SIGURNOST MOBILNIH UREĐAJA

Čičak, Dominik

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Dominik Čičak

SIGURNOST MOBILNIH UREĐAJA

ZAVRŠNI RAD

Karlovac, 2021

Karlovac University of Applied Sciences
Safety and Protection Department
Professional graduate study of Safety and Protection

Dominik Čičak

SAFETY OF MOBILE DEVICES

FINAL PAPER

Karlovac, 2021

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Dominik Čičak

SIGURNOST MOBILNIH UREĐAJA

ZAVRŠNI RAD

Mentor:

Dr.Sc.Nikola Trbojević

Karlovac, 2021

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni/specijalistički studij:..Specijalistički stručni studij sigurnost I zaštita.....

Usmjerenje:.....Zaštita na radu .....Karlovac, 03.03.2021.....

ZADATAK ZAVRŠNOG RADA

Student:...Dominik Čičak.....Matični Broj:0420418034.....

Naslov:.....Sigurnost mobilnih uređaja.....

Opis zadatka:

Korištenje istraživačkih metoda u svrhu izrade diplomskog rada

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
.....01/2021.....	03/2021..	03/2021

Mentor:

Dr.Sc.Nikola Trbojević

Predsjednik Ispitnog povjerenstva:

Dr.Sc.Z.Matusinović

PREDGOVOR

Ovaj rad nastao je kao produkt interesa za informacijske tehnologije, točnije mobilne uređaje, te iz znatiželje za saznavanjem više o tome. Tijekom pisanja rada naišao sam na mnoštvo starijih i novijih informacije, stoga ih je sve trebalo provjeravati više puta što mi je predstavljalo izazov po pitanju točnosti informacija.

Ovim putem zahvaljujem svom mentoru na podršci te pomoći pri izradi rada, te svojoj obitelji i prijateljima na podršci tijekom studiranja.

Sažetak

Informacijski sustavi danas predstavljaju ključan problem sigurnosti općenito. Podaci su odavno prebačeni u kompjuterski oblik, stoga je njihova zloupotreba postala dostupnija i jednostavnija, a očuvanje sigurnosti postalo je glavni izazov. Obzirom da danas većina ljudi pretražuje Internet putem mobitela, te veliki dio dana koristi isključivo pametni telefon, svaka njegova komponenta mora biti osigurana od napada kako bi cjelokupni sustav bio zaštićen. Komponente mobitela u današnje su vrijeme brojnije nego nekad, a uz to operacijski sustavi i aplikacije predstavljaju značajnu prepreku sigurnosti. Ljudi postaju sve svjesniji ovoga problema, no još uvijek je potrebno poraditi na edukaciji i podizanju svijesti o ozbiljnosti problema sigurnosti informacija na mobilnim telefonima.

Ključne riječi: informacijski sustav, sigurnost identiteta, privatnost, zaštita podataka, pametni telefon

SADRŽAJ:

1.UVOD

Kroz povijest sasvim vrlo kompleksni i skupi uređaji, danas postaju dostupni svima, od onih slabije platežne moći, preko djece i starijih osoba. Mobilni telefoni posve su promijenili nekadašnje funkcioniranje društva te su se proširili tolikom brzinom da danas nema kućanstva u kojemu nije prisutan mobilni uređaj. Situacija se toliko promijenila, da je život danas praktički nezamisliv bez mobitela, te dostrajalošću jednog mobitela korisnik odmah kreće u potragu za drugim, a osobe slabije platežne moći uspijevaju si ga priuštiti stavljajući ga kao prioritet. Obzirom na količinu i dostupnost ovih uređaja, sve veće brojke predstavljaju i sve kompliciraniji zadatak zaštite mobilnih telefona.

1.1.Predmet i cilj rada

Predmet ovoga rada bio je „Sigurnost mobilnih uređaja“. U radu se nastoje pojasniti osnovni pojmovi vezani za sigurnost, podatke te mobilne tehnologije, vračajući se u povijest ovoga fenomena. Kroz rad se prikazuju glavni uzroci nesigurnosti mobilnih uređaja, te glavni rizici na koje treba obratiti pažnju, te se nastoji hijerarhijski doći do srži problema, kako bi se naposljetku pružilo određeno rješenje.

Cilj rada je pojasniti pojedinačne pojmove kroz svu dostupnu literaturu, te prikazati koliko današnji mobiteli zapravo jesu ili nisu sigurni, te koji aspekti predstavljaju rizike za njegov sustav, a koji su dijelovi zaštićeni od napada.

1.2.Izvori podataka i metode prikupljanja

Izvori podataka prikupljani su sa relevantnih stranica, a većinom iz knjiga, članaka i publikacija poznatih imena iz područja informatike i informacijskih tehnologija.

Metode korištene u izradi ovog rada su kompilacija na temelju proučavanja postojeće literature o temi rada, metoda analize i sinteze te metoda deskripcije.

1.3.Sadržaj i struktura rada

Struktura rada poredana je hijerarhijski od najopćenitijih pojmova i definicija, prema samoj srži onoga što je od njegovog primarnog interesa. Rad se sastoji od sedam poglavlja, zajedno sa uvodom i zaključkom, u kojima se potom tematika grana u podpoglavlja i podpodpoglavlja, ovisno o potrebi.

Prema tome rad je podijeljen na slijedeća poglavlja:

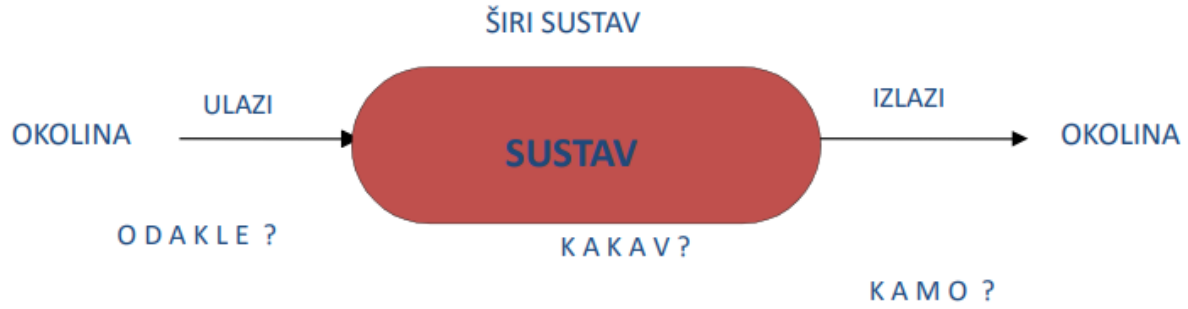
1. Uvod
2. Informacijski sustav
3. Mobilne komponente i njihova sigurnost
4. Mobilne platforme
5. Mobilne aplikacije
6. Metode zaštite
7. Zaključak

U drugome poglavlju koje govori o informacijskim sustavima govori općenito o informacijskim sustavima te njihovoj sigurnosti, te je prikazana važnost, čimbenici i komponente ovog sustava te su dane osnovne definicije i zakoni ovog sustava .

U slijedećem poglavlju prikazana je sigurnost mobitela na temelju svih ključnih mobilnih komponenti. Na isti način prikazani su u narednom poglavlju svi operacijski sustavi, te je prikazana sigurnost onih osnovnih i najviše korištenih danas. Isto tako je i u petome poglavlju koje govori o mobilnim aplikacijama, kroz povijest i sve njihove komponente prikazana njihova sigurnost, te je u šestom poglavlju predstavljeno nekoliko metoda zaštite uređaja. Naposljetku je u zadnjem poglavlju sukladno svemu dan određen zaključak.

2.INFORMACIJSKI SUSTAV

Kako bi se pojasnila sigurnost mobilnih uređaja potrebno je započeti od samog korijena te pojasniti pojam sustava, odnosno informacijskog sustava. Općenito govoreći sustav je „skup elemenata i podsustava koji su međusobno povezani i djeluju jedan na drugi element ili podsustav.“ [1] Sam se sustav pak nalazi u jednom širem sustavu čiji je ujedno dio te je sa njim u vezi. Međusobna djelovanja i veze među podsustavima zove se sučelje, a onaj dio koji nije obuhvaćen sustavom naziva se okolina (Slika 1.). [2]



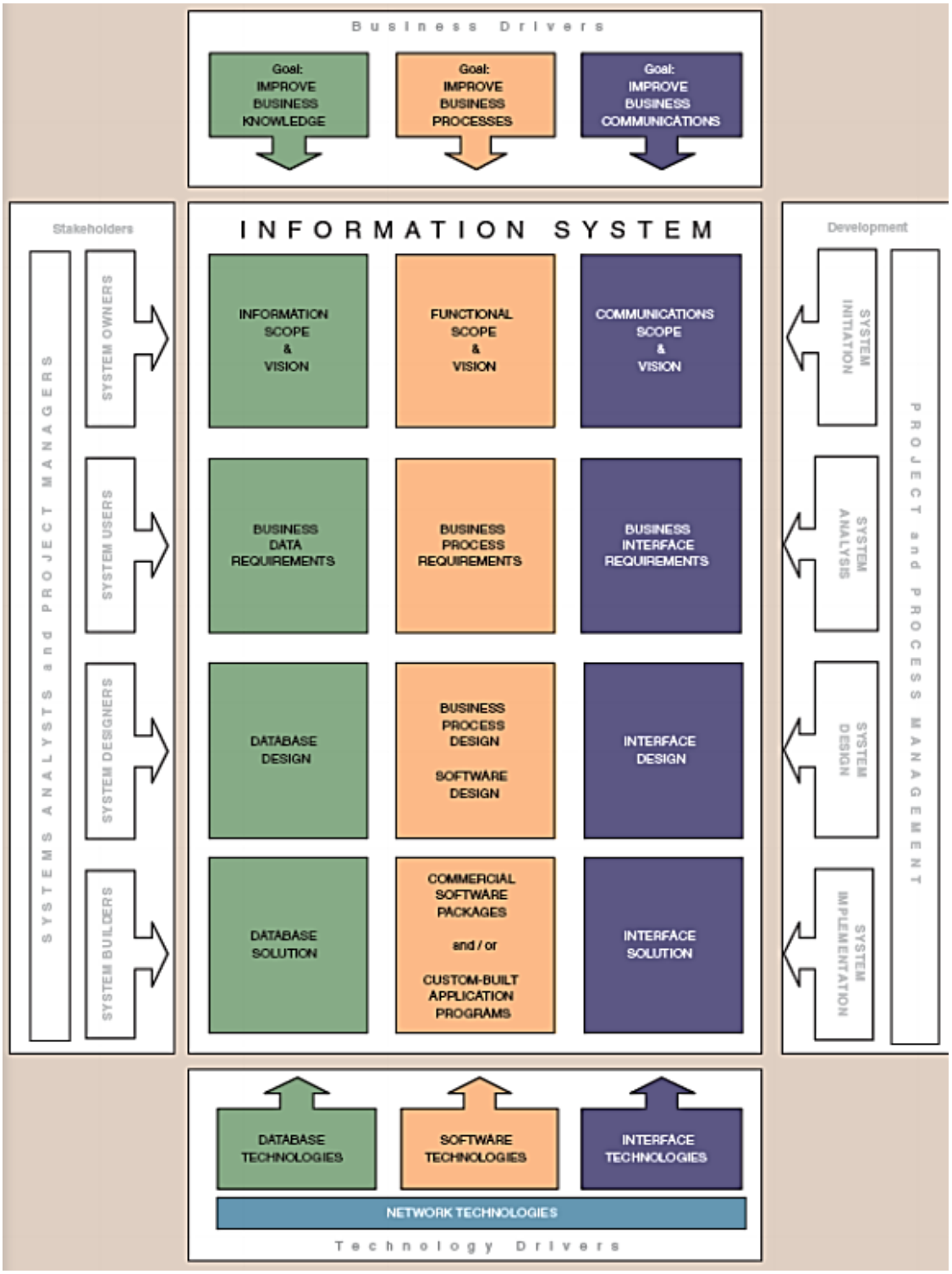
Slika 1.Komponente sustava [2]

Također definicija govori kako je sustav „skup elemenata, bilo prirodnih, organskih, tehničkih, apstraktnih ili misaonih koji su povezani u funkcionalnu cjelinu, kao primjerice sunčev sustav, probavni, energetski, koordinatni ili filozofijski sustav.“ Odnosno sustav je „ukupnost načela, pravila, propisa, postupaka kojima se uređuje neko područje kao primjerice školski, politički, ekonomski, prometni sustav ili nastoji ostvariti neki cilj kao što je to slučaj kod sustava obrane optuženika.“[3]

Sustav može biti sačinjen od različitog broja elemenata ili podsustava, stoga je broj ostvarivih sustava velik. Sukladno sa rastom sustava eksponencijalno raste i broj elemenata ili podsustava. Svim je sustavima zajedničko, bez obzira na njihovu veličinu, da imaju svoj ulaz i izlaz. [1]

Informacijski sustav možemo definirati kao „skup povezanih dijelova (primjerice softver, hardver, ljudi, procedure, informacije te komunikacijske mreže) kojima je cilj pribaviti i prenijeti informacije i podatke za funkcioniranje, planiranje, odlučivanje i/ili upravljanje poslovnom organizacijom.“ To je “uređeni skup elemenata, odnosno komponenata koje u interakciji obavljaju funkcije prikupljanja, obradbe, pohranjivanja i diseminacije (izdavanja na korištenje) informacija.“

Informacijski je sustav sastavnica svakoga poslovnog sustava, te je njegov razvoj kontinuiran i zahtjevan posao. Danas je nemoguće zamisliti poslovnu organizaciju bez informacijskog sustava koji se zasniva na informacijsko-komunikacijskoj tehnologiji. (Slika 2.) [4]



Slika 2.Informacijski sustav [5]

Informacija je ključan resurs za uspješno odvijanje poslovnih procesa, te sam uspjeh poslovne organizacije ovisi o informacijama, inovacijama, znanju i konkurentnosti. Osim pojma sustav,

drugi je važan pojam informacija, za koju se vezuju mnogi pojmovi, između ostalog i podatak, signal, kanal i znanje.

Podatak se definira kao „bilo koji predmet mišljenja koji može prenijeti informaciju; formalizirani znakovni prikaz činjenica, pojmova i naredaba pogodan za priopćavanje, interpretiranje te analognu i digitalnu obradbu. „ Informacija se prema tome protumačeni podatak, a tomu je tako ovisno o samome kontekstu. Stoga se može zaključiti kako je svaki podatak u informacijskom sustavu zapravo informacija.

Glavna uloga informacijskog sustava je „da u najkraćemu mogućem obliku zapišu podatke u bazu podataka kako bi njima lakše i brže manipulirali, ali da svakom relevantnom i neupućenom korisniku pri pogledu na bilo koji dio informacijskoga sustava uvijek bude podastrta jasna informacija.“ [4]

Povezanost ljudi sa informacijskim sustavima s godinama se povećavala, te je slučaj da se danas sa njima susrećemo na dnevnoj bazi, što je ranije bilo nezamislivo. Baš iz tog razloga sve je veći napad na sigurnost informacija stoga se ovo postavlja kao glavni problem ovoga sustava i predmet ovoga rada.

2.1. Osnovni pojmovi računalstva

Informatika je „znanost je koja se bavi obradbom, uporabom i primjenom podataka te proučava strukturu i svojstva obavijesti, teoriju, metodologiju, zakonitosti, povijesti organizaciju informacijske djelatnosti. Ona se bavi informacijama, njihovim oblikovanjem, prenošenjem, registriranjem, obradbi i uporabi, koja se razvila s primjenom tehničkih sredstava za obradbu podataka, a posebno elektroničkih računala.

Pod računalom smatramo elektronički uređaj namijenjen obradbi podataka. Ono prihvaća naredbe i podatke, izvodi nad podatcima zadane naredbe i prikazuje rješenja u odgovarajućem

obliku.

Mrežno računalstvo su sve one usluge koje „krajnjim korisnicima i aplikacijama omogućuju da dijele informacije i izvore u heterogenim računalnim okruženjima, a korisnik mrežu računala doživljava kao virtualno superračunalo.

