UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Marko Vovko

Varnost uporabnikovih podatkov in tveganja pri uporabi tabličnih računalnikov in pametnih telefonov

Diplomsko delo

Ljubljana, 2013

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Marko Vovko

Mentor: izr. prof. dr. Jaroslav Berce

Varnost uporabnikovih podatkov in tveganja pri uporabi tabličnih računalnikov in pametnih telefonov

Diplomsko delo

Ljubljana, 2013

Zahvala

Zahvaljujem se mentorju izr. prof. dr. Jaroslavu Bercetu za vso strokovno pomoč in nasvete pri izdelavi diplomskega dela.

Posebna zahvala gre staršem in celi družini, ki mi je s svojo pomočjo omogočila študij in me ves čas podpirala na poti.

Zahvaljujem se tudi prijateljem in sošolcem. Brez njih bi bila študijska leta manj zanimiva in prijetna.

Varnost uporabnikovih podatkov in tveganja pri uporabi tabličnih računalnikov in pametnih telefonov

V današnjem času so pametni telefoni in tablični računalniki zelo razširjeni. Uporaba pametnih mobilnih naprav namreč iz leta v leto strmo narašča. Cilj in predmet diplomskega dela je bil, zaradi vedno večje razširjenosti in priljubljenosti, narediti pregled in analizo ključnih tveganj oziroma varnostnih sklopov povezanih z uporabo tabličnih računalnikov in pametnih telefonov ter podati predloge za varnejšo uporabo teh naprav. Uvod v diplomsko delo je analiza sekundarnih virov strokovne literature in spletnih virov z opredelitvijo relevantnih pojmov, povezanih z obravnavano tematiko. Nadaljeval sem s poglavjem Varnost in tveganja, v katerem sem pregledal štiri sklope glavnih varnostnih tveganj. S pregledom literature in sekundarnih virov sem sprejel prvo hipotezo, da tablični računalniki in pametni telefoni sami po sebi niso dovolj varni za uporabo in tudi drugo hipotezo, da lahko uporabniki sami poskrbijo za manj tvegano in varnejšo uporabo svojih tabličnih računalnikov in pametnih telefonov. V zaključku sem povzel ugotovitve in navedel sklep, da za uporabnike ni dovolj, da svojo novo mobilno napravo samo prižgejo in jo začnejo uporabljati. Pomembno je tudi, da se malo bolj poglobijo v same funkcije in nevarnosti, ki grozijo njihovim napravam.

Ključne besede: pametni mobilni telefon, tablični računalnik, varnost, tveganja, uporabnikovi podatki.

Safety of user date and risks of using tablets and smart phones

Nowadays, smartphones and tablet computers are widely distributed. The use of smart mobile devices is growing rapidly from year to year. The aim and object of the thesis was, due to the increasing prevalence and popularity to do a review and analysis of key risks, and security components related to the use of tablet computers and smartphones, and to provide suggestions for safer use of these devices. Introduction to the thesis is the analysis of secondary source literature and web sources related to the topic and drawn the definition of terms related to the subject matter. I continued with chapter Security section and risks, where I reviewed four sets of major security risks. A review of security risks helped me accept the first hypothesis, that tablet computers and smartphones by themselves are not sufficiently safe to use and also the second hypothesis, that users may provide less risky and safer use of their tablet computers and smartphones. Through the study I have come to the conclusion that it is not enough for users to just turn on their new mobile device and start using it. It is also important for the users to be more deeply informed about functions and threats to their devices.

Keywords: smartphone, tablet computer, security, risks, user data.

KAZALO VSEBINE

KAZALO TABEL

KAZALO GRAFOV

KAZALO SLIK

1 UVOD

V današnjem času so pametni telefoni in tablični računalniki zelo razširjeni. Uporaba pametnih mobilnih naprav namreč iz leta v leto strmo narašča (IDC 2013). Po podatkih Mobitela so leta 2011 pametni telefoni predstavljali manj kot četrtino vseh telefonov v Mobitelovem omrežju. V letu 2012 se je delež uporabnikov pametnih telefonov povzpel na eno tretjino (Mobitel Tehnik 2012). Pametni telefoni in tablice so postali prava konkurenca računalnikom in prenosnikom. Z njimi sicer v prvi vrsti še vedno kličemo in pošiljamo SMS sporočila, vendar jih vedno bolj razširjeno uporabljamo za brskanje po internetu, sodelovanje v raznih družbenih omrežjih, igranje iger, nakupovanje preko spleta, opravljanje bančnih storitev in tako dalje (White 2013).

Mobilna naprava ima torej vse, kar ima računalnik: lasten operacijski sistem (najbolj razširjeni v letu 2012 so bili Android, iOS, BlackBerry, Windows Phone in Symbian (IDC 2012)) in brskalnik, s katerim lahko brskamo po spletu. Na splet se lahko povežemo kjerkoli s prenosom podatkov našega mobilnega operaterja ali pa preko mnogih brezžičnih povezav, ki so že zelo razširjene. Namesto programov na pametnih telefonih in tablicah uporabljamo aplikacije, ki jih lahko kupimo ali si jih brezplačno naložimo preko aplikacijskih trgovin.

Mobilne naprave tako vključujejo vse funcionalnosti domačih računalnikov, le videz naprave in uporabniškega vmesnika je drugačen. Priljubljenost teh naprav gre pripisati temu, da se gradijo vedno hitrejša in bolj razširjena mobilna omrežja, ki omogočajo, da smo lahko vedno povezani na splet. Polega tega so te naprave majhne, prenosljive, enostavne za uporabo ter vedno cenejše. Tudi dostop do pomembnih uporabnikovih podatkov na teh napravah je zelo preprost in premalo zavarovan.

Zaradi teh lastnosti tabličnih računalnikov in pametnih telefonov se v zadnjih letih povečujejo varnostna tveganja ob njihovi uporabi, uporabniki, ki uporabljajo tablične računalnike in pametne telefone, pa so mnenja, da je uporaba le teh enako varna kot uporaba osebnega računalnika (Bernik in Prislan 2012).

2 CILJ, POTEK IN METODA DELA

2.1 Cilj in predmet diplomskega dela

Cilj diplomskega dela je, narediti pregled in analizo ključnih tveganj oziroma varnostnih sklopov povezanih z uporabo tabličnih računalnikov in pametnih telefonov ter podati predloge za varnejšo uporabo teh naprav. V diplomskem delu bom analiziral štiri glavna tveganja oz. varnostne sklope: fizični dostop do mobilnih naprav in njenih podatkov, možnosti zavarovanja podatkov ob kraji ali izgubi naprave, nevarnosti ob omrežnem povezovanju in varnost pri uporabi ter nameščanju aplikacij na mobilne naprave.

2.2 Hipotezi

Za potrebe diplomskega dela sem postavil dve hipotezi, ki ju bom med pregledom in analizo tveganj skušal dokazati:

H1: Tablični računalniki in pametni telefoni sami po sebi niso dovolj varni za uporabo.

Pametne mobilne naprave imajo vgrajeno, vrsto varnostnih funkcij, ki ob nakupu naprave niso vključene. Uporabniki niso dovolj seznanjeni z novimi napravami, njihovimi funkcijami, niso seznanjeni s tehnološkim razvojem, ne uporabljajo vgrajenih varnostnih funkcij v svojih napravah (Markelj in Bernik 2013). S hipotezo predvidevam, da mobilne naprave, če jih ob nakupu samo prižgemo in začnemo uporabljati, niso dovolj varne. Potrebno je dodatno urejanje nastavitev s strani uporabnikov, da naprave postanejo primerne za varno uporabo.

H2: Uporabniki lahko sami poskrbijo za manj tvegano in varnejšo uporabo, svojih tabličnih računalnikov in pametnih telefonov.

Stalna uporaba in dostop v kibernetski prostor z mobilnimi napravami je odprl mnogo priložnosti za napadalce in izpostavljenost uporabnikov za (kibernetsko) kriminaliteto, zato je upravljanje s tveganji nujno. Če se zavedamo, da omenjene naprave niso varne, in sprejmemo vsaj osnovne ukrepe za varnejše delo, pa se izpostavljenost

tveganjem pomembno zmanjša (Bernik in Prislan 2012). Na osnovi te ugotovitve predvidevam, da lahko uporabniki mobilnih naprav poskrbijo za varnejšo uporabo svojih naprav, če na svojih mobilnih napravah uporabljajo vse varnostne nastavitve, se ne povezujejo v nezaščitena brezžična omrežja in ne nameščajo aplikacij, ki niso preverjene s strani aplikacijskih trgovin.

2.3 Metoda dela

Relevantne pojme bom opredelil na podlagi analize sekundarnih virov, strokovne literature in spletnih virov. Tudi hipotezi bom skušal dokazati s pomočjo metode zbiranja sekundarnih virov in njihove analize. Ker so pametni telefoni in tablični računalniki razmeroma mlado področja raziskovanja je večino sekundarnih podatkov na razpolago v obliki člankov v različnih znanstvenih revijah, znanstvenih publikacijah, dostopnih preko znanstvenih baz podatkov ali v člankih, objavljenih na spletu.

Analiziral bom dosedanja spoznanja in ugotovitve v znanstvenih virih s področja varnosti in tveganj pri uporabi tabličnih računalnikov in pametnih telefonov ter iz njih izpeljal ugotovitve, ki se bodo navezovale na področje mojega raziskovanja.

2.4 Potek dela

V uvodu v diplomsko delo se bo najprej naredilo opredelitev relavantnih pojmov, povezanih z obravnavano tematiko, kot so pametni mobilni telefoni, tablični računalniki, operacijski sistemi mobilnih naprav, mobilne aplikacije, mobilna in lokalna brezžična omrežja, uporabniški podatki, informacijska varnost in varnostna tveganja.

Nadaljeval bom s poglavjem Varnost in tveganja, v katerem bom pregledal štiri sklope glavnih varnostnih tveganj: fizični dostop do mobilne naprave in njenih podatkov; varnost podatkov ob okvari, kraji ali izgubi naprave in možnosti, ki jih ima uporabnik za povrnitev svojih podatkov; nevarnosti in tveganja ob povezovanju v različna omrežja in na koncu še varnost pri nameščanju in uporabi aplikacij.

V zaključku bom strnil ugotovitve in poskušal sprejeti ali ovreči svoje hipoteze.

3 OPREDELITEV POJMOV

3.1 Pametni mobilni telefon

Pametnih mobilnih telefonov danes ne bi bilo brez izuma prvega praktičnega telefona za ročno uporabo. Leta 1973 je raziskovalec Martin Cooper skupaj s podjetjem Motorola izumil prvi mobilni telefon, ki je tehtal dva kilograma (Teixeira 2010).

Od takrat naprej so mobilni telefoni postajali vedno manjši, tanjši in lažji. Tudi baterije so postajale vedno bolj zmogljive. Ena izmed značilnosti mobilnih telefonov je tudi, da se kljub zmanjševanju samih telefonov zasloni izboljšujejo in postajajo vedno večji ter prikazujejo bolj kakovostno sliko (Hribar v Vehovar 2007).

