Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Grega Štravs

Zasebnost pri javno dostopnih zdravstvenih aplikacijah

magistrsko delo

magistrski program druge stopnje
računalništvo in informatika

Mentor: dr. Andrej Brodnik
Somentor: prof. dr. Denis Trček

Ljubljana, 2019

Zahvala

Zahvaljujem se mentorju dr. Andreju Brodniku in somentorju prof. dr. Denisu Trčku za pomoč in napotke pri izdelavi magistrskega dela. Prav tako se zahvaljujem svoji družini, prijateljem in punci za podporo in spodbudo.

Grega Štravs, 2019

"All your base are belong to us."

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
ADB	Android Debug Bridge	Povezava za razhroščevanje v Androidu
AOT	Ahead Of Time	Vnaprej
API	Aplication Programming Interface	Programski vmesnik aplikacije
APK	Android Application Package	Paket Android aplikacije
ART	Android Runtime	Izvajalno okolje v Androidu
DEX	Dalvik Executable Format	Dalvik izvedljiv format
DVM	Dalvik Virtual Machine	Dalvik navidezni stroj
GDPR	General Data Protection Regulation	Splošna uredba EU o varstvu podatkov
GPS	Global Positioning Service	Globalni sistem pozicioniranja
HAL	Hardware Abstraction Layer	Abstrakcijska raven strojne opreme
HTTP	Hypertext Transfer Protocol	Protokol za prenašanje hipertekste
IMEI	International Mobile Equipment Identity	Mednarodni numerični identifikator naprave

kratica	angleško	slovensko
IV	Initialization vector	Inicializacijski vektor
JAR	Java Archive	Arhiv Java
JIT	Just In Time	Ravno pravi čas
JSON	JavaScript Object Notation	Objektni zapis JavaScript
MAC	Media Access Control	Nadzor do dostopa večpredstavnosti
MITM	Man-in-the-middle Attack	Napad s posrednikom
PCAP	Packet Capture	Zajem paketov
PID	Process Identification Number	Identifikacijska številka procesa
SDK	Software Development Kit	Paket za razvoj programske opreme
SMS	Short Message Service	Sistem kratkih sporočil
SSL	Secure Sockets Layer	Varnostni protokol, ki omogoča šifrirano povezavo
TLS	Transport Layer Security	Naslednik protokola SSL, ki omogoča šifrirano povezavo
XML	Extended Markup Language	Razširljivi označevalni jezik

Povzetek

Naslov: Zasebnost pri javno dostopnih zdravstvenih aplikacijah

Industrija mobilnih zdravstvenih aplikacij se nenehno širi, zato je pomembno, da se poveča skrb za zaščito občutljivih zdravstvenih informacij. Na žalost na trgu obstaja veliko zdravstvenih aplikacij, ki podatkov ne ščitijo dovolj dobro in niso skladne s trenutno veljavno zakonodajo.
Cilj magistrskega dela je ovrednotenje mobilnih zdravstvenih aplikacij z vidika varovanja zasebnosti in s stališča skladnosti s splošno uredbo EU o varstvu podatkov. V našem delu smo razvili kazalnike varovanja občutljivih podatkov pri zdravstvenih aplikacijah in kazalnike skladnosti z uredbo o varstvu podatkov. Na osnovi odprtokodnih orodij smo razvili arhitekturo za varnostno analizo mobilnih aplikacij. Izbrali smo deset aplikacij, jih z razvito arhitekturo analizirali in ovrednotili s kazalniki. Z ovrednotenjem smo dobili vpogled v stanje varovanja zasebnosti in skladosti z veljavno zakonodajo zdravstvenih mobilnih aplikacij.

Ključne besede

varnost, zasebnost, GDPR, Android, zdravstvene aplikacije

Abstract

Title: Privacy in publicly accessible healthcare applications

The industry of mobile healthcare applications is constantly expanding, so it is important to increase our concern about protection of sensitive health information. Unfortunately, the market consists of many healthcare applications that do not protect data well enough and are not in line with current European regulation.
The goal of this thesis is an evaluation of mobile health applications in terms of privacy protection and in terms of compliance with the General Data Protection Regulation. We developed indicators for the protection of sensitive data in health applications and indicators of compliance with the General Data Protection Regulation. Using open source tools, we developed an architecture for security analysis of mobile applications. We chose ten applications, which we analyzed and evaluated against the developed indicators. With the evaluation, we gathered insight into the state of privacy protection and compliance with current legislation of healthcare mobile applications.

Keywords

security, privacy, GDPR, Android, healthcare applications

Poglavje 1

Uvod

V zadnjih letih je vse več poudarka na spremljanju našega zdravja s pametnimi telefoni. Ti zbirajo informacije tako neposredno kot posredno. Svetovna zdravstvena organizacija WHO definira mobilno zdravje (angl. *mobile health*) kot »prakso na področju medicinskega in javnega zdravja, podprto z mobilnimi napravami, kot so mobilni telefoni, naprave za spremljanje pacientov, tablični računalniki in druge ročne brezžične naprave« [1]. Krebs in Duncan sta v letu 2015 raziskala mobilne zdravstvene aplikacije pri ameriških lastnikih pametnih telefonov in ugotovila, da je kar 58 odstotkov uporabnikov naložilo zdravstveno aplikacijo [2]. Ljudje najpogosteje uporabljajo aplikacije povezane z načinom prehranjevanja, življenskim slogom, fitnesom, diagnosticiranjem in zdravljenjem. Aplikacije predstavljajo veliko priložnost za zbiranje osebnih zdravstvenih informacij ter hkrati izboljšujejo kakovost oskrbe pacientov in zmanjšujejo stroške [2]. Kljub številnim prednostim, povezanim z uporabo mobilnih naprav, obstajajo tudi številne slabosti glede zasebnosti in varnosti pri uporabi mobilnih zdravstvenih aplikacij [3]. Veliko ljudi se ne zaveda, da so lahko zbrane informacije občutljive narave in hitro uidejo izpod nadzora.

Spoštovanje zasebnosti osebe je priznavanje pravice do svobode in prav tako priznavanje posameznika kot avtonomnega človeškega bitja [4]. V Sloveniji osebnostne pravice posameznika ščiti Ustava Republike Slovenije [5], ki v 38.

členu določa tudi varstvo osebnih podatkov. »Prepovedana je uporaba osebnih podatkov, ki je v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.« Poleg ustave imamo v ta namen na državni ravni trenutno na voljo tudi ZVOP - Zakon o varstvu osebnih podatkov [6], ki preprečuje neustavne, nezakonite in neupravičene posege v zasebnost posameznika pri obdelavi podatkov. Ta definira *osebni podatek* kot katerikoli podatek, ki se nanaša na posameznika ne glede na izraženo obliko.

Splošna uredba Evropske unije o varstvu podatkov (angl. *General Data Protection Regulation*, v nadaljevanju GDPR) se je začela uporabljati maja letos in prinaša novo uredbo, ki velja vzporedno z ZVOP. GDPR poskrbi za nove pravne zahteve upravljavcev podatkov, ki delujejo na ozemlju Evropske unije, in predvideva stroge sankcije za neizpolnjevanje svojih določb glede zaščite osebnih in posebej občutljivih podatkov. Ščiti osebne podatke oziroma katerokoli informacijo v zvezi z določenim ali določljivim posameznikom. *Določljiv posameznik* je tisti, ki ga lahko posredno ali neposredno identificiramo z naslednjimi identifikatorji: ime, priimek, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika [7].

Poleg zgornje opredelitve osebnih podatkov GDPR vsebuje še tri dodatne pomembne opredelitve, ki se nanašajo na zdravstvene podatke. Pod osebne podatke spadajo tudi

- podatki o zdravstvenem stanju, katere GDPR opredeljuje kot podatke, ki se »nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju«[7],
- biometrični podatki, ki so »rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, kateri

omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki≪[7],

- genetski podatki, ki so »podatki v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, kateri dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika≪[7].

Vzporedno z GDPR-jem je bil podan predlog za nov zakon o varstvu podatkov - ZVOP2, ki naj bi slovensko ureditev varstva osebnih podatkov uskladil z določbami GDPR.
V našem delu bomo raziskali grožnje zasebnosti pri javno dostopnih mobilnih zdravstvenih aplikacijah iz trgovine Google Play. Iz trgovine bomo izbrali deset zdravstvenih aplikacij, ter skozi njihovo uporabo in z obstoječimi varnostnimi raziskavami aplikacij Android razvili kazalnike stopnje varovanja zasebnosti pri mobilnih zdravstvenih aplikacijah. Pri tem nam bodo za osnovo služili tudi standardi mobilne varnosti OWASP [8]. Na podlagi kazalnikov bomo razvili arhitekturo za testiranje mobilnih zdravstvenih aplikacij, kjer bomo s statično analizo iskali ranljivosti, ki bi napadalcem omogočile dostop do občutljivih podatkov, ter z dinamično analizo preverili, ali iz aplikacije uhajajo občutljive informacije, s katerimi lahko posameznik postane določljiv. Na podlagi rezultatov analiz ter na podlagi politike zasebnosti bomo ovrednotili skladnost mobilnih zdravstvenih aplikacij z GDPR. Testne aplikacije bomo ovrednotili z razvitimi kazalniki ter predstavili, kakšna je trenutna situacija varovanja zasebnosti in skladnosti z GDPR na področju mobilnega zdravstva in kakšne izboljšave lahko uvedejo razvijalci in podjetja.

1.1 Struktura naloge

V naslednjem poglavju bomo naredili pregled sorodnih del, kjer pregledamo obstoječe raziskave in predlagamo izboljšave. V tretjem poglavju na splošno predstavimo arhitekturo Android, izzive mobilnega zdravstva ter razvijemo

kazalnike varovanja zasebnosti in skladnosti z GDPR. V četrtem poglavju je predstavljena razvita spletna aplikacija za varnostno pregledovanje aplikacij Android. Analizirali smo izbrane mobilne zdravstvene aplikacije ter v petem poglavju predstavili rezultate analiz in ovrednotenja na podlagi razvitih kazalnikov.

Poglavje 2

Sorodna dela

Trg mobilnih zdravstvenih aplikacij je v zadnjih letih postal zelo nasičen. Leta 2017 je dosegel kar 50-odstotno rast v primerjavi z letom 2016 in tako platformo Android popeljal na vodilno mesto mobilnih zdravstvenih aplikacij. Skupaj s hitro rastjo števila aplikacij se je povečalo tudi število raziskav o varnosti in zasebnosti za uporabnike. V delu [9] je izvedena študija, kjer je na podlagi sedmih tarč napada, analiziranih 22 naključnih aplikacij iz trgovine Google Play. Na podlagi pregleda obstoječih del so določili naslednja področja nevarnosti: internet, storitve tretjih oseb, Bluetooth, dnevniški zapisi, shranjevanje na zunanji pomnilnik, javne komponente in stranski kanali. Rezultati pokažejo, da je glavna težava priljubljenih aplikacij ravno nešifrirana internetna komunikacija s strežniki in zapisovanje občutljivih informacij v dnevniške datoteke. Zubaydi idr. se v delu [10] ukvarjajo z vprašanji o varnosti in zasebnosti mobilnih zdravstvenih sistemov, predstavijo varnostne zahteve za snovanje varnih mobilnih zdravstvenih aplikacij, navajajo možne napade in grožnje, ki so enaki kot v viru [9], ter prav tako obravnavajo učinkovite protiukrepe. Kotz idr. v delu [11] analizirajo grožnje in predlagajo metodo varnostnega testiranja s študijo primera, aplicirano na mobilne zdravstvene aplikacije Android, ki nadzirajo hipertenzijo in sladkorno bolezen. Ugotovili so, da številne aplikacije nimajo politik zasebnosti in ne uporabljajo varnega omrežnega komuniciranja ter imajo nizko kakovost

programske kode. Razvijalcem predlagajo uporabo orodij za varnostno testiranje aplikacij, kot sta `MalloDroid` ter `Drozer`, in tudi testiranje spletnih strežnikov, na katere se povezuje aplikacija. Dehling idr. so v delu [12] na podlagi informacij, ki jih je mogoče pridobiti iz trgovin Google Play in App Store, naredili pregled razpoložljivih mobilnih zdravstvenih aplikacij, jih razvrstili v pet kategorij in ocenili vpliv informacijske varnosti in zasebnosti. Aplikacije so bile razvrščene v kategorije glede na zdravstvene specifičnosti informacij, možne posledice zaradi uhajanja podatkov, škodo zaradi manipulacije s podatki, škodo zaradi izgube podatkov in glede na potencialno vrednost podatkov za tretje osebe. Ugotovili so, da kar 95 odstotkov aplikacij lahko povzroči škodo zaradi kršitve informacijske varnosti in zasebnosti.
V članku [13] Sunyaev idr. ocenjujejo razpoložljivost, obseg in preglednost pravilnikov o zasebnosti mobilnih zdravstvenih aplikacij. Od 600 najpogosteje uporabljenih aplikacij je politiko zasebnosti vsebovalo samo 183 aplikacij. Politike zasebnosti, ki so na voljo, niso dovolj transparentne, zahtevajo dobro razumevanje ter se ponavadi sploh ne osredotočajo na samo aplikacijo.
V delu [14] so Bachiri idr. prav tako preverili politike zasebnosti dvanajstih aplikacij iOS in sedmih aplikacij Android za spremljanje nosečnosti. Nobena od ocenjenih politik zasebnosti ni v celoti ustrezala zahtevam raziskave. Razvijalci bi morali tako posvečati več pozornosti strukturi in vsebini pravilnikov o zasebnosti izdanih aplikacij.
Martinez idr. v delu [15] predstavijo pregled akademske literature o varnosti in zasebnosti mobilnega zdravstva ter povzetek vseh dobrih razvijalskih praks, ki ustrezajo veljavni zakonodaji.
Zaradi nenehnih razprav o zasebnosti mobilnega zdravstva je nedavni razvoj prinesel prvi resnejši korak v pravo smer pri varnosti in zasebnosti mobilnih zdravstvenih aplikacij. Kodeks [16], ki ga podpira Evropska komisija, od aprila 2015 razvijajo organizacije iz industrije mHealth (med njimi so App Association (ACT), App developers Alliance, Apple, COCIR, DigitalEurope, DHACA, ECHA, EFPIA, Google, Intel, Microsoft, Qualcomm in Samsung). Ta naj bi krepil zaupanje med uporabniki mobilnih zdravstvenih aplikacij in

razvijalci, ki se držijo kodeksa. Z uvedbo GDPR maja 2018 kodeks še ni bil odobren, saj še ni v celoti obravnaval zahtev te uredbe. Trenutni osnutek kodeksa vsebuje praktična navodila o varstvu podatkov za razvijalce aplikacij, ki se nanašajo predvsem na pravice in soglasje uporabnika, oglaševanje, omejevanje in posredovanje podatkov tretjim osebam ter varnostne ukrepe.

2.1 Razširitve

Naše delo je razširitev zgoraj navedenih člankov v zvezi z oceno varnosti in zasebnosti mobilnih zdravstvenih aplikacij, ki so na voljo v spletni trgovini Google Play. Analizo mobilnih zdravstvenih aplikacij smo razširili z razvitimi kazalniki varovanja zasebnosti in z uporabo orodja `TaintDroid` [17] za zaznavanje uhajanja občutljivih podatkov pri dinamični analizi. Dela, ki ocenjujejo politike zasebnosti smo razširili s pregledovanjem in ocenjevanjem politik z razvitimi kazalniki skladnosti z GDPR.
Varnostne ranljivosti iz sorodnih del smo preverili še z varnostnimi projekti organizacije OWASP ter delom [18]. OWASP Mobile Security Project [8] je standard za preverjanje varnosti aplikacij. Določa osnovne varnostne zahteve za mobilne aplikacije, ki so uporabne v mnogih scenarijih, vključno z:

- življenskim ciklom razvoja aplikacij, kjer so določene varnostne zahteve, ki jim morajo slediti arhitekti in razvijalci, ter
- penetracijskimi testi, da zagotovijo popolnost in doslednost testov.

Poleg standarda [8] je na voljo tudi OWASP Mobile Security Testing Guide [19], ki je celovit priročnik za testiranje varnosti mobilnih aplikacij in obratnega inženiringa. Opisuje tehnične postopke za preverjanje aplikacij, ki so navedene v [8]. V OWASP Mobile Top 10 [20] je zbranih deset kategorij, ki so pomembne za varnost na mobilnih platformah in so povzetek varnostnih vidikov iz del [8, 19]. Six v delu [18] bralcu nudi vpogled v varnostni model sistema Android ter kako obravnavati in zavarovati aplikacijo pred

grožnjami. Osredotoči se na zaščito datotečnega sistema, podatkovne baze in komponent, uporabo dovoljenj in zaščitenih sistemskih API-jev, uporabo kriptografskih orodij in zaščito podatkov pri komunikaciji s strežniki.

