Sigurnosni aspekti mobilnih bankovnih aplikacija

Benić, Igor

Undergraduate thesis / Završni rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:848930

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Image not found or type unknown

Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula

zir.nsk.hr

Image not found or type unknown

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

IGOR BENIĆ

SIGURNOSNI ASPEKTI MOBILNIH BANKOVNIH APLIKACIJA

Završni rad

Pula, 2015.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

IGOR BENIĆ

SIGURNOSNI ASPEKTI MOBILNIH BANKOVNIH APLIKACIJA

Završni rad

JMBAG: 0246043151,redoviti student

Studijski smjer: Informatika

Predmet: Elektroničko poslovanje

Mentor: Prof. dr. sc. Vanja Bevanda

Pula, kolovoz 2015.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student:

U Puli, 17. 09. 2015. _____

SADRŽAJ

UVOD **1**

1. DEFINICIJA MOBILNOG BANKARSTVA **2**

1.1 PRIMJER APLIKACIJE - M-ZABA 3

1.2 EKOSUSTAV MOBILNE BANKOVNE APLIKACIJE 5

2. SIGURNOSNI ASPEKTI I NAPOMENE KORISNICIMA **7**

3. TEHNOLOGIJE MOBILNIH BANKOVNIH APLIKACIJA **9**

3.1 MREŽNE TEHNOLOGIJE 9

3.2 PROTOKOLI 10

3.3 NEAR FIELD COMMUNICATIONS PLAĆANJE 11

3.4 SECURE ELEMENT 12

3.5 TRUSTED SERVICE MANAGER 12

3.6 WEBROOT ALAT 14

3.7 HARDVERSKA VIRTUALIZACIJA 14

4. ZAŠTITA PRISTUPA **16**

4.1 SMS VIŠE-FAKTORSKA AUTENTIKACIJA 16

4.2 BIOMETRIČKA AUTENTIKACIJA 17

4.3 SANDBOX METODA 17

5. GLAVNI RIZICI **19**

5.1 MALWARE 20

5.2 ROOT I JAILBREAK 21

5.3 RELAY NAPAD 22

5.4 MAN IN THE MIDDLE NAPADI 23

5.5 PHISHING NAPAD 24

5.6 KRAJNJI RAZVOJ APLIKACIJE 24

6. ZAKLJUČAK **26**

7. LITERATURA **27**

Uvod

Bankarske usluge, kao i mnoge druge pogodnosti današnjeg doba, oslanjaju se na informacijske i komunikacijske tehnologije. Otkad su bankarske usluge zaživjele na web sjedištima interneta, pojavljivali su se problemi povezani sa sigurnošću ove usluge koja ovisi o iznimno osjetljivim korisničkim podacima. Od potrebe za povećanjem sigurnosti vlastite infrastrukture pa sve do povećanja sigurnosti samih korisnika, sva komunikacija, poslovanje i korištenje bankarskih usluga zahtijevaju iznimno visoke razine sigurnosti ukoliko će infrastruktura biti stabilna na strani korisnika, banke pa i između banke i korisnika dok su informacije u tranzitu. Najnoviji pothvati u bankarstvu usmjereni su prema mobilnih platformama i samim time donekle se mijenjaju i sigurnosni zahtjevi obzirom na promjene okružja u kojem se zatražuju i provode bankarske usluge. Mobilni uređaji, njihovi operacijski sustavi i hardver i periferija predstavljaju potpuno novi ekosistem koji zahtjeva nove pristupe sigurnosti i razvoju aplikacija. Po nastanku mobilnog bankarstva ubrzo su se pojavile i maliciozne aplikacije sa namjerom eksploatacije ovog sustava i njegovih sigurnosnih propusta. Budući da je teško napraviti onoliki broj sigurnosnih testiranja nad cijelim ekosustavom u kojem se nalazi mobilna aplikacija zlonamjerni napadači uvijek imaju prostora za kreativnost u pogledu iskorištavanja te činjenice u svoju korist. U namjeri da se sigurnosni propusti aplikacije, operacijskog sustava i komunikacijskih kanala kojima se aplikacija služi ne ponove potrebno je preispitati sigurnosne aspekte mobilnih aplikacija i ustanoviti trenutno stanje sigurnosti i rješenja na postojeće probleme. Neke probleme rješavaju i kompanije zadužene za održavanje mobilnih operacijskih sustava, ostale probleme rješavaju kompanije čije periferne i hardverske jedinice koriste mobilni uređaji te je u svemu tome jedna bankovna aplikacija ovisna o mnogo vanjskih faktora. U ovom radu govoriti će se o sigurnosnim aspektima mobilnih bankovnih aplikacija na način da će se analizirati općeniti pristup rješavanju sigurnosnih problema iz više pogleda, od mana i vrlina sigurnosnih značajki operacijskog sustava na kojem se aplikacija nalazi do potencijalnih napada zlonamjernih aplikacija te kako i zašto korisnike upozoriti na rizike neopreznog korištenja mobilnog uređaja pri instalaciji nepoznatih aplikacija i sa nepoznatih izvora pa sve do sigurnosnih mjera kojih se potrebno držati i kakve je komunikacijske kanale poželjno koristiti prilikom provođenja transakcija i razgovora sa korisnikom kako bi se sačuvao integritet aplikacije, poslužitelja i svih stranaka koje su potrebne za ostvarivanje bankovnih usluga jedne bankovne mobilne aplikacije.

1. Definicija mobilnog bankarstva

Zbog ubrzanog napretka tehnološkog i telekomunikacijskog aspekta aplikacija općenito, samim time i mobilnih financijskih aplikacija, potrebno je ustanoviti o kojem obliku mobilnog bankarstvu će se govoriti u ovom radu te na koji će se način pristupiti rješavanju problema mobilne sigurnost. Jedna od definicija mobilnog bankarstva jest da je to korištenje bankovne mobilne aplikacije u svrhu pristupa informacijama i funkcijama koje nam banka pruža što može uključivati transfer i plaćanje (Khosrow-Pour, 2013: 227), za razliku od mobilnog plaćanja koje uključuje povezivanje kartica sa mobilnim uređajem kako bi mogli plaćati mobilnim uređajem koristeći primjerice Near Field Communications(NFC) tehnologiju, u kojem se slučaju plaćanje izvršava preko mreže i POS sistema prodavača ne oslanjajući se na mrežu i mobilni uređaj kupca osim za slanje potrebnih podataka uređaju za procesiranje plaćanja koristeći NFC tehnologiju.(Pegueros, 2012: 3)

Vanessa Pegueros(2012: 3) također navodi kako se mobilno bankarstvo može podijeliti na tri glavna područja: informacijsko, transakcijsko i servis, marketing i akvizicija. Informacijsko područje podrazumijeva korištenje mobilne bankovne aplikacije za transfer novaca između računa, plaćanje računa, uplate fizičkim ili pravnim osobama na račun i korištenje digitalnih fotografija kao dokaz o plaćanju čekova ili računa. Servisi predstavljaju funkcije koje poboljšavaju korisničko iskustvo, kao što su opcije za kontakt, podrška i obavijesti. Dodatni servisi uključuju obavijesti o obnovi usluge, obavijesti koje se okidaju po određenim promjenama na korisničkim računima i lokacijski ovisne opcije primjerice za putno osiguranje. Vezano uz marketing i akviziciju, postoje servisi poput kupona/poticaja, barkodova, informacija o novim proizvodima, istraživanje o korisnicima te prodaja dodatnih artikala i akvizicija.

U ovom radu osvrnuti će se na sigurnost mobilnih bankovnih aplikacija prema definiciji Khosrow-Pour-a uzimajući u obzir informacijsko područje mobilnog bankarstva prema Pegueros, što znači da je mobilna bankovna aplikacija sredstvo kojim imamo direktan uvid u stanje svojih bankovnih računa, ponuđene su nam funkcije bankovnog poslovanja kao što su transakcije(uključujući i mogućnost korištenja NFC tehnologija za plaćanje), povijest transakcija, plaćanje računa, plaćanje drugoj osobi, prenošenje novaca između vlastitih računa i tome slične funkcije jedne mobilne bankovne aplikacije.

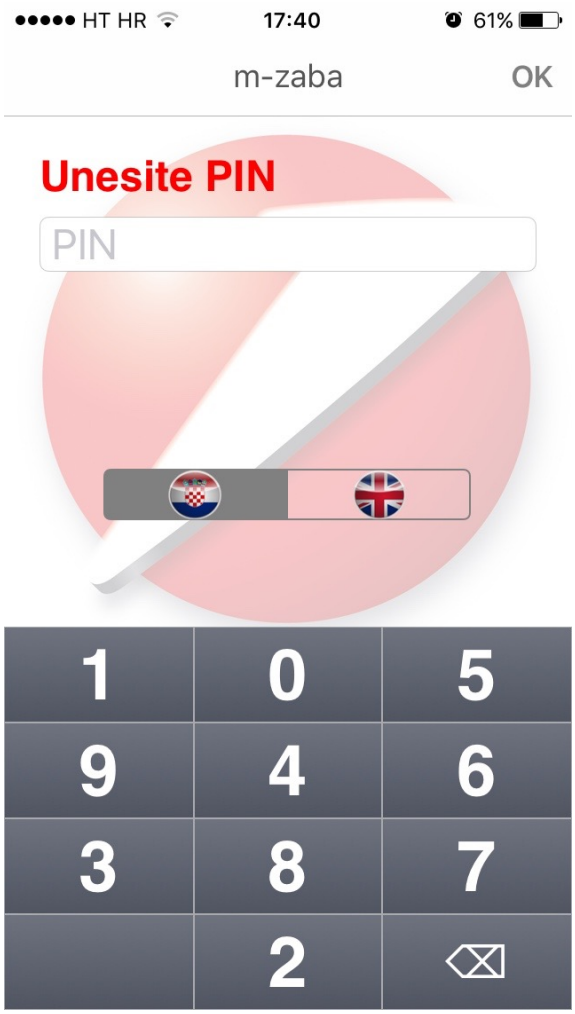
1.1 Primjer aplikacije - m-zaba

Za primjer mobilne bankovne aplikacije koristiti će se m-zaba mobilna bankovna aplikacija Zagrebačke banke(Zaba). Zaba svojim korisnicima na službenim web stranicama preporuča i navodi sljedeće sigurnosne aspekte mobilne aplikacije(Zaba, 2014: 4):