Običajni mobilni telefoni so v glavnem namenjeni telefoniranju, vendar že omogočajo določene dodatne funkcionalnosti in storitve. Povprečen telefon ima barvni zaslon, podpira večglasno zvonjenje, omogoča prenos podatkov preko GPRS (General Packet Radio Service), kratka SMS sporočila, večpredstavnostna sporočila MMS (Multimedia Message Service), igre, dostop do interneta z brskalnikom WAP (Wireless Application Protocol) in ima vgrajen fotoaparat za zajemanje slik in videa (Hribar v Vehovar 2007). Mobilni telefoni so pridobivali na vse večji popularnosti in so danes ena najbolj razširjeni elektronskih naprav na svetu. Konec leta 2012 je bilo na svetu že 6,8 milijarde uporabnikov mobilnih telefonov. To znaša kar 96 % celotne svetovne populacije (Mobithinking 2013).

Pametni mobilni telefoni so se v prvi vrsti razvili zato, da bi zadostili potrebam poslovnih uporabnikov po boljši povezljivosti, zmožnosti pošiljanja in prejemanja spletne pošte, organizatorjev in koledarjev ter ostalih funkcij, ki naj bi jih poslovneži potrebovali za vsakodnevno delo. Začetki pametnih telefonov segajo v leto 1992. IBM je takrat izdelal prvi telefon, imenovan IBM Simon, ki je zmogel več funkcij kot le klicanje in pošiljanje tekstovnih sporočil. V tistem času je bil zelo napreden in je ponujal koledar, svetovno uro, imenik, odjemalec pošte in zaslon na dotik. Na voljo je bil le v Združenih državah Amerike (Sager 2012).

Leta 1997 je podjetje Ericsson predstavilo svetu prvi telefon, ki se je imenoval pametni telefon. Telefon, imenovan Penelope, je imel celotno tipkovnico ”qwerty” in je lahko poleg klicev sprejemal tudi fakse in e-maile. Penelope ni bil nikoli v masovni

proizvodnji, ampak je odprl pot nasledniku Ericssonu R380, ki je bil prvi komercialno dostopni pametni telefon (DigitalNewsTestKitchen 2010).

Od leta 2000 naprej so vsa glavna podjetja začela s prodajo svojih pametnih mobilnih telefonov. Leta 2002 so se pojavili prvi telefoni z barvnimi zasloni. Leta 2005 je Nokia izdala N serijo pametnih telefonov, trženih kot mobilni multimedijski računalnik, namenjen poslovnežem. Leta 2007 je Apple s predstavitvijo svojega lastnega pametnega telefona, imenovanega iPhone, ustvaril revolucijo na področju pametnih telefonov. Pametni telefoni niso bili več namenjeni samo poslovnežem, ampak tudi množicam. iPhone je pritegnil veliko ljudi. Zaradi svoje uporabniške prijaznosti in možnosti aplikacij je začel pridobivati na priljubljenosti in je počasi nakazoval propad ostalih pametnih telefonov, ki niso sledili novim trendom (TechInfo2 2013).

Konec leta 2008 je na tržišče prišel prvi pametni telefon HTC Dream, ki je uporabljal Android, odprtokodni mobilni operacijski sistem, razvit s strani Googla. Tako kot iPhone je tudi Android začel pridobivati veliko število uporabnikov na račun vmesnika, odprtokodnosti in možnosti prenašanja aplikacij. Applu in Googlu se je leta 2010, s svojim lastnim operacijskim sistemom Windows Phone, pridružil še Microsoft. Ti trije danes obvladujejo trg pametnih telefonov (TechInfo2 2013).

Pametni telefoni so tako bolj napredni kot navadni telefoni, saj imajo operacijski sistem, ki uporabnikom omogoča, da delajo na svojem telefonu mnoge stvari, ki so bile včasih prednost osebnih računalnikov. Uporabniki lahko brskajo po spletu pri visokih hitrostih, gledajo in urejajo dokumente, prenašajo datoteke, glasbo, filme, revije, knjige ali pa urejajo več poštnih računov naenkrat (AT&T 2013). Pametni telefoni imajo poleg vseh že omenjenih funkcij tudi vse funkcije navadni telefonov, na primer pošiljanje kratkih SMS sporočil.

3.2 Tablični računalniki

Razvoj tabličnih računalnikov se ni začel leta 2010 z začetkom prodaje Applovega iPada. Že leta 1888 je bil podeljen patent za elektronsko tablico za tako imenovani Telautograph, daljnega prednika faksov. Naprava naj bi znala prepoznati pisavo ali risbe, ki jih s peresom naredimo na temu namenjeni površini. Leta 1915 pa je bil podeljen patent za sistem, ki preko analize gibanja pisala prepozna "na roke" zapisano besedilo (Moj Mikro 2013).

Današnji tablični računalniki so se pravzaprav razvili iz grafičnih tablic, ki so delovale kot periferni vmesniki za risanje. Prva takšna naprava je prišla na trg leta 1964. RAND je bil namizni računalnik s katodnim zaslonom. Priloženo je bilo pisalo (stilus, povezan s kablom), ki je zaznavalo električne impulze s posebne mreže na zaslonu in te informacije pošiljalo v računalnik (Moj Mikro 2011).

Do leta 2000 je na trg prišlo veliko grafičnih tablic in manj uspešnih tabličnih računalnikov, ki pravega uspeha niso doživeli zaradi velikega zanimanja za mobilne telefone in osebne organizatorje. Leta 2000 je Microsoft prvič začel uporabljati izraz osebni tablični računalnik. Šlo naj bi za tablični računalnik, ki bi za vnašanje ukazov uporabljal zaslon na dotik in bi imel naložen poseben operacijski sistem. V resnici je šlo za prenosnik brez tipkovnice, z Microsoftovim operacijskim sistemom in upravljanje s pisalom. Naprava v naslednjih 10 letih ni dosegla večjega poslovnega uspeha (Moj Mikro 2013).

Vse se je spremenilo leta 2010 s predstavitvijo Applovega iPada. Velik uspeh iPada gre pripisati iPhonu. Zaradi njegove velike priljubljenosti so se pri Applu odločili narediti povečano verzijo iPhona, ki so mu dodali bolj zmogljivo strojno opremo, večji zaslon in ga preimenovali v iPad. Zaradi velike priljubljenosti iPada so zgledu Appla sledili tudi proizvajalci Android telefonov, ki so na trg ponudili lastne tablice. Zadnji je na trg tablic leta 2012 prišel še Microsoft s svojim novim operacijskim sistemom Windows RT (Moj Mikro 2013).

Tablični računalniki so povečane verzije pametnih mobilnih telefonov. V večini primerov imajo vse funkcije in zmogljivosti pametnih telefonov, razen možnosti klicanja in pošiljanja SMS sporočil (majhno število tablic to omogoča). Za upravljanje s tablicami se uporablja uporabniški vmesnik na dotik.

3.3 Operacijski sistemi mobilnih naprav

Funkcionalnost in način uporabe mobilnih naprav sta odvisna predvsem od operacijskih sistemov, ki jih poganjajo (Hribar v Vehovar 2007). Mobilni operacijski sistem je sistem, ki upravlja s strojno in programsko opremo ter nadzoruje pametne mobilne telefone, tablične računalnike in druge naprave (Hribar v Vehovar 2007). Vsebujejo funkcije prenosnih računalnikov skupaj z uporabniškim vmesnikom na dotik, omogočajo brezžično povezljivost, sprejemanje in opravljanje klicev, pošiljanje sporočil, GPS-navigacijo, zajemanje videa in slik s pomočjo kamere ter predvajalnik multimedijskih vsebin (Geek 2009). Odvisno od operacijskega sistem lahko naložimo nove združljive programe (aplikacije) v pomnilnik mobilne naprave in s tem razširimo uporabnost mobilnih naprav (Hribar v Vehovar 2007).

Mobilne naprave niso kot prenosni računalniki, da bi lahko nanje poljubno nameščali operacijske sisteme, če ti prednaloženi sistem ne bi bil všeč. Od proizvajalcev je odvisno kateri operacijski sistem bo imela naprava naložen. Operacijski sistemi mobilnih naprav so sprogramirani specifično za pametne telefone in tablične računalnike (Geek 2009).

Danes so najpogostejši operacijski sistemi, ki poganjajo pametne telefone in tablične računalnike, z največjim deležem Android in iOS. Obema sledijo BlackBerry, Symbian in Windows Phone (IDC 2013).

Tabela 3.1: Pet mobilnih operacijskih sistemov z največjim deležem v letu 2012

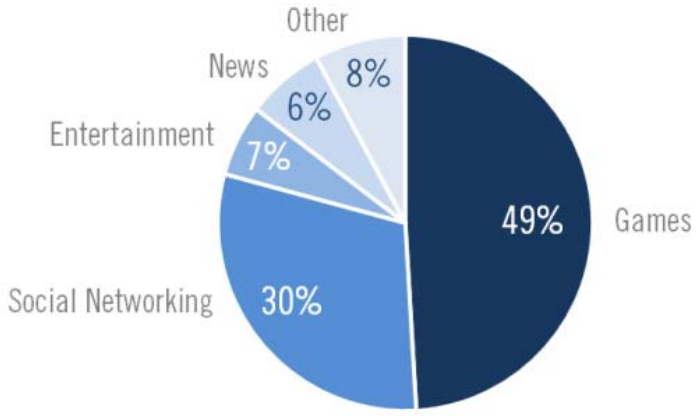
Operating System	2012 Unit Shipments	2012 Market Share	2011 Unit Shipments	2011 Market Share	Year over Year Change
Android	497.1	68.8%	243.5	49.2%	104.1%
iOS	135.9	18.8%	93.1	18.8%	46.0%
BlackBerry	32.5	4.5%	51.1	10.3%	-36.4%
Symbian	23.9	3.3%	81.5	16.5%	-70.7%
Windows Phone/ Windows Mobile	17.9	2.5%	9.0	1.8%	98.9%
Others	15.1	2.1%	16.3	3.3%	-7.4%
Total	**722.4**	**100.0%**	**494.5**	**100.0%**	**46.1%**

Vir: IDC (2013).

3.4 Mobilne aplikacije

Mobilne naprave niso z razvojem prinesle samo komuniciranja in povezovanja, temveč tudi uporabo storitev in aplikacij (Hribar v Vehovar 2007). Mobilne aplikacije so posebni programi, ki jih naložite na svoj mobilni telefon. Na pospešen razvoj mobilnih aplikacij je vplival predvsem pojav pametnih telefonov, ki omogočajo preprost dostop do mobilnih aplikacij preko aplikacijskih trgovin. Vse aplikacije ne delujejo na vsakem mobilnem telefonu, zato je potrebno pred namestitvijo preveriti, kakšne aplikacije podpira določen mobilni telefon. Trenutno je na voljo skupno že več kot milijon različnih aplikacij. Najbolj priljubljene, z največ prenosov so naslednje: aplikacije za zagotavljanje dodatne funkcionalnosti družabnih omrežij, igre, aplikacije za novice in informacije, zemljevidi ipd. (SAFE.si 2013).

Graf 3.1: Najbolj priljubljene aplikacije v ZDA v letu 2011



Vir: Mobitel tehnik (2012b).

