Sigurnost mobilnog poslovanja

Šalov-Tadić, Kristina

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

KRISTINA ŠALOV- TADIĆ

SIGURNOST MOBILNOG POSLOVANJA

Završni rad

Pula, rujan 2016. godine

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

KRISTINA ŠALOV- TADIĆ

SIGURNOST MOBILNOG POSLOVANJA

Završni rad

JMBAG: 0303046619, redoviti student

Studijski smjer: Sveučilišni preddiplomski studij Informatika

Predmet: Elektroničko poslovanje

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: prof. dr. sc. Vanja Bevanda

Pula, rujan 2016. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisana Kristina Šalov- Tadić, kandidat za prvostupnika Informatike 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

Kristina Šalov- Tadić

U Puli, rujan 2016. godine

IZJAVA

o korištenju autorskog djela

Ja, Kristina Šalov- Tadić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom

Sigurnost mobilnog poslovanja koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 20. rujan 2016.

Potpis

Kristina Šalov- Tadić

SADRŽAJ

1. UVOD

U zadnja dva desetljeća, mobilno računalstvo se brzo razvijalo. Tradicionalno, korisnici su morali pomoću svojih osobnih računala pokretati programe ili pristupati uslugama interneta. Računala su bila povezana preko žice s drugim uređajima, drugim računalima. Taj nedostatak mobilnosti znatno je ograničavao performanse ljudi u prodaji, usluge popravka, obrazovanje, provođenje zakona i slične poslove čiji rad se odvija izvan ureda.

Klasičan odlazak u banku, sve više zamjenjujemo koristeći mobilne aplikacije koje postaju sve popularnije i broj korisnika raste. Mobilno poslovanje obuhvaća korištenje mobilnih tehnologija u poslovne svrhe, sa ciljem što uspješnijeg obavljanja posla.

Bežična tehnologija omogućuje mobilno računalstvo i trgovinu kao izvorište velikih mogućnosti za poduzetnike.

Sigurnost predstavlja vjerojatno najvažniji zahtjev mobilnih aplikacija, jer bez sigurnosti i pouzdanosti sustava nema ni povjerenja korisnika.

U drugom poglavlju objašnjeno je mobilno poslovanje- poslovanje u pokretu i njihovi modeli.

Treće poglavlje objašnjava mobilno trgovanje.

Infrastruktura mobilnoga poslovanja i izvođenje transakcija obrađeni su u četvrtom poglavlju, a peto se bavi s pojmom mobilnog plaćanja i WAP terminom.

Na kraju u poglavlju šest bavimo se temeljnim pojmovima rizika i sigurnosti te završava s primjerom mobilnog bankarstva sa sedmim poglavljem.

2. MOBILNO POSLOVANJE- POSLOVANJE U POKRETU

E-poslovanje je oblik organizacije koji podrazumijeva primjenu informatičke, tj. internetske tehnologije. Predstavlja najsuvremeniji oblik organizacije poslovanja kojim teže sva poduzeća kako bi osvojila što bolju tržišnu poziciju i intenzivno ulagala u razvojne poslovne aktivnosti. „Elektroničko trgovanje uključuje razmjenu dobara i usluga između kupaca, poslovnih partnera i prodavatelja. Primjerice, dobavljač integrira s proizvođačem, kupci s prodavačima, a otpremnici (špediteri) s distributerima. Elektroničko poslovanje čine svi ti elementi, ali i operacije što se obavljaju unutar same tvrtke. Takve su operacije, primjerice, upravljanje proizvodnjom, razvojem, korporacijskom infrastrukturom i proizvodima.“[1]

Moguće je plaćati račune, izdavati naloge za plaćanje, općenito upravljati svojom imovinom preko mobilnih transakcija.

Prema Panianu e-poslovanje se dijeli na e-trgovanje, online prodaju dobara i usluga, zabavu i rekreaciju, e-bankarstvo i online financijske transakcije te e-izdavaštvo i nakladništvo.

Aktivnosti e-trgovanja nisu proizvodnja već ponuda potrošačima onoga što je proizvedeno ili ono što kao uslugu nude drugi. Zato je njegovo web mjesto daleko više usmjereno na tržište, na potrošače i konkurenciju. E-trgovci prodaju robu i usluge iz većeg broja izvora i zato njihovo web mjesto mora imati raznolike oblike komunikacije, a funkcionalnost mora moći brzo reagirati, ne samo na promjene na tržištu prodaje već i na tržištu nabave.

Prema australskom znanstveniku Richi Nayak m-poslovanje je definirano kao: "Mobilno se poslovanje može definirati kao korištenje mobilnih tehnologija u razmjeni dobara, usluga, informacija i znanja. M-poslovanje je izvršavanje transakcija obavljanih pomoću pokretne opreme putem mobilnih mreža koje mogu biti bežične i javne birane mreže. M-poslovanje uključuje širok spektar poslovnih aktivnosti u okruženju poslovanja tvrtke s krajnjim korisnicima (B2C) i među tvrtkama (B2B)."[2]

Da bi povezali pokretnu tehnologiju i uklopili je u elektroničko poslovanje moramo prilagoditi primjenu aplikacije mogućnostima pokretnih uređaja. To znači da je količina

[1] Panian Ž., *Izazovi elektroničkog poslovanja*, Zagreb, Narodne novine d.d., 2002., str.71.
[2] Panian, Ž., *Elektroničko poslovanje druge generacije*, Ekonomski fakultet Zagreb, trg J. F. Kennedyja 6 Zagreb, 2013., str. 125.

informacija koje se mogu prikazati na mobilnom uređaju manja te ima manje funkcionalnosti za razliku od stacionarnih informatičkih uređaja. Zatim se mora stvoriti kultura pokretljivosti u poduzeću- u malim zemljama kultura prostorne pokretljivosti je manja nego u više razvijenim zemljama no postupak globalizacije i to polako miče. Isto tako, usluga ugradnje glasovnih aplikacija i ugradnja te usluge u portfelj e-poslovanja može puno pridonijeti kvaliteti i uspješnoj primjeni e-poslova. Iako se e-poslovanje većinom odvija virtualno, potrebno je imati dio na stvarnoj konkretnoj zemljopisnoj lokaciji. Te lokacije ovise o poslu kojim se bavimo. Najbitnija stvar je posvetiti se problemu sigurnosti podataka ali ne smijemo zaboraviti ni sigurnost svih sudionika u e-poslovanju.

Postoji više modela mobilnog poslovanja. Oni se koriste za kupnju i plaćanje u pokretu. To su modeli korisničkih troškova, trgovački model, marketing poslovni model, poslovni model poboljšanja efektivnosti, oglašavači modeli i modeli dijeljenja prihoda.

MODELI KORISNIČKIH TROŠKOVA

Imamo dvije vrste tog modela: pretplata i korištenje gdje se usluga naplaćuje ovisno o korištenju. Ovaj model nerijetko uključuje i treću stranu koja može biti pružatelj usluge naplate ili mreža operatora koja naplaćuje nastale troškove.

TRGOVAČKI MODELI

Ponašaju se kao umreženi e-veletrgovci, služe se s drugim distribucijskim kanalima kao što su Amazon i eBay.

MARKETING POSLOVNI MODEL

Marketinški kanal i prisutnost su osnovna aktivnost, mobilni Internet je u današnjici osnovni prodajni kanal.

POSLOVNI MODEL POBOLJŠANJA EFEKTIVNOSTI

Pomaže u rezanju troškova i koristi se u mobilnom bankarstvu i za prodaju ulaznica. Smanjuje operacijske troškove kao što su troškovi uredskog osoblja, pozivni centri…

OGLAŠAVAČI MODELI

Plaća se temeljem broja prikaza (traffic-per Fees) ili temeljem klika i poziva (click-throughts or call-throughts). Ista je cijena prikaza oglasa u jednom razdoblju.

MODELI DIJELJENJA PRIHODA

Nastaje između kompanija poslovnih partnera. Prikuplja plaćanja korisnika i spaja različite korisnike uključene u isporuku usluge (prikaz stanja na cestama s vremenom i vijesti…).

3. MOBILNA TRGOVINA

Definicija mobilne trgovine (eng. mobile commerce) predstavlja transakciju novčane vrijednosti koja je realizirana preko mobilne telekomunikacijske mreže. U skladu s ovom definicijom, m-Commerce predstavlja podskup svih E-commerce transakcija, kako u B2C (business-to-customer), tako i u B2B (business-to-business) dijelu. Mobilni telefoni predstavljaju prvu točku pristupa Internetu.

Danas većina istraživanja m-Commerce sustava predviđa uspješnu budućnost, s vjerojatnošću da taj model trgovine postane i dominantan na nekim nacionalnim i regionalnim tržištima.

Mobilna trgovina koristi prednosti mobilnih uređaja i tehnologiju za bežični prijenos podataka, za poslovanje na Internetu. Mobilna mreža, Wi-Fi i bežična mreža koriste komunikacijske protokole i dostupne resurse kako bi povezali mobilne korisnike na Internet. Najveća prednost m-trgovine jest siguran pristup Internetu s bilo kojeg mjesta u bilo koje vrijeme korištenjem bežičnim mobilnim uređajima.

