CARNET

Sigurnosni pregled Android operacijskog sustava

CERT.hr-PUBDOC-2018-8-365

CERT.hr

Sadržaj

1 Uvod

U današnje vrijeme sve se više koriste mobilni uređaji, skoro svima su dostupni i teško je zamisliti život bez istih. Popularnost pametnih telefona i aplikacija koje su namijenjene njima dovodi u pitanje sigurnost i privatnost korisnika.

U ovom dokumentu obrađena je tema sigurnosti najpopularnijeg operacijskog sustava za pametne mobilne uređaje – Android OS. Uz osnovne informacije o operacijskom sustavu, njegovoj povijesti i trendovima koji ga prate, u ovom dokumentu se mogu pronaći opisani sigurnosni mehanizmi Android OS-a kojima se štiti operacijski sustav i sam uređaj.

Osim toga, obrađena je tema sigurnosti aplikacija za ovaj operacijski sustav. Uz sigurnosne karakteristike okruženja u kojem se pokreću aplikacije, u dokumentu su opisane i mjere koje provode servisi za distribuciju aplikacije te trendovi koji prate same aplikacije.

2 Osnovno o *Android* operacijskom sustavu

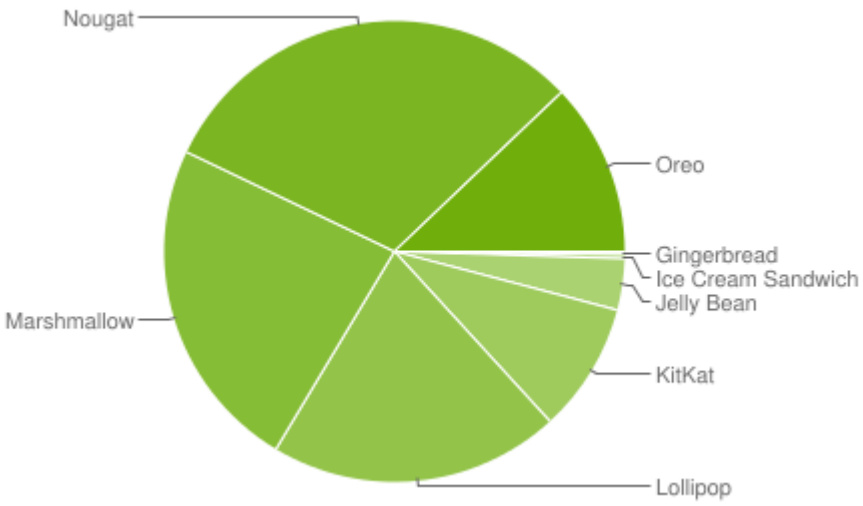
U 2018. godini, prema istraživanju tvrtke Newzoo koja se bavi marketinškom inteligencijom za područje mobilnih tehnologija, u svijetu se koristi 2,3 milijarde Android uređaja što osim pametnih mobilnih uređaja uključuje i TV uređaje, automobile, pametne satove i druge.

Android operacijski sustav razvijen od strane Google-a prvotno je predstavljen 2007. godine, a prvi komercijalni uređaj s Android OS-om na tržište je izašao 2008. godine. Od tad je ovaj operacijski sustav prošao kroz više značajnih promjena, a trenutačna verzija je 8.1 „Oreo“ koja je izašla u prosincu 2017. godine.

Udio Android operacijskog sustava na tržištu pametnih mobilnih uređaja iznosi preko 85%, pokazuje istraživanje tvrtke Gartner. Zajedno s Apple-ovim iOS-om, Android drži duopol na tržištu operacijskih sustava za mobilne uređaje.

Sama činjenica da je Android popularniji od iOS-a, ali i zbog otvorenog pristupa, čini uređaje s tim operacijskim sustavom češćom metom zlonamjernih aktivnosti.

Uz to, kako je prikazano na slici 1, veliki udio Android korisnika ne koriste najnoviju verziju operacijskog sustava. Jedan od razloga je moguće ograničenje samog uređaja, ali i nemarnost samih korisnika.



