QR-KEY

Pavel Fojtík

High School Student (4), Purkyně Grammar School, Strážnice

E-mail: pavelfojtik@gmail.com

Supervised by: Oldřich Vyoral

E-mail: vyoral@gys.cz

Abstract: By using system developed within this project, we will make whole process of basic authentication safer, using active and computationally powerful device. It also has benefits for users. They don't need to carry superfluous utilities anymore. We replace them with object of everyday use - mobile phone, precisely smartphone with OS Android. For very own realization we have chosen to utilize benefits of QR codes, which are currently very often used and whose importance significantly grows. Those codes provide user-friendly access to system even with use of cryptographically strong, safe authentication protocols.

Keywords: QR code, cryptography, Android, smartphone, safety systems

1. ÚVOD

Práce se zabývá vývojem zabezpečovacího systému použitelného například v podobě elektronického vrátného. Byl tedy kladen důraz na systémy, které autentizují a autorizují subjekty na základě vlastnictví nějakého předmětu (klíče). Cílem práce pak bylo vytvoření a názorné předvedení nově navrženého systému, a jeho porovnání s dosavadními systémy.

Za pomocí nových poznatků v oblasti moderní kryptografie a znalostí programovacího jazyka Java byly tedy navrhnuty a vytvořeny funkční a použitelné programy, který slouží jako zabezpečovací systém. Díky užití transparentního způsobu je celý proces velmi názorný a snadno pochopitelný. Práce má sloužit taktéž k edukativním účelům, byl tedy kladen důraz na co nejvyšší míru transparentnosti. V praxi pak bylo uvažováno o použití mírně odlišných metod, založených na NFC technologii.

2. ZÁKLADNÍ STRUKTURA SYSTÉMU

Vše se zakládá na naprosto jednoduché myšlence. Uživatel se autentizuje pomocí klientské aplikace. Tedy potvrdí, že je skutečně ten, za koho se vydává. Serverová aplikace následně vyhodnocuje, zda má daný uživatel příslušná práva (vstup do budovy, přístup ke střeženým datům). Pokud serverová aplikace vyhodnotí, že uživatel se prokázal správným autentizačním klíčem a současně má práva přístupu tam, kam žádá, bude následně autorizován, čímž dojde například k otevření dveří, či zpřístupnění databáze údajů.

3. FAST MODE

Jak již z názvu vypovídá, jedná se o model autentizace, který zajišťuje minimální zabezpečení, ale vysokou rychlost a snadnou opakovatelnost autentizace. Byl zde tedy implementován jednoduší systém autentizace, který se běžně používá například v bezkontaktních čipech a kartách. Tento systém zajišťuje malou bezpečnost, disponuje snadnou prolomitelností a minimální obranou proti odcizení přístupového klíče.

Zvolený protokol obsahuje jednoduchou (jednoúrovňovou) výzvu (Challenge) v podobě přiložení zařízení a očekává odpověď (Response) v podobě statického, stálého (neměnného a nezávislého) hexadecimálního 32místného řetězce. Samotné předání tohoto řetězce asi nejlépe zprostředkuje technologie NFC, ovšem pro potřeby této práce bylo využito potenciálu QR kódů.

Po přijetí příslušného klíče provádí serverová část vyhodnocování a testování klíče a následné přiřazení klíče k danému uživateli vedeného v databázi na základě otisku jeho hesla a předem určených početních úkonů a využití soil (viz…)

Výhodou tohoto systému je především rychlost a systém při dané konfiguraci dokonce umožňuje, aby jedno ze zařízení bylo zcela pasivní (např. vytištěný QR Code).

4. SAFE MODE

V tomto modelu již bylo použito složitého procesu autentizace, který využívá silného výpočetního výkonu použitých zařízení. Zajišťuje běžnými metodami v reálném časem neprolomitelnou obranu, a to proti všem známým typům útoků. V případě správného a bezpečného užívání zařízení i vysokou odolnost proti případům odcizení. Hlavní výhodou tohoto systému je znemožnění výroby kopií přístupového klíče.

Implementovaný protokol zahrnuje víceúrovňový Challange. Je potřeba, aby zařízení byla plně aktivní a disponovala určitým výpočetním výkonem. V prvním kroku serverová část předá uživatelské části subnáhodně generovanou hodnotu v hexadecimálním tvaru předepsaných náležitostí. Následně dojde ke zpracování uživatelskou částí, zakomponování tohoto subnáhodného řetězce do výpočtů a k vygenerování autentizačního řetězce, který je na další výzvu předán serverové části. Ta pak následně provede vyhodnocení přístupových práv obdobným způsobem jako u fast mode.