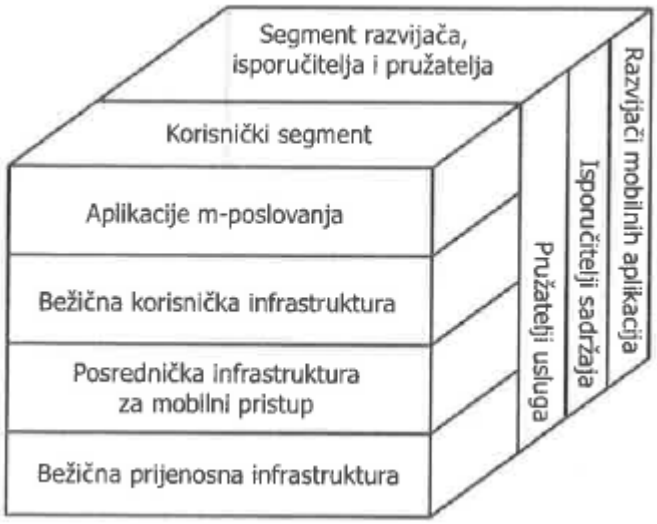
Danas, najveće platforme za razvoj m-poslovanja su iPhone (iza kojega stoji Apple) i Android (Google). Većina kompanija u svijetu ima prilagođene svoje stranice za mobilne telefone (Amazon, e-bay…) te tako omogućavaju i trgovinu.

Osim toga prisutne su i bankarske usluge, praćenje vijesti, plaćanje usluga (parking), on-line trgovina i sl.

4. INFRASTRUKTURA MOBILNOG POSLOVANJA

Prema Panianu, organizacijski okvir sustava poslovanja u pokretu čine četiri dijela: aplikacije za poslovanje u pokretu, posrednička infrastruktura za mobilni pristup, te bežična korisnička i prijenosna (mrežna) infrastruktura. Uz takav organizacijski okvir sama tvrtka ne mora sama raditi na uspostavi svih komponenti sustava, već ga može raditi služeći se funkcionalnostima i uslugama koje pruža netko drugi. On može biti isporučitelj sadržaja, pružati mobilne usluge ili pak kreirati mobilnu aplikaciju.

Isporučitelj sadržaja gradi svoje usluge koristeći aplikacije upotrebom više kreatora aplikacija, a vlastiti sadržaj agregira iz sadržaja drugih isporučitelja sadržaja. Taj se sadržaj dostavi operatoru mreže ili pružatelju mobilnih usluga. Pružatelji mobilnih usluga mogu biti i agregatori sadržaja, ali najčešće ne kao i kreatori mobilnih aplikacija ili isporučitelji sadržaja jer se koncentriraju na uslužne i mrežne aspekte mobilnih poslovanja.



Slika 1 Organizacijski okvir sustava poslovanja u pokretu

Izvor: Panian, Ž. „Elektroničko poslovanje druge generacije“

Operatori bežičnih mreža mogu imati aktivnu ulogu u aplikaciji i usluzi mobilnog poslovanja jer korisnik putuje kroz njihovu mrežu kad obavlja sve transakcije u mobilnom poslovanju. Korisnik očekuje kvalitetu usluga kako pri prijenosu glasa, tako i podataka i usluga pri mobilnom poslovanju gdje im se nudi široko područje za djelovanje i zaradu.

Da bi mogli razumjeti kako funkcionira sustav poslovanja u pokretu, prvo je potrebno objasniti ukratko četiri faze životnog ciklusa sustava poslovanja u pokretu. To se su faza inicijalizacije, faza ekspanzije, faza konsolidacije i na kraju faza zrelosti.

Faza inicijalizacije ili pokretanje razvojnog projekta započinje idejom o razvoju aplikacije. To je faza gdje se razmišlja, proučava literatura, istražuje tržište i Internet, odvija se konzultacija sa suradnicima i moguće i krajnjim korisnicima i provjera da li već nešto slično našoj ideji postoji. Ideja se razrađuje do detalja, obavlja se detaljna analiza funkcionalnosti buduće aplikacije ili usluge, od raznih tržišnih analiza do analiza troškova i koristi tj. moguće ostvarive dobiti. U najmanju ruku potrebno je izraditi stopu povrata ulaganja (ROI[3]) i ukupne troškove posjedovanja (TCO) od učinaka izrade projekta.

Druga faza ili faza ekspanzije dovodi do naglog rasta sustava. U izradi mobilne aplikacije najviše se vremena programira. Aplikacija se može programirati pomoću više jezika i platformi, ovisno o tome za koje je okružje namijenjena. Ta faza kratko traje.

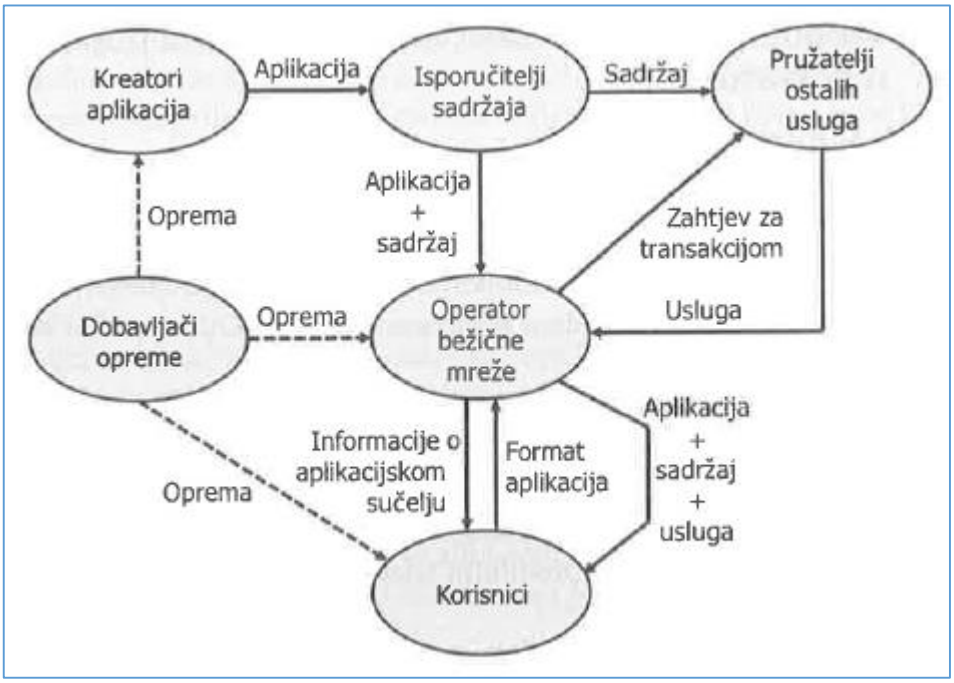
Faza konsolidacije ili faza sazrijevanja uključuje aktivnost testiranja i verifikacije razvijene aplikacije. Ta se faza bavi ispravkom određenih grešaka ili ispravljanjem nedostataka. Da bi aplikacija s greškama izašla u upotrebu, ne bi uzrokovala samo dodatne troškove zbog obveze otklanjanja grešaka već i gubitak ugleda među korisnicima, što uglavnom dovodi do većih gubitaka nego što iznose izravni troškovi koje mora snositi.

Na kraju imamo fazu zrelosti koja je zapravo faza eksploatacije ili možemo još je nazvati i fazom uporabe sustava. To je faza rutinskog korištenja sustava mobilnog poslovanja.

Prije ulaska u fazu eksploatacije sustava, isporučitelji opreme isporučuju svu potrebnu opremu kreatorima aplikacija, mrežnim operaterima i krajnjim korisnicima. U fazi eksploatacije ta se oprema može mijenjati, nadograđivati, nadopunjavati i modificirati. Kreatori aplikacije razvijaju aplikaciju i šalje je isporučitelju sadržaja koji je puni sadržajem i šalje bežičnom mrežnom operatoru. Taj sadržaj isporučitelj sadržaja može isporučiti pružatelju drugih dodatnih mrežnih usluga koji na to uzvrati uslugom. Da bi

[3] ROI (return on investment) je povrat od uloženog ukupnog kapitala, pokazatelj rentabilnosti odnosno profitabilnosti uloženog kapitala ili investicije. Dobiva se tako da se u brojniku koristi neka od veličina koje odražavaju povrat (neto dobitak, bruto dobitak, neto ili bruto dobitak uvećan za iznos plaćenih kamata) i podijeli s vrijednošću ukupnog kapitala te se pomnoži sa 100.

aplikacija uopće mogla biti isporučena s odgovarajućim sadržajem, operator bežične mreže šalje korisniku informaciju o sučelju preko koje će korisnik primiti završenu aplikaciju. Ciklus završava s isporukom mrežnog operatora aplikacije korisniku s cijelim sadržajem sa svim dodatnim uslugama. Zatim korisnik može tražiti novi proces, s drugim sadržajima i uslugama u nekom drugom formatu.



Slika 2 Sustav poslovanja u pokretu

Izvor: Panian, Ž. „Elektroničko poslovanje druge generacije“

Tehnička infrastruktura mobilnog poslovanja omogućuje obradu podataka u bežičnom mobilnom okruženju (engl. wireless mobile computing). To je način obrade podataka koji spaja mobilni uređaj s mrežom ili drugim uređajima za obrađivanje podataka u bilo koje vrijeme, s bilo kojeg mjesta.

Temeljna infrastruktura mobilnog poslovanja jesu mobilni uređaji, mobilni operativni sustavi, softver i bežične mreže.

Mobilnost je počela kada su računala postala prenosiva. Prvi mobilni uređaji su bili malo manji od desktop računala. No i dalje su bili teški i nezgrapni. Prijenosna računala su puno lakša i praktičnija. Na raspolaganju imamo dlanovnik, pametne telefone (smartphone), razne tablet uređaje…

U nastavku objašnjeni su najčešće korišteni uređaji.

Dlanovnik (personal digital assistant- PDA) je ručno računalo koje se uglavnom koristi za upravljanje osobnim informacijama.

Slika 3 Dlanovnik

Izvor: http://dayintechhistory.com/wp-content/uploads/2013/01/HP_PDA1-300x300.jpg

Pametni telefon (smartphone) mobilni telefon koji ima mogućnosti slične osobnom računalu. Prvi pametni mobilni telefon izrađen je sredinom 1970-ih, Motorola.

