Sigurnosni izazovi pametnih mobilnih i nosivih uređaja

Ripli, Mihaela

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

SIGURNOSNI IZAZOVI PAMETNIH MOBILNIH I NOSIVIH UREĐAJA

SECURITY CHALLENGES OF SMART MOBILE AND WEARABLE DEVICES

Mentor: dr. sc. Ivan Cvitić

Studentica: Mihaela Ripli

JMBAG: 0135258064

Zagreb, kolovoz 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Informacije i komunikacije**

ZAVRŠNI ZADATAK br. 6859

Pristupnik: **Mihaela Ripli (0135258064)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnosni izazovi pametnih mobilnih i nosivih uređaja**

Opis zadatka:

U okviru završnog rada potrebno je pružiti prikaz razvoja pametnih mobilnih i nosivih uređaja. S obzirom na njihovu rasprostranjenost i heterogenost nužno je analizirati postojeće metode napada na takve uređaje kao i metode zaštite i prevencije identificiranih kibernetičkih prijetnji. Uz dostupne metode potrebno je istražiti i dostupne programske alate primjenjive u zaštiti.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

SAŽETAK

U suvremeno doba korištenje pametnih mobilnih i nosivih uređaja postala je nužna svakodnevica. Postoje razni uređaji koje koriste djeca i odrasli ljudi. Značajna je sigurnost korištenja pametnih mobilnih i nosivih uređaja. Prisutni su ljudi koji žele ukrasti podatke određenom korisniku, a nazivaju se napadači. Postoje razne metode napada putem kojih je moguće pristupiti privatnim i osjetljivim podacima određenog korisnika. Ovaj završni rad donosi metode napada koje se primjenjuju na pametnim mobilnim i nosivim uređajima, a zatim donosi i metode zaštite i prevencije od kibernetičkih prijetnji, odnosno metoda kibernetičkih napada. Kako bi se spriječile razne metode kibernetičkih napada, postoji i nekoliko programa, odnosno mobilnih aplikacija koje sprječavaju kibernetičke napade.

KLJUČNE RIJEČI: zaštita pametnih mobilnih i nosivih uređaja; metode napada; metode zaštite

SUMMARY

In modern times, the use of smart mobile and wearable devices has become an everyday necessity. There are various devices used by children and adults. The safety of using smart mobile and wearable devices is important. There are people who want to steal data from a certain user, and they are called attackers. There are various attack methods through which it is possible to access the private and sensitive data of a particular user. This undergraduate thesis present methods of attacks that are applied to smart mobile and wearable devices, and then presents methods of protection and prevention against cyber threats, i.e. methods of cyber attacks. In order to prevent various methods of cyber attacks, there are also several programs or mobile applications that prevent cyber attacks.

KEY WORDS: cyber protection of smart mobile and wearable devices; attack methods; protection methods

Sadržaj

1. UVOD

Razvojem tehnologija, od svih danas dostupnih uređaja, pojavljuju se pametni mobilni uređaji te pametni nosivi uređaji. Pametni nosivi uređaji su *Bluetooth* načinom razmjene podataka povezani na pametni mobilni uređaj. Za određene usluge na pametnom mobilnom uređaju koristi se globalna računalna mreža, Internet. Podaci koji se prenose računalnim mrežama su osjetljivi i vrlo jednostavno može doći do kibernetičkog napada.

Kibernetički napad je neovlašteni pristup uređajima, među kojima su i pametni mobilni i nosivi uređaji. Osoba koja izvršava kibernetički napad, naziva se napadač. Putem raznih metoda kibernetičkih napada vrlo je jednostavno otkriti korisničke privatne i osjetljive podatke. Poznato je da svi podaci koji su jednom povezani s Internetom, zauvijek ostaju na Internetu. Sigurnost korisnika vrlo je važna i zato je potrebno educirati korisnika kako bi zaštitio vlastite podatke i sigurno koristio svoje pametne mobilne i nosive uređaje.

Cilj i svrha ovog završnog rada su sigurnosni izazovi pametnih mobilnih i nosivih uređaja, pri čemu se u radu obrađuju pametni mobilni uređaji i pametni satovi. Završni rad sastoji se od šest poglavlja:

1. Uvod
2. Razvoj pametnih mobilnih i nosivih uređaja
3. Metode napada na pametne mobilne i nosive uređaje
4. Metode zaštite i prevencije od kibernetičkih prijetnji
5. Programski alati za zaštitu od kibernetičkih prijetnji
6. Zaključak.

U drugom poglavlju obrađena je povijest pametnih mobilnih i nosivih uređaja. Prikazan je razvoj istih od njihovog prvog korištenja sve do danas kroz pet generacija mobilnih mreža.

Treće poglavlje donosi razne metode kibernetičkih napada kojima napadač pristupa korisničkim povjerljivim podacima. Definirana je računalna sigurnost, sigurnosni zahtjevi te su prikazane metode kibernetičkih napada na pametne nosive uređaje te metode kibernetičkih napada kroz šest glavnih izvora sigurnosnih prijetnji.

U četvrtom poglavlju prikazane su i razjašnjene metode zaštite i prevencije od kibernetičkih prijetnji. Za pametne mobilne i nosive uređaje postoji šest metoda zaštita i prevencije.

Peto poglavlje prikazuje razne programske alate koji se koriste za zaštitu od kibernetičkih prijetnji. Svi navedeni programski alati su aplikacije koje se instaliraju na pametni mobilni uređaj.

Obzirom da je pametni sat povezan *Bluetoothom* na pametni mobilni uređaj, samom zaštitom mobilnog uređaja, štiti se i pametni sat.

2. RAZVOJ PAMETNIH MOBILNIH I NOSIVIH UREĐAJA

U današnje doba, korisnici uređaja očekuju konstantnu dostupnost usluga na uređajima, samim time i pristup računalnim mrežama. Velike brzine prijenosa, dostupnost mrežnog signala, dostupnost Interneta samo su neke od karakteristika koje današnji uređaji trebaju podržavati. Raznolikost mobilnih terminalnih uređaja dosta je opsežna. Oni se mogu podijeliti na [1]:

- mobilne uređaje
- nosive uređaje
- fiksne uređaje
- računala: prijenosna, stolna, tablet, netbook i dr.
- i ostale uređaje.

2.2 POVIJEST PAMETNIH MOBILNIH UREĐAJA

Postoje dvije vrste bežičnih telefonskih uređaja, a to su bežični telefoni i bežični mobilni terminalni uređaji. Bežični telefoni su uređaji koji se sastoje od bazne stanice i slušalice, poznati pod nazivom fiksni telefoni. U prošlosti su postojali telefoni s brojčanikom, a danas su popularni bežični telefoni bez brojčanika. Bežični (fiksni) telefoni podržavaju samo glasovnu komunikaciju, odnosno komutaciju kanala [1].

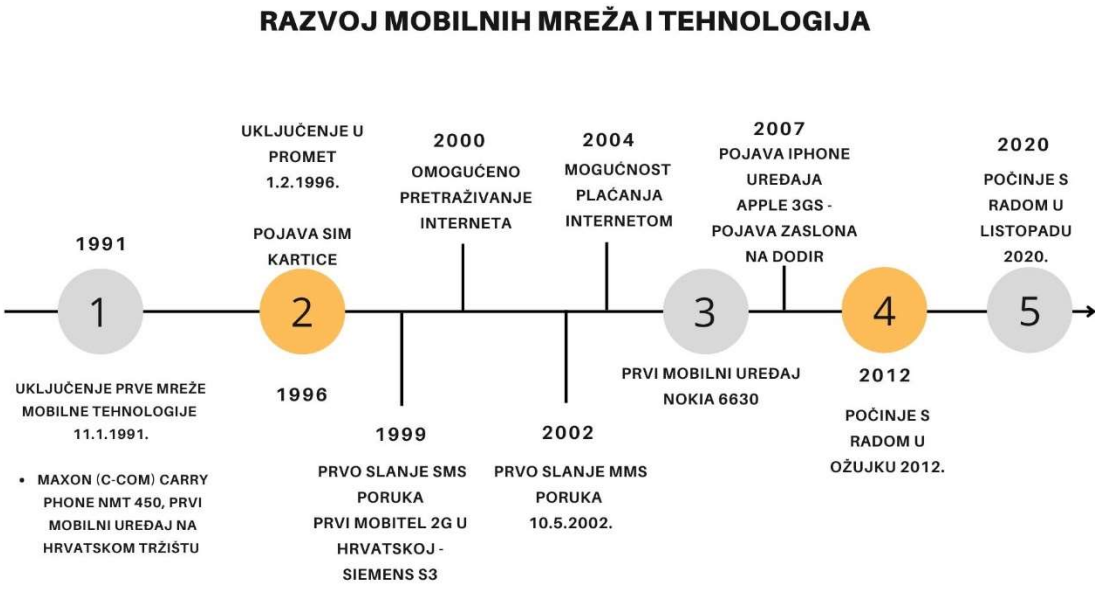
Pametni mobilni uređaj je uređaj koji pruža više mogućnosti od klasičnog mobilnog telefona. Neke od mogućnosti su video telefonija ili korištenje aplikacija. Mobilni uređaji podržavaju komutaciju kanala i komutaciju paketa. Dakle, mobilni uređaji podržavaju glasovnu i podatkovnu komunikaciju. Postoji pet generacija mobilnih mreža, a može biti analogna ili digitalna mobilna telefonija [1].

Analogna mobilna telefonija koristila se u prvoj generaciji mobilnih mreža i podržavala je komutaciju kanala. Navedena tehnologija koristila se povremeno za potrebe pomorske i vojne komunikacije. Analogni sustavi su: *Nordic Mobile Telephone* (NMT), *Advanced Mobile Phone Service* (AMPS) i *Total Access Communication System* (TACS). U europskim državama koristio se NMT analogni sustav. Obzirom da su NMT analogni sustavi koristili samo jedan veliki odašiljač, jedan kanal koristio se za slanje i za primanje signala. Kako bi se ostvarila komunikacija, bilo je potrebno pritisnuti tipku koja omogućuje korištenje odašiljača, a onemogućuje prijemnik [1]. Tako bi se ostvarila dvosmjerna komunikacija. Primjer takve tehnologije je građanski opseg (engl. *Citizens band* - CB) radio, koji se koristi također za potrebe taksi prijevoznika te u policijskim automobilima [1].

U drugoj generaciji mobilnih mreža pojavljuje se digitalna mobilna telefonija. Digitalni sustavi su: *Global System for Mobile Communications* (GSM), *Digital AMPS* (D-AMPS) i *Personal Digital Cellular* (PDC). U europskim državama koristi se GSM sustav. Druga generacija mobilnih mreža omogućava prijenos govora i mogućnost slanja i primanja SMS poruka (eng. *Short Message Service*). Omogućava i dodatne usluge poput faksa i govorne pošte [2].

Treća generacija mobilnih mreža koristi digitalni sustav *Universal Mobile Telecommunication System* (UMTS). UMTS omogućuje audio, video i podatkovno područje, govor te igre i ostale multimedijske i Internet sadržaje, što treću generaciju predstavlja kao višeuslužnu mobilnu mrežu. Podržava i komutaciju kanala i komutaciju paketa. Četvrta generacija donosi veće brzine. Četvrta generacija ne podržava komutaciju kanala, ali omogućava komunikaciju koja se temelji na Internet protokolu. Internet protokol omogućava razne usluge poput: Internet Protokol (IP) telefonije, video konferencija, računalnog oblaka te visoke propusnosti mrežnog prometa. Četvrta generacija poznata je pod nazivom *Long Term Evolution* (LTE) [2].

