Varnost mobilnih naprav z operacijskim sistemom Android

Aleš Rumež, Boštjan Vlaovič

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Koroška cesta 46, 2000 Maribor
E-pošta: ales.rumez@student.um.si, bostjan.vlaovic@um.si

Security of mobile devices with Android operating system

With the constant growth of mobile devices, their users should be aware of potential dangers. Most of the people still passively use their devices without sufficient protection. One can never be too cautious when using a mobile device, since the data that is sent can be very important and personal. Security mechanisms given by the manufacturers is not enough. People with malicious intentions are almost always one step ahead of them. That is the reason why the user has to ensure security on the device by various methods. This article would like to raise awareness of the possible threats and give some suggestions on how to avoid them.

1 Uvod

Število uporabnikov mobilnih naprav je, po raziskavah iz zadnjih let, preseglo število uporabnikov namiznih računalnikov [1]. Prenosnost in možnost uporabe povsod sta ena izmed dejavnikov, zaradi katerih mobilne naprave postajajo vse bolj uporabne. Tudi njihova zmogljivost je v zadnjih letih postala bistveno primerljivejša namiznim računalnikom in zato se vse več populacije odloči za njihovo uporabo.

Večje število uporabnikov pomeni tudi večjo možnost napadov zlonamernih združb. V večini ljudje pasivno uporabljamo internetne storitve. Poznavanje nevarnosti je temelj, da se lahko na njih pripravimo in pred njimi zavarujemo. Ker je operacijski sistem Android najpogosteje uporaben, je tudi zlorab največ. V svetovnem merilu je nameščen na 65 odstotkov vseh mobilnih naprav. Na drugem mestu je iOS ameriškega proizvajalca Apple, ki je uporabljen na 31 odstotkih mobilnih naprav [1]. Te dve platformi sta tudi najbolj razširjeni na področju mobilne tehnologije. Število žrtev napadov se je v zadnjih letih povzpelo na vsakega 5. uporabnika mobilnega sistema Android [2]. Po raziskavah je še zmeraj najbolje varnostno zaščiten operacijski sistem iOS. Vendar se je tudi pri iOS v letu 2016 povečalo število zlonamerne programske opreme za sedemkrat glede na preteklo leto [3]. Najprimerneje in najučinkoviteje se pred zlorabami in izsiljevanji zaščitimo z rednim shranjevanjem pomembnih podatkov in z uporabo edinstvenih gesel primerne dolžine.

V drugem poglavju pojasnimo pojma varnost in zasebnost ter predstavimo, kakšne težave povezane s socialnim inženiringom in korenskim dostopom z vidika varnosti uporabnika. V trejem poglavju predstavimo najbolj pogosto škodljivo programsko opremo, ki lahko ogrozi mobilno napravo uporabnika in dodamo primere. V četrtem poglavju naredimo pregled varnostnih priporočil, s katerimi lahko pripomoremo k večji varnosti naših podatkov na mobilnih napravah.

2 Varnost in zasebnost

Varnost in zasebnost sta dva različna pojma, ki sta si v veliko pogledih podobna. Predvsem v mobilni tehnologiji, kjer vsak uporabnik na svoji napravi dnevno uporablja svoje podatke, se je potrebno zavedati, da v primeru vdora v zasebnost in krajo njegovih podatkov, lahko nastopijo težave.

2.1 Varnost

V poročilu [4] je predstavljeno, da polovica uporabnikov mobilnih naprav z operacijskim sistemom Android ne uporablja osnovnih varnostnih načinov, kot so gesla ali programska oprema za zaščito [4].

Mobilna varnost pomeni zaščito osebni in poslovnih informacij, ki so shranjene na mobilnih napravah in jih uporabniki dnevno prenašamo. Mobilna varnost je širok pojem. Poznamo več oblik ogrožanja varnosti uporabnika. V nadaljevanju bomo predstavili dve: socialni inženiring in korenski dostop.