Od tada, mobilni telefoni su od velikih, jednostavnih uređaja koji se koriste za dvosmjernu komunikaciju, došli kao mali, ali moćni umreženi aparati. Značajke su višezadaćne (multitasking) funkcije, pristup internetu preko Wi-Fi ili 3G mreže (danas imamo i 4G mrežu), razni izbor multimedijskih funkcija (kamera i player videozapisa ili glazbe), kalendar, upravljanje kontaktima, GPS navigacija i mogućnost čitanja raznih dokumenata u više formata kao što je PDF ili Microsoft Office. 2000.g započinje masovna upotreba pametnih telefona popularizacijom iPhone uređaja, i uređaja koji podržavaju Android operativni sustav.

Slika 4 Smartphone nekad i danas

Izvor: http://i.dailymail.co.uk/i/pix/2011/05/03/article-1383133-0BDEBFD000000578-685_468x546.jpg, http://howng.com/wp-content/uploads/2015/10/ngrvanguard.com_.jpg

Tablet je mobilni uređaj s ekranom, sklopovima i baterijom u jednoj cjelini; obično je opremljen kamerom, mikrofonom i ekranom osjetljivim na dodir i obično je veći od dlanovnika i smartphonea.

Slika 5 Tablet

Izvor: http://fotos.pccomponentes.com/ipad/tablets_ipad/apple_ipad_mini_16gb_blanco.jpg

Pojam tablet je postao sinonim za uređaje kao što su Apple iPad, koji koriste zaslon osjetljiv na dodir ili olovku umjesto klasične tipkovnice.

Prema autorima Turban, Volonino i Wood postoje tri dominantna operativna sustava: Microsoft Windows, Apple, i Linux. Programeri koji pišu aplikacije ciljaju jedan ili više od ovih platformi za njihove programe. Pisanje aplikacije za mobilne uređaje je teže zbog više različitih uređaja i operacijskih sustava.

Android OS je od 2005. godine u većinskom vlasništvu Googlea a 2007. godine razvija ga Open Handset Alliance organizacija koja je sastavljena od 78 kompanija. Android OS je najpopularniji operativni sustav s 46 posto globalnog tržišnog udjela (Nielsen, 2012.). Kao što je Apple iOS, njegova uporaba nije ograničena samo na pametnim telefonima; može se naći na tablet uređajima i e-čitačima. Prvi uređaj na tržištu s Android operacijskim sustavom je bio HTC Dream.

Slika 6 Android OS logo

Izvor: http://www.androidphons.com/wp-content/uploads/2013/07/Android-OS.jpg

iOS (Apple, Inc.) nazivan i kao iPhone OS, ova inovativna platforma je često zaslužna za veći rast u svijetu smartphonea. iOS koristi Appleov iPhone, iPod Touch i iPad i Apple TV.

Slika 7 iOS logo

Izvor: https://s-media-cacheak0.pinimg.com/236x/ee/22/f9/ee22f97addbb92a5eae941e95b18696b.jpg

Ti uređaji su među prvima počeli koristiti zaslon osjetljiv na dodir, koji se sada nalazi i na uređajima drugih proizvođača. IOS je drugi najveći popularni mobilni OS na globalnoj razini, što čini oko 19 posto tržišta (Canalys, 2012.).

Ostali mobilni operacijski sustavi poput Windows Mobile (Microsoft), Palm (Palm, Inc), the Bada (Samsung) imaju samo mali dio globalnog tržišta. Potrošači očekuju da imaju pristup web-mjestima sa svojim pametnim telefonom i drugim uređajem i frustrirani su kada tvrtke nemaju web stranice koje su u skladu s njihovim uređajima, operacijskim sustavima i mobilnom konfiguracijom preglednika.

Slika 8 the Bada, Palm, Windows Mobile logo

Izvor: https://upload.wikimedia.org/wikipedia/commons/1/17/Bada_logo_1.png, http://www.scripophily.com/webcart/vigs/palmvig.jpg, http://www.geek.com/wp-content/uploads/2009/09/windows_mobile_vista_v_web.jpg

To predstavlja poseban izazov za programere, jer sada oni moraju dizajnirati web stranice s više konfiguracija. Ako tvrtka ne može razvijati mobilne mjesta za sve moguće konfiguracije, onda će ciljati najdominantnije platforme.

Developeri se suočavaju s izazovom da se njihova mobilna web stranica prikazuje ispravno u različitim mobilnim preglednicima.

4.1. IZVOĐENJE TRANSAKCIJA

Mobilno bankarstvo je financijski servis banke koji omogućava korisniku osobno i izravno obavljanje i pregledavanje financijskih transakcija i stanja na računu, koristeći se Internetom kao kanalom distribucije za izvršavanje bankarskih aktivnosti.

Prije samog korištenja usluga internetskog bankarstva ili obavljanja transakcija potrebno je izvršiti postupak autorizacije[4]. Privatni korisnici u pravilu imaju TAN-ove ili token, a pravni koriste smart-kartice. Razne banke nekada nude izbor između tih metoda.

Token nalikuje na džepni kalkulator, takav uređaj se daje klijentu na privremeno korištenje kada se registrira na uslugu Internet bankarstva. Prestankom korištenja usluge klijent se obvezuje vratiti uređaj u banku u kojoj je imao uslugu.

Slika 9 Token OTP banke

Izvor: https://elementa.otpbanka.hr/gradjani/upute/tokenotp.jpg

Tipke na tokenu omogućavaju korisniku unos PIN-a (Personal Identification Number) koji je važan za aktivaciju tokena. PIN sadržava 4-8 znamenaka koje dodjeljuje banka. Naravno, korisnik nakon prvog korištenja tokena ima mogućnost promjene PIN-a za otključavanje tokena. Kad završi postupak autorizacije generira se niz slučajnih brojeva koji se sa serijskim brojem tokena unosi u aplikaciju. Svaki token ima jedinstveni serijski broj koji je dio kriptografskog ključa koji omogućava generiranje koda za pristup mreži.

[4] Autorizacija- automatizirani proces kojim izdavatelj kartice (banka) odobrava financijsku transakciju korisnika kartice

Pri validaciji[5] i autorizaciji podataka poslužitelj generira brojčanu vrijednost koja se sastoji od šest znamenaka. Znamenke se dobiju iz datuma, vremena izvođenja transakcije i novčane vrijednosti transakcije. Da bi transakcija uspješno se izvršila, korisnik mora taj dobiveni broj unijeti u token koji zatim generira novi broj (i on se sastoji od šest brojeva) koji se koristi samo za izvođenje trenutne transakcije. Taj je broj generiran za jednu upotrebu, dakle ne postoji vjerojatnost ponavljanja jednog generiranog niza. Korisnik ima vrlo malo vremena u kojem mora upisati generirani niz. To traje 30-60 sekundi nakon čega se token automatski isključuje.

Takva vrsta autorizacije se sastoji od dva faktora (niza brojeva koje token generira i serijskog broja tokena) i omogućuje računalu u banci da identificira klijenta te mu osigura pristup svim njegovim računima. Sigurnosni mehanizam ugrađen u token je u skladu s poslužiteljem koji provjerava da li je korisnik taj koji se predstavlja. Ako se upiše neispravan PIN nekoliko puta, najčešće je to tri puta za redom, token se automatski zaključa. Administrator, odnosno banka, je jedina ovlaštena i autorizirana osoba za otključavanje uređaja. Ako se unese neispravan kod za autorizaciju korisnika, web aplikacija se zaustavlja. Svaki se takav pokušaj zabilježava na poslužitelju. Administrator tako može uočiti sumnjive radnje kod autorizacije.

Autorizacija s TAN-ovima najčešće podrazumijeva list papira s pedesetak ili stotinjak nizova znamenaka koje klijent dobiva od banke. Nakon što klijent iskoristi nizove s liste, banka mu pošalje novu listu. Neke banke daju karticu s više brojeva TAN-ova koje korisnik koristi u krug pa nema potrebe za slanjem novih TAN-ova. TAN-ovi nalikuju na telefonske brojeve te je tako manja zloupotreba ako se TAN ukrade ili provali. Najveća prednost ove vrste autorizacije jest nenošenje uređaja za obavljanje bankarskih transakcija. Korisnik može uvijek imati nekoliko TAN-ova ako dođe do potrebe za izvršavanjem transakcije. Mana TAN-ova je velika administracija. Banka mora čuvati u bazi popis TAN-ova svih svojih klijenata, i starih i novih.

Smart-kartica je kartica koja sadrži memorijski čip s ne programskom logikom ili mikroprocesor i memorijski čip. Kartica koja sadrži mikroprocesor ima opcije upisivanja podataka, brisanja ili neke druge vrste manipulacije podacima. Kartica koja ima samo memorijski čip izvodi samo predefinirane funkcije. Smart-kartice sadrže sve potrebne funkcije i informacije potrebne za autorizaciju, zato u trenutku transakcije nije potreban

[5] Validacija- potvrda, ovjera

pristup udaljenim bazama podataka. Da bi ih mogli koristiti, potreban je čitač smart-kartica koji mora biti instaliran na računalu. Čitač i softver potreban za instalaciju čitača na računalo, korisnik kupuje od banke prilikom registracije na uslugu.

Kartica je temeljena na PKI (Public Key Infrastructure) tehnologiji koja je zasnovana na asimetričnoj kriptografiji, tj. na paru javnih i tajnih ključeva za šifriranje podataka. Svaki korisnik ima svoj javni ključ i tajni ključ. Javni ključ korisnika je dostupan drugima na uvid. Korisnik podatke koje šalje nekome šifrira svojim tajnim ključem. Kada bi se takvi podaci slali, pročitao bi ih svatko tko posjeduje javni ključ pošiljatelja. Zato pošiljatelj šifrira podatke još jednom, javnim ključem onoga tko podatke prima. Tako su podaci vidljivi samo primatelju. Primatelj ih dešifrira prvo pošiljateljevim javnim ključem, a zatim i svojim tajnim ključem. I javni i tajni ključ je u digitalnom obliku pohranjen na smart-kartici.