Peta generacija (5G), kao najnovija mobilna mreža trenutno se razvija. Jedna od značajki je brzina koja bi iznosila do 10 Gbit/s. Peta generacija mreža trebala bi poboljšati kapacitet i stabilnost mreže. Obzirom da će se u petoj generaciji mreža koristiti milimetarski valovi koji nemaju mogućnost prekrivanja velikih geografskih površina, bit će potrebno više manjih baznih postaja [3]. Na slici 1. prikazan je razvoj generacija mobilnih mreža i komunikacijskih tehnologija od njihove pojave do danas.



Slika 1. Razvoj mobilnih mreža i tehnologija

Izvor: [4]

2.1. POVIJEST PAMETNIH NOSIVIH UREĐAJA

Osim pametnih mobilnih uređaja, prisutni su i pametni nosivi uređaji. Pametni nosivi uređaji su uređaji koje korisnik može nositi na određenim dijelovima tijela. Opisuju se kao mala računala koja su izrađena u obliku satova, narukvica, naočala, prstenja, majica ili tenisica, a postoje još razni pametni nosivi uređaji [5].

Prvi nosivi uređaji pojavili su se oko 13. stoljeća od strane engleskog fratra Rogera Bacona, koji je opisao znanstvene principe koji stoje iza upotrebe korekcijskih leća. Naočale koje je osmislio Roger Bacon, bile su prve nosive stvari osmišljene za besprijekorno nošenje i poboljšanje vida, čime su postale prve pametne naočale [6].

Prvi džepni mehanički sat, pojavljuje se početkom 16. stoljeća. Petar Henlein ga je osmislio 1505. godine kao prijenosni, ali neprecizni sat. Navedeni sat pokrenuo je publicitet u razvoju nosivih satova. Kasnije su se džepni satovi razvili s evolucijom minijaturizacije, što je u 19. stoljeću dovelo do ideje o remenima za uređaj koji bi se nosio na zapešću [6].

Prvi pametni prsten pojavljuje se početkom 17. stoljeća za vrijeme dinastije Qing, a bio je poznat pod nazivom Abakus Prsten. Standarni abakus je bio kombiniran od 10 paralelnih žica smještenih između dvije ploče na okviru s devet zrna na svakoj od njih. Standarni abakus služio je kao pomoć trgovcima, a vodio je put prema modernim nosivim računalima i u isto vrijeme prema modernim pametnim prstenovima [6].

Sljedeći veliki korak u razvoju nosive tehnologije bio je prema virtualnoj stvarnosti (engl. *Virtual Reality* – VR) Mortona Heiliga, koji je 1960. godine patentirao televizijski zaslon smješten na glavu [6].

Početak 1990-ih godina obilježen je stvaranjem *The Active Badge*, prvim prijenosnim uređajem za praćenje lokacije u zatvorenom prostoru. Izradio ga je Olivetti Research Laboratory i bio je prikladan za prijenos jedinstvenih infracrvenih signala za priopćavanje lokacije korisnika, što bi se moglo smatrati rođenjem koncepta pametnih kuća [6].

U ožujku 1996. godine, tvrtka Palm pokrenula je prvu serijsku proizvodnju osobnog digitalnog asistenta (engl. Personal Digital Assistant -PDA) [6].

Fitbit se pojavljuje 2007. godine, a osnovali su ga James Park i Eric Friedman. Godine 2008. *Fitbit Classic* bio je prvi bežični uređaj za praćenje aktivnosti, a imao je mogućnost sinkronizacije podataka s Internetom te dostupnost istih podataka na mobilnom uređaju [6].

Godine 2009. predstavljen je Samsung S9110 pametni sat. Bio je to dvopojasni GPRS (*General Packet Radio Services*) telefon s podrškom za razmjenu električne pošte. Navedeni

pametni sat bio je prvi pametni sat koji je uključivao zaslon osjetljiv na dodir u punoj boji, *Bluetooth* vezu, slušanje glazbe i značajku prepoznavanja glasa [6].

Sljedeći napredak za krajnje korisnike dogodio se kasnije u 2014. godini uvođenjem *Android Weara*, trenutno poznatog kao *Wear* operativni sustav. Navedeni operativni sustav bio je prvi operativni sustav posebno osmišljen za nosive uređaje, a posebno za pametne satove. *Apple* 2015. godine iznosi na tržište svoj prvi nosivi uređaj, *Apple Watch* [6].

Klasifikacija nosivih uređaja mogla bi se prikazati iz različitih perspektiva na temelju različitih čimbenika. Najšira klasifikacija temelji se na vrsti aplikacije, a podjela je navedena u nastavku [6]:

1. nosivi uređaji namijenjeni za glavu korisnika – uglavnom usmjereni na aspekte percepcije i kontrole. Primjeri su: VR naočale, maske za lice za opuštanje, audio uređaji koji se odnose na slušalice, osobni asistenti te samostalna grupa s neuronskim sučeljima
2. nosivi uređaji koji se nose na tijelu mogu se podijeliti na podskupine:
   a) nose se uz tijelo i namijenjeni su sportu: pametne narukvice i senzori za praćenje aktivnosti
   b) nose se na tijelu: ekrani za elektroencefalografiju (engl. *electroencephalogram* – EEG) i ekrani za elektrokardiografiju (eng. *electrocardiogram* – EKG), uređaji za ispravljanje držanja tijela, sigurnosni uređaji te razna pametna odjeća
   c) nose se u tijelu: pametne tetovaže
3. nosivi uređaji za donji dio tijela: pametne cipele, pametni pojasevi, pametni ortopedski ulošci i pametne hlače. Većina njih ima specifičnu funkciju nadzora za profesionalni sport ili medicinske svrhe.
4. nosivi uređaji koji se nose na zapešću i u ruci, a oni su najrasprostranjeniji. Takvi uređaji su: pametni satovi, pametne narukvice, pametno prstenje te uređaji za upravljanje gestama.

Pametni sat (engl. *Smartwatch*) je nosivi uređaj koji je klasični sat zamijenio ekranom na dodir. Tvrtka Hamilton Watch 1978. godine razvija prvi digitalni sat, koji je imao LED ekran, složen krug od 25 čipova te je bio vrlo skup [7]. Casio 1982. godine započinje proizvodnju satova koji imaju mogućnost programiranja. Bill Gates 2003. godine predstavlja sat koji ima mogućnost upravljati kućanskim aparatima, osobnim računalima i telefonima. Međutim, prvi pravi pametni sat proizvela je tvrtka Pebble. Samsung je 2001. godine proizveo narukvicu koja je imala ugrađen minijaturni mobilni uređaj, koja je tada bila glavna inovacija [8].

Pametna narukvica je nosivi uređaj koji je sličan pametnom satu, ali manje je veličine i koristi se prvenstveno za sport, *fitness* i općenito, fizičko zdravlje. Prema cijeni, narukvice su jeftinije od pametnih satova. Pametna narukvica povezana je *Bluetoothom* na pametni uređaj te

se na aplikaciju na uređaju sinkroniziraju podaci s narukvice. Na identičan način funkcioniraju i pametni satovi [9].

Pametne naočale su primjer proširene stvarnosti koja kombinira virtualnu okolinu sa stvarnom okolinom. Na naočalama je moguće pronaći mikrofon, kamere te zaslon koji je vidljiv samo osobi koja nosi pametne naočale. Prema [9], takva tehnologija vrlo brzo napreduje te je moguće da će u skorije vrijeme zamijeniti pametne mobilne uređaje. Godine 2013. Google započinje s prodajom pametnih naočala. *Google Glass* naočale funkcioniraju na način da korisnik dodirne naočale sa strane, a zatim se pojavljuje zaslon. Korisnik ima mogućnost upravljanja naočalama tako da klizanjem unatrag vidi primjerice, vremensku prognozu, a klizanjem unaprijed vidi telefonske pozive ili fotografije. Moguće je fotografirati ili snimati s pametnim naočalama. Pametne naočale su poput pametnih satova i pametnih uređaja povezane *Bluetoothom* na pametni mobilni uređaj. Za povezivanje na Internet koristi se bežični način prijenosa podataka (engl. *Wireless Fidelity* - Wi-Fi*)* [9].

Širok raspon nosivih uređaja i tehnologija za povezivanje omogućuje različita rješenja za povezivanje koja su definirana različitim zahtjevima. Zahtjevi nosivog uređaja odnose se na: domet, brzinu prijenosa podataka, ograničenja napajanja, vrste mreže, postavke programera te brojne druge segmente. Specifičnosti prijenosa podataka, uključujući razinu enkripcije, sheme kodiranja i prijenosa, modulaciju i ciklički prefiks, također se pojedinačno definiraju ovisno o korištenoj tehnologiji. Najčešće korištene tehnologije prijenosa podataka u nosivim uređajima su: *Near Field Communication* (NFC), *Bluetooth Low Energy* (BLE), Wi-Fi, *Zigbee* i *Low-Power Wide Area Network* (LPWAN) [6]. Karakteristike pojedinih komunikacijskih tehnologija prikazane su u tablici 1.

Tablica 1. Karakteristike komunikacijskih tehnologija

Komunikacijska tehnologija	Karakteristike
Near Field Communication (NFC)	- rad na principu magnetske indukcije - stvara se inducirano polje kroz koje se mogu slati podaci
Bluetooth Low Energy (BLE)	- bežični komunikacijski protokol za razmjenu podataka kratkog dometa - *Bluetooth* verzija 5.0. ima domet do 400 m, što znači da se komunikacija između uređaja provodi u radijusu do 240 m.
Wireless Fidelity (Wi-Fi)	- cilj: povezivanje mobilnih uređaja unutar bežične lokalne mreže - definirana standardom IEEE 802.11

Zigbee	- bežična tehnologija kratkog dometa
Low-Power Wide Area Network (LPWAN)	- bežični prijenos na velike udaljenosti, niska potrošnja energije - pogodna za male količine podataka koje imaju ograničene resurse poput baterije i kapaciteta prijenosa. - postoji i LPWAN protokol dugog dometa (engl. *Long Range*- LoRa) koji predstavlja bežičnu tehnologiju velikog dometa te nudi prijenos do 25 km operativne udaljenosti

Izvor: [6]

3. METODE NAPADA NA PAMETNE MOBILNE I NOSIVE UREĐAJE

Računalna sigurnost, koja se može zvati i kibernetičkom sigurnošću, zaštita je računalnih sustava i informacija od oštećenja, krađe i neovlaštenog pristupa [10]. Sigurnosni kibernetički napad pokušaj je neovlaštenog pristupa informacijama ili uslugama koji nanosi štetu informacijskom sustavu. Pod navedenim se podrazumijeva bilo koji oblik zlonamjernih radnji koje narušavaju sigurnost komponenti informacijskog sustava [11].

Sigurnosni zahtjevi predstavljaju osnovna načela koji su potrebni za uspostavu sigurnosti informacijskog sustava. Postoje tri sigurnosna zahtjeva, koja su poznata pod kraticom CIA (*Confidentiality, Integrity, Aviailability*), a to su [12]:

- povjerljivost (engl. *Confidentiality*)
- cjelovitost (engl. *Integrity*)
- dostupnost (engl. *Availability*).