Informacijska tehnologija je „bilo koji oblik tehnologije (oprema ili tehnika) kojom se ljudi koriste za upravljanje i obradbu informacija.“ Danas pod tim pojmom smatramo računalsku tehnologiju kao što je to hardver i softver te telekomunikacijsku tehnologiju odnosno mreže

za prijenos podataka, slike i zvuka. Ona obuhvaća mikroelektroniku, računala, telekomunikacije i softver, te sve te komponente omogućuju unos, obradbu i distribuciju informacija

Softver je računalni program koji stoji kao sinonim za „sve programske proizvode, a čini dio računalnog sustava koji nema fizikalnih dimenzija. Možemo ga dijeliti u odnosu na primjenu, jer je korisnički softver namijenjen krajnjim korisnicima dok je sustavni namijenjen informatičarima za upravljanje računalnim sustavom.“

Hardver je skupni naziv za sve „materijalne dijelove računala i pratećih uređaja kao što je kućište, čipovi, elektronički sklopovi, kabeli, međusklopovi, tipkovnica, monitor i slično.“

Naredbe programa pišu se prema pravilima odabranoga

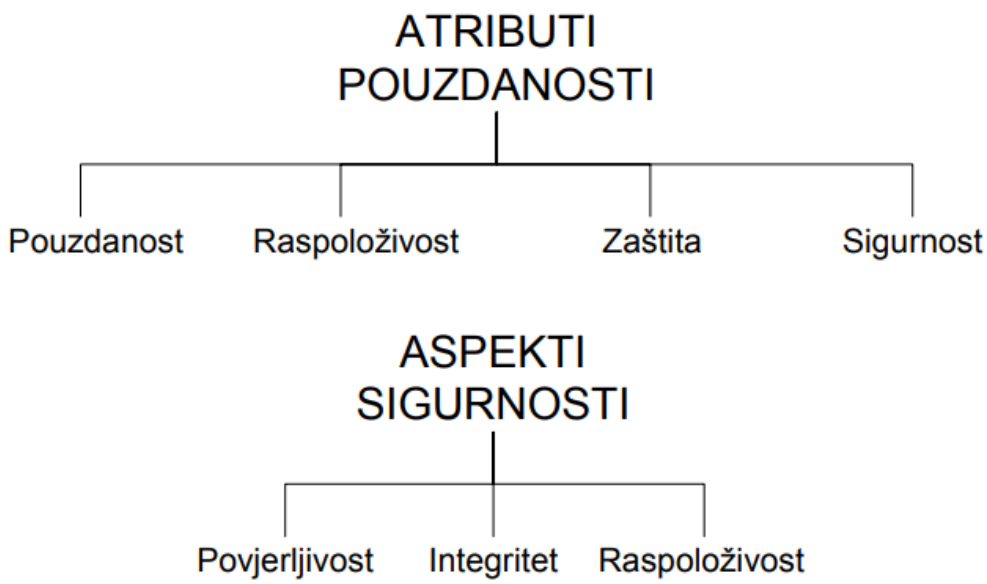
programskog jezika.

Program je općenito „skup naredaba izvedenih poznatim redoslijedom s određenim ciljem." Aplikacijski program je „korisnički računalni program određene namjene, kao što je npr. program za knjigovodstvo, program za obračun plaća, program za obradbu teksta.“[4]

2.2.Sigurnost

Kako bi se uopće definirala sigurnost nečega, potrebno je utvrditi što ona jest. Prvotno je uveden pojam pouzdanosti koji obuhvaća izraze: pouzdanost, raspoloživost, zaštita i sigurnost“, a definira se u pojmovima "ispunjavanja zadataka" i "pružanjem očekivane usluge".

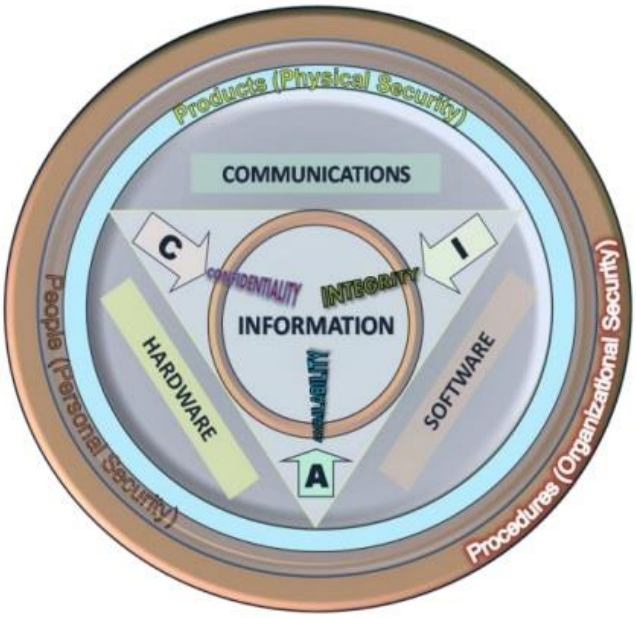
Sigurnost se u vidu toga sagleda kao jedan od atributa pouzdanosti. Osim sigurnosti, svi ostali atributi odnose se na ponašanje sustava, odnosno uslugama koje sustav daje svom okruženju; zbog toga oni formiraju adekvatnu bazu za pristup proučavanja ponašanja. Pojam sigurnosti definira se putem tri različita aspekta, a to su: povjerljivost, integritet i raspoloživost. (Slika 3.) [6]



Slika 3.Aspekti pouzdanost i sigurnost [6]

Time se može zaključiti kako koncept sigurnosti u okviru svoje definicije ne opisuje samo ponašanje sustava ili usluge koju on pruža okolini, već i mogućnost sustava da se odupre vanjskim čimbenicima odnosno napadima.[6]

„Cilj zaštite informacijsko komunikacijskog sustava podrazumijeva očuvanje tri osnovna načela informacijske sigurnosti, povjerljivost (eng. Confidentiality), cjelovitost (eng. Integrity) i dostupnost (eng. Availability). Osnovna načela informacijske sigurnosti obuhvaćena su terminom CIA model.“ [7]



Slika 4.Načela informacijske sigurnosti [7]

Kako bi se osigurala osnovna načela sigurnosti u sustav informacijske sigurnosti navedena je primjena procedura, proizvoda i ljudskih resursa na razini elemenata ovoga sustava. Uz ova tri elementa često se primjenjuju i termini autentikacije, autorizacije i revizije ili nadzora.
Načelo povjerljivosti tiče se „otkrivanja informacija i podataka isključivo autoriziranim osobama, entitetima i procesima, u definirano vrijeme i definiranom procedurom.“ Povjerljivost danas ima ključnu ulogu u svim organizacijama, iako je prije bilo mišljenje kako je ono rezervirano isključivo za državne institucije ili pak financijske sustave. Taj čimbenik igra važnu ulogu u sigurnosti stoga je vrlo bitno zaštititi povjerljive informacije određene organizacije.

Načelo cjelovitosti odnosi se na točnost informacija, jer ona kao takva jedino može imati vrijednost. Pod cjelovitošću sustava smatra se i zaštita „informacija od namjerne ili slučajne neovlaštene modifikacije uzrokovane ljudskim utjecajem ili pogreške u radu sustava“ kao što je to primjer kod online transakcija novca.

„Ukoliko osoba A, online putem, vrši transakciju novca osobi B te prilikom tog procesa dođe do narušavanja cjelovitosti informacije (npr. izmjena vrijednosti poslane novčane sume) osoba A može pretrpjeti neočekivani financijski gubitak.“

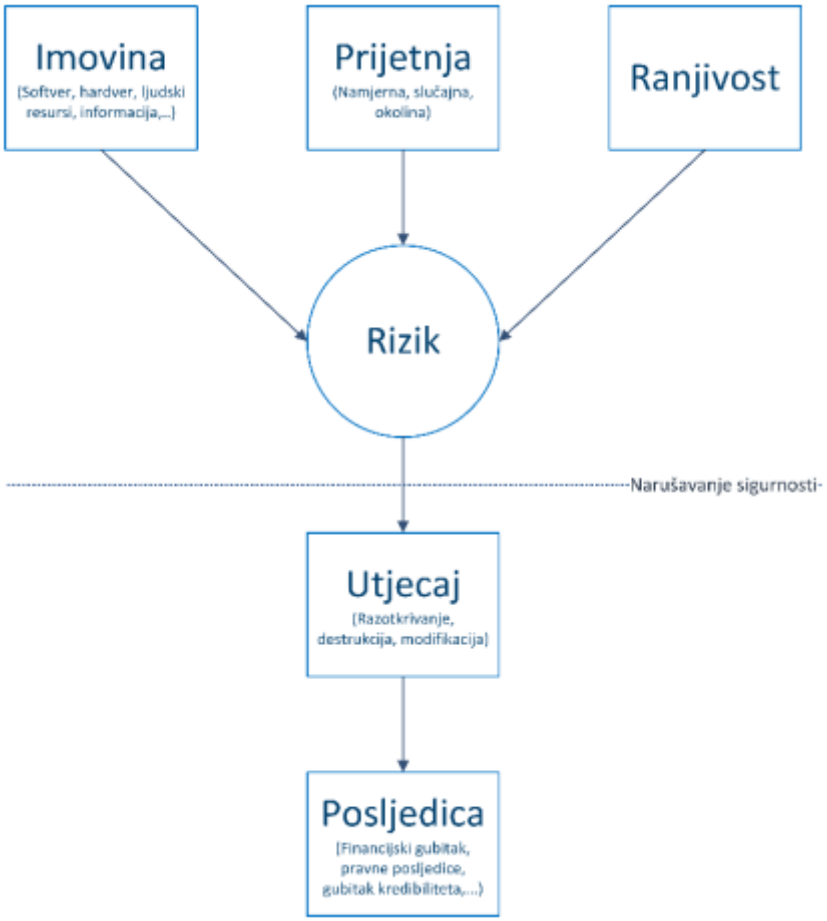
Kada je pak riječ o određenoj organizaciji, ovdje dolazi i do mnogo većih problema, jer dolazi i do narušavanja integriteta informacija, dok se ne mora nužno raditi o novčanim transakcijama, no one naposljetku mogu dovesti do ozbiljnih financijskih gubitaka ili gubitka vjerodostojnosti organizacije i drugih loših posljedica.

Vrijednost informacija ovisi i o dostupnosti, te se dostupnost informacije odnosi na njezinu raspoloživost ovlaštenim korisnicima onda kada je potrebna te prema zadanim uvjetima, u što je uključena povjerljivost i integritet. Svi uvjeti pritom moraju biti ispunjeni kako primarna funkcija sustava ne bi izgubila značaj. [7]

2.3.Čimbenici informacijske sigurnost

Radilo se o organizacijskom sustavu ili pak pojedincu, rad informacijsko komunikacijskog sustava mora uvijek postizati svoju optimalnu djelotvornost. Djelotvornost sustava ovisi o učinkovitosti svih elemenata koje on obuhvaća, stoga se on treba pomno planirati i istraživati te treba težiti njegovu poboljšanju. Pristup projektiranja i izgradnje informacijsko komunikacijskog sustava zasnovan je na „zadovoljenju funkcionalnosti i ekonomičnosti svakog pojedinog elementa i sustava kao cjeline.“

„Svaki od elemenata informacijsko komunikacijskog sustava posjeduje određene ranjivosti koje mogu biti iskorištene u svrhu narušavanja njegove sigurnosti čime se paralelno narušava i sigurnost informacija koje se unutar sustava pohranjuju, obrađuju ili prenose.“ (Slika 5.)[7]



Slika 5. Elementi koji utječu na informacijsku sigurnost [7]

Kako je vidljivo na slici, pod elementima koji utječu na informacijsku sigurnost smatramo imovinu, prijetnju i ranjivost, koji stvaraju rizik za određenu organizaciju ili osobu, te time utječu na njezinu sigurnost, a naposljetku ono radi toga snosi određene posljedice.

„Upravo iz tog razloga potrebno je obratiti pozornost na slijedećih nekoliko čimbenika koje je nužno promatrati, analizirati i njima upravljati kako bi se optimizirala razina sigurnosti sustava i informacija.“

Pod imovinom smatramo „svaki opipljiv i neopipljiv objekt ili karakteristika koja sadrži vrijednost za organizaciju. „

Imovinu možemo podijeliti na:

1. Informacijsku (sistemska dokumentacija, korisničke informacije, baze podataka)

2. Softversku (aplikacijski softveri i operativni sustavi)
3. Fizičku imovinu (računalna oprema, mrežna oprema, komunikacijska oprema, fizički mediji, ostala popratna tehnička oprema)

Prijetnja predstavlja „okolnost ili pojavu koja ima potencijal uzrokovati štetu ili gubitak.“ Po pitanju informacijskog sustava prijetnja može biti potencijalna aktivnost ili pojava koja može negativno utjecati na osnovna načela informacijske sigurnosti. Prijetnje većinom sadrže uzroke koji mogu biti predstavljeni „ljudskim faktorom ili prirodnom pojavom ili nesretnim događajem.“

Ljudski faktor u slučaju informacijske sigurnosti djeluje kao osnovni uzrok prijetnji sustavu. Neke od prijetnji, koje uzrokuje ljudski faktor mogu biti:

1. „Neposlušnost
2. Otkrivanje osjetljivih podataka
3. Sabotaža
4. Nenamjerno oštećenje imovine
5. Zlouporaba ovlasti
6. Neovlašten pristup podacima ili imovini
7. Krađa
8. Korištenje malicioznih programa.“

Ranjivost je „vjerojatnost da prijetnja postane realnost, odnosno slabosti sustava koje mogu biti iskorištene u svrhu uzrokovanja gubitka informacija ili nanošenja štete sustavu. To je stanje, nedostatak ili slabost u sigurnosnim procedurama, tehničkim kontrolama, fizičkim i drugim kontrolama sustava, dizajnu i implementaciji tih kontrola i procedura koje je moguće iskoristit. Slučajno ili namjerno iskorištavanje može prouzrokovati operativne i financijske gubitke sustavu.“

Po pitanju informacijske sigurnosti ranjivosti je moguće podijeliti prema:

1. „Ranjivosti okoline i infrastrukture
2. Ranjivosti hardvera
3. Ranjivosti softvera
4. Ranjivosti komunikacije
5. Ranjivosti ljudi.“

Rizik definiramo kao „funkciju vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost i utjecaja koji taj neželjeni događaj može imati na organizaciju.“

Utjecaj se odnosi na „ostvarenja nepoželjnog događaja, a rezultat je pojave sigurnosnog propusta odnosno iskorištavanja ranjivosti te time predstavlja neuspjeh očuvanja povjerljivosti, dostupnosti i integriteta sustava. „

Utjecaji potom dovode do posljedica stoga one predstavljaju rezultat utjecaja, odnosno štetu sustava uzrokovanu sigurnosnim incidentom. [7]

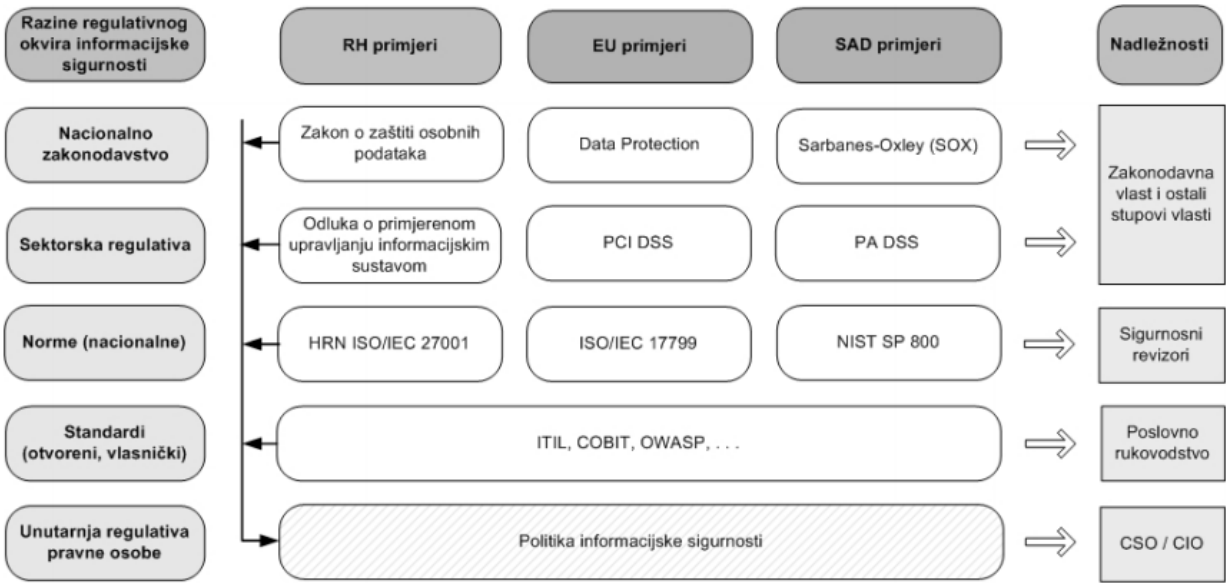
2.4.Zakoni informacijske sigurnosti

Proces upravljanja informacijskom sigurnošću odgovoran je za „trajno usavršavanje zakonskog okvira počevši od sigurnosne politike, preko provedbenih uredbi, pravilnika i smjernica, do detaljnih procedura postupanja pojedinih tijela državne uprave. Osim toga upravljanje informacijskom sigurnošću obuhvaća postupke kao što su identifikacija resursa, klasifikacija podataka, upravljanje rizikom, planiranje i implementacija mjera, postupci certifikacije osoblja i uređaja, postupci akreditacije sustava za rad, nadzor implementacije i učinkovitosti mjera i postupaka, praćenje informacijskih sustava tijekom životnog ciklusa te sustavnu edukaciju.“ [7]

Politika informacijske sigurnosti, predstavlja „dokumente kojima se utvrđuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose. „

Sa sve užurbanijim promjenama u području informacijske sigurnosti nastala je potreba za određenim regulatornim okvirima, stoga su se dosadašnje nacionalne prakse u Hrvatskoj uskladile sa sigurnosnim smjernicama NATO-a i Europske unije te je to dovelo do donošenja nacionalne regulative i postavljanja temelja za „implementaciju propisanih mjera i standarda informacijske sigurnosti u svim državnim tijelima, tijelima jedinica lokalne i područne samouprave, pravnim osobama s javnim ovlastima i drugim pravnim osobama koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.“

Stoga zakonodavni propisi obuhvaćaju široku paletu međunarodnih i nacionalnih zakonskih propisa koji se međusobno nadograđuju, uredbi, normi, standarda, regulativa. Svi ti propisi različito utječu na razvoj unutarnje politike informacijske sigurnosti pravne osobe, što je prikazano u nastavku. (Slika 6) [8]



Slika 6.Utjecaj različitih regulativa na razvoj unutarnje politike [8]

U Hrvatskoj postoje brojni zakoni, regulative i strategije koji se tiču sigurnosti podataka i informacijske sigurnosti, a to su:

1. „Zakon o informacijskoj sigurnosti (NN 79/07)
   - U sklopu kojega je i Uredba o mjerama informacijske sigurnosti (NN 46/08)
2. Zakon o sigurnosnim provjerama (NN 85/08)
3. Uredba o sadržaju, izgledu, načinu ispunjavanja i postupanju s upitnikom za sigurnosnu provjeru (NN 114/08)
4. Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (NN 102/07)
5. Zakon o tajnosti podataka (NN 79/07, 86/12)
   - U sklopu kojega je i Pravilnik o tajnosti službenih podataka Ministarstva unutarnjih poslova (NN 107/12)
6. Zakon o zaštiti tajnosti podataka (NN 108/96- samo glava VII i IX)
7. Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11 i 106/12 – pročišćeni tekst), u sklopu kojega su i:
   - Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04)
   - Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN 105/04).
8. Zakon o pravu na pristup informacijama (NN 25/13)

- U sklopu kojega je i Pravilnik o ustroju, sadržaju i načinu vođenja službenog upisnika o ostvarivanju prava na pristup informacijama (NN 137/04)“ [9]

9. „Ustav Republike Hrvatske
10. Strategija nacionalne sigurnosti
11. Zakon o sustavu domovinske sigurnosti
12. Zakon o sigurnosno-obavještajnom sustavu RH
13. Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti
    - Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga
14. Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga
15. Smjernice za postupanje s neklasificiranim podacima
16. Pravilnik o standardima sigurnosti neklasificiranih informacijskih sustava.“[10]

2.5.Komponente informacijskog sustava

Informacijski sustav sa stajališta teorije sustava skup je povezanih dijelova, a to su:

1. „materijalno-tehničke komponente (hardver, strojevi, infrastruktura),
2. nematerijalne komponente (softver, programski alati, aplikacije),
3. ljudske komponente (lifeware, analitičari, dizajneri, programeri i poslovni korisnici),
4. prijenosne komponente (netware, mreža, oprema za prijenos podataka.),
5. organizacijske komponente (orgware, hijerarhija, timovi, pravila, propisi, ograničenja, znanja, metodologija).“ [4]

Pod materijalno-tehničkom odnosno sklopovskom komponentom ubrajamo hardver, odnosno sve one strojeve i infrastrukturu namijenjene isključivo ili pretežito obradi podataka, odnosno informacija.