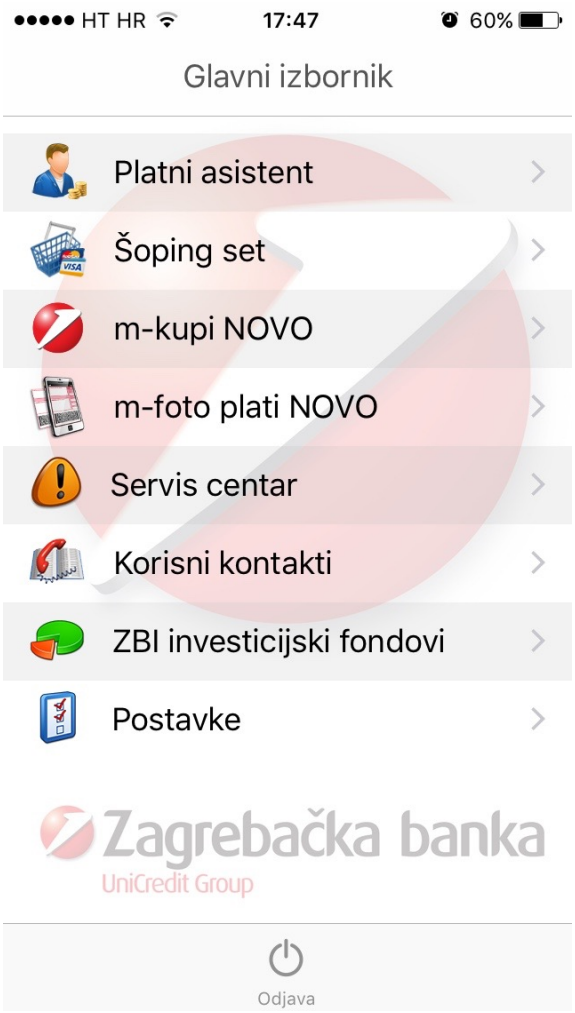
- Automatski se gasi nakon tri minute ako se ne koristi
- Automatski se zaključava nakon višestrukog unosa pogrešnog PIN-a
- Preuzimanjem m-zabe u mobitel instalira se softverski token koji jamči potpunu sigurnost rada
- Podaci u vezi s računima i PIN-om ne čuvaju se u mobitelu

Za korištenje m-zaba mobilne bankovne aplikacije potrebno je u banci ili na web sjedištu Zagrebačke banke(e-zaba) "ugovaranje" m-zabe. Prilikom ugovaranja unose se potrebni detalji o mobilnom uređaju kao što je model, broj telefona i operativni sustav uređaja koji će koristiti m-zaba aplikaciju te se na isti dostavlja SMS poruka sa linkom za preuzimanje aplikacije na uređaj. Nakon preuzimanja aplikacije potrebno je u aplikaciju unijeti identifikacijski i aktivacijski ključ koji se kod ugovaranja može naći na e-zabi nakon čega se odabire PIN koji će se koristiti prilikom prijave u aplikaciju kao što se može vidjeti na slici 1. PIN je jedini oblik zaštite od strane korisnika, te po unosu PIN-a korisnik ima potpuni pristup svim korisničkim dijelovima aplikacije, odnosno svemu što aplikacija pruža, što znači da je po unosu točnog PIN-a moguće obavljati transakcije, uplate i plaćanja bez dodatnih provjera identiteta korisnika. Kao što se može vidjeti na slici 1, kod prijave numerička tipkovnica za unos PIN-a nasumično raspoređuje tipke, čime se nastoji smanjiti rizik čitanja PIN-a od strane ostalih osoba u blizini korisnika. Ova zaštita, zaključavanje aplikacije nakon određenog vremena nekorištenja i zaključavanje aplikacije nakon višestrukog unosa pogrešnog PIN-a jedina su zaštita od neovlaštenog fizičkog pristupa u aplikaciju što može biti mana sa sigurnosne strane aplikacije.

Prilikom testiranja aplikacije također je pronađen sigurnosni propust aplikacije u procesu prijave, odnosno unosa PIN-a, te je moguće aplikaciji pristupiti bez obzira na vrijeme neaktivnosti aplikacije uz uvjet da je točan PIN unesen u polje. Nakon vremena neaktivnosti dužeg od naznačenog kao potrebnog za zaključavanje aplikacije, aplikacija je ponovno pokrenuta te je PIN unos naočigled uklonjen, ali se PIN ispunjava po unosu nasumičnog broja u PIN polje, brisanjem zadnjeg unosa koji je upisan samo kako bi se PIN polje ispunilo prijašnjim unosom, odnosno točnim PIN-om, PIN prolazi te je moguće aplikaciju koristiti u potpunosti. Ovaj sigurnosni propust predstavlja rizik koji u potpunosti zaobilazi sigurnosne



Slika 1 Unos PIN-a u m-zaba aplikaciji



Slika 2 Glavni izbornik m-zaba aplikacije

mjere nasumične tipkovnice i zaključavanja aplikacije nakon određenog vremena neaktivnosti, te izlaže riziku mobilnu bankovnu aplikaciju bilo kojoj osobi koja koristi mobilni uređaj nakon što korisnik unese PIN u mobilnu bankovnu aplikaciju. Iako vrlo specifičan sigurnosni propust, ipak ostavlja prostora za eksploatiranje u zlonamjerne svrhe.

Osim osnovnih mogućnosti poput provjere stanja računa, provođenja i pregleda obavljenih i pristiglih transakcija moguće je također i plaćanje mobilnim uređajem uslugom m-kupi. Kao tehnologija za plaćanje koristi se barkod kojega se na mjestima koja podržavaju takav oblik plaćanja može pokazati te se skeniranjem tereti tekući račun korisnika. Za provođenje transakcije potrebna je veza na internet budući da je m-zaba bankovna aplikacija bazirana na web sučelju što znači da su sigurnosne značajke i mjere direktno povezane sa onima koje se pojavljuju kod e-zaba aplikacije na web sjedištu o čemu će se pored Near Field Communications(NFC) tehnologije za provođenje beskontaktnog mobilnog plaćanja, kao još jednog od oblika mobilnog plaćanja, više govoriti u nadolazećim poglavljima.

Jedna od bitnih sigurnosnih mjera mobilne bankovne aplikacije jest i dio aplikacije u kojem se navode korisni kontakti, odnosno službeni kontakti prema banci. Na ovaj način korisnik može biti siguran da ga kontaktira njegova banka, uz pretpostavku da službenici banke koriste isključivo službene puteve za komunikaciju sa korisnikom. Ovaj izbornik, korisni kontakti, kao što je vidljivo na slici 2, sadrži sve potrebne informacije za kontaktiranje banke, poput komunikacijskih kanala vezanih uz opće informacije, podrške vezane uz e-zaba i m-zaba servise, investiranje, osiguranje pa sve do prijave krađe ili gubitka i reklamacije kartica.

U glavnom izborniku se također može vidjeti i m-foto plati opciju koja omogućava plaćanje računa slikanjem istog te se dodatni potrebni detalji za plaćanje računa unose direktno u aplikaciju na način na koji bi se unosili i kod regularnog plaćanja računa putem mobilne aplikacije ili uplate na tuđi račun.

1.2 Ekosustav mobilne bankovne aplikacije

Okružje ili ekosustav mobilnih bankovnih aplikacija znatno se razlikuje od okružja aplikacija kojima sigurnost nije ili ne mora biti na prvom mjestu. Bankovna aplikacija podrazumijeva komunikaciju mobilne bankovne aplikacije korisnika i banke radi ostvarivanja mogućnosti koje aplikacija pruža. Ukoliko se radi i o aplikaciji koja pruža mobilno plaćanje, bilo to predstavljanjem barkoda ili pak NFC tehnologijom, potrebno je osigurati i komunikacijske tehnologije prema i od kupaca i prodavača i njihovih uređaja budući da se korisnikove podatke koristi za odobravanje provođenja transakcije. Potrebno je osigurati i komunikacijski kanal kojim podaci dospijevaju na internet, odnosno mobilni signal ili bežičnu konekciju. Također, same mobilne aplikacije nalaze se u ekosustavu vrlo različitih mobilnih uređaja govorimo li o Android operacijskom sustavu, što predstavlja mnoge različite hardverske pa čak i softverske pojedinosti između uređaja koje je potrebno podržavati sigurnosno i biti upoznat sa manama koje bi takva raznolikost mogla predstavljati. Kako bi se osigurala komunikacija i smanjila potreba za održavanjem aplikacije direktno na mobilnom uređaju korisnika, mobilne bankovne aplikacije koriste web sučelje za prikaz informacija, komunikaciju i rad aplikacije. Korisnikovoj se aplikaciji stoga ne vjeruje u potpunosti te je sigurnost aplikacije u rukama poslužitelja koji je na strani banke te mobilna bankovna aplikacija može biti i oblik tankog klijenta koji se koristi za unos korisničkih podataka za autentikaciju kod prijave u sustav bankovne aplikacije. Kao mjeru zaštite potrebno je koristiti sigurnosni element ili Secure Element(SE) mobilnog uređaja ukoliko postoji potreba za spremanjem osjetljivih korisničkih podataka na sam uređaj. U sigurnosni element potrebno je na prikladan način spremiti kriptografske ključeve koji će se koristiti prilikom komunikacije unutar

ekosustava mobilne bankovne aplikacije. Kako bi se smanjila potreba za osiguravanjem svakog komunikacijskog kanala između mnogo različitih sudionika u provođenju transakcija ili pak samo korištenja mobilne bankovne aplikacije za pregled korisničkih detalja u svrhu zaštite i povezivanja mobilnih bankovnih aplikacija i aplikacija za plaćanje koristi se Trusted Service Manager ili TSM. Uloga TSM-a jest sigurno povezivanje svih sudionika u komunikaciji prilikom plaćanja i korištenja mobilnih bankovnih aplikacija. TSM jest osnova provođenja transakcija i sigurnosti komunikacije mobilne bankovne aplikacije te će se o TSM uslugama i upravljanju aplikacijom i komunikacijom više govoriti u nastavku ovog rada.