Socialni inženiring je ena izmed metod napada, pri kateri napadalec uporabi tehnike, s katerimi prepriča uporabnika, da mu izda svoje avtentikacijske podatke. Napadalci z nastavljanjem vabe izkoristijo in zavedejo uporabnike. Napad je sestavljen iz štirih faz. Najprej napadalec zbere podatke o žrtvi. Nato vzpostavi zaupljiv odnos, kar je temelj za nadaljnji potek. V tretji fazi začne z izkoriščanjem pridobljenega zaupanja, kar pa dokončno obrne sebi v prid v četrti fazi, kjer izvede napad. Najpogostejši primer je ribarjenje (angl. phishing). Napadalec se preko elektronskega sporočila izdaja za uslužbenca določenega podjetja in tako poizkuša pridobiti podatke, kot so spol, naslov, uporabniško ime in geslo [5].

Korenski dostop pomeni, da uporabnik popolnoma prevzame nadzor nad operacijskim sistemom mobilne naprave. Vsak uporabnik se sam odloči za taško obliko uporabe mobilne naprave. Korenski dostop ne obstaja samo na napravah, ki uporabljajo operacijski sistem Android.

Najdemo ga tudi na napravah, ki uporabljajo operacijski sistem iOS pod imenom "jailbreak".
Korenski dostop omogoča nameščenim aplikacijam, da lahko brez naše vednosti spreminjajo in dostopajo do vseh vsebin, ki jih imamo na mobilni napravi. Razlogov, za kaj uporabniki želijo uporabljati mobilno napravo s korenskim dostopom je več. S tem lahko iz naprave odstranijo vso nepotrebno programsko opremo, ki jo proizvajalci namestijo na mobilno napravo. Pri uporabi korenskega dostopa, lahko na mobilno napravo namestimo programsko opremo, katera ne bo preverjena po standardnih varnostnih procesih operacijskega sistema. S korenskim dostopom uravnavamo hitrost delovanja procesorja. V primeru, da zvišamo takt procesorju, povečamo njegovo učinkovitost in hitrost delovanja. Če pa želimo povečati zmogljivost in življensko dobo baterije pa takt procesorja znižamo. Uporabnikova previdnost je pri uporabi mobilne naprave z korenskim dostopom še posebaj pomembna. V tem primeru proizvajalec več ne jamči za varnost, saj uporabnik namensko omogoči vsem aplikacijam dostop do vseh vsebin. Uporabnik pridobi, saj prevzame popoln nadzor nad programsko opremo. Negativna stran pa je gotovo, da lahko naprava postane neuporabna in izguba garancije proizvajalca [6].

2.2 Zasebnost

Zasebnost je pravica posameznika, da sam svobodno odloča o deljenju svojih osebnih podatkov in informacijm. Zasebnost ogrožajo trije dejavniki, ki so močno spremenili življenje posameznika v zadnjih desetih letih. To so: globalizacija, konvergenca med tehnologijami in multimedialnost [7]. Ti trendi so omogočili težave na področju zasebnosti, ki jih države poskušajo rešiti s spremembo zakonodaje. Zakonodaja zagotavlja tajnost pri telefonski komunikaciji in elektronskih sporočilih v javnem komunikacijskem omrežju in tudi v zasebnem. Vendar je komunikacijska zasebnost, ko zaposleni uporabljajo telekomunikacijsko omrežje podjetja manjša [8]. Nadzorovanje uporabnikov medmrežja ne poteka samo iz vidika varnosti. Podjetja tako nadzorujejo ljudi in spremljajo njihove aktivnosti na spletu tudi za svojo korist. Te nadzore lahko za podjetja opravljajo hekerji, kateri pa lahko delujejo tudi samostojno. V večini namen hekerjev, ko delujejo samostojno, ni škodovanje ali nadzor ljudi ampak samodokazovanje in zabava.
Črpanje in prestrezanje podatkov sta dve najpopularnejši metodi napada. Mobilne naprave v omrežju prepoznamo po številki IP, ki predstavlja lokacijo naprave v omrežju. Številka IP je lahko statična ali dinamična. Če ima naprava v omrežju statični IP pomeni, da bo zmeraj ob ponovnemu vklopu na določeno omrežje imela isto številko IP. V primeru, da naprava uporablja dinamični IP pa se bo le ta zmeraj spremenila. V omrežju, je lažje identificirati uporabnika s statičnim naslovom IP, saj je pri dinamičnem najprej potrebno ugotoviti, kateri napravi ob priklopu na omrežje pripada katera številka IP. V primeru napada črpanja podatkov napadalec, ko je naprava povezana na omrežje, s pomočjo številke IP, identificira napravo, katero želi napasti. Ker pa vsaka mobilna naprava dnevno pridobi več različnih številk IP pa je možnost črpanja podatkov časovno omejena, dokler je naprava na tem omrežju. Prestrezanje podatkov je za hekerje lažji način, saj s spremljanjem prometa, ki se pretaka preko omrežja, pridobiva vse informacije od uporabnika. Napadalec za to potrebuje program, ki mu to omogoča. V večini so takšni programi brezplačno dostopni na spletu. Primeri takšnega programa je Wireshark s katerim je možno nadzorovati promet na omrežju [7].
Škodljivo programska oprema se lahko naloži tudi z nameščanjem različnih aplikacij. V naslednjem poglavju bomo predstavili programsko opremo, ki lahko škodi mobilnim napravam.