Najpogosteje se mobilne aplikacije delijo na operacijske sisteme in delovne programe, na katerih delujejo Symbian, BlackBerry, Windows Phone, Android in iOS. Dostopne so preko različni aplikacijskih trgovin. Največji trgovini sta App Store za naprave z operacijskim sistemom iOS in Google Play za naprave z Androidom. Windows Phone, BlackBerry in Symbian uporabljajo vsak svojo lastno trgovino, ki pa so v primerjavi z App Store in Google Play veliko manjše.

Poleg pozitivnih lastnosti pa uporaba mobilnih aplikacij prinaša tudi določena tveganja, ki so povezana predvsem s povečano možnostjo zlorabe osebnih podatkov ter visokimi stroški, ki so posledica nepazljive uporabe mobilnih aplikacij (SAFE.si 2013).

3.5 Mobilna in lokalna brezžična omrežja

Omrežja predstavljajo osnovno infrastrukturo in uporabnikom z mobilnimi napravami omogočajo uporabo mobilnih storitev. Mobilna in brezžična omrežja so vsa omrežja, ki za komunikacijo namesto žičnih povezav izkoriščajo radijske valove in združujejo: mobilna telefonska omrežja, brezžična lokalna omrežja (WLAN) in druge brezžične komunikacije, ki uporabnikom omogočajo uporabo mobilnih storitev (Hribar v Vehovar 2007).

3.5.1 Mobilna omrežja

Razvoj mobilnih telefonskih omrežij opisujemo z generacijami. Omrežje prve generacije, ki je delovalo tudi v Sloveniji od leta 1991 dalje, se je imenovalo Nordic Mobile Telephone (NMT). Leta 1996 se je v Sloveniji začela vzpostavitev in delovanje omrežja druge generacije (2G) imenovano Global System for Mobile Communication (GSM). GSM omrežje je prineslo pošiljanje kratkih SMS sporočil in SIM kartice (Hribar v Vehovar 2007).

Drugi generaciji mobilnih omrežij je sledila druga in pol generacija mobilnih omrežij (2,5G), ki je bila predvsem usmerjena v izboljšanje hitrosti prenosa podatkov preko mobilnih omrežij. Začel se je uporabljati General Packet Radio Service (GPRS), ki je teoretično omogočal prenos podatkov do hitrosti 115 kbit/s. Kmalu je sledila nadgradnja GPRS omrežja na Enhanced Date Rates for Global Evolution (EDGE 2,75G), ki je omogočala še hitrejši prenos podatkov. Teoretično do 473,6 kbit/s (Sauter 2011, 65).

Tretja generacija mobilnega omrežja (3G), imenovana Universal Mobile Telecommunications System (UMTS), je nadgradnja prejšnjega EDGE omrežja in omogoča občutno višje hitrosti od prejšnje generacije. Večje hitrosti UMTS omrežja omogočajo mnoge nove lokacijske storitve, večpredstavnostne storitve, kot je video na zahtevo, in seveda zelo hiter dostop do spleta (Hribar v Vehovar 2007).

Tehnologiji UMTS je sledila tretja in pol generacija (3,5G) imenovana High-Speed Protocol Access, ki je omogočala še višje hitrosti prenosa podatkov in z nadgradnjo na HSPA+ je tehnologija teoretično omogočala hitrosti v smeri proti uporabniku do 21,6 Mbit/s in od uporabnika 5,76 Mbit/s. Prvič pa sta bila mobilno omrežje in prenos

podatkov namenjena tako mobilnim kot stacionarnim uporabnikom (Sauter 2011, 175−205).

Najnovejša omrežja, ki so se pojavila v zadnjem času, imenovana Log Term Evolution (LTE), še niso čisto prava[1] omrežja četrte generacije, kot jih večina proizvajalcev mobilnih naprav trži, vendar omogočajo v teoriji hitrosti do 100 Mb/s. Glavna značilnost poleg visokih hitrosti je bistveni napredek v odzivnosti sistema (Mobitel Tehnik 2011).

LTE v Sloveniji od začetka leta 2013 ponujata tudi dva največja ponudnika mobilnih storitev Simobil in Mobitel. Ostale tehnologije, razen LTE, pa v Sloveniji ponujata še Tušmobil in T-2.

Tabela 3.2: Pokritost Slovenije z mobilnimi omrežji

	UMTS	HSDPA	HSUPA	LTE
Mobitel	90,60 %	80,63 %	80,63 %	42,24%
Si.mobil	90,00 %	88,30 %	30,00 %	ni podatka
Tušmobil	81,35 %	81,35 %	81,35 %	
T-2	35,00 %	35,00 %	35,00 %	-

Vir: Svet Idej (2013).

3.5.2 Brezžična lokalna omrežja

Brezžično lokalno omrežje (Wireless Local Area Network − WLAN ali WiFi) je računalniško omrežje kratkega dosega, ki deluje na osnovi radijskih valov frekvence 2,4 in 5 Ghz. WLAN je lokalno omrežje, v katerega se lahko povezujejo uporabniki s prenosnimi računalniki, pametnimi telefoni in tabličnimi računalniki brez žičnih povezav. Uporabniki se na ta omrežja povezujejo preko dostopnih točk, ki so lahko nezaščitene ali zaščitene z geslom, plačljive ali zastonj. Te dostopne točke pokrivajo določeno območje z brezžičnim signalom, preko katerega se uporabniki povežejo v lokalno omrežja in nato s svojimi napravami brskajo po spletu (Hribar v Vehovar 2007).

[1] Omrežje četrte generacije (4G) bo šele nadgradnja LTE omrežja, imenovana LTE-Advanvced, ki bo omogočala gigabitne hitrosti (Mobitel Tehnik 2011).

3.6 Uporabniški podatki

Osebni ali uporabniški podatki so tisti podatki, ki kažejo na lastnosti, stanje ali razmerje posameznika, ne glede na to, v kakšni obliki so izraženi. Posameznik ima pravico do varovanja svoje zasebnosti tako, da sam določi, na kakšen način in v kolikšni meri se lahko podatki o njem zbirajo, obdelujejo, shranjujejo in sporočajo drugim (Cvetko 1999, 30).

Podatke lahko delimo na občutljive in manj občutljive. Med prve sodijo podatki o značajskem in socialnem stanju, bančnem stanju, podatki o političnem, verskem ali filozofskem prepričanju, članstvu v sindikatih, zdravstvenem stanju ter tudi osebne fotografije, če sporočajo podatke o rasnem, narodnem ali narodnostnem poreklu. Med manj občutljive podatke spadajo podatki o imenu, priimku in naslovu stalnega prebivališča. Varstvo osebnih podatkov postaja vse bolj težavno predvsem zaradi hitrega razvoja informacijske tehnologije (Cvetko 1999).

Vse današnje mobilne naprave imajo neke vrst pomnilnik ali trdi disk, na katerem se shranjujejo naši podatki. Podatke v večini primerov shranjujemo sami. To so razne slike, video posnetki, dokumenti in sporočila. Veliko naših osebnih podatkov pa te naprave shranjujejo same, brez da bi uporabnik to vedel. Poleg podatkov, ki smo jih sami shranili, se shranjujejo še podatki o naših lokacijah in pogovorih, naša zgodovina brskanja po spletu, gesla, bančne številke in tudi podatki, ki so bili že zbrisani (Honan 2013).

Zbiranje in obdelava osebnih podatkov lahko poteka samo s privoljenjem posameznika (Cvetko 1999).

3.7 Informacijska varnost

Varnost je stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbene skupnosti in narave (Grizold 1999).

Sodobne razprave o varnosti se v zadnjem času usmerjajo predvsem na njene referenčne objekte (na koga se varnost nanaša), kdo ali kaj to varnost ogroža (grožnje varnosti) in seveda na kakšen način se varnost zagotavlja − varnostne mehanizme (kakšna oz. katera so sredstva za doseganje varnosti) (Liotta 2002, 474−475).

Pojem varnosti se nanaša na zelo širok spekter človekovega delovanja. Za potrebe svoje diplomske naloge se bom osredotočil predvsem na področje IKT[2], ki postaja referenčni objekt, na katerega se varnost nanaša. Varnost omrežij in informacij je zmožnost omrežja ali informacijskega sistema, da na določeni stopnji prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo ta omrežja ali sisteme (Svete 2005).

Informacijska varnost obravnava več različnih področij povezanih z informacijami. Ni omejena samo na računalniške sisteme, mobilne naprave, prav tako pa ne le na informacije v elektronski obliki. Nanaša se na vse vidike zaščite in varovanja informacij in podatkov v kakršnikoli obliki. Računalniški slovar podjetja IBM informacijsko varnost opredeljuje kot koncepte, tehnike, tehnične in administrativne ukrepe, ki se jih uporablja za zaščito informacij pred namernimi ali nenamernimi nepooblaščenimi pridobitvami, povzročanjem škode, razkritjem informacij, spremembo informacij, manipuliranje z njimi ali izgubo in uporabo informacij (McDaniel 1994, 94).

Državni slovar informacijske sistemske varnosti Združenih držav Amerike pa informacijsko varnost sistemov (INFOSEC) opredeljuje kot zaščito informacijskih sistemov pred nepooblaščenimi dostopi ali modifikacijami informacij ali v shranjeni obliki, v procesu ali prenosu ter zaščito pred zatajitvijo delovanja pooblaščenim uporabnikom in zagotovitvijo delovanja nepooblaščenim uporabnikom, vključno z

[2] IKT je Informacijsko komunikacijska tehnologija.

vsemi ukrepi za odkrivanje, dokumentiranje in zavračanje tovrstnih groženj (Hayden 2003, 33)

Grožnje informacijsko komunikacijski tehnologiji tako vključujejo širok spekter aktivnosti, vključujoč programske napake, ki lahko vodijo do sesutja ali ranljivosti sistemov; mobilne prevare in kraje; posameznike in zaposlene znotraj sistema, ki namerno onemogočajo delovanje sistemov; nedelovanje podpore fizične strukture; aktivnosti hekerjev in drugih računalniških kriminalcev; industrijsko in drugo zasebno in družbeno vohunjenje ter zlonamerno kodo in programe, kot so virusi, črvi, trojanski konji ipd. (Svete 2005).

3.8 Varnostna tveganja

Mobilne naprave, kot so pametni telefoni in tablični računalniki, so pomemben del vsakdanjega življenja. Imajo veliko računsko in spominsko zmogljivost, ovito v majhnem in lahko prenosnem formatu. Žal te prednosti pomenijo tudi tveganja, saj jih je zaradi majhnosti lažje odtujiti ali izgubiti, predvsem na javnih mestih. Manjše in zmogljivejše kot so naprave, večje je število tatvin (Bernik in Prislan 2012). Zaradi lahkih materialov, ki omogočajo, da so naprave vedno manjše in lažje, so današnje mobilne naprave veliko manj vzdržljive kot v preteklosti. Veliko naprav se kvari kot posledica pregrevanja ali mehanskih poškodb.