Slika 1 – Udjeli Android OS po verzijama (izvor)

Prema statistici iz srpnja 2018. godine samo nešto više od 10% korisnika koriste jednu od dvije zadnje verzije sustava, to jest 8.0 i 8.1 „Oreo“. Dok čak tri četvrtine uređaja su na jednoj od tri verzije koje su prethodile „Oreu“.

Podrška za verziju „Lollipop“ se ne pruža već neko vrijeme, dok se prestanak izdavanja sigurnosnih zakrpa za „Marshmallow“ očekuje uskoro (do kraja 2018. godine). Na taj će način veliki dio korisnika ovoga operacijskog sustava ostati na verzijama na kojima se ne otklanjaju sigurnosni nedostatci.

3 Zaštita uređaja i operacijskog sustava

Android je operacijski sustav otvorenog koda izgrađen na Linux jezgri operacijskog sustava (eng. *kernel*) i pruža okruženje koje omogućuje rad više aplikacija istovremeno.

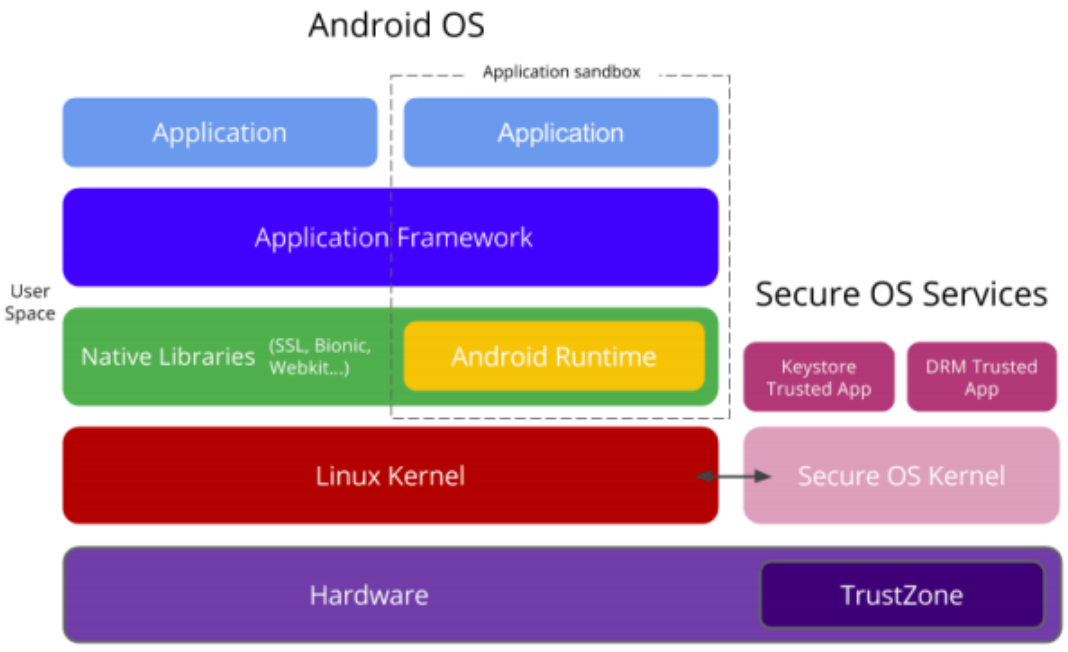
Ove aplikacije su potpisane i izolirane u sigurnom aplikacijskom virtualnom okruženju (eng. *sandbox*) povezanim s potpisom te aplikacije i on je zadužen za dodjeljivanje potrebnih privilegija aplikaciji. One ostvaruju komunikaciju putem okvira koji definira sustavske servise, platformu aplikacijskog programskog sučelja - API (eng. *Application Programming Interfaces*) i format poruka.

Sustavski servisi implementirani su kao aplikacije i kao takvi su ograničeni aplikacijskim sandboxom. Iznad kernela ne postoji koncept *root* ili superkorisnika koji ima nesputan pristup sustavu.

Kako je Android višenamjenski operacijski sustav, mnogi uređaji pružaju dodatno izolirano okruženje za izvršavanje procesa s višim ovlastima ili sigurnosno osjetljivih procesa koji ne zahtijevaju funkcionalnosti višenamjenskog operacijskog sustava.