Poglavje 3

Problem, okolje in orodja

V tem poglavju bomo predstavili mobilno platformo Android, mobilno zdravstvo in njegove izzive, razvili kazalnike varovanja zasebnosti in skladnosti z GDPR ter predstavili orodja, s katerimi smo zgradili spletno aplikacijo za analizo mobilnih zdravstvenih aplikacij.

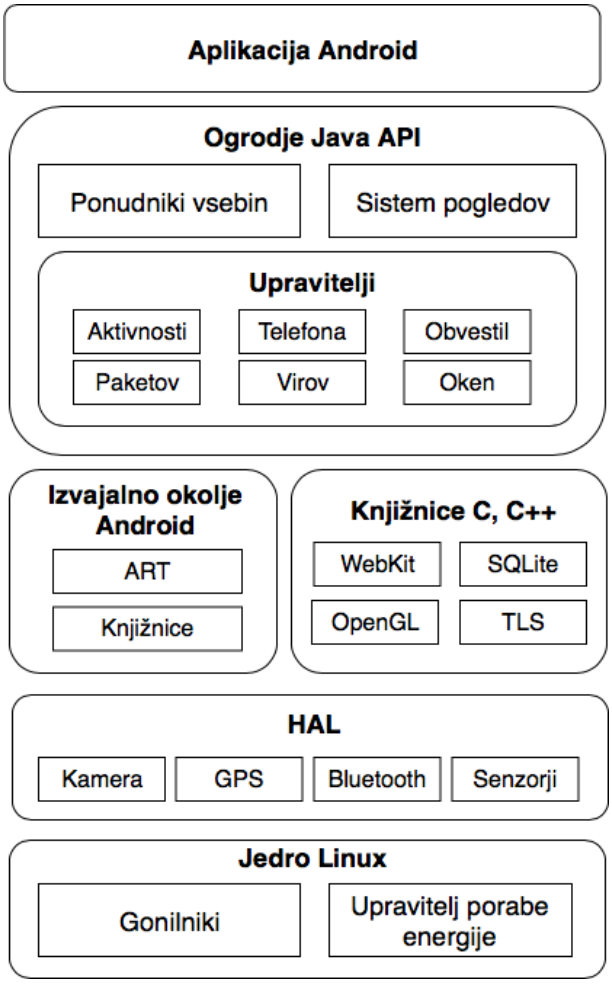
3.1 Android

Za analizirano platformo smo zaradi odprtokodnosti in popularnosti izbrali platformo Android. Preden nadaljujemo, je potrebno vedeti, kako Android in aplikacije delujejo. V tem podpoglavju je predstavljena sistemska arhitektura Android, zgradba aplikacij, njihovi varnostni mehanizmi in ključne točke analize.

3.1.1 Arhitektura sistema

Android je odprtokodni operacijski sistem, ki temelji na jedru Linux. Na sliki 3.1 je prikazana arhitektura sistema Android, ki je sestavljen iz naslednjih slojev:

- Jedro (angl. *kernel*) vsebuje vse ključne gonilnike za delovanje naprave, upravlja s procesi in pomnilnikom, nadzira dostop, porabo energije ter omogoča medprocesno komunikacijo.



Slika 3.1: Arhitektura sistema Android

- Abstrakcijska raven strojne opreme (angl. *hardware abstraction layer*) omogoča standarden vmesnik med strojno opremo ter ogrodji Java API. Vsebuje knjižnice, ki implementirajo vmesnike za specifične strojne komponente, kot sta na primer kamera in modul WiFi.

- Knjižnice C in C++, katerih funkcionalnosti so izpostavljene preko ogrodja Java API.

- Izvajalno okolje Android katerega gradijo jedrne knjižnice ter okolje izvajanja aplikacij, ki je pravzaprav navidezni stroj Java, specifično

prilagojen za Android. Zadnje verzije sistema uporabljajo izvajalno okolje ART, ki uporablja vnaprejšnje prevajanje Dalvik bajtne kode. To pomeni, da se prevajanje kode zgodi ob namestitvi aplikacije. ART se uporablja od sistema Android KitKat 4.4 naprej, pred tem se je uporabljal DVM (angl. *Dalvik virtual machine*). Ta za razliko od ART uporablja način prevajanja kode JIT (angl. *just in time*), ki se zgodi ob vsakem zagonu aplikacije.

- Ogrodje Java API omogoča grajenje aplikacij skozi vmesnike Java, kateri nudijo ustvarjanje aplikacij s poenostavitvijo ponovne uporabe jedra, modularnih delov sistema ter storitev in vključujejo:
  - sistem pogledov (angl. *view system*): omogoča grajenje uporabniškega vmesnika,
  - upravitelj virov (angl. *resource manager*): omogoča dostop do virov, kot so grafike, postavitve ter lokalizirane besede,
  - upravitelj obvestil (angl. *notification manager*): omogoča prikazovanje obvestil in opozoril,
  - upravitelj aktivnosti (angl. *activity manager*): omogoča upravljanje življenjskega cikla aplikacij,
  - ponudnik vsebin (angl. *content providers*): omogoča dostop do podatkov drugih aplikacij oziroma deljenje svojih podatkov.
- Sistemske aplikacije so najvišji nivo arhitekture, to so aplikacije kot je naprimer e-pošta, sporočila SMS, koledar, brskalnik in drugo.

3.1.2 Arhitektura aplikacij

Aplikacije Android so lahko napisane v programskih jezikih Kotlin, Java ali C++. Android SDK (angl. *software development kit*) kodo z vsemi potrebnimi dodatnimi datotekami zapakira v datoteko `APK` (angl. *Android application package*). Na sliki 3.2 je prikazana zgradba datoteke `APK`, ki vsebuje

manifest, meta podatke, vire, knjižnice, sredstva in bajtno kodo Dalvik. Ta se namesti na napravo Android, kjer se nato izvaja v lastnem peskovniku (angl. *sandbox*) in je zaščitena z varnostnimi mehanizmi, predstavljenimi v nadaljevanju poglavja.

Slika 3.2: Zgradba datoteke `APK`

3.1.3 Komponente aplikacije

Komponenta je gradnik in hkrati vstopna točka v aplikacijo. Obstajajo štiri različne vrste komponent, od katerih ima vsaka svoj namen in življenjski cikel. Pri specifikaciji komponent je pomembna tudi pravilna omejitev dostopa do javnih komponent.

- Aktivnost (angl. *activity*) predstavlja grafični izgled aplikacije in je začetna točka interakcije uporabnika. Aplikacija je ponavadi sestavljena iz več aktivnosti, ki s skupnim delovanjem predstavljajo celovito uporabniško izkušnjo, vendar so med seboj neodvisne. Če aplikacija

dovoli, lahko druga aplikacija zažene aktivnost prve aplikacije, na primer iz klepetalnika lahko zaženemo kamero in pošljemo sliko.
Aktivnost je lahko v različnih stanjih, in sicer v aktivnem stanju, ko je ta v ospredju in prikazuje uporabniški vmesnik, v zaustavljenem stanju, ko izgubi fokus, vendar je še vidna, in v ustavljenem stanju, ko aktivnost ni več vidna uporabniku. Aktivnost v zaustavljenem in ustavljenem stanju hrani informacije o aktivnosti, ki jih lahko povrne takrat, ko aktivnost spet preide v aktivno stanje.

- Storitev (angl. *service*) je namenjena opravljanju dolgotrajnih operacij v ozadju in nima uporabniškega vmesnika. Primer je predvajanje glasbe, saj uporabniku omogoča nemoteno izvajanje drugih aplikacij. Storitev je lahko zagnana z drugo komponento, kot je aktivnost ali sprejemnik namenov, ter se lahko izvaja tudi potem, ko je aplikacija uničena oziroma izbrisana.

- Namen (angl. *intent*) je sporočilo za komunikacijo med komponentami aplikacije. Nudi tudi komunikacijo s komponentami druge aplikacije. Namen je lahko ekspliciten, če je prejemnik točno določen s polnim imenom razreda, ter impliciten, če prejemnik namena ni točno določen in je izbrana le naloga, ki jo mora komponenta izvesti.

- Sprejemnik namenov (angl. *broadcast receiver*) je komponenta, ki aplikaciji omogoča odziv na dogodke oziroma namene, ki jih bodisi pošlje sistem bodisi druge aplikacije. Prav tako nudi tudi oddajanje namenov drugim aplikacijam. Tako lahko na primer aplikacija sproži prikaz obvestila, ko zazna nek dogodek.

- Ponudnik vsebin (angl. *content provider*) upravlja podatke aplikacije, ki so lahko shranjeni v datotečnem sistemu, podatkovni bazi SQLite ali katerikoli drugi obliki obstojne shrambe. S ponudnikom vsebin lahko aplikacija dostopa do podatkov drugih aplikacij, če ima za to pravice.

3.1.4 Datoteka *AndroidManifest.xml*

Datoteka `AndroidManifest.xml` vsebuje potrebne informacije o aplikaciji, ki omogočajo sistemu zagon komponent. Vsaka komponenta aplikacije mora biti zapisana v datoteki manifest, kjer so prav tako zapisana:

- uporabniška dovoljenja, ki jih aplikacija potrebuje, kot na primer za dostop do interneta, dostop do lokacije, dostop do kontaktov idr.;
- najnižja verzija Android API-ja, ki jo aplikacija še podpira;
- funkcije strojne in programske opreme, ki jih aplikacija uporablja. Te na primer vključujejo uporabo kamere, pospeškometra ali storitev Bluetooth;
- knjižnice API, ki niso del Android-a, na primer knjižnica Google Maps.

3.1.5 Peskovnik in medprocesna komunikacija

Android aplikacije so zavarovane z znanimi varnostnimi funkcijami.

- Operacijski sistem Android je večuporabniški sistem Linux, kjer vsaka aplikacija predstavlja uporabnika.
- Sistem dodeli aplikaciji uporabniški ID ter ji nastavi dovoljenja za dostop samo do njenih datotek.
- Vsak proces oziroma aplikacija ima svoj navidezni stroj (angl. *virtual machine*), kjer se koda izvaja ločeno od drugih aplikacij.
- Privzeto se vsaka aplikacija izvaja v svojem procesu. Ko je potrebno, Android zažene proces in ga ustavi, ko zapremo aplikacijo, da sprosti pomnilnik za druge aplikacije.

Vsaka aplikacija ima (privzeto) dostop zgolj do tistih komponent, ki jih potrebuje za svoje delo. Obstajajo pa tudi načini za delitev podatkov med aplikacijami.

- Dve aplikaciji si lahko delita Linux uporabniški ID in imata tako omogočen skupni dostop do datotek. Prav tako sta lahko aplikaciji zagnani v enem procesu, kjer si delita en navidezni stroj. Pogoj za to je, da sta aplikaciji podpisani z istim digitalnim potrdilom.

- Če uporabnik aplikaciji izrecno da dovoljenja, lahko ta dostopa do podatkov naprave, kot so kontakti, sporočila SMS, kartica SD, kamere in povezave Bluetooth.

- Komponente različnih aplikacij lahko med seboj komunicirajo in si izmenjujejo podatke, če imajo nastavljen filter namena ali pa so izrecno izvožene.

3.1.6 Mehanizem dovoljenj

Dovoljenja se uporabljajo za omejevanje dostopa aplikacij do občutljivih sistemskih programskih vmesnikov. Vsa dovoljenja, ki jih aplikacija potrebuje, morajo biti navedena v datoteki manifest. Preden je aplikacija nameščena na napravo, sistem vpraša uporabnika, ali želi odobriti dovoljenja. Na voljo so štiri vrste dovoljenj, in sicer:

- normalna, ki se odobrijo samodejno,

- nevarna, ki jih mora odobriti uporabnik,

- podpisana, ki so odobrena znotraj istega peskovnika,

- sistemska, ki so odobrena prednameščenim aplikacijam.

3.2 Mobilno zdravstvo

Mobilno zdravstvo (angl. *mHealth*) izhaja iz e-zdravstva in je zaradi izboljšav strojne opreme ter telekomunikacij v zadnjih letih postalo zelo priljubljeno in privabilo ogromno zanimanja potrošnikov in sprejetje s strani

večjih ponudnikov zdravstvenih storitev. Mobilno zdravstvo ima velik potencial za izboljšanje kakovosti zdravstvenega varstva, razširitev dostopa do storitev, zmanjšanje stroškov ter izboljšanje javnega zdravja. Te koristi se lahko doseže le, če bodo posamezniki prepričani v varovanje zasebnosti svojih informacij, povezanih z zdravjem, in če ponudniki zaupajo v varnost in celovitost zbranih podatkov [21].

Na žalost rast mobilnega zdravstva ni vzporedna s povečanjem mehanizmov za zaščito integritete podatkov in zasebnosti posameznika. V zdravstvu osebje dela namreč z občutljivimi zdravstvenimi podatki bolnikov, zato je varnost teh podatkov visoko prednostna. Kljub temu raziskave kažejo, da se kar 44 odstotkov vseh zlorab podatkov zgodi ravno v zdravstvu, predvsem zaradi privlačnosti medicinskih podatkov za kriminalce, saj na črnem trgu ti podatki dosegajo relativno visoko vrednost [22]. Do velikega deleža zlorab občutljivih podatkov v zdravstvu pride zaradi kraje in izgube mobilnih naprav oseb, ki so uporabljale zdravstvene aplikacije [23]. Dodatno težavo pri tem povzroča dejstvo, da zdravstvene ustanove z ukrepi za varovanje podatkov ne sledijo hitremu tempu uvajanja mobilnih naprav za uporabo v zdravstvene namene [15].

Svetovni trg mobilnega zdravstva naj bi do leta 2025 znašal 111,8 milijard dolarjev, pri čemer se je v skladu z novim poročilom podjetja Grand View Research, Inc. skupna letna stopnja rasti (angl. *Compound Annual Growth Rate - CAGR*) povečala na 44,2 odstotkov. Potreba po zmanjšanju dolgih čakalnih dob za dostop do zdravstvenih storitev je s strani strokovnjakov glavni vzrok za uvedbo mobilnega zdravstva [24]. Poleg aplikacij za naročanje bolnikov je tukaj še množica različnih aplikacij, ki nam lahko predlagajo nasvete za izgubo teže, merijo krvni tlak ter krvni sladkor, ženskam pomagajo spremljati menstrualni ciklus ali nosečnost idr. Da mobilne zdravstvene aplikacije prikažejo rezultate oziroma ponudijo predloge, morajo najprej zbrati uporabnikove podatke širokega spektra, kot so na primer njihova vsakodnevna aktivnost, prehrana, način življenja, njihova lokacija, višina krvnega tlaka idr. Uporabniki se morajo zavedati vedno večjih tveganj uporabe mobilne teh-

nologije, ki se nenehno spreminja. Aplikacije namreč omogočajo veliko večje in daljše zbiranje podatkov in ne zbirajo samo podatkov, ki jih uporabnik ročno vnese v telefon [9].

3.3 Kazalniki ogroženosti zasebnosti

S sorodnimi deli in obstoječimi raziskavami [9, 10, 11, 15, 17, 18, 19, 20, 25, 26, 27] smo raziskali varnostne ranljivosti operacijskega sistem Android, ki bi ogrozile občutljive podatke v mobilnih aplikacijah. Nato smo s pregledom aplikacij iz našega niza določili, kateri podatki so lahko ogroženi. Na podlagi napadnih površin in ranljivosti ter ogroženih podatkov smo razvili kazalnike varovanja zasebnosti, na katerih bomo gradili našo arhitekturo za analizo ter z njimi na koncu ovrednotili aplikacije.
Pri ogroženosti zasebnosti pri mobilnih zdravstvenih aplikacijah in vrsti ogroženih podatkov imamo dve situaciji. V prvi imamo podatke, ki jih uporabnik vnese v aplikacijo namerno ali da aplikaciji izrecno dovoljenje, da zbira določene podatke. To so na primer elekronska pošta, geslo, teža, višina, krvni tlak, krvni sladkor, podatki o nosečnosti. Aplikacija mora poskrbeti za pravilno ter varno hranjenje podatkov na telefonu ali pa mora poskrbeti za varno komunikacijo in posredovanje podatkov, če pride do prenosa v zaledni sistem. Če za to ni poskrbljeno, lahko občutljive informacije postanejo dostopne zlonamernim aplikacijam ali napadalcem. Varnostne grožnje razdelimo v naslednje kategorije, iz katerih lahko izpeljemo naše kazalnike varovanja zasebnosti.

- Nezavarovana medprocesna komunikacija, ki lahko predstavlja tveganje in ogrozitev zasebnosti pri uporabi aplikacij. Operacijski sistem Android je sestavljen iz komponent, ki med seboj komunicirajo. Nepravilna implementacija dovoljenj komponent lahko pripelje do izvajanja zlonarmene kode ter do dostopanja do možnih občutljivih informacij v nezaščitenih komponentah. Če je katera od komponent izrecno izvožena in ni zaščitena z nobeno pravico, lahko druga aplikacija dostopa do

njenih podatkov in metod [28]. Iz tega izpeljemo prvi **kazalnik VZ1**: aplikacija mora imeti s pravicami zavarovane vse svoje izvožene komponente.