3.8.1 Okvara

Če pametni mobilni telefoni ali tablični računalniki, kljub polni bateriji, ne delujejo, gre v večini primerov za okvaro. Okvara je vse, kar nastane pri napravi, stroju, aparatu in onemogoča normalno delovanje. To je stanje, ki ni v skladu z normalnim delovanjem naprave, in nastane zaradi poškodb (SSKJ 2013a). Poškodbe so lahko vidne, če so na zunanjosti naprave, ali pa nevidne, če se skrivajo v notranjosti naprave.

3.8.2 Kraja

Kraja je jemanje česa s prisvojitvenim namenom na skrivaj in brez dovoljenja in vednosti lastnika (SSKJ 2013b). Zaradi svoje velike priljubljenosti današnje mobilne naprave privabijo vse več tatov. Pri kraji mobilne naprave ne gre samo za odtujitev materialne lastnine in izgubo premoženja. Ogrožene so tudi intimne informacije, ki posameznika opredeljujejo kot svojevrstno bitje in ga ločujejo od drugih. Govorimo lahko o kraji identitete (Caeton 2007, 12).

Krajo identitete lahko razumemo kot skupek dejanj, katerih cilj je kraja osebnih informacij določenega posameznika. Do kraje največkrat pride zaradi morebitne koristi, ki jo lahko kraja identitete prinese, kar je bolj poznano kot finančna kraja identitete (Monahan 2009, 156−157).

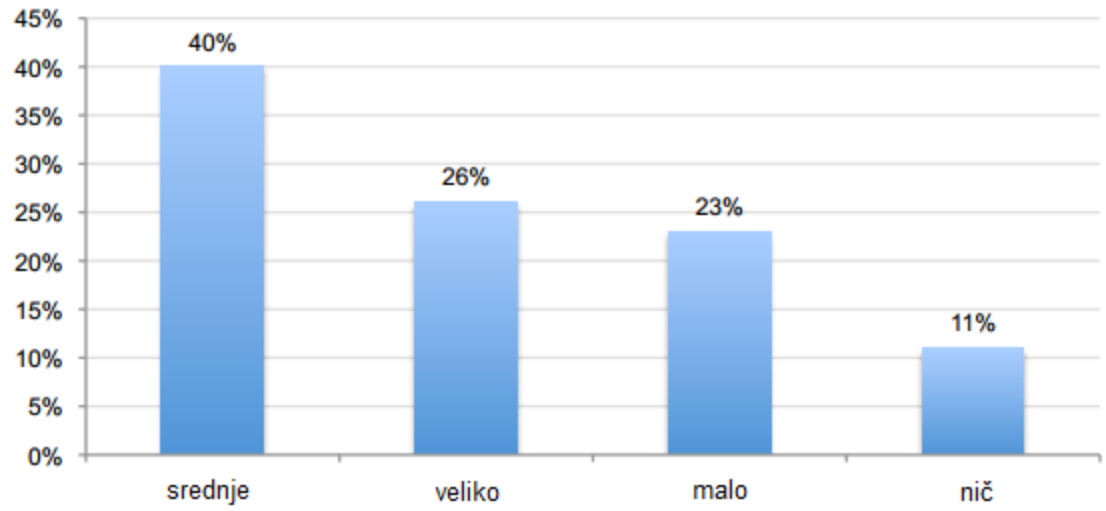
4 VARNOST IN TVEGANJA

V tem poglavju bom pregledal štiri glavna varnostna tveganja, ki se pojavljajo ob uporabi pametnih telefon in tabličnih računalnikov, in podal priporočila za varnejšo uporabo in delo z mobilnimi napravami.

4.1 FIZIČNI DOSTOP DO MOBILNE NAPRAVE IN NJENIH PODATKOV

Pametni telefoni in tablice imajo pomnilnik, kamor uporabniki shranjujemo velike količine osebnih, službenih ali ostalih podatkov. V raziskavi med ameriškimi potrošniki leta 2011 je kar 66 % uporabnikov mobilnih naprav povedalo, da ima na svojih napravah shranjeno od srednje veliko do veliko osebnih podatkov (glej Graf 4.1). Samo 11 % vseh uporabnikov ni imelo shranjenih nič podatkov (Ponemon Institute 2011).

Graf 4.1: Odstotek uporabnikov, ki imajo shranjene osebne podatke na mobilnih napravah



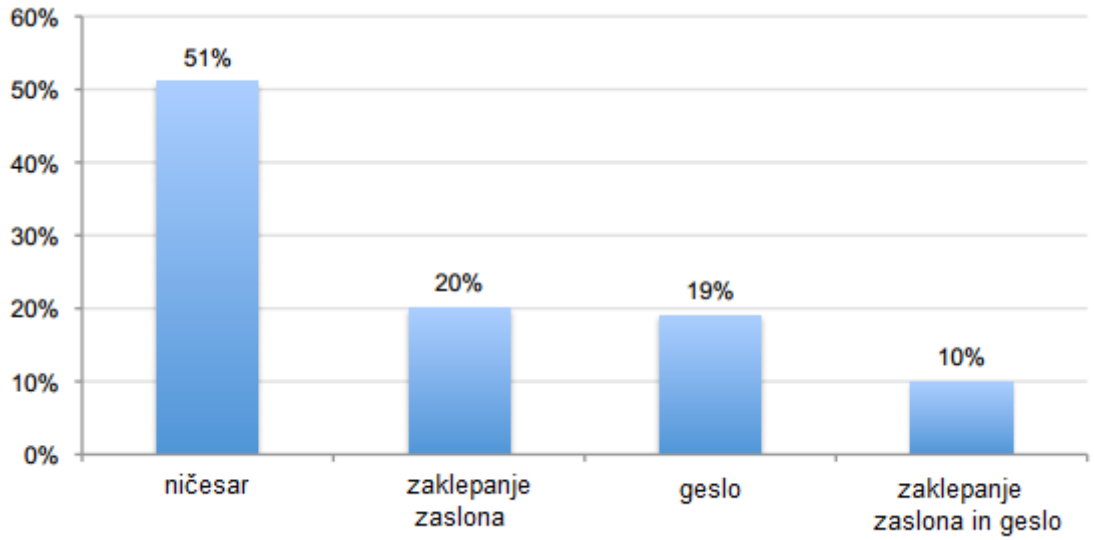
Vir: Ponemon Institute (2011).

Ker je fizični dostop do mobilnih naprav veliko lažji, so tudi vsi shranjeni podatki bolj izpostavljeni, za kar ni kriva mobilna naprava. Najšibkejši člen v samem procesu shranjevanja in prenašanja podatkov je uporabnik sam. Na splošno uporabniki niso dovolj seznanjeni z novimi napravami, njihovimi funkcijami, hranjenjem podatkov in njihovo varno uporabo. Uporabniki niso seznanjeni s tehnološkim razvojem, ne uporabljajo vgrajenih varnostnih funkcij v svojih napravah in so zato ranljivi.

Nepridipravi se ne trudijo več z vdiranjem v informacijske sisteme, osebne računalnike ali serverje, če lahko vse podatke dobijo z mobilnih naprav, ki so velikokrat manj zaščitene (Markelj in Bernik 2013).

Glavna zaščita pred nedovoljenim dostopom do naprave in njenih podatkov je zaklepanja svoje naprave z geslom ali zaklepanjem zaslona. Kar 51 % vseh ameriških uporabnikov mobilnih naprav je v raziskavi leta 2011 reklo, da ne uporablja nobene zaščite za dostop do svoje naprave (glej Graf 4.2). Zaklepanje zaslona ali geslo za vstop v telefon uporablja 39 % odstotkov vprašanih. Ostali uporabniki uporabljajo kombinacijo obojega (Ponemon Institute 2011).

Graf 4.2: Ali uporabljate zaklepanje zaslona ali geslo za dostop do svoje naprave



Vir: Ponemon Institute (2011).

Prvi korak do boljše zaščite je, da se prepreči nepooblaščenim osebam, da bi sploh prišle do podatkov. Pri pametnih telefonih je za zaščito najprej na voljo uporaba PIN[3] kode, ki jo vsak dobi poleg svoje SIM kartice. Druga možnost za vse mobilne naprave je zaklepanje zaslona. Naprave z operacijskim sistemom Android omogočajo veliko različnih možnosti zaklepanja zaslona in s tem naprave. Najboljša možnost je uporaba gesla. Sledita ji uporaba vzorca na zaslonu in PIN kode za zaklepanje zaslona (glej Sliko 4.1). Ostale možnosti so manj varne in jih je lažje zaobiti.

[3] PIN (Personal identification number) je osebna identifikacijska številka.

Slika 4.3: Možnosti zaklepanja zaslona v sistemu Android

Vir: Varni na internetu (2013).

Enake možnosti kot Android za zaklepanje zaslona z geslom imajo tudi naprave z operacijskim sistemom iOS in Windows Phone (glej Sliko 4.2).

Slika 4.4: Možnosti zaklepanja zaslona v sistemih iOS in Windows Phone

Vir: Varni na internetu (2013).

Gesla, ki jih uporabimo za zaščito, morajo zagotavljati željeni nivo varnosti. Pri oblikovanju gesel lahko uporabimo več metod, pomembno pa je, da je geslo čim daljše in čim kompleksnejše (mešanica črk in številk, po možnosti tudi mešanica velikih in malih črk ter številk). Težava pri geslih je, da si je kompleksna gesla težko zapomniti, zato se pri oblikovanju gesel vprašamo, ali želimo večjo varnost ali enostavnejšo uporabo. Pri oblikovanju gesel je potrebno paziti tudi na dejstvo, da lahko pri vnašanju gesel naletimo na različne lokalizacije sistemov oziroma različne razporede tipkovnic. Angleške tipkovnice tako ne vsebujejo slovenskih znakov (“č, š, ž”), nekatere črke so zamenjane (npr, “z” in “y”). Pred nastavitvijo gesla je zato treba preveriti, kateri jezik je nastavljen kot privzeti (Kovačič 2012).

Ker gesla in razne kombinacije niso popolnoma varne in jih je možno zaobiti ter tako priti mimo zaklepa naprave do uporabnikovih podatkov, ni priporočljivo shranjevati pomembnih podatkov v čisti obliki. Take podatke je priporočljivo šifrirati. Enkripcija pomeni spremembo podatkov v obliko imenovano "ciphertext" oz. šifriran tekst, ki ne more biti zlahka razumljiv nepooblaščeni osebi. Dekripcija pa je sprememba oblike podatkov v originalno obliko, ko jo lahko razume tudi nepooblaščena oseba (Rouse 2006).

Operacijski sistem Android omogoča od verzije 4.0 (Ice Cream Sandwich) naprej šifriranje podatkov v meniju varnost. Ostale naprave z različnimi operacijskimi sistemi omogočajo to s pomočjo aplikacij, ki jih lahko namestimo preko aplikacijskih trgovin.

4.2 VARNOST PODATKOV OB OKVARI, KRAJI, IZGUBI IN MOŽNOSTI POVRNITVE

Med mobilnimi napravami so najbolj ogroženi pametni telefoni, saj so v primerjavi s tabličnimi računalniki veliko manjši in jih je tako lažje odtujiti, izgubiti ali poškodovati. Po statističnih podatkih podjetja Micro Trax vsako leto 25 % Američanov izgubi ali poškoduje svoje pametne telefone. Vsako minuto je ukradenih 113 pametnih telefonov (MicroTrax 2013). Ukradena, izgubljena ali pokvarjena naprava predstavlja velik strošek za uporabnika. Poleg same vrednosti naprave je potrebno upoštevati še vrednost s tem izgubljenih podatkov, ki so bili shranjeni na napravi. Strošek je lahko še veliko večji, če so bili na napravi poleg osebnih podatkov shranjeni tudi kakšni službeni ali poslovni podatki.