3 Potencialno škodljiva programska oprema

Programe, ki se brez vednosti uporabnika naložijo v računalniški sistem skupaj z drugimi programi, imenujemo škodljiva programska oprema. V nadaljevanju so predstavljeni najbolj poznani primeri, za katere bomo podali predloge za zaščito.

3.1 Vohunski programi

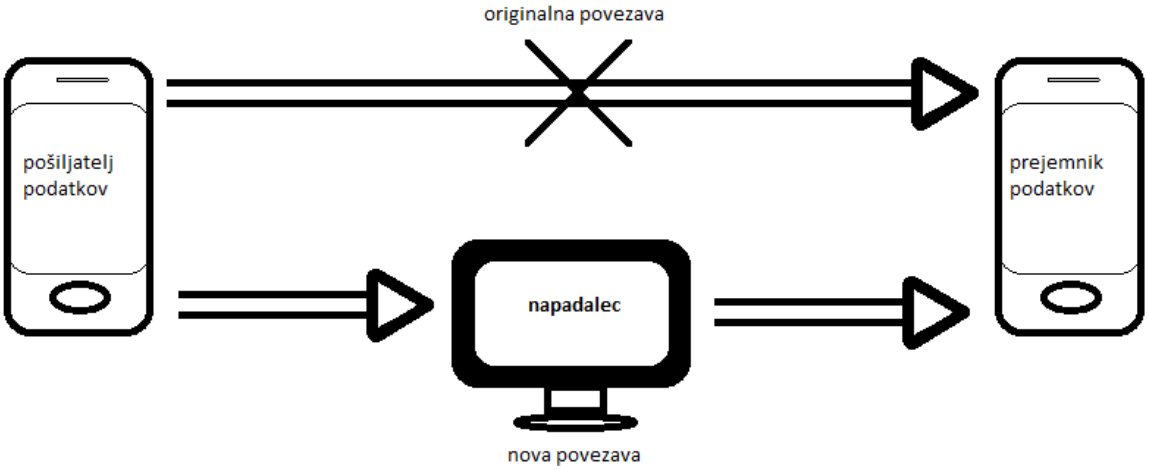
Vohunski programi so tisti, ki spremljajo in prikrito zbirajo podatke o brskanju uporabnika po internetu. Najpogostejši znak, da je naša mobilna naprava okužena z vohunskim programom, je počasnejše odpiranje aplikacij. Vohunski programi so zlonamerni. Uporabnik jo namesti, kot del aplikacije, v okvir katere pa jo ponudi razvijalec. Ko je aplikacija nameščena vohunski program sam začne z zbiranjem podatkov. S takšnimi programi je možno zbirati podatke o datotekah na trdem disku, geslih in kreditnih karticah.
Neškodljiva a nadležna oblika vohunskih programov so oglaševalski. Predstavljajo dober kanal za oglaševalce. Prisotnost oglaševanja pri aplikacijah je danes že stalnica. Oglaševalski programi se v okviru aplikacije naložijo na mobilno napravo ob prenosu aplikacije. Prikazujejo se v uporabniškem vmesniku aplikacije. Delujejo tako, da analizirajo katere spletne strani obiskuje uporabnik in na podlagi tega oglašuje ustrezen tip blaga ali storitev. Število okuženih aplikacij z oglasi se je med letoma 2012 in 2014 povečalo za štirikrat [9]. Razvijalcu aplikacije, ki jih vključi v sklop aplikacije, predstavljajo vir dohodka s katerim si povrne stroške razvoja in nadaljnje podpore.