2. Sigurnosni aspekti i napomene korisnicima

Kao što je slučaj kod nekih mobilnih bankovnih aplikacija, moguće je da sve osjetljive informacije, detalji o karticama i mogućnost provođenja transakcija stoje iza samo jednog PIN-a ili password-a kojega korisnik postavlja prilikom prvog postavljanja aplikacije. Ovakav pristup potencijalno predstavlja rizik budući da je za pristup svim korisničkim detaljima dovoljno fizički domoći se tuđeg mobilnog uređaja, posjedovati PIN za otključavanje samog uređaja i PIN ili password za pristup bankovnoj aplikaciji. Odgovori na ovakav napad nisu nužno samo rješenja bankovne aplikacije već je potrebna edukacija i upozorenje korisnicima. Za potrebe ovog rada analizirano je jedanaest mobilnih bankovnih aplikacija koje na području Hrvatske pružaju banke. Analizom banaka u Hrvatskoj koje pružaju uslugu mobilnog bankarstva na svojim web lokacijama navode slijedeće točke sigurnosti i tehnologije koje aplikacija koristi:

- Aplikacija se gasi nakon tri do pet minuta nekorištenja
- Prilikom pristupanja aplikaciji stvara se One Time Password(OTP) koji korisnik prima SMS porukom
- Nakon određenoj broja krivih unosa pristupnog PIN-a ili passworda aplikacija se zaključava te je za ponovnu aktivaciju potrebno podnošenje zahtjeva za distribuciju aplikacije putem web aplikacije banke
- Prilikom instalacije na mobilni uređaj automatski se instalira i softverski token
- Podaci vezani uz račune, transakcije, korisnika i pristupni PIN ili password ne spremaju se na mobilni uređaj
- Aplikacija je definirana sigurnosnim standardom 27001:2005
- Sva komunikacija između uređaja i Gateway aplikacijskog poslužitelja zaštićena je SSL/TLS kriptiranim protokolom
- Mobilna bankovna aplikacija vezana je za samo jedan uređaj

Ovi detalji o radu bankovne mobilne aplikacije, o kojima će se više govoriti u sljedećim poglavljima, govore nam kako rad aplikacije štiti korisnika i komunikaciju korisnika, banke i povezanih stranaka te kojim sigurnosnim tehnologijama i standardima to postižu. Banke također navode sljedeće napomene kako bi korisnik ostao siguran prilikom korištenja aplikacije pa i samog uređaja:

- Održavanje operativnog sustava pametnog telefona ažurnim
- Preuzimanje najnovije verzije bankovne mobilne aplikacije

- Zaštititi uređaj PIN-om, password-om, ili biometričkom identifikacijom
- Postaviti automatsko zaključavanje uređaja
- Sačuvati integritet mobilnog uređaja na način da si korisnik ne aktivira povišene razine pristupa i dodatnih opcija u sustavu koristeći Jailbreaking, Rooting i slično
- Instalirati aplikacije iz sigurnih i povjerenih izvora, odnosno sa trgovine predviđene za operacijski sustav uređaja
- Provjeriti dopuštenja koja se daju aplikacijama prilikom instalacije
- Za dodatnu zaštitu razmotriti i dodatne mogućnosti enkripcije osjetljivih podataka
- Čuvati uređaj dalje od tuđih pogleda prilikom unošenja PIN-ova za pristup uređaju i osjetljivih aplikacijama

Korisnika bi također trebalo upozoriti kako je svaka komunikacija prema banci izvan komunikacijskih kanala preporučenih od strane banke rizik te da je najbolje takvu komunikaciju izbjegavati. Bankovna aplikacija također bi trebala sadržavati popis službenih komunikacijskih kanala poput brojeva službenih telefona, E-mail-ova i ostalih načina stupanja u kontakt sa bankom, kako bi korisnik bio siguran da zaista razgovara sa djelatnikom banke.

3. Tehnologije mobilnih bankovnih aplikacija

Nakon što se postavi definicija mobilnog bankarstva, bitno je odrediti koje se tehnologije i sigurnosne mjere koriste pri realiziranju takvog oblika mobilnog bankarstva kako bi iz pogleda mobilne sigurnosti mogli razložiti funkcioniranje jedne takve aplikacije. Sagledavati će se mobilne aplikacije prvenstveno na Android i iOS operacijskim sustavima, te prema tome sigurnosne prednosti i mane tih sustava i na koji način pristupiti mogućim propustima sustava i njegove periferije. Većinski dio mobilnih bankovnih aplikacija za prikaz samog sučelja aplikacije koristi dinamičko pozivanje web komponenti sa web sjedišta banke te se u web pogled komponenti(WebView) prikazuje kao dio mobilne aplikacije korisniku. Zbog toga, mobilne bankovne aplikacije dijele mnoge komponente i sigurnosne propuste koji se mogu naći kod internet bankarstva i web bankovnih sjedišta. Trusted Service Manager(TSM) upravitelju servisima poželjno je prepustiti upravljanje komunikacijom podataka, sigurnosti pohrane i distribucije podataka te razgovora sa različitim strankama mobilnog bankovnog sustava. Osim komunikacijske infrastrukture, zanima nas i pohrana podataka ukoliko je potrebno na mobilni uređaj pohraniti osjetljive korisničke podatke ili pak identifikacijske tokene ili certifikate. Ukoliko su korisnički podaci dobro zaštićeni, čak niti propusti u našoj aplikaciji im neće napraviti toliku štetu, stoga je potrebno posebnu pažnju posvetiti enkripciji i sigurnom spremanju i prikazu podataka na mobilnom uređaju.

Mobilne bankovne aplikacije osim tradicionalnih usluga bankarstva također mogu sadržavati i funkcionalnosti plaćanja mobilnim uređajem koristeći Near Field Communications(NFC) tehnologiju ili pak koristeći bar kodove, što predstavlja dodatne sigurnosne rizike i potrebna rješenja. Ovakav oblik plaćanja beskontaktnim tehnologijama sličan je tehnologijama beskontaktnih kartica dok mobilno beskontaktno plaćanje ipak pruža veću sigurnost i fleksibilnost.(Bergman et al., 2012: 236-239)

3.1 Mrežne tehnologije

Najzastupljenija tehnologija na mobilnim uređajima je 2G(GSM/EDGE) i 3G(UMTS/HSPA) tehnologija uz Long Term Evolution(LTE) tehnologiju koja se predstavlja kao 4G. Osnovne komponente bežične mreže su: spektar za bežično sučelje, antene i radio uređaji za radio procesiranje u baznoj stanici ili mobilnim stanicama, te konekcija(T1, mikrovalna) od mobilne stanice do mobilnog switch centra koji sadrži uređaje za procesiranje glasa i podataka. 3G tehnologija sastoji se i od enkripcije za podatke u prijenosu, te uzajamne autentikacije između korisnika i mreže.(Pegueros, 2012: 8-9)

Komunikacija mobilne bankovne aplikacije koja se provodi 2G/3G i LTE mrežama bez popratnih sigurnosnih protokola podložna je različitim vrstama napada na komunikacijski kanal korisnika i bankovnog poslužitelja. Madan(2013) preporuča korištenje GPRS rješenja za sigurnu mobilnu mrežnu komunikaciju bankovne aplikacije i poslužitelja banke. Po prijavi korisnika u aplikaciju stvara se par jednokratnih ključeva, javni ključ se potom šalje poslužitelju te se stvara digitalni potpis za korisnika čiji se mobilni uređaj pritom i autentificira na poslužitelju. Nakon autentikacije uređaja, sigurnim Secure GPRS Protocol(SGP) protokolom odvija se transfer podataka između korisničke aplikacije i banke.

3.2 Protokoli

Prema istraživanju koje su proveli Eric Filiol i Paul Irolla(2015: 15) nad 50 mobilnih bankovnih aplikacija ustanovili su da većina aplikacija dinamički učitava grafičke komponente i podatke sa udaljenog servera. Također navode kako ovaj pristup stvara propuste omogućavajući napadačima napade tipa Main-in-the-middle, odnosno napade kod kojih napadač unosi kod i JavaScript naredbe usred komunikacije klijenta sa serverom ukoliko se koristi HTTP protokol, te je stoga osobitno važno da se koristi sigurniji protokol kao što je HTTPS protokol. Sve konekcije i komunikacijski kanali moraju biti sigurni, odnosno prolaziti osiguranim prijenosnim protokolima. Sa strane bankovne aplikacije potrebno je osigurati komunikaciju prema serveru te propustiti komunikaciju samo u slučaju ako je komunikacija sa serverom certificirana SSL certifikatom pouzdanog izvora.