- Uporaba nevarnih pravic lahko omogoči dostop do sistemskih virov in ogrozi občutljive podatke. Varnostni mehanizem sistema Android temelji na pravicah oziroma dovoljenjih, ki ščitijo dostop do občutljivih zasebnih podatkov (telefonski imenik, koledar, e-pošta, lokacija, itd.) in sistemskih virov (Kamera, WiFi, GPS in drugi) [29]. Uporabnik mora pri namestitvi aplikacije odobriti zahtevana dovoljenja. Pri preverjanju nevarnih pravic uporabimo **kazalnik VZ2**: aplikacija ne zahteva nobenega nevarnega dovoljenja, ki bi ogrozilo občutljive zasebne podatke.

- Nezavarovana shramba podatkov predstavlja naslednjo nevarnost za ogrožanje zasebnih informacij. Podatki na zunanjem pomnilniku ali kartici SD ter podatki, shranjeni v skupnih preferencah (v primeru uporabe načina *world readable*, ki ga je mogoče uporabiti do verzije Android 4.2), so dostopni vsem ostalim nameščenim aplikacijam. Aplikacija z upravljalskimi pravicami lahko iz nešifrirane podatkovne baze SQLite prav tako prebere morebitne občutljive informacije [19]. Za to kategorijo ranljivosti določimo **kazalnik VZ3**: aplikacija ne sme zapisovati podatkov na zunanji pomnilnik in mora uporabljati šifrirano bazo.

- Zapisovanje občutljivih informacij v dnevniške zapise ali začasne datoteke ter vprogramirane občutljive informacije predstavljajo grožnjo zasebnim podatkom. Ostale nameščene aplikacije imajo možnost branja dnevniških zapisov naprave, od koder lahko preberejo morebitne občutljive informacije [19]. **Kazalnik VZ4** tako pravi, da aplikacija ne zapisuje podatkov v dnevniške zapise in začasne datoteke ter nima vprogramiranih občutljivih informacij.

- Nepravilna implementacija ali uporaba šibkih načinov šifriranja lahko

ogrozi zasebne podatke. Android ponuja različne algoritme za šifriranje podatkov, ki se jih mora razvijalec držati, saj so ponavadi ravno lastne implementacije tiste, ki niso prav implementirane in ogrozijo podatke. Nujno je tudi pravilno izvajanje varnostnih praks pri mrežni komunikaciji, da se napadalcem prepreči prisluškovanje občutljivim podatkom ali napade MITM. Rešitev za to je uporaba in pravilna implementacija šifriranja pri protokolu TLS ter preverjanje digitalnih potrdil. Neustrezno preverjanje in omogočanje samopodpisanih digitalnih potrdil predstavlja grožnjo za izvedbo napada MITM [20]. Za neustrezno šifiranje omrežne komunikacije ali odstotnost šifriranja tako določimo **kazalnik VZ5**.

- Uporaba zastarelih algoritmov za šifriranje ter uporaba šibkih inicializacijskih vektorjev, slabih generatorjev naključnih števil in šibkih zgoščevalnih funkcij s trčenji pri uporabi šifriranja predstavlja grožnjo zašifriranim podatkom, saj jih napadalec lažje dešifrira [27]. **Kazalnik VZ6** zato pravi, da aplikacija uporablja zgoščevalne funkcije brez trčenj in ne uporablja šibkih IV-jev, slabih generatorjev števil ter zastarelih algoritmov za šifriranje.

V drugi situaciji imamo podatke, ki jih aplikacija lahko pridobi iz naprave, na kateri je nameščena. To so identifikacijske številke naprave, stiki, sporočila, lokacija naprave ter informacije o uporabniškem računu, ki jih aplikacija lahko nezaznavno posreduje iz telefona. Dostop do podatkov, kot so lokacija, sporočila in stiki, lahko zaznamo že s statično analizo nevarnih pravic, kar pa ne moremo storiti pri identifikatorjih naprave, saj lahko aplikacija te podatke prebere brez uporabe pravic. Posledično za uhajanje podatkov uporabimo dinamično analizo sledenja podatkov od izvora do ponora. Uhajanje podatkov lahko označimo kot kakršno koli obliko prenosa osebnih podatkov ali kakršnih koli informacij, ki omogočajo unikatno identifikacijo naprave ali uporabnika naprave. Za to situacijo lahko izpeljemo še **kazalnik VZ7**, ki pravi, da iz aplikacije ne uhajajo podatki, s katerimi je mogoče identificirati napravo.

V tabeli 3.1 so zbrani vsi naši kazalniki, s katerimi bomo v naslednjem poglavju gradili našo arhitekturo za analizo mobilnih zdravstvenih aplikacij.

Kazalnik	**Opis**
VZ1	Aplikacija ima s pravicami ustrezno zavarovane vse komponente
VZ2	Aplikacija ne zahteva nevarnih dovoljenj za dostop do sistemskih API-jev
VZ3	Aplikacija varno shranjuje podatke v šifrirano bazo in podatke ne zapisuje na zunanji pomnilnik
VZ4	Aplikacija nima vprogramiranih občutljivih informacij, ne zapisuje podatkov v dnevniške zapise ali začasne datoteke
VZ5	Aplikacija uporablja varen način omrežne komunikacije
VZ6	Aplikacija uporablja zgoščevalne funkcije brez trčenj, ne uporablja slabih generatorjev naključnih števil, šibkih inicializacijskih vektorjev ter zastarelih algoritmov za šifriranje
VZ7	Iz aplikacije ne uhajajo občutljivi podatki oz. podatki, s katerimi je mogoče identificirati napravo

Tabela 3.1: Kazalniki varovanja zasebnosti

3.4 Kazalniki skladnosti z GDPR

Mobilne zdravstvene aplikacije predstavljajo velik potencial v zdravstvu, vendar zaradi narave komunikacijske tehnologije in mobilnih naprav izpostavljajo veliko šibkosti. Lahko so ranljive za širok nabor varnostnih napadov[10], ki med drugim vključujejo zlonamerne aplikacije, katere lahko na napravi pridobijo shranjene občutljive podatke, jih spremenijo ali pošljejo iz naprave, ter slabe razvijalske prakse aplikacije, kjer se ne uporabljajo ustrezni varno-

stni protokoli in ogrozijo zasebne podatke. Same mobilne naprave so prav tako občutljive na nepooblaščen dostop ali fizično tatvino, ki bi lahko pripeljala do razkritja občutljivih informacij. Kot smo že omenili v uvodu, je maja lani v veljavo stopila nova Evropska uredba o varstvu podatkov GDPR (angl. *General Data Protection Regulation*), ki predstavlja velik korak na področju zasebnosti za vse članice Evropske unije. To je ključni trenutek za povečanje zaupanja potrošnikov in uporabnikov mobilnih zdravstvenih aplikacij, saj bodo uporabniki veliko raje in brezskrbno uporabljali aplikacije in storitve, ki so skladne z uredbo GDPR.

Pomembno je razlikovati med osnovnimi podatki ter občutljivimi osebnimi podatki. Obstajajo podatki, ki so neškodljivi za sklepanje o zdravju posameznika in ne padejo v kategorijo občutljivih zdravstvenih podatkov. Imenujemo jih tudi osnovni podatki (angl. *raw data*). Kljub temu lahko ti podatki v nekaterih primerih postanejo občutljivi in se obravnavajo kot občutljivi zdravstveni podatki posameznika. Do tega pride v primeru daljšega zbiranja podatkov in kombinacije z dodatnimi podatkovnimi nizi. Ni preprostega načina za določitev, da nekateri podatki, ki se zbirajo v mobilnih zdravstvenih aplikacijah, res spadajo v kategorijo občutljivih zdravstvenih podatkov. Za določitev občutljivih podatkov je potrebno poznati in razumeti celoten kontekst in uporabo aplikacije [30]. Ko uporabnik v aplikacijo samo enkrat vnese svojo trenutno težo, potem to morda ni občutljiva zdravstvena informacija. Če pa aplikacija spremlja spremembe teže uporabnika dlje časa, lahko iz tega nekaj sklepamo. V primeru, da se teža povečuje, potem lahko rečemo, da ima uporabnik morda težave z debelostjo, v primeru hitrega zmanjševanja teže pa ima lahko uporabnik anoreksijo ali težave z depresijo.

Med novosti uredbe sodijo soglasje za zbiranje in obdelavo osebnih podatkov, kjer morajo zbiralci podatkov poskrbeti za soglasje zbiranja in obdelovanja podatkov, ki posamezniku, na katerega se osebni podatki nanašajo, zagotavlja jasne informacije o tem, kdo bo obdeloval te podatke, zakaj in kako dolgo se bodo podatki obdelovali, in posamezniku dati vse možnosti za upravljanje svojih podatkov.

Pravica do pozabe je naslednja novost, kjer ima posameznik pravico do dostopa in nadzorovanja svojih podatkov. To pomeni, da ima uporabnik pravico do popolnega izbrisa svojih osebnih podatkov, kakor tudi ustavitev obdelave podatkov pri tretjih osebah.
Če pride do napada oziroma vdora v strežnike, kjer se hranijo osebni podatki, morajo podjetja v 72 urah obvestiti uporabnike kot tudi organe oblasti o uhajanju podatkov.
Z uvedbo GDPR je zasebnost postala pravna zahteva. To pomeni, da mora podjetje skrbeti za varstvo in zasebnost podatkov v celotnem ciklu projekta in ne samo v postprodukciji. To vključuje šifriranje in ali psevdonimizacijo osebnih podatkov pri obdelavi, zagotavljanje trajne zaupnosti, vzpostavitev postopka za redno preverjanje varnosti in oceno varnostnih praks.
Podjetja oziroma pravne osebe katera obdelujejo večje količine osebnih podatkov, bodo morale imeti pooblaščene osebe za varstvo osebnih podatkov, ki so jasno navedene v politiki zasebnosti.
Pri skladnosti z novo uredbo je pomembno tudi, da upravljavec ali obdelovalec v politiki zasebnosti posamezniku poda dodatne informacije o zbiranju in obdelavi podatkov. Politika zasebnosti mora tako navesti

- informacije o podjetju, ki zbira ali obdeluje informacije in se mora identificirati kot upravljavec ali obdelovalec,
- vse kontaktne informacije podjetja ali pooblaščene osebe za nadzor podatkov,
- katere osebne informacije zbira,
- kako in zakaj zbira informacije,
- pravno podlago, na kateri so bili podatki zbrani (primer tega je posameznikovo soglasje za obdelavo podatkov za določen namen),
- kako so osebne informacije zavarovane,
- če ima kdo od tretjih oseb dostop do informacij,

- kako lahko posameznik nadzira svoje informacije, to pomeni, da lahko informacije kadar koli spremeni, jih izvozi ali pa izbriše.

Na podlagi zgornjih zahtev uredbe smo tako lahko razvili naslednje kazalnike skladnosti z GDPR.

- **GDPR1** soglasje. Po namestitvi aplikacije ali pred prvo uporabo mora uporabnik privoliti o morebitnem zbiranju in obdelavi podatkov. V politiki zasebnosti mora biti navedeno, kateri podatki se zbirajo ter v kakšne namene se uporabljajo. Soglasje mora biti jasno in nedvoumno izraženo ter je lahko pridobljeno na različne načine. Aplikacija lahko od uporabnika zahteva soglasje za vse funkcije samo enkrat, ob prvi uporabi, ali pa soglasje zahteva v različnih fazah aplikacije ali v različnih kontekstih, ko aplikacija začne zbirati ali obdelovati nove podatke. Kontekstualno soglasje ponuja uporabniku več nadzora nad svojimi zasebnimi podatki.

- **GDPR2** možnost odvzema soglasja. Uporabnik mora imeti možnost kadar koli preklicati soglasje in zahtevati izbris zbranih podatkov.

- **GDPR3** sprememba in prenosljivost podatkov. Uporabnik mora imeti možnost izvoza vseh podatkov, ki jih aplikacija zbira, ter možnost kadar koli spremeniti osebne podatke.

- **GDPR4** informacije o obdelovalcu, upravljavcu ter pooblaščeni osebi za varstvo podatkov. V politiki zasebnosti mora biti jasno navedeno, kdo zbira podatke in jih obdeluje. Navedena mora biti tudi kontakna oseba ali pooblaščena oseba za varstvo podatkov. Pooblaščena oseba za varstvo podatkov je dolžna tudi obvestiti uporabnike o morebitnih vdorih in krajah podatkov.

- **GDPR5** profiliranje, marketing ter tretje osebe. Politika zasebnosti mora jasno navesti, če se kateri koli zbrani podatki pošiljajo tretjim osebam ter če se ti uporabljajo za profiliranje ali marketing.

- **GDPR6** vgrajena varnost in zasebnost (angl. *Privacy by design*). Vsaka aplikacija, ki je skladna z GDPR, mora biti zasnovana tako, da ščiti osebne podatke pred morebitnimi napadi in vdori skozi celoten življenjski cikel aplikacije. Ta kazalnik potrdimo le, če so potrjeni vsi prejšnji kazalniki varovanja zasebnosti.

Zaradi narave zbiranja velike količine podatkov in velikega števila možnih tarč napadov morajo zdravstvene aplikacije izpolnjevati zahteve glede varnosti in zasebnosti, ki jih opredeljuje evropski GDPR. V Ameriki pa zdravstvene podatke varuje HIPAA (angl. *Health Insurance Portability and Accountability Act*), vendar se v našem delu zaradi obsežnosti osredotočimo samo na evropsko uredbo. V tabeli 3.2 so zbrani vsi razviti kazalniki skladnosti z GDPR.

Kazalnik	**Opis**
GDPR1	Po namestitvi aplikacije ali pred prvo uporabo mora uporabnik izrecno soglašati z morebitnim zbiranjem in obdelavo podatkov
GDPR2	Uporabnik ima možnost odvzema soglasja
GDPR3	Uporabnik ima možnost spremeniti ali izvoziti zbrane podatke
GDPR4	Politika zasebnosti vsebuje informacije o obdelovalcu, upravljavcu ter pooblaščeni osebi za varstvo podatkov
GDPR5	Politika zasebnosti vsebuje informacije o morebitni uporabi osebnih podatkov za profiliranje, marketing in morebitnem posredovanju podatkov tretjim osebam
GDPR6	Aplikacija je zasnovana tako, da ščiti osebne podatke pred morebitnimi napadi in vdori

Tabela 3.2: Kazalniki skladnosti z GDPR

3.5 Orodja za analizo

Predstavimo orodja za varnostno analizo aplikacij Android, ki smo jih uporabili pri gradnji naše arhitekture.

Statična analiza se izvaja na izvorni kodi aplikacije, zato se mora zapakirana datoteka `APK` pred analizo razpakirati v izvorno kodo. `ApkTool` je orodje za obratno inženirstvo aplikacij Android, ki omogoča dekodiranje aplikacije v skoraj popolnoma izvirno obliko izvorne kode, nad katero se lahko izvaja statična analiza. Iz arhiva `APK` ustvari datoteko `AndroidManifest.xml` ter mapo, ki vsebuje vse izvorne vire in meta podatke. Datoteka `dex` je razstavljena na posamezne datoteke `smali`, kjer vsaka predstavlja razred Java v datoteki `dex`. Datoteka `smali` vsebuje zbirni jezik Smali, ki ga uporablja navidezni stroj Dalvik. Postopek obratnega inženirstva je zelo učinkovit in za pretvorbo posamezne datoteke `APK` porabi od deset do dvajset sekund.

`MobSF` (angl. *Mobile Security Framework*) [31] je odprtokodno ogrodje za varnostno analizo mobilnih aplikacij iOS, Android in Windows. Pri gradnji naše arhitekture smo uporabili statični analizator orodja `MobSF`, ki omogoča samodejen pregled kode. Zazna nevarne programerske prakse, kot so neuporaba protokola TLS oziroma sprejemanje samopodpisanih digitalnih potrdil, uporabo šibkih kriptografskih funkcij ter slabih generatorjev naključnih števil, vprogramirane skrivnosti, nevarno implementacijo shranjevanja podatkov, zapisovanje informacij v dnevniške datoteke, zapisovanje podatkov na zunanji pomnilnik ter nevarne implementacije spletnih pogledov Android.

`TaintDroid` [17] je ena prvih sistemskih razširitev za dinamično analizo s postopkom sledenja označenim podatkom, ki je bila razvita v sodelovanju z Intel Labs ter univerzama Penn State in Duke University. Sistemska rešitev omogoča hkratno sledenje več označenim vhodnim virom občutljivih podatkov oziroma uporablja postopek sledenja označenim podatkom skozi program, od izvora do ponora (angl. *taint analysis*). V času izvajanja aplikacije `TaintDroid` natančno analizira, na kakšen način so zasebni podatki pridobljeni (izvor) in kam se posredujejo (ponor). Tako zagotavlja analizo v realnem času z uporabo virtualiziranega okolja Android in za svojo ana-

lizo porabi samo 14 odstotkov več procesorskega vira. Ob vedenjski analizi aplikacij je potrebno imeti zadostne kontekstualne informacije, od kod so podatki pridobljeni ter kdaj in kako zapustijo napravo. `TaintDroid` samodejno označuje (angl. *taints*) podatke iz virov, ki so občutljivi na zasebnost, ko ti potujejo prek programskih spremenljivk, datotek in medprocesnih sporočil. Ko označeni podatki s pomočjo interneta ali na kakšen drug način zapustijo sistem, `TaintDroid` v dnevniške datoteke zapiše oznake podatkov, aplikacijo, ki je podatke prenesla, in njihovo destinacijo.

