HM14.

Keywords: Authentication, NFC, Bluetooth LE, HM14, Host-based Card Emulation, Android, Contactless chip cards emulation

1 ÚVOD

Předložená práce je zaměřena na autentizaci s pomocí mobilního zařízení, jenž pracuje na operačním systému Android verze 4.4 a vyšší. Autentizace je provedena prostřednictvím Bluetooth Low Energy (BLE) a Near Field Communication (NFC) technologie. Obě tyto autentizační metody jsou zabezpečeny pomocí kryptografického protokolu HM14.

Ve výsledné aplikaci bude možné ověřit uživatelovu identitu jak pomocí BLE, tak i pomocí NFC. V praxi by tato aplikace mohla najít využití například při odemykání dveří, přičemž NFC by bylo využito v bezprostřední blízkosti a BLE v dosahu několika metrů.

2 AUTENTIZACE POMOCÍ NFC

NFC lze využít k celé řadě funkcí, v současnosti je tato technologie nejčastěji využívána pro bezkontaktní platbu v obchodech. Využití ale najde například v dopravě - zaplacení parkovného, jako náhrada klíčů, i jako nástroj obchodníků při tvorbě reklamy.

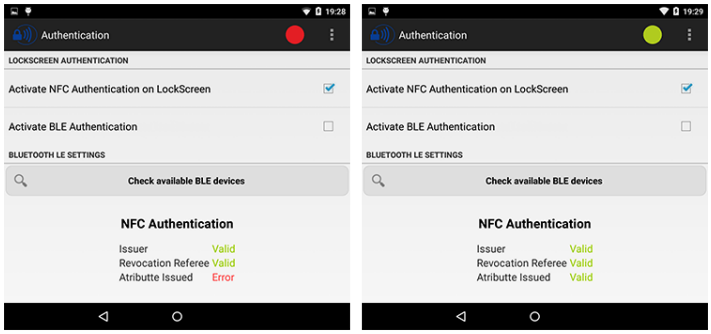
Mnoho zařízení s operačním systémem Android, které nabízejí NFC funkcionalitu, již podporují emulaci NFC karty. V mnoha případech je karta emulována samostatným čipem umístěným v zařízení tzv. bezpečnostním prvkem [1].

Android 4.4 přináší další způsob emulace karty bez bezpečnostního prvku tzv. Host-based Card Emulation. HCE umožňuje jakékoliv Android aplikaci emulovat kartu a komunikovat přímo s NFC čtečkou [1].

2.1 ZÁKLADNÍ KONCEPT NFC

Pro autentizaci pomocí NFC je nutné, aby tato funkce byla v aplikaci aktivní, přičemž mobilní zařízení musí být následně uzamknuto, ale zároveň nesmí být v režimu spánku. Po uzamčení mobilního zařízení přiložíme autentizační zařízení k NFC čtečce, ta ověří autentizační data, a na základě tohoto ověření umožní uživateli přístup či jej zamítne. Stav autentizace se poté zobrazí na ploše zařízení, a to

ve vrchním menu, kde je vyobrazena ikona indikující stav autentizace. V případě úspěšné autentizace je zobrazena ikona se zelenou výplní, v případě zamítnutí ikona zůstává nadále červená. Na obrázku 1 vlevo je znázorněna neúspěšná autentizace pomocí NFC, zatímco vpravo je autentizace úspěšná.



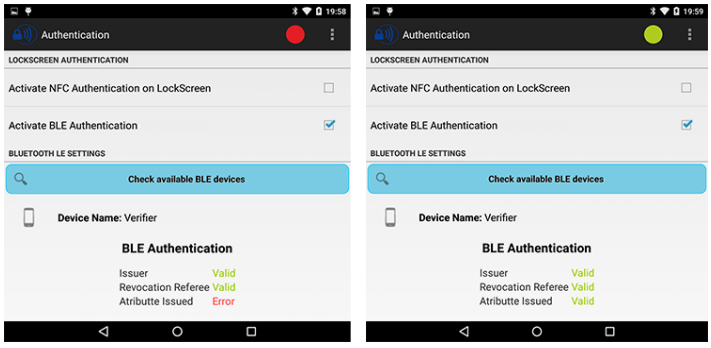
Obrázek 1: Autentizace pomocí NFC

3 AUTENTIZACE POMOCÍ BLE

Nízko energetický Bluetooth je zabudován na všech zařízeních s podporou operačního systému Android počínaje verzí 4.3. Bluetooth Low Energy (BLE, uvedený na trh jako Bluetooth Smart), se stal součástí specifikace jádra pro Bluetooth 4.0. BLE je optimalizováno pro nízkou cenu, malou šířkou pásma, nízkou spotřebu a uživatelskou i komunikační jednoduchost [2].