Da se uporabniki izognejo stroškom izgubljenih ali ukradenih podatkov, morajo najprej za to poskrbeti sami. Kot je omenjeno že v prejšnjem poglavju, morajo uporabiti zaklep zaslona z geslom ali vzorcem, uporabo PIN kode ob vklopu telefonov in šifriranje pomembnih podatkov, da se prepreči nepooblaščen dostop do njih ob morebiti izgubi ali kraji mobilne naprave. Priporočljiva je tudi namestitev aplikacije, ki uporabniku omogoča brisanje podatkov na daljavo. Če imamo nameščeno tako aplikacijo, lahko v primeru kraje ali izgube naprave izbrišemo vse občutljive podatke in se zavarujemo pred tem, da bi naši podatki prišli v neprave roke (Dnevnik 2013).

S krajo, izgubo ali uničenjem mobilne naprave pa ni nujno, da uporabnik nikoli več ne vidi svojih podatkov. Vsi glavni operacijski sistemi imajo na mobilnih napravah možnost vključitve varnostnega kopiranja (sinhronizacije) podatkov, hranjenih na napravi. Sinhronizacija podatkov poteka v shrambo v oblaku (ang. *cloud storage*)[4]. Podatki so dostopni na vseh napravah (npr. koledarji in imeniki), ob okvari, izgubi ali kraji naprave pa lahko podatke zelo enostavno povrnemo v novo napravo. Ponudnika oblačne storitve ne moremo prosto izbirati − zanj se odločimo z nakupom naprave. Podatki o kontaktih, sporočilih in koledarju se pri Android napravah sinhronizirajo z računom Google, Windows Phone telefoni in tablice se sinhronizirajo na račun

[4] Shramba v oblaku je shranjevanje podatkov v oddaljeno bazo podatkov, ki se nahaja na neki oddaljeni lokaciji in je v lasti neke tretje osebe. Internet omogoča povezavo med uporabnikovo napravo in podatkovno bazo (Strickland 2011).

live.com pri Microsoftu. Apple pa za svoje naprave iPhone in iPad uporablja svojo oblačno storitev iCloud (Varni na Internetu 2013). Slike, video posnetke, glasbo, dokumente in ostale podatke lahko sinhroniziramo s temi oblačnimi storitvami ali pa izberemo katere druge, kot so Google Drive, Microsoft SkyDrive ali DropBox. Vsa zaščita dostopa do shramb v oblaku pa temelji samo na uporabnikovem geslu. Ponovno je pomembno, da se uporablja čim daljše in čim bolj zapleteno geslo.

Naprave z operacijskim sistemom Android omogočajo s pomočjo aplikacije Titanium Backup preprosto varnostno kopiranje celotnega sistema, ki se ga lahko povrne nazaj na napravo ob morebitni okvari, izgubi ali kraji. Za uporabo te aplikacije je potreben root naprave[5]. Vendar ta prinaša določene nove ranljivosti kot možnost naložitve zlonamerne programske opreme preko nalaganja po meri sprogramiranih aplikacij. Root naprave onemogoča uradno nadgradnjo operacijskega sistema ter lahko povzroči izgubo garancije (John 2011). Če upoštevamo prednosti in slabosti root naprave, na koncu slabosti odtehtajo prednosti. Rootanje naprav z operacijskim sistemom Andorid tako ni priporočljivo, saj poslabšajo varnost mobilnih naprav (Phelps 2013).

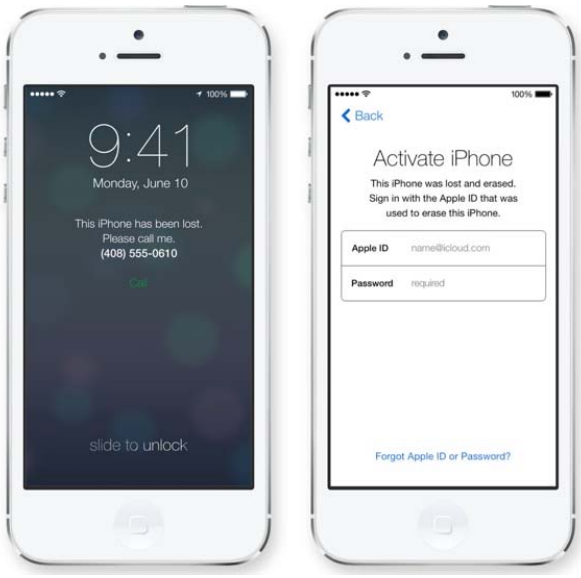
Poleg zaščite podatkov lahko uporabnik poskrbi tudi za lociranje naprave ob izgubi ali kraji in tako bistveno izboljša svoje možnosti za povrnitev naprave. Vse to je možno, če uporabnik pred tem na svojo napravo namesti kakšno aplikacijo, ki je zmožna pošiljati podatke o lokaciji telefona ali tablice. Ena izmed takih je Lookout, ki je na voljo za naprave z operacijskim sistemom Android in iOS. Če take aplikacije ni nameščene na mobilni napravi, se lahko uporabi aplikacijo Plan B (dostopna je samo za naprave z operacijskim sistemom Android 2.3 ali manj), ki se namesti na napravo na daljavo (pod pogojem, da je naprava povezana v WiFi ali mobilna podatkovna omrežja) in enako pošlje lokacijo naprave uporabniku (Lookout 2013).

Posebej za svoje naprave z operacijskim sistemom iOS Apple svojim uporabnim že dolga leta ponuja aplikacijo Find My iPhone (Najdi moj iPhone), ki podobno kot Lookout omogoča lociranje iOS naprave, njen zaklep in brisanje podatkov. Brisanje vseh podatkov iz naprave je tako predstavljalo neke vrste predajo ter nepridipravom, ki niso naprave ukradli z namenom polastitve naših podatkov, omogočalo, da prodajo

[5] Root naprave je pridobitev administratorskih pravic nad svojo napravo, kar omogoča uporabniku, da lahko na napravo nalaga prilagojeno ali po meri sprogramirano programsko opremo (aplikacije) ali odstranjuje sistemske aplikacije, ki jih je naložil na napravo prodajalec in jih ne potrebuje (John 2011).

naprej popolnoma prazen telefon. V najnovejšo verzijo operacijskega sistema iOS (iOS 7) je Apple vključil možnost, imenovano Activation Lock (Aktivacijska ključavnica), ki v kombinaciji z aplikacijo Find My iPhone in brisanjem vseh podatkov zaklene telefon in ga naredi neuporabnega, dokler se v njega uporabnik ne vpiše ponovno s svojim Apple uporabniškem imenom in geslom (glej Sliko 4.3). To naredi samo preprodajo telefona manj privlačno, saj je takšen telefon neuporaben (Eddy 2013).

Slika 4.5: Activation Lock



Vir: Eddy (2013).

Poleg vseh omenjenih stvari za ohranitev podatkov in možnosti povrnitve naprave je priporočljivo, da uporabnik v primeru kraje ali izgube mobilne naprave takoj pokliče svojega operaterja in prekliče SIM kartico, če gre za mobilni telefon. Če ima preko mobilne naprave omogočen neposreden dostop do drugih računov (elektronska pošta, družbena omrežja), takoj spremeni vsa gesla. Nekdo lahko z naprave dostopa do uporabniških profilov. Če se krajo naprave prijavi policiji, naj jim uporabnik posreduje tudi IMEI[6] številko naprave, ki je zapisana na embalaži, na garancijskem listu in na nalepki pod baterijo mobilnega telefona. IMEI se izpiše tudi na zaslonu telefona po vnosu ukaza *#06# (Dnevnik 2013).

[6] IMEI (International Mobile Station Equipment Identity) je mednarodna identifikacijska številka mobilne naprave .

4.3 OMREŽNO POVEZOVANJE

Nepogrešljiva lastnost pametnih telefonov in tabličnih računalnikov je omrežna povezljivost. Vsi pametni telefoni omogočajo povezavo s spletom preko brezžične lokalne povezave (WiFi) ali s prenosom podatkov mobilnega operaterja. Vsi tablični računalniki omogočajo povezavo preko WiFi, nekateri bolj redki in dražji pa tudi povezavo s prenosom podatkov mobilnega operaterja. Povezave s prenosom podatkov mobilnega operaterja so možne skoraj po celi Sloveniji, saj dva največja operaterja (Mobitel in Simobil) pokrivata preko 90 % vsega prebivalstva (glej Tabelo 3.2) z UMTS signalom (Svet Idej 2013). Brezžična lokalna omrežja so na voljo doma, v službi, šoli, hotelu, baru ali na ulici. Nekatera od teh omrežij so bolj varna kot druga (Varni na internetu 2013).

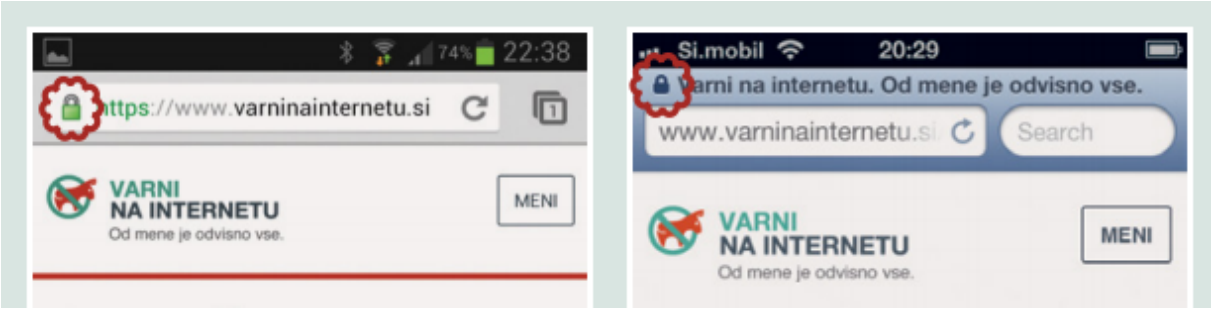
Najvarnejša je uporaba mobilnega interneta preko prenosa podatkov. Za dokaj dobro varnost mobilnih omrežij in povezave je poskrbljeno s strani samih operaterjev. Slaba stran tovrstne uporabe so morebitni visoki stroški, ki nastanejo pri tem (Varni na internetu 2013). Večja varnostna tveganja predstavljajo brezžična lokalna omrežja. Večino WiFi dostopnih točk ni šifriranih, zato lahko vsakdo preverja podatke, ki jih mobilna naprava pošlje in prejme. Preverjanje brezžičnih lokalnih omrežij ni težko, potreben je le radoveden posameznik z brezplačnimi orodji in nekaj prostega časa. Obstaja ker nekaj programov, ki lahko prikažejo te podatke (Web-Center 2012). Prav posebno previdnost pa zahteva t. i. Ad-hoc[7] brezžično omrežje, ki ga ustvari nekdo kar na svojem računalniku. V tem primeru se mobilna naprava poveže neposredno na prenosnik neznanca. Taka omrežja so ponavadi prikazana z nekoliko drugačno ikono (Varni na internetu 2013).