Povjerljivost predstavlja načelo koje omogućava zaštitu podataka od neautoriziranih subjekata i nepouzdanih postupaka. Opisuje se kao kombinacija tajnosti, autentičnosti i neporecivosti. Podaci se prikazuju samo autoriziranim i autentificiranim korisnicima. Do gubitka povjerljivosti dolazi u trenutku otkrivanja podataka. Najčešći kibernetički napadi na povjerljive informacije su: lažno predstavljanje, neovlašteni pristup, napadači, zlonamjerni programi te kopiranje podataka na lokacije s nedovoljnom razinom zaštite [13].

Cjelovitost, odnosno integritet načelo je koje predstavlja zaštitu od svih izmjena informacija i sustavnih procesa od strane neovlaštenih korisnika, ali i ovlaštenih korisnika koji namjerno ili nenamjerno krše povjerljivost. Osigurava točnost i pouzdanost podataka tijekom cijelog životnog ciklusa [13].

Dostupnost, odnosno raspoloživost je načelo koje omogućuje pristup i korištenje informacija i procesa. Osigurava korisnicima pristup resursima onda kada im je to potrebno. Dostupnost može biti narušena u slučaju napada uskraćivanjem usluge (engl. *Denial of Service* – DoS) i gubitkom mogućnosti obrade podataka [13].

S vremenom, broj prijetnji i kibernetičkih napada na pametne mobilne i nosive uređaje se povećava te se očekuje i daljnji rast broja pokušaja kibernetičkih napada. Postoji šest izvora sigurnosnih prijetnji, a to su [15]:

- fizički zasnovane prijetnje
- aplikacijski zasnovane prijetnje
- web zasnovane prijetnje
- mrežno zasnovane prijetnje
- socijalni inženjering

- BYOD (engl. *Bring Your Own Device*).

3.1. FIZIČKI I APLIKACIJSKI ZASNOVANE PRIJETNJE

3.1.1. FIZIČKI ZASNOVANE PRIJETNJE

Fizički zasnovana prijetnja vrsta je prijetnje koja može dovesti do gubitka, krađe ili fizičke štete pametnog mobilnog ili nosivog uređaja. Pod fizički zasnovane prijetnje spadaju i potresi, poplave, požari te djela terorizma. Fizička sigurnost predstavlja sigurnost korisnika, hardvera, programa i aplikacija te mreža od događaja koji mogu izazvati ozbiljne gubitke i štetu privatne ili poslovne prirode [15]. U fizički zasnovane prijetnje spada i metoda kibernetičkog napada na uređaje koji su namijenjeni za recikliranje, a to se odnosi na već korištene pametne mobilne telefone i nosive uređaje koji su prodani ili poklonjeni drugom korisniku. Prema [16] pokazalo se da 54% mobilnih terminalnih uređaja sadrži osobne podatke poput elektroničke pošte, tekstualnih poruka i bankovnih podataka. Do olakšane krađe podataka dolazi ukoliko osoba ne koristi zaporku, osobni identifikacijski broj (engl. *Personal Identification Number* – PIN) , otisak prsta i dr. za otključavanje pametnog mobilnog ili nosivog uređaja [16].

Podaci u mobilnom uređaju mogu biti od visoke vrijednosti za korisnika. Ponekad korisnik ima mogućnost izgubiti svoje vlastite podatke. Primjerice to može biti pad te lom uređaja, koji se nakon takvog događaja više ne može ponovno pokrenuti. Ukoliko korisnik nema sigurnosno kopiranje svojih podataka na računalstvo u oblaku (engl. *Cloud*), dolazi do trajnog gubitka podataka. Također se kao primjer može navesti i korisnik koji na svoj uređaj postavlja zaporku, no onda korisniku zaporka ne ostaje u pamćenju te tako više nema mogućnost otključati svoj uređaj. Mnogi servisi nude otključavanje mobilnog uređaja, no ne garantiraju očuvanje podataka. Najjednostavniji primjer gubitka bankovnih podataka jest korisnikova nepažnja prilikom prijave u bankovne aplikacije. Napadač ima mogućnost vidjeti PIN ili zaporku za aplikaciju te nakon toga ukrasti mobilni uređaj korisniku, a nakon toga najčešće dolazi do gubitka sredstava s bankovnog računa. Nosive uređaje poput pametnih satova moguće je ukrasti, no manje su šanse da napadač može doći do većeg broja podataka o korisniku nego na mobilnom uređaju. Postoje pametni nosivi uređaji koji imaju mogućnost beskontaktnog plaćanja bankovnom karticom te postoji veća mogućnost da će takvi uređaji biti ukradeni [16].

3.1.2. APLIKACIJSKI ZASNOVANE PRIJETNJE

Zlonamjerni softver (engl. *Malware*), nenamjerno otkrivanje podataka i nadziranje pametnih mobilnih uređaja, metode su aplikacijsko baziranih prijetnji. Zlonamjerni softver je svaki nametljivi softver koji je razvijen od strane napadača, a koristi se za krađu podataka i oštećenje ili uništavanje pametnih mobilnih i nosivih uređaja i njihovih sustava. Postoji sedam tipova kibernetičkih napada temeljenih na zlonamjernom softveru, a to su: računalni virusi, računalni crvi, računalni trojanski konj, špijunski softver, softver koji podržava oglašavanje, *ransomware* i *fileless malware* [17].

Računalni virusi predstavljaju zlonamjerni softver koji se instalira na pametni mobilni i nosivi uređaj te se širi s uređaja na uređaj. Virus je u stanju mirovanja dok se datoteka ne otvori i ne počne koristiti. Virusi mogu promijeniti ili uništiti podatke na pametnom mobilnom i nosivom uređaju te uzrokovati velike operativne probleme. Obzirom da virus ima negativan učinak na uređaj, njegovu prisutnost moguće je primjetiti na nekoliko načina. Primjerice, ukoliko su uređaj, aplikacije i brzina interneta sporiji nego inače, a pri tome ne postoje snažne aplikacije koje mogu uzrokovati značajno manju brzinu od uobičajene. Također, najčešće su prisutni i neželjeni skočni prozori koji se pojavljuju na Internet pregledniku [18].

Računalni crvi predstavljaju zlonamjerni softver, odnosno računalni kod koji se širi na bilo koji uređaj unutar mreže te ima mogućnost vrlo brzog samostalnog repliciranja na iste. Za razliku od virusa, računalni crvi ne trebaju interakciju korisnika. Crv zarazi pametni mobilni i nosivi uređaj putem preuzete datoteke ili mrežne veze bez znanja korisnika. Crvi, kao i virusi, mogu poremetiti rad mobilnih i nosivih uređaja te uzrokovati gubitak podataka. Postoji mogućnost i krađe podataka, instalacije „stražnjih vrata“ (engl. *backdoor*) i omogućavanja napadaču preuzimanje kontrole nad računalom i postavkama računalnog sustava. Računalne crve moguće je prepoznati prema smanjenoj procesorskoj snazi, odnosno učestalom rušenju programa ili neispravnosti rada istih programa. Poželjno je pratiti brzinu i performanse sustava [19].

Računalni trojanski konj metoda je kibernetičkog napada koja se predstavlja kao koristan softverski program. Nakon što ga korisnik preuzme, trojanski konj može pristupiti osjetljivim podacima te ih izmijeniti, onemogućiti ili obrisati. Naspram virusa i crva, trojanski konj nema mogućnost samostalnog repliciranja na ostale uređaje [17].

Špijunski softver (engl. *spyware*) zlonamjerni je softver koji se tajno pokreće, odnosno instalira na pametnom mobilnom i nosivom uređaju, prikuplja podatke s uređaja i šalje ih udaljenim uređajima bez korisnikovog pristanka. Čini krađu podataka pomoću snimaka zaslona, tehnologije pritiskanja tipki i kodova za praćenje. Najčešće se koristi za krađu financijskih i osobnih podataka. Navedena metoda kibernetičkog napada jedna je od najčešćih koju korisnik može teško prepoznati. Špijunski softver funkcionira na način da se na korisnikovom mobilnom uređaju špijuniraju njegove aktivnosti, posjećene Internet stranice i ostali osjetljivi podaci. Dakle, napadač ima mogućnost prikupljanja i prodavanja vrlo osjetljivih podataka poput korisničkih adresa elektroničke pošte i zaporki, zatim informacija o korištenju interneta i navikama pregledavanja, financijskih podataka i zaporki osobnog identifikacijskog broja računa [20].

Softver koji podržava oglašavanje (engl. *adware*) metoda je kibernetičkog napada koji prikazuje neželjene oglase i reklame na računalu. Softver koji podržava oglašavanje je lako prepoznati prema većem broju skočnih prozora koji sadrže neki oglas ili reklamu. Funkcionira na način da prikuplja korisničku povijest pregledavanja Interneta te postavlja reklame koje su prilagođene interesu korisnika. Najčešći razlog za navedeno je zarada od oglašavanja. Postoji

također i mobilni softver za oglašavanje (engl. *mobile adware*). Mobilni softver za oglašavanje je metoda kibernetičkog napada na pametnom mobilnom uređaju. Takav kibernetički napad najčešće započinje instalacijom aplikacije koja sadrži reklamni softver koji je najčešće besplatan. Neke od karakteristika kojima se može prepoznati prisutnost mobilnog softvera za oglašavanje su: usporen uređaj i veće zauzeće memorije nego inače, veća količina skočnih oglasa i reklama, učestalo padanje sustava te slaba internetska veza [21].

Ransomware šesta je metoda kibernetičkog napada koja predstavlja zlonamjerni softver koji dobiva pristup osjetljivim podacima unutar mobilnog uređaja, šifrira podatke i onemogućava ih korisniku. Napadač prijeti korisniku javnim objavljivanjem i oštećenjem podataka te ima mogućnost onemogućiti korisniku pristup i rad na mobilnom uređaju. U tom slučaju korisnik mora platiti veću svotu novaca kako bi mu se podaci vratili. Kada napadač primi uplatu, podaci se otključavaju. Korisnik preuzima *ransomware* klikom na poveznicu. Moguće je i da korisnik posjeti Internet stranicu koja je slučajno zaražena te se zlonamjerni softver na tom mjestu preuzima i instalira, bez korisnikovog znanja. Navedena metoda kibernetičkog napada postaje sve učestalija [22].

Posljednja metoda napada zlonamjernog softvera je *fileless malware*. Predstavlja metodu kibernetičkog napada koja se razlikuje od mnogih drugih prijetnji temeljenih na zlonamjernom softveru. Nalazi se u memoriji, a ne u datotekama na tvrdom disku. Zbog toga ga je teško otkriti. Otežava digitalnu forenziku obzirom da zlonamjerni softver nestaje svaki put kad se korisnikov mobilni uređaj ponovno pokrene. Postoje veze koje se učitavaju u memoriju pametnog mobilnog uređaja, koje omogućuju napadačima daljinsko učitavanje kodova putem skripti koje preuzimaju i dijele korisničke povjerljive podatke. Također, zlonamjerni kod može se instalirati i u već povjerljive aplikacije poput Jave i Microsoft Worda [23].