`Android SDK` (angl. *Android software development kit*) vsebuje platformna orodja, med njimi je tudi orodje ukazne vrstice `adb` (angl. *Android debug bridge*). Ta omogoča komunikacijo in izvajanje ukazov na povezani napravi Android ali emulatorju. Za izvajanje ukazov smo naredili knjižnico, ki uporablja `adb`.

`TCPDUMP` je orodje za analizo paketov, ki mogoča prestrezanje in prikazovanje prenešenih paketov TCP/IP. `TCPDUMP` deluje na večini Unix podobnih operacijskih sistemov, kot so Linux, Solaris, BSD, Mac OS, in za zajemanje paketov uporablja knjižnico `libpcap`. Ker pa nima uporabniku prijaznega uporabniškega vmesnika za pregledovanje zajetega prometa, smo za nadaljnjo ročno analizo mrežnega prometa uporabili `Wireshark`, ki je tako kot `TCPDUMP` odprtokodno orodje za profiliranje omrežnega prometa in analiziranje paketov. Ta poleg grafičnega vmesnika omogoča prikaz enkapsulacije in pomen zajetih paketov ter prikaz podatkov z uporabo filtrov [32].

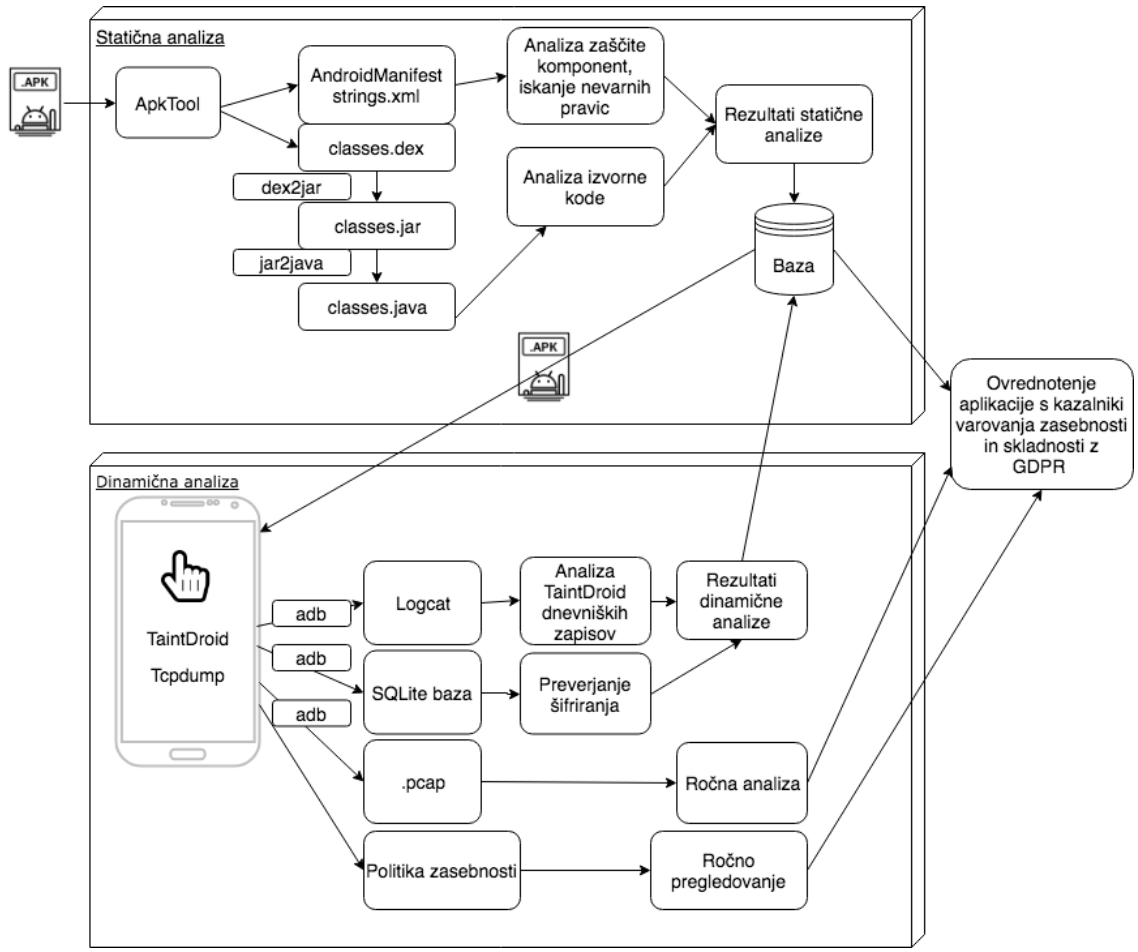
Poglavje 4

Arhitektura za varnostno analizo in zaznavanje uhajanja podatkov

V tem poglavju predstavimo arhitekturo za varnostno analizo in zaznavanje uhajanja podatkov, ki smo jo izdelali na podlagi razvitih kazalnikov iz tretjega poglavja.

4.1 Opis spletne aplikacije

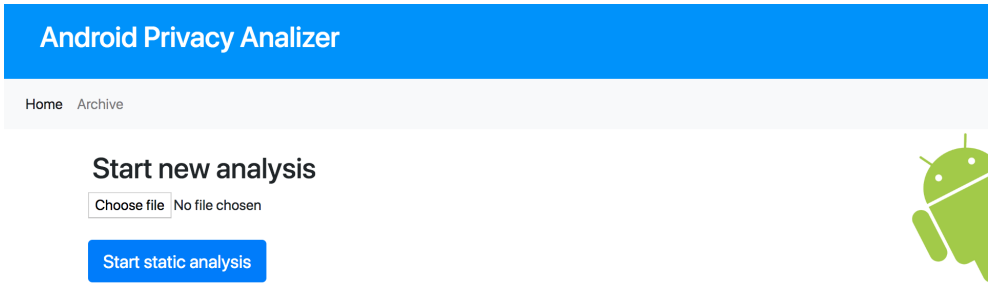
Arhitekturo za analizo smo implementirali kot spletno aplikacijo, ki smo jo razvili v odprtokodnem ogrodju Django, ki uporablja programski jezik Python. Spletna aplikacija je sestavljena iz uporabniškega vmesnika za pregledovanje rezultatov ter zalednega sistema, kjer se z odprtokodnmi orodji izvaja analiza. Za shranjevanje rezultatov analiz uporablja podatkovno bazo SQLite. Spletna aplikacija je sestavljena modularno. Vsebuje modul za statično analizo, kjer sta implementirani analiza datoteke `AndroidManifest.xml` ter analiza izvorne kode, ki se izvaja s pomočjo orodja `MobSF`[31]. Modul za dinamično analizo je sestavljen iz funkcij za komunikacijo z napravo Android preko `adb` ter analizatorja dnevniških zapisov razširitve `TaintDroid`[17]. Vsak



Slika 4.1: Potek analize

modul prav tako vsebuje konfiguracijsko datoteko, preko katere lahko dodajamo ali spreminjamo pravila in nastavitve analize. Spletna aplikacija je skupaj s podatkovno bazo zapakirana v vsebnik Docker [33], ki omogoča preprosto zaganjanje tako v lokalnem okolju, kot tudi v oblačni infrastrukturi. Na sliki 4.1 je prikazan potek analize aplikacije. Začetni prikaz spletne aplikacije je prikazan na sliki 4.2, kjer najprej naložimo datoteko `APK`, ki vsebuje analizirano aplikacijo. Datoteka `APK` se shrani nato pa se zažene orodje `APKTool`, ki jo razpakira na datoteko `AndroidManifest.xml` ter datoteko `dex`, ki vsebuje izvorne razrede aplikacije. Datoteka `dex` se nato z orodji `dex2jar` in `jar2java` razpakira v datoteko `Java`, ki vsebuje izvorno kodo,

nad katero se začne izvajati statična analiza kode.



Slika 4.2: Začetni pogled

4.2 Postopek statične analize

Ko iz datoteke `APK` dobimo izvorne datoteke, lahko začnemo s statično analizo. Spletna aplikacija za vsako analizirano aplikacijo na začetku ustvari objekt, ki ga shrani v podatkovno bazo. Ta objekt napolni s ključnimi infomacijami o analizirani aplikaciji, ki jih dobi s pregledovanjem datoteke `AndroidManifest.xml`:

- ime datoteke `APK`,
- zgoščena vrednost datoteke `APK`,
- ime aplikacije,
- ime paketa,
- minimalna in maksimalna verzija sistema Android.

Ko je objekt analizirane aplikacije ustvarjen, naša spletna aplikacija začne s statično analizo. Prvi korak je analiziranje datoteke `AndroidManifest.xml`,

kjer se začne z iskanjem nevarnih pravic, ki predstavljajo grožnjo občutljivim podatkom. Nevarne pravice, ki jih spletna aplikacija išče med analizo, so določene v konfiguracijski datoteki. Največkrat uporabljena pravica, ki lahko ogrozi zasebne podatke, je WRITE_EXTERNAL_STORAGE, saj omogoča pisanje podatkov na zunanji pomnilnik, tj. kartico SD, od koder lahko podatke prebere vsaka nameščena aplikacija in tudi morebitni napadalec, ki ima fizičen dostop do kartice SD. V tabeli 4.1 so navedene vse nevarne vrste pravic, ki jih naša spletna aplikacija zabeleži pri analizi. Nekatere nevarne pravice aplikacija lahko zahteva zaradi njenega delovanja oziroma nudenja funkcionalnosti, na primer uporaba kamere za merjenje utripa in uporaba lokacije za spremljanje prehojene razdalje. Uporabo nevarnih pravic bomo potrdili ali ovrgli s **kazalnikom VZ2**, vendar pri tem *ne bomo upoštevali* tistih, ki se uporabljajo za zagotovitev funkcionalnosti.

Nevarna pravica	**Opis možnosti**
READ_EXTERNAL_STORAGE	Branje iz zunanjega pomnilnika
WRITE_EXTERNAL_STORAGE	Pisanje na zunanji pomnilnik
RECORD_AUDIO	Zajemanje audio posnetkov
PROCESS_OUTGOING_CALLS	Procesiranje zunanjih klicev, lahko nadzoruje, preusmeri ali prekine klic
CAMERA*	Zajemanje posnetkov s kamero
ACCESS_FINE_LOCATION*	Poizvedba trenutne GPS lokacije
ACCESS_COARSE_LOCATION*	Poizvedba trenutne lokacije na podlagi mobilnega omrežja
SEND_SMS	Pošiljanje kratkih sporočil
SEND_SMS_NO_CONFIRMATION	Pošiljanje kratkih sporočil brez potrditve uporabnika
READ_SMS	Branje kratkih sporočil iz naprave ali kartice SIM
CALL_PHONE	Izvajanje klicev brez intervencije uporabnika

READ_CONTACTS	Branje stikov iz imenika naprave
READ_PROFILE	Branje podatkov iz uporabnikovega osebnega profila
READ_SOCIAL_STREAM	Branje uporabnikovega družbenega profila
READ_CALENDAR	Branje dogodkov in opomnikov iz koledarja
READ_HISTORY_BOOKMARKS	Branje vse zgodovine in zaznamkov internetnega brskalnika
AUTHENTICATE_ACCOUNTS	Upravljanje z up. računi na napravi, ustvarjanje novih in prav tako branje gesel
INSTALL_PACKAGES	Namestitev Android paketov oziroma aplikacij
READ_PHONE_STATE	Branje podatkov o napravi, kot so telefonska ali serijska številka

Tabela 4.1: Nevarne pravice, ki jih zabeležimo pri statični analizi. Legenda: * nevarnih pravic ne upoštevamo pri ovrednotenju s kazalnikom VZ2.

Drugi korak analize datoteke `AndroidManifest.xml` je branje vseh navedenih komponent, ki sestavljajo analizirano aplikacijo. Vsaka komponenta se zabeleži in označi, ali je ta izvožena, tj. javna ter če je zaščitena s pravicami. Pri tem se upošteva, da mora biti komponenta zavarovana s pravico, če je

- izvožena eksplicitno (atribut `exported` ima vrednost `true`),
- izvožena implicitno (to pomeni da ima nastavljen filter namenov).

Če javna ali implicitno izvožena komponenta nima dodeljene nobene pravice za dostop, potem dobi oznako, da je nezaščitena, saj je dostopna katerikoli aplikaciji na napravi. Javni dostop ima seveda svojo funkcijo, saj

je vsaka glavna aktivnost javna, zato da lahko aplikacijo zaženemo od koder koli. Ampak v večini primerov morajo komponente specificirati, katere aplikacije lahko dostopajo do njih. Sistem dovoljenj pri sistemu Android omogoča različnim komponentam določanje omejitev glede dostopnosti drugih komponent. Večina osnovnih aplikacij je ponavadi sestavljena le iz nekaj aktivnosti, medtem ko so bolj zahtevne aplikacije poleg aktivnosti sestavljene tudi iz storitev, ponudnikov storitev in sprejemnikov namenov. Poleg tega Android spodbuja uporabo navezanih komponent in komunikacijo z nameni, kjer več različnih aplikacij skupaj izpolni željeno funkcionalnost. Poleg prednosti takšnega načina oblikovanja aplikacij pa to lahko privede do aplikacij, ki imajo dostop do podatkov in občutljivih informacij, a ga ne bi smele imeti. Tako mora razvijalec upoštevati, katere vrste podatkov in katero vrsto storitev zagotavljajo komponente in katere druge komponente imajo dostop do podatkov. Z rezultati analize zaščite komponent lahko pri analizirani aplikaciji potrdimo ali ovržemo **kazalnik VZ1**.

Po končani analizi datoteke `AndroidManifest.xml`, spletna aplikacija zažene statični analizator kode orodja `MobSF`[31], ki v izvorni kodi analizirane aplikacije išče morebitne ranljivosti. Vsako nevarnost, ki jo lahko zazna statični analizator orodja `MobSF` lahko povežemo z razvitimi kazalniki varovanja zasebnosti iz tretjega poglavja, ki jih po analizi potrdimo ali ovržemo. **Kazalnik VZ3** lahko potrdimo, če v izvorni kodi ni nobene od naslednjih nevarnosti:

- **Datoteka ima odprte pravice pisanja in branja.** Vsaka aplikacija lahko bere ali piše v datoteko, kar predstavlja ranljivost.
- **Aplikacija piše in bere podatke iz zunanjega pomnilnika.** Datoteke na zunanjem pomnilniku lahko spremeni vsaka nameščena aplikacija na napravi.
- **Aplikacija ustvari začasno datoteko.** Varne aplikacije ne smejo nikoli ustvarjati začasnih datotek, saj lahko te vsebujejo občutljive informacije.

- **Android spletni pogled naloži datoteke iz zunanjega pomnilnika.** Datoteke na zunanjem pomnilniku lahko spremeni vsaka nameščena aplikacija na napravi.

Da **kazalnik VZ3** v celoti potrdimo ali ovržemo, je potrebno preveriti tudi, če aplikacija uporablja podatkovno bazo SQLite in če je ta šifrirana. To preverimo pri izvajanju dinamične analize. **Kazalnik VZ4** lahko potrdimo, če analizator `MobSF` ne najde nobene od nevarnosti:

- **Vprogramirane občutljive informacije**, kot so uporabniška imena, gesla ali ključi.
- **Zapisovanje informacij v dnevniške zapise** med katerimi so lahko občutljive informacije.
- **Skriti elementi v pogledu Android**, ki lahko vsebujejo občutljive informacije.

Kazalnik VZ5 lahko potrdimo, če v izvorni kodi ni nobene od nevarnosti:

- **Nevarna implementacija protokola TLS.** Zaupanje in sprejemanje samopodpisanih digitalnih potrdil je kritična varnostna luknja. Aplikacija je ranljiva na napade MITM.
- **Nevarna implementacija spletnega pogleda Android.** Spletni pogled ignorira napake protokola TLS in sprejme vsa digitalna potrdila. To lahko privede do ranljivosti na napade MITM.