Pod nematerijalnom komponentom smatramo „ukupnost ljudskoga znanja ugrađenog u strojeve, opremu i uređaje koje se skupno naziva softver, te ta komponenta predstavlja predmet obrade ili diktira način obrade u sustavu.„

Ljudsku komponentu poslovnih upravljačkih informacijskih sustava čine „svi ljudi koji u bilo kojoj funkciji i s bilo kakvom namjerom sudjeluju u radu sustava i koriste rezultate obrade podataka, odnosno informacija.“

Prijenosnu komponentu čine „sredstva i veze za prijenos podataka na daljinu, odnosno telekomunikacijska sredstva i veze u sustavu, a organizacijsku komponentu tvore sve mjere, metode i propisi kojima se usklađuje rad prethodno navedenih četiriju komponenata, kako bi one tvorile skladnu cjelinu.“ [11]

3.MOBILNE KOMPONENTE I NJIHOVA SIGURNOST

Današnji svijet gotovo je nezamisliv bez mobilnih uređaja, što je sredinom prošlog desetljeća bilo nezamislivo, a mnogi su smatrali kako je sam razvoj prvih mobilnih uređaja gotovo nemoguć. Tehnologija je srećom od tada uvelike napredovala, stoga danas više ne govorimo niti o mobilnim telefonima kao takvim, odnosno o uređajima kakvi su bili u početku, već govorimo o pametnim telefonima.

Pametni telefon može se definirati kao „uređaj koji proširuje mogućnosti klasičnog mobilnog telefona.“ Danas je na tržištu velik broj vrsta mobilnih telefona sa raznim karakteristikama, stoga dodatne funkcije koje se očekuju od pametnog telefona ne mogu biti strogo definirane i mijenjaju se s vremenom. Oni se također razlikuju ovisno o cijeni, kvaliteti sastavnica, veličini i slično, a ključne su komponente koje ovakav uređaj ipak treba sadržavati slijedeće:

• „operacijski sustav (npr. iOS, Android i sl.),

• aplikacije,

• puna QWERTY tipkovnica i

• stalni pristup Internetu. „

Razvoj pametnih telefona započeo je 1992. kada IMB predstavlja pametni telefon Simon. To je tada bio prvi takav uređaj te je objedinjavao mobilni telefon, osobnog asistenta i faks uređaj. To znači kako je uz uobičajene mogućnosti zvanja i slanja SMS poruka, sadržavao kalendar, adresar, svjetski sat, kalkulator, blok za bilješke, klijent elektroničke pošte, mogućnost slanja i primanja faksova te igre.

Tada je ovakav mobitel bio čudo tehnike, no danas telefoni služe i kao zamjena za GPS navigator, digitalni fotoaparat ili videokameru, za slušanje muzike i slično. Današnji pametni telefoni imaju više procesorske snage i radne memorije, te mnogo više značajki nego ranije. [12]

Slika 7.Primjer unutrašnjosti pametnog telefona Samsung galaxy S9+ [13]

Baš iz tog razloga njihova sigurnost sada je puno ugroženija jer se može utjecati na više elemenata sigurnosti. Razlozi zbog kojih su pametni telefoni zanimljivi napadačima su:

- „broj pametnih telefona sve više raste,
- imaju stalnu vezu s internetom,
- na pametnim telefonima se nalaze osjetljive korisničke informacije kao što su: osobni podaci korisnika i njegovih poznanika, elektronička pošta, korisnikov osobni kalendar itd.,
- pametni telefon koristi SIM karticu koja je povezana s pretplatničkim računom i
- pametni telefoni se mogu koristiti za osjetljive bankovne transakcije. „

Što više korisnika koristi neku tehnologiju to je veća vjerojatnost da će napadač odabrati baš tu tehnologiju napada. Sa te strane pametni telefoni su najbolja opcija za napadače obzirom da se povezuje na internet na dva načina:

1. „preko mobilnog Interneta što je povezano s pretplatničkim brojem ili bežično,
2. preko Wi-Fi bežičnog pristupa, zbog čega se pametni telefoni mogu nalaziti u različitim mrežama. „

Danas ovdje dodatnu opasnost predstavljaju društvene mreže, servisi elektroničke pošte te udaljeni poslužitelji na kojima se nalaze udaljene datoteke odnosno Cloud computing (oblak).

3.1.Podaci

Ljudi danas svoje pametne telefone nose svugdje sa sobom, stoga oni zapravo postaju osobna računala u pravom smislu. Korisnici se pouzdaju u svoje pametne telefone za čuvanje raznih osobnih podataka što napadači često koriste za špijuniranje korisnika, a potom ucjenu ili prodaju korisničkih informacija kao što je primjerice adresa elektroničke pošte.

Glavni motiv napadačima je novac. Do novca napadač dolazi putem SIM kartice koja je ujedno povezana sa pretplatničkim računom. Napadač to može iskoristiti kako bi na neki način ukrao novac s korisničkog računa i tako zaradio. Najčešći način na koji se može izvesti ovaj vid napada je postavljanje zlonamjernog programa koji poziva određeni telefonski broj.

Najčešće se radi o pozivu na neku uslugu s dodatnom vrijednosti (npr. telefonski brojevi koji počinju s brojevima 060) nad kojom napadač ima ovlasti. Svaki puta kada pametni telefon pozove taj broj, dio novaca se prebacuje s korisnikovog računa na napadačev.

Bankovne transakcije također mogu biti meta napadača, te je to danas rastući problem obzirom da sve veći broj korisnika pristupa svojim računima putem mobitela. Pomoću takvih aplikacija korisnik može pregledavati stanje svojih bankovnih računa, ali i prebacivati novac sa svojeg računa na tuđi. Ukoliko napadač uspije dobiti nadzor nad ovim aplikacijama u mogućnosti je ukrasti sredstva s korisnikovog bankovnog računa. [12]

U nastavku poglavlja navedene su komponente koje predstavljaju rizike pri korištenju pametnih telefona.

3.2.Kamera i mikrofon

Kamera i mikrofon su komponente koje posjeduje svaki pametni telefon današnjice. Mikrofon se može koristiti kako za snimanje zvuka u videu tako i za komunikaciju ptem mobitelja, dok se kamera koristi za fotografiranje i u svim povezanim aplikacijama koje za nju traže dopuštenja, u što spadaju i bakarske aplikacije, aplikacije za prepoznavanje određenih predmeta i slično.

Obzirom da se ovim komponentama upravlja programski, napadač može iskoristiti to za uključivanje kamere i mikrofona bez korisnikovog znanja. On na taj način dobiva informacije o korisnikovoj okolini ili ga pak može prisluškivati pomoću nekih zločudnih programa.

Primjer takvog programa je Androidov NickiSpy. Ovu aplikaciju korisnik odnosno njegov napadač, skida na svoj pametni telefon. Kada se aplikacija instalira počinju djelovati pozadinski procesi koje korisnik ne može vidjeti, stoga ih nije svjestan. Oni bilježe njegove telefonske razgovore te ih pohranjuje na memorijsku karticu, te se oni naknadno mogu i poslati.

Na taj način napadač može preslušati sve korisnikove telefonske razgovore od trenutka instaliranja zloćudne aplikacije, što mu može biti od određene koristi u vidu ucjene u novcu. Ova aplikacija prikuplja i razne druge podatke vezane uz lokaciju uređaja ili jedinstvene oznake mobilnog telefona. [12].

Slika 8.Kamera pametnog telefona [13]

3.3.Lokacija

Danas svi mobilni telefoni imaju lokacijsku opciju sa kojom mogu koristiti razne aplikacije kao što su Google karte, ali i društvene mreže na kojima mogu označiti svoju lokaciju ili ju pak poslati putem neke komunikacijske aplikacije. Iako vrlo koristan u pojedinim situacijama, GPS posjeduje osjetljivu informaciju o poziciji korisnika, te ta informacija napadačima služi za praćenje vlasnika. Programi koji prate osobu pomoću GPS sustava mogu se skinuti na većini operacijskih sustava. Mnogi su operacijski sustavi, pa tako i iOS imali problema sa podacima GPS sustava. Problem je bio u pohrani GPS položaja s iPhone telefona u nezaštićenu datoteku koju je mogao pročitati bilo tko ukoliko je imao pristup samoj datoteci.

Kako se ovaj problem ne bi ponovio potrebno je na razini operacijskog sustava ograničiti pristup GPS podacima, što današnji operacijski sustavi pametnih telefona rade sve bolje.[12]

Slika 9. Primjer uključene lokacije na pametnom telefonu [14]

3.4.Baterija

Kada ne bi bilo baterije, uređaj ne bi mogao raditi, stoga se može reći kako je baterija jedan od ključnih faktora za rad pametnog telefona. Pametni telefon ovisi o bateriji. Što češće koristimo mobitel, te što više aplikacija paralelno na njem imamo upaljeno ili ih pak koristimo, intenzivnije je korištenje procesora i memorije stoga on i troši više baterije. Iz tog razloga mobitel je potrebno češće puniti, a ukoliko se on prazni brže nego ga je moguće napuniti, baterija nije iskoristivi. Kako bi izdržali što dulje s jednim punjenjem baterije, uređaji prelaze u stanje mirovanja kada se uređaj određeno vrijeme ne koristi što ga održava dulje vrijeme upaljenim i dostupnim na korištenje.

Kada ne bi postojalo vrijeme mirovanja, uređaj bi bio neupotrebljiv, stoga je za napadače ova činjenica jedan od glavnih načina napada. Taj napad naziva se DoS odnosno Denial of Service napad. Za napad je potrebno napraviti takav programski kod koji intenzivno troši procesor i memoriju i pri tome sprječava prelazak u stanje mirovanja. Time je moguće jako brzo istrošiti cijelu bateriju zbog čega uređaj postaje neupotrebljiv. [12]

Slika 10. Baterija telefona Samsung galaxy S9+ sa matičnom pločom [13]

4.MOBILNE PLATFORME

Jezgra operacijskih sustava iOS i Android temelji se na Unix/Linux operacijskim sustavima što je čini poprilično sigurnom., no ne i potpuno otpornom a napade. U naporima da se sigurnost poboljša naknadno se dodaju poboljšanja postojećeg operacijskog sustava.

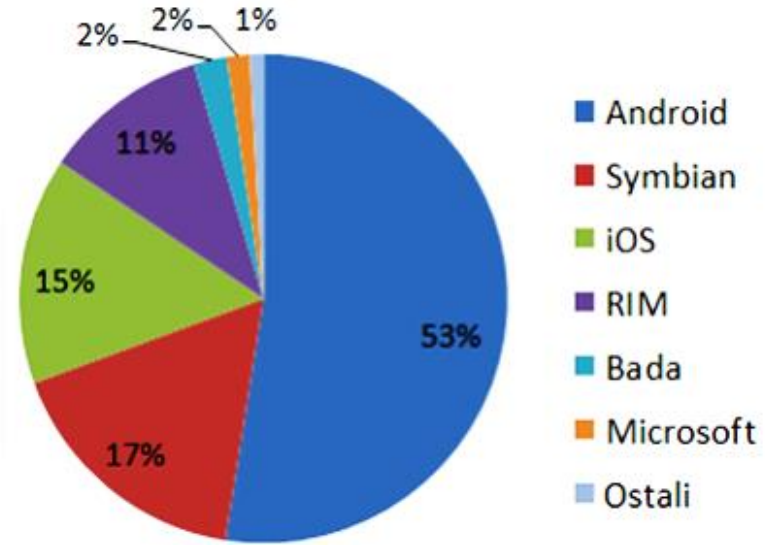
Čest je slučaj da zbog tržišnog natjecanja i želje da se novi proizvod izda prije konkurentskog, novi dijelovi operacijskog sustava često nisu dovoljno ispitani sa stajališta sigurnosti, čime se stavlja u pitanje početna sigurnost jezgre operacijskog sustava jer sigurnost cijelog sustava ovisi o sigurnosti najslabijeg dijela.

4.1.Povijest

Kroz povijest su postojali mnoge platforme za pametne telefone na tržištu koji su dijelili različite udjele, od čega su 2011. godine slijedeći imali veće udjele:

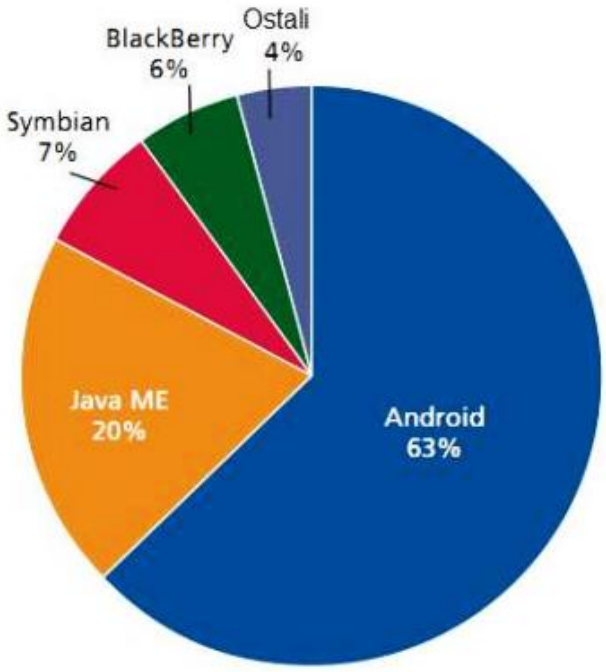
1. Android
2. iOS
3. Microsoft
4. Symbian
5. RIM
6. Bada
7. Ostali

2011. godine stanje na tržištu bilo je obasuto različitim operacijskim sustavima odnosno platformama, koje su se borile za svoje mjesto. Sve te platforme pokušavale su osigurati bolju kvalitetu i sigurnost za svoje korisnike, a njihov udio prikazan je u nastavku. (Slika 11.) [12]