Slika 10 Smart-kartice

Izvor: http://www.jatrgovac.com/usdocs/kartice-visa-mastercard-midi.jpg

Najčešće primjene smart-kartice su za Internet bankarstvo, kreditne kartice, kod mobilnih uređaja na karticu, elektroničke kartice, kao identifikacije u vladinim institucijama, kod bežične komunikacije, kod kodiranih satelitskih programa i kod računalnih sigurnosnih sustava.

5. TEMELJNI POJMOVI RIZIKA I SIGURNOSTI

Poslovanje u pokretu nije moguće bez sigurne okoline u kojoj će se održavati a posebno u slučaju mobilnih transakcija. Na sigurnost može se gledati s više strana. Kao prvo, moramo osigurati da povjerljivi korisnički podaci na mobilnom telefonu kao i sam telefon budu zaštićeni od neovlaštenog korištenja. Sigurnosni mehanizam uključuje autentifikaciju korisnika, kao što je autentifikacija PIN-a ili lozinke. Također podatke moramo pohraniti na sigurno mjesto koje može biti SIM kartica mobilnog telefona. I sam operacijski sustav treba biti siguran.

Zatim osobni korisnički podaci trebaju biti zaštićeni od krađe. Dakle, pristup telekomunikacijskoj mreži osigurava zaštitu prenošenih podataka što obuhvaća povjerljivost, integritet i autentičnost. Otvara se pitanje sigurnosti korisničkih podataka u mreži kojoj se pristupa. Sama infrastruktura mrežnog operatera mora osigurati sigurno korektno obračunavanja i naplatu usluge. Aplikacije poslovanja u pokretu moraju biti osigurane kako s obzirom na klijente, tako i s obzirom na trgovce i mrežnog operatora. Uz samu autentičnost, bitna je povjerljivost i integritet poslanih informacija o plaćanju, te je isto tako bitna i neporecivost informacija koje šalje bilo koja strana bilo kojoj strani.

Bez obzira na sve pretpostavke koje pokretne tehnologije uvode u e-poslovanje, ono je komplicirano i traži veliki trud i veliki ulog sredstava kojima će ostvariti sljedeće poslovne koristi: povećava se prilagodljivost zaposlenih pri izvršavanju posla, manje je vrijeme reakcije na događaje unutar poduzeća, manje se čeka na odgovoru na upit i na zahtjev klijenata, poslovnih partnera i drugih, povećanje mogućnosti na vrijeme pružiti vremenski i lokacijski osjetljive podatke i informacije onima koji donose odluke i povećanje kvalitete usluga k klijentima.

Korištenje mobilnih tehnologija u e-poslovanju ima sljedeće prednosti. Mobilni uređaj je sveprisutan, pokretan, i to znači da pristupanje aplikaciji u pokretu može biti u stvarnom vremenu i s bilo kojeg mjesta. Korisnik je dostupan bilo gdje u bilo koje vrijeme. Možemo biti zadovoljni što je pokrivenost geografskih područja bežičnom i satelitskom mrežom danas u svijetu vrlo visoka, a s klasičnom kabelskim vezom i vezom preko žice nekad može biti često i nemoguće poslovati (primjerice u vozilu). Proizvođači su svjesni sigurnosnih rizika i u svoje proizvode uglavnom ugrade neke oblike osiguranja i zaštite. Ona osiguravaju neku razinu sigurnosti. Još jedna prednost m-poslovanja je da operator komunikacijske mreže može lokalizirati registrirane

korisnike pomoću sustava za pozicioniranje poput GPS i GSM. Korisnik uglavnom svoj mobilni telefon ne dijeli pa se tako uređaj personalizira, tj. prilagodi korisniku prema njegovim potrebama, željama, i mogućnostima. Isto tako i operater može ponuditi dodatne usluge ovisno o osobinama o lokaciji korisnika.

Mane m-poslovanja su u sposobnosti funkcionalnosti mobilnih uređaja u usporedbi sa stacionarnim gdje su u pravilu manje mogućnosti. Najbitnija je ona veličina ekrana koju stacionarni uređaji imaju veće nego mobilni uređaji. Ne rijetko su mobilni uređaji nestandardni s operacijskim sustavom i mrežnom tehnologijom koja je na raspolaganju na korištenje u poslovanju u pokretu i može biti poteškoća pri konfiguraciji sustava. Zato proizvođači nastoje surađivati s međunarodnom tijelima i drugim organizacijama koje se bave standardizacijom kako bi došli do općeprihvaćenih rješenja. Rezultati toga su da se većina današnjih mobilnih uređaja oslanja na skup IP protokola koji garantiraju standardnu mrežnu povezanost. Na aplikacijskom nivou Java Micro Edition, prije Micro Edition i Java 2 platforme, nudi platformu za heterogene mobilne uređaje. Mobilne je uređaje puno lakše uništiti ili ukrasti. Zbog sposobnosti da uređaj bude personaliziran potrebno ga je štititi u skladu s najvišim mogućim standardima što dovodi do povećanja troškova njihove nabave, korištenja i održavanja. Na kraju i bežična komunikacija stvara dodatni rizik koji se s nastankom novih tehnologija povećava i diverzificira[6].

RIZICI VEZANI ZA BEŽIČNO KORISNIČKO SUČELJE I POSREDNIČKI SOFTVER

Svaka malo sofisticiranija primjena jednostavnog prijenosnog uređaja zahtjeva i dodatne funkcionalnosti. To su dinamička, prilagodljiva i pametna korisnička sučelja koja uče od korisnika i s njim, mogućnost prihvaćanja korisničkih ulaza u različitim oblicima koji što je i glas, prikaz bogatih sadržaja koje možemo više puta upotrijebiti, mogućnost praćenja korisnika i proizvoda i uređaja kao i svijest o lokaciji, sučelje za pristup više različitih mreža, sigurnosne funkcije za obranu od zlođudnog koda i podrška autentifikaciji korisnika, usluga i aplikacija, rad s aplikacijama u pokretu i njenim raznim zahtjevima i prilagodbom tih aplikacija. Potrebna je podrška svijesti o sadržaju i prilagodbi aplikacije karakteristikama sadržaja, sposobnost otkriti i preuzeti

[6] Diverzifikacija- upotpunjavanje ili proširivanje prodajnog ili proizvodnog asortimana uključivanjem novih proizvoda i usluga koji se razlikuju od sadašnjih

unaprijeđenu ili proširenu aplikaciju s raznim zahtjevima, i imati operacijski sustav koji upravlja resursima za podršku mnogim različitim funkcijama.

RIZICI VEZANI UZ STRUKTURU BEŽIČNE MREŽE

Po Panianu, aplikacija poslovanja u pokretu postavlja pet zahtjeva koje korištene mreže moraju ispuniti. To su upravljanje lokacijama, mrežna ovisnost, podrška kvaliteti usluga, višestruko razašiljanje poruka i mogućnost povezivanja mreža. Više o tome u tablici broj 1.

Tablica 1 Zahtjevi pred infrastrukturom bežične mreže

Zahtjev	Atributi
upravljanje lokacijama	- mogućnosti praćenja korisnika - mogućnosti praćenja proizvoda - mogućnosti praćenja uređaja
podrška višestrukom razašiljanju poruka	- podrška višestrukom razašiljanju poruka korištenjem infrastrukture bežične mreže - podrška višestrukom razašiljanju poruka ad hoc bežičnim mrežama - grupna povezivost u uvjetima mobilnosti - sinkronizacija / atomarnost transakcija u kojima sudjeluje veći broj korisnika
mrežna ovisnost	- utjecaj i učestalost otkazivanja / kvara komponenata - dizajn otporan na pogreške - mogućnost pristupa korisnika većem broju mreža - razine raspoloživosti mreže
kvaliteta usluge	- zahtjevi glede širine pojasa - kašnjenje i varijacije kašnjenja - karakteristike gubitaka koje se mogu tolerirati
mogućnost povezivanja mreža (Roaming)	- mogućnosti slanja poruka kroz više mreža - praćenje korisnika kroz više mreža

Izvor: Panian, Ž. „Elektroničko poslovanje druge generacije“

RIZICI VEZANI UZ KREATORE APLIKACIJA I MREŽNE OPERATORE

Veći problemi s kojima se suočavaju kreatori aplikacija u poslovanju u pokretu su procesni i memorijski kapaciteti, razvoj u aplikacija, kompatibilnost i interoperabilnost, i poželjna obilježja. Detaljnije je objašnjeno u nastavku.

Tablica 2 Problemi kreatora aplikacija

Zahtjev	Komentar
procesni i memorijski kapaciteti	- širina pojasa i kašnjenje (za aplikacije u stvarnom vremenu i aplikacije izvan stvarnog vremena) - kapaciteti mobilnih uređaja - moguće operacije kada uređaji nisu priključeni na mrežu - višestruko razašiljanje poruka u grupnoj komunikaciji. - simetrična i asimetrična obrada i pohrana
razvoj aplikacija	- korištenje raspoloživih paketa za razvoj softvera (eng. Software Development Kit, SDK) - simulacija okruženja u kakvom će aplikacija biti korištena - maksimalan broj istovremenih korisnika - dimenzije aplikacijskog koda - podrška sigurnim transakcijama - podrška za fiksne korisnike
kompatibilnost i interoperabilnost	- neovisnost o tehnologijama bežičnog pristupa - neovisnost o funkcionalnostima i uređaja - interoperabilnost putem IP-a (akr. eng. Internet Protocol) - kompatibilnost s WAP-om (akr. eng. Wireless Aplication Protocol)
poželjna obilježja	- podrška povezivosti s prekidima - prilagodljivost korisničkom i mrežnom okruženju - podrška "atomarnim" transakcijama - jednostavna nadogradnja - dodavanje obilježja prema korisničkim specifikacijama

Izvor: Panian, Ž. „Elektroničko poslovanje druge generacije“

Dvije najznačajnije softverske platforme na kojima se rade servisi u mobilnom poslovanju su aplikacije zasnovane na SMS uslugama i aplikacije razvijene kao posebni softverski programi koje korisnici instaliraju u svoje mobilne aparate putem kojih se onda spajaju na mobilni internet preko svog poslužitelja.