Ovakvo okruženje, često nazvano *Secure OS*, može biti implementirano na zasebnom procesoru ili izolirano ispod kernela na zajedničkom procesoru. *Secure OS* može biti korišten od strane proizvođača uređaja kako bi osigurali usluge i aplikacije koje su specifične za uređaj.

Na slici 2 prikazana je arhitektura *Android* operacijskog sustava na *ARM*-u sa *TrustZone* tehnologijom. *TrustZone* je pouzdano okruženje za izvršavanje namijenjeno procesorima ARM arhitekture.



Slika 2 - Arhitektura operacijskog sustava s pouzdanim okruženjem za izvršavanje (izvor)

Kriptografija[1] je korištena širom Android operacijskog sustava kako bi se osigurala povjerljivost i cjelovitost podataka. Na Android uređajima kriptografija se najčešće koristi za šifriranje uređaja, potpisivanje aplikacija te za mrežnu povezivost i šifriranje, uključujući SSL (eng. *Secure Sockets Layer*), bežičnu (Wi-Fi) mrežu i virtualnu privatnu mrežu VPN (eng. *Virtual Private Network*).

Šifriranje Android uređaja temeljeno je na dm-crypt podsustavu Linux kernela. Korišteni kriptografski algoritam je 128 AES s CBC i ESSIV:SHA256, a glavni ključ šifriran je sa 128-bitnim AES putem poziva Android OpenSSL biblioteci. Android pruža kriptografske API-je na korištenje aplikacijama za uporabu standardnih i često korištenih kriptografskih primitiva kao što su AES, RSA, DSA i SHA te za protokole viših slojeva kao što su SSL i HTTPS.

S Android-om 4.0 „Ice Cream Sandwich“ i Android-om 4.3 „Jelly Bean“ uvode se KeyChain i KeyStore. Klasa KeyChain aplikacijama dozvoljava korištenje pohrane za vjerodajnice sustava kako bi pohranile privatne ključeve i certifikate, dok KeyStore omogućava pohranu privatnih ključeva unutar kontejnera kako bi se otežala njihova ekstrakcija s uređaja.

[1] kriptografija – znanstvena disciplina koja se bavi metodama pohranjivanja i prijenosa informacija na način da su razumljive samo onima kojima su i namijenjene

4 Sigurnost aplikacija

Kao što je prije spomenuto, svaka Android aplikacija pokreće se unutar sandboxa. Taj virtualni sandbox onemogućuje aplikaciji komunikaciju ili pristupanje bilo čemu osim resursima dodijeljenim samim sandboxom. Kako bi se aplikacijama omogućio pristup drugim resursima i funkcionalnostima uređaja koristi se sustav dozvola. Dozvolama se prije same instalacije aplikacije odobravaju resursi i funkcionalnosti uređajima koji će biti omogućeni za korištenje aplikaciji.

Korištenjem korisnički zasnovanim modelom zaštite identificiraju se i izoliraju resursi aplikacija, što znači da prilikom pokretanja aplikacije Android sustav pojedinoj aplikaciji dodjeljuje korisnički identifikacijski broj (UID) i pokreće aplikaciju kao taj korisnik u zasebnom procesu. Ova je funkcionalnost specifična za Android operacijski sustav jer ostali operacijski sustavi, uključujući i tradicionalne Linux konfiguracije, pokreću više aplikacija pod istim korisnikom.

Aplikacije prema zadanim postavkama nemaju mogućnost međusobne komunikacije. Kako aplikacijski sandbox počinje iz kernela - on se proteže kroz sve razine operacijskog sustava. Iz tog razloga, u slučaju da dođe do izmjene dijelova memorije (eng. *memory corruption*, izvršavanje proizvoljnog programskog koda moguće je samo unutar te aplikacije s dozvolama dodijeljenim od strane operacijskog sustava.

Obvezna kontrola pristupa (eng. *Mandatory Access Control* - MAC) nad svim procesima je osigurana kroz tzv. *Security Enhanced Linux* (SELinux). SELinux omogućuje tri načina rada: *disabled*, *permissive* i *enforcing*. U *permissive* načinu rada SELinux samo bilježi logove dok u *enforcing* on aktivno provodi politiku uskraćujući pristup ako dođe do pokušaja kršenja iste politike.