Korištenje SSL protokola znači provjeravanje SSL certifikata po spajanju na server koji certifikat vraća kao odgovor putem SSL protokola. SSL certifikat se provjerava koristeći postojeće SSL certifikate koji se nalaze na mobilnom uređaju korisnika. Ukoliko SSL certifikat nije izdan od strane Certificate Authority uprave kojoj operacijski sustav vjeruje, odnosno posjeduje kao povjerljiv izvor certifikata, konekcija se ne uspostavlja. U protivnom, konekcija prolazi te se korisnik povezuje na server sigurnim putem. Za zlouporabu ovakvog sustava provjere sigurnosti servera na kojega se aplikacija spaja zahtjeva da napadač posjeduje sigurnosni SSL certifikat koji se nalazi na popisu pouzdanih certifikata ili u slučaju da je jedan od povjerljivih certifikata kompromitiran, u kojem slučaju napadač i putem HTTPS protokola interferira komunikaciju aplikacije sa poslužiteljem predstavljajući se kao povjerljiv, certificiran izvor. Kako bi se izbjegla i ta mogućnost koristi se SSL Pinning metoda. Na mobilni uređaj postavlja se kopija sigurnog SSL certifikata koji će služiti za provjeru prilikom spajanja na server koji odgovara tim certifikatom, odnosno server na koji se spaja aplikacija čime se certifikat na serveru i kopija certifikata na aplikaciji poklapaju i stvara se sigurna konekcija.

SSL pinning zaobilazi standardne certifikate operacijskog sustava te je za provjeru korištena isključivo kopija certifikata na mobilnom uređaju korisnika.

3.3 Near Field Communications Plaćanje

Kao što je već rečeno, plaćanje samim mobilnim uređajem moguće je koristeći Near Field Communications čip koji se nalazi na mobilnom uređaju i ukoliko mobilna bankovna aplikacija podržava takav način provođenja transakcije. Sigurnost mobilne bankovne aplikacije prilikom korištenja NFC za beskontaktno plaćanje sagledati će se po različitim aspektima; njenim prednostima, manama te na koji način zaštititi bankovnu aplikaciju prilikom korištenja NFC tehnologije. Kako su sa iPhone 6 i iPhone 6 Plus stigli i NFC čipovi za mobilno plaćanje i na iOS platformi, gotovo svi vodeći smartphone proizvođači sada već koriste NFC tehnologiju u nekom obliku te je vidljivo da NFC tehnologija uzima zamaha i kreče se uzlaznom putanjom.(IHS Technology, 2015) Stoga je potrebno analizirati ovu tehnologiju kako bi ustanovili je li i sigurna ili pak samo pristupačna. NFC se definira ISO 18092 standardom te prema tome ima slijedeće atribute:

- Ograničenje brzine prenošenja podataka na 424 kilobita po sekundi
- Omogućava komunikaciju na udaljenosti do 20 centimetara
- Ne posjeduje enkripciju

NFC komunikacija se aktivira ukoliko su dva kompatibilna uređaja na potrebnoj udaljenosti jedan od drugoga. Ukoliko se NFC koristi za plaćanje, ta udaljenost se postavlja na mnogo manji raspon od par milimetara. RF signal koji NFC odašilje moguće je prepriječiti i očitati na udaljenosti od nekoliko metara koristeći odgovarajuću opremu, te je zbog toga osobito važno koristiti enkripciju i sam NFC modul u kombinaciji sa Secure Elementom. (Pegueros, 2012: 10-15)

Osim korištenja NFC tehnologije za plaćanje, postoje i druge namjene poput NFC Tag-ova. NFC Tag može sadržavati poveznice na web sjedišta te se sadržaj otvara kako se NFC na uređaju približi NFC Tag-u. NFC Tag može sadržavati zlonamjerne podatke, slati korisnika na maliciozno web sjedište ili na mobilnu trgovinu kako bi korisnik skinuo malicioznu aplikaciju ili pak može direktno napadati neku od aplikacija u sustavu sa neočekivanim podatkovnim unosom. Sigurnost Tag-ova rješava mobilni operacijski sustav, ali samo u toj mjeri da upozorava korisnika o korištenju te zahtjeva interakciju korisnika ukoliko mobilni uređaj detektira NFC Tag.

3.4 Secure Element

Budući da NFC ne sadrži modul za enkripciju, potrebno je NFC plaćanje razvijati zajedno sa sigurnosnim elementom Secure Element(SE). SE je kriptografski modul koji se obično nalazi kao zaseban čip u mobilnom uređaju. Prema GlobalPlatform(2015) kompaniji, zaduženoj za sigurnost i razvoj Secure Element tehnologije, dan danas SE implementacija nije standardizirana te se trenutno dijeli na:

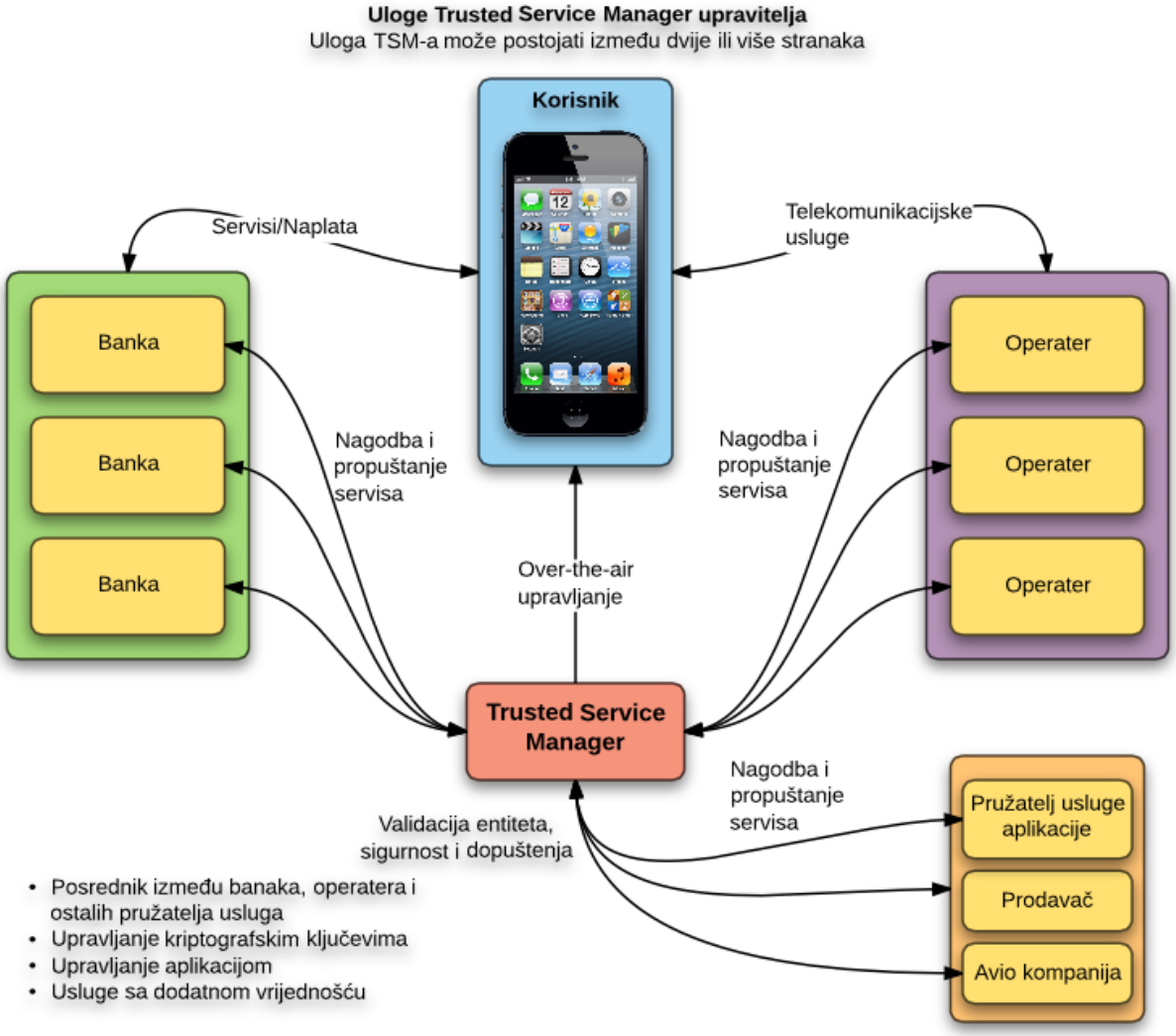
- Ugradnja Secure Element u čip mobilnog uređaja(eSE)
- Implementacija u SIM čip
- Implementacija koristeći SD karticu

Prema Pegueros(2012, 15-16) od navedenih sigurniji su Secure Element čipovi na SIM karticama i na samom uređaju budući da oni dobivaju dodatnu sigurnost iz mobilnog operativnog sustava koji aplikacije sprječava pristup Secure Element podacima, iako su i podaci SE izloženi i napadu i neautoriziranom čitanju ukoliko pristup SE nije adekvatno zaštićen od neovlaštenog korištenja i pristupa. Kako NFC ne posjeduje mogućnost enkripcije, koristimo Secure Element za enkripciju signala koji NFC odašilje. Mobilne bankovne aplikacije i bankovne aplikacije za plaćanje posjeduju PIN autentikaciju ili password koji je potreban za otključavanje podataka u Secure Element modulu prilikom plaćanja. Očuvanje integriteta Secure Element čipa osigurava se na način da samo vlasnik SE može pristupati i mijenjati podatke u SE. GlobalPlatform asocijacija sastoji se od preko 100 organizacija, uključujući proizvođače uređaja, mobilnih operatera i kompanija platnih kartica, koji određuju specifikacije i standardni protokol upravljanja Secure Element-om.