Da bi se uporabniki zavarovali pred nepooblaščenim preverjanjem podatkov med brskanjem po spletu, je dobro, da vzpostavljajo povezavo z brezžičnim omrežjem, ki zahteva omrežni varnostni ključ (protokol WPA ali WPA2). Na brezžična lokalna omrežja se povezujemo, le ko ga potrebujemo, v nasprotnem primeru izključimo samodejno povezovanje na dostopne točke. Sinhronizacije mobilne naprave v oblačne shrambe ne opravljamo preko nezaščitenih brezžičnih omrežij. Enako velja tudi za finančne transakcije − ne vpisujemo številk kreditnih kartic ali opravljamo

[7] Ad-hoc prihaja iz lat. in pomeni 'za ta namen, rešitev, ki je specifična za to nalogo ali problem'.

bančne storitve na nezaščitenih omrežjih (Varni na internetu 2013). Če že moramo v nezaščitenih javnih omrežjih uporabiti storitev, kjer moramo posredovati uporabniško ime in geslo (elektronska pošta, družbena omrežja), naredimo to na straneh, ki so zavarovane s SSL šifriranjem (glej Sliko 4.4). Če je spletna stran zavarovana, se bo spletni naslov začel s "https" namesto s "http" in v večini brskalnikov je to prikazano s ključavnico, ki nakazuje, da je SSL šifriranje v uporabi. Nepooblaščene osebe vidijo le nekaj podatkov, ki jih ob SSL šifriranju ne razumejo (Web-Center 2012).

Slika 4.6: SSL šifriranje na Android in iOS operacijskem sistemu



Vir: Varni na internetu (2013).

Poleg zgoraj naštetih varnostnih ukrepov lahko uporabniki na svojih mobilnih napravah ali dostopni točki uporabijo tudi Virtual Private Network (VPN)[8]. Če je uporabnik povezan z VPN, vsi njegovi podatki potujejo skozi šifriran tunel, ki varuje podatke pred nepooblaščenimi osebami. Operacijska sistema iOS in Android sta operacijska sistema, ki podpirata VPN (Web-Center 2012).

Če svoje mobilne naprave uporabljamo v večini primerov za hipno sporočanje (*ang. instant messaging)*[9]*,* lahko sporočila zaščitimo s šifriranjem. Uporabiti moramo protokol oziroma dodatek, ki ga je skupina pod vodstvom kriptologa Iana Goldberga začela razvijati leta 2004. Gre za OTR oz. Off-the-Record, ki “na vrhu” kateregakoli podprtega IM protokola omogoča šifriranje, avtentikacijo in zanikanje. To pomeni, da so šifrirana sporočila avtenticirana (overjena), avtentikacija pa je mogoča samo, ko je sporočilo poslano, kasneje pa ne več. Protokol omogoča tudi zanikanje vsebine sporočila (potem, ko je bilo sporočilo uspešno poslano, oziroma tudi v primeru, če je bilo sporočilo prestreženo) (Kovačič 2013).

[8] VPN je virtualno privatno omrežje.

[9] Hipno sporočanje je posebna oblika komunikacije preko spleta, ki omogoča hitro izmenjavo tekstovnih sporočil preko omrežja. Tako je hipno sporočanje pravzaprav analogno SMS sporočilom, le da poteka preko spleta. Sodobni IM odjemalci prenašajo tudi datoteke, zvočna in video sporočila ter še marsikaj (Kovačič 2013).

4.4 VARNOST PRI UPORABI APLIKACIJ

Z veliko razširjenostjo pametnih telefonov in tabličnih računalnikov so se v zadnjih letih razširile tudi aplikacije. Slednje so dodana vrednost mobilnih naprav, ki si jih lahko uporabniki poljubno prenašajo na svoje naprave iz različnih aplikacijskih trgovin (Google Play, App Store itd.) ter so izredno enostavne in hitre za namestitev. Uporabniki se ne zavedajo, da s tem, ko brezskrbno nameščajo aplikacije, izpostavljajo svojo mobilno napravo velikim tveganjem. Največjo grožnjo mobilnim napravam predstavljajo aplikacije, ki vsebujejo oglaševalsko programsko opremo (adware), in aplikacije, ki vsebujejo zlonamerno programsko kodo (malware) (Varni na internetu 2013).

4.4.1 Oglaševalska programska oprema

Adware je tip programske opreme, ki doda oglaševano vsebino, potencialno na način, ki je nezaželen s strani uporabnikov, v programe, aplikacije in spletne brskalnike. Mnoge aplikacije, ki vsebujejo oglaševalsko programsko opremo, imajo sposobnost sledenja uporabnikovega vedenja ali premikanja (LavaSoft 2013).

V raziskavi, ki so jo izvedli na Cambriški univerzi, so ugotovili, da je 73 % aplikacij v aplikacijskih trgovinah brezplačnih. Od teh jih je 80 % uporabljalo oglaševalsko programsko opremo znotraj aplikacije kot glavni vir zaslužka. Zastonjske aplikacije so med uporabniki veliko bolj priljubljene. Samo 20 % plačljivih aplikacij je bilo prenesenih več kot stokrat in samo 0,2 % plačljivih aplikacij je bilo prenesenih več kot deset tisočkrat. Po drugi strani pa je bilo 20 % vseh brezplačnih aplikacij prenesenih več kot deset tisočkrat (Manoogian 2012).

Če na svojo napravo naložimo brezplačno aplikacijo, ki uporablja oglaševanje za svoj vir dohodka, se lahko zgodi, da je bila cena za uporabnika skrita nekje drugje. Aplikacij je veliko, težava pa je, da običajno zahtevajo veliko dovoljenj (ang. *permissions*), ki jih uporabniki avtomatsko podelijo aplikaciji, ne da bi sploh prebrali, kaj želi od nas. Če uporabnik naloži samo preprosto aplikacijo, ki omogoči, da lahko svoj telefon uporablja kot svetilko ali pa zabavno igro, je čisto mogoče, da se strinja, da aplikacija dostopa do njegovih klicev, kontaktov, da lahko spreminja podatke na

spominski kartici, da lahko bere SMS sporočila, sledi uporabniku preko GPS[10] in deli podatke o uporabniku z drugimi, npr. z oglaševalci. Zgodi se lahko tudi, da aplikacije snemajo zvok in sliko brez dovoljenja, poljubno pišejo ali brišejo po pomnilniku ali pa celo samovoljno aktivirajo kakšno plačljivo storitev (Varni na internetu 2013).

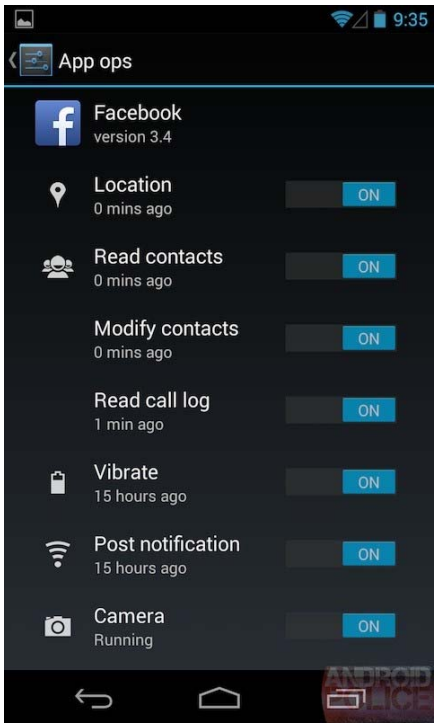
Aplikacije z oglaševalsko programsko opremo ne povzročajo samo škode uporabnikom, ampak tudi bateriji same naprave. Raziskovalci pri Microsoftu so s testiranjem priljubljene igre Angry Birds ugotovili, da je bilo 20 % energije iz baterije naprave namenjene samemu igranju igre, medtem ko je bilo kar 45 % energije namenjene iskanju lokacije uporabnika, ki lahko služi za oglaševanje (Pash 2012).

Podjetje Bitdefender, ki se ukvarja s spletno varnostjo, je v svoji raziskavi mobilnih aplikacij ugotovilo, da so aplikacije tako na operacijskem sistemu Android kot iOS enako vsiljive in radovedne. Ugotovili so, da ima več kot 45 % vseh iOS in 34 % Android aplikacij zmožnosti določanja točne lokacije uporabnika. Dobrih 7 % Android in skoraj 19 % iOS aplikacij lahko pregleduje in pošilja na oddaljene serverje kontakte uporabnikov. Več kot 14 % vseh Android aplikacij posreduje uporabnikov e-mail naslov oglaševalcem. 8 % Android aplikacij tudi posreduje uporabnikovo telefonsko številko (Bitdefender 2013).

Za varno rabo mobilnih aplikacij mora uporabnik najprej vedno preveriti, katera dovoljenja zahteva aplikacija. Če jih zahteva preveč, naj raje naloži drugo aplikacijo, saj je izbira pestra. Plačljive aplikacije običajno od uporabnika zahtevajo manj dovoljenj. Uporabniki naprav z operacijskim sistemom iOS lahko podelijo dovoljenja aplikaciji, ko jo zaženejo in ji tako onemogočijo dostop do nekaterih resursov (Bitdefender 2013). Na napravah z Androidom podeli uporabnik vsa dovoljenja aplikaciji ob namestitvi. Vendar je z nadgradnjo operacijskega sistema Android na verzijo 4.3 (Jelly Bean) možna namestitev sistemske aplikacije, imenovane App ops (glej Sliko 4.5), ki omogoča uporabniku, da za vsako aplikacijo posebej določa njena dovoljenja (Amadeo 2013).

[10] GPS (Global Positioning System) je sistem globalnega določanja lege.

Slika 4.7: Aplikacija App ops



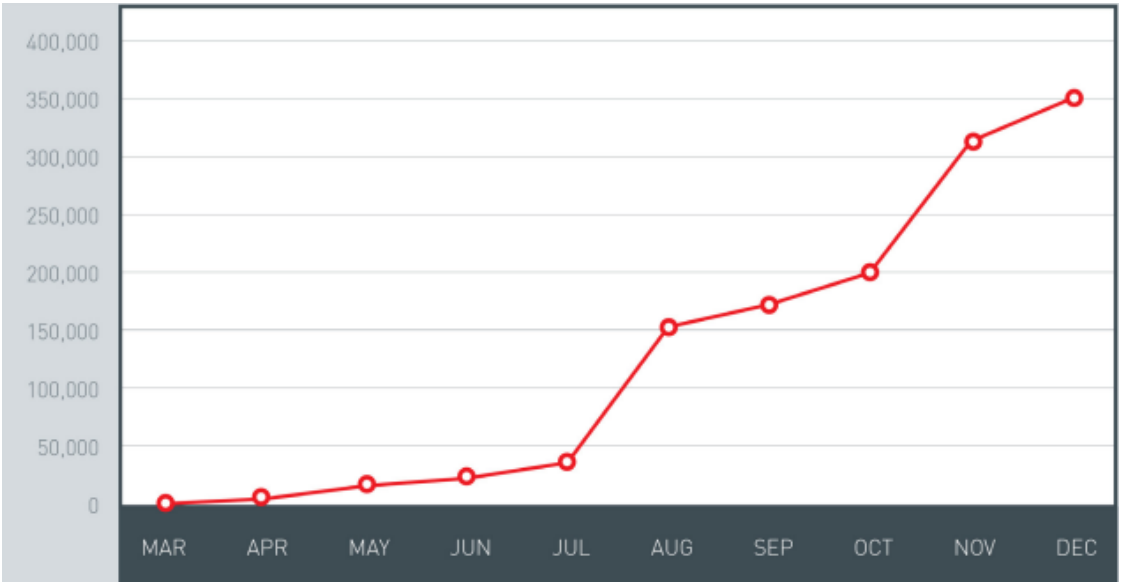
Vir: Android Police (2013).