Nespornou výhodou tohoto systému je velmi vysoká úroveň zabezpečení a přitom zachování etiky autentizace, u které díky silným výpočtům není potřeba snímání otisků prstů či jiných biometrických údajů.

5. GENEROVÁNÍ QR KÓDU

Pro generování QR kódu bylo použito vlastností knihovny zXing . Hlavní metodu pro využití této knihovny máte na následujícím obrázku.

```
43  public void genQRcode (){
44      Bitmap bmp;
45      int bitmapWidth = 300;
46      int bitmapHeight = 300;
47
48      String context;
49      String userid;
50      String username;
51      String userpassword;
52      String usernamefilename;
53      String userpasswordfilename;
54      String md5fmchash;
55
56      usernamefilename="jmeno";
57      username =readFromFile(usernamefilename);
58      userpasswordfilename="heslo";
59      userpassword=readFromFile(userpasswordfilename);
60      md5fmchash=ziskejMd5Hash(username+userpassword);
61      userid=getUserId(username);
62
63      context="IDFMC"+userid+md5fmchash;
64      writeToFile(md5fmchash, "authstring");
65      writeToFile(context,"qrstring");
66
67
68      String data=context;
69
70      com.google.zxing.Writer writer = new QRCodeWriter();
71      String finaldata = Uri.encode(data, "UTF-8");
```

```
72
73          BitMatrix bm;
74          try {
75              bm = writer.encode(finaldata, BarcodeFormat.QR_CODE, bitmapWidth,bitmapHeight);
76                      bmp= Bitmap.createBitmap(bitmapWidth, bitmapHeight,Config.ARGB_8888);
77
ent         for (int i = 0; i < bitmapWidth; i++) {
79              for (int j = 0; j < bitmapHeight; j++) {
80                  bmp.setPixel(i, j, bm.get(i, j) ? Color.BLACK: Color.WHITE);
81              }
82          }
83          iv.setImageBitmap(bmp);
84          } catch (WriterException e) {
85              // TODO Auto-generated catch block
86              e.printStackTrace();
87          }
88
89
90
91  }
```

6. ZÁVĚR

Navrhl jsem a vytvořil funkční program, který lze použít jako zabezpečovací systém a který, po několika málo dodatečných úpravách, může být uveden na trh, kde si jistě vydobude místo mezi svými konkurenty, pro něž bude více než zdatným soupeřem.

V aplikaci jsem vytvořil celkem dva módy umožňující autentizaci. Jedním z nich je rychlé ověření, které jak již je z názvu patrné, funguje velmi rychle, ovšem za cenu ztráty téměř veškeré bezpečnosti. Naproti tomu ověření bezpečné přidává jeden nutný krok autentizace navíc, který ale celé zabezpečení posouvá na novou úroveň. Díky tomuto rozdělení se stává z mého programu nástroj, kterým můžu upozornit na ne-úplně ideální stávající zabezpečení, a zároveň nastiňuji způsob, jakým lze některá bezpečnostní rizika minimalizovat, či dokonce odstranit.

Nabízí se tu i možnost modifikace a přizpůsobení programu. V současnosti je systém navržen tak, že klientská část je spuštěna na mobilních zařízeních s OS Android, serverová část pak potřebuje pro svůj běh jednu z Linuxových distribucí. Systém je navržen tak, že umožní komunikaci i se serverem, který běží taktéž na zařízení s OS Android.

Z celkového hlediska musím hodnotit celý tento projekt jako úspěšný. Nabyl jsem mnoho nových poznatků o oblasti, která je centrem mého zájmu a věřím v jejich budoucí využití. Celá práce má tedy přínos především pro mne jako studenta, který rozvinul své znalosti, ale také pro širokou veřejnost, která tento program bude moct využívat, ale především pro studenty kterým tato práce dokáže přiblížit fungování bezpečnostních systémů.

REFERENCE

[1] UJBÁNYAI, Miroslav. *Programujeme pro Android*. Vyd. 1. Praha: Grada, 2012, 187 s. Průvodce (Grada). ISBN 978-80-247-3995-3.

[2] PIPER, F a Sean MURPHY. *Kryptografie*. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.