Nenamjerno otkrivanje podataka odnosi se na korisničko nepravilno rukovanje vlastitim podacima. Navedena metoda kibernetičkog napada proizlazi najčešće iz neznanja korisnika. Korisnici nisu svjesni kakve sve funkcionalnosti imaju pametni mobilni i nosivi uređaji. Samim time korisnici pristaju npr. na dijeljenje podataka o lokaciji, a da ni ne znaju tko sve može saznati njegovu lokaciju. Primjerice, nenamjerno otkrivanje podataka su sve dozvole na koje korisnik pristaje prilikom instalacije određene aplikacije [12].

Nadziranje korištenjem pametnih mobilnih i nosivih uređaja je metoda napada koja se odnosi na [12]:

- prisluškivanje razgovora
- snimanje okoline
- praćenje lokacije
- preuzimanje tekstualnih datoteka

- preuzimanje elektroničke pošte.

3.2. WEB I MREŽNO ZASNOVANE PRIJETNJE

3.2.1. WEB ZASNOVANE PRIJETNJE

Web zasnovane prijetnje predstavljaju sigurnosni rizik za korisnika pametnog mobilnog i nosivog uređaja. Neke od metoda kibernetičkih napada zasnovanih na web prijetnjama su [12]:

- *phishing* napadi
- *smishing* napadi
- iskorištavanje Internet preglednika
- automatsko preuzimanje aplikacija.

Phishing je metoda kibernetičkog napada koja se najčešće odvija putem elektroničke pošte. Napadači ciljaju određenu skupinu korisnika i kreiraju elektroničke poruke koje izgledaju sigurno, iz pouzdanog izvora, ali zapravo sadrže poveznice, privitke ili druge mamce koji privuku korisnika na otvaranje privitka ili pritiska na poveznicu. Ovom metodom kibernetičkog napada, napadač ima mogućnost olakšano pristupiti korisnikovom pametnom mobilnom i nosivom uređaju, svim osobnim podacima, izmijeniti i iskoristiti povezane sustave. Postoji mogućnost i da napadač ošteti cijele računalne mreže sve dok korisnik ne uplati na bankovni račun otkupninu napadaču. Najčešće su napadačima dovoljni korisnički osobni podaci koji uključuju i bankovne podatke, odnosno informacije o bankovnoj kartici [24].

Phishing kibernetički napad moguće je primijetiti na dva načina [24]:

- sumnjiva e-mail adresa
- usporedba URL (engl. *Uniform Resource Locator*) poveznice s poveznicom dostupnom u e-mail poruci.

Smishing kibernetički napadi kombinacija su *phishing* metode kibernetičkog napada i SMS poruka. Navedena metoda kibernetičkog napada može se prikazati u tri koraka. Prvi korak je da napadač šalje uvjerljivu poruku korisniku koja sadrži poveznicu ili privitak. U drugom koraku korisnik otvara navedenu poveznicu ili privitak te upisuje svoje osobne podatke poput: korisničkog imena, zaporki ili kontrolnog broja kreditne kartice. U trećem koraku napadač koristi povjerljive podatke kako bi ih oštetio ili prodao na skrivenom Internetu (engl. *dark web*) [25].

Treća web zasnovana prijetnja je iskorištavanje Internet preglednika. Ovom metodom kibernetičkog napada napadač ima mogućnost otkriti informacije o korisniku na dva načina koja su navedena u nastavku. Prvi način je proučavanje datoteka koje korisnik pregledava, a drugi način je navođenje korisnika na postupke koje ga dovode u kompromitirajuće situacije. Informacije o korisniku moguće je otkriti putem datoteka iz priručne memorije, datoteka koje

sadrže povijest pregledavanja i *bookmark* oznaka. Navođenje korisnika u kompromitirajuće situacije odnosi se na zlonamjerne Internet stranice na kojima korisnik unosi svoje osobne podatke [26].

Zadnja web metoda kibernetičkog napada je automatsko preuzimanje aplikacija koja podrazumijeva nenamjerno preuzimanje i instalaciju aplikacija koje mogu naštetiti pametnom mobilnom i nosivom uređaju. Automatsko preuzimanje aplikacija odnosi se na nenamjerno preuzimanje i instalaciju zlonamjernih softvera koji imaju mogućnosti naštetiti pametnom mobilnom i nosivom uređaju. Ovakva vrsta kibernetičkog napada događa se samom posjetom određenoj web stranici, bez pritiskanja na sumnjive poveznice ili privitke [26].

3.2.2. MREŽNO ZASNOVANE PRIJETNJE

Mrežno zasnovane prijetnje moguće je podijeliti na dvije metode kibernetičkih napada, a to su: kibernetički napadi podvalom mreže i iskorištavanje mreže.

Kod metode kibernetičkog napada podvalom mreže, napadač se korisniku predstavlja kao neka druga ovlaštena osoba kako bi dobio mogućnost pristupanja određenim resursima koji imaju ograničenje. Cilj kibernetičkog napada je krađa podataka krajnjeg korisnika. Podaci mogu biti vrlo osjetljivi, poput korisničkih podataka iz banke. Kibernetički napad može se dogoditi putem mrežne pristupne točke poput GSM (engl. *Global System for Mobile*) mobilne mreže, na koju se određeni korisnik povezuje i tim putem napadač pristupa osobnim podacima korisnika [12].

Prilikom metode kibernetičkog napada iskorištavanjem mreže, napadač koristi sigurnosne propuste na mobilnom operativnom sustavu na određenoj lokalnoj ili mobilnoj mreži kako bi pristupio korisnikovim podacima. Primjeri sustava na lokalnoj mreži su: *Bluetooth* i Wi-Fi, a na mobilnoj mreži: SMS ili MMS (engl. *Multimedia Messaging Service*). Prilikom kibernetičkog napada ne zahtijevaju se nikakvi dodatni postupci korisnika, tako da korisnik niti ne zna da je proveden kibernetički napad [12].

3.3. SOCIJALNI INŽENJERING I BYOD METODE NAPADA

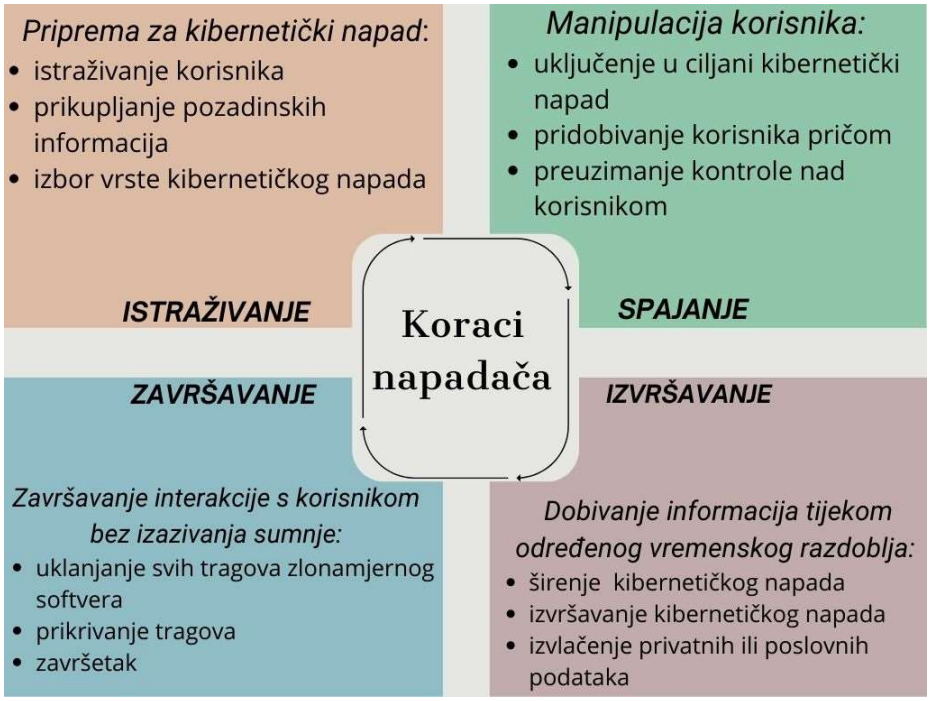
Posljednje dvije metode kibernetičkih napada: socijalni inženjering i korištenje vlastitog uređaja u poslovne svrhe, opisane su u nastavku.

3.3.1 SOCIJALNI INŽENJERING METODA KIBERNETIČKOG NAPADA

Socijalni inženjering metoda je kibernetičkog napada koja se koristi za široki raspon zlonamjernih aktivnosti koje se postižu kroz ljudsku manipulaciju. Psihološkom manipulacijom napadač navodi korisnika na poduzimanje određenih koraka i otkrivanje korisničkih povjerljivih podataka. Kibernetički napad odvija se u nekoliko koraka. Prvi korak je da napadač istražuje korisnika te prikuplja informacije poput slabih sigurnosnih protokola. Zatim napadač manipulira

korisnikom te ga navodi na određene korake kako bi korisnik otkrio napadaču svoje osobne podatke instaliranjem zlonamjerne aplikacije na vlastiti pametni mobilni ili nosivi uređaj [27].

Napadač ima mogućnost otkriti zaporke koje se koriste za enkripciju podataka te pristupiti otključanom pametnom mobilnom ili nosivom uređaju ili dobiti potpuni pristup mobilnom uređaju udaljenim pristupom. Navedena metoda kibernetičkog napada uključuje prepakiranje aplikacija i kibernetičke napade korištenjem novijih verzija softvera. Prepakiranje aplikacija odnosi se na modifikaciju zlonamjernim kodom i distribuciju podataka. Kibernetički napadi korištenjem novijih verzija softvera odnose se na najnoviju verziju određene aplikacije u kojoj se već nalazi zlonamjerni kod. Na slici 2. opisani su koraci koje napadač poduzima pri prethodno navedenoj metodi kibernetičkog napada [12].



Slika 2. Socijalni inženjering

Izvor: [27]

3.3.2 KORIŠTENJE VLASTITOG UREĐAJA U POSLOVNE SVRHE KAO METODA KIBERNETIČKOG NAPADA

Posljednja metoda kibernetičkog napada je *Bring your own device* (BYOD), a označava korištenje privatnog pametnog mobilnog uređaja u poslovne svrhe. Odnosno, zaposlenici određene poslovne organizacije koriste privatni pametni mobilni uređaj za pristup svim poslovnim podacima i sustavima koji su povezani s poslovnom organizacijom. Takvi podaci su vrlo osjetljivi. Osim pametnih mobilnih uređaja, zaposlenici koriste i vlastite tablete, prijenosna

računala ili USB pogone. Većina zaposlenika nije svjesna svih sigurnosnih prijetnji, odnosno sigurnosnih propusta, pri korištenju vlastitih uređaja umjesto poslovnih uređaja [28].

Ukoliko napadač pristupi ukradenom ili izgubljenom uređaju, ima tri moguće i glavne opcije za nanošenje štete, a to su [28]:

- krađa pohranjenih podataka na pametnom mobilnom uređaju
- korištenje vjerodajnica za pristup mreži poslovne organizacije
- uništavanje svih podataka na uređaju, koji mogu biti vrlo značajni za poslovnu organizaciju.

Pri svakom korištenju privatnih pametnih mobilnih uređaja u poslovne svrhe, najvažnije je identificirati trenutni operativni sustav koji radi na uređaju zaposlenika te osigurati primjenu najnovijih ažuriranja. Na taj način osigurava se sigurnost korištenja BYOD [28].