3.2 Trojanski konj

Trojanski konji so bolj znani iz računalništva. Trojanski konj se na nobeno napravo ne namesti sam in je odvisen od neprevidnosti uporabnikov. Vendar pa je velikokrat skrit v določenih aplikacijah za katere ne bi nikoli pomislili, da so zlonamerne. Težave, ki jih povzroča trojanski konj so: brisanje, spreminjanje, blokiranje in kopiranje datotek.

3.3 Zadnja vrata

Prvotni cilj vsakega napadalca je, da bi pri svojem napadu ostal neopažen. Pri metodi zadnja vrata, napadalec zaobide vse običajne postopke preverjanja prisotnosti v večini preko običajne internetne povezave. Zadnja vrata na mobilnih napravah z operacijskim sistemom Android



Slika 1: Napad s posrednikom

omogočajo dostop do uporabniških podatkov mimo vseh zaščit.
Mobilne naprave vsebujejo dve vrsti procesorja: aplikacijski procesor, kateri se uporablja za operacijski sistem ter uporabniške aplikacije in radijski procesor, na katerem teče zaprtokodni in realnočasovni operacijski sistem. Radijski procesorji vsebujejo varnostne ranljivosti, ki omogočajo dostop do mobilne naprave preko zadnjih vrat. V novejših mobilnih napravah so zadnja vrata radijskega procesorja že onemogočena. Še vedno pa lahko napadalec pridobi nadzor nad aplikacijskim procesorjem in s pomočjo tega ustvari nova zadnja vrata [10].

3.4 Virusi in črvi

Virusi in črvi so zlonamerna programska oprema, ki se lahko neskončno razširjajo med napravami. Na mobilnih napravah se v večini prenašajo s slikovnimi in tekstovnimi sporočili (MMS/SMS) ali z različnimi datotekami. Pri svojih dejanjih največkrat ne potrebujejo posebnih dovoljenj uporabnika. Razlika med črvi in virusi je v tem, da se virus lahko naloži na napravo le s klikom na določeno datoteko, medtem ko se črvi lahko razširijio brez delovanja uporabnikov. Virusi v večini poškodujejo datoteke, programsko opremo ali tudi strojno opremo. Črvi delujejo tako, da se kopirajo zato zavzemajo spomin naprave. Kopirajo pa se tudi med vsemi napravami, ki so v istem omrežju [11].

4 Varnostna priporočila

Poznavanje možnih varnostnih ukrepov lahko v veliki meri pripomore k boljši uporabniški izkušnji. Operacijski sistem Android ima že vgrajenih veliko varnostnih funkcij, ki skrbijo za zaščito podatkov uporabnika. Kljub temu pa smo uporabniki tisti, ki moramo poskrbeti za svoje mobilne naprave. V tem poglavju bomo pregledali osnovna varnostna priporočila s katerimi se izognemo nevšečnostim in zaščitimo svoje podatke.
Pazljivost in zavedanje nevarnosti lahko prepreči nadaljnje nevšečnosti. V primeru socialnega inženiringa praktično ni nobene zaščite. Največ za varnost svojih podatkov lahko naredi uporabnik, s poznavanjem problema. Posredovanje gesel v telefonskih pogovorih ali spletnih klepetalnicah zagotovo niso priporočljiva [12].