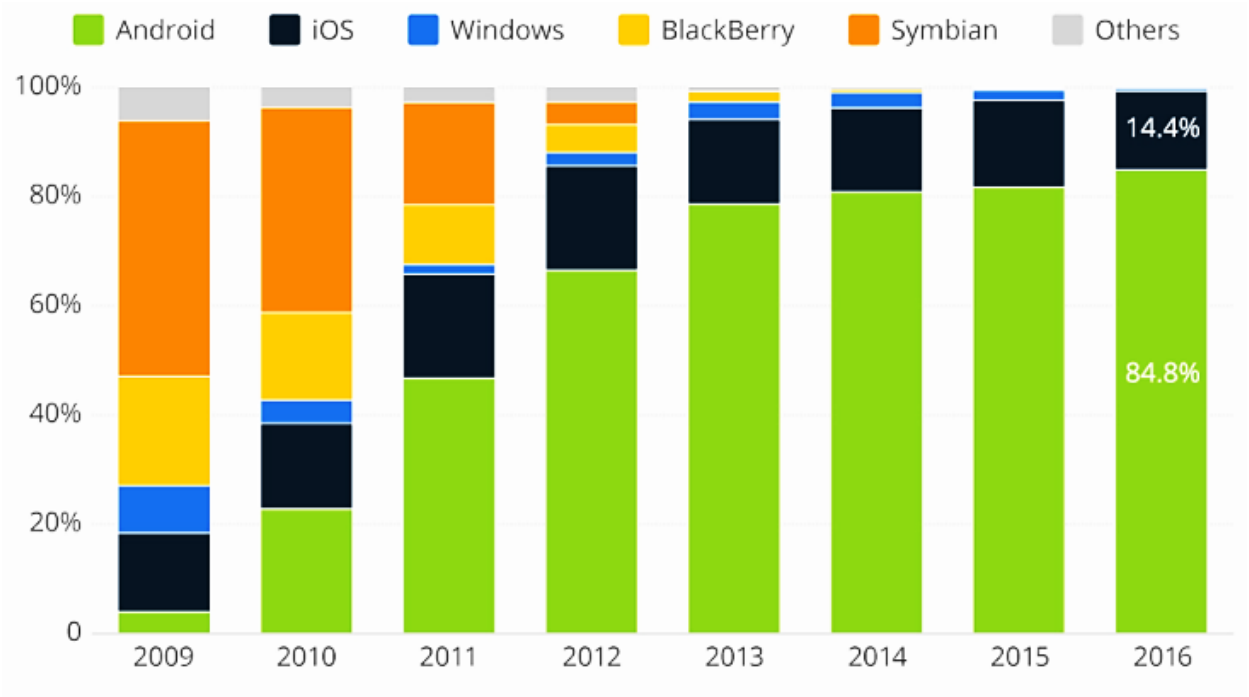
Slika 11. Udio operacijskih sustava na tržištu 2011. godine [12]

Iste godine izbačeno je i izvješće o udjelu zločudnih programa u pojedinim sustavima, gdje je vidljiv veliki udio zloćudnih programa namijenjenih operacijskom sustavu Android. Dosta veliki udio imaju i zloćudni programi koji se javljaju u aplikacijama temeljenim na Javi. Ovdje je riječ o programima koji nisu namijenjeni isključivo za pametne telefone, nego se nalaze pretežno na klasičnim telefonima, a mahom je riječ o Java igricama u koje je ubačen zloćudni kod. (Slika 12) [12]



Slika 12. Udio zloćudni programa kod pojedinih operacijskih sustava [12]

Razvojem novih tehnologija te unapređenjem dosadašnjih sustava, kroz godine se situacija uvelike promijenila. Iako je globalno tržište pametnih telefona konkurentno kao i uvijek u smislu proizvođača koji se bore za ljubav potrošača, čini se da je dugotrajni rat gotov. Prema nedavnom izvješću Android i iOS sada čine više od 99 posto globalne prodaje pametnih telefona, što svaku drugu platformu čini nevažnom, iako je njihov udio prije 10 godina bio tek 40 % globalne prodaje pametnih telefona. (Slika 13) [16]



Slika 13. Udio pojedinih mobilnih platformi [16]

4.2.Podjela

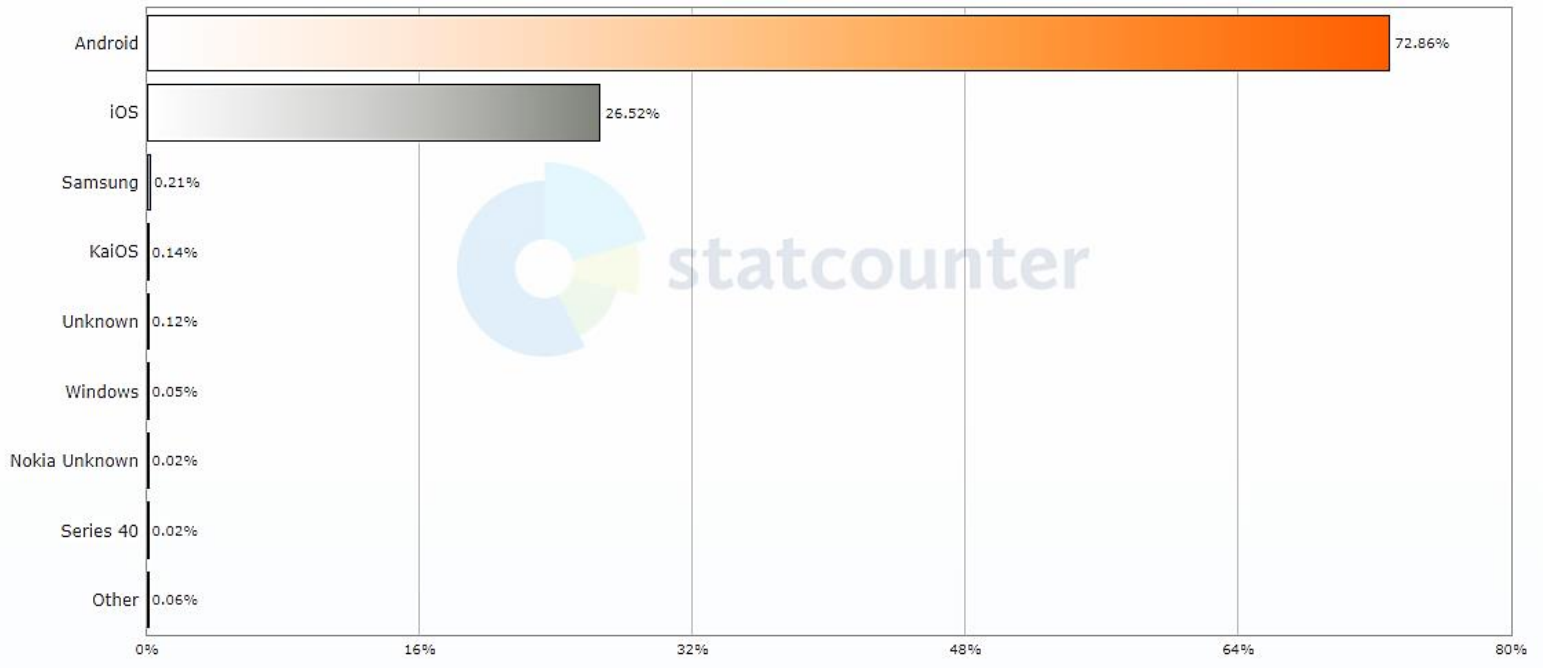
Operacijski sustavi napravljeni su i prilagođeni isključivo za uređaje poput pametnog telefona, osobnog digitalnog asistenta (PDA), tableta i slično. Ovi su mobilni operativni sustavi posebno odgovorni za prepoznavanje i definiranje mobitela kroz njegove prepoznatljive funkcionalnosti te sučelje.

Iako je na tržištu dostupno puno mobilnih operacijskih sustava, a u začetcima ih je bilo još i više, iOS i Android i dalje dominiraju tržištem po popularnosti. Iako možda dominiraju tržištem, ne znači da su savršene platforme, stoga se na tržištu pojavljuju i mnogi drugi sustavi, koji se razlikuju od onih koji su nekoć postojali obzirom da se dosta njih ugasilo, dok su se sa druge strane pojavili i neki noviji, a to su:

1. Sailfish OS
2. Tizen Open-Source OS

3. Ubuntu Touch
4. KaiOS
5. Plasma OS
6. PostmarketOS
7. PureOS
8. LineageOS.

Ovi sustavi su u vlasništvu nekoliko većih tvrtki koje su na tržištu već duže vrijeme te ne odustaju u konkurentskoj borbi za suparnicima na tržištu pametnih telefona. U nastavku je prikazan udio tvrtki u čijem posjedu su određeni operacijski sustavi, gdje je vidljivo kako iOS i Android sustavi uvelike prednjače, no u svrhu usporedbe prikazani su i ostali udjeli. (Slika 14.) [17]



Slika 14. Tržišni udio pojedinih platformi u razdoblju 02.2020-02.2021 [18]

Zbog tako velikog postotka od čak 99% tržišnog udjela evidentno je kako nema smisla promatrati značajke te sigurnost ostalih platformi, stoga će se u nastavku rada komentirati isključivo sigurnost Android i iOS operacijskih sustava, uz kratki osvrt na ostale platforme na kraju poglavlja.

4.2.1. Android OS

Android uključuje sigurnosne značajke koje su vodeće u industriji i surađuje s programerima i implementatorima uređaja kako bi platforma i ekosustav bili sigurni, stoga i ne čudi što na

tržištu sudjeluje sa udjelom od čak 72.86%. Ovo tržište u tolikom je usponu te se neprestano mijenja, a postoci neprestano padaju i rastu za nekoliko decimala.

Android je od 2005. godine u većinskom vlasništvu Googlea, a temelji se na operacijskom sustavu Linux te je otvorenog koda. Godine 2007. prvi je put predstavljen na tržištu te je razvijan od strane organizacije Open Handset Alliance, koja se sastoji od 78 kompanija, od kojih su najznačajniji predstavnici: Google, HTC, Dell, Intel, Motorola, Samsung, Qualcomm, Texas Instruments, T-Mobile, Nvidia i LG Electronics.

Prvi mobilni uređaj sa ovim operacijskim sustavom bio je HTC Dream. Aplikacije ovog sustava pisane su u programskom jeziku Java i one koje se nalaze na Android Marketu imaju sigurnosno jamstvo. U nastavku je prikazan primjer Android korisničkog sučelja. (Slika 15) [15]

Slika 15. Primjer Android korisničkog sučelja [21]

Android operativni sustav koriste mnogi uređaji, od jeftinih proračunskih uređaja do vodećih. Zbog svoje otvorene izvorne prirode može se naći na mnogim drugim uređajima, uključujući sustave za zabavu, televizore, e-čitače, netbooke, pametne satove, automobilska računala i igraće konzole. Android je mobilna platforma koja ima najveći tržišni udio od svih dostupnih mobilnih operativnih sustava.

Ovim postignućem dolazi i pažnja mnogih hakera širom svijeta koji žele razotkriti sigurnosne nedostatke u ovom sustavu i popularnim aplikacijama na platformi. Iako su mnoge trgovine aplikacija dostupne korisnicima Androida, promatranje samo službene statistike Google Play

trgovine da Google Play trgovina ima više od 1,1 milijun aplikacija za preuzimanje. Ranjivosti se neprestano otkrivaju u popularnim aplikacijama različitog stupnja ozbiljnosti, a zbog zrelosti alata i informacija o pronalaženju tih ranjivosti, čini se da se ovaj trend neprestano povećava.[20]

4.2.2. Apple iOS

Apple iOS predstavljen je godine te je namijenjen samo mobitelima iPhone. Danas se nalazi na svim Apple-ovim uređajima Razvijen je iz operacijskog sustava Mac OS X, koji je pak temeljen na Unix OS-u. Aplikacije se nalaze na AppStoreu za razliku od Androidovog Play store-a i pišu se u programskom jeziku Objective-C. Apple drži reputaciju inteligentnog kreatora korisničkog sučelja koji se temelji na konceptu izravne manipulacije, koristeći geste s više dodira, odnosno, za razliku od Androida, iOS nema izbornik koji se otvara u novom prozoru, već se sve nalazi na početnom zaslon kako je prikazano u nastavku, uz padajuće izbornike za pojedine . (Slika 16) [15]

Slika 16. Primjer iOS korisničkog sučelja [21]

Danas Appleov iOS koriste iPhone, iPad i iPod touch uređaji, te je jedan od najpopularnijih dostupnih mobilnih operativnih sustava nakon Androida. Iz tog razloga, hakeri ciljaju ovu platformu te je pod najvećim nadzorom zbog ranjivosti aplikacijskog sloja.

S više od milijun aplikacija u Appleovom App Storeu, površina napada je značajna. Zabilježeni su brojni primjeri sigurnosnih nedostataka utemeljenih na aplikacijama, koji utječu na širok spektar aplikacija, uključujući, ali ne ograničavajući se na one koji se koriste u bankarskom, maloprodajnom i poslovnom okruženju. [20]

4.3.Sigurnost

4.3.1. Android OS

Snažan sigurnosni model neophodan je za omogućavanje snažnog ekosustava aplikacija i uređaja izgrađenih na i oko Android platforme i podržanih uslugama u oblaku. Kao rezultat toga, Android je tijekom cijelog svog razvojnog životnog ciklusa bio podvrgnut rigoroznom sigurnosnom programu.

Android je dizajniran da bude otvoren, stoga njegove aplikacije koriste napredni hardver i softver, kao i lokalne podatke koji se poslužuju, izložene putem platforme kako bi potrošačima donijeli inovacije i vrijednost. Da bi shvatila tu vrijednost, platforma nudi okruženje aplikacija koje štiti povjerljivost, integritet i dostupnost korisnika, podataka, aplikacija, uređaja i mreže.

Osiguranje otvorene platforme zahtijeva jaku sigurnosnu arhitekturu i rigorozne sigurnosne programe. Android je dizajniran s višeslojnom sigurnošću koja je dovoljno fleksibilna da podržava otvorenu platformu, a istovremeno štiti sve korisnike platforme.

Android je također dizajniran za programere, te su sigurnosne kontrole osmišljene kako bi se smanjio teret za programere stoga oni mogu lako raditi i oslanjati se na fleksibilne sigurnosne kontrole. Programeri manje upoznati sa sigurnošću zaštićeni su sigurnim zadanim postavkama.

Osim što pruža stabilnu platformu za nadogradnju, Android pruža dodatnu podršku programerima na brojne načine. Androidov sigurnosni tim traži potencijalne ranjivosti u aplikacijama i predlaže načine za rješavanje tih problema. Za uređaje s Google Playom usluge Play isporučuju sigurnosna ažuriranja za kritične softverske knjižnice, poput OpenSSL-a, koji se koristi za zaštitu komunikacije aplikacija. Osim toga odjel Android sigurnosti izdao je alat za testiranje SSL-a koji pomaže programerima pronaći potencijalne sigurnosne probleme na bilo kojoj platformi koju razvijaju.

Gledajući sa strane korisnika, Android pruža uvid u dopuštenja koja zahtijeva svaka aplikacija i nadzor nad tim dopuštenjima. Ovaj dizajn uključuje očekivanje da će napadači pokušati izvesti uobičajene napade, poput napada socijalnog inženjeringa kako bi uvjerili korisnike uređaja da instaliraju zlonamjerni softver i napade na programe trećih strana na Androidu. Android je osmišljen kako bi smanjio vjerojatnost ovih napada i uvelike ograničio utjecaj

napada u slučaju da je bio uspješan. Androidova sigurnost nastavlja napredovati nakon što je uređaj u korisnikovim rukama. [19]

Nekoliko je značajki koje Android koristi kako bi njegov sustav bio što sigurniji, a to su:

1. Sandbox aplikacije- Android platforma koristi prednost Linux-ove korisničke zaštite za prepoznavanje i izoliranje resursa aplikacija. Da bi to učinio, Android svakoj aplikaciji za Android dodjeljuje jedinstveni korisnički ID i pokreće ga u svom procesu. Android koristi ovaj ID za postavljanje aplikacijskog okruženja na razini jezgre.

2. Potpisivanje aplikacije- Potpisivanje aplikacija omogućava programerima da identificiraju autora aplikacije i ažuriraju svoju aplikaciju bez stvaranja složenih sučelja i dozvola. Svaka aplikacija koja se izvodi na Android platformi mora biti potpisana od strane programera.

3. Ovjera- Android koristi koncept kriptografskih ključeva s autentifikacijom korisnika koji zahtijevaju pohranu kriptografskih ključeva i davatelja usluga i autentifikatore korisnika. Na uređajima sa senzorom otiska prsta korisnici mogu upisati jedan ili više otisaka prstiju i pomoću njih otključati uređaj i obaviti druge zadatke. Podsustav Gatekeeper izvodi provjeru autentičnosti uzorka uređaja / lozinke u pouzdanom izvršnom okruženju. Android 9 i novije verzije uključuju Protected Confirmation, što korisnicima daje način da formalno potvrde kritične transakcije, poput plaćanja.

4.Biometrija- Android 9 i novije verzije uključuju API BiometricPrompt koji programeri aplikacija mogu koristiti za integriranje biometrijske provjere autentičnosti u svoje aplikacije na agnotički način rada uređaja i modaliteta. Samo se snažne biometrije mogu integrirati s BiometricPromptom.

5. Šifriranje- Jednom kada je uređaj šifriran, svi podaci koje je stvorio korisnik automatski se šifriraju prije predavanja na disk i sva štiva automatski dešifriraju podatke prije vraćanja u proces pozivanja. Šifriranje osigurava da čak i ako neovlaštena strana uspije pristupiti podacima, neće ih moći pročitati.

6. Trgovina ključeva- Android nudi pohranu ključeva s hardverskom podrškom koja omogućuje stvaranje, uvoz i izvoz asimetričnih ključeva, uvoz sirovih simetričnih ključeva, asimetrično šifriranje i dešifriranje s odgovarajućim načinima popunjavanja i još mnogo toga.

7. Linux poboljšana sigurnost- Kao dio sigurnosnog modela Androida, Android koristi poboljšani Linux kako bi nametnuo obveznu kontrolu pristupa nad svim procesima, čak i procesima pokrenutim s privilegijama.

8. Pouzdano Trusty izvršno okruženje- Trusty je siguran operativni sustav koji pruža pouzdano izvršno okruženje za Android. Trusty OS radi na istom procesoru kao i Android OS, ali Trusty je od ostatka sustava izoliran i hardverom i softverom.