Kazalnik VZ6 pa potrdimo, če v izvorni kodi ni naslednjih nevarnosti:

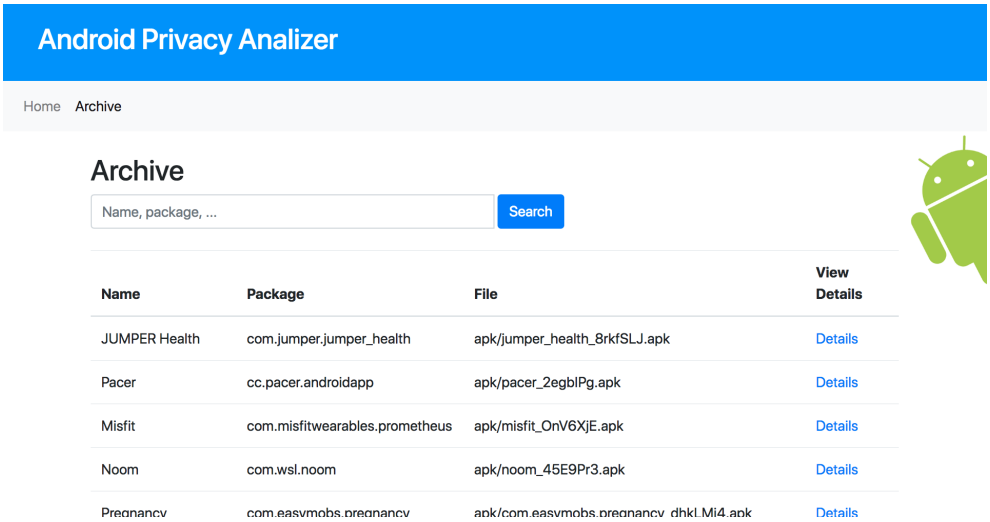
- **Uporaba načina šifriranja ECB**. Slednji proizvede enak šifrirani blok za enakovreden blok besedila. To napadalcu olajša odšifriranje in ne zagotavlja celovitosti.
- **Uporaba šifriranja RSA brez sheme OAEP.** Osnovna implementacija RSA ni varna. Potrebno je namreč vnesti naključnost, npr. z uporabo sheme OAEP.

- **Uporabljena zastarela algoritma za šifriranje RC2, RC4 ali šibke zgoščevalne funkcije MD4, MD5 ali SHA-1.** Algoritma za šifriranje RC2 in RC4 nista več varna za uporabo, saj sta ranljiva na napade kot sta napad povezanih ključev (angl. *related key attack*) in Fluhrer, Mantin in Shamir napad [34]. Za varno implementacijo šifriranja morajo biti uporabljene zgoščevalne funkcije, ki so krepko brez trčenj. To pomeni, da je računsko nemogoče poiskati dve različni sporočili z enakim izvlečkom.

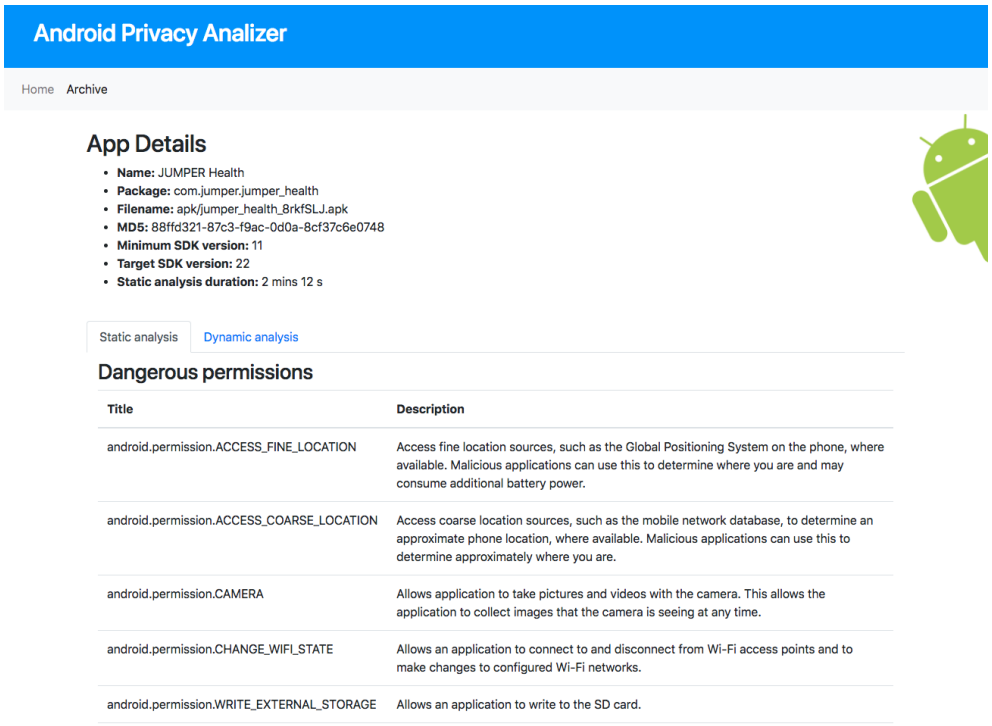
- **Aplikacija uporablja slab generator naključnih števil.**

- **Aplikacija uporablja šibke inicializacijske vektorje**, kot so [0x00, 0x00,0x00,0x00,0x00,0x00,0x00,0x00] ali [0x01,0x02,0x03,0x04,0x05, 0x06,0x07] in je zato bolj dovzetna za napade s slovarjem.

Ko statični analizator orodja `MobSF` pregleda celotno izvorno kodo, se najdene nevarnosti iz izvorne kode analizirane aplikacije shranijo v podatkovno bazo. Slika 4.4 prikazuje rezultate po končani statični analizi, kjer lahko odpremo tudi zavihek za dinamično analizo. Na sliki 4.3 pa je prikazan pogled za pregledovanje in iskanje že opravljenih analiz.



Slika 4.3: Arhiv opravljenih analiz



Slika 4.4: Pogled rezultatov statične analize

4.3 Postopek dinamične analize

Pri dinamični analizi spremljamo obnašanje aplikacije v času njenega izvajanja. Da dosežemo celotno pokritost aplikacije, to je sprožimo vse možne uporabniške akcije, moramo v aplikaciji ročno izvesti vse možne scenarije uporabe. Za ročno pregledovanje aplikacij smo se odločili predvsem zaradi narave zdravstvenih aplikacij, ki zahtevajo uporabniško prijavo in registracijo, skozi katero orodje ne more priti [35].

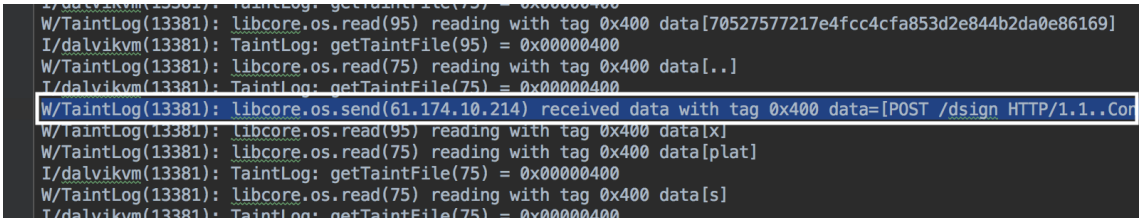
Izvorno kodo Android in izvorno kodo razširitve `TaintDroid`[17] smo prevedli v operacijski sistem Android verzije 4.3, ki z vgrajeno razširitvijo omogoča sledenje občutljivim podatkom od izvora do ponora. Operacijski sistem smo nato naložili na telefon LG Nexus 4, ki ga uporabljamo za izvajalno okolje pri dinamični analizi. Telefon mora biti med izvajanjem dinamične analize povezan z računalnikom, na katerem poganjamo našo spletno aplikacijo. Na

telefon smo naložili tudi orodje `TCPDUMP`, s katerim zajemamo omrežni promet med izvajanjem aplikacij. Vsa komunikacija med telefonom in našo spletno aplikacijo poteka preko ukazov orodja ukazne vrstice `adb`. S sledenjem podatkov od izvora do ponora lahko odkrijemo, ali aplikacija povzroči uhajanje občutljivih podatkov. Če gre tok občutljivih podatkov od informacijskega izvora skozi katerega od ponorov, ki so opisani v nadaljevanju, potem ta tok predstavlja uhajanje podatkov [17]. Informacijski izvori so označeni kot spremenljivke, ki dobijo vrednost iz klicev Android API. V tabeli 4.2 so prikazani izvori občutljivih podatkov, ki jim sledimo skozi analizo, ter njihove heksadecimalne označbe, ki nam pomagajo identificirati podatke pri analizi dnevniških datotek `TaintDroid`. Občutljivi podatki lahko zapustijo napravo na več načinov. `TaintDroid` kot ponore označi naslednje klice metod:

- *OutputStreamWriter.write()* in *SSLOutputStream.write()*: s temi klici metod lahko podatki zapustijo napravo skozi omrežje.

- *DataOutputStream.write()*: klic te metode predstavlja zapisovanje podatkov v datoteko.

- *GsmSMSDispatcher.sendSMS()* in *CdmaSMSDispatcher.sendSMS()*: s klici teh metod lahko občutljivi podatki zapustijo napravo preko poslanega SMS-a.



Slika 4.5: `TaintDroid` dnevniški zapis.

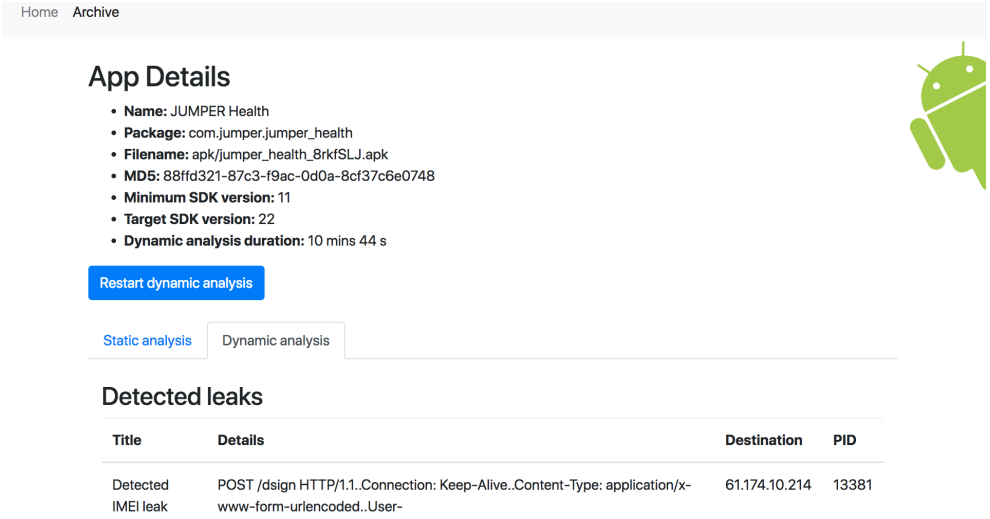
Podatek	**Opis**	**Oznaka**
Lokacija	Zadnja znana lokacija naprave	0x1
Kontakti	Kontakti telefonskega imenika	0x2
Mikrofon	Posnetek prek mikrofona naprave	0x4
Telefonska številka	Telefonska številka kartice SIM	0x8
Lokacija GPS	Trenutna lokacija GPS	0x10
Omrežna lokacija	Trenutna lokacije glede na mobilno omrežje	0x20
Kamera	Posnetek posnet s kamero naprave	0x80
SMS	Kratka sporočila	0x200
IMEI	Edinstven numerični identifikator naprave	0x400
IMSI	Edinstven numerični identifikator naročnika kartice SIM	0x800
ICCID	Edinstven numerični identifikator kartice SIM	0x1000
Serijska številka	Serijska številka naprave	0x2000
Uporabniški račun	Informacije o uporabniškem računu	0x4000
Internetna zgodovina	Zgodovina internetnega brskalnika	0x8000

Tabela 4.2: Izvori občutljivih informacij, ki jim sledimo skozi dinamično analizo

V zavihku dinamične analize s pritiskom na gumb *Start* začnemo analizo. Spletna aplikacija s pomočjo `adb` na napravo namesti datoteko `APK` aplikacije, zatem pa se zažene glavna aktivnost aplikacije, ki smo jo zabeležili pri statični analizi. Ob zagonu analizirane aplikacije se zažene tudi `TCPDUMP`, ki med izvajanjem aplikacije zapisuje mrežni promet v datoteko `pcap` na zunanji pomnilnik.
Po zagonu dinamično analize, začnemo uporabljati aplikacijo ter poskušamo

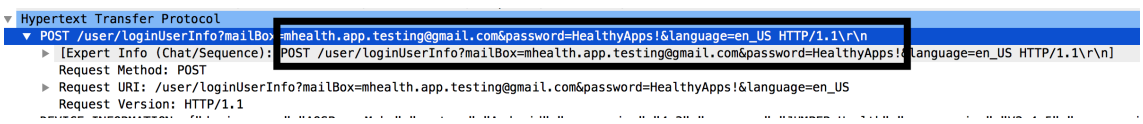
sprožiti vse njene funkcionalnosti. Večina mobilnih zdravstvenih aplikacij zahteva registracijo uporabniškega računa. V ta namen smo uporabili elektronski naslov `mhealth.app.testing@gmail.com` in geslo `HealthyApps!`, ki bi se lahko pojavila v nešifriranem omrežnem prometu. Med izvajanjem aplikacije smo pozorni tudi na prisotnost politike zasebnosti, ki jo lahko analiziramo s kazalniki GDPR.

Ko smo aplikacijo ročno pregledali, lahko dinamično analizo v naši spletni aplikaciji ustavimo s pritiskom na gumb *Stop* in v zaledju se bodo analizirali dnevniški zapisi `TaintDroid`, rezultati pa bodo shranjeni v bazo in vidni v uporabniškem vmesniku, kot je prikazano na sliki 4.6. Za pridobitev dnevniških zapisov, ki vsebujejo tudi zapise `TaintDroid`, uporabljamo ukaz `adb logcat`, tj. ukaz za zbiranje dnevniških zapisov različnih aplikacij. Primer `TaintDroid` dnevniškega zapisa je prikazan na sliki 4.5. `TaintDroid` samodejno označuje vire podatkov s heksadecimalnimi števili ter zapiše tudi, kako zapustijo sistem. Za zaznavo uhajanja podatkov se dnevniški zapisi analizirajo z regularnimi izrazi, kjer je pomembno še filtriranje glede na `PID` (angl. *process identification number*) trenutne analizirane aplikacije. Ob koncu dinamične analize preverimo tudi, če aplikacija uporablja SQLite podatkovno bazo in če je ta šifrirana. SQLite podatkovna baza uporablja datoteko s končnico `sqlite3`, ki se s pomočjo orodja `adb` skopira v datotečni sistem kjer je zagnana spletna aplikacija, nato pa nad datoteko podatkovne baze izvede izpis vsebine z orodjem `hexdump`. Z regularnim izrazom se preveri, če vsebina izpisa vsebuje niz $\gg$ |`sqlite format 3.`| $\ll$, ki predstavlja glavo podatkovne baze. To pomeni, da baza ni šifrirana. V primeru šifrirane baze bi izpis vseboval naključne znake.



Slika 4.6: Pogled rezultatov dinamične analize

V bazo spletne aplikacije se prav tako shrani datoteka `PCAP` analize mrežnega prometa, ki jo nato s pomočjo orodja `WireShark` ročno pregledamo. Moderne mobilne aplikacije za komunikacijo z zalednimi sistemi uporabljajo protokol HTTP ali HTTPS, kjer komunicirajo z zahtevki GET in POST, informacije pa pošiljajo v objektnem zapisu JSON ali XML. V orodju `Wireshark` najprej preverimo, ali se za komunikacijo uporablja šifriran protokol TLS ali nezavarovan protokol HTTP. Če se šifriranja ne uporablja, ročno analiziramo vso HTTP komunikacijo, kjer smo pozorni, če so v zahtevkih občutljivi podatki. V primeru uporabe protokola TLS pa preverimo zaznane nevarnosti pri statični analizi, kjer zaznamo če je implementacija protokola TLS napačna. Na sliki 4.7 je zaslonski posnetek programa `Wireshark`, kjer lahko vidimo, da ena izmed analiziranih aplikacij pošilja e-poštni naslov in geslo kar v golem besedilu.



Slika 4.7: E-poštni naslov in geslo poslano v golem besedilu

4.4 Analiza skladnosti z GDPR

Med izvajanjem dinamične analize smo preverili, ali aplikacije izpolnjujejo nove zahteve za varstvo osebnih podatkov, ki so določene v uredbi o varstvu osebnih podatkov. V analizo smo vključili le tiste zahteve, ki jih je mogoče jasno preveriti skozi statično analizo ter ročno izvajanjanje aplikacij. S pridobljenimi rezultati statične in dinamične analize ter z ročnim pregledovanjem politike zasebnosti, smo s kazalniki skladnosti z GDPR (3. poglavje), ovrednotili izbrane aplikacije. Skladnost z GDPR je pomembna z vidika zaupanja uporabnika mobilne aplikacije. Mobilne zdravstvene aplikacije morajo uporabnikom zagotavljati jasno politiko zasebnosti skladno z vsemi zahtevanimi informacijami nove uredbe, s katero se uporabnik strinja pred prvo uporabo aplikacije.