4.4.2 Zlonamerna programska koda

V zadnjem letu se je povečala razširjenost zlonamerne programske kode s posebnim poudarkom na operacijskem sistemu Android. Ne samo da ima operacijski sistem Android največji delež naprav na trgu, zasnovan je tudi na bolj odprti platformi, ki izvira iz Linuxa[11] kot pa Windows Phone ali iOS in je posledično bolj ranljiv za napade hekerjev. Pri varnostnem podjetju Trend Micro so ugotovili, da je bilo v letu 2012 zaznanih 350.000 groženj zlonamerne programske opreme (glej Graf 4.3). V podjetju predvidevajo, da bi se lahko to število do konca leta 2013 povečalo na en milijon (Trend Micro 2013).

[11] Linux je prost operacijski sistem, podoben Unixu s prosto dostopno izvorno kodo.

Graf 4.8: Razširjenost zlonamerne programske kode za naprave s sistemom Android v letu 2012



Vir: Trend Micro (2013).

V večini primerov gre za trojanske konje, skrite v aplikacijah ali SMS sporočilih, ransomware (koda, ki onemogoči delovanje naprave in zahteva plačilo za ponovno vzpostavitev delovanja) in zlonamerno kodo s področja e-bančništva, ki se predstavlja kot varnostni certifikati in jo uporabnik naloži na svojo napravo (Arsene 2013).

Uporabnik najlažje okuži svojo napravo z nameščanjem nepreverjenih aplikacij iz neuradnih aplikacijskih trgovin, ki vsebujejo škodljivo kodo, ali z odpiranjem neznanih povezav v SMS sporočilih ali na spletu. Uporabnik najlažje ugotovi, ali je naprava okužena, če se baterija naprave izredno hitro prazni, klici postanejo popačeni ali prekinjajo, račun za telefon se enormno poveča, naprava deluje počasneje, poveča se tudi poraba podatkovnih podatkov (Cosi 2013).

Uporabniki se lahko zavarujejo pred zlonamerno programsko kodo z namestitvijo antivirusnega programa. Poznamo jih predvsem za računalnike, vendar so se s potrebo po zaščiti pametnih telefonov in tabličnih računalnikov pojavile različice tudi za te naprave. Eden boljših in brezplačnih je Avast Mobile Security&Antivirus (Google Play 2013).

Aplikacije prenašamo izključno iz zaupanja vrednih virov, kot so uradne aplikacijske trgovine. Vedno preučimo aplikacijo in avtorja, pregledamo komentarje ostalih uporabnikov in preverimo oceno aplikacije. Redno posodabljamo operacijski sistem in aplikacije, saj posodobitve odpravijo na novo odkrite varnostne luknje. Uporabniki morajo biti pazljivi tudi pri elektronski pošti in socialnih omrežjih, ker lahko tudi tu staknejo škodljivo programsko opremo (Rodriguez 2011).

5 ZAKLJUČEK

5.1 Ugotovitve

Namen diplomskega dela je bil narediti pregled in analizo ključnih tveganj oziroma varnostnih sklopov, povezanih z uporabo tabličnih računalnikov in pametnih telefonov, ter podati predloge za varnejšo uporabo teh naprav. Osredotočil sem se na štiri glavne sklope.

Iz pregleda sklopa Fizičnega dostopa do mobilne naprave in njenih podatkov sem ugotovil, da več kot polovica uporabnikov shranjuje na svoje naprave veliko osebnih podatkov, ki so zaradi lahkega dostopa do samih mobilnih naprav pogosto izpostavljeni kraji. Glavna zaščita pred nepooblaščenim dostopanjem do uporabnikovih podatkov na napravah je zaklepanje zaslona (z geslom ali vzorcem) ali zaklepanje naprave (geslo). Raziskave med ameriškimi uporabniki mobilnih naprav so pokazale, da kar 51 % uporabnikov ne uporablja nobene vrste zaklepanja. Ker je zaklepanje naprave in zaslona z geslom varno samo toliko, kot je varno oziroma močno samo geslo, je pri izbiri gesla pomembno, da je čim daljše in čim bolj kompleksno (mešanica črk in številk, po možnosti tudi mešanica velikih in malih črk ter številk). Ker pa gesla in razne kombinacije niso popolnoma varne, je priporočljivo podatke tudi šifrirati, da tako postanejo nerazumljivi nepooblaščeni osebi.

V sklopu varnosti uporabnikovih podatkov ob okvari, izgubi ali kraji uporabnikove naprave sem pregledal rešitve, kako se zavarovati pred izgubo podatkov in s tem povezanih stroškov. Kraji in izgubi so zaradi svoje majhnosti izpostavljeni predvsem pametni telefoni. V Združenih državah Amerike je vsako minuto ukradenih 113 pametnih telefonov. Da ne bi uporabniki za vedno izgubili svojih podatkov, imajo vsi glavni operacijski sistemi na mobilnih napravah možnost vključitve varnostnega kopiranja (sinhronizacije) podatkov, hranjenih na napravi. Sinhronizacija podatkov poteka v shrambo v oblaku. Poleg zaščite podatkov lahko uporabnik tudi poskrbi za lociranje naprave ob izgubi ali kraji in tako bistveno izboljša svoje možnosti za povrnitev naprave. Vse to je možno, če uporabnik pred tem na svojo napravo namesti aplikacijo, ki je zmožna pošiljati podatke o lokaciji telefona ali tablice. Priporočljivo je tudi, da spremeni vsa gesla raznih storitev (elektronska pošta,

družbena omrežja), do katerih je dostopal z napravo in krajo ali izgubo prijavi policiji ter svojemu operaterju.

Iz pregleda sklopa Omrežno povezovanje sem ugotovil, da je najvarnejša uporaba mobilnega interneta preko prenosa podatkov. Za dokaj dobro varnost mobilnih omrežij in povezave je poskrbljeno s strani samih operaterjev. Slaba stran tovrstne uporabe so morebitni visoki stroški, ki nastanejo pri tem. Večja varnostna tveganja predstavljajo brezžična lokalna omrežja. Večina WiFi dostopnih točk ni šifriranih, zato lahko vsakdo preverja podatke, ki jih mobilna naprava pošlje in prejme. Da bi se uporabniki zavarovali pred nepooblaščenim preverjanjem podatkov med brskanjem po spletu, je priporočljivo, da vzpostavljajo povezavo z brezžičnim omrežjem, ki zahteva omrežni varnostni ključ (protokol WPA ali WPA2). Sinhronizacije mobilne naprave v oblačne shrambe ne opravljamo preko nezaščitenih brezžičnih omrežij. Enako velja tudi za finančne transakcije − ne vpisujemo številk kreditnih kartic ali opravljamo bančnih storitev na nezaščitenih omrežjih. Če že moramo v nezaščitenih javnih omrežjih uporabiti storitev, kjer moramo posredovati uporabniško ime in geslo (elektronska pošta, družbena omrežja), naredimo to na straneh, ki so zavarovane s SSL šifriranjem. Če pa svoje mobilne naprave uporabljamo v večini primerov za kratkotrajno sporočanje, lahko sporočila zaščitimo s šifriranjem.

V sklopu Varnosti pri uporabi mobilnih aplikacij sem ugotovil, da so se slednje v zadnjih letih zelo razširile. Vendar se uporabniki ne zavedajo, da s tem, ko brezskrbno nameščajo aplikacije, izpostavljajo svojo mobilno napravo velikim tveganjem. Največjo grožnjo mobilnim napravam predstavljajo aplikacije, ki vsebujejo oglaševalsko programsko opremo (adware), in aplikacije, ki vsebujejo zlonamerno programsko kodo (malware). Če na svojo napravo naložimo brezplačno aplikacijo, ki uporablja oglaševanje za svoj vir dohodka, se lahko zgodi, da ob namestitvi zahteva veliko dovoljenj. S tem, ko se uporabnik strinja, omogoči aplikaciji dostop do praktično vseh informacij na svoji napravi. Aplikacija dostopa do klicev, kontaktov lahko spreminja podatke na spominski kartici, bere SMS sporočila, sledi uporabniku preko GPS in deli podatke o uporabniku z drugimi, na primer z oglaševalci. Uporabnik mora vedno preveriti, katera dovoljenja zahteva aplikacija. Če jih zahteva preveč, naj raje naloži drugo aplikacijo, saj je izbira raznolika. Plačljive aplikacije običajno od uporabnika zahtevajo manj dovoljenj.

V zadnjem letu se je povečala razširjenost zlonamerne programske kode (malware) s posebnim poudarkom na operacijskem sistemu Android, ker je najbolj razširjen in odprtokoden. Uporabnik najlažje okuži svojo napravo z nameščanjem nepreverjenih aplikacij iz neuradnih aplikacijskih trgovin, ki vsebujejo škodljivo kodo, ali odpiranjem neznanih povezav v SMS sporočilih ali na spletu. Uporabniki se lahko pred zlonamerno programsko kodo zavarujejo z namestitvijo antivirusnega programa.

5.2 Sklep

Danes trg pametnih telefonov in tabličnih računalnikov izredno hitro raste. Vsak dan je prodanih več naprav, ki nam vedno bolj nadomeščajo osebne računalnike. Z večjim številom naprav se večajo tudi varnostna tveganja ob njihovi uporabi. Težava nastane zato, ker se večina uporabnikov ne zaveda teh tveganj in so o njihovi brezskrbni uporabi prepričani, da je uporaba mobilne naprave vsaj toliko varna kot uporaba osebnega računalnika.

Prvo hipotezo »**Tablični računalniki in pametni telefoni sami po sebi niso dovolj varni za uporabo«** lahko sprejmem, saj so kupljene mobilne naprave opremljene z vgrajenimi zaščitnimi funkcijami, ki pa žal niso vključene in je vse odvisno od uporabnika, če jih želi uporabljati.

Sprejmem lahko tudi drugo hipotezo »**Uporabniki lahko sami poskrbijo za manj tvegano in varnejšo uporabo, svojih tabličnih računalnikov in pametnih telefonov«** s tem, ko uporabljajo že vgrajene funkcije zaščite v mobilne naprave in redno sinhronizirajo svoje podatke ter se ne povezujejo na nezaščitena lokalna brezžična omrežja.