4.1 Protivirusna zaščita

Delovanje protivirusnih programov na računalnikih in na mobilnih napravah se nekoliko razlikuje. Na mobilnih napravah protivirusni program le zazna zlonameren program tako, da ga mora uporabnik ročno izbrisati. Na računalnikih protivirusni programi zaznajo in sami odstranijo neprimerno datoteko. Protivirusna zaščita deluje pozitivno predvsem v primerih, ko se odločimo za uporabno s korenskim dostopom, trojanskimi konji, virusi in črvi. Ne preprečuje oglaševalskih in vohunskih programov. Večina protivirusnih aplikacij vsebuje oglaševalske programe [13].

4.2 Preverjene aplikacije in posodobitve platforme Android

V letu 2015 je le 33 odstotkov ljudi uporabljalo plačljive aplikacije [14]. Z uporabo plačljivih aplikacij zmanjšamo možnost oglaševalskih in vohunskih programov na naši mobilni napravi. Najpomembneje pa je, da ne nameščamo aplikacij iz neznanih virov. Tudi redna posodobitev aplikacij in programske opreme v veliki meri pripomore k varnosti mobilne naprave. Razvijalci Androida z rednimi posodbitvami programske opreme razrešujejo varnostne pomanjkljivosti. Pri starejših različicah operacijskega sistema Android se je pojavljala težava, saj je omogočala stranska vrata, preko katerih je lahko napadalec prišel do uporabnikovih podatkov mimo varnostne zaščite. S posodobitvijo so razvijalci to pomankljivost odpravili [10].

4.3 Varnostne kopije

Pomen varnostnega kopiranja podatkov se uporabniki večinoma zavemo šele takrat, ko ostanemo brez njih. Že sama okvara naprave lahko povzroči nevščenosti, katerim se

lahko izognemo z rednim ustvarjanjem varnostnih kopij [15]. Tudi v primeru izgube ali kraje naprave ter trojanskega konja in virusov je to ustrezna rešitev. S tem se zaščitimo, da če že nekdo ukrade podatke imamo mi vsaj varnostno kopijo njih in nas napadalec ne more izsiljevati za ponoven dostop do njih. Izsiljevalski so v zadnjem letu postali zelo razširjeni. Zadnji primer takšnega je bil Petya/Petrweap, ki je okužil sisteme v veliko državah. Varnostne kopije so primeren način za obrambo podatkov pred takšnimi napadi [16]

4.4 Previdnost pri uporabi odprtih WIFI omrežij

Velik del brežičnih omrežij je prosto dostopnih. Potrebno se je zavedati posledic, ki se lahko pojavijo. Na spletu obstaja ogromno prosto dostopnih programov, s katerimi lahko nekdo z računalniškim znanjem preverja promet na omrežju, ki ga uporabniki sprožimo na prosto dostopnih WIFI omrežjih. Najpogostejši napadi na brezžičnih omrežjih so: napad s posrednikom, kraja identitete, zlonamerne povezave. Pri napadu s posrednikom ves promet teče čez napadalčev vmesni člen. V večini je to računalnik lahko pa je tudi mobilna naprava. Tako da ima napadalec celoten nadzor nad pretokom nad omrežjem [17]. Zato se je potrebno izogibati vpisovanju različnih gesel in bančnih računov v primeru prosto dostopnih omrežij. Tudi izmenjava datotek pri takšni internetni povezavi ni primerna, saj lahko napadalci te datoteke prestrežejo. Če se želimo izognit takšnim črpanjem in prestrezanjem podatkov, je bolj smiselno uporabljati navidezno zasebno omrežje. Pri takšni uporabi podatki potujejo skozi šifriran tunel, ki skrbi za varnost podatkov pred zlonamerneži [18].