5.1. **SMS POSLOVANJE**

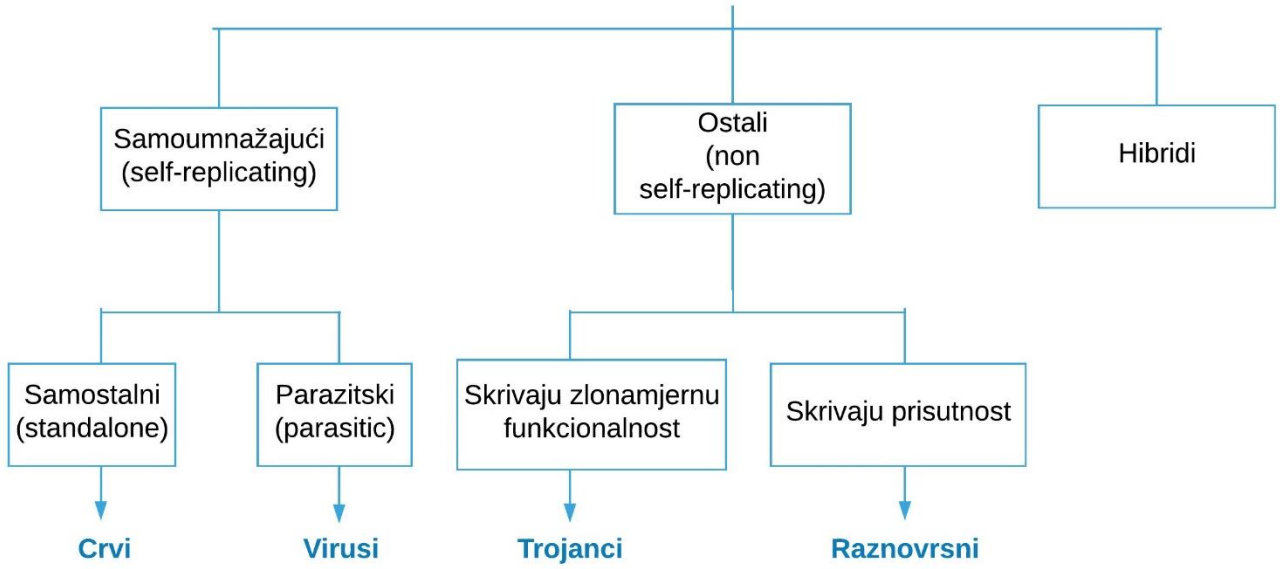
Davatelj usluga, dakle banka ili neki vanjski partner kojeg je banka odabrala mora da razvije SMS platformu koji bi svojim korisnicima omogućavala korištenje tog servisa. Klijenti željenu informaciju dobiju u određeno vrijeme ili na zahtjev, tako da su podržani pull i push modeli poslovanja. Pull model poslovanja je tehnologija u kojoj klijent potiče komunikaciju koristeći svoj telefon za poziv i traži podatke. Ti se podaci dovlače s aplikacijskog servera na mobilni uređaj. U push modelu poslovanja aplikacijski server ima veću kontrolu nad mobilnim uređajima. On donosi odluku kada će poslati podatke mobilnom uređaju, te za push tehnologiju nije potreban zahtjev korisnika. Usluga omogućava korisniku, u svakom trenutku:

- obavljanje transakcija, ali se plaćanja mogu činiti samo na unaprijed navedene račune
- provjeru stanja na računu, na zahtjev, dnevno ili po promjeni

5.2. **WAP POSLOVANJE**

WAP poslovanje je nastalo razvojem WAP standarda koji je omogućio pristup Internetu putem mobilnih uređaja. Korisnicima banke je omogućeno da pomoću mobilnog uređaja, a preko Interneta pristupe svom računu u banci. Putem mobilnog telefona koji u sebi ima ugrađen WAP uređaj ostvaruje se Veza s bankom. Da bi se WAP usluga mogla koristiti, korisnik mora imati mobilni uređaj koji podržava WAP. Pri tome korisnik plaća za ostvareni GPRS promet mobilnom operateru. WAP bankarstvo ima pristup bankarskim uslugama direktno putem mobilnog interneta ili indirektno posredstvom posebno instaliranog programa (aplikacije) u mobilnom uređaju putem kojeg se on spaja na mobilni internet.

Nastanak i razvitak zlonamjernih programa za mobilne platforme završio je kombiniranjem različitih trendova u razvoju mobilnih telefona. Jedan od njih je sam napredak u tehnici, tj. sam razvoj memorije, procesora i svih elemenata koji su ključni za svu veću funkcionalnost mobilnih uređaja. On je omogućio razvoj složenih zlonamjernih programa. Na mobilnim telefonima prvi operacijski sustavi bili su specifični, razlikovali su se od proizvođača do proizvođača pa i od uređaja do uređaja. Za razliku od njih, danas iste operacijske sustave za mobilne uređaje koriste različiti prodavači različitih uređaja. Baš zato, u kombinaciji sa sve većim funkcionalnostima takvih sustava, danas je moguće napisati zlonamjerni program za skup od više stotina tisuća žrtava.



Slika 11 Klasifikacija zlonamjernih programa za mobilne platforme

Izvor: security.LSS.hr- Zlonamjerni programi za mobilne platforme

Velik broj tehnologija, usluga i mogućnosti kao što su CDMA 2000 (Code Division Multiple Access), HSPA+, UMTS i dr. su sve dostupnije i pružaju adekvatnu podlogu za širenje zlonamjernih programa. Također, sama cijena tehnologije temeljena na Bluetooth tehnologiji sve je manja, pa i ona olakšava zlonamjernim programima lakše i brže širenje.

Veliki broj aplikacija kao što su igre i melodije zvona za mobilne telefone su prisutne od samog početka razvoja mobilnih telefona. Korisnici znaju kako ih naći i kako ih mogu preuzeti. Velik broj njih je dostupan relativno jednostavno i besplatno. Mogućnost da ćemo preuzeti igricu ili aplikaciju s ugrađenim zloćudnim kodovima sve su veće.

Kako bežične podatkovne mreže dobivaju na popularnosti korisnici danas često koriste svima dostupne usluge kao što su SMS i MMS, elektronička pošta, elektroničko bankarstvo i slično. Međutim korisnici nisu svjesni prijetnji i rizika koji postoje prilikom uporabe tih usluga. Korisnik zna da zlonamjerni program na osobnom računalu može izazvati slanje poruka elektroničke pošte sa zloćudnim sadržajem svim kontaktima iz imenika, no malo njih je svjesno činjenica da je isti scenarij mogući na njihovim mobilnim telefonima. Zato kada na svoj mobilni uređaj prime poruku koja sadrži sumnjivu poveznicu ili privitak često taj sadržaj pregledavaju ili preuzimaju bez provjere. Pošiljatelj zlonamjernih programa na mobilni uređaj baš računa na korisničku naivnost.

Zlonamjerni programi za korisnike pametnih telefona i tableta rastu velikom brzinom. Dijelimo ih na spyware i adware, trojanca, viruse, crve i hibride. Oni se uglavnom šire sinkronizacijom i dijeljenjem podataka, e-poštom, SMS i MMS porukama, bluetoothom i webom.

Spyware ili špijunski softver sakuplja privatne informacije o korisniku mobilnog telefona i njih šalje najčešće marketinškim tvrtkama koje se bave oglašavanjem pa zato ga i nazivamo adware (Zwinky, ErrorSafe, Gator i BonziBUDDY). Najčešće se nalazi u besplatnim aplikacijama tako da autori pokrivaju troškove izrade ali dolazi i s ograničeno djeljivim aplikacijama. Uglavnom se instalira na telefon bez znanja i pristanka korisnika, ponašajući se kao sasvim obična aplikacija i tako zarazi aplikaciju na uređaju. On iskorištava mobilnu povezanost kako bi sakupio korisnikove kontakte, navike slanja poruka, lokaciju i ostalo.

Trojanci su zloćudni programi koji se pretvara kao neki drugi program koji radi nešto zanimljivo i korisno. Izgleda bezopasno, no vrlo je opasan kada se pokrene. Trojanac se ne može izvršavati sam, već njegovo izvršavanje ovisi o postupcima žrtve. Čak i ako se i replicira i izvrši sam, svaka osoba mora sama pokrenuti trojanski program. On

izvodi razne aktivnosti kao što je krađa korisničkih lozinki, brojeva kreditne kartice i drugih privatnih informacija koje zatim šalje drugoj osobi.

Crv je lukav program koji se širi mrežom. Može biti mrežni ali može se bazirati na računalu korisnika. Također postoje oni koji završavaju svoj kod kada uspješno zaraze uređaj- rabbits. Mrežni crv ima više dijelova a svaki se dio nalazi na drugom uređaju. Kopiranjem određenog dijela se širi na druga računala. Međutim, najčešće se širi e-poštom. Da bi se pokrenuo može tražiti korisničku akciju ili se sam aktivira.

Novi programi za mobilne platforme sve su jači te jako dobro kombiniraju elemente nekih ili svih opisanih kategorija kako bi što bolje ispunili svoj zadatak (širenje, inficiranje, prikupljanje tajnih podataka, mobilni spam, onesposobljavanje antivirusne zaštite i ostalo). Isto tako, javljaju se i zlonamjerni programi koji prvo onesposobe antivirusnu zaštitu na mobilnim uređajima kako bi se mogli posvetiti svojoj pravoj namjeni.