3.1 ZÁKLADNÍ KONCEPT BLE

Po odemknutí mobilního zařízení a spuštění aplikace je nutné ověřit, zda je autentizace pomocí BLE aktivní. Po aktivaci si uživatel vyhledá, zda se v dosahu jeho zařízení vyskytuje ověřovatel (BLE čtecí zařízení). Všechna dostupná BLE čtecí zařízení jsou zobrazena v seznamu, z něhož si uživatel vybere to zařízení, u kterého provede autentizaci. Jednotlivé kroky s výsledky autentizace jsou poté zobrazeny v aplikaci na ploše zařízení. Na obrázku 2 vlevo je znázorněna neúspěšná autentizace pomocí BLE, vpravo je autentizace provedena úspěšně.



Obrázek 2: Autentizace pomocí BLE

4 BEZPEČNOSTNÍ ANALÝZA

4.1 BEZPEČNOST DAT

Data potřebná pro autentizaci uživatele jsou uložena v zabezpečeném prostředí Android KeyStore a chráněna pomocí AES šifrování, přičemž klíč AES šifry je chráněn RSA šifrou. Data protokolů jsou tedy zabezpečena, pokud nedojde k odcizení, či získání root oprávnění škodlivou aplikací.

4.2 DEKOMPILACE APLIKACE A MOŽNOST ZNEUŽITÍ KÓDU

K dekompilaci aplikace by mohlo dojít při odcizení přístroje, nebo pokud by útočník (škodlivá aplikace) získal root oprávnění. Toto oprávnění může škodlivá aplikace získat od uživatele (v případě, že se například vydává za jinou aplikaci), nebo pokud aplikace hledá chyby v systému a využívá je k jeho získání. Tento postup ale není příliš používaný. Při následné dekompilaci by byly odhaleny veškeré zdrojové kódy, a útočník by tak mohl získat tajné klíče.

4.3 BEZPEČNOST BĚHEM AUTENTIZACE

V případě NFC technologie je zde další bezpečnostní hrozba. Při autentizaci je aplikace spuštěna nad úrovní zamykací obrazovky, a hrozí zde tedy reálné nebezpečí zneužití při odcizení přístroje. U BLE technologie je tato hrozba zmírněna tím, že autentizace probíhá pod úrovní zamykací obrazovky.

5 PROTOKOL HM14

Jedná se o protokol, který se zabývá autentizací a řízením přístupu. Slouží k prokázání, že uživatel je vlastníkem daného atributu, aniž by došlo ke sdělení dalších atributů ověřovateli. Atributy mohou být například věk, národnost či zaplacení jízdného. Protokol dále umožňuje identifikaci škodlivých uživatelů a to i přesto, že ověřování atributů je anonymní [3].

Protokol HM14 se skládá ze čtyř entit: vydavatele, ověřovatele, uživatele a odvolávatele. Vydavatelova role spočívá ve vydávání atributů uživateli, přičemž vydavatel jako jediný zná uživatelovy údaje. Ověřovatel ověřuje uživatelovo vlastnictví atributu a eviduje každé ověření. V případě porušení pravidel může ověřovatel požádat odvolavatele o zrušení relace. Uživatel je držitelem čipové karty s vydanými atributy, a je schopen anonymně prokázat vlastnictví čipové karty. Odvolavatel zajišťuje záruku ochrany osobních údajů, protože rozhoduje o typu zrušení na základě informací poskytnutých ověřovatelem [3].

6 ZÁVĚR

Tento projekt představil implementaci přístupového systému využívající mobilní zařízení s operačním systémem Android jako autentizační zařízení. K přenosu dat mezi telefonem a čtecím zařízením bylo využito rozhraní NFC a BLE. Autentizace pomocí NFC byla navržena pro ověření identity uživatele bez použití bezpečnostního prvku, a tudíž je potřeba, aby na zařízení byla verze OS Android 4.4 a vyšší. U autentizace pomocí BLE musí čtecí zařízení podporovat periferní mód, tj. odesílání beaconů. Výsledná aplikace tedy umožňuje provedení autentizace jak pomocí NFC, tak i pomocí Bluetooth Low Energy.

REFERENCE

[1] Host-based Card Emulation. In: *Developers* [online]. © 2014 [cit. 1. 3. 2015]. Dostupné z: <https://developer.android.com/guide/topics/connectivity/nfc/hce.html >.

[2] TOWNSEND, Kevin, Carles CUFI a Robert DAVIDSON. *Getting started with bluetooth low energy: tools and techniques for low-power networking*. První vydání. S.l.: O'Reilly Media, Inc, Usa, 2014. ISBN 978-149-1949-511.

[3] HAJNÝ, Jan; MALINA, Lukáš. *Unlinkable Attribute-Based Credentials with Practical Revocation on Smart- Cards*. In *Smart Card Research and Advanced Applications*. Lecture Notes in Computer Science. LNCS. Berlin: Springer, 2013. s. 62-76. ISBN: 978-3-642-37287- 2. ISSN: 0302- 9743.