Pri dinamični analizi in pregledovanju skladnosti z uredbo smo zabeležili tudi, kateri podatki spadajo v kategorijo osebnih podatkov in kategorijo zdravstvenih podatkov uredbe. Kot smo navedli že v prejšnjem poglavju, je osebni podatek vsaka informacija, s katero je uporabnik določljiv, občutljiva zdravstvena informacija pa je tista informacija, na osnovi katere lahko nekaj sklepamo o zdravju posameznika.

Poglavje 5

Rezultati in ovrednotenje

V tem poglavju bomo predstavili rezultate analize mobilnih zdravstvenih aplikacij iz našega izbranega niza. Za naš niz analiziranih aplikacij smo izbrali 10 aplikacij iz trgovine Google Play pri čemer smo upoštevali, da je aplikacija:

- v angleškem ali slovenskem jeziku,
- spada v kategorijo medicina ali zdravo življenje,
- ima vsaj 1000 prenosov,
- ima oceno vsaj treh zvezdic,
- združljiva najmanj z operacijskim sistemom Android 4.3 ali več.

Za poganjanje spletne aplikacije za analizo smo uporabljali prenosni računalnik s procesorjem Core i5 (I5-4258U), z 8 GB pomnilnika ter operacijskim sistemom MacOS 10.13.6 in telefon LG Nexus 4 z 1.5 GHz štirijedrnim Krait procesorjem, 2 GB pomnilnika ter operacijskim sistemom Android 4.3 Jelly Bean, ki vsebuje razširitev `TaintDroid` ter orodje `TCPDUMP`. Po končani analizi z našo razvito spletno aplikacijo smo na podlagi rezultatov lahko ovrednotili mobilne zdravstvene aplikacije z razvitimi kazalniki varovanje zasebnosti in skladnosti z GDPR, kar prikazuje tabela 5.1 na strani 67.

5.1 Rezultati analiz

5.1.1 Jumper Health

- Razvijalec: Jumper-Medical
- Paket: com.jumper.jumper_health
- Opis iz trgovine Google Play: Jumper Health je zdravstvena aplikacija, ki spremlja indikatorje človeškega zdravja, kot so telesna teža, temperatura in količina kisika v krvi z uporabo izdelkov Jumper.
- Čas statične analize: 2 minuti 12 skund
- Čas dinamične analize: 15 minut 44 sekund

Nevarne pravice

ANDROID.PERMISSION.ACCESS_FINE_LOCATION
ANDROID.PERMISSION.ACCESS_COARSE_LOCATION
ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.CHANGE_WIFI_STATE
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE
ANDROID.PERMISSION.GET_TASKS
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.RECORD_AUDIO

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	0	53
Storitev	0	2
Sprejemnik namenov	2	2

Odkrite nevarnosti v izvorni kodi

Zapisovanje informacij v dnevniške zapise
Spletni pogled Android ne preverja digitalnih potrdil
Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v začasno datoteko
Uporaba šibke zgoščevalne funkcije MD5
Uporaba šibke zgoščevalne funkcije SHA-1
Zapisovanje podatkov na zunanji pomnilnik
Slab generator naključnih števil

Dinamična analiza

- Uhajanje informacij: Zaznali smo uhajanje številke IMEI, kar smo ugotovili tudi pri analizi omrežnega prometa.
- Analiza internetnega prometa: Odkrili smo, da aplikacija za komunikacijo ne uporablja šifriranja. Aplikacija pošlje vpisno uporabniško ime in geslo preko protokola HTTP z metodo POST v golem besedilu. Med poslanimi podatki je tudi številka IMEI.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija vsebuje politiko zasebnosti, s katero se moramo strinjati, preden ustvarimo uporabniški račun. V politiki zasebnosti manjka informacija o tem, kateri podatki in v kakšne namene se zbirajo. Uporabnik nima možnosti izbrisa ali spremembe podatkov. V politiki zasebnosti je navedeno samo to, da se zbrane podatke ščiti in ne pošilja tretjim osebam, kar pa ne velja, saj smo z analizo pokazali, da podatki niso zaščiteni.

- Zbrani osebni podatki: e-naslov, geslo, spol, vzdevek, datum rojstva, višina, lokacija, fotografija.

- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh podatkov lahko določimo zdravstveno ali fizično stanje uporabnika aplikacije: teža, količina kisika v krvi, telesna temperatura, krvni tlak, srčni utrip ploda.

5.1.2 Pacer

- Razvijalec: Pacer Health

- Paket: cc.pacer.androidapp

- Opis iz trgovine Google Play: Aplikacija Pacer vsebuje števec korakov, merjenje prehojene razdalje, porabljenih kalorij in ustvarjanje ciljev za izgubo teže. Svoje rezultate lahko uporabnik pregleduje in deli z drugimi na družbenem omrežju Pacer.

- Čas statične analize: 6 minut 30 sekund

- Čas dinamične analize: 20 minut 39 sekund

Nevarne pravice

ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.READ_EXTERNAL_STORAGE
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.ACCESS_FINE_LOCATION
ANDROID.PERMISSION.READ_CONTACTS
ANDROID.PERMISSION.DISABLE_KEYGUARD

Nezaščitene komponente

Komponenta	Število nezaščitenih	Število vseh
Aktivnost	7	156
Storitev	4	25
Ponudnik vsebin	0	7
Sprejemnik namenov	7	16

Odkrite nevarnosti v izvorni kodi

Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v dnevniške zapise
Zapisovanje podatkov na zunanji pomnilnik
Vprogramirane občutljive informacije
Uporaba šibke zgoščevalne funkcije MD5
Slab generator naključnih števil
Zapisovanje informacij v začasno datoteko
Uporaba šibke zgoščevalne funkcije SHA-1

Dinamična analiza

- Uhajanje informacij: Zaznali smo uhajanje številke IMEI, vendar smo bili na to opozorjeni že v politiki zasebnosti, kjer je navedeno, da ponudnik zbira tudi informacije o napravi.

- Analiza internetnega prometa: Pri analizi internetnega prometa smo ugotovili, da aplikacija za komunikacijo uporablja protokol TLS, pri statični analizi pa ni bilo najdenih nobenih nepravilnosti pri implementaciji šifriranja.

- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija vsebuje politiko zasebnosti, s katero se moramo strinjati, preden ustvarimo uporabniški račun. V politiki zasebnosti je jasno navedeno, kateri podatki se zbirajo, v kakšne namene se uporabljajo, uporabniku je navedena možnost izbrisa podatkov in kontakt, kamor se obrne za spremembo podatkov. Prav tako je navedeno, da se podatki, kot je lokacija in identifikatorji naprave, pošiljajo tretjim osebam v marketinške namene.

- Zbrani osebni podatki: e-naslov, geslo, spol vzdevek, datum rojstva, višina, lokacija, fotografija, identifikatorji naprave.

- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje uporabnika aplikacije: fizična aktivnost, poraba kalorij, izguba teže, srčni utrip in krvni tlak.

5.1.3 Misfit

- Razvijalec: Misfit Wearables Corporation

- Paket: com.misfitwearables.prometheus

- Opis iz trgovine Google Play: Misfit je preprosta aplikacija za spremljanje telesne aktivnosti in spanja, ki lahko deluje samostojno ali pa v povezavi z napravami Misfit.

- Čas statične analize: 4 minut 32 sekund

- Čas dinamične analize: 22 minut 48 sekund

Nevarne pravice

ANDROID.PERMISSION.ACCESS_FINE_LOCATION
ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.READ_SMS
ANDROID.PERMISSION.RECEIVE_SMS
ANDROID.PERMISSION.READ_CONTACTS

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	10	83
Storitev	3	8
Ponudnik vsebin	0	2
Sprejemnik namenov	11	20

Odkrite nevarnosti v izvorni kodi

Slab generator naključnih števil
Zapisovanje informacij v dnevniške zapise
Vprogramirane občutljive informacije
Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje podatkov na zunanji pomnilnik
Uporaba šibke zgoščevalne funkcije MD5
Zapisovanje informacij v začasno datoteko
Nevarna implementacija protokola TLS
Uporaba šibke zgoščevalne funkcije SHA-1
Uporaba načina šifriranja ECB

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize smo zaznali uhajanje številke IMEI.
- Analiza internetnega prometa: Aplikacija za komunikacijo uporablja protokol TLS, vendar smo pri statični analizi zaznali, da pri implementaciji protokola TLS zaupa tudi samopodpisanim digitalnim potrdilom. To predstavlja varnostno ranljivost za napad MITM.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija vsebuje politiko zasebnosti, s katero se moramo strinjati pred registracijo. Vsebuje informacije o tem, kdo zbira informacije, katere informacije zbira in v kakšne namene jih uporablja. V politiki zasebnosti so navedene tudi pravice za odvzem soglasja, izbris in spremembo podatkov. Tretje osebe so navedene, saj se uporabljajo za marketing in analitiko.

- Zbrani osebni podatki: ime, e-naslov, geslo, datum rojstva, lokacija.
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje uporabnika aplikacije: dnevna aktivnost in porabljene kalorije, količina spanca, teža, srčni utrip.

5.1.4 Noom: Health & Weight

- Razvijalec: Noom Inc.
- Paket: com.wsl.noom
- Opis iz trgovine Google Play: Noom je aplikacija za izgubo teže. Njen pristop temelji na psihologiji. Na podlagi misli in sprožilcev zgradi načrt, ki uporabiku omogoča hitrejšo pridobitev zdravih navad.

- Čas statične analize: 5 minut 33 sekund
- Čas dinamične analize: 19 minut 35 sekund

Nevarne pravice

ANDROID.PERMISSION.ACCESS_FINE_LOCATION
ANDROID.PERMISSION.ACCESS_COARSE_LOCATION
ANDROID.PERMISSION.USE_CREDENTIALS
ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.READ_EXTERNAL_STORAGE
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	5	83
Storitev	3	17
Ponudnik vsebin	0	2
Sprejemnik namenov	23	27

Odkrite nevarnosti v izvorni kodi

Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v dnevniške zapise
Vprogramirane občutljive informacije
Uporaba šibke zgoščevalne funkcije MD5
Zapisovanje podatkov na zunanji pomnilnik
Uporaba šibke zgoščevalne funkcije SHA-1
Slab generator naključnih števil
Zapisovanje informacij v začasno datoteko

Dinamična analiza

- Uhajanje informacij: Zaznali smo uhajanje številke IMEI. Na to smo bili opozorjeni v politiki zasebnosti.
- Analiza internetnega prometa: Pri analizi internetnega prometa smo ugotovili, da aplikacija za komunikacijo uporablja protokol TLS, pri statični analizi pa ni bilo najdenih nobenih nepravilnosti pri implementaciji protokola TLS.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija vsebuje politiko zasebnosti, s katero se moramo strinjati, preden ustvarimo uporabniški račun. V politiki zasebnosti je jasno navedeno, kateri podatki se zbirajo, v kakšne namene se uporabljajo, uporabniku navedejo možnost izbrisa podatkov ter navedejo kontakt, kamor se uporabnik obrne za spremembo podatkov. Prav tako je navedeno, da se podatki, kot sta lokacija in identifikatorji naprave, pošiljajo tretjim osebam za marketinške namene.

- Zbrani osebni podatki: e-naslov, geslo, spol vzdevek, datum rojstva, višina, lokacija, fotografija, identifikatorji naprave.
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje uporabnika: fizična aktivnost, poraba kalorij, izguba teže, srčni utrip in krvni tlak.

5.1.5 Pregnancy Week By Week

- Razvijalec: Amila
- Paket: com.easymobs.pregnancy

- Opis iz trgovine Google Play: Pregnancy Week By Week je brezplačna aplikacija za nosečnice, ki omogoča sledenje nosečnosti, izračuna datum poroda, spremlja težo nosečnice, brce dojenčka in omogoča vnašanje in spremljanje nosečniških simptomov.
- Čas statične analize: 3 minute 3 sekunde
- Čas dinamične analize: 18 minut 51 sekund

Nevarne pravice

Brez odkritih nevarnih pravic.

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	3	8
Storitev	1	5
Ponudnik vsebin	1	2
Sprejemnik namenov	5	7

Odkrite nevarnosti v izvorni kodi

Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v dnevniške zapise
Zapisovanje podatkov na zunanji pomnilnik
Uporaba šibke zgoščevalne funkcije SHA-1
Vprogramirane občutljive informacije
Slab generator naključnih števil

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize nismo zaznali uhajanja informacij.

- Analiza omrežnega prometa: Pri analizi internetnega prometa smo ugotovili, da aplikacija za komunikacijo uporablja protokol TLS, pri statični analizi pa ni bilo najdenih nobenih nepravilnosti pri implementaciji protokola TLS.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija vsebuje politiko zasebnosti, vendar ta ni ustrezna. Ne vsebuje informacije o tem, kdo zbira podatke, katere podatke in v kakšne namene jih zbira. Navedeno je, da se uporabnik strinja s politiko zasebnosti, če uporablja aplikacijo, kar je napačno. Uporabnik mora izrecno podati soglasje in se strinjati s politiko zasebnosti. Navedeno je, da aplikacija pošilja informacije o telefonu in lokacijo uporabnika tretjim osebam za marketinške namene.

- Zbrani osebni podatki: datum zadnje menstruacije, predviden datum rojstva, lokacija.
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje uporabnika: teža nosečnice, brce otroka, nosečniški simptomi.

5.1.6 Health Manager

- Razvijalec: Digit Groove
- Paket: com.androidapps.healthmanager
- Opis iz trgovine Google Play: Aplikacija omogoča vodenje zdravega načina življenja. Spremlja dnevne aktivnosti, kot so hoja, tek, vnos kalorij in količino popite vode.
- Čas statične analize: 2 minuti 47 sekund
- Čas dinamične analize: 12 minut 31 sekund

Nevarne pravice

ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.READ_EXTERNAL_STORAGE
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	0	76
Sprejemnik namenov	8	8

Odkrite nevarnosti v izvorni kodi

Slab generator naključnih števil
Zapisovanje podatkov na zunanji pomnilnik
Zapisovanje informacij v dnevniške zapise
Vprogramirane občutljive informacije
Uporaba šibke zgoščevalne funkcije MD5
Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v začasno datoteko
Uporaba načina šifriranja ECB

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize nismo zaznali uhajanja informacij.
- Analiza omrežnega prometa: Pri analizi internetnega prometa smo ugotovili, da aplikacija za komunikacijo uporablja protokol TLS, pri statični analizi pa ni bilo najdenih nobenih nepravilnosti pri implementaciji protokola TLS.

- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

V aplikaciji nismo našli politike zasebnosti, kar ni skladno z novo uredbo.

- Zbrani osebni podatki: ime, e-naslov, geslo, datum rojstva.
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje: teža, višina, obseg pasu, dnevni vnos kalorij, dnevni vnos popite vode.

5.1.7 iCare Health Monitor

- Razvijalec: BigBig Studio
- Paket: com.androidapps.healthmanager
- Opis iz trgovine Google Play: Aplikacija omogoča merjenje srčnega utripa, vida in sluha brez dodatnih naprav.
- Čas statične analize: 3 minute 16 sekund
- Čas dinamične analize: 14 minut 59 sekund

Nevarne pravice

ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.RECORD_AUDIO
ANDROID.PERMISSION.CHANGE_WIFI_STATE
ANDROID.PERMISSION.DISABLE_KEYGUARD
ANDROID.PERMISSION.GET_TASKS

Nezaščitene komponente

Komponenta	Število nezaščitenih	Število vseh
Aktivnost	9	119
Storitev	0	6
Sprejemnik namenov	2	5

Odkrite nevarnosti v izvorni kodi

Zapisovanje informacij v dnevniške zapise
Uporaba šibke zgoščevalne funkcije Java Hash Code
Slab generator naključnih števil
Vprogramirane občutljive informacije
Nevarna implementacija protokola TLS
Uporaba šibke zgoščevalne funkcije MD5
Zapisovanje podatkov na zunanji pomnilnik
Zapisovanje informacij v začasno datoteko
Uporaba šibke zgoščevalne funkcije SHA-1

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize nismo zaznali uhajanja informacij.

- Analiza omrežnega prometa: Aplikacija za komunikacijo uporablja protokol TLS, vendar smo pri statični analizi zaznali, da pri implementaciji protokola TLS zaupa tudi samopodpisanim digitalnim potrdilom. To predstavlja varnostno ranljivost za napad MITM.

- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

V aplikaciji nismo našli politike zasebnosti, kar ni skladno z novo uredbo.

- Zbrani osebni podatki: e-naslov, geslo.

- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje uporabnika: srčni utrip, krvni tlak, krvni sladkor, količina kisika v krvi, telesna temperatura, višina, teža, obseg pasu. Aplikacija vsebuje tudi teste za spremljanje vida, sluha, kapaciteto pljuč in psihološke teste za določanje depresije in avtizma.

5.1.8 Lefun Health

- Razvijalec: TENG JINDA

- Paket: com.androidapps.healthmanager

- Opis iz trgovine Google Play: Aplikacija, ki s pomočjo pametne ure zbira dnevno količino prehojene razdalje, število korakov, višino srčnega utripa, kakovost spanca, prav tako pa omogoča sledenju vnosa kalorij.