3.4. KIBERNETIČKI NAPADI NA PAMETNE NOSIVE UREĐAJE

Po pitanju sigurnosti, pametni nosivi uređaji prikupljaju razne osjetljive podatke te se zbog toga na njih treba obratiti veća pozornost. Oni su na pametni mobilni uređaj spojeni najčešće *Bluetooth* komunikacijskom tehnologijom te će se stoga u radu razmatrati sigurnost navedene komunikacijske tehnologije. Obzirom da nosivi uređaji koriste bežičnu vezu za spajanje na mobilni uređaj, mogući su mnogi rizici i nedostaci koji potencijalno mogu dovesti do kršenja privatnosti i sigurnosti [5].

Postoji nekoliko istraživanja koja su dokazala da napadači najjednostavnije napadnu dječje pametne nosive uređaje, a navedena su u nastavku.

3.4.1 KIBERNETIČKI NAPADI NA DJEČJE PAMETNE NOSIVE UREĐAJE

Dječji pametni nosivi uređaji imaju nekoliko značajnih karakteristika, a to su [29]:

- usluge poziva
- praćenje lokacije
- hitni pozivi
- obavijest roditeljima ukoliko dijete izađe iz zadanog područja.

Međutim, prema [29] dokazano je da napadači najčešće i najlakše pristupe lokaciji dječjih pametnih nosivih uređaja. Društvo za zaštitu potrošača u Norveškoj provelo je istraživanje iz kojeg je dokazano da su pronađeni sigurnosni propusti kod određenih proizvođača pametnih nosivih uređaja. Naime, pokazalo se da se podaci mogu razmjenjivati i pohranjivati bez ikakve zaštite. Zbog toga, napadači imaju mogućnost na jednostavan način pristupiti trenutnoj lokaciji djeteta, promijeniti lokaciju, prisluškivati ih i razgovarati s djecom. Proizvođači modela nosivih uređaja koji su imali takve sigurnosne propuste su riješili navedeni slučaj. Međutim, Velika

Britanija je odlučila da će takve modele pametnih nosivih uređaja povući sa tržišta, dok je u Njemačkoj u potpunosti zabranjena prodaja dječjih pametnih nosivih uređaja, kako bi se spriječilo praćenje, tj. špijuniranje djece [29].

Krajem 2020. godine, istraživanje jednog njemačkog sveučilišta pokazalo je da pet od šest testiranih modela ima ozbiljne sigurnosne probleme te da je sve je teže pronaći sigurne uređaje [30].

3.4.2 SIGURNOSNI RIZICI PAMETNIH NOSIVIH UREĐAJA

Tržište pametnih nosivih uređaja u značajnom je porastu prema proizvodnji, međutim zbog toga pametni nosivi uređaji će postati sve ranjiviji na kibernetičke napade, ovakva razmjena podataka je vrlo vrijedna i postala je meta napadača. Zabrinutost o privatnosti najviše se temelji na opasnosti povezane tehnologije i nedostatku standarda kibernetičke sigurnosti. Općenito Internet stvari (engl. *Internet of Things* - IoT) zahtijevaju kibernetičku sigurnost. Pametni nosivi uređaji ulaze u tzv. sigurnosno „sivo područje“, gdje nitko ne obazire pažnju na IoT proizvode na temelju kvalitete njihove zaštite i sigurnosti korisnika. Ne postoji jamstvo koje potvrđuje da pametni nosivi uređaj ima osiguranu zaštitu od kibernetičkih napada [31].

Bluetooth Low Energy (BLE) primjer je bežične veze koja potencijalno može dovesti do narušavanja privatnosti i sigurnosti korisnika. Loša implementacija *Bluetooth* uređaja može mnogim napadačima olakšati lociranje uređaja unutar određenog dometa, kao i praktično izvođenje različitih metoda kibernetičkih napada. Jedna od takvih metoda kibernetičkih napada je “Čovjek u sredini” (engl. *Man-In-The-Middle* – MITM), gdje napadači mogu lako prisluškivati različite korisnike [5].

Jedna od značajki pametnih nosivih uređaja je lokacija. Iako se navedena značajka smatra vrlo vrijednom za mnoge korisnike, postoje mnogi potencijalni rizici koji mogu dovesti do kršenja privatnosti. Ovakvo kršenje se može dogoditi putem samog uređaja ili tijekom prijenosa podataka između drugih uređaja – npr. slanje satelitskog radionavigacijskog sustava (engl. *Global Positioning System* – GPS) prikupljenih ruta s pametnog sata na pametni mobilni uređaj. Mogućnost kršenja privatnosti proizlazi iz procesa prijenosa GPS-a praćene lokacije između različitih uređaja korištenjem bežične veze poput *Bluetootha* ili Wi-Fi-ja. Osim lokacije, podaci se prikupljaju i preko mikrofona i kamere iako korisnici toga nisu svjesni. Takvi podaci se obično prikupljaju u marketinške svrhe [5].

Postoje tri grupe sigurnosnih prijetnji na *Bluetooth* tehnologiju, a to su [14]:

1. prijetnja otkrivanja podataka – napadači mogu prisluškivati ciljani uređaj te ukrasti podatke
2. prijetnja na integritet – neovlašteno izmjenjivanje podataka na putu od pošiljatelja do primatelja

3. prijetnja uskraćivanja usluge – uskraćivanje *Bluetooth* veze od strane neovlaštenih napadača.

Napadači mogu pristupiti korisničkim podacima i njegovim aktivnostima putem pametnog nosivog uređaja. Potrebno je obrazovati korisnika što se događa s njegovim podacima, tj. kako proizvođači postupaju s podacima. Što se tiče prikupljanja podataka, pametni nosivi uređaji prikupljaju mnogo osobnih informacija o korisniku putem *Bluetooth* i Internet veze. Ukoliko napadač pristupi lokaciji, kalendaru i transakcijama putem kreditnih kartica moguć je pristup i svim zaporkama, pa tako i onima za bankarstvo. Ukoliko proizvođač koristi centralizirane, interne usluge za pohranu i obradu korisničkih podataka, samo jedna povreda poslovne organizacije može omogućiti krađu korisničkih podataka. Što se tiče prikupljanja podataka, oni se šalju od davatelja usluga do aplikacija trećih strana, što nije nužno zlonamjerno, nego služi za pohranjivanje, obrađivanje i analizu podataka kako bi korisniku bilo pruženo što bolje iskustvo. Svaki proizvođač ima javno dostupna pravila o prikupljanju podataka s kojima se korisnik svojevoljno slaže pri kupnji pametnog nosivog uređaja [31].

Kao što je već navedeno, pametni nosivi uređaji mogu biti kibernetičko ugroženi. Postoje tzv. bijeli napadači, tj. „dobri“ napadači. Oni pomažu poslovnim organizacijama kako bi uočili slabosti svojih proizvoda, odnosno programa i softvera te pomažu u otkrivanju sigurnosnih propusta [31].

4. METODE ZAŠTITE I PREVENCIJE OD KIBERNETIČKIH PRIJETNJI

Nakon analize metoda kibernetičkih napada pametnih mobilnih i nosivih uređaja, u ovom radu bit će obrađene i metode zaštite pametnih mobilnih i nosivih uređaja. Mobilna tehnologija nudi niz hardverskih i softverskih rješenja za sigurnosnu zaštitu mobilnih i nosivih uređaja. Zaštita mobilnih uređaja i aplikacija jedan je od zahtjevnih izazova koji osiguravaju sigurnost i privatnost korisnika. Sigurnosne protumjere trebaju zaštititi sve podatke, informacije i aplikacije u svim fazama njihovog korištenja [32].

Za pametne nosive uređaje navedena su četiri rješenja za sigurnost i privatnost pametnih nosivih uređaja [6]:

- nosivi uređaj kao samostalni uređaj – nema potrebe za povezivanjem s drugim uređajem
- dodavanje različitih pravila za održavanje privatnosti korisnika – korisnik treba biti upoznat s dokumentacijom i uputama uređaja, kako bi znao tko ima pristup njegovim podacima i koji podaci se dijele
- korisničke upute i uvjeti korištenja – dodavanje smjernica za korištenje od strane proizvođača
- transparentnost s korisnicima – razvojni programeri trebaju korisnicima omogućiti informacije o njihovim pametnim nosivim uređajima

Postoji nekoliko metoda zaštita i prevencija od kibernetičkih prijetnji koje se koriste na pametnim mobilnim i nosivim uređajima, a one su [33]:

- sigurnosna kopija podataka
- osiguranje korisničkih uređaja i mreže
- enkripcija osjetljivih i privatnih podataka
- višestruka provjera autentičnosti
- korištenje kompleksnih zaporki
- poduka korisnika mobilnih i nosivih uređaja.

4.1. SIGURNOSNA KOPIJA PODATAKA

Sigurnosna kopija podataka je kopija ili arhiva važnih podataka koji su pohranjeni na pametnom mobilnom ili nosivom uređaju. Svrha sigurnosne kopije podataka je omogućavanje vraćanja svih podataka koji su se nalazili na mobilnom ili nosivom uređaju u slučaju krađe, gubitka, određene metode kibernetičkog napada ili prestanka rada pametnog mobilnog ili nosivog uređaja. Ona se obično pohranjuje na sigurnom, odvojenom mjestu od izvornog uređaja, primjerice na oblaku. Istraživanja [34] pokazuju da 30% korisnika ne vrše sigurnosnu kopiju podataka, a otprilike 70 milijuna mobilnih telefona godišnje je izgubljeno ili ukradeno, čak 113

mobilnih telefona su izgubljeni ili ukradeni svake minute. Također, procjenjuje se da se putem metode kibernetičkog napada *ransomware* neovlašteno pristupljuje određenoj poslovnoj organizaciji svakih 14 sekundi u danu. Smisao sigurnosne kopije podataka je sačuvati važne podatke poput privatnih ili poslovnih, fotografija, kontakata, poruka ili poziva [34].

Uobičajena rješenja za sigurnosnu kopiju podataka su: prijenosni mediji male pohrane, vanjski tvrdi diskovi koji imaju dovoljno prostora za pohranu i sigurnosna kopija u oblaku prilagodljive pohrane. Najvažnije od svega je redovno sigurnosno kopirati podatke na jednu ili više usluga od prethodno navedenih [34].

Prijenosni mediji male pohrane odnose se na uređaje koji se koriste za prijenos datoteka na drugi uređaj. Pod uređaje male prijenosne pohrane spadaju: CD, DVD i USB. Što se tiče kapaciteta pohrane, neki mogu biti samo 128 MB, dok ostali imaju mogućnost pohranjivanja do 256 GB. Pametni mobilni uređaji mogu pohraniti od 32 GB do 256 GB. Primjerice, s pametnog mobilnog uređaja moguće je podatke pohraniti na USB pogon [34].

Vanjski tvrdi diskovi su povezani s računalom ili prijenosnim računalom. Povezanost je moguća putem kabela ili bežično. Vanjski tvrdi diskovi mogu biti USB *flash* pogoni i pogoni čvrstog stanja (eng. *Solid-State Drive* – SSD). Prijenosni su i jednostavni za korištenje, ali mogu pohraniti veće datoteke od 128 GB do 10 TB. Najviše se koriste za sigurnosnu kopiju podataka s računala [34].