5 Zaključek

Zavedanje nevarnosti, ki nam preti v svetu mobilne tehnologije, je pomembna tudi za običajnega uporabnika. Zaradi svoje priljubljenosti, je operacijski sistem Android popularen tudi pri piscih zlonamerne programske kode. Če smo uporabniki pripravljeni na varnostne grožnje se lahko z njimi soočimo in tudi pred njimi preventivno zaščitimo. Če uporabnik pozna še varnostne ukrepe s katerimi lahko določene zadeve prepreči je uporabniška izkušnja z mobilno napravo še bistveno boljša. Ker nam mobilne naprave ponujajo veliko več, kot samo pisanje sporočil je tudi groženj več.

V članku je predstavljen pregled varnostnih groženj in podane določene rešitve s katerimi se lahko zavarujemo pred nevarnostjo.

Literatura

[1] SRC. Računalništvo in povezave. Dostopno na: http://www.src.si/uploads/SRC-brezmejna-omrezja.pdf [26.6.2016]

[2] Mobile/Tablet Operating System. Dostopno na: https://www.netmarketshare.com/ [15.5.2017].

[3] Cybercriminals will target Apple in 2016, say experts. Dostopno na: http://www.bbc.com/news/technology-35070853 [28.6.2017]

[4] Lomas N. Android remains main target for mobile malware writers despite iOS having more vulnerabilities, says symantec. Dostopno na: https://techcrunch.com/2013/04/16/symantec-mobile-malware/ [10.5.2017].

[5] Socialni inženiring in kako se pred njim ubraniti?. Dostopno na: https://www.ip-rs.si/fileadmin/user-upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf [28.6.2017]

[6] Šavc B. Varnost v Androidu. Monitor, 23, (december 2013), 12/13, str. 64-74

[7] Kovačič M. Zasebnost na internetu, Ljubljana: Mirovni inštitut, 2003

[8] Ustava Republike Slovenije. Dostpono na: http://www.us-rs.si/media/ustava.republike.slovenije.pdf [2.7.2017]

[9] How to remove virus from Android (Pop-up Ads and Redirects Removal). Dostopno na: https://malwaretips.com/blogs/remove-android-virus/ [22.5.2017].

[10] Kovačič M. Šifriranje notranjega pomnilnika telefonov s sistemom Android. Dostopno na: https://pravokator.si/index.php/2014/03/17/sifriranje-notranjega-pomnilnikatelefonov- s-sistemom-android/ [23.5.2017].

[11] Shekov M. Viruses, Worms and Trojans on mobile phones. (2011). Dostopno na: http://cosec.bit.uni-bonn.de/fileadmin/user-upload/teaching/10ws/10ws-sem-mobsec/talks/shekow.pdf [28.6.2017]

[12] What is social Engineering?. Dostopno na: https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering [22.6.2017].

[13] Android antivirus apps CAN'T kill nasties on sight like normal AV-and that's Google's fault. Dostopno na: http://www.theregister.co.uk/2013/12/17/android-anti-malware/ [20.6.2017].

[14] Only 33 percent of US mobile users will pay for apps this year. Dostopno na: https://www.emarketer.com/Article/Only-33-of-US-Mobile-Users-Will-Pay-Apps-This-Year/1011965 [22.6.2017].

[15] Šavc B. Zavarujmo svoj Android!. Dostopno na: http://www.monitor.si/clanek/zavarujmo-svoj-android/170424/ [23.6.2017]

[16] Širjenje Petya/Petrwrap izsiljevalskega virusa. Dostopno na: https://www.cert.si/si-cert-2017-05/ [2.7.2017]

[17] Brezžična omrežja. Dostopno na: https://sl.wikipedia.org/wiki/Brezžično-omrežje-Tipi-nepoobla.C5.A1.C4.8Denega-dostopa-v-omre.C5.BEja [28.6.2017]

[18] Center informacijske varnosti. (2012). Teden varnosti brezžičnih omrežij. Dostopno na: http://web-center.si/clanki/teden-varnosti-brezzicnih-omrezij.pdf [23.6.2017]

[19] Schneir B. Data and goliath, New York, 2015