- Čas statične analize: 4 minute 19 sekund

- Čas dinamične analize: 11 minut 55 sekund

Nevarne pravice

ANDROID.PERMISSION.ACCESS_FINE_LOCATION
ANDROID.PERMISSION.ACCESS_COARSE_LOCATION
ANDROID.PERMISSION.USE_CREDENTIALS
ANDROID.PERMISSION.CAMERA
ANDROID.PERMISSION.CHANGE_WIFI_STATE
ANDROID.PERMISSION.READ_EXTERNAL_STORAGE
ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE
ANDROID.PERMISSION.READ_CONTACTS
ANDROID.PERMISSION.READ_SMS
ANDROID.PERMISSION.SEND_SMS
ANDROID.PERMISSION.RECEIVE_SMS
ANDROID.PERMISSION.CALL_PHONE
ANDROID.PERMISSION.READ_CALENDAR
ANDROID.PERMISSION.GET_TASKS
ANDROID.PERMISSION.READ_PHONE_STATE
ANDROID.PERMISSION.RECORD_AUDIO

Nezaščitene komponente

Komponenta	**Število nezaščitenih**	**Število vseh**
Aktivnost	2	37
Storitev	1	8
Sprejemnik namenov	0	1

Odkrite nevarnosti v izvorni kodi

Slab generator naključnih števil
Zapisovanje informacij v dnevniške zapise
Spletni pogled Android sprejme vsa digitalna potrdila
Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v začasno datoteko
Uporaba šibke zgoščevalne funkcije MD5
Vprogramirane občutljive informacije
Zapisovanje podatkov na zunanji pomnilnik
Uporaba načina šifriranja ECB
Uporaba šibke zgoščevalne funkcije SHA-1

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize nismo zaznali uhajanja informacij.
- Analiza omrežnega prometa: Aplikacija za komunikacijo uporablja protokol TLS, vendar smo pri statični analizi zaznali, da pri implementaciji protokola TLS zaupa tudi samopodpisanim digitalnim potrdilom. To predstavlja varnostno ranljivost za napad MITM.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

V aplikaciji nismo našli politike zasebnosti.

- Zbrani osebni podatki: ime, priimek, spol, višina, datum rojstva
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi teh lahko določimo zdravstveno ali fizično stanje: srčni utrip, količina spanca, prehojena razdalja, število porabljenih kalorij.

5.1.9 My Health Tracker

- Razvijalec: Walter Gross
- Paket: com.androidapps.healthmanager
- Opis iz trgovine Google Play: Aplikacija za sledenje telesne mase in krvnega tlaka ter sladkorja. Omogoča enostavno uporabo, prikaz seznamov in grafov zgodovine zapiskov. Lahko shranjuje vrednosti desetih uporabnikov.
- Čas statične analize: 18 sekund
- Čas dinamične analize: 11 minut 1 sekunda

Nevarne pravice

ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE

Nezaščitene komponente

Komponenta	Število nezaščitenih	Število vseh
Aktivnost	0	2

Odkrite nevarnosti v izvorni kodi

Vprogramirane občutljive informacije
Zapisovanje podatkov na zunanji pomnilnik

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize smo zaznali uhajanje številke IMEI.
- Analiza omrežnega prometa: Aplikacija ne komunicira z zalednim sistemom. Vse podatke shranjuje lokalno.

- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

Aplikacija ne vsebuje politike zasebnosti. Vendar kljub temu, da vse podatke shranjuje lokalno, to je na napravi, mora aplikacija vsebovati politiko zasebnosti, kjer je jasno navedeno, da ne zbira in pošilja nobenih podatkov.

- Zbrani osebni podatki: e-naslov, geslo.
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi katerih lahko določimo zdravstveno ali fizično stanje: teža, krvni tlak, krvni sladkor.

5.1.10 YAZIO Calorie Counter, Nutrition Diary & Diet Plan

- Razvijalec: YAZIO
- Paket: com.yazio.android
- Google Play opis: Aplikacija za spremljanje vnosa kalorij in pripomoček za izgubljanje teže. Omogoča nastavljanje ciljne teže, vsebuje različne zdrave jedilnike in programe za izgubo teže.
- Čas statične analize: 4 minut 20 sekund
- Čas dinamične analize: 12 minut 42 sekund

Nevarne pravice

ANDROID.PERMISSION.WRITE_EXTERNAL_STORAGE

Nezaščitene komponente

Komponenta	Število nezaščitenih	Število vseh
Aktivnost	12	156
Storitev	6	18
Ponudnik vsebin	0	4
Sprejemnik namenov	25	29

Odkrite nevarnosti v izvorni kodi

Uporaba šibke zgoščevalne funkcije Java Hash Code
Zapisovanje informacij v dnevniške zapise
Slab generator naključnih števil
Zapisovanje podatkov na zunanji pomnilnik
Uporaba šibke zgoščevalne funkcije SHA-1
Vprogramirane občutljive informacije
Zapisovanje informacij v začasno datoteko

Dinamična analiza

- Uhajanje informacij: Med izvajanjem dinamične analize nismo zaznali uhajanja informacij.
- Analiza omrežnega prometa: Pri analizi omrežnega prometa smo ugotovili, da aplikacija uporablja protokol TLS, pri statični analizi pa nismo zaznali napak pri implementaciji šifriranja.
- Šifriranje podatkovne baze: Ugotovili smo, da podatkovna baza ni šifrirana.

Skladnost z GDPR

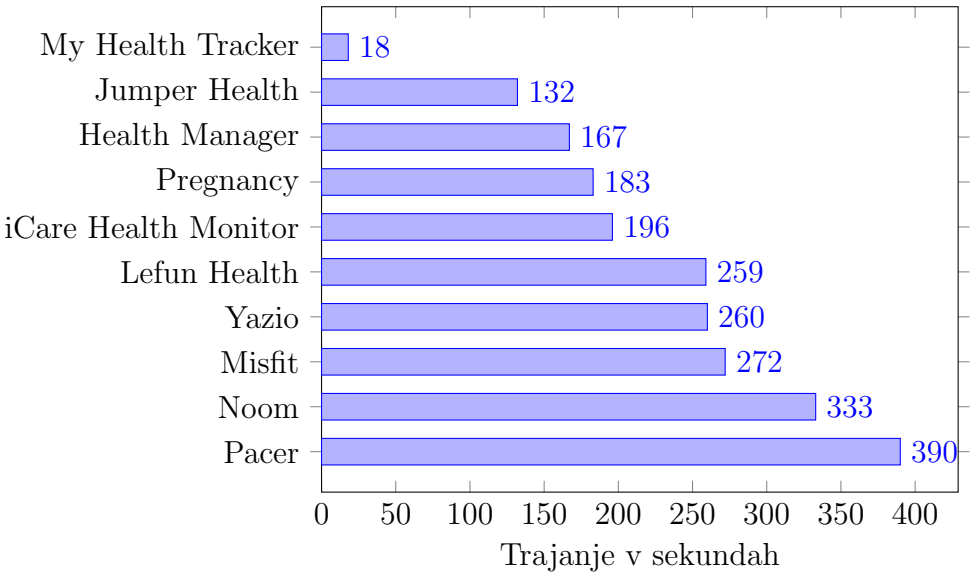
V aplikaciji nismo našli politike zasebnosti, pri registraciji smo se morali strinjati samo s pogoji uporabe.

- Zbrani osebni podatki: spol, datum rojstva, višina.

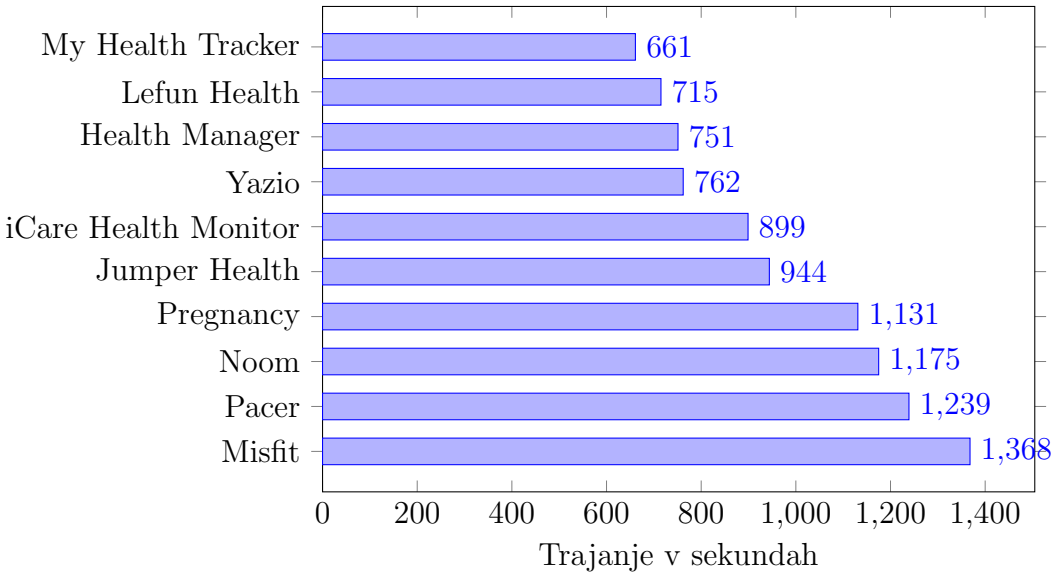
- Zbrani občutljivi podatki, ki se zbirajo dlje časa, na podlagi katerih lahko določimo zdravstveno ali fizično stanje: dnevni vnos kalorij, dnevna aktivnost, teža, višina sladkorja v krvi.

5.2 Ugotovitve

Na sliki 5.1 so prikazana trajanja statičnih analiz, kjer je najkrajši čas statične analize znašal 18 sekund, najdaljši čas 390 sekund, povprečni čas pa je znašal 221 sekund s standardnim odklonom 106 sekund. Na sliki 5.2 so prikazana trajanja dinamičnih analiz, kjer je najkrajši čas dinamične analize znašal 661 sekund, najdaljši čas 1368 sekund, povprečni čas pa je znašal 965 sekund s standardnim odklonom 248 sekund. V čas dinamične analize je zajeto tudi ročno pregledovanje aplikacije in ročno analiziranje politike zasebnosti.



Slika 5.1: Trajanje statičnih analiz

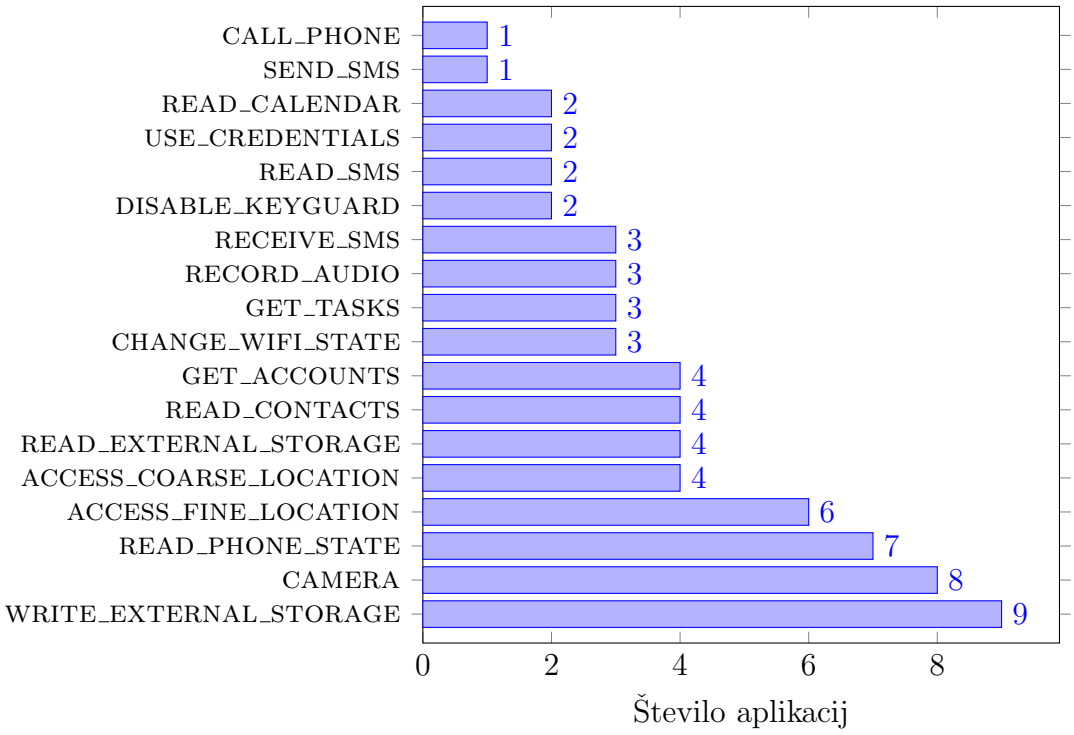


Slika 5.2: Trajanje dinamičnih analiz

Pri analizi nevarnih pravic se največkrat pojavi pravica WRITE_EXTERNAL_STORAGE, ki omogoča pisanje na zunanji pomnilnik. S stališča zasebnosti aplikacija ne sme zapisovati na zunanji pomnilnik, saj imajo vse druge nameščene aplikacije dostop do zunanjega pomnilnika. Zunanji pomnilnik je lahko zašifriran, kar zaščiti podatke pred zunanjimi napadalci, ki imajo fizični dostop do kartice SD, druge nameščene aplikacije pa imajo še vedno omogočen dostop.

Kot druga najbolj pogosta nevarna pravica se pojavi pravica za dostop do kamere, saj se uporablja za merjenje srčnega utripa. Prav tako ne predstavlja nevarnosti pravica za branje lokacije, saj se uporablja za merjenje prehojene ali pretečene razdalje. Pravici za dostop do kamere in lokacije se uporabljata zaradi funkcionalnosti, vendar še vedno predstavljata nevarnost zasebnosti. Večjo nevarnost predstavljata pravici READ_CONTACTS in GET_ACCOUNTS, ki sta bili najdeni pri štirih aplikacijah, pravici GET_TASKS in RECEIVE_SMS, ki sta bili najdeni pri treh aplikacijah, READ_CALENDAR, USE_CREDENTIALS, READ_SMS so bile najdene pri dveh aplikacijah ter pravici CALL_PHONE in SEND_SMS, ki sta bili najdeni pri eni aplikaciji. Te nevarne pravice ne spa-

dajo v kontekst zdravstvenih aplikacij in se lahko uporabljajo za dostop do občutljivih informacij, kot so stiki, koledar, kratka sporočila in informacije o drugih aplikacijah. Dve aplikaciji lahko prav tako onemogočita zaklepanje telefona, kar ne bi smeli. Na sliki 5.3 so prikazane najdene nevarne pravice in njihovo število pojavitev v aplikacijah.



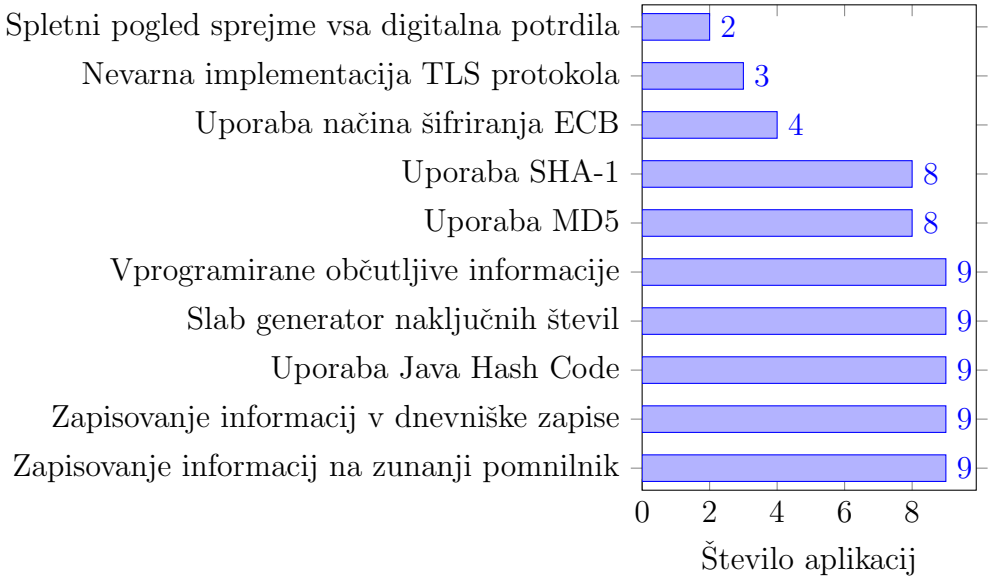
Slika 5.3: Najdene nevarne pravice

Pri analizi zaščite komponent smo ugotovili, da devet aplikacij ne implementira ustrezne zaščite komponent. To lahko predstavlja problem, če komponenta, kot je storitev ali aktivnost, dostopa do občutljivih informacij. Potem lahko zlonamerna aplikacija prevzame storitev in aktivnost in tako pridobi dostop tudi do občutljivih informacij.