Sigurnosna kopija podataka u oblaku omogućava sigurnosno kopiranje podataka na hardver koji se nalazi na udaljenoj lokaciji. Korisnici mogu pristupiti vlastitim podacima i upravljati njima u bilo koje vrijeme i s bilo koje lokacije na pametnom mobilnom uređaju putem Internet mreže. Najpoznatija rješenja koja se koriste za pohranu su: *iCloud*, *Google Drive* i *Dropbox*. Većina usluga za pohranu podataka u oblaku imaju veliku količinu pohrane te su sve usluge kompatibilne s pametnim mobilnim uređajima. Svi podaci su kriptirani zbog sigurnosti podataka [34].

4.2 OSIGURANJE KORISNIČKIH UREĐAJA I MREŽE

Kako bi korisnički uređaji i mreža bili osigurani treba redovno provoditi ažuriranje softvera, odnosno operativnog sustava i antivirusnih softvera. Ažuriranja softvera mogu sadržavati važne sigurnosne nadogradnje za nedavne viruse i kibernetičke napade. Većinu ažuriranja operativnog sustava moguće je zakazati u bilo koje, korisniku odgovarajuće vrijeme. Primjerice, pametni mobilni uređaji se najčešće ne koriste tijekom noći, tako da se u navedeno doba operativni sustav može ažurirati. Ažuriranja su od velikog značaja jer popravljaju ozbiljne sigurnosne propuste te je stoga vrlo važno redovito ažurirati operativni sustav. U suprotnom moguće je da pametni mobilni ili nosivi uređaj poput pametnog sata neće funkcionirati kao uobičajeno. Osim ažuriranja softvera, preporuča se instalirati sigurnosni softver na pametni mobilni uređaj kako bi se spriječili potencijalni kibernetički napadi. Primjeri sigurnosnih softvera

su antivirusni filteri, antišpijunski filteri i filteri neželjene pošte, koji smanjuju mogućnost kibernetičkog napada na mobilni uređaj. Što se tiče neželjene pošte i *phishing* elektroničke pošte koju prima pametni mobilni uređaj, potrebno je koristiti filtere neželjene pošte, odnosno anti-spam filtere [35].

Korisničke uređaje i mrežu moguće je zaštititi korištenjem vatrozida (engl. *Firewall*). Vatrozid je softver ili *firmware* koji sprječava neovlašteni pristup mreža. *Firmware* je softver koji pruža osnovne strojne upute koje omogućuju hardveru da funkcionira i komunicira s drugim softverom koji radi na uređaju. Vatrozid provjerava dolazni i odlazni promet koristeći skup pravila za prepoznavanje i blokiranje prijetnji. Vatrozidi su od velikog značaja zato što imaju veliki utjecaj na moderne sigurnosne tehnike. Njihova prva pojava bila je u ranim danima Interneta, kad su mreže trebale nove sigurnosne metode koje su mogle podnijeti sve veću kompleksnost zaštite uređaja. Od tada su vatrozidi postali temelj mrežne sigurnosti u modelu klijent-poslužitelj [33]. Danas većina uređaja koristi vatrozid ili slične alate za pregled prometa i ublažavanje kibernetičkih prijetnji. Vatrozid funkcionira na način da postavlja granicu između vanjske i unutarnje mreže. Postavlja se u unutarnju mrežu i pregledava sve pakete koji dolaze i odlaze iz zaštićene mreže. Vatrozid pregledava pakete na način da koristi unaprijed konfiguriran skup pravila za prepoznavanje zlonamjernih paketa. Paket sadrži informacije o podacima koji su konfigurirani za prijenos putem Interneta. Vatrozidi imaju omogućeno korištenje istih informacija o paketu kako bi utvrdili pridržava li se određeni paket unaprijed konfiguriranog skupa pravila. Ukoliko nije tako, paket ima zabranu ulaska u zaštićenu mrežu [36].

Mobilni vatrozid je sličan standardnom vatrozidu, ali također pruža zaštitu za mobilne korisnike povezane na mrežni sustav. Navedena vrsta vatrozida djeluje kao virtualna ograda između mobilnih uređaja i mreže, nadzire sav dolazni promet prije nego što mu se dopusti pristup mrežnim resursima. Nakon što je dolazni promet odobren, prolazi kroz vatrozid i omogućen mu je pristup bilo kojoj od traženih mrežnih usluga. Korisnik pametnog mobilnog uređaja šalje zahtjev mreži za provjeru, mobilni vatrozid kontaktira bazu podataka i provjerava autentičnost uređaja na popisu ovlaštenih pretplatnika. Ukoliko se pronađe podudaranje u bazi podataka, otvara se vatrozid i pametnom mobilnom uređaju se omogućava pristup uslugama na traženoj mreži. U suprotnom, pametnom mobilnom uređaju nije dopušten pristup i veza je odbijena. Ako je mreža projektirana za značajne količine povezanih mobilnih uređaja, koristiti će se više povezanih mobilnih vatrozida za obradu zahtjeva za autentifikaciju [37].

4.3. ENKRIPCIJA OSJETLJIVIH I PRIVATNIH PODATAKA

Jedan od načina zaštite podataka na uređaju je enkripcija. Enkripcija podataka je proces kodiranja podataka na način da samo ovlašteni korisnici imaju pristup šifriranim podacima. Osjetljivi podaci se šifriraju pomoću algoritama za šifriranje, generirajući šifrirani tekst koji je moguće pročitati samo ako je tekst dekriptiran. Pomoću ključa za šifriranje moguće je pristupiti

podacima, a ukoliko se on izgubi ili ošteti postoji vjerojatnost da neće biti moguće vratiti šifrirane podatke. Postoji i maskiranje podataka koje funkcionira na način da se lažnim podacima zamjenjuju stvarni podaci za neovlaštene korisnike i osigurava se prikrivenost podataka. Dinamično maskiranje podataka vrsta je maskiranja podataka koje može transformirati podatke na temelju korisničkih uloga i privilegija. Uz maskiranje podataka, podaci se zadržavaju u izvornom obliku i nije potreban ključ za dešifriranje. Enkripciju je moguće primijeniti na krajnje pogone, poslužitelje, elektroničku poštu, baze podataka i datoteke. Kod pametnih mobilnih uređaja moguće je šifrirati samo pohranu, a ne cijeli disk. Šifriranoj pohrani moguće je pristupiti pomoću kriptografskog ključa [38].

Kako bi se poboljšala učinkovitost određenog poduzeća te smanjili troškovi, sve više se koristi računalstvo u oblaku i IoT uređaji. Enkripcija služi za zaštitu podataka, no jako malo poduzeća odabire tu opciju. Prema [39], samo je jedna trećina osjetljivih korporativnih podataka pohranjenih u obliku šifrirana. Međutim, ostatak ispitanika smatra da su usluge temeljene na oblaku važne za poslovanje njihovog poduzeća, a 81% smatra da će pohrana u oblaku postati značajna u bliskoj budućnosti. Malo IoT uređaja je osigurano. Jedna od opcija za poboljšanje sigurnosti je šifriranje podataka koji se prenose IoT uređajima, a posebno onima koji se bežično povezuju s mrežom poput pametnih satova [38].

4.4. VIŠESTRUKA PROVJERA AUTENTIČNOSTI, KORIŠTENJE KOMPLEKSNIH ZAPORKI I EDUKACIJA KORISNIKA

Višestruka provjera autentičnosti je slojeviti pristup autentifikaciji, a odnosi se na odobravanje pristupa aplikaciji, računu ili uređaju. Prva razina pristupa je klasično unošenje korisničkog imena i zaporke. Druga razina pristupa odnosi se na unošenje jednokratne zaporke koju je moguće zaprimiti putem SMS poruke ili elektroničke pošte. Osim jednokratne zaporke, koristi se i autentifikacija korištenjem biometrijskih metoda poput skeniranja otiska prsta i prepoznavanja lica [39].

Prednosti višestruke provjere autentičnosti su [39]:

1. povećanje sigurnosti
2. bavi se propisima o usklađenosti
3. smanjuje pravne rizike – smanjuje rizik od kibernetičkih napada i prekida rada sustava, sprječava kršenje dogovora o razini usluge (engl. *Service Level Agreement* – SLA)
4. smanjuje mogućnost kršenja lozinki – omogućuje siguran zamjenski mehanizam za zaštitu podataka
5. poboljšava funkcionalnost – korištenje biometrijskih metoda poput otiska prsta.

Obzirom na korištenje kompleksnih zaporki, prema Microsoftu, kompleksna zaporka sastoji se od najmanje sedam znakova, a uključuje: velika i mala slova, numeričke znakove i simbole poput $, #, *, & ili !. Napadači najlakše pristupe korisničkom računu ukoliko korisnička zaporka sadrži korisničko ime i prezime, inicijale, mjesto rođenja ili drugi javno dostupni podatak o korisniku. Iz tog razloga potrebno je postaviti što kompleksniju zaporku, kako bi se napadačima otežao ili onemogućio pristup u korisnikov račun ili pametni mobilni ili nosivi uređaj [39].

Ukoliko korisnici nisu dovoljno educirani o metodama kibernetičkih napada, iste će postajati sve češće. Potrebno je korisnicima omogućiti edukaciju o stvaranju što kompleksnije zaporke, višestrukoj provjeri autentičnosti, sigurnosnoj kopiji podataka, osiguranju korisničkih pametnih mobilnih i nosivih uređaja i mreže te enkripciji osjetljivih i privatnih podataka. Metode kibernetičkih napada moguće je smanjiti ako korisnici nauče kako prepoznati kibernetički napad i kako postupiti ukoliko naiđu na kibernetički napad [39].

Za pametne nosive uređaje postoje sigurnosne postavke na uređaju kojima se može zaštititi podatke. Neke od njih su [31]:

- blokiranje neovlaštenog uparivanja
- dvostruka autentifikacija
- zaštita zaporkom na zaključanom zaslonu, postavljanje PIN-a ili uzorka
- zaključavanje ukoliko je pametni nosivi uređaj predaleko od mobilnog uređaja.

5. PROGRAMSKI ALATI ZA ZAŠTITU OD KIBERNETIČKIH PRIJETNJI

Kako bi se pametni mobilni i nosivi uređaji zaštitili od neželjenih napada, postoje razni programi za zaštitu od kibernetičkih napada. Programi, odnosno aplikacije koje su potrebne za zaštitu od metoda kibernetičkih napada na pametnom mobilnom i nosivom uređaju, opisani su u nastavku ovog rada [40]:

1. *Avast Antivirus & Security*
2. *Malwarebytes Mobile Security*
3. *VIPRE Android Security*
4. *Nox Security, Antivirus, Clean*
5. *Safe Security – Antivirus, Booster, Phone Cleaner*
6. *Bouncer – Temporary App Permisions*
7. *Firefox Focus*: privatnost
8. *Sophos Intercept X for Mobile*
9. *Signal Private Messenger*
10. *Secure Call*
11. Google pronađi moj uređaj
12. *NoRoot Firewall*
13. *Orbot: Tor za Android*
14. *LastPass*.