Android operacijski sustav od svih aplikacija zahtjeva da budu digitalno potpisane certifikatom prije nego što su instalirane. Android koristi ove certifikate kako bi identificirao autore aplikacija, najčešće se radi o samopotpisanim certifikatima te autor aplikacije zadržava privatni ključ. U slučaju ažuriranja aplikacije uspoređuje se certifikat nove verzije s certifikatom trenutačne verzije aplikacije te se u slučaju podudaranja certifikata odobrava ažuriranje.

Ako aplikacije to zahtijevaju, Android dozvoljava pokretanje aplikacija s istim certifikatom u jednom procesu te ih sustav tretira kao jednu aplikaciju. Potpisivanjem više aplikacija istim certifikatom i korištenjem potpisom zasnovanih dozvola omogućuje se dijeljenje koda i podataka među aplikacija na siguran način.

4.1 Dozvole aplikacija

Kako se sve Android aplikacije pokreću unutar granica aplikacijskog sandboxa, ograničen im je pristup resursima sustava.

Tako operacijski sustav štiti korisnički doživljaj, uređaj, podatke i mrežu od pogrešnog ili zlonamjernog korištenja resursa od strane aplikacije. Pristup resursima van aplikacijskog sandboxa rješava se putem dozvola aplikacija. Preporučeno je korištenje što je moguće manjeg broja dozvola aplikacija kako bi se umanjila mogućnost zlouporabe istih (eng. *principle of least privilege*).

Prilikom instalacije aplikacije na uređaj korisniku se prikazuje dijaloški okvir u kojemu su prikazane dozvole koje zahtjeva ta aplikacija. Ako korisnik prihvati zahtjev, aplikacija zadržava pravo korištenja tih funkcija sve dok je instalirana na uređaju.

Neke od funkcija koje se inače dodjeljuju putem dozvola moguće je isključiti na globalnoj razini uređaja, kao što je npr. lokacija, i tako spriječiti korištenje te funkcionalnosti iako aplikacija ima potrebnu dozvolu.

4.2 Distribucija aplikacija

Google Play, prethodno poznat kao Android Market, službena je platforma za distribuciju aplikacija namijenjenim Android operacijskom sustavu. Unutar sebe Google Play ima nekoliko mehanizama koji štite korisnike od potencijalno štetnih aplikacija. Sami razvijatelji (eng. *developers*) aplikacija provjeravaju se u dvije faze: kod same registracije Google play *developerskog* računa te kod podnošenja nove aplikacije.

Sadržaj na Google Play-u redovno se skenira u potrazi za zlonamjernim kodom i ranjivostima, a ako se prekrše uvjeti *developerskog* programa njihov se račun suspendira. Osim toga, ova platforma sadržava ocjene i recenzije aplikacije od strane drugih korisnika te na taj način korisniku pruža relevantne informacije o samoj aplikaciji prije nego što on instalira istu na svoj uređaj. Osim toga Android uređaji s Google Play imaju mogućnost verificiranja aplikacija. *VerifyApps* provjerava aplikacije kako bi se uvjerio da su aplikacije sigurne čak i nakon instalacije.