9. Provjereno pokretanje- provjereno pokretanje nastoji osigurati da sav izvršeni kod dolazi iz pouzdanog izvora, a ne od napadača. Uspostavlja puni lanac povjerenja, počevši od hardverski zaštićenog korijena povjerenja do pokretača, do particije za pokretanje i ostalih provjerenih particija. [19]

4.3.2. Apple iOS

Ovaj operacijski sustav temelji se na Appleovom operacijskom sustavu OS X za kućna i prijenosna računala, koji je poznat po vrlo dobroj sigurnosti što je slučaj i kod iOS-a. U iOS-u je postavljeno dosta ograničenja koja onemogućuju aplikacijama pristup važnim dijelovima operacijskog sustava.

Kod iOS-a je teže povezivanje s drugim uređajima, kao primjerice računalima koji mogu biti prijenosnici zlоćudnog koda, zbog čega je i napad ograničen. Zlоćudni programi za iPhone postoje, ali napadaju samo namjerno otključane uređaje koji su napravljeni kako bi zaobišli Appleovu zaštitu. Jedino je na otključane iPhone uređaje moguće instalirati programsku podršku koju Apple nije prethodno dozvolio, što ujedno uzrokuje povećani rizik od napada. [12]

Apple se zalaže za zaštitu kupaca vodećim tehnologijama za zaštitu privatnosti i sigurnosti - dizajniranim za zaštitu osobnih podataka - i sveobuhvatnim metodama koje pomažu u zaštiti korporativnih podataka u poslovnom okruženju. Apple nagrađuje istraživače za posao na otkrivanju ranjivosti nudeći nagradu za sigurnost.

Nadovezujući se na iskustvo stvaranja najnaprednijeg svjetskog mobilnog operativnog sustava, Apple je stvorio sigurnosne arhitekture koje se bave jedinstvenim zahtjevima mobilnih uređaja, satova, stolnih računala i kuće. Svaki Appleov uređaj kombinira hardver, softver i usluge osmišljene za zajedničku suradnju radi maksimalne sigurnosti i transparentnog korisničkog iskustva u službi krajnjeg cilja zaštite osobnih podataka. Na primjer, Apple-ov silicijski i sigurnosni hardver pokreće kritične sigurnosne značajke, dok softverske zaštite djeluju na zaštitu operacijskog sustava i nezavisnih aplikacija.

Konačno, usluge pružaju mehanizam za sigurna i pravovremena ažuriranja softvera, napajaju zaštićeni ekosustav aplikacija i olakšavaju sigurnu komunikaciju i plaćanja. Kao rezultat toga, Apple uređaji štite ne samo uređaj i njegove podatke već i čitav ekosustav, uključujući sve ono što korisnici rade lokalno, na mrežama i uz ključne internetske usluge. Baš kao što dizajnira svoje proizvode tako da budu jednostavni, intuitivni i sposobni, tako pazi i da budu sigurni.

Ključne sigurnosne značajke, poput hardverske enkripcije uređaja, ne mogu se slučajno onemogućiti. Ostale značajke, poput Touch ID-a i Face ID-a, poboljšavaju korisničko iskustvo čineći jednostavnijim i intuitivnijim osiguravanje uređaja. Budući da su mnoge od ovih značajki omogućene prema zadanim postavkama, korisnici ili IT odjeli ne trebaju izvoditi opsežne konfiguracije.

Apple-ov sustav organiziran je na nekoliko razina sigurnosti:

1. Hardverska sigurnost i biometrija: silicijski hardver čini temelj sigurnosti na Apple uređajima, uključujući Secure Enclave, namjenski kriptografski mehanizam, Touch ID i Face ID
2. Sigurnost sustava: Integrirane hardverske i softverske funkcije koje pružaju sigurno pokretanje, ažuriranje i trajni rad Appleovih operativnih sustava
3. Šifriranje i zaštita podataka: Arhitektura i dizajn koji štite korisničke podatke ako se uređaj izgubi ili ukrade ili ako ga neovlaštena osoba pokuša koristiti ili izmijeniti
4. Sigurnost aplikacija: softver i usluge koji pružaju siguran ekosustav aplikacija i omogućuju aplikacijama sigurno rad i bez narušavanja integriteta platforme
5. Sigurnost usluga: Appleove usluge za identifikaciju, upravljanje lozinkom, plaćanja, komunikacije i pronalaženje izgubljenih uređaja
6. Mrežna sigurnost: Standardni mrežni protokoli koji osiguravaju sigurnu provjeru autentičnosti i šifriranje podataka u prijenosu
7. Sigurnost kompleta za programere: Okvirni "setovi" za sigurno i privatno upravljanje domom i zdravljem, kao i proširenje mogućnosti Apple uređaja i usluga na treće strane aplikacije
8. Sigurno upravljanje uređajima: metode koje omogućuju upravljanje Apple uređajima, sprječavaju neovlaštenu upotrebu i omogućavaju daljinsko brisanje ako se uređaj izgubi ili ukrade. [22]

5.MOBILNE APLIKACIJE

Nema sumnje da su mobiteli promijenili svijet, od načina na koji radimo, komuniciramo, družimo se, koji se drastično razlikuje u odnosu na prošlo stoljeće. Mobiteli i intenet su nam donijeli beskrajne mogućnosti nadohvat ruke, dostupne cijelo vrijeme. Mogućnost obavljanja internetskog bankarstva, provjere e-pošte, sudjelovanja na burzi i još mnogo toga jedan je potez daleko. Zapravo, razvoj aplikacija sada je toliko popularan da Appleov zaštitni znak "Postoji aplikacija za to" graniči sa stvarnošću. [20]

Aplikacije su dodatni programi koje korisnik može instalirati na svojem pametnom telefonu kako bi proširio njegove mogućnosti, te na taj način svaki korisnik može pametni telefon prilagoditi svojim potrebama. Aplikacije su najveći sigurnosni problem pametnih telefona zbog sigurnosnih rizika koje kod njih postoje, stoga stoga se većina napada izvodi upravo preko aplikacija. Aplikacije se tada koriste kao prijenosnik zloćudnog programskog koda koji izvodi pravi napad.[12]

Mobilne aplikacije predstavljaju posebne rizike za sigurnost i privatnost, kako zbog svoje prirode, tako i zbog cjelokupnog konteksta razvoja mobilnih aplikacija. Osnovni principi kojih se treba pridržavati pritom su sljedeći:

1. Zakonitost i transparentnost- Osobni podaci obrađivat će se poštujući poštenost i transparentnost prema nositelju podataka i ispunjavajući zahtjev legitimnog osnova za obradu osobnih podataka
2. Ograničenje svrhe- kada aplikacija obrađuje osobne podatke, aplikacija za to mora imati određenu zakonitu svrhu i mora obavijestiti korisnika sukladno tome. Daljnja obrada u druge svrhe dopuštena je samo na temelju određenog skupa kriterija u GDPR-u. I dalje je uobičajeno da programeri aplikacija prikupljaju podatke na temelju široko tumačene opće namjene, što nije dovoljno da bi se udovoljilo obvezama iz GDPR-a.
3. Minimizacija podataka- Osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je potrebno u odnosu na svrhe u koje se obrađuju.
4. Točnost- Osobni podaci moraju biti točni i po potrebi ažurirani. Uz to, moraju se poduzeti svi razumni koraci kako bi se osiguralo da se osobni podaci koji nisu točni brišu ili ispravljaju bez odgađanja, uzimajući u obzir svrhe u koje se obrađuju.
5. Ograničenje pohrane- Osobni podaci moraju se čuvati u obliku koji dopušta identifikaciju subjekata podataka najdulje onoliko koliko je potrebno za svrhe u koje

se osobni podaci obrađuju. Podaci se mogu pohranjivati dulje razdoblje u svrhe čuvanja od javnog interesa ili u statističke svrhe prema GDPR-u.

6. Integritet i povjerljivost- Osobni se podaci obrađuju na način koji osigurava odgovarajuću sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade i od slučajnih gubitaka, uništenja ili oštećenja. S obzirom na to, voditelji obrade podataka provode odgovarajuće tehničke ili organizacijske mjere. [35]

Mobilne aplikacije stvorene su za gotovo sve zamislive svrhe. Smatra se da samo u kombiniranim distribucijskim trgovinama Applea i Googlea postoji više od 2 milijuna aplikacija koje pokrivaju širok raspon funkcija, uključujući neke od sljedećih:

1. Internetsko bankarstvo (Barclays)
2. Kupovina (Amazon)
3. Društvene mreže (Facebook)
4. Streaming (Sky Go)
5. Kockanje (Betfair)
6. Instant poruke (WhatsApp)
7. Glasovni chat (Skype)
8. E-pošta (Gmail)
9. Dijeljenje datoteka (Dropbox)
10. Igre (Angry Birds)

Mobilne se aplikacije često preklapaju s funkcionalnošću koju pružaju web aplikacije, u mnogim se slučajevima koriste isti API-ji jezgre na poslužitelju i prikazuju sučelje kompatibilno sa pametnim telefonom na prezentacijskom sloju. Uz aplikacije dostupne na raznim tržištima distribucije, mobilne su aplikacije široko prihvaćene u poslovnom svijetu kao podrška ključnim poslovnim funkcijama. Mnoge od ovih aplikacija pružaju pristup vrlo osjetljivim korporativnim podacima, uključujući neke od sljedećih, s kojima se već susrelo autori tijekom konzultantskih angažmana:

1. Aplikacije za pohranu dokumenata omogućuju korisnicima pristup osjetljivim poslovnim dokumentima na zahtjev
2. Aplikacije za putovanje i troškove koje korisnicima omogućavaju stvaranje, pohranu i prijenos troškova u interne sustave
3. HR aplikacije omogućuju korisnicima pristup platnom spisku, vremenskim odmacima, informacijama o odmoru i drugim osjetljivim funkcijama

4. Aplikacije internih usluga poput mobilnih aplikacija koje su optimizirane za pružanje internih resursa poput korporativnog intraneta
5. Interne aplikacije za razmjenu trenutačnih poruka koje korisnicima omogućuju chat u stvarnom vremenu s drugim korisnicima, bez obzira na njihovo mjesto

U svim ovim primjerima aplikacije se smatraju „internim“ aplikacijama i obično se razvijaju vlastito ili posebno za organizaciju. Stoga mnoge od tih aplikacija zahtijevaju virtualnu privatnu mrežu (VPN) ili pristup unutarnjoj mreži kako bi mogle funkcionirati tako da komuniciraju s osnovnom unutarnjom infrastrukturom. [20]

5.1.Povijest

Prve aplikacije za mobilne telefone razvili su proizvođači slušalica. Dokumentacija je bila oskudna, a malo je podataka postojalo u javnoj domeni o operativnim unutrašnjostima. To se možda može pripisati strahu dobavljača da bi otvaranje platformi za razvoj treće strane moglo otkriti poslovne tajne onoga što još nije bila potpuno razvijena tehnologija.

Rane aplikacije bile su slične mnogim aplikacijama izvorno instaliranim na mobitelu, poput kontakata i kalendara, te jednostavnim igrama poput popularne Nokijine zmije. Kad su se pametni telefoni pojavili kao nasljednici osobnih digitalnih asistenata (PDA), razvoj aplikacija zaista je počeo kretati. Rast mobilnih aplikacija možda se može izravno pripisati povećanoj procesorskoj snazi i mogućnostima pametnog telefona u kombinaciji s rastućom potražnjom za funkcionalnošću koju pokreće potrošačko tržište.

Kako su se pametni telefoni razvijali, tako su mobilne aplikacije mogle iskoristiti poboljšanja platformi. Poboljšanja u sustavu globalnog pozicioniranja (GPS), kameri, trajanju baterije, zaslonima i procesoru doprinijeli su programima bogatim značajkama koje danas poznajemo. Razvoj aplikacija treće strane ostvario se 2008. godine kada je Apple najavio prvu uslugu distribucije aplikacija treće strane, App Store.

To je uslijedilo nakon prvog pametnog telefona tvrtke, iPhonea, koji je objavljen prethodne godine. Google je pomno pratio Android Market, danas poznat i kao Google Play. Danas postoji niz dodatnih tržišta distribucije, uključujući Windows Phone Store, Amazon Appstore i BlackBerry World.

Povećana konkurencija za razvoj aplikacija treće strane učinila je da su tržišta programera donekle fragmentirana. Većina mobilnih aplikacija specifična je za platformu, a dobavljači softvera prisiljeni su raditi s različitim operativnim sustavima, programskim jezicima i alatima

kako bi osigurali pokrivenost više platformi. Odnosno, iOS programi su se tradicionalno razvijali pomoću Objective-C, Android i BlackBerry aplikacija koristeći Javu i Windows Phone aplikacije pomoću .NET Framework. Ova fragmentacija često može dovesti do toga da organizacije zahtijevaju više razvojnih timova i održavaju više baza koda. Međutim, nedavno se dogodio porast u razvoju više-platformskih mobilnih aplikacija jer organizacije žele smanjiti razvojne troškove i opće troškove. Među-platformni okviri i razvoj aplikacija temeljenih na pregledniku HTML5 postali su popularni upravo iz tih razloga. [20]

5.2.Privatnost korisnika i sigurnost podataka

Na mobilne aplikacije utječe niz sigurnosnih ranjivosti, od kojih su mnoge naslijeđene od tradicionalnih napada na web i stolne programe. Međutim, nekoliko drugih klasa napada specifično je za mobilno područje i nastaje zbog načina na koji se koriste mobilne aplikacije i relativno jedinstvenih ulaznih točaka i površina napada koje te aplikacije stvaraju. Moguće površine napada na mobilnu aplikaciju kojih bi programeri trebali biti svjesni i od kojih se moraju braniti su:

1. Većina mobilnih aplikacija vrši neku vrstu mrežne komunikacije, a zbog prirode u kojoj se koriste mobilni uređaji, ta se komunikacija često može dogoditi preko nepouzdane ili nesigurne mreže, poput Wi-Fi-ja hotela ili kafića, mobilne žarišne točke ili mobilne mreže. Ako podaci nisu adekvatno zaštićeni u prijevozu, mogu izložiti aplikaciju velikom broju mogućih rizika, uključujući otkrivanje osjetljivih podataka i napade injekcijama.
2. Mobilni uređaji nose se sa sobom kamo god krenuli, stvarajući brojne mogućnosti da ih se izgubi ili ukrade. Programeri mobilnih aplikacija moraju prepoznati rizike od pokušaja oporavka podataka protiv datotečnog sustava uređaja. Bilo koji preostali sadržaj koji aplikacija ostavi na datotečnom sustavu, bilo putem trajne pohrane ili privremenog predmemoriranja, potencijalno može izložiti osjetljive podatke napadaču.
3. Scenarij koji je prilično jedinstven za mobilne aplikacije je svijest o prijetnjama koje potječu od glavnog računala. Zlonamjernog softvera ima puno u mobilnom prostoru, posebno na neslužbenim tržištima distribucije, stoga programeri moraju biti svjesni napada iz drugih aplikacija.
4. Mobilne aplikacije mogu izvući podatke iz velikog broja mogućih izvora, što stvara značajan broj mogućih ulaznih točaka. Na primjer, neuobičajeno je vidjeti da aplikacije prihvaćaju podatke jednog ili više sljedećih: komunikacija u blizini-

plaćanje (NFC), bluetooth, kamera, mikrofon, usluga kratkih poruka (SMS) i univerzalna serijska sabirnica (USB) ili brzi odgovor (QR) kod.

Najozbiljniji napadi na mobilne aplikacije su oni koji izlažu osjetljive podatke. Te su ranjivosti karakteristične za sve uređaje, a ne samo za mobitle. Iako ranjivosti na poslužitelju predstavljaju najveći rizik za implementacije mobilnih aplikacija u cjelini, jer mogu izložiti neograničen pristup pozadinskim sustavima, ti su problemi dobro dokumentirani i razumljivi.

Sigurnost mobilne aplikacije još uvijek je pogrešno shvaćena i nije sazrela u potpunosti kao područje fokusa te se većina mobilnih aplikacija i dalje smatra nesigurnima.