3.5 Trusted Service Manager

Za provođenje transakcija, osim NFC, Secure Element čipova i softvera, potreban nam je i Trusted Service Manager. TSM koristimo kao sučelje ekosistema za plaćanje u svrhu provođenja transakcija jedne financijske institucije. Sve osjetljive aplikacije, odnosno aplikacije koje koriste osjetljive informacije o korisniku kao što su informacije koje se nalaze na Secure Element čipu, potrebno je osigurati sa aspekta distribucije informacija, dopuštenja za pristup informacijama i dopuštenja za upravljanje informacijama te iz tog razloga kod provođenja plaćanja na mobilnim uređajima koristimo TSM. Kako bi ostvario komunikaciju između različitih mrežnih operatera, banaka, distributera, prodavača i marketing kompanija, TSM mora biti neutralna stranka kako ne bi došlo do sukoba interesa na mobilnom uređaju

korisnika budući da TSM radi sa osjetljivim podacima i obično nedostupnim dijelovima



Slika 3 Ekosustav mobilne bankovne aplikacije kojega je osnova TSM, prema Pegueros(2012, 11)

sustava kao što je Secure Element. Na slici 3 može se vidjeti komunikacija koju TSM omogućava, veliki broj operatera, banaka i različitih pružatelja aplikacija i prodavača ima potrebu za TSM upraviteljem kako bi se osigurala komunikacija i nepristranost stranaka koje sudjeluju u realizaciji jedne bankovne mobilne aplikacije i njenih servisa poput mobilnog plaćanja za što je potrebna i komunikacija sa prodavačima i pružateljima usluga koje korisnik želi plaćati. TSM, budući da je neutralan u komunikaciji, pokriva mnogo više prodavača, operatera i banaka nego što bi bio slučaj ukoliko bi pružatelji TSM-a bili pristrani određenim bankama ili operaterima, ovima se osigurava dostupnost plaćanja svima bez obzira na pripadnost određenoj banci ili mobilnom operateru.

Prema Chris Cox-u(2009: 7) glavni zadaci TSM-a su:

- Upravljanje mrežnim operaterima
- Upravljanje korisničkim mobilnim novčanikom putem interneta i upravljanje uređajem

- Upravljanje servisima poslužitelja i upravljanje aplikacijama
- Upravljanje poslužiteljima servisa

Kako bi povezali trgovca, autoritet za komunikacijsku i banku koristeći infrastrukturu mrežnih operatera bez potrebe za održavanjem posebnih veza između stranaka potrebno je upravljanje mrežnim operaterima. U protivnom je potrebno za svakog trgovca, komunikacijski autoritet i banku povezati sa svakim mrežnim operaterom posebno. TSM također podržava administratorske funkcije, naplatu i namirenje između stranaka prilikom transakcije.

TSM putem mreža operatera poslužuje različite stranke u komunikaciji sa potrebnim informacijama za provođenje transakcija. TSM stvara Secure Element po prvom pokretanju mobilne aplikacije te osigurava ažuriranje aplikacije nakon puštanja aplikacije u opticaj na trgovinu.

Poslužitelj servisa jest kompanija koja nudi nekakvu korisničku aplikaciju. Kako bi se osigurala jednostavnost komunikacije između poslužitelja servisa TSM također pruža mogućnost upravljanja podacima za različite aplikacije poslužitelja, to može uključivati i administrativne i transakcijske funkcije.

TSM također održava informacije o mobilnim uređajima, čipovima i softveru koji su potrebni za uspješnu komunikaciju putem mreže koristeći različite mobilne uređaje.

3.6 Webroot alat

Jedan od načina prevencije napada na sustav mobilne bankovne aplikacije jest korištenje Webroot skupa alata za razvoj, odnosno Software Development Kit(SDK). Webroot SDK je namjenjen za ugradnju u mobilnu aplikaciju. Po implementaciji Webroot alat se pokreče u pozadini te u realnom vremenu banci šalje informacije o korištenju aplikacije. Na ovaj način banka može praviti profil korištenja aplikacije, analizirati korištenje aplikacije i iskoristiti korisnikove uzorke ponašanja za uspoređivanje u svrhu identificiranja abnormalnog ponašanja korisnika. Ukoliko se na vrijeme ustanovi da aplikaciju ne koristi pravi korisnik aplikacije moguće je i prije nego što je učinjena šteta uskratiti pristup aplikaciji sa udaljene lokacije.

3.7 Hardverska virtualizacija

Hardverska virtualizacija postaje jedna od najzastupljenijih sigurnosnih rješenja na mobilnim uređajima. Noviji ARM procesori podržavaju hardversku virtualizaciju pod nazivom TrustZone u obliku ekstenzije samom procesoru. Na ovaj način moguće je na jednoj jezgri procesora pokretati dva paralelna operacijska sustava, osigurani operacijski sustav i normalni operacijski sustav. TrustZone radi na principu tri domene, korisnikove aplikacije pokreću se u

"normal" domeni, kernel sistemske instrukcije u "system" domeni te se za potrebe sigurnosti koristi i "monitor" sigurna domena za izvođenje kernel instrukcija. Iz razloga što je TrustZone hardversko rješenje zaobilazi se potreba za provjerom Root stanja mobilnog uređaja budući da arhitektura domena po kojoj TrustZone funkcionira sprječava pristup čak i aplikacijama kojima je dopušten povišeni Root način rada.(Open Virtualization for ARM TrustZone, 2013) Sve instrukcije obilježavaju se kako bi se ustanovilo koji put će pratiti. Obilježje instrukcije služi kao prekidač između sigurne i normalne domene. Softverski monitor presreće transakcije mikroprocesora i zahtjeve prema i od sistemskih resursa, kao što je periferija uređaja. Ovim načinom određuje se kojoj domeni instrukcija pripada te je efektivna izolacija i procjena instrukcija koje se postavljaju u sigurnu domenu krucijalna.

4. Zaštita pristupa

Istraživanjem aktualnih bankovnih aplikacija kako je navedeno u trećem poglavlju ovoga rada, vidi se kako mobilne bankovne aplikacije banaka u Hrvatskoj koriste PIN ili password pristup aplikaciji i eventualno sigurnosnu provjeru One Time Password(OTP) metodom po prvom pokretanju bankovne aplikacije. Ovakav oblik zaštite ne štiti korisnika od napadača koji mogu vidjeti koji PIN ili password korisnik unosi prilikom prijave u aplikaciju čime se dobiva potpuno pravo na korištenje aplikacije uključujući pristup osjetljivim informacijama i provođenju transakcija. Ukoliko se za pristup aplikaciji koristi samo PIN ili password te je namjera korisniku olakšati korištenje dodatne autentikacije poželjno ju je koristiti u kombinaciji sa prije navedenim Webroot razvojnim alatom kako bi se prikupljali podaci o korištenju aplikacije i u slučaju neovlaštenog pristupa po prepoznavanju abnormalnog ponašanja korisnika spriječila šteta pravom korisniku aplikacije. U ovom poglavlju govoriti će se o rješenjima koja se oslanjaju na postojeća rješenja poput PIN i password provjere prilikom pristupa i rješenjima koja mogu djelomično ili čak u potpunosti zamijeniti ovakav način pristupa aplikaciji zbog njihove lakše i sigurnije identifikacije korisnika.

4.1 SMS Više-faktorska autentikacija

Kao primjer više-faktorske autentikacije neke bankovne aplikacije koriste SMS uslugu slanjem OTP-a korisniku koji se potom unosi u aplikaciju prilikom prijave ili provođenja transakcije. Prema istraživanju koje je proveo Ken Baylor 2013. godine ovakav oblik više-faktorske autentikacije ne preporuča iz razloga što je u svrhu zaobilaženja SMS autentikacije nastao veliki broj trojanaca koji se predstavljaju kao dobronamjerni softver sa namjerom prosljeđivanja SMS poruka napadaču. Rizik korištenja ovakvog oblika više-faktorske autentikacije pokazuje i činjenica da je devedeset i devet posto Malware aplikacija korišteno kao Spyware i SMS trojanci. Tako je Zitmo maliciozna aplikacija tipa trojanac prilikom prijave na stranice banke bilježio SMS poruke korisničkog uređaja koje su bile namijenjene autentikaciji korisnika u pretraživaču kod provođenja transakcije. Zeus Malware aplikacija za stolna računala koristila bi se u kombinaciji sa Zitmo Malware mobilnom aplikacijom te na taj način napadač dobiva sve potrebne informacije o SMS autentikaciji. Za distribuciju Zeus aplikacije koristile su se Phishing E-mail kampanje, odnosno lažno predstavljanje u obliku legitimnog izvora u E-mail-ovima te traženje instalacije softvera ili login na stranice koje izgledaju legitimno dok u stvarnosti prikupljaju login podatke korisnika legitimne web stranice, te se na taj način inficira ili korisničko računalo ili prikupljaju osjetljivi podaci o korisniku. Zeus aplikacija služila je samo za preusmjeravanje HTTP prometa sa bankovne web aplikacije

na inficiranom korisničkom računalu. Korisnika se navodilo na instalaciju mobilnog sigurnosnog softvera koji izgledao legitimno, ali glavna mu je funkcija Zitmo Malware koji omogućava čitanje korisničkih SMS poruka.

4.2 Biometrička autentikacija

Pojavom biometričkih senzora na mobilnim uređajima poput Apple Touch ID tehnologije i Samsung Finger Scanner tehnologije koje koriste otisak prsta za autentikaciju korisnika, otvaraju se mogućnosti autentikacije korisnika biometričkim senzorima. Ovakav oblik autentikacije je još u razvoju, ali ima potencijal zamijeniti trenutne autentikacijske metode na mobilnim uređajima te se već koristi za autentikaciju prilikom plaćanja koristeći Apple Pay i Samsung Pay tehnologije.

Pored autentikacije otiskom, pojavljuju se i druge tehnologije za biometričku autentikaciju korisnika. Digital Insight kompanija razvija tehnologiju Eyeprint ID koja slikanjem uzorka kapilara na oku običnom kamerom pametnog telefona autentificira korisnika. Banke u kolaboraciji sa Digital Insight kompanijom eksperimentiraju sa primjenom ove tehnologije u mobilnom bankarstvu što nam govori da ova tehnologija ima svoje mjesto u budućnosti kao jedna od zamjena tradicionalnom pristupu autentikaciji korisnika.