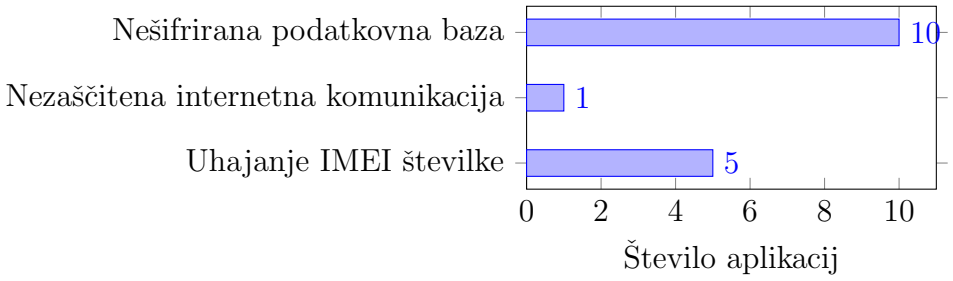
Pri analizi izvorne kode so prevladovale šibke zgoščevalne funkcije, zapisovanje v dnevniške zapise in pisanje na zunanji pomnilnik. Pri treh aplikacijah smo zaznali neustrezno implementacijo protokola TLS, pri treh aplikacijah

pa sprejemanje samopodpisanih digitalnih potrdil v spletnih pogledih Android. Slika 5.4 prikazuje najdene ranljivosti in njihovo število pojavitev v aplikacijah pri statični analizi.

Prav tako smo ugotovili, da ena aplikacija pošilja uporabniško ime in geslo kar v golem besedilu v zahtevku POST. Pet aplikacij pošilja tretjim osebam tudi identifikator naprav IMEI, vendar so nas na to opozorile le tri aplikacije. Ugotovili smo tudi, da nobena od testiranih aplikacij ni imela šifrirane baze. Na sliki 5.5 so prikazana števila najdenih ranljivosti in uhajanja podatkov pri dinamični analizi.



Slika 5.4: Rezultati statične analize



Slika 5.5: Rezultati dinamične analize

Z rezultati analiz smo izbrane aplikacije ovrednotili z vnaprej določenimi kazalniki varovanja zasebnosti in s kazalniki skladnosti z GDPR. V tabeli 5.1 je prikazano ovrednotenje aplikacij, kjer lahko vidimo, da nobena aplikacija ni zadostila vsem kazalnikom.

Nobena od aplikacij ni zadostila kazalnikoma VZ3 in VZ4, kjer smo preverjali varno shranjevanje podatkov in zapisovanje podatkov v dnevniške in začasne datoteke. Kazalnik VZ1 zaščite komponent ima potrjena samo ena aplikacija. Prav tako je pri kazalniku VZ2, ki je potrjen prav tako samo pri eni aplikaciji. Pri preverjanju kazalnika VZ5 lahko vidimo, da pet aplikacij pravilno implementira varno omrežno komunikacijo, pri preverjanju kazalnika VZ6 pa vidimo, da šest aplikacij uporablja zgoščevalne funkcije s trki, slabe generatorje naključnih števil ali pa način šifriranja ECB. Z dinamično analizo smo pri polovici aplikacij potrdili kazalnik VZ7. Pri petih aplikacijah namreč uhajajo občutljivi podatki (v našem primeru številka IMEI), vendar smo bili na to opozorjeni v politiki zasebnosti le pri treh aplikacijah.

Politika zasebnosti je popolnoma skladna z GDPR-jem samo pri treh aplikacijah (potrjeni kazalniki GDPR1-GDPR5), vendar je zadnji kazalnik GDPR6 ovržen pri vseh analiziranih aplikacijah, saj nobena aplikacija nima potrjenih vseh kazalnikov varovanja zasebnosti. Pet aplikacij ni skladnih z uredbo zaradi odsotnosti politike zasebnosti, pri dveh aplikacijah pa politika zasebnosti ni vsebovala vseh informacij, ki jih zahteva uredba.

Če za skladnost z novo uredbo upoštevamo vse kazalnike, med njimi tudi kazalnik, da morajo imeti aplikacije implementirano ustrezno varnost in zasebnost (angl. *Privacy and security by design*), potem nobena aplikacija iz našega niza ni skladna z uredbo.

Kljub nekaj pomanjkljivostim lahko vidimo, da so najboljše rezultate dosegle aplikacije Pacer, Misfit in Noom, najslabša izmed vseh je bila aplikacija Jumper Health, sledili pa sta ji aplikaciji iCare Health Monitor in Lefun Health.

	VZ1	VZ2	VZ3	VZ4	VZ5	VZ6	VZ7	GDPR1	GDPR2	GDPR3	GDPR4	GDPR5	GDPR6
Jumper Health	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘
Pacer	✘	✘	✘	✘	✔	✘	✘*	✔	✔	✔	✔	✔	✘
Misfit	✘	✘	✘	✘	✘	✔	✘*	✔	✔	✔	✔	✔	✘
Noom: Health & Weight	✘	✘	✘	✘	✔	✔	✘*	✔	✔	✔	✔	✔	✘
Pregnancy Week By Week	✘	✔	✘	✘	✔	✘	✔	✘	✘	✘	✘	✔	✘
Health Manager	✘	✘	✘	✘	✔	✘	✔	✦	✦	✦	✦	✦	✘
iCare Health Monitor	✘	✘	✘	✘	✘	✘	✔	✦	✦	✦	✦	✦	✘
Lefun Health	✘	✘	✘	✘	✘	✘	✔	✦	✦	✦	✦	✦	✘
My Health Tracker	✔	✘	✘	✘	✧	✔	✔	✦	✦	✦	✦	✦	✘
Yazio Calorie Counter	✘	✘	✘	✘	✔	✔	✘	✦	✦	✦	✦	✦	✘
Število potrjenih	1/10	1/10	0/10	0/10	5/9	4/10	5/10	3/5	3/5	3/5	3/5	4/5	0/10

Tabela 5.1: Rezultati ovrednotenja aplikacij s kazalniki.

Legenda:

✔- potrjen kazalnik

✘- ovržen kazalnik

✦- politika zasebnosti v aplikaciji ni prisotna

✧- aplikacije ne komunicira z zalednim sistemom

* - pošiljanje številke IMEI navedeno v politiki zasebnosti

5.2.1 Omejitve

Pri dinamični analizi je bila ena od omejitev nezmožnost uporabe orodja [35], ki samodejno izvaja uporabniške akcije, kot so kliki, dotiki in geste. Z uporabo orodja [35] in emulatorja, bi lahko dinamična analiza potekala samodejno in bi lahko analizirali večje število aplikacij. V našem primeru smo tako zaradi omejitve morali ročno ustvarjati uporabniške račune in prijave v aplikacijah, kar je onemogočilo samodejno analizo. Pri dinamični analizi se nismo odločili za uporabo emulatorja, saj ta ne podpira pravilne emulacije številke IMEI (vedno vrne 00000), naslova MAC, lokacije GPS, kamere in senzorjev naprave. Zaradi te omejitve smo se odločili za uporabo telefona Nexus 4.

Pri dinamični analizi smo uporabili razširitev `TaintDroid`, ki je bila izvorno razvita za sisteme Android verzije 2.1-4.3 in uporabljajo virtualni stroj Dalvik. Glavna funkcionalnost razširitve `TaintDroid` je uporaba notranjega pomnilnika virtualnega stroja Dalvik za shranjevanje spremenljivk z občutljivimi vhodi in shranjevanje toka podatkov. Zaradi zmogljivosti je Google odstranil virtualni stroj Dalvik in ga nadomestil s sistemom ART, ki uporablja prevajanje AOT (angl. *ahead of time*). Zato lahko razširitev `TaintDroid` uporabimo samo do Android verzije 4.3 in smo posledično omejeni z izbiro aplikacij.

Poglavje 6

Zaključek

V našem delu smo z razvitimi kazalniki varovanja zasebnosti in skladnosti z novo uredbo (GDPR) ovrednotili deset izbranih zdravstvenih aplikacij Android iz trgovine Google Play. Za analizo aplikacij smo razvili arhitekturo za iskanje ranljivosti in zaznavanje uhajanja podatkov iz aplikacij. Našo arhitekturo smo zasnovali v obliki spletne aplikacije, ki je zgrajena modularno in je preprosto nadgradljiva. Vsebuje modul za statično analizo, dinamično analizo ter knjižnico za komunikacijo z napravami Android preko `adb`. Prav tako vsebuje datoteko nastavitev za analizo, preko katere lahko dodajamo ali spreminjamo pravila in nastavitve analiz. Spletna aplikacija je zapakirana v vsebnik Docker in jo je tako možno poganjati v lokalnem okolju in tudi v oblačni infrastrukturi.

Z našim ovrednotenjem varstva podatkov pri mobilnih zdravstvenih aplikacijah smo dobili okvirno sliko trenutnega stanja varovanja osebnih podatkov in skladnosti z novo uredbo. V analiziranih aplikacijah so se pokazale številne večje in manjše pomanjkljivosti, ki ogrožajo zasebnost uporabnikov mobilnih zdravstvenih aplikacij. Ugotovili smo, da velik del ocenjenih aplikacij ogroža zasebnost in varnost uporabnika zaradi neustreznega shranjevanja podatkov, odsotnosti pravic pri javnih komponentah, uporabe slabih zgoščevalnih funkcij, odsotnosti šifriranja pri internetni komunikaciji in zapisovanja podatkov v dnevniške zapise ter odsotnosti politike o zasebnosti in varstvu podat-

kov. Razvijalci in podjetja bi morali pri snovanju aplikacij nameniti več časa implementaciji varnostnih mehanizmov in oblikovanju ustrezne politike zasebnosti.

Največ potencialnih groženj zasebnosti in neskladnosti z novo uredbo smo našli ravno pri aplikacijah azijskih razvijalcev, kar pa je morda zaradi majhnega vzorca analiziranih aplikacij čisto naključje.

Razvito spletno aplikacijo bi lahko namestili na oblačno infrastrukturo in tretjim osebam omogočili izvajanje analiz in pregledovanje arhiva že opravljenih analiz. Prav tako pa naša arhitektura z nekaj nadgradnje, kot je na primer podpora za aplikacije iOS ter samodejno preverjanje skladnosti z novo uredbo, predstavlja odlično zasnovo za ekosistem varnih mobilnih zdravstvenih aplikacij. Ekosistem bi lahko prav tako ponujal certificiranje aplikacij na področju mobilnega zdravstva, napotke za razvijanje varnih aplikacij in varnih zalednih sistemov, vzdrževanje varne oblačne infrastrukture ter samodejno generiranje skladnih politik zasebnosti.

Literatura

[1] M. Kay, J. Santos in M. Takane, *mHealth: New horizons for health through mobile technologies*, World Health Organization, 64(7) str. 66-71, WHO Geneva, 2011.

[2] P. Krebs in D. T. Duncan, *Health app use among US mobile phone owners: a national survey*, JMIR mHealth and uHealth, 3(4), JMIR Publications Inc., 2015.

[3] R. Adhikari, D. Richards in K. Scott, *Security and privacy issues related to the use of mobile health apps*, v 25th Australasian Conference on Information Systems, ACIS, 2014.

[4] G. Štravs, *Grožnje zasebnosti uporabnika pametne televizije*, diplomsko delo, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, 2015.

[5] Uradni list Republike Slovenije, *Ustava Republike Slovenije*, `https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1991-01-1409?sop=1991-01-1409`. [Dostopano 1. 9. 2018].

[6] Uradni list Republike Slovenije, *Zakon o varstvu osebnih podatkov*, `https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/82668`. [Dostopano 1. 9. 2018].

[7] Uradni list Evropske unije, *Splošna uredba o varstvu podatkov*, `https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex%3A32016R0679`. [Dostopano 1. 9. 2018].

[8] OWASP, *Mobile Security Project*, `https://www.owasp.org/index.php/OWASP_Mobile_Security_Project`. [Dostopano 1. 9. 2018].

[9] D. He, M. Naveed, C. Gunther in K. Nahrstedt, *Security concerns in Android mHealth apps*, v AMIA Annual Symposium Proceedings 2014, str. 645-654, American Medical Informatics Association, 2014.

[10] F. Zubaydi, A. Saleh, F. Aloulin A. Sagahyroon, *Security of mobile health (mHealth) systems*, v IEEE 15th International Conference on Bioinformatics and Bioengineering 2015, str. 1-5, IEEE, 2015.

[11] K. Knorr, D. Aspinall in M. Wolters, *On the privacy, security and safety of blood pressure and diabetes apps*, v IFIP International Information Security Conference, str. 571-584, Springer, 2015.

[12] T. Dehling, F. Gao, S. Schneider in A. Sunyaev, *Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android*, JMIR mHealth and uHealth, 3(1), JMIR Publications Inc., 2015.

[13] A. Sunyaev, T. Dehling P. L. Taylor in K. D. Mandl, *Availability and quality of mobile health app privacy policies*, Journal of the American Medical Informatics Association, 22(1) str. 28-33, Oxford University Press, 2014.

[14] M. Bachiri, A. Idri, J. L. Fernández-Alemán in A. Toval, *Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring*, Journal of Medical Systems, 42(8) str. 144, Springer, 2018.

[15] B. Martínez-Pérez, I. De La Torre-Díez in M. López-Coronado, *Privacy and security in mobile health apps: a review and recommendations*, Journal of Medical Systems, 39(1) str. 181, Springer, 2015.

[16] European Commission, *Privacy Code of Conduct on mobile health apps*, `https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps`. [Dostopano 1. 9. 2018].

[17] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B. Chun, L. P. Cox, J. Jung, P. McDaniel in A. N. Sheth, *TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones*, ACM Transactions on Computer Systems (TOCS), 57(3) str. 99-106, ACM, 2014.

[18] J. Six, *Application Security for the Android Platform: Processes, Permissions, and Other Safeguards*, O'Reilly Media, Inc., 2011.

[19] OWASP, *Mobile Security Testing Guide*, `https://github.com/OWASP/owasp-mstg`. [Dostopano 1. 9. 2018].

[20] OWASP, *Mobile Top 10 2016*, `https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10`. [Dostopano 1. 9. 2018].

[21] D. Kotz, C. Gunter, S. Kumar in J. P. Weiner, *Privacy and security in mobile health: a research agenda*, Computer, 49(6) str. 22-30, IEEE, 2016.

[22] L. Myers, *Stolen Medical Data Is Now A Hot Commodity*, `https://www.darkreading.com/cloud/stolen-medical-data-is-now-a-hot-commodity--/a/d-id/1316598`. [Dostopano 1. 9. 2018].

[23] L. Storbrauck, *Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners*, La Salle University, 2015.

[24] Grand View Research Inc., *mHealth Apps Market Size Worth $111.8 Billion By 2025 — CAGR: 44.2%*, `https://www.grandviewresearch.com/press-release/global-mhealth-app-market`. [Dostopano 1. 9. 2018].

[25] M. Grace, Y. Zhou, Z. Wang in X. Jiang, *Detecting capability leaks in android-based smartphones*, tehnično poročilo, North Carolina State University, 2011.

[26] D. Sbîrlea, M. G. Burke, S. Guarnieri M. Pistoia in V. Sarkar, *Automatic detection of inter-application permission leaks in Android applications*, IBM Journal of Research and Development, 57(6) str. 10-12, IBM, 2013.

[27] A. Chatzikonstantinou, C. Ntantogian, G. Karopoulos in C. Xenakis, *Evaluation of cryptography usage in android applications*, v Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), str. 83-90, ICST, 2016.

[28] Carnegie Mellon University, Software Engineering Institute, *Android Secure Coding Standard*, `https://wiki.sei.cmu.edu/confluence/display/android/Android+Secure+Coding+Standard`. [Dostopano 1. 9. 2018].

[29] Y. Wang, J. Zheng, C. Sun in S. Mukkamala, *Quantitative security risk assessment of android permissions and applications*, v IFIP Annual Conference on Data and Applications Security and Privacy, str. 226-241, Springer, 2013.

[30] K. Raud, *Data protection in mHealth*, doktorska disertacija, Tartu Ülikool, 2016.

[31] OpenSecurity, *Mobile Security Framework (MobSF)*, `https://github.com/MobSF/Mobile-Security-Framework-MobSF`. [Dostopano 1. 9. 2018].

[32] P. Asrodia in H. Patel, *Analysis of various packet sniffing tools for network monitoring and analysis*, International Journal of Electrical, Electronics and Computer Engineering, 1(1) str. 55-58, IJEECE, 2012.

[33] D. Merkel, *Docker: lightweight linux containers for consistent development and deployment*, Linux Journal, 2014(239) str. 2, Belltown Media, 2014.

[34] T. Gunasundari in K. Elangovan, *A Comparative Survey on Symmetric Key Encryption Algorithms*, International Journal of Computer Science and Mobile Applications, 2(2) str. 78-83, IJCSMA, 2014.

[35] Google, *UI/Application Exerciser Monkey*, `https://developer.android.com/studio/test/monkey`. [Dostopano 1. 9. 2018].