Utvrđeno je da na postotak mobilnih aplikacija testiranih od 2012. najčešće utječu neke uobičajene kategorije ranjivosti na strani klijenta:

1. Nesigurna pohrana podataka (63%) - Ova kategorija ranjivosti uključuje razne nedostatke koji dovode do toga da aplikacija pohranjuje podatke na mobilni uređaj u jasnom tekstu, zamućenom formatu, koristeći kodirani ključ ili bilo kojim drugim sredstvima koje napadač lako može poništiti.
2. Nesigurni prijenos podataka (57%) - To uključuje bilo koji primjer u kojem aplikacija ne koristi šifriranje transportnog sloja za zaštitu podataka u prijenosu. Također uključuje slučajeve u kojima se koristi šifriranje transportnog sloja, ali je provedeno na nesiguran način.
3. Nedostatak binarne zaštite (92%) - Ovaj nedostatak znači da aplikacija ne koristi bilo koji oblik zaštitnog mehanizma koji komplicira obrnuti inženjering, zlonamjerno miješanje ili uklanjanje pogrešaka.
4. Ubrizgavanje na strani klijenta (40%) - Ova kategorija ranjivosti opisuje scenarije u kojima se nepouzdani podaci šalju aplikaciji i njima se rukuje na nesiguran način.
5. Tvrdo kodirane lozinke / ključevi (23%) - Ova greška nastaje kada programer u aplikaciju ugradi osjetljiv podatak poput lozinke ili ključa za šifriranje.
6. Propuštanje osjetljivih podataka (69%) - To uključuje slučajeve kada aplikacija nenamjerno propušta osjetljive podatke kroz bočni kanal, što posebno uključuje curenje podataka koje nastaju korištenjem okvira ili OS-a i događaju se bez znanja programera.[20]

5.2.1. Dozvole aplikacija

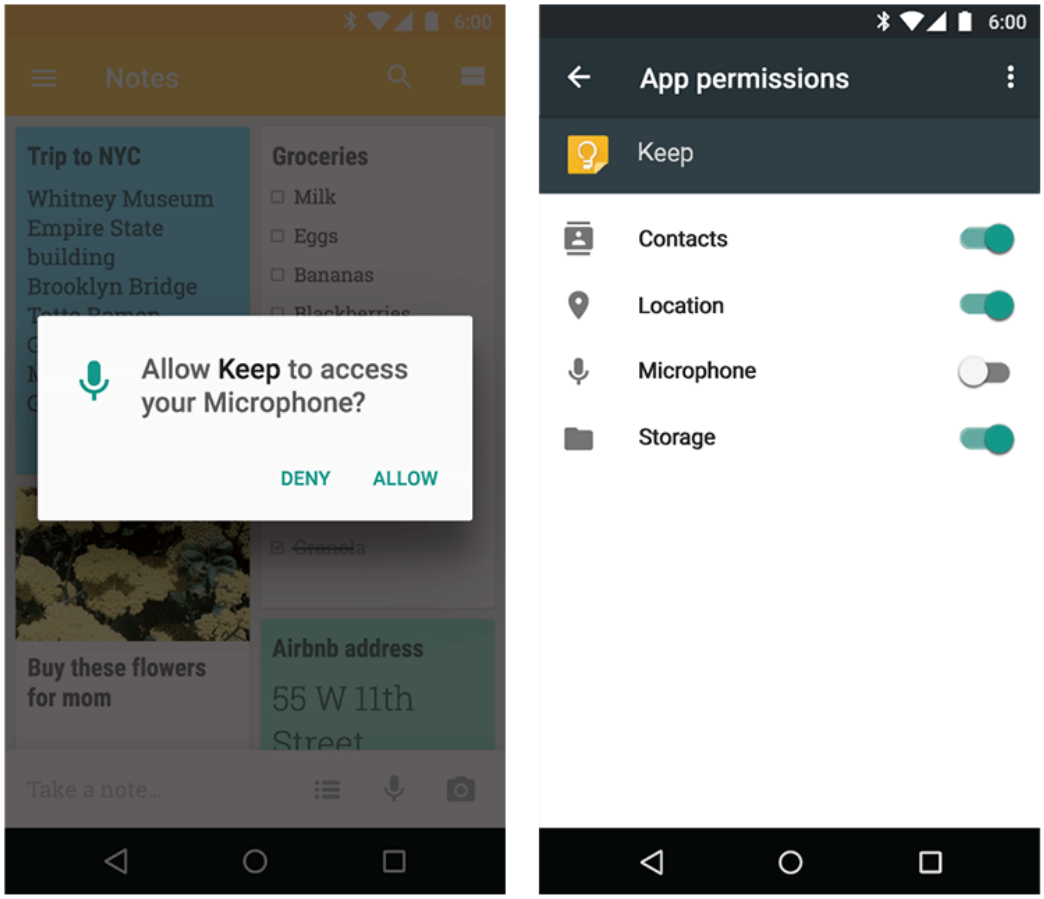
Dozvole štite privatnost korisnika i pružaju transparentnost o tome kojim resursima ili informacijskim aplikacijama žele pristupiti. Da bi aplikacije mogle pristupiti značajkama sustava, poput kamere i weba, ili korisničkim podacima, poput kontakata i SMS-a, aplikacija

mora izričito zatražiti dopuštenje. Te su upute za dopuštenje dizajnirane tako da korisnik ima jasnu vidljivost zahtjeva i mogućnost da ga odobri ili odbije.

Središnja točka dizajna sigurnosne arhitekture je da niti jedna aplikacija prema zadanim postavkama nema dopuštenje za sprečavanje bilo kakvih operacija koje bi imale negativan utjecaj na druge aplikacije, operativni sustav ili korisnika. To uključuje čitanje ili pisanje korisnikovih privatnih podataka (poput kontakata ili e-pošte), čitanje ili pisanje datoteka druge aplikacije, nesmetan pristup mreži, držanje uređaja budnim i druge.

Dijaloški okviri dopuštenja za aplikacije zahtijevaju od korisnika odobrenje pristupa navedenom dopuštenju. Ovaj pristup pojednostavljuje postupak instalacije i ažuriranja aplikacije, jer korisnik ne mora dodijeliti dozvole kada instalira ili ažurira aplikaciju. Također daje korisniku veću kontrolu nad funkcionalnošću aplikacije; na primjer, korisnik bi mogao odabrati da aplikaciji kamere omogući pristup kameri, ali ne i mjestu uređaja. Korisnici mogu opozvati dozvole u bilo kojem trenutku.

Neke novije verzije operativnih sustava uključuju poboljšanja koja korisnicima omogućavaju kontrolu nad upotrebom identifikatora. Trajni identifikatori uređaja osjetljivi na privatnost više nisu dostupni ili se nalaze iza dozvole za izvršavanje. (Slika 17) [26]



Slika 17.Primjer dijaloškog okvira za dopuštenje aplikacija [25]

5.2.2 Biometrijski podaci

Podaci mobitela predstavljaju osjetljivo područje jer napadač može stvoriti percepciju o identitetu osobe, kao što je ime, adresa e-pošt, adresa i slično. Ovi podaci u stvarnosti e smatraju vrlo osjetljivim i ne smiju se otkriti nepouzdanoj strani. Korisniku pametnog telefona neovlašteno otkrivanje njezinog identiteta može otkriti puno privatnih podataka o njoj kao što je i zdravstveno stanje, spolna orijentacija i slično.

Ispravna identifikacija korisnika bitan je uvjet za pouzdanu kontrolu pristupa i kao takav ključni je pokretač elektroničke trgovine. Provjera identiteta odnosno autentičnosti u računalnim sustavima tradicionalno se temelji na nečemu što netko ima (ključ, magnetska ili čip kartica) ili što zna (PIN, lozinka).

Biometrija se temelji na principu mjerljivih fizioloških karakteristika ili karakteristika ponašanja poput otiska prsta ili uzorka glasa. Biometrijski sustavi mogu se koristiti u dva različita načina:

1. Provjera identiteta- prvi način je provjera identiteta te se ona događa kada korisnik tvrdi da je već upisan u sustav (predstavlja osobnu iskaznicu ili ime za prijavu). U ovom se slučaju biometrijski podaci dobiveni od korisnika uspoređuju s podacima korisnika koji su već pohranjeni u bazi podataka.
2. Identifikacija- naziva se i pretraživanjem, prepoznavanjem ili usporedbom jedan-prema-više. Događa se kada je identitet korisnika a priori nepoznat. U ovom se slučaju korisnički biometrijski podaci uspoređuju sa svim zapisima u bazi podataka, jer korisnik može biti bilo gdje u bazi podataka ili zapravo uopće ne mora biti tamo.

Autentifikacija je obično preduvjet autorizacije (za prijavu, pristup datotekama, ulazak u zrakoplov itd.). Iako je biometrijska provjera autentičnosti privlačna jer prvenstveno ovjerava korisnika (a ne nešto što se može otkriti ili proslijediti kolegi), njezini se nedostaci odnose na probleme s točnošću, zaštitom privatnosti, tajnošću biometrijskih podataka, a time i na potrebi za pouzdanim ispitivanje živosti. Prije nego što sustav može uspješno provjeriti ili identificirati korisnika, ona mora biti registrirana u biometrijskom sustavu. Korisnički biometrijski podaci se snimaju, obrađuju i pohranjuju, a proces registracije korisnika u biometrijski sustav naziva se upisom.

U osnovi postoje dvije vrste biometrijskih sustava:

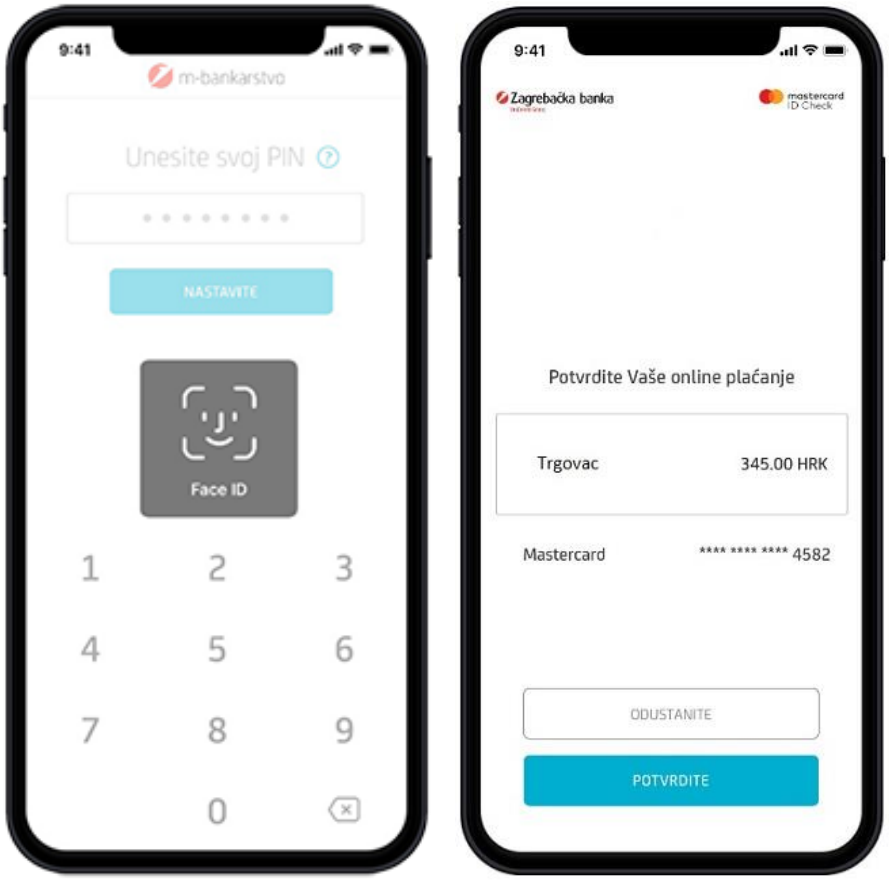
1. Automatizirani sustavi za identifikaciju kojima upravljaju profesionalci (npr. Policijski automatizirani sustavi za identifikaciju otiska prsta - AFIS)- svrha takvih sustava je identificirati dotičnu osobu ili pronaći počinitelja kaznenog djela prema tragovima ostavljenim na mjestu zločina. Upisani korisnici obično nemaju pristup takvim sustavima, a operateri takvih sustava nemaju puno razloga za varanje.
2. Biometrijski sustavi za provjeru autentičnosti koji se koriste za kontrolu pristupa- ti se sustavi koriste običnim korisnicima kako bi stekli privilegiju ili pravo pristupa, te se ovdje primarno radi o pametnim telefonima. Osiguranje takvog sustava puno je složeniji zadatak, a primjer takvog sustava vidljiv je u nastavku. (Slika 19) [30]

Slika 18.Primjer autentifikacije osobe [31]

Primarna prednost metoda biometrijske provjere autentičnosti u odnosu na druge metode provjere autentičnosti korisnika je u tome što oni stvarno rade ono što bi trebali, tj. autentificiraju korisnika te se ne oslanjaju na predmete koje korisnik nosi. Biometrijske metode autentifikacije koriste stvarne ljudske fiziološke ili bihevioralne karakteristike za autentifikaciju korisnika. Biometrijska provjera autentičnosti ima i neke druge prednosti. Većina biometrijskih tehnika temelji se na nečemu što se ne može izgubiti ili zaboraviti. To je prednost za korisnike kao i za administratore sustava jer se može izbjeći upravljanje izgubljenim, ponovno izdanim ili privremeno izdanim tokenima / karticama / lozinkama.

Izvedba biometrijskih sustava nije još idealna te biometrijske sustave još treba poboljšati u smislu točnosti, a ponekad i brzine. Karakteristike biometrije ne bi se trebale niti duplicirati, ali nažalost često je moguće stvoriti kopiju koju biometrijski sustav prihvaća kao pravi uzorak pa se na taj način može zloupotrijebiti nečiji mobitel. [30]

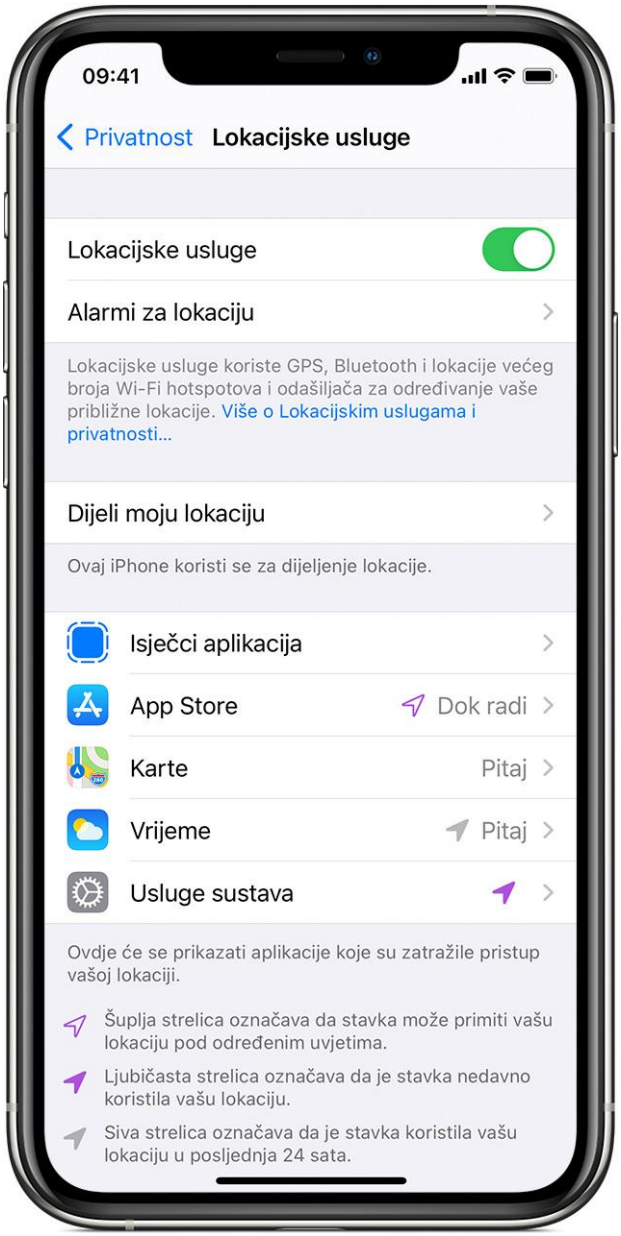
Biometrija je rastući sustav identifikacije i zaštite po pitanju raznih aplikacija, dok je jedna od aplikacija najviše sklona riziku, obzirom da se radi o novcu, prikazana u nastavku. (Slika 19)



Slika 19. Primjer biometrije pri plaćaju mobitelom u aplikaciji Zagrebačke banke [32]

5.2.3 Geolokacijski podatci

Prema istraživanju iz 2008 godine tvrtke HPE Security Fortify, moderne mobilne aplikacije prikupljaju, prenose i pohranjuju širok spektar podataka koji često nisu potrebni za funkciju aplikacije, a mogu prouzročiti značajnu financijsku i reputacijsku štetu ako se ranjivost iskoristi. S obzirom na sve veći interes napadača za mobilnim uređajima, presudno je da programeri od samog početka ugrade sigurnost u aplikacije, a organizacije proaktivno pristupe sigurnosti podataka kako bi bolje zaštitile osobne i korporativne podatke. Iz tog razloga, kako je već rečeno u dozvolama za aplikacije, na svakome je mobitelu moguće ograničiti domet lokacije u aplikacijama, te upravljati svakom pojedinom komponentom. (Slika 18) [27]



Slika 20. Primjer upravljanja lokacijskim uslugama na iOS operativnom sustavu [2]

Najvažniji nalazi iz izvješća govore kako većina mobilnih aplikacija prati lokaciju, iako to nije nužno. Više od 50 posto skeniranih aplikacija pristupilo je podacima o geolokaciji. To može stvoriti ozbiljne implikacije na privatnost u slučaju napada, jer napadač može dobiti pristup fizičkom mjestu inače anonimnih, nesumnjivih korisnika. Iako za prometnu aplikaciju ima smisla pratiti lokaciju, studija je otkrila da je to učinilo i više od 70% obrazovnih aplikacija na iOS-u, što je uznemirujuće jer se obrazovni programi često prodaju djeci. [27]

Najnoviji sistem prepoznavanja lokacije korisnika više se ne oslanja na davatelja mobilnih usluga koji će izvršiti traženje lokacije, već Google putem interneta na svoj poslužitelj za geolokaciju šalje ID kako bi utvrdio lokaciju korisnika. Lokacija vraćena na mobitel korisnika

prenosila bi se zatim na poslužitelj Google Maps kako bi trenutna lokacija korisnika bila prikazana kao "čarobni plavi krug" na karti trenutnog okruženja. Ova metoda određivanja lokacije mobitela korisnika značajno se razlikuje od prethodnih pristupa. Umjesto pasivnog pristupa ili oslanjanja na davatelja infrastrukture koji će ponuditi mjerodavan odgovor, prihvaćen je interaktivni pristup temeljen na podacima, koji ilustrira moderni lokacijski pristup. Softver Google Maps Mobile nudi mogućnost onemogućavanja značajke "Moja lokacija".