Nuance Communications kompanija razvija autentikaciju glasom, što se također pokazuje kao uspješan pothvat te je već prihvaćena metoda autentikacije od strane američkih banaka poput Wells Fargo, Barclays i US Bank. Prednost ove tehnologije jest i pristupačnost korištenja osobama sa posebnim potrebama kako autentikacija ne zahtjeva direktno korištenje samog uređaja ukoliko se korisnik mobilnim uređajem koristi putem glasovnih naredbi te je sama autentikacija jednostavnija samim time što nije potrebno pamtiti PIN ili password za prijavu. (Stanganelli, 2015)

Budući da je za potrebe mobilnog bankarstva potreban robustan i siguran oblik autentikacije ovakve tehnologije se pokazuju kao odlični alati, ali svakako je potrebno još neko vrijeme da biometričke tehnologije na mobilnim uređajima sazriju do te razine pouzdanosti i jednostavnosti korištenja kada bi se mogle zamijeniti tradicionalni oblici autentikacije.

4.3 Sandbox metoda

Da bi zaštitili korisnika i podatke aplikacije, potrebno je spriječiti ili barem ograničiti komunikaciju ostalih aplikacija i dijelova mobilnog uređaja sa aplikacijom. Svaka aplikacija ima pristup svojim podacima, postavkama i postavkama mrežne komunikacije. Jedan od načina da se aplikacija, njeni podaci i rad zaštiti jest Sandboxing metoda koja se koristi pri razvoju

aplikacije. iOS primjerice podržava Sandbox zaštitu aplikacija zajedno sa enkripcijom osjetljivih podataka. Sandboxing ne sprječava napad na aplikaciju već umanjuje potencijalnu štetu te otežava pristup osjetljivim podacima. Sigurnost samih podataka, ukoliko i dođe do kompromitiranja Sandbox zaštite i enkripcije podataka, potrebno je osigurati pri razvoju aplikacije i ograničiti dostupnost osjetljivih podataka ostalim aplikacijama u sustavu. Komuniciranje aplikacije sa ostalim aplikacijama u sustavu moguće je striktno definirati opcijama za dijeljenje podataka ili Sharing dopuštenja aplikacije.

5. Glavni rizici

Budući da se komunikacija klijentske aplikacije sa serverom odvija putem interneta većina prijetnji koje se pojavljuju kod online bankovnih aplikacija prijeti i mobilnim bankovnim aplikacijama te će se iz tog razloga govoriti i o problemima i napadima na komunikacijsku infrastrukturu aplikacije pored sigurnosti aplikacije u okružju u kojem se nalazi. Osim rizika mrežne komponente osnovni problem mobilnih operacijskih sustava jesu njihove aplikacije, ukoliko se ne provodi dovoljno rigorozna provjera aplikacija koje se postavljaju na trgovinu sustava, lako je sa lažno predstavljenom aplikacijom napraviti veliku štetu korisniku i njegovoj privatnosti.(Pengueros, 2012: 13) Ovaj problem je tim veći ukoliko se zlonamjernoj aplikaciji daju prevelike privilegije prilikom instalacije. Sa povišenim privilegijama i samim time sa većom slobodom u sustavu, zlonamjerne aplikacije mogu naštetiti resursima operacijskog sustava i komunikaciji procesa u sustavu. Bankovne aplikacije moraju se zaštititi i od ovakvih napada, unutar samog sustava na kojem se nalaze. Ukoliko maliciozna aplikacija ipak završi na operacijskom sustavu na kojem se nalazi i bankovna mobilna aplikacija problem se pokušava riješiti metodom Sandboxing-a, odnosno sprječavanjem pristupa aplikaciji iz ostalih dijelova sustava i smanjuje pristup aplikaciji prema sustavu i njegovim resursima samo na potrebne resurse. Ukoliko je korisnik dopustio povišeni pristup na mobilnom uređaju koristeći Root, Jailbreak ili slične metode o kojima će se u ovome poglavlju više govoriti, postoji mogućnost zlonamjerna aplikacija, budući da može posjedovati povišeni pristup, ne nalazi u sigurnom Sandbox okružju te na taj način napada mobilni uređaj korisnika.

Prema Pegueros(2012) mobilni uređaji podložni su sigurnosnim rizicima iz razloga što još uvijek na mobilnim platformama ne postoje odgovarajuća i dovoljno zrela sigurnosna rješenja, kao razlog navodi manjak procesorske snage i relativno kratko trajanje baterije budući da bi je kontinuirano provjeravanje sigurnosnog stanja, pregledavanje podataka i procesa sustava bilo potrebno koristiti dio procesorske snage mobilnog uređaja što može imati veliki utjecaj na trajanje baterije mobilnog uređaja. Kao glavne sigurnosne rizike mobilnih bankovnih aplikacija navodi sljedeće:

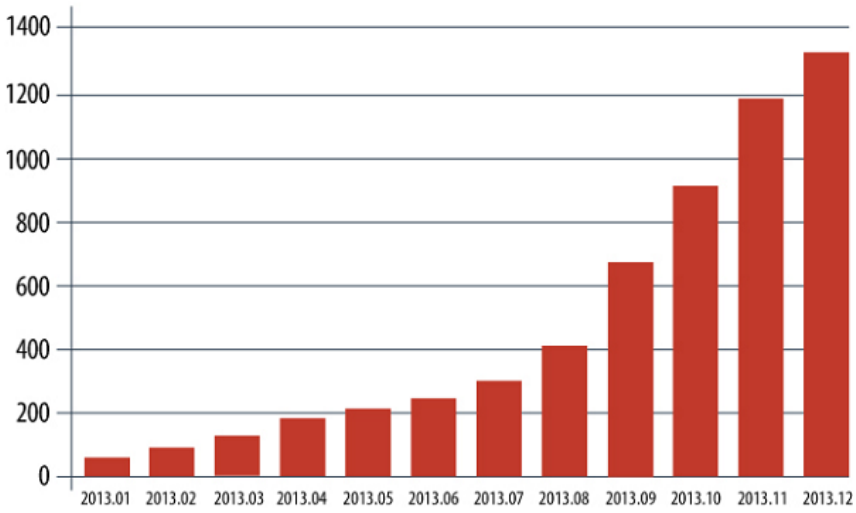
- Malware
- Maliciozne aplikacije
- Narušavanje privatnosti ovisno o kolekciji i distribuciji podataka
- Mrežna infrastruktura
- Infrastruktura i ekosistem plaćanja

- SMS ranjivosti
- Ranjivosti hardvera i operacijskog sustava
- Kompleksan lanac opskrbe i pridošlice u mobilni ekosistem
- Manjak zrelosti sigurnosnih kontrola i alata

U sljedećem poglavlju govoriti će se o prevenciji ovih sigurnosnih rizika te na koji način omogućavaju zlonamjerno iskorištavanje mobilne bankovne aplikacije, njene komunikacije i integriteta za nanošenje štete korisniku ili sustavu.

5.1 Malware

Prema Kaspersky Lab artiklu iz 2013. godine u periodu od početka 2012. godine do kraja 2013. godine može se vidjeti pojavljivanje deset milijuna jedinstvenih Malware mobilnih aplikacija. Kao što se može vidjeti na slici ispod, istraživanje Kaspersky Lab-a pokazuje veliki porast Malware mobilnih aplikacija u 2013. godini kada je sa 67 jedinstvenih bankovnih Malware aplikacija početkom godine taj broj narastao na 1321 jedinstvenu Malware aplikaciju do kraja godine.



Slika 4 Kaspersky Lab izvještaj o Malware-u i Malware aplikacijama koje pogađaju mobilne bankovne aplikacije, godina 2013.

Kao što je već spomenuto Zitmo i Zeus jedan su od razloga velikog povećanja opreza i razvoja novih rješenja autentikacije kada se govori o SMS više-faktorskoj autentikaciji i općenito sigurnosti kod autentikacije. Sličan primjer Malware aplikacije koja napada više-faktorsku autentikaciju jest FakeToken. Tehnički cilj ove maliciozne aplikacije bio je da se izbaci potreba za infekcijom računala i mobilnog uređaja, već samom infekcijom mobilnog

uređaja se nastojalo dobiti dovoljno informacija za napad na korisnički bankovni račun. FakeToken lažno se predstavlja kao bankovna token aplikacija koja generira broj tokena i zahtjeva unos korisnikove lozinke, po unosu šalje se SMS poruka napadačima sa svim potrebnim podacima o korisniku.

Kao odgovor na veliki broj malicioznih aplikacija na Android platformi, Google je 2012. godine objavio da će se za povećanje sigurnosti od Malware aplikacija odsada koristiti automatizirani alat pod nazivom Bouncer ili izbacivač. Bouncer skenira aplikacije koje se prijavljuju na Google Play trgovinu te na taj način se nastoji ustanoviti je li aplikacija maliciozna prije nego što se aplikaciju stavlja u opticaj. Ubrzo nakon što je Bouncer stavljen u funkciju na Google Play trgovini, istraživači su počeli testirati mogućnosti i efektivnost ovoga alata. Ustanovljeno je da nije potrebno mnogo napora kako bi se Bouncer provjera zaobišla te da bi maliciozna aplikacija završila na trgovini. Nešto kasnije pojavljuje se i Android Verification Service koji također služi kao obrana od malicioznog softvera, ali na uređaju korisnika. Android Verification Service skenira i aplikacije instalirane sa ostalih trgovina na Android platformi uključujući i direktne instalacije ukoliko se aplikacija skida sa web preglednikom. Obrana od Malware aplikacija i kreativnost napadača koji proizvode Malware aplikacije raste sa vremenom te je potrebno zaštiti aplikaciju, pogotovo ukoliko se radio o aplikaciji sa osjetljivim podacima korisnika, te je potrebno korisnika educirati o rizicima lakomnog instaliranja softvera i iz ne povjerljivih izvora.