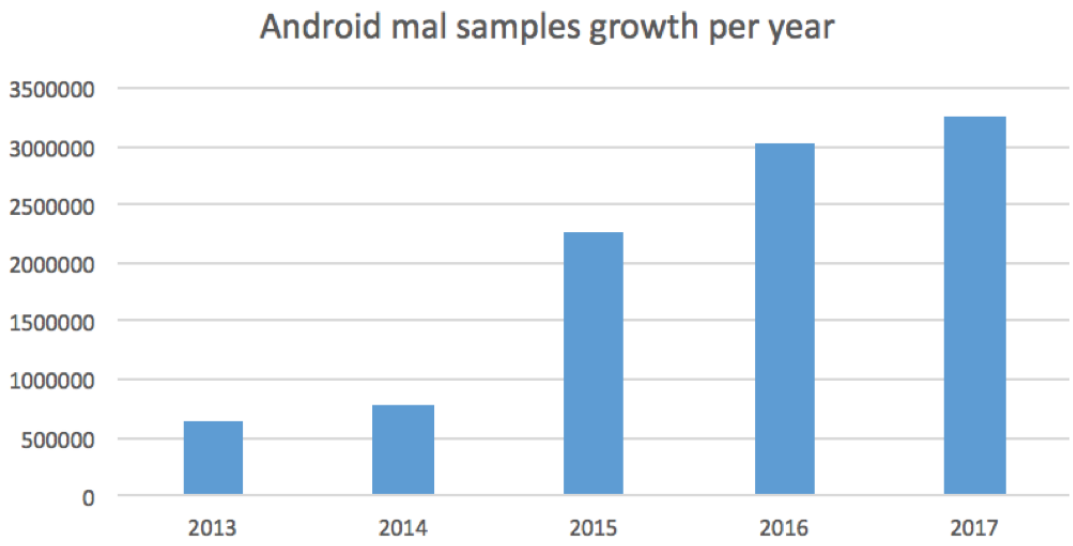
Osim službene platforme, Android aplikacije se distribuiraju putem raznih *third-party* marketa. Developeri često koriste te alternativne platforme kako bi doprijeli do što većeg broja korisnika ili ciljane skupine korisnika. Korisnici ovakvih platformi podložniji su zlonamjernom sadržaju zbog moguće nedostatne provjere aplikacija na isti.

4.3 Zlonamjerne aplikacije

Unatoč svim mjerama zaštite koje omogućuje sam Android operacijski sustav i dodatnim mjerama provjere koje se provode prije i za vrijeme distribucije aplikacije, do krajnjih korisnika ipak stigne određeni broj zlonamjernih aplikacija. U prvom tromjesečju 2015. godine registrirano je 4 900 novih uzoraka zlonamjernog sadržaja namijenjenih Android operacijskom sustavu. Najveći problem predstavljaju detektori zlonamjernog sadržaja, to jest nezadovoljavajuća uspješnost istih. Naime, od 40% ukupnog broja zlonamjernog sadržaja namijenjenog uređajima s Android operacijskim sustavom, više od polovice uspješno zaobilazi detektor istih.

Detektori zlonamjernog sadržaja unutar aplikacija tradicionalno su razvijeni tako da se ponašanje maliciozne aplikacije ručno ispituje ili da se analizira dekompilirani kod poznatih zlonamjernih aplikacija kako bi se uspostavio uzorak zlonamjernog sadržaja kojeg će detektor pokušati prepoznati. Ovaj model nije skalabilan za veliki broj aplikacija koje je potrebno provjeriti pogotovo ako se uzme u obzir da je novi zlonamjerni sadržaj konstruiran kako bi zaobišao postojeće detektore.

Android, kao sveprisutan operacijski sustav otvorenog koda, napadačima služi kao savršena platforma koju mogu iskoristiti kako bi distribuirali svoj zlonamjerni sadržaj koji je najčešće financijski motiviran. Broj malicioznih aplikacija za Android operacijski sustav godinama raste te je 2017. godine dostigao brojku od skoro 3,5 milijuna kao što je vidljivo na slici 3.



Slika 3 - Rast broja uzoraka zlonamjernih aplikacija u zadnjih 5 godina (izvor)

Prema istraživanju tvrtke Sophos u kojem je izrađena revizija zlonamjernog sadržaja za 2017. godinu i predviđanja za 2018. godinu najzastupljenija skupina ili „obitelj“ zlonamjernog sadržaja (eng. *malware family* - obuhvaća više različitih inačica istog zlonamjernog softvera) je Rootnik s 42% od svih zlonamjernih aplikacija za Android operacijski sustav. Slijede ga skupine zlonamjernog sadržaja PornClk, Axent i Slocker s 14%, 9% i 8%. Ostale slabije zastupljene skupine su Dloadr, Dropr, Xgen, Obfus i SmsSend.