Činjenica je kako je danas velik broj zlonamjernih programa sposoban izvršavati se i na mobilnim platformama i na osobnim računalima. Tako se prijetnje iz svijeta osobnih računala poput spywarea, adwarea i ostalih sele i u svijet mobilnih uređaja.

Sposobnost malicioznog programa da radi bez prestanka u pozadini korisnikovog mobilnog uređaja jedan je od najvažnijih dijelova njegovog razvoja. Što duže trojanac „živi“ na mobilnom uređaju, više novaca izvuče od korisnika. Na tome stvaratelji malicioznog softvera stalno rade, i na kraju dolazi do velikog broja tehnoloških inovacija. Što se više radi na kreiranju kompleksnih kodova, lakše će se sakriti i više će trebati antivirusnom programu da se maliciozan kod neutralizira.

Ranjivosti pametnih telefona se iskorištavaju na tri načina: zaobilaženja provjere integriteta koda kada se neka aplikacija instalira, povećavanje mogućnosti malicioznog softvera i njezino što teže uklanjanje. Također, sama verifikacija digitalnog potpisa se može izbjeći davanjem istoga imena malicioznoj datoteci kao i legalnoj datoteci i postavljajući je na isto mjesto. Sustav na uređaju potvrđuje digitalni potpis legalne datoteke kad vrši instalaciju malicioznog softvera.

Problem je da bi uklonili mane našeg pametnog telefona, moramo redovito ažurirati naš uređaj i prihvaćati nadogradnju od proizvođača. Korisnici to najčešće ne rade redovito, a ako nije uređaj ažuriran dulje vrijeme, vrlo vjerojatno da proizvođač i ne

pruža više zakrpe za maliciozne programe. Zato moramo koristiti antivirusne programe.

Kako se zaštititi

Da bi zaštitili svoje računalo nikad ne smijemo instalirati dodatan softver za bankarstvo osim onog koji nam je dala banka na početku. Moramo koristiti sigurno računalo, ne pristupati uslugama ako računalo koristi veći broj osoba. Također je potrebno redovito održavati računalo i koristiti antivirusnu zaštitu i Firewall kako bi se zaštitili od neovlaštene komunikacije.

Nikada ne otkrivati svoje podatke za pristup usluzi kao što su korisničko ime, zaporka, jednokratna zaporka ili broj kartice. Uvijek trebamo pristupati usluzi preko službene stranice banke. Ne pohranjivati povjerljive podatke na računalu.

Da smanjimo potencijalne opasnosti, potrebno se redovito informirati o potencijalnim prijetnjama na Anti-Botnet Nacionalnom centru podrške (http://www.antibot.hr/). Obavezno pripaziti na telefonske pozive i e-poštu koja navodno dolazi od banke. Nije naodmet podsjetiti na čestu provjeru svoga računa i provjeriti nalog za plaćanje prije potvrde transakcije- provjerite upisani iznos, poziv na broj i broj računa primatelja.

6. MOBILNO PLAĆANJE I WAP

Mobilno plaćanje je novi alternativni način plaćanja. Za razliku od plaćanja u gotovini, kreditnim karticama ili čekom, korisnicima je omogućeno da plaćaju razne usluge koristeći vlastiti mobilni uređaj. Npr. naplata prijevoza, parkinga, on-line igara…

Sustavi e-plaćanja ostvaruju mogućnost plaćanja dobara ili usluga preko Interneta. Kupac šalje prodavatelju podatke relevantne sa strane Interneta, a nije potrebno imati vanjsku interakciju poput fakture ili potvrda preko e-pošte. Do danas je razvijeno oko stotinu različitih sustava elektroničkih plaćanja.

Veliki broj sustava e-plaćanja nije prikladan u mobilnoj komunikacijskoj tehnologiji zbog ograničenja mobilnog uređaja i mobilnih komunikacija. Međutim možemo birati između raznih vrsta mobilnog plaćanja. To su telefonski brojevi s posebnim tarifama koji se upotrebljavaju za plaćanje na velikim udaljenostima, ima iznose koji se dodaju računu da bi koristili mobilni telefon i ponekad nude i popuste prema unaprijed određenim planovima. Zatim imamo kreditne kartice a neki pružatelji usluga omogućuju da se kreditna kartica poveže sa SIM karticom korisnikova mobilnog telefona. Ponuđena nam je i usluga mobilnih mikro plaćanja kao i vrijednosne kartice za plaćanje digitalnih sadržaja poput aplikacije za mobilni telefon i glazbe.

Postoji tri načina e-plaćanja. To su softverski elektronički žetoni, hardverski elektronički žetoni i pozadinski računi. Softverski elektronički žetona monetarna je vrijednost pohranjena u mobilnom telefonu tako da klijent ima potpunu kontrolu nad svojim novcem di god bio.

Elektronički žeton je datoteka u kojoj je pohranjena informacija o iznosu novca koji posjedujemo, rok valjanosti i elektronički potpis banke koja je izdala taj žeton. Kako je žeton lako kopirati njegova sigurnost je označena serijskim brojem. Korisnik daje žeton prodavatelju koji ga onda šalje banci koja ga je izdala da bi ona provela test dvostrukog trošenja. Ako je žeton već potrošen transakcija se odbija. U suprotnom, njegov serijski broj se unosi u bazu podataka i novac se prenosi na račun prodavatelja.

Ako je riječ o hardverskim elektroničkim žetonima monetarna vrijednost je spremljena hardverskom elementu. To je najčešće memorija pametne kartice tj. u mobilnom uređaju. Kako bi razmijenili novac klijenti pametne kartice i prodavateljev poslužitelj se međusobno autentificiraju pa se između njih stvara siguran komunikacijski kanal. Zatim

slijedi transfer novca od klijenata k prodavatelju. To je dobar pristup jer se te kartice mogu koristiti i na e-blagajni.

Treći način je pohrana novca na udaljenom računu. Taj račun može biti račun kreditne kartice, vrsta računa kod banke ili račun koji održava mrežni operator.

Funkcionira isto kao i prethodni računi. Po primitku računa za kupljenu robu ili uslugu, klijent šalje prodavatelju autentifikacijsku i autorizaciju poruku koji omogućava trećoj strani identifikaciju klijenata i verifikaciju autorizacije plaćanja. Zatim se obavlja transakcija.

Razlike su u trećoj povjerljivih strani i načinu slanja autentifikacijskih i autorizacijskih podataka. U nekim se slučajevima podaci šalju u nezaštićenom obliku i dok se drugi podvrgnu enkripciji.

Najvažniji dio plaćanja u pokretu je standardizacija. Radi tehnologija na koju se oslanjaju mobilni uređaji i radi nužnosti prijenosa podataka i izvršenja transakcija plaćanja bežičnim putem važno je naći i primijeniti pristup koji će biti isti i na nacionalnoj i međunarodnoj razini.

S tim se pitanjima bave Mobile Payment Forum, svjetska organizacija koja se bavi razvojem okvira za standardizirano, sigurno i autentificirano poslovanje u pokretu pri plaćanju putem kreditnim karticama.

PayCircle je nezavisna neprofitna organizacija kojoj je zadatak unaprijediti tehnologiju mobilnog plaćanja i razvitak i potpora za usvajanje novih sučelja za mobilna plaćanja bazirana na XML-u, SOAP-u, Javi i drugim jezicima i alatima.

mSign je konzorcij za elektroničke potpise, skup kompanija i organizacija iz mobilne telefonije i Interneta čiji je zadatak razvoj i uspostava sigurne među aplikacijske infrastrukture za korištenje mobilnih digitalnih potpisa.

Imamo još i Mobile Wireless Internet Forum, međunarodnu neprofitnu organizaciju koja radi na tome da se što više prihvati jedinstvena otvorena mobilna bežična i internetska arhitektura koja nije ovisna o tehnologiji pristupa.

Mobilni uređaji moraju imati pretraživački softver koji čita WML (Wireless Mark-Up Language) s nekog od poslužitelja na mreži globalnog sustava za mobilne komunikacije, GSM. Osim WML, postoji još i HDML (Handheld Device Markup

Language) koji nije baziran na XML-u. On također služi za pregledavanje teksta na Web-u pomoću bežičnih uređaja.

„WAP standard definira otvorenu, standardnu arhitekturu i protokole koji omogućuju pristup Internetu iz mobilne mreže. Međunarodna organizacija zadužena za stvaranje i razvoj WAP standarda naziva se WAP forum, a nastala je 1997. godine na inicijativu Ericssona, Motorole, Unwired Planeta i Nokie. Trenutačno odobrena verzija standarda je WAP 1.2.“[7]

[7] Izvor: http://www.ericsson.hr/etk/revija/Br_2_2001/wap.htm (pristupano 23.7.16.)

7. PRIMJERI

7.1. M-BANKING OTP BANKE

Usluga OTP m-bankarstvo omogućuje upravljanje vlastitim financijama bilo kad i na bilo kojem mjestu. Aplikacija se može instalirati na operativnim sustavima iOS i Android mobilne telefone.

Funkcionalnosti koji mogu biti otvoreni dio aplikacije[8] su uvid u važeću tečajnu listu i arhivu tečajnih lista, navigacija k najbližoj banci ili OTP bankomatu, demo verzija aplikacije i prijava u OTP direkt.

Sve što je potrebno za ugovaranje ove usluge je popuniti zahtjev te ga dostaviti u najbližu poslovnicu OTP banke i moramo biti klijent OTP banke.

Aplikacija se aktivira s odobravanjem zahtjeva, kada dobijemo putem SMS poruke na mobilni uređaj link za preuzimanje aplikacije te zaporku koja je potrebna za njenu aktivaciju. Nakon preuzimanja, pomoću jednostavnih uputa preuzimamo i pokrećemo aplikaciju. Kad pokrećemo aplikaciju moramo upisati točan PIN i potvrditi točnu asocijacijsku sliku (zastavu), a ako tri puta pogriješimo aplikacija se blokira.