Avast Antivirus & Security program štiti pametni mobilni i nosivi uređaj od virusa i drugih zlonamjernih softvera. Ovim programom moguće je zaštititi internetsku privatnost i očistiti neželjene datoteke. Mogućnosti ovog programa su [41]:

- redovna skeniranja kako bi se otkrile prijetnje i ranjivosti
- prepoznavanje zlonamjernih aplikacija prije instalacije
- blokiranje zlonamjernih veza i web stranica, označavanje onih osjetljivih na svim preglednicima
- provjera sigurnosti određene Wi-Fi mreže.

Avast Antivirus & Security aplikacija prepoznaje metode kibernetičkih napada poput: računalnog trojanskog konja, *ransomware-a*, softvera za oglašavanje i špijunskog softvera. Pomoću ove aplikacije moguće je zaštititi korisničke podatke na daljinu. Daljinsko upravljanje omogućuje sprječavanje napadača pri pristupanju korisničkim podacima i pruža pomoć korisniku za povratak uređaja ukoliko je uređaj izgubljen ili ukraden. Dakle, moguće je pratiti lokaciju uređaja, zaključavanje uređaja i brisanje svih osjetljivih podataka. Aplikacija nudi mogućnosti poboljšanja performansi uređaja poput: oslobađanja prostora za pohranu i ubrzanjem uređaja uz opciju RAM *Boost*. Osim navedenoga, aplikacija omogućuje uvid u digitalno stanje, odnosno

vrijeme korištenje uređaja. Korisnik ima mogućnost vidjeti na kojim aplikacijama provodi najviše vremena, ima mogućnost saznati koje aplikacije je bolje koristiti na Wi-Fi mreži te provjeriti dopuštenja aplikacija kako bi razumio na koji način instalirane aplikacije pristupaju njegovom pametnom mobilnom uređaju. Primjer sučelja *Avast Antivirus & Security* aplikacije naveden je na slici 3 [41].

Slika 3. *Avast Antivirus & Security* aplikacija

Izvor: [41]

Malwarebytes Mobile Security aplikacija za pametni mobilni i nosivi uređaj otkriva i uklanja opasne prijetnje poput zlonamjernog softvera, softvera za oglašavanje i *ransomware-a*. Otkriva *ransomware,* prije nego isti napada i zaključava korisnikov uređaj. Aplikacija omogućava otkrivanje reklamnog softvera i potencijalno neželjenih programa. Osim navedenoga, skenira

internetske poveznice koje žele ukrasti identitet prilikom korištenja *Google Chrome* preglednika te o tome obavještava korisnika. *Malwarebytes Mobile Security* aplikacija identificira privilegije pristupa svakoj aplikaciji na pametnom mobilnom i nosivom uređaju te prikazuje koje aplikacije prate korisnikovu lokaciju, pozive ili dodatno naplaćuju skrivene naknade. Prema [42], dokazano je da *Malwarebytes Mobile Security* aplikacija pronalazi zlonamjerni softver na 39% uređaja koji već imaju instaliran antivirusni program. Kupnjom *Malwarebytes Premiuma* moguće je ukloniti zlonamjerni softver, viruse i druge prijetnje s mobilnog i nosivog uređaja u nekoliko sekundi te zaustaviti buduće moguće kibernetičke napade zaštitom u stvarnom vremenu, koja je dostupna 24/7. Na slici 4 prikazan je primjer skeniranja pametnog mobilnog uređaja, gdje je vidljivo da je u 14:25 minuta skenirano 323 aplikacija i 27035 datoteka te nije pronađen niti jedan zlonamjerni softver [42].

Slika 4. *Malwarebytes* aplikacija

Izvor: [43]

VIPRE Android Security sigurnosna aplikacija štiti pametni mobilni i nosivi uređaj od više od 20 000 poznatih zlonamjernih programa i virusa. Značajke ove aplikacije su [44]:

- autopilot
- skener zlonamjernog softvera
- privatnost računa
- zaključavanje aplikacija

- web zaštita
- zaštita od krađe.

Autopilot je opcija koja nudi duboki uvid u sigurnosni status uređaja, funkcionira kao korisnikov sigurnosni savjetnik. Prilikom instalacije određene aplikacije, skener zlonamjernog softvera štiti pametni mobilni i nosivi uređaj i podatke na njemu od metoda kibernetičkih napada. Skener se pokreće automatski prilikom svake instalacije. Pokretanjem *VIPRE Android Security* aplikacije, moguće je saznati jesu li otkriveni korisnički podaci o računu, primjerice elektroničke pošte, Facebook ili Instagram računa ili bankovnog računa i na taj način moguće je zaštititi privatnost korisničkih podataka. Osim navedenoga *VIPRE Android Security* aplikacija omogućava snimanje fotografije svake osobe koja pokuša neovlašteno pristupiti pametnom mobilnom uređaju. Značajka web zaštita omogućava otkrivanje zlonamjernog sadržaja i održavanje sigurnosti tijekom pregledavanja na mrežnom pretraživaču. Zaštitom od krađe moguće je zaključati, locirati te postaviti zvuk alarma na ukradenom ili izgubljenom pametnom mobilnom ili nosivom uređaju putem daljinskog upravljanja preko Interneta. Kako bi bilo moguće koristiti ovu aplikaciju potrebno je platiti korištenje $15.99/godišnje po jednom pametnom mobilnom ili nosivom uređaju [44].

Nox Security je sigurnosna i antivirusna aplikacija koja nudi sljedeće opcije [45]:

- čistač virusa
- čišćenje prostora za pohranu
- održavanje memorije
- zaključavanje aplikacija zaporkom ili otiskom prsta
- blokiranje neželjenih obavijesti
- zaštita uređaja od pregrijavanja
- sigurnost poruka
- zaštita uređaja od mrežnih kibernetičkih napada
- zaustavljanje aplikacija koje troše energiju mobilnog i nosivog uređaja.

Nox Security aplikacija pruža jake antivirusne usluge, omogućava zaštitu od mobilnih virusa, špijunskog softvera i ostalih internetskih prijevara. Čistač virusa pomaže u pronalaženju i čišćenju virusa te štiti korisničke privatne podatke. Sigurnost uređaja održava se u stvarnom vremenu te korisnik prima upozorenje ukoliko dođe do pojave virusa. Na slici 5. prikazano je sučelje *Nox Security aplikacije* gdje su prikazane značajke aplikacije. [45]

Slika 5. *Nox Security* aplikacija

Izvor: [45]

Safe Security je aplikacija slična prethodnim aplikacijama. Omogućava pojačavanje brzine, čišćenje virusa, optimizaciju pozadinskih aplikacija, pohrane memorije, neželjenih datoteka i napajanja baterije te štiti pametni mobilni i nosivi uređaj od kibernetičkih napada. Omogućava sigurnost automatskim skeniranjem instaliranih aplikacija i svih podataka na uređaju. Pomoću *Safe Security* aplikacije moguće je izbrisati sve nepotrebne datoteke poput predmemorije sustava, predmemorije slika, predmemorije videozapisa i predmemorije oglasa kako bi se oslobodio prostor za pohranu. Uz ovu aplikaciju moguće je i poboljšati instalirane igre na pametnom mobilnom uređaju kako bi bolje radile. Navedena aplikacija sadrži i filter za poruke i pozive. Omogućava blokiranje neželjenih poziva i poruka te dodavanje anonimnih brojeva na crnu listu iz zapisnika poziva i poruka te kontakata. Osim toga, provjerava i štiti pametni mobilni i nosivi uređaj od otvorenih Wi-Fi mreža. Kao i ostale aplikacije *Safe Security* aplikacija nudi opcije: zaključavanja aplikacija, snimanje fotografije osobe koja pokuša neuspješno pristupiti pametnom mobilnom uređaju, zaključavanje otiskom prsta te zaštita u stvarnom vremenu [46].

Bouncer aplikacija služi za zadržavanje ili uklanjanje svih dozvola aplikacije koje su potrebne kako bi aplikacija funkcionirala. Ukoliko korisnik ne želi da se kamera i mikrofon koriste konstantno u određenoj aplikaciji, *Bouncer* aplikacija omogućava korištenje kamere i mikrofona u istoj aplikaciji samo privremeno, dok korisnik ne izađe iz aplikacije. Čim korisnik izađe iz

aplikacije, *Bouncer* automatski uklanja dopuštenje korištenja kamere ili mikrofona. Dakle, aplikacija je dizajnirana za sva jednokratna dopuštenja. Obzirom da *Bouncer* aplikacija nema omogućen pristup Internetu, znači da ukoliko i dođe do preuzimanja osjetljivih podataka, ne može ih prenijeti nigdje [47].

Firefox Focus je aplikacija koja omogućava bezbrižno pretraživanje. Nudi opcije blokiranja ostalih korisnika koji prate drugog korisnika na Internetu. Služi za brisanje povijesti pregledavanja, zaporki i kolačića kako korisnika ne bi ometali neželjeni oglasi. Obzirom da nudi prethodne opcije, moguće je da će pretraživanje biti brže nego inače na običnom pregledniku [48].

Sophos Intercept X je aplikacija koja štiti pametne mobilne i nosive uređaje od zlonamjernog softvera i ostalih metoda kibernetičkih napada. Pri tome, skenira aplikacije i podatke na pametnom mobilnom i nosivom uređaju u potrazi za zlonamjernim ili neprikladnim sadržajem. *Sophos Intercept X* aplikacija provjerava web stranice te ukoliko postoji zlonamjerni ili neprikladni sadržaj, ona blokira takvu web stranicu, samim time provjerava i poveznice na određenu web stranicu. Aplikacija omogućava savjetnike za sigurnost i privatnost pametnog mobilnog i nosivog uređaja te sigurnosne provjere prilikom skeniranja QR kodova. Nudi zaštitu aplikacija zaporkama te bazu podataka svih korištenih zaporki kojoj može pristupiti samo korisnik. Osim toga nudi opciju autentifikator koja označava stvaranje jednokratnih zaporki višestrukom autentifikacijom. Aplikaciji su potrebne određene dozvole, no ne prikuplja nikakve korisničke podatke, čak ni podatke koji su joj potrebni za rad [49].

Signal Private Messenger je aplikacija koja omogućava besplatnu izmjenu poruka, poziva ili video poziva. Omogućava sigurnost i privatnost koristeći s kraja na kraj (engl. *end-to-end*) enkripciju što označava da se ništa ne pohranjuje na njihovom poslužitelju. Ukoliko primatelj nema instaliranu *Signal Private Messenger* aplikaciju svejedno je moguće šifrirati poslane poruke [40].

Postoji i *Secure Call* aplikacija koja omogućava glasovne pozive za pametne mobilne uređaje, a pri tome je anonimna, koristi od točke do točke (engl. *peer-to-peer* – P2P) komunikaciju i s kraja na kraj enkripciju. Osigurava kvalitetne i šifrirane glasovne pozive čak i uz 2G mrežu. Komunikacija od točke do točke u ovoj aplikaciji označava da poslužitelji usluge *Secure Call* povezuju samo pozivatelja i primatelja poziva. Nakon toga, svi podaci se razmjenjuju izravno između pozivatelja i primatelja poziva uz enkripciju. Omogućava potpunu anonimnost jer nisu potrebni korisnički podaci poput broja mobitela, adrese elektroničke pošte i sličnih podataka. Time je nemoguće otkriti identitet korisnika. Funkcionira na način da se prilikom instalacije aplikacije generira jednokratni broj sigurnog poziva [50].