5 Preporuke korisnicima

Kako bi se povećala sigurnost korisnika uređaja s Android operacijskim sustavom (iako se većina ovih preporuka odnosi i na sve ostale uređaje) i očuvala privatnost njihovih podataka u nastavku slijedi nekoliko preporuka:

- **Koristite opciju zaključavanja zaslona**

  Kao što je opće poznato, ako ne koristite opciju zaključavanja zaslona uređaja PIN-om, uzorkom ili lozinkom ne postoji niti jedan sloj zaštite koji štiti podatke na uređaju u slučaju da uređaj nije uz vas. Dodatna preporuka – ako koristite uzorak za otključavanje preporučuje se redovno brisanje zaslona uređaja kako bi ste onemogućili izvođenje tzv. *smudge* napada[2].

- **Ne spajajte se na nesigurne mreže**

  Spajanje na mreže ugostiteljskih objekata, javnih mjesta ili drugih otvorenih bežičnih mreža može biti rizično, pogotovo ako prenosite osjetljive podatke. Ako baš morate koristiti takve mreže, preporučuje se korištenje virtualne privatne mreže (VPN).

- **Koristite uređaj od proizvođača koji redovito ažuriraju**

  Pravovremena reakcija proizvođača i brzo izdavanje zakrpa, pogotovo onih vezanih za sigurnosne propuste, trebalo bi biti uzeto u obzir prilikom odabira uređaja.

- **Šifriranje pohrane podataka**

  Šifriranje podataka uređaja uglavnom koristi mnogo kompleksniji kriptografski algoritam od samog zaključavanja zaslona. Tako su vaši podatci dodatno zaštićeni u slučaju gubitka ili krađe uređaja.

- **Ne dozvoljavajte instalaciju aplikacija iz vanjskog izvora**

  Kao što je prije spomenuto, aplikacije koje se distribuiraju putem službene platforme, to jest Google Play servis, prolaze kroz mnogo rigorozniju provjeru nego aplikacije s alternativnih marketa.

- **Koristite „anti-malware“ aplikaciju**

  Instalacijom i korištenjem aplikacije koja štiti uređaj od zlonamjernog sadržaja stvarate još jedan dodatni sloj zaštite na vašem uređaju.

[2] *smudge* napad – metoda kojom napadač pokušava otkriti uzorak, PIN ili lozinku analiziranjem obrisa na zaslonu uređaja

Poveznice za neke od tih aplikacija dostupne su na:
http://www.antibot.hr/tools/scaniranje-virusa.html

- **Provjerite potrebne dozvole aplikacije prije instalacije**

Ako se pojavljuju nelogičnosti između opisa aplikacije i potrebnih dozvola moguće je da se ne radi o sigurnoj aplikaciji.

- **Zaključajte SIM karticu**

Otključavanje SIM kartice PIN-om korisnički doživljaj ne umanjuje znatno jer ga je potrebno upisati samo prilikom pokretanja uređaja, a kao i šifriranje podataka i zaključavanje zaslona pruža dodatni sloj zaštite u slučaju gubitka ili krađe uređaja.

- **Isključite Wi-Fi, Bluetooth i HotSpot kada ih ne koristite**

Osim što ubrzavaju potrošnju baterije, uključeni Wi-Fi, Bluetooth i HotSpot čine vaš uređaj vidljivim drugim uređajima i podložnim potencijalnim napadima.

- **Isključite lokaciju ako ju ne koristite**

Iako ovo nije izravno povezano sa sigurnošću vašeg uređaja, uključena usluga lokacije ugrožava vašu privatnost. Osim toga isključivanjem ove opcije smanjuje se potrošnja baterije i prijenosa podataka.

- **Koristite „Do Not Track“ opciju u pregledniku**

Korištenjem ove opcije onemogućujete, barem djelomično, prikupljanje podataka o vašim navikama pregledavanja koje su najčešće korištene za ciljano oglašavanje.

6 Zaključak

U ovome dokumentu opisani su sigurnosni aspekti Android operacijskog sustava i njemu pripadajućih aplikacija kojima Android OS pruža okruženje sa sigurnosnim mehanizmima u kojemu se te aplikacije pokreću. Osim toga, prvi sloj zaštite u ovom ekosustavu pruža Google Play koji pokušava spriječiti samo postavljanje mogućih zlonamjernih aplikacija na platformu za distribuciju i na taj način štiti korisnike od preuzimanje zlonamjernih aplikacija.