Kada se prijavimo u aplikaciju nude nam se sljedeće opcije: razni pregledi po prometnim i štednim računima, financijske transakcije.

Slika 12 Početna strana i glavni izbornik OTP m-bankarstva

Izvor: https://play.google.com/store/apps/details?id=hr.asseco.android.jimba.otp.hr&hl=hr

Usluge koje su omogućene OTP m-bankarstvom su zadavanje kunskih platnih naloga u i izvan OTP banke (uz mogućnost najave), zadavanje naloga internih prijenosa, kupnja i prodaja valute, prijenos na MasterCard contactless prepaid karticu, Visa web prepaid karticu i na račun revolving kartice, plaćanje skeniranjem 2D bar koda s uplatnice, pohrana i ažuriranje internih prinosa i predložaka platnih naloga, pregled

[8] Otvoreni dio aplikacije- dio aplikacije koji je u funkciji neposredno po preuzimanju i aktiviranju aplikacije bez prijave korisnika

zadanih naloga po statusu i željenom periodu, pregled prometa računa i podataka o računima, pregled detalja bankovnih kartica i prometa računa bankovnih kartica, aktivne štednje, aktivnih kredita, stanja udjela u investicijskim fondovima, aktivnih trajnih naloga, kalkulator kredita, valuta i depozitni kalkulator, slanje potvrde plaćanja na e-mail adresu, poštanski pretinac (mailbox) i razne korisne informacije i automatske poveznice.

Aplikacija OTP m-bankarstvo za iOS i Android platforme mobilnih telefona je zaštićena osobnim PIN-om i on je poznat samo vlasniku mobilnog uređaja, te s ostalim ugrađenim sigurnosnim mehanizmima omogućuje apsolutnu sigurnost korisnika u slučaju krađe ili gubitka mobilnog telefona. Svi podaci u vezi računa i PIN ne spremaju se u mobilni telefon, i tako je osigurana tajnost naših podataka. Aplikacija se automatski gasi ako se ne koristi nakon 3 minute te se sama blokira nakon 3 puta za redom unosa pogrešnog PIN-a.

7.2. M-BANKING ERSTE

Za korištenje Erste mBanking usluge potrebno je ispuniti pristupnicu koja se nalazi u svakoj poslovnici ili na internetskoj stranici Erste banke, www.erstebank.hr ili u rubrici <NetBanking>. Pristupnicu je potrebno ispisati i zatim ispuniti. Ispunjena pristupnica se predaje u poslovnicu Erste banke gdje se dobiva korisničko ime i zaporka, a kasnije se poštom prima TAN kartica sa sigurnosnim ključevima.

Samu aplikaciju moguće je koristiti s bilo kojeg mjesta s kojeg imamo pristup Internetu s mobilnim telefonom.

Instalacija aplikacije na svoj mobilni telefon se odvija na isti način kao i instalacija svih aplikacija na Android.

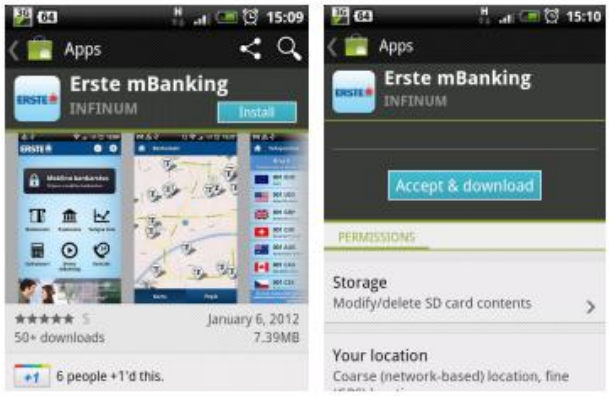
„Stranici aplikacije u Android Market-u možete pristupiti na sljedeće načine:

1) Putem linka iz SMS-a nakon ugovaranja usluge

2) Pretragom u Android Market-u na svom Android telefonu

3) Skeniranjem QR koda na promotivnim materijalima i web stranici Erste banke“[9]

Nakon pristupa linku, odaberemo Install i Accept & download pa se aplikacija instalira.



Slika 13 Instalacija aplikacije

Izvor: Erste m-banking

Erste mBanking aplikacija nudi sljedeće opcije: „Računi“, „Novi nalog“, „Slikaj i plati“, „Pregled plaćanja“, „Predlošci“, „Mjenjačnica“, „Kreditne kartice“, „Krediti“, „Štednja“, „GSM bonovi“, „Fondovi“, „Tečajna lista“, „Poslovnice“, „Bankomati“, „Kalkulatori“ i „Kontakt“. U glavnom izborniku imamo opcije "Postavke" i "Odjava". U postavkama možemo promijeniti kontakt podatke, zaporku, uključiti i isključiti ikone s glavnog izbornika. Na kraju rada u aplikaciji potrebno se odjaviti, a ako to ne učinimo sami, sustav će nas sam automatski odjaviti nakon 10 min. neaktivnosti.

Slika 14 Glavni izbornik aplikacije

Izvor: Erste m-banking

[9] Izvor: https://www.erstebank.hr/hr/Elektronicko_bankarstvo/Poslovni_subjekti/Erste_NetBanking

Odabirom opcije „Računi“ imamo prikaz svih naših otvorenih računa u Erste banci gdje kad odaberemo neki od računa imamo grafički prikaz prometa po računu, sve promete po računu i osnovne podatke o računu. Možemo promijeniti naziv ili promijeniti sliku te ih i vratiti.

Slika 15 Prikaz opcije "Računi"

Izvor: Erste m-banking

Odabirom opcije „Novi nalog“ možemo plaćati račune izvan granica banke („Nalog za plaćanje - HUB1“- plaćanje vode, struje, telefona...) i prenositi na račune u drugim bankama. Slikaj i plati je usluga koja omogućuje plaćanje bez potrebe za prepisivanjem podataka s uplatnice, to odrađuje nas smartphone za nas. Možemo prebaciti sredstva na račune unutar banke („Prijenos između računa“). „Novi nalog iz predloška“ omogućuje da plaćamo iz prethodno kreiranih predložaka. Imamo i kupoprodaju deviza.

Slika 16 Prikaz opcije "Novi nalog"

Izvor: Erste m-banking

Pomoću opcije „Prijenos između računa“ možemo prenositi sredstva između vlastitih računa i na račune drugih u Erste banci. Koristimo ga za plaćanje kredita i obveza po kreditnoj kartici, kupoprodaju deviza i slično.

Nalog se dijeli na tri dijela:

1. „S računa“- broj računa s kojeg želimo platiti ne upisujemo već ga odaberemo s popisa svih računa s kojih možemo prenijeti sredstva. Tu odaberemo i valutu u kojoj je račun otvoren s popisa mogućih valuta i odaberemo iznos koji želimo prenijeti na drugi račun.
2. „Na račun“- ako se radi o transakciji između vlastitih računa, račun na koji se prenosi sredstva odabiremo iz ponuđenih vlastitih računa, a ako prenosimo na račun drugih u istoj banci onda broj računa upisujemo sami pomoću opcije „Unesite“.
3. „Plaćanje“- imamo opis plaćanja što je proizvoljan opis transakcije i datum kada želimo izvršiti nalog.

Dodatni podaci imaju i e-mail potvrdu kao potvrda putem slanja e-mail poruke o izvršenju transakcije.

Slika 17 Prijenos između računa

Izvor: Erste m-banking

Pomoću opcije „Nalog za plaćanje“ jednostavno je plaćati račune. I on se sastoji od tri dijela. To su:

1. Podaci o računu s kojeg želimo provesti plaćanje - osim broja računa s kojeg želimo platiti, valute u kojoj je račun otvoren i željenog iznosa koji želimo prenijeti potreban je još i naziv uplatitelja.
2. Podaci o računu na koji se sredstva prenose - broj računa i poziv na broj koji mora biti naveden u skladu s pravilima kreiranja poziva na broj.
3. Opis i datum transakcije - tu ulaze šifra i opisa plaćanja u skladu s regulativom HNB, opis i razlog transakcije i datum kada transakcija treba biti provođena.

Slika 18 Nalog za plaćanje

Izvor: Erste m-banking

Pomoću opcije „Slikaj i plati“ najlakše i najbrže plaćamo račune i opće uplatnice. Nema prepisivanja niza podataka s uplatnice jer to pametni telefon radi sam. Postupak plaćanja se odvija u tri koraka:

1. Odabir opcije „Slikaj i plati“
2. Pozicioniranje ruba uplatnice na ekran, i obrada uplatnice
3. Nakon učitavanja podataka s uplatnice, samo odabir opcija „Provjeri“ i „Potvrdi“

U opciji „Pregled plaćanja“ imamo prikaz svih plaćanja s Erste NetBanking, Erste mBanking ili Erste Fon Banking uslugama.

Dostupna su četiri prikaza plaćanja:

1. Izvršena plaćanja – pregled izvršenih naloga
2. Plaćanja u najavi – pregled naloga koji čekaju izvršenje
3. Neizvršena plaćanja – pregled naloga koji se nisu izvršili
4. Stornirana plaćanja – pregled storniranih naloga

Odabirom jedne opcije otvara se pregled naloga gdje možemo kreirati novi nalog na temelju postojećeg (opcija „Kopiraj u novi nalog“), kreirati novi predložak na temelju postojećeg (opcija „Kopiraj u novi predložak“) i slati e-mail potvrdu o nalogu (opcija „Pošalji e-mail potvrdu“)

Opcija „Predlošci“ pojednostavljuje plaćanje računa koji se ponavljaju iz mjeseca u mjesec. To je unaprijed kreiran nalog za plaćanje na temelju kojeg zadajemo novo plaćanje. Prikazuje popis svih predložaka kreiranih Erste mBankingom i Erste NetBankingom ako koristimo uslugu. Možemo unijeti novi, izmijeniti ili obrisati postojeći predložak, pregledati sve transakcije provedene na temelju pojedinog predloška te provesti transakciju koristeći predložak.