Za razliku od Android platforme Malware nije toliko zahvatio iOS operacijski sustav kada se govori o sigurnosti bankovnih mobilnih aplikacija i ugrožavanja osjetljivih podataka aplikacije osim uređaja na kojima se koristi povišeni pristup koristeći Jailbreak metodu budući da bi korisnici Jailbreak metodom dobili povišeni pristup funkcijama sustava, a nebi ga potom zaštitili od zlonamjernog iskorištavanja povišenog pristupa od strane ostalih aplikacija ili napadača. O Jailbreak i Root metodama za postizanje povišenog pristupa sustavu više će se govoriti u sljedećem poglavlju.

5.2 Root i Jailbreak

Rooting, Jailbreak i slične metode, način su za ostvarivanje povlaštenog pristupa podacima i mogućnostima mobilnih uređaja. Povlašteni pristup također omogućava i eksploataciju metoda i podataka ne predviđenih za modifikaciju i korištenje od strane krajnjeg korisnika što otvara vrata korisniku, ali i napadačima za iskorištavanje kompromitirane pozicije u koju se uređaj postavlja primjenjivanjem Root, Jailbreak i sličnih alata. Povlašteni pristup mobilnom uređaju od strane korisnika kompromitira integritet mobilnog uređaja i u najgorem

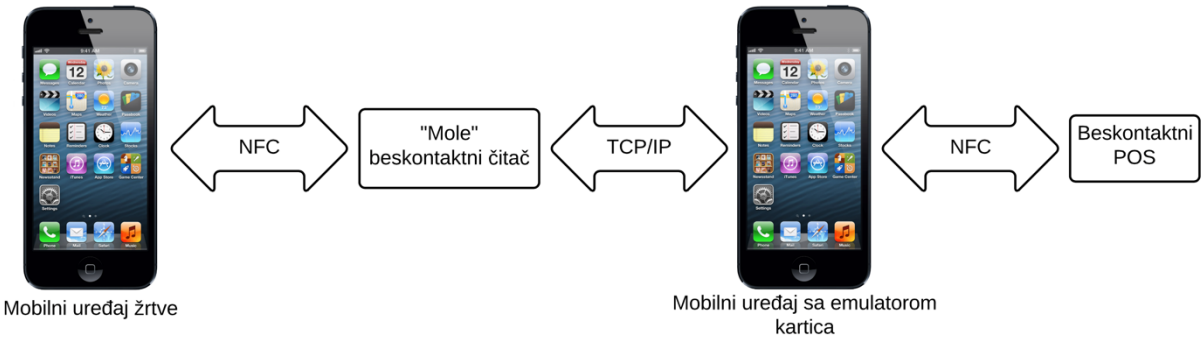
slučaju zlonamjernim napadačima omogućava pravljenje mnogo veće štete mobilnom uređaju nego što je slučaj kod uređaja sa tvorničkim postavkama proizvođača. Mobilna bankovna aplikacija trebala bi moći detektirati stanje integriteta mobilnog uređaja te upozoriti korisnika na rizike koji nastaju korištenjem bankovne aplikacije u kombinaciji sa Root, Jailbreak i ostalim alatima za ostvarivanje povlaštenog pristupa na mobilnom uređaju. Zbog sigurnosti korisnika također je preporučljivo ne dopustiti korištenje ili instalaciju osjetljive aplikacije kao što je bankovna aplikacija na uređaj sa povlaštenim pristupom. Ukoliko se aplikacija razvija koristeći TrustZone hardversku virtualizaciju moguće je zaobići potrebu za provjerom stanja integriteta mobilnog uređaja budući da, kao što je navedeno u prošlom poglavlju, TrustZone ne dopušta pristup čak niti aplikacijama koje imaju povlašteni pristup sustavu te se na taj način može riješiti problema Root pristupa mobilnom uređaju.

5.3 Relay napad

Relay napad započinje prikupljanjem podataka komunikacije između klijentske aplikacije i poslužitelja. Prikupljene podatke se potom koristi za ne dopušteni pristup odašiljajući poruku. Napadač šalje poruku odredišnom poslužitelju bez obzira zna li sadržaj poruke, budući da je poruka prikupljena od klijenta čija je poruka bila prihvaćena od strane poslužitelja. Relay napadi su također mogući i kod NFC beskontaktnog plaćanja. Prema Bergman et al., Relay napad na mobilni uređaj koji koristi NFC za beskontaktne transakcije odvija se na sljedeći način:

1. "Mole" ili špijun beskontaktni čitač kojim upravlja napadač približi se mobilnom uređaju koji se napada ili beskontaktnoj kartici
2. Mobilni uređaj napadača postavlja se kraj beskontaktnog POS terminala kako bi napravio transakciju. Mobilni uređaj napadača zatim koristi NFC imitaciju kartica, odnosno mogućnost koja dopušta NFC uređajima da imitiraju beskontaktne kartice softverom.
3. POS terminal zatim šalje prvu naredbu napadačevom mobilnom uređaju. Prva naredba traži informacije o dostupnim načinima plaćanja mobilnim uređajem.
4. Mobilni uređaj napadača šalje tu poruku beskontaktnom "Mole" čitaču putem interneta ili nekog drugog komunikacijskog kanala kao što je Bluetooth.
5. -"Mole" beskontaktni čitač reproducira naredbu mobilnom uređaju koji napada putem NFC.
6. Napadnuti uređaj odgovara sa podacima potrebnim za provođenje plaćanja i popisom dostupnih oblika plaćanja.

7. "Mole" beskontaktni čitač šalje odgovor nazad napadačevom mobilnom uređaju putem komunikacijskog kanala.
8. Mobilni uređaj napadača šalje naredbu dalje POS terminalu. POS terminal odabire odgovarajući oblik plaćanja te dohvaća potrebne opcije za procesiranje, akreditaciju plaćanja i sve što je potrebno za uspješno provođenje transakcije.



Slika 5 Kompromitiranje NFC tehnologije za plaćanje koristeći Relay napad, prema Hacking Exposed: Mobile Security Secrets & Solutions(2013, 249)

Na slici 5 može se vidjeti kako se napad realizira, odnosno na koji se način odvija komunikacija između uređaja žrtve do Mole čitača putem NFC-a, TCP/IP protokolom do uređaja napadača te NFC-om do beskontaktnog POS uređaja i nazad prema uređaju žrtve, te je također bitno napomenuti da se podaci prenose direktno i ne izmijenjeni između napadnutog uređaja i POS terminala putem "Mole" čitača i mobilnog uređaja napadača, stoga napadač ne mora znati sadržaj poruke već je samo potrebno imitirati legitiman mobilni uređaj žrtve za provođenje transakcije.

5.4 Man in the middle napadi

Napad tipa Man in the middle ili MITM jest metoda praćenja, čitanja, umetanja i promijene podataka u transferu između klijenta i poslužitelja. Bankovni protokoli koriste Message Authentification Code(MAC), odnosno hash vrijednost odgovora ili upita u transakciji, kako bi spriječili ovakav oblik napada.

Kako bi riješili problem MITM napada, potrebno je koristiti siguran protokol za transfer podataka poput HTTPS protokola i provjeru certifikata koristeći SSL Pinning metodu kako bi se izbjeglo lažno predstavljanje SSL certifikata te provjera autentičnosti poslužitelja provodila isključivo koristeći kopiju sigurnog SSL certifikata.

Također je potrebno onemogućiti manipulaciju mrežnih podataka između korisnika i poslužitelja tako što se po završetku razvoja aplikacije onemogućava alatima za ispravljanje grešaka povezivanje na aplikaciju što bi napadaču pokazalo koje pozive aplikacija radi sa sustavom i prema poslužitelju. Kao što je već rečeno problemi koje web aplikacije imaju dijele

i mobilne aplikacije ukoliko koriste mrežno povezivanje i protokole te se za otklanjanje nedostataka takve komunikacije preporuča ne vjerovanje podacima koje klijentska aplikacija šalje budući da napadači mogu interferirati mrežnu komunikaciju. Postavljanjem sigurne i detaljne validacije podataka koji se šalju od klijentske aplikacije i podataka koje aplikacija prima smanjuje rizik od napada i mogućnost interferiranja u komunikaciju.

5.5 Phishing napad

Phishing je metoda lažnog predstavljanja koja je osobito popularna u internet bankarstvu. Primjerice, korisnik dobiva lažni E-mail koji se predstavlja kao legitiman E-mail njegove banke te traži da se korisnik logira koristeći poveznicu u E-mail poruci, poveznica korisnika odvodi na također lažnu i prividno legitimnu stranicu te korisnik po upisivanju login podataka zapravo podatke šalje napadaču. Phishing se također koristi i za mamljenje korisnika na instalaciju malicioznih softvera koji se potom koriste za prikupljanje podataka o korisniku i napad na osjetljive podatke korisnika.

5.6 Krajnji razvoj aplikacije

Tijekom razvoja aplikacije koriste se alati za ispravljanje grešaka kako bi se otklonile greške u razvoju. Informacije o sustavu, korištenim metodama i podacima koji se prilikom razvoja prate u svrhu otklanjanja grešaka potencijalna su prijetnja za samu aplikaciju ukoliko se prilikom puštanja aplikacije u opticaj ne spriječi pristup aplikaciji alatima za ispravljanje grešaka. U protivnom napadač potencijalno iskorištava informacije o stanju aplikacije, pozivima metoda i podataka za vrijeme korištenja aplikacije u namjeri da se napravi reverzni inženjering same aplikacije te na taj način eksploatira prikupljene podatke u zlonamjerne svrhe. Potrebno je onemogućiti prikazivanje svih razvojnih metoda i informacija vezanih uz razvoj po završetku razvoja aplikacije.