Kako se radi o operacijskom sustavu velike popularnosti napadačima nije potrebna velika stopa uspješnosti kako bi svoj zlonamjerni kod proširili na veliki broj korisnika, a broj uzoraka zlonamjernog sadržaja svake godine raste. Stoga, vrlo je važna ažurnost Google Play-a i ostalih servisa za distribuciju aplikacija kod detektiranja uzoraka zlonamjernog koda u aplikacijama. Također, svjesnost samog korisnika u obliku prepoznavanja mogućih zlonamjernih aplikacija, pravovremenog ažuriranja sustava i generalnog izbjegavanja korištenja *third-party* marketa nužni su za sprječavanje širenja zlonamjernog sadržaja.

Navedeno je nekoliko preporuka za korisnike uređaja s Android OS kako bi se povećala njihova sigurnost i očuvala privatnost njihovih podataka.

7 Literatura

1. **van der Wielen, Bernd.** Insights into the 2.3 Billion Android Smartphones in Use Around the World. [Mrežno] 17. sječanj 2018. [Citirano: 23. srpanj 2018.] https://newzoo.com/insights/articles/insights-into-the-2-3-billion-android-smartphones-in-use-around-the-world/.
2. **Google.** Android security white paper. [Mrežno] 2016. [Citirano: 23. srpanj 2018.] http://parabal.com/application/files/8914/8434/0051/android-for-work-security-white-paper.pdf.
3. **Google.** Android Developers: Distribution dashboard. [Mrežno] srpanj 2018. [Citirano: 28. srpanj 2018.] https://developer.android.com/about/dashboards/.
4. **Google.** Google Security Blog: Android Security 2017 Year review. [Mrežno]15. travanj 2018.[Citirano: 27. srpanj 2018.] https://security.googleblog.com/2018/03/android-security-2017-year-in-review.html.
5. **Raphael, JR.** Android 8.0 in-depth: Oreo's not-so-obvious security enhancements. [Mrežno] 29. kolovoz 2017. [Citirano: 27. srpanj 2018.] https://www.computerworld.com/article/3220446/android/android-8-oreo-security.html.
6. **Google.** Android Open Source Project: Security. [Mrežno] 19. ožujak 2018. [Citirano: 27. srpanj 2018.] https://source.android.com/security/.
7. **Google.** Android Security 2016 Year In Review. [Mrežno] ožujak 2017. [Citirano: 27. srpanj 2018.] https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf.
8. **Huang, Min, i dr.** Reviving Android Malware with DroidRide: And How Not To. [Mrežno] 2016. [Citirano: 27. srpanj 2018.] http://ugrs.zju.edu.cn/chinese/yzjxj/attachments/pxcl/2017-11/99999-1510637569-22465.pdf.
9. **McLaughlin, Niall i dr.** Deep Android Malware Detection. [Mrežno] 2017. [Citirano: 27. srpanj 2018.] http://sefcom.asu.edu/publications/deep-android-malware-detection-codaspy2017.pdf.
10. **Chien, Eric.** Symantec: Motivations of Recent Android Malware. [Mrežno] 2011. [Citirano: 27. srpanj 2018.] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf.
11. **Brenner, Bill.** 2018 Malware Forecast: the onward march of Android Malware. [Mrežno] 7. studeni 2017. [Citirano: 27. srpanj 2018.] https://nakedsecurity.sophos.com/2017/11/07/2018-malware-forecast-the-onward-march-of-android-malware/.
12. **Sophos.** SophosLabs 2018 Malware Forecast. [Mrežno] 2017. [Citirano: 27. srpanj 2018.] https://www.sophos.com/en-us/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf.
13. **Kaspersky Lab.** Android Security - Five Must Know Tips. [Mrežno] 2018. [Citirano: 27. srpanj 2018.] https://www.kaspersky.com/resource-center/preemptive-safety/android-security-tips.
14. **Wallen, Jack.** TechRepublic: 10 things you can do to make Android more secure. [Mrežno] 2018. [Citirano: 27. srpanj 2018.] https://www.techrepublic.com/blog/10-things/10-things-you-can-do-to-make-android-more-secure/.