Opcija „Kupnja i prodaja deviza“ omogućava kupovinu, prodaju i konverziju deviza za što je potrebno popuniti podatke o računu koji se tereti i računu na koji se prenose sredstva.

U opciji „Kreditne kartice“ imamo mogućnost uvida u sve ugovorene kreditne kartice, prometa po kartici i prikaz detalja.

Opcija „Krediti“ nudi uvid u sve naše kredite, promete po kreditu i prikaz detalja o kreditu.

„Štednja“ je za oročavanje sredstava s nekog od računa (tekući, devizni, žiro i štedni računi) bez odlaska u neku od poslovnica. Moguće je oročiti sredstva na rok od jedan mjesec i jedan dan do 180 mjeseci u kategoriji nenamjenskih oročenja, do neograničenog iznosa.

GSM bon kupujemo odabirom računa koji se tereti, operatora (T-Mobile, VIP, Tele2…) te vrijednosti bona odabiremo u padajućem izborniku.

Slika 19 Prikaz kupnje GSM bona

Izvor: Erste m-banking

Za pregledavati stanje svojih udjela u mirovinskim fondovima, i za promet po računu kao i pregled investicijskih fondova imamo opciju „Fondovi“.

8. ZAKLJUČAK

Mobilno poslovanje započelo je novi trend u današnjem poslovanju. Taj trend je sve prisutniji svugdje u svijetu. Informacijska tehnologija predstavlja ključni faktor za poslovanje danas. Mobilno poslovanje pomoću mobilnih mreža je dio samog elektroničkog poslovanja i on rješava problem fiksne lokacije u poslovanju. Koristeći mobilno poslovanje doprinosimo razvitku i širenju naših poduzeća. Ograničenja koja nam zadaje fizička lokacija u poslovanju se smanjuje ako koristimo mobilno poslovanje. U mobilnom poslovanju, elektronička usluga nam je dostupna s bilo kojeg mjesta. Tako se ukidaju ograničenja tradicionalnog poslovanja (stacionarnog poslovanja).

Ne trebamo plaćati gotovinom na parkingu, ići u poslovnice banaka kako bi uplatili novac na račun, ili kako bi plaćali račune. Sve to možemo uraditi bez da čekamo u redu od kuće.

U m-poslovanju možemo jednostavnije i efikasnije raditi koristeći mobilne uređaje s bilo kojeg mjesta i u bilo kojem trenutku.

Iako zlonamjerni programi za mobilne uređaje još nisu toliko jaki da stvore onoliko štete koliko je stvaraju osobnim računalima, to takvo stanje neće još dugo trajati. Kako se razvijaju mobilni uređaji tako ih prati razvoj i samih zlonamjernih programa, primjećuje se kako je svijet pokretne komunikacije privukao pozornost autora brojnih zlonamjernih programa raznih vrsta.

Sigurnost mobilnih uređaja teže je osigurati nego sigurnost osobnih računala, ali to je moguće postizanjem odgovornim ponašanjem korisnika i upotrebljavanjem odgovarajuće zaštite.

Mobilni uređaji danas su često meta zlonamjernih programa svih vrsta. Porast broja pametnih telefona i njihova složenost i funkcionalnost u stalnom su rastu, pa se ti trendovi u rastu preslikavaju na razvoj zlonamjernih programa. Propusti se dešavaju zato što je mobilne aplikacije teže ispitati, a ni proizvođači tih aplikacija ni ne provjeravaju sigurnost gotovih proizvoda. Mnoge aplikacije koje se nalaze na poznatim servisima za preuzimanje mobilnih aplikacija ni ne prolaze sigurnosnu provjeru. Nužno ih je u početi ispitivati kako ne bi došlo do krađe povjerljivih podataka korisnika.

Svaka mobilna platforma zahtjeva druge alate i uređaje za ispitivanje sigurnosti, a i nužno je znati koje dijelove sigurnosno provjeriti. Najbolje je koristiti dostupne, provjerene i jednostavne alate. Potrebno je raditi na sigurnosti aplikacija kako bi ih učinili potpuno sigurnima, jer ima mnogih zlonamjernih programa koji se brzo šire. Samo obrazovanjem krajnjih korisnika, ali i programera koji razvijaju aplikacije za pametne uređaje možemo se kvalitetno obraniti od prijetnji koje nam donosi ne tako daleka budućnost.

Pretpostavlja se kako će u budućnosti razvoj mobilne tehnologije intenzivirati pa se očekuje više funkcija i primjena mobilnog poslovanja.

9. SLIKE

10. TABLICE

11. LITERATURA

KNJIGE

1. Panian, Ž., *Elektroničko poslovanje druge generacije*, Ekonomski fakultet Zagreb, trg J. F. Kennedyja 6 Zagreb, 2013.
2. Panian, Ž., *Izazovi elektroničkog poslovanja*, Zagreb, Narodne novine d.d., 2002.
3. Turban, E., Volonino, L. i Wood, G.R., *Information technology for management advancing sustainable, profitable business growth* , Wiley, 2013.

INTERNET

1. CIS- centar informacijske sigurnosti, *Ispitivanje sigurnosti mobilnih aplikacija*, studeni 2011., http://www.cis.hr/files/dokumenti/CIS-DOC-2011-11-CIS-030.pdf
   (pristupano 9. kolovoz 2016.)
2. D. Biljana, *Mobilno poslovanje*, http://biljanadelic85.wix.com/mobilnoposlovanje#! (pristupano 23. srpanj 2016.)
3. *E-trgovina*, http://www.slideshare.net/suzanainformatika/e-trgovina-34065219 (pristupano 23. srpanj 2016.)
4. ERSTE banka, *Što možete učiniti da se zaštitite?*, https://www.erstebank.hr/hr/Sigurnost/Sigurnost_Erste_NetBanking_usluge/Sto_mozete_uciniti;GPJSESSIONID=HRP9XrWLpX2BsJhnGbXXhyxLZ2cNBbTRpQxnnSnVgVShVxQqwGPH!1954360152 (pristupano 10. kolovoz 2016.)
5. Erste m-banking, lipanj 2014, https://www.erstebank.hr/hr/Elektronicko_bankarstvo/Poslovni_subjekti/Erste_NetBanking (pristupano 10. kolovoz 2016.)
6. Hosch, W.L. „Smartphone“, *Enciklopedija Britannica,* 1.8.2016., https://www.britannica.com/technology/smartphone,
   (pristupano 29. srpanj 2016.)

7. I. Malić, *Bežični aplikacijski protokol*, http://www.ericsson.hr/etk/revija/Br_2_2001/wap.htm (pristupano 23. srpanj 2016.)
8. LSS (Laboratorij za sustave i signale), *Zlonamjerni programi za mobilne platforme*, 2010., http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-001.pdf (pristupano 10. kolovoz 2016.)
9. N. DuPaul, *Common Mobile Malware Types: Cybersecurity 101*, 2013, https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101/ (pristupano 9. kolovoz 2016.)
10. OTP banka.hr, *OTP mobilno bankarstvo*, https://www.otpbanka.hr/hr/gradani/otp-mobilno-bankarstvo, https://elementa.otpbanka.hr/gradjani/upute/m-banking.htm (pristupano 8. kolovoz 2016.)
11. PBZ, *Mobilno bankarstvo- mPBZ*, http://onlinebanka.pbz.hr/mpbz.html#.V6hryvmLTIV (pristupano 8. kolovoz 2016.)
12. Poslovni forum, *Internet bankarstvo*, http://www.poslovniforum.hr/info/internet_bankarstvo.asp (pristupano 7. kolovoz 2016.)

PREZENTACIJE

1. Dr. sc. Vanja Bevanda, *ELEKTRONIČKO POSLOVANJE Poslovni modeli elektroničkog poslovanja 2015/2016,* http://e-ucenje.unipu.hr/mod/resource/view.php?id=672 (pristupano 25. srpanj 2016.)
2. Izv. prof. dr. sc. Blaženka Knežević, *Mobilna trgovina, engl. m-commerce (prema 6. poglavlju knjige: Turban i dr.(2012), E-commerce 2012…)*, http://web.efzg.hr/dok//trg/bknezevic/eet2014/m-trg.pdf (pristupano 23. srpanj 2016.)

Sigurnost mobilnog poslovanja

SAŽETAK- U radu se obrađuje uloga i sigurnost mobilnog poslovanja. Rad je baziran na pojam mobilnog poslovanja, te primjenu u različitim modelima poslovanja i njegovoj sigurnosti. Mobilne tehnologije se primjenjuju u mobilnom poslovanju. Mobilno poslovanje i njegova sigurnost predstavljaju novi trend poslovanja u današnjem svijetu. Današnje poslovanje je veoma dinamično i zahtjeva stalnu povezanost i trenutnu reakciju na događanja na tržištu stoga je veoma bitna sigurnost mobilnog poslovanja. Mobilno poslovanje je nevezano za neku fiksnu lokaciju, te je nužno biti stalno dostupan. Osnovna zadaća rada je ukazati na značaj poslovanja putem mobilnih uređaja, kao i na važnost sigurnosti podataka na mobilnim uređajima.

Ključne riječi – sigurnost mobilnog poslovanja, mobilno poslovanje, m-poslovanje

SUMMARY- The subject matter of this thesis is the role and security of mobile business. The thesis focuses on the concept of mobile business and its use in various business models, as well as its security. Mobile technologies are used in mobile business. Mobile business and its security present a new business trend in the modern world. Nowadays, business is very dynamic and demands constant connectivity and immediate reaction on the market. Therefore, its security is of the utmost importance. Mobile business is not linked to a specific location it is necessary to be available at all times. The goal of this thesis is to show the importance of doing business through mobile devices, as well as the importance of data security on mobile devices.

Keywords – security of mobile business, mobile business, m-business