Osim primarno mobilnih geolokacijskih usluga, veliku ulogu igraju i WiFi tehnologije na koje se uređaji spajaju. WiFi geolokacijske tehnologije koriste prednost popularnosti, sveprisutnosti i široke primjene bežičnih mreža IEEE 802.11 u urbanim područjima, u domovima, tvrtkama i institucijama.

Usluge geolokacije WiFi-a djeluju hvatanjem jedinstvenih identifikatora bežičnih pristupnih točaka, nazvanih identifikatorima osnovnih servisnih skupova, koje emitira svaki identifikatora bežičnih pristupnih točaka unutar radio dometa. Ovi se identifikatori zatim traže u bazi podataka koja ih preslikava na zemljopisne lokacije. Time identifikacijska baza podataka može točno odrediti mjesto mobilnog uređaja. WiFi geolokacija postaje popularna zbog prednosti koje nudi u odnosu na druge metode geolociranja. Usluge geolociranja WiFi-a nude brzo vrijeme popravljanja, kašnjenje između uključivanja usluge i utvrđivanja vašeg mjesta, manje od sekunde u usporedbi s približno trideset sekundi GPS-a. Te usluge također djeluju mnogo učinkovitije u zatvorenim i urbanim područjima, gdje su stanični ili GPS signali loši ili nedostupni.

Mobilni uređaji, iako možda najmanje uključeni u stvarno pružanje tehnologija temeljenih na lokaciji, služe kao platforma za korištenje aplikacija i usluga temeljenih na lokaciji i tako mogu igrati važnu ulogu u određivanju sigurnosnog rizika povezanog s korištenjem tehnologija temeljenih na lokaciji. [28]

5.2.4 Kolačići

Kolačić je datoteka koja sadrži informacije specifične za korisnika, koji prolazi kroz Internet protokol poput web preglednika (ili mobilnog web preglednika) i pohranjuje se na uređaju osobe. Međutim, Propisi se primjenjuju na bilo koju opremu koja se koristi za „pohranu ili pristup informacijama pohranjenim u terminalnoj opremi“. U mobilnim uređajima pohrana takve vrste podataka može se dogoditi putem različitih tehnoloških kanala. Osim mobilnih web preglednika, uključuje i osobne podatke pohranjene u aplikacijama.

Aplikacije nude jednu značajnu pogodnost u pogledu usklađenosti; kada korisnik prvi put otvori aplikaciju nakon preuzimanja ili prije preuzimanja, od njega se može tražiti da prihvati skup uvjeta i odredbi u kojima se može dobiti pozitivan pristanak na upotrebu kolačića ili druge tehnologije praćenja.

Apple je prethodno dopuštao praćenje u aplikacijama putem jedinstvenog koda uređaja ili jedinstvenog identifikatora uređaja (UDID). Iako to više ne namjeravaju staviti na raspolaganje programerima aplikacija za praćenje, važno je napomenuti da bi svaki jedinstveni uređaj za praćenje, poput UDID-a, trebao pozitivan pristanak prema Propisima. [33]

Većina kampanja digitalnog oglašavanja izvršenih na stolnim uređajima isporučuje se putem preglednika. Međutim, na mobilnim uređajima korisničko je iskustvo više fragmentirano. Korisnici pregledavaju web putem mobilnih preglednika, ali također instaliraju niz aplikacija koje mogu sadržavati i oglase. Sposobnosti praćenja kolačića razlikuju se u različitim okruženjima, stoga razlikujemo kolačiće prve i treće strane. "Kolačić prve strane" odnosi se na kolačić čija je domena ista kao i domena posjećene web stranice, dok se "Kolačić treće strane" odnosi na onoga čija se domena razlikuje od posjećene web stranice.

Unutar mobilnih aplikacija, web prikazi se koriste za prikaz internetskih sadržaja poput web mjesta ili oglasa. Kolačići se mogu pohraniti u internetskom prikazu slično načinu na koji se pohranjuju u postavkama preglednika. Internetski pregled (i, prema tome, pohranjeni kolačići) jedinstven je po aplikaciji. Na isti način na koji preglednici Chrome i Firefox ne dijele kolačiće na uređaju, mobilne aplikacije ne mogu dijeliti podatke o kolačićima međusobno ili s mobilnim web preglednikom uređaja.

Svaka aplikacija ima svoj privatni prostor na uređaju, koji se obično naziva „sandbox“ okruženje. Ovo okruženje u zaštićenom okruženju ograničava mogućnost aplikacije za pristup podacima iz drugih aplikacija. Aplikacija i dalje može pohranjivati i pristupati podacima u samoj aplikaciji, ali je zabranjeno prikupljanje podataka iz bilo koje druge aplikacije na uređaju.

Zbog toga oglašivači ne mogu pratiti korisnika od aplikacije do aplikacije na temelju kolačića na isti način na koji mogu pratiti ponašanje u prozoru preglednika, što svakako povećava sigurnost uređaja. [34]

5.2.5.Ostale prijetnje

Sigurnosne prijetnje mobilnim uređajima nepredvidive su i raznolike. Osim svih navedenih prijetnji, sigurnosne prijetnje pametnim mobilnim uređajima mogu biti i:

1. Gubitak ili krađa mobilnog uređaja
2. Neovlašten pristup uređaju
3. Nesvjesna pohrana podataka na neupravljane podatkovne (Cloud) servise
4. Iskorištavanje sigurnosnih propusta operativnih sustava ili aplikacija
5. Zlonamjerne mobilne aplikacije
6. Zlonamjerno presretanje podataka između uređaja
7. Zlonamjerno presretanje osjetljivih podataka između aplikacija na uređaju [7]

S obzirom na brojne sigurnosne prijetnje, sustavna zaštita mobilnih uređaja i njihovog pristupa podacima je imperativ te je važno povećati svijest korisnika te ih educirati o metodama zaštite, o čemu će biti više govora u nastavku.

5.3.Svijest korisnika o rizicima

Koristeći pametne telefone na dnevnoj razini koristimo i aplikacije koje se na njima nalaze. Bile one početne aplikacije s kojima je uređaj došao ili pak one skinute aplikacije, u svome opusu imaju dozvole koje je potrebno označiti kako bi se aplikacija koristila. Kada aplikaciju dobijemo zajedno sa uređajem, dozvole su već unaprijed označene, stoga dosta često kod ovih aplikacija rizik za sigurnost nije očit.

Osim obavljanja zadaća kojima su pojedinačne aplikacije namijenjene, kao primjerice svjetiljka, kompas, kalkulator, budilica i slično, one također u pozadini obavljaju radnje te prikupljaju različite vrste podataka o korisniku.

Istraživanja iz 2015. godine pokazala su kako korisnici vrlo često nisu svjesni količine podataka koji se tako prikupljaju, te da se isti mogu zlouporabiti i u kojoj mjeri to predstavlja potencijalnu opasnost za sigurnost korisnika. U uzorku od 237 studenata preddiplomskog i diplomskog studija na tri visokoškolske institucije u Hrvatskoj, 2017. godine provedeno je novije istraživanje o svjesnosti korisnika o rizicima mobilnih telefona.

Dobiveni rezultati pokazali su da gotovo polovica ispitanika, neovisno o vrsti završenog srednjoškolskog obrazovanja i vrsti upisanog studijskog obrazovanja ne obraća pozornost na dozvole koje daje aplikacijama prilikom instaliranja. Rezultati govore kako izrazito veliki broj

ispitanika dozvole daje automatski te davanje dozvole ne promatra kao upozorenje, već korake koje je jednostavno potrebno obaviti.

Sukladno tomu iznenađuju podaci da su ispitanici djelomično zabrinuti ili zabrinuti radi podataka koje aplikacije prikupljanju na njihovim pametnim telefonima i radi toga što aplikacije prikupljaju previše privatnih podataka. Ta je zabrinutost nešto izraženija kada je riječ o prikupljanju osobnih podataka.

Veliki dio ispitanika (66,4%) tvrdi kako je odustao od instaliranja aplikacija zbog dozvola koje su bile potrebne, dok mali dio ispitanika tvrdi kako to nije učinio (18,4) ili pak nije siguran dali je to učinio (15,2), što govori u prilog činjenici da dozvole gotovo i ne primjećuju.

U slučaju postajanja mogućnosti davanja pojedinačnih dozvola većina bi ispitanika koristila tu mogućnost. Također, na pitanje o tome koje ih dozvole brinu ili ne brinu, najmanje ih brinu dozvole koje uključuju pristup kalendaru i mogućnost da aplikacija šalje obavijesti dok bi najviše njih zabranilo pristup SMS porukama, lokacijskim podacima i kontaktima jer ih smatraju svojim privatnim podacima. [23]

Među glavnim čimbenicima koje su sudionici spomenuli bili su:

1. fizički gubitak telefona (propadanje i krađa)
2. fizičko oštećenje
3. gubitak podataka i (nedostatak) sigurnosne kopije
4. jačina prijema / signala
5. život baterije
6. aplikacije s povjerenjem

17 osoba izrazila je zabrinutost zbog gubitka telefona, zabrinutost od štete izrazilo je 11 osoba i gubitka podataka 5 osoba. Osobe su često motivirane brigom o sigurnosti i privatnosti, a ne samo zbog neugodnosti ili novčanog gubitka telefona. [24]

6. METODE ZAŠTITE

Danas postoji jako puno aplikacija za pametne telefone koje povećavaju njegovu sigurnost. Jedna od prvih, boljih i najpoznatijih svakako je aplikacija „Lookout“. „Lookout“ je jedna od najpoznatijih sigurnosnih aplikacija za pametne telefone koja štiti nadgledajući aplikacije, obzirom da se one smatraju najvećim sigurnosnim rizikom pametnih telefona.[12]

Sigurnosna i antivirusna aplikacija „Lookout“ pruža besplatne značajke kao što su:

1. Skeniranje aplikacija- Neprekidna i bežična zaštita od virusa, štetnih softvera, programa s neželjenim oglasima i špijunskih softvera
2. Pronalazak mobitela- moguće je pronaći svoj mobitel te reproducirati zvuk čak i u bešumnom načinu rada.
3. Slanje signala o posljednjem zabilježenom položaju- aplikacija automatski bilježi položaj telefona kada je baterija skoro prazna
4. Savjetnik za sustav- Provjerava izvorni kod uređaja kako bi bio siguran da operativni sustav ispravno radi. [35]

Kada korisnik instalira određenu aplikaciju, aplikacija „Lookout“ provjerava aplikaciju sa svojom bazom – „Lookout Mobile Threat Network“, koja sadržava više od milijun mobilnih aplikacija i najveća je takva baza u svijetu.

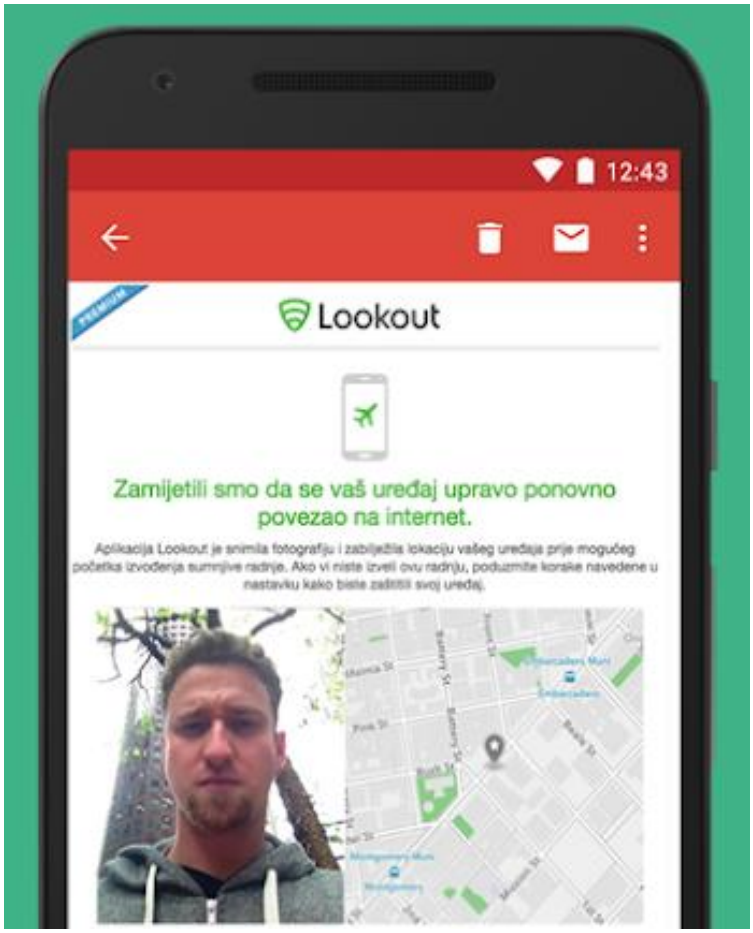
„Aplikacije u ovoj bazi stalno se provjeravaju kako bi se pronašle nepravilnost u njihovom radu. Kada se nepravilnost otkrije, svi pametni telefoni s Lookout aplikacijom dobivaju obavijest o potencijalnoj opasnosti. U svom osnovnom, besplatnom paketu, uz nadgledanje aplikacija, Lookout ima i neke druge sigurnosne mogućnosti. Jedna od njih je „Find My Phone“ mogućnost koja korisniku olakšava pronalaženje svog pametnog telefona, a za pronalazak se koristi Google Maps i GPS. Još jedna mogućnost koja dolazi besplatno s aplikacijom je „Backup and Restore“ mogućnost s kojom korisnik može pohraniti svoje osjetljive podatke na sigurno mjesto. Ukoliko korisnik izgubi svoj telefon, na novi pametni telefon može vrlo jednostavno dohvatiti sve podatke koje je prethodno pospremio.“

U premium verziji aplikacije otvaraju nove mogućnosti koje dodatno osiguravaju pametni telefon:

1. „sigurno pretraživanje Interneta,
2. povećana zaštita privatnosti,

3. udaljeno zaključavanje uređaja i brisanje podataka (jako korisno u slučaju krađe uređaja) i
4. poboljšana „Backup and Restore“ mogućnost.“[12]

Aplikacija „Lookout“ trenutno ima preko 100 milijuna skidanja te je jedna od najpopularnijih sigurnosnih aplikacija. Interesantna značajka ove aplikacije je i snimanje fotografije te slanje obavijesti prilikom sumnjive prijave sa sumnjive lokacije. (Slika 21) [35]

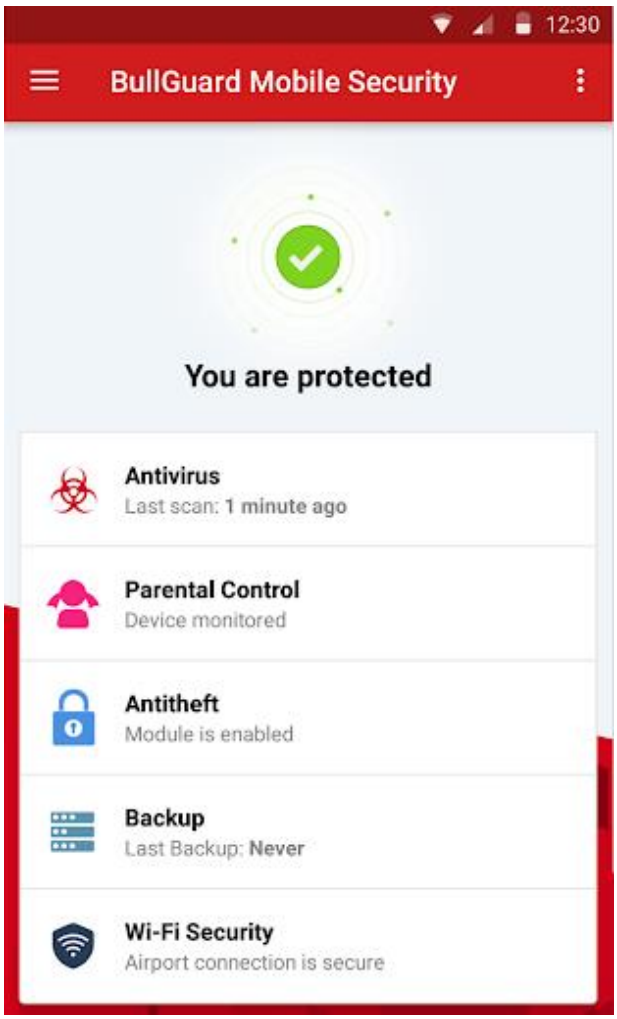


Slika 21.Primjer obavijesti za sumnjivu prijavu na aplikaciji "Lookout" [35]

Među najboljim sigurnosnim aplikacijama nalazi se i aplikacija „BullGuard Mobile Security 10“. Ova aplikacija dostupna je za većinu operacijskih sustava te podržava mogućnosti kao što su:

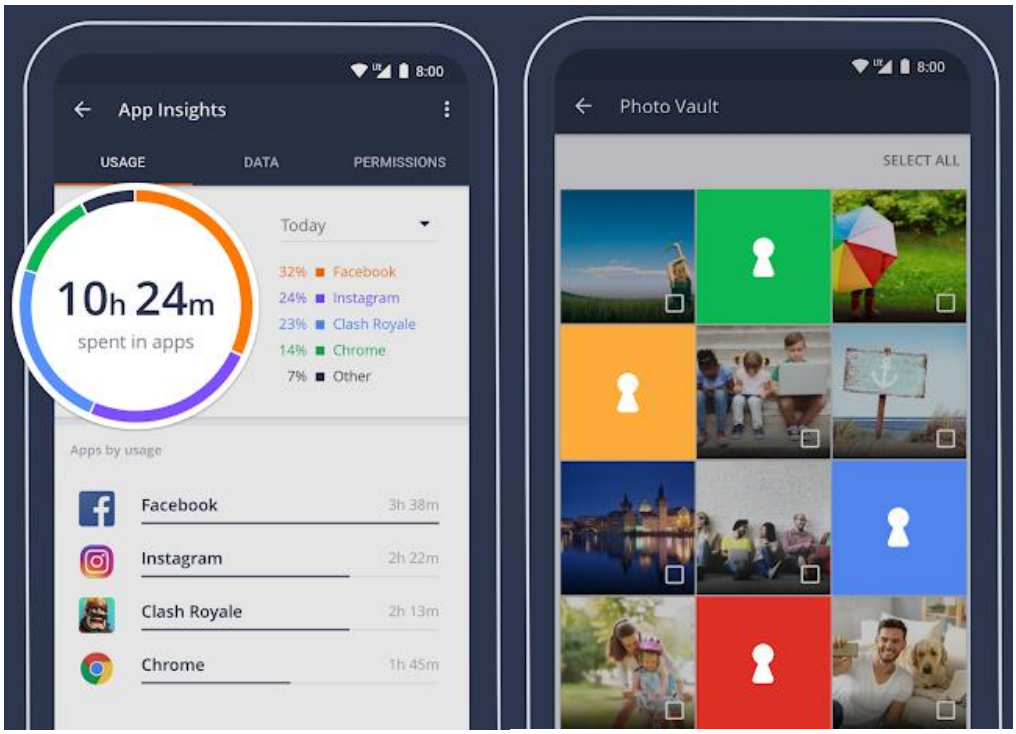
1. Antivirus - zaustavlja viruse, špijunski softver, adware, trackware u izvanmrežnom načinu rada
2. Protiv krađe - zaključava, pronalazi i briše podatke u slučaju gubitka ili krađe uređaja na daljinu
3. SIM zaštita - automatski zaključava uređaj ako se SIM ukloni, uključuje opcionalno brisanje podataka na daljinu

4. Sigurnosna kopija - jednostavna sigurnosna kopija jednim dodirom kako biste zaštitili svoje podatke
5. Mobile Security Manager - mrežna platforma za daljinsko upravljanje uređajem i nadzor nad njim. Budući da se BullGuard sastoji od aplikacije koja je instalirana na uređaju i web usluge kojoj se može pristupiti putem računala, uvijek je prisutna potpuna kontrolu čak i ako uređaj nije kod korisnika, odnosno na daljinu.
6. Security Wi-Fi sigurnost- Pokreće upozorenje svaki put kad se povežete na nezaštićeni Wi-Fi te prati ranjive Wi-Fi veze koje su uspostavljene u posljednjih 30 dana. [36]
7. Roditeljska zaštita
8. Anti-spam zaštita,
9. Karantena zloćudnih programa
10. Vatrozid,
11. Blokiranje određenih brojeva. [12]



Slika 22.Sučelje BullGuard aplikacije [36]

Proizvođači antivirusnih programa za računala Norton i AVG također imaju besplatne mobilne inačice svojih antivirusnih alata koje pružaju zaštitu od zloćudnih programa skeniranjem uređaja na isti način kao u izvornim inačicama na računalima. Pružaju većinu značajki kao i prethodno navedene apikacije, dok osim toga nude i pregled najčšće korištenih aplikacija te zaštitu željenih fotografija. (Slika 23) [12]



Slika 23. Primjer sigurnosnih opcija AVG antivirusne aplikacije [37]

Većina ovih aplikacija namijenjena je za Android i ostale uređaje, obzirom da se smatra kako iPhone uređaji imaju dovoljno dobru sigurnost, stoga nije potrebno instalirati dodatnu programsku podršku. Sa strane proizvođača također je veći fokus na operacijske sustave za koje postoji više zloćudnog programa jer to znači da će više korisnika preuzeti i instalirati njihovu aplikaciju. U slučaju iOS sustava najčešće se radi o aplikacijama za:

1. „Sigurnije pretraživanje Interneta (npr. Webroot SecureWeb Browser, Smart Surfing),
2. Provjeru datoteka koje korisnik dohvaća s web stranica ili kao privitke elektroničke pošte (npr. Intego VirusBarrier),
3. Udaljeno zaključavanje uređaja (npr. iLocalis),
4. Udaljeno brisanje podataka s uređaja (npr. Lookout),
5. Pronalaženje izgubljenog uređaja pomoću GPS-a (npr. Lookout, GadgetTrak, iLocalis),
6. Pohranjivanje podataka tj. backup (npr. Lookout, McAfee WaveSecure iOS Edition),
7. Vatrozid (npr. Firewall iP) i sl.“ [12]

7. ZAKLJUČAK

Današnji svijet gotovo je nezamisliv bez mobilnih uređaja, što je sredinom prošlog desetljeća bilo nezamislivo, a mnogi su smatrali kako je sam razvoj prvih mobilnih uređaja gotovo nemoguć. Danas telefoni služe i kao zamjena za GPS navigator, digitalni fotoaparat ili videokameru, za slušanje muzike i slično. Današnji pametni telefoni imaju mnogo više značajki nego ranije, stoga je i njihova sigurnost sada puno ugroženija.

Svaki mobitel može biti na meti napadača, jer je mobitela sve više, imaju stalnu vezu s internetom, kroz njih se dijeli sve više podataka, između ostalog i bankovnih, te ih ljudi nose svuda sa sobom. Korisnici se često i previše pouzdaju u svoj uređaj, te je baš iz tog razloga svaki mobitel zanimljiv napadaču. Napadači podatke potom koriste za špijuniranje korisnika ucjenu ili prodaju korisničkih informacija kao što je primjerice adresa elektroničke pošte.

Po pitanju mobilnih komponenti, svaka komponenta sa sobom donosi određene sigurnosne rizike, obzirom da svaka od njih sprema određeni dio podataka, te ih koristi ovisno o dozvoli koju za to dobije. Čest je slučaj pritom da je zatražena dozvola koja nije nužno potrebna za određenu aplikaciju ili komponentu.

Osim njih, aplikacije same po sebi donose rizik zloupotrebe, pogotovo radi čestog povezivanja aplikacija te skupnih dozvola koje one traže. Dozvole i jesu jedan od većih problema sigurnosti na mobitelima obzirom da ih često čitamo površno te potvrđujemo bez daljnjeg razmatranja, što naposljetku dovodi do velikih rizika za sigurnost uređaja. Središnja točka dizajna sigurnosne arhitekture je da niti jedna aplikacija prema zadanim postavkama nema dopuštenje za sprečavanje bilo kakvih operacija koje bi imale negativan utjecaj na druge aplikacije, operativni sustav ili korisnika.

Osim toga, operacijski sustavi zbog tržišnog natjecanja i želje da se novi proizvod izda prije konkurentskog, često nisu dovoljno ispitani sa stajališta sigurnosti, čime se stavlja u pitanje početna sigurnost jezgre operacijskog sustava jer sigurnost cijelog sustava ovisi o sigurnosti najslabijeg dijela.

Obzirom da su dva glavna operacijska sustava, Android i iOS, njihove su značajke najčešće promatrane. Android je otvorena platforma, a osiguranje otvorene platforme zahtijeva jaku sigurnosnu arhitekturu i rigorozne sigurnosne programe. Android je dizajniran s višeslojnom sigurnošću koja je dovoljno fleksibilna da podržava otvorenu platformu, a istovremeno štiti sve korisnike platforme. Neovisno o tome Android se ipak smatra manje sigurnom

platformom, stoga se uz njega preporuča koristiti neki od antivirusnih aplikacija koje se nude na Google play-u.

Kod iOS-a je teže povezivanje s drugim uređajima, kao primjerice računalima koji mogu biti prijenosnici zlućudnog koda, zbog čega je i napad ograničen. Zlućudni programi za iPhone postoje, ali napadaju samo namjerno otključane uređaje koji su napravljeni kako bi zaobišli Apple-ovu zaštitu, te je jedino na otključane iPhone uređaje moguće instalirati programsku podršku koju Apple nije prethodno dozvolio, što ujedno uzrokuje povećani rizik od napada.

Zaključno tome, jasno je kako je po pitanju operacijskih sustava Iphone sigurniji po pitanju samog sustava, dok Android boljku otvorenog sustava nadoknađujem odličnim aplikacijama za zaštitu, što ga dovodi na prvo mjesto po broju korisnika, gdje prednjači sa udjelom od čak 84.8%. Može se pretpostaviti da u ovom slučaju korisnicima više odgovara sloboda odabira sigurnosnog sustava, no ovdje je vjerojatno prije riječ o većoj personalizaciji uređaja, obzirom na podatke istraživanja koja govore kako korisnici i nisu previše odgovorni prema zaštiti svog uređaja. Naime velik broj korisnika izražava zabrinutost prema podacima o krađi podataka i uređaja, ali u stvarnom životu ne koriste opcije dostupne za zaštitu svog uređaja. Osim toga, zabrinjavaju ih i kolačići dok često iste niti ne pročitaju već automatski potvrđuju.

Po ovome sa daje zaključiti kako su korisnici sve više svjesni opasnosti i rizika sigurnosti mobilnih uređaja , no kada je riječ o primjeni većih razina sigurnosti u praksi ne pridaju tome previše pažnje. Ovaj podatak donekle je razumljiv, gledajući primjere iz vlastitih života. Iako smo svi svjesni da određeni rizici postoje, često nismo previše oprezni kakve dozvole dajemo aplikacijama ili stranicama, te na koji način i kome dajemo svoju lozinku jer smatramo kako neće nitko napadati baš naš uređaj.

Obzirom na to da danas mobiteli sa nama idu svuda, smatram da je ovom problemu potrebno posvetiti više pažnje, te poraditi na edukaciji korisnika svih operacijskih sustava, kako bi ne samo bili svjesni rizika koje korištenje uređaja donosi, već kako bi ih se obrazovalo o metodama i načinima zaštite, ne samo uređaja, nego u ovome slučaju i vlastitog identiteta.

POPIS LITERATURE

[1] Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. http://www.enciklopedija.hr/Natuknica.aspx?ID=58904 Pristupljeno 05. 2. 2021.

[2] Teoretska podloga rada informacijskih sustava, https://www.weboteka.net/fpz/Informacijski%20sustavi%20mrežnih%20operatera/03_-_Teoretska_podloga_rada_informacijskih_sustava.pdf

[3] Automatski sustavi, Fakultet prometnih znanosti. Skripta s predavanja; https://www.fpz.unizg.hr/ztos/AUTOM/3autom-sustavi.pdf pristupljeno 05.02

[4] Pavlić M., Informacijski sustavi, Školska knjiga, Zagreb, 2011

[5] L. Whitten, J.; D. Bentley, L.: Systems Analysis and Design Methods, McGraw-Hill/Irwin, USA, 2007

[6] Integrirani okvir za sigurnost i pouzdanost, CIS; https://www.cis.hr/www.edicija/Integriraniokvirzasigurnostipouzdanost.html ;pristupljeno 05.02.2021

[7] Peraković D, Cvitić I. ,Sigurnost i zaštita informacijsko komunikacijskog sustava, Zagreb, 2017; http://e-student.fpz.hr/Predmeti/S/Sigurnost_i_zastita_informacijsko_komunikacijskog_sustava/Materijali/SZIKS_-_P01-P02-S01-P03-P4-P5-S02-P06-P07-S03-P08-P9-S04.pdf ;pristupljeno 06.02.2021

[8] A. Klaić, A. Perešin – Koncept regulativnog okvira informacijske sigurnosti; https://bib.irb.hr/datoteka/521742.AK_AP_Koncept_regulativnog_okvira_inf_sig_DKU_032011.pdf ; pristupljeno 06.02.2021

[9] Ministarstvo unutarnjih poslova; https://mup.gov.hr/print.aspx?id=175295&url=print ;pristupljeno 06.02.2021

[10]Zavod za sigurnost informacijskog sustava; https://www.zsis.hr/default.aspx?id=346 pristupljeno 06.02.2021

[11]Panian Ž., Poslovna informatika za ekonomiste, Masmedia, Zagreb, 2005

[12] Centar Informacijske Sigurnosti, Programi za zaštitu pametnih telefona, Zagreb, 2011, http://larra2.lss.hr/CIS-novi/files/dokumenti/CIS-DOC-2011-12-034.pdf pristupljeno 07.02.2021

[13] https://sushiandbox.ru/hr/rabota-v-internete/samsung-s6-kak-otkryt-kryshku-kak-otkryt-zadnyuyu-kryshku-telefona.html pristupljeno 07.02.2021

[14] https://www.androidmobitel.com/mobiteli/kako-promijeniti-postavke-za-otkrivanje-vase-lokacije-na-androidu/ pristupljeno 07.02.2021
[15] Centar Informacijske Sigurnosti, Ispitivanje sigurnosti mobilnih aplikacija, Zagreb, 2011; https://www.cis.hr/files/dokumenti/CIS-DOC-2011-11-CIS-030.pdf pristupljeno 07.02.2021
[16] Statista, The smartphone platform war is over; https://www.statista.com/chart/4112/smartphone-platform-market-share/ pristupljeno 07.02.2021
[17] Cellularnews.com, 8 Existing Mobile Operating Systems Besides Android & iOS; https://cellularnews.com/mobile-operating-systems/8-existing-mobile-operating-systems-besides-android-ios/ pristupljeno 08.02.2021
[18] Statcounter.com, Mobile Operating System Market Share Worldwide; https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202002-202101-bar pristupljeno 08.02.2021
[19] Source, Secure an Android Device; https://source.android.com/security pristupljeno 08.02.2021
[20] Chell D., Erasmus T., Colley S., Whitehouse O., The Mobile Application Hacker's Handbook, John Wiley & Sons, Indianapolis, 2015; https://www.academia.edu/40654302/The_web_application_hackers_handbook pristupljeno 09.02.2021
[21] Bajtbox.com; https://www.bajtbox.com/samsung-oneui-2-0-android-10-video/ , https://www.bajtbox.com/kada-stize-novi-iphone8/yzfncntpghacfwvyliy3hd-650-80/ pristupljeno 09.02.2021
[22] Apple Platform Security, 02. 2021 https://support.apple.com/en-gb/guide/security/welcome/web pristupljeno 08.02.2021 pristupljeno 09.02.2021
[23] Saletović, Frketić, Salopek: Razina svijesti hrvatskih studenata o dozvolama koje daju aplikacijama, Zagreb, 2017; https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=279440 pristupljeno 09.02.2021
[24] Chin E.Felt A.P., Sekar V., Wagner D., Measuring User Confidence in Smartphone Security and Privacy; https://cups.cs.cmu.edu/soups/2012/proceedings/a1_Chin.pdf pristupljeno 09.02.2021
[25] https://preporucamo.com/26173-2/2016/01/31/ pristupljeno 15.02.2021

[26] Android Enterprise Security White Paper, siječanj 2020; https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf pristupljeno 15.02.2021
[27]Hp.com; https://www8.hp.com/us/en/hp-news/press-release.html?id=2184153#.YDN84-nPzIV pristupljeno 15.02.2021
[28] Post C.C., Woodrow S., Location is Everything- Balancing Innovation, Convenience, and Privacy in Location-based Technologies, 2008; https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall08-papers/location-is-everything.pdf pristupljeno 15.02.2021
[29]Apple.com; https://support.apple.com/hr-hr/HT207092 pristupljeno 16.02.2021
[30] M.Vashek, R.Zdenek, Security of Biometric Authentication Systems, 2010; https://www.researchgate.net/publication/251971395_Security_of_Biometric_Authentication_Systems pristupljeno 16.02.2021
[31] https://www.racunalo.com/sony-ce-demonstrirati-3d-biometriju-lica-na-xperiji/ pristupljeno 16.02.2021
[32] Zaba.hr; https://www.zaba.hr/home/placanje-na-internetu-metodom-3ds-biometrije pristupljeno 20.02.2021
[33] How to guide Mobile and cookies legislation, DMA; https://dma.org.uk/uploads/Mobile_and_Cookies_Legislation_53cfc279d03a7.pdf 20.02.2021
[34] Mobile Cookies 101- Understanding the Limitations of Cookie-Based Tracking for Mobile Advertising, 2013; http://docplayer.net/21229197-Mobile-cookies-101-understanding-the-limitations-of-cookie-based-tracking-for-mobile-advertising-december-2013.html pristupljeno 20.02.2021
[35]Google play, Lookout aplikacija; https://play.google.com/store/apps/details?id=com.lookout&hl=hr&gl=US pristupljeno 22.02.2021
[36] Google play, BullGuard aplikacija; https://play.google.com/store/apps/details?id=com.bullguard.mobile.mobilesecurity&hl=hr&gl=US pristupljeno 22.02.2021
[37]Google play, AVG; https://play.google.com/store/apps/details?id=com.antivirus&hl=hr&gl=US pristupljeno 22.02.2021

POPIS SLIKA

POPIS KRATICA

- NATO - North Atlantic Treaty Organisation, odnosno Sjevernoatlanski vojni savez
- Eng.- engleski
- Npr.- na primjer
- Sl.- slično
- IBM- Tvrtka International Business Machines
- SIM - Subscriber Identity Module
- SD - eng. Secure Digital
- GPS- Global Positioning System
- DoS- Denial of Service napad
- PDA- Personal Digital Assistent
- ID- identity card
- VPN- virtualna privatna mreža
- GDPR- General Data Protection Regulation