Od uporabnikov ni dovolj, da svojo novo mobilno napravo samo prižgejo in jo začnejo uporabljati, pomembno je tudi, da se bolj poglobijo v same funkcije in nevarnosti, ki grozijo njihovim napravam. Če uporabniki poznajo grožnje, lahko ustrezno upravljajo s tveganji in zagotovijo varnejše delo in višjo varnost same naprave.

6 LITERATURA

1. A., John. 2011. *What is Rooting on Android? The Advantages and Disadvantages.* Dostopno prek: http://droidlessons.com/what-is-rooting-on-android-the-advantages-and-disadvantages/ (1. avgust 2013).
2. Amadeo, Ron. 2013. *App Ops: Android 4.3's Hidden App Permission Manager, Control Permissions For Individual Apps!.* Dostopno prek: http://www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-app-permission-manager-control-permissions-for-individual-apps/ (30. julij 2013).
3. Arsene, Liviu. 2013. *Malware Shifting from SMS Trojans to Ransomware and Banking.* Dostopno prek: http://www.hotforsecurity.com/blog/malware-shifting-from-sms-trojans-to-ransomware-and-banking-6651.html (30. julij 2013).
4. AT&T. 2013. *What is a smartphone?* Dostopno prek: http://www.att.com/esupport/article.jsp?sid=KB101001&cv=821&title=What%20is%20a%20smartphone%3F#fbid=2fzdaUX7vLn (10. julij 2013).
5. Bernik, Igor in Katja Prislan. 2012. *Upravljanje varnostnih tveganj pri rabi mobilnih naprav.* Dostopno prek: Bernik_Prislan.pdf (12. julij 2013).
6. Bitdefender. 2013. *Mobile Operating System Wars - Android vs. iOS.* Dostopno prek: http://www.bitdefender.com/files/News/file/bd-study-ios.pdf (30. julij 2013).
7. Caeton, A. Danie. 2007. The Cultural Phenomeon of Identity Theft and the Domestication od the World Wide Web. *Bulletin of Science, Technology & Society* 27 (1): 11−23.
8. Cvetko, Aleksej. 1999. *Varovanje zasebnosti v delovnih razmerjih.* Ljubljana: Gospodarski vestnik.
9. Cosi, Catalin. 2013. *5 Signs Your Android Smartphone Is Infected With Malware.* Dostopno prek: http://readwrite.com/2013/04/23/5-signs-android-smartphone-infected-malware#awesm=~od5Dxv0okt1OVA (30. julij 2013).
10. Digital News Test Kitchen. 2010. *Market Overview 2010: The state of the smartphone revolution.* Dostopno prek: smartphone-market/ (10. julij 2013).
11. *Dnevnik.* 2013. Kako ohraniti varnost na pametnih mobilnih napravah, 28. januar. Dostopno prek: kako-ohraniti-varnost-na-pametnih-mobilnih-napravah# (1. avgust 2013).

12. Eddy, Max. 2013. *New Features in iOS 7 Make iPhone More Secure Than Ever.* Dostopno prek: http://securitywatch.pcmag.com/mobile-security/312473-new-features-in-ios-7-make-iphone-more-secure-than-ever (1. avgust 2013).
13. Geek. 2009. *Smartphone buyers guide: Operating system.* Dostopno prek: http://www.geek.com/smartphone-buyers-guide/operating-system/ (11. julij 2013).
14. Google Play. 2013. *Mobile Security & Antivirus.* Dostopno prek: https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity (30. julij 2013).
15. Grizold, Anton. 1999. *Evropska varnost.* Ljubljana: Fakulteta za družbene vede.
16. Hayden, Michael. 2003. *National information assurance glossary, Committee on national Security Systems.* Dostopno prek: Assets/pdf/cnssi_4009.pdf (12. julij 2013).
17. Honan, Mat. 2013. *Break Out a Hammner: You'll Never Belive the Data "Wiped" Smartphones Store.* Dostopno prek: smartphone-data-trail/all/ (11. julij 2013).
18. Hribar, Uroš. 2007. Mobilne refleksije. V *Razvoj mobilnih tehnologij,* ur. Vasja Vehovar, 285—322. Ljubljana: Fakulteta za družbene vede.
19. IDC. 2013. *Android and iOS Combine 91.1 % of the Worldwide Smartphone OS Market in 4Q12 and 87.6 % for the Year, According to IDC.* Dostopno prek: http://www.idc.com/getdoc.jsp?containerId=prUS23946013#.UR0SHVpMStU (11. julij 2013).
20. Kovačič, Matej. 2012. *Gesla in varna hramba gesel (mala šola informacijske varnosti, 1. del).* Dostopno prek: http://pravokator.si/index.php/2012/07/30/gesla-in-varna-hramba-gesel-mala-sola-informacijske-varnosti-1-del/ (31. julij 2013).
21. Kovačič, Matej. 2013. *Šifriranje hipnih sporočil (mala šola informacijske varnosti, 11. del).* Dostopno prek: mala-sola-informacijske-varnosti-11-del/ (6. avgust 2013).
22. LavaSoft. 2013. *Malware from A to Z.* Dostopno prek: lavasoft.com/mylavasoft/securitycenter/spyware-glossary#Adware (30. julij 2013).
23. Liotta, H., Peter. 2002. *Boomerang Effect: The Convergaence of National and Human Security.* Security Dialouge (33) 3: 474−475.
24. Lookout. 2013. *Security for the post-PC era.* Dostopno prek: https://www.lookout.com/ (1. avgust).
25. McDaniel, George. 1994. *IBM Dictionary of computing.* New York: McGraw – Hill.

26. Manoogian, John. 2012. *How Free Apps Can Make More Money Than Paid Apps.* Dostopno prek: http://techcrunch.com/2012/08/26/how-free-apps-can-make-more-money-than-paid-apps/ (30. julij 2013).
27. Merkelj, Blaž in Igor Bernik. 2013. *Mobile devices and effective information security.* Innovative Issues and Approaches in Social Sciences (6) 2: 40−53.
28. MicroTrax. 2013. *Alarming Statistics.* Dostopno prek: http://www.micro-trax.com/statistics/ (1. avgust 2013).
29. Mobitel Tehnik. 2011. *LTE: Dobrodošli v prihodnost mobilnih komunikacij.* Dostopno prek: http://tehnik.mobitel.si/lte-dobrodosli-v-prihodnost-mobilnih-komunikacij/ (11. julij 2013).
30. Mobitel Tehnik. 2012a. *Delež uporabnikov pametnih telefonov pri nas vztrajno raste predvsem na račun Androida.* Dostopno prek: http://tehnik.mobitel.si/delez-uporabnikov-pametnih-telefonov-pri-nas-vztrajno-raste-predvsem-na-racun-androida/ (9. julij 2013).
31. --- 2012b. *Uporaba mobilnih aplikacij strmo narašča.* Dostopno prek: http://tehnik.mobitel.si/uporaba-mobilnih-aplikacij-strmo-narasca/ (11. julij 2013).
32. MobiThinking. 2013. *Global mobile statistics 2013 Part A: Mobile subscribers; handset market share; mobile operators.* Dostopno prek: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers (10. julij 2013).
33. Moj Mikro. 2011. *Dolga pot od zgodovinskih do sodobnih tablic.* Dostopno prek: http://www.mojmikro.si/pod_lupo/strojna_oprema/dolga_pot_od_zgodovinskih_do_sodobnih_tablic (10. julij 2013).
34. --- 2013. *Zgodovina tabličnih računalnikov.* Dostopno prek: http://www.mojmikro.si/preziveti/kar_tako/zgodovina_tablicnih_racunalnikov (10. julij 2013).
35. Monahan, Torin. 2009. Identity theft vulnerability. *Theoretical Criminology* 13 (2): 155−176.
36. Pash, Adam. 2012. *Free, Ad-Supported Mobile Apps Are Killing Your Battery.* Dostopno prek: http://lifehacker.com/5894619/free-ad+supported-mobile-apps-are-killing-your-battery (30. julij 2013).
37. Phelps, Thomas. 2013. *To Root or Not to Root.* Dostopno prek: http://google.about.com/od/socialtoolsfromgoogle/a/root-android-decision.htm (30. julij 2013)

38. Ponemon Institute. 2011 *Smartphone Security: Survey of U.S. consumers.* Dostopno prek: http://aa-download.avg.com/filedir/other/Smartphone.pdf (31. julij 2013).
39. Rodriguez, Armando. 2011. *Keep Malware Off Your android Phone: 5 Quick Tips.* Dostopno prek: keep_android_phone_free_of_malware.html (30. junij 2013).
40. Rouse, Marget. 2006. *Encryption.* Dostopno prek: definition/encryption (31. julij 2013).
41. Sager, Ira. 2012. *Before Iphone and Android Came Simon, the First Smartphone.* Dostopno prek: http://www.businessweek.com/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone (10. julij 2013).
42. SAFE.si. 2013. *Kaj so mobilne aplikacije?* Dostopno prek: http://www.safe.si/c/1569/Aplikacije_na_pametnih_telefonih/?preid=1056 (11. julij 2013).
43. Sauter, Martin. 2011. *From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband.* Chichester, West Sussex, U.K: Wiley.
44. SSKJ. 2013a. *Okvara.* Dostopno prek: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=okvara&hs=1 (12. julij 2013).
45. --- 2013b. *Kraja.* Dostopno prek: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=kraja&hs=1 (12. julij 2013).
46. Strickland, Jonathan. 2011. *How Cloud Storage Works.* Dostopno prek: http://computer.howstuffworks.com/cloud-computing/cloud-storage.htm (1. avgust 2013).
47. Svet Idej. 2013. *Pokritost omrežja UMTS (Slovenija): Mobitel, Si.mobil, Tušmobil, T-2.* Dostopno prek: http://www.svetidej.com/informacije/mobilna-telefonija/79-pokritost-umts.html (11. julij 2013).
48. Svete, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
49. TechInfo2. 2013. *History Review of the Smartphones over 20 Years.* Dostopno prek: http://www.techinfo2.com/smartphones-history-reveiew-over-20-years.html (10. julij 2013).
50. Teixeira, Tania. 2010. *Meet Marty Cooper - the inventor of the mobile phone.* Dostopno prek: http://news.bbc.co.uk/2/hi/programmes/click_online/8639590.stm (10. julij 2013).

51. Trend Micro. 2013. *Repeating History.* Dostopno prek: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf (30. julij 2013).
52. Web-Center. 2012. *Uporabljanje Wi-Fi varnostnega sistema na mobilnih telefonih.* Dostopno prek: http://web-center.si/informacijska-varnost/brezzicna-omrezja/301-uporabljanje-wi-fi-varnostnega-sistema-na-mobilnih-telefonih- (6. avgust 2013).
53. White, Tyler. *Tablets trump smartphones in global website traffic.* Dostopno prek: http://blogs.adobe.com/digitalmarketing/digital-index/tablets-trump-smartphones-in-global-website-traffic/ (10. julij 2013).
54. Varni na internetu. 2013. *Priročnik za varno uporabo mobilnih naprav.* Dostopno prek: https://www.varninainternetu.si/content/uploads/2013/01/Varnost-in-zasebnost-na-mobilnih-napravah.pdf (31. julij 2013).