Sigurnosna stanja aplikacije trebalo bi pratiti u svrhu analize sigurnosnih stanja i potencijalnih prijetnji sustavu. Prilikom korištenja aplikacije sigurnosna stanja se mogu spremati na korisnikov uređaj te po završetku korištenja poslati sigurnosna stanja predviđenom poslužitelju na analizu i prikupljanje stanja. Prije spomenuti Webroot razvojni alat jedno je od rješenja na prikupljanje i analizu sigurnosnih podataka koje također posjeduje mogućnost prikupljanja i obrade bihevioralnih podataka o korisniku koji u konačnici omogućavaju veću razinu sigurnosti od prikupljanja isključivo sigurnosnih podataka o aplikaciji i okružju u kojem se nalazi.

Po izdavanju nove verzije aplikacije poželjno je spriječiti korištenje starih verzija aplikacije dok se aplikacija ne ažurira na posljednju verziju kako bi se iskoristila najnovija sigurnosna rješenja primijenjena na aplikaciju budući da korištenje starije verzije predstavlja potencijalni rizik za korisnika. Provjera verzije korisnikove mobilne aplikacije može se vršiti usporedbom sa verzijom aplikacije zapisanom na poslužitelju. Ažuriranje je poželjno provoditi službenim stranicama banke kako bi se izbjeglo kompromitiranje sigurnosti.

6. Zaključak

Sigurnost mobilnih bankovnih aplikacija ovisi o mnogim faktorima. Ovisi o ekosustavu u kojem se mobilni uređaj nalazi, u kojem se odvija komunikacija i okružju u kojem se nalazi sama mobilna aplikacija. Potrebno je nastojati da mobilni bankovni sustavi budu korak ispred napadača te da se stoga posebna pažnja posveti sigurnosti korisnika i njihovih osjetljivih podataka. Postoje mnogi odgovori na mnoge sigurnosne propuste svakog aspekta mobilne bankovne aplikacije, bitno je ne dopustiti da se takvi propusti ponove te zbog toga istražiti koje su sve potrebne mjere kako bi se osigurao integritet aplikacije. Korisnike je isto tako potrebno educirati kako koristiti mobilni uređaj na kojem se nalazi aplikacija sa njihovim osjetljivim podacima i kako koristiti aplikaciju, a da se ne dovodi sustav i podatke u poziciju da ih netko može zlonamjerno iskoristiti. Kod razvoja mobilne bankovne aplikacije potreban je mnogo veći napor i oprez da se aplikaciju postavi na pravi put od samoga početka obzirom da svaki propust puno znači te će ga zlonamjerni napadači vrlo rado iskoristiti.

7. Literatura

1. Pegueros, V. (2012). *Security of Mobile Banking and Payments*. [online] Dostupno na: http://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062 [Pristupljeno 24. 8. 2015].
2. Bergman, N., et al. (2013). *Hacking exposed: Mobile security secrets & solutions*. McGraw-Hill
3. Filiol, E. i Irolla, P. (2015). *(In)Security of Mobile Banking...and of Other Mobile Apps**. ESIEA.
4. Globalplatform.org, (2015). *GlobalPlatform*. [online] Dostupno na: https://www.globalplatform.org/mediaguideSE.asp [Pristupljeno 28. 8. 2015].
5. IHS Technology, (2015). *Digital Security Intelligence Service - Near Field Communications Topical Report – 2015.*
6. Meghanathan, N., Kaushik, B. i Nagamalai, D. (2011). *Advances in computer science and information technology.* Berlin: Springer.
7. Khosrow-Pour, M. (2013). *E-commerce for organizational development and competitive advantage*. Hershey, PA: Business Science Reference.
8. Openvirtualization.org, (2013). *ARM TrustZone Software - Open Virtualization FAQ*. [online] Dostupno na: http://www.openvirtualization.org/open-source-arm-trustzone.html [Pristupljeno 30. 8. 2015].
9. Campagna, R., Iyer, S. and Krishnan, A. (2011). *Mobile device security for dummies*. Hoboken, N.J.: Wiley.
10. Madan, K. (2013). *Secure GPRS solution for mobile banking: an efficient security protocol.* Surya World Institute of Engg. & Technology, Rajpura, Punjab.
11. He, W., Tian, X. and Shen, J. (2015). *Examining Security Risks of Mobile Banking Applications through Blog Mining.* Old Dominion University, Norfolk, VA, USA.
12. Kentbank, (2014). *INTERNET BANKARSTVO – Preporuke za osiguravanje sigurnosti u sustavu.* [online] Dostupno na: http://www.kentbank.hr/1504/preporuke-za-osiguravanje-sigurnosti-u-sustavu [Pristupljeno 30. 8. 2015].
13. NSS Labs, (2015). *Mobile financial malware.* [online] Dostupno na: https://www.nsslabs.com/sites/default/files/public-report/files/View%20From%20The%20Precipice%20-%20Mobile%20Financial%20Malware.pdf [Pristupljeno 3. 8. 2015].

14. Stanganelli, J. (2015). *4 Hot Mobile Banking Security Developments* [online] Bank Systems & Technology. Dostupno na: http://www.banktech.com/security/4-hot-mobile-banking-security-developments/d/d-id/1319161?image_number=1 [Pristupljeno 30. 8. 2015].
15. Madan, K. (2013). *Secure GPRS solution for mobile banking: an efficient security protocol.* [Online] Rajpura, Punjab: World Institute of Engg. & Technology. Dostupno na: http://www.ijeemc.com/January2013/5.pdf [Pristupljeno 30. 8. 2015].
16. Hoang Ngo, H., Dandash, O., Dung Le, P., Srinivasan, B. and Wilson, C. (2011). *Formal Verification of a Secure Mobile Banking Protocol.* Faculty of Information Technology, Monash University, Melbourne, Australia.
17. Mobile Iron, (2015). *Mobile Security: Threats and Countermeasures*. [online] Dostupno na: http://www.mobileiron.com/sites/default/files/security/Mobile-Security-Threats-and-Countermeasures-WP-MKT-6361-V1.pdf [Pristupljeno 28. 8. 2015].
18. Securelist - Information about Viruses, Hackers and Spam (2014). *Mobile Malware Evolution: 2013*. [online] Dostupno na: https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/ [Pristupljeno 6 Sep. 2015].
19. Zaba.hr, (2014). *Uputa za korištenje m-zabe.* [online] Dostupno na: https://www.zaba.hr/home/wps/wcm/connect/25f27945-5c35-4d1f-b564-7d6f94633e50/Uputa_za_koristenje_m-zabe.PDF?MOD=AJPERES [Pristupljeno 25. 8. 2015].
20. Raiffeisenbank.ba, (2013). *Priručnik za korištenje servisa Raiffeisen mobilno bankarstvo – Android/iPhone.* [online] Dostupno na: https://raiffeisenbank.ba/templates/default/users_data/pages_content/prirucnik_za_koristenje_servisa_raiffeisen_mobilno_bankarstvo.pdf [Pristupljeno 25. 8. 2015].
21. onlinebanka.pbz.hr, (2014). *SIGURNOST mPBZ USLUGE.* [online] Dostupno na: http://onlinebanka.pbz.hr/dokumenti/Letak%20za%20mPBZ%20uslugu%20.pdf [Pristupljeno 25. 8. 2015].
22. otpbanka.hr, (2014). *OTP mobilno bankarstvo.* [online] Dostupno na: https://www.otpbanka.hr/html/g_otpdirekt_mb.htm [Pristupljeno 25. 8. 2015].
23. bks.hr, (2014). *BKS mobile.* [online] Dostupno na: http://www.bks.hr/BKSWebp/BKS/bks_hr/Gradanstvo/Racuni__karticno_poslovanje/BKS_mobile/index.jsp [Pristupljeno 25. 8. 2015].

24. hypo-alpe-adria.hr, (2014). *UPUTE ZA SIGURNO KORIŠTENJE.* [online] Dostupno na: http://www.hypo-alpe-adria.hr/home.nsf/r/Direktno_bankarstvo/$file/Upute_sigurno_koristenje_mobilno.pdf [Pristupljeno 25. 8. 2015].
25. jadranska-banka.hr, (2014). *JABAnet i mJABA PREPORUKE ZA SIGURNIJE KORIŠTENJE.* [online] Dostupno na: http://www.jadranska-banka.hr/css/upload/documents/Preporuke_za_sigurnije_kori%C5%A1tenje_JABAnet-a_i_mJABA-e.pdf [Pristupljeno 25. 8. 2015].
26. erstebank.hr, (2014). *Opći uvjeti korištenja Erste NetBanking, Erste mBanking i Erste FonBanking usluga za građane.* [online] Dostupno na: http://www.erstebank.hr/hr/Downloads/aa5e7708-0c6f-4a91-8fb8-5c388103e179/OpciUvjetiKoristenjaErsteNetBankingmBankingFonBankingUslugaZagradane.pdf [Pristupljeno 25. 8. 2015].
27. ibg.hpb.hr, (2014). *HPB mBanking Uputa za korisnike.* [online] Dostupno na: https://ibg.hpb.hr/download/uputa_mBanking.pdf [Pristupljeno 25. 8. 2015].
28. venetobanka.hr, (2014). *POSEBNI UVJETI KORIŠTENJA USLUGE MOBILNOG BANKARSTVA VENETO BANKE D.D.*. [online] Dostupno na: http://www.venetobanka.hr/fgs.axd?id=422 [Pristupljeno 25. 8. 2015].
29. Cox, C. (2009). *Trusted Service Manager: The Key to Accelerating Mobile Commerce*. [online] Dostupno na: http://www.firstdata.com/downloads/thought-leadership/fd_mobiletsm_whitepaper.pdf [Pristupljeno 28. 8. 2015].
30. Graves, J. (2013). SSL *Pinning for Increased App Security by Jay Graves of Double Encore.* [online] Possible Mobile. Dostupno na: https://possiblemobile.com/2013/03/ssl-pinning-for-increased-app-security/ [Pristupljeno 1. 9. 2015].