„Google pronađi moj uređaj“ je aplikacija koja omogućava pronalazak izgubljenog ili ukradenog pametnog mobilnog ili nosivog uređaja. Putem aplikacije moguće je zaključati mobilni uređaj ili pametni sat, pronaći ih na karti, a ukoliko nije dostupna trenutna lokacija, moguće je vidjeti posljednju zabilježenu lokaciju. Također je moguće udaljenim putem upaliti zvukove i alarme na mobilnom uređaju ili pametnom satu. Osim toga, moguće je izbrisati sve podatke s uređaja ili zaključati uređaj i postaviti prilagođenu poruku na zaključanom zaslonu [51].

NoRoot Firewall je aplikacija koja kontrolira koriste li se mobilni podaci nepotrebno. Omogućava kontrolu pri korištenju Interneta. Osim toga, *NoRoot Firewall* nudi opciju biranja može li određena aplikacija pristupiti Internetu samo putem Wi-Fi-ja ili samo korištenjem mobilnih podataka ili niti jedno niti drugo [40].

Orbot je aplikacija koja koristi *The Onion Router* (TOR) pretraživač te omogućuje usmjeravanje mrežnog prometa kroz TOR mrežu. TOR mreža sprječava analizu prometa, koristi distribuiranu anonimnu mrežu, *Onion* komutaciju i skrivene usluge. *Onion* komutacija označava šifriranje sadržaja u više slojeva što podsjeća na luk (engl. *Onion*). Aplikacija *Orbot* stvara privatnu mobilnu podatkovnu vezu gdje se podaci svaki put iznova šifriraju. Podaci su kroz cijelu TOR mrežu šifrirani, sve dok se ne dođe do posljednje mreže gdje se dešifriraju i odlaze prema krajnjem uređaju. Time se sprječava praćenje korisnika [40].

LastPass aplikacija omogućava upravljanje zaporkama koje korisnik koristi za različite račune. Korisnik ima mogućnost pristupiti svojim zaporkama s bilo kojeg uređaja. Pristup *LastPass* aplikaciji je šifriran tajnom „glavnom“ zaporkom. Dakle potrebna je jedna „glavna“ zaporka kako bi korisnik pristupio svim ostalim zaporkama [40].

6. ZAKLJUČAK

Kako godinama napreduje tehnologija, tako raste učestalost kibernetičkih napada na pametne mobilne i nosive uređaje. Ovaj završni rad donosi šest izvora kibernetičkih napada, a to su: fizički, aplikacijski, web i mrežno zasnovane prijetnje te socijalni inženjering i korištenje vlastitog uređaja u poslovne svrhe. Prethodnim metodama kibernetičkih napada, najčešće se napada na pametne mobilne uređaje koji su Bluetooth-om i aplikacijom povezani na pametne nosive uređaje. Napadač ima mogućnost pristupiti korisničkim podacima putem pametnog sata, a ti podaci se najčešće odnose na bankovne podatke i trenutnu lokaciju.

Korisnik ima mogućnost zaštititi se od kibernetičkih napada na pametne mobilne i nosive uređaje. Kao metode zaštite i prevencije od kibernetičkih prijetnji, u ovom završnom radu, obrađene su: sigurnosna kopija podataka, osiguranje korisničkih uređaja i mreže, enkripcija osjetljivih i privatnih podataka, višestruka provjera autentičnosti, edukacija korisnika te korištenje kompleksnih zaporki. Korisnik treba više pažnje posvetiti sigurnosti vlastitih podataka. Postoje korisnici koji svjesno ispunjavaju određene sumnjive i neprovjerene obrasce svojim osjetljivim podacima i tako daju otvoreni pristup napadaču.

Kako bi se spriječile razne metode kibernetičkih napada koje su obrađene u ovom završnom radu, postoje i programski alati, odnosno aplikacije koje sprječavaju kibernetičke napade. Postoji 14 aplikacija koje se mogu instalirati na pametni mobilni uređaj.

Prvi korak u zaštiti vlastitog uređaja od napada je edukacija korisnika. Korisniku treba objasniti kako funkcioniraju metode kibernetičkih napada, kako prepoznati sumnjive poveznice na Internetu te sumnjive elektroničke i SMS poruke. Potrebno je i obratiti pažnju na sve dozvole korištenja podataka na koje korisnik pristaje instalacijom aplikacije na vlastiti pametni mobilni uređaj. Kako bi se osigurala sigurnost djece, važno je obratiti pažnju je li pametni sat određenog proizvođača zaista siguran.

LITERATURA

[1] A.S. Tanenbaum. *Computer Networks*. Prentice Hall, 1996.

[2] Tehnologija telekomunikacijskog prometa 1. *Mobilne mreže*. Preuzeto s: https://moodle.srce.hr/2021-2022/pluginfile.php/5657928/mod_resource/content/4/Mobilne%20mre%C5%BEe%2020202021za%20objavu.pdf [Pristupljeno: srpanj 2022.]

[3] Liović H. *Razvoj telekomunikacijskih mobilnih sustava*. Završni rad. Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek; 2019. Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:200:980924 [Pristupljeno: srpanj 2022.]

[4] Hrvatski Telekom. *Digitalna izložba*. Preuzeto s: https://www.ht-muzej.hr/mobilne-mreze-u-novom-tisucljecu/ [Pristupljeno: rujan, 2022.]

[5] Alrababah Z. Privacy and Security od Wearable Devices. *International Journal of Innovative Science and Research Technology*. 2020;5(12): 289-305. Preuzeto s: https://ijisrt.com/assets/upload/files/IJISRT20DEC242.pdf [Pristupljeno: rujan 2022.]

[6] Ometov A, Shubina V, Klus L… Lohan ES. A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks.* 2021;193 (108074): 1-37. Preuzeto s: https://www.sciencedirect.com/science/article/pii/S1389128621001651 [Pristupljeno: rujan 2022]

[7] Hervis. *Sve o pametnim satovima*. Preuzeto s: https://www.hervis.hr/store/pametni_satovi [Pristupljeno: srpanj 2022.]

[8] Erich Hartmann. *Pametni satovi povijest i dizajn.* Preuzeto s: https://hr.erich-hartmann.com/pametni-satovi-povijest-os-aplikacije-i-dizajn.html#operativni-sustavi-smartwatch [Pristupljeno: srpanj 2022.]

[9] Tahiri D. *Mogućnosti i sigurnost primjene nosivih terminalnih uređaja.* Završni rad. Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2017. Preuzeto s: urn:nbn:hr:119:248625 [Pristupljeno: srpanj 2022.]

[10] Britannica. *Computer security*. Preuzeto s: https://www.britannica.com/technology/computer-security. [Pristupljeno: srpanj 2022.]

[11] IGI Global. *Security attack*. Preuzeto s: https://www.igi-global.com/dictionary/big-data-security-management/43257 [Pristupljeno: srpanj 2022.]

[12] Terminalni uređaji. *Sigurnost primjene terminalnih uređaja.* Preuzeto s: https://moodle.srce.hr/20212022/pluginfile.php/5443921/mod_resource/content/2/7_Sigurnost_terminalnih_ure%C4%91aja_21_22.pdf [Pristupljeno: srpanj 2022.]

[13] Oštrić D. I. *Sigurnosni aspekti i metode zaštite informacijskih sustava*. Završni rad. Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2015. Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:119:692260 [Pristupljeno: srpanj 2022.]

[14] Mankas I. *Sigurnost Bluetooth uređaja*. Završni rad. Sveučilište u Zagrebu, Fakultet organizacije i informatike; 2021. Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:211:258099 [Pristupljeno: rujan 2022]

[15] Tutorials point. *What are the Physical Threats in Information Security?*. Preuzeto s: https://www.tutorialspoint.com/what-are-the-physical-threats-in-information-security# [Pristupljeno: srpanj 2022.]

[16] Bullguard. *The Dangers of Recycling your Smartphone*. Preuzeto s: https://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/the-dangers-of-recycling-your-smartphone.aspx [Pristupljeno: srpanj 2022.]

[17] Cisco. *What Is Malware?*. Preuzeto s: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html [Pristupljeno: srpanj 2022.]

[18] Fortinet. *What Are Computer Viruses?*. Preuzeto s: https://www.fortinet.com/resources/cyberglossary/computer-virus [Pristupljeno: srpanj 2022.]

[19] Norton. *What is a computer worm, and how does it work?*. Preuzeto s: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html [Pristupljeno: srpanj 2022.]

[20] Fortinet. *What is Spyware?*. Preuzeto s: https://www.fortinet.com/resources/cyberglossary/spyware [Pristupljeno: srpanj 2022.]

[21] Norton. *What Is Adware?*. Preuzeto s: https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html [Pristupljeno: srpanj 2022.]

[22] Fortinet. *What Is Ransomware?*. Preuzeto s: https://www.fortinet.com/resources/cyberglossary/ransomware [Pristupljeno: srpanj 2022.]

[23] Norton. *What is fileless malware and how does it work?*. Preuzeto s: https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html [Pristupljeno: srpanj 2022.]

[24] Cisco. *What is phishing?* Preuzeto s: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works [Pristupljeno: srpanj 2022.]

[25] Norton. *What is smishing + smishing attack protection tips for 2022.* Preuzeto s: https://us.norton.com/internetsecurity-emerging-threats-smishing.html [Pristupljeno: srpanj 2022.]

[26] Mišić V. *Istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju*. Diplomski rad. Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2016. Preuzeto s: urn:nbn:hr:119:786663 [Pristupljeno: srpanj 2022.]

[27] Imperva. *Social Engineering*. Preuzeto s: https://www.imperva.com/learn/application-security/social-engineering-attack/ [Pristupljeno: srpanj 2022.]

[28] Perception Point. *BYOD Security: Threats, Security Measures and Best Practices*. Preuzeto s: https://perception-point.io/byod-security-threats-security-measures-and-best-practices/ [Pristupljeno: srpanj 2022.]

[29] Zimo. *Zabranjena prodaja dječjih pametnih satova*. Preuzeto s: https://zimo.dnevnik.hr/clanak/njemacka-zabranjuje-prodaju-pametnih-satova-za-djecu---496585.html [Pristupljeno: kolovoz 2022.]

[30] Netokracija. *Dječji pametni satovi: Više sigurnosti ili izloženost hakerima?*. Preuzeto s: https://www.netokracija.com/djecji-pametni-satovi-182303 [Pristupljeno: kolovoz 2022.]

[31] Kaspersky. *Should You Worry About Smartwatch Security?*. Preuzeto s: https://www.kaspersky.com/resource-center/threats/smartwatch-security-risks [Pristupljeno: kolovoz 2022.]

[32] Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, I.Romdhani. *Artificial Intelligence and Blockchain for Future Cybersecurity Applications.* Springer, 2021.

[33] Paun L. *Pregled metoda i alata zaštite osobnih računala od kibernetičkih prijetnji.* Završni rad. Sveučilište u Zagrebu, Fakultet prometnih znanosti; 2021. Preuzeto s: urn:nbn:hr:119:965688 [Pristupljen: kolovoz 2022.]

[34] Norton. *Data backup: Why it's important plus strategies to protect your information.* Preuzeto s: https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html [Pristupljeno: kolovoz 2022.]

[35] Business Australian Government. *Protect your business from cyber threats.* Preuzeto s: https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats [Pristupljeno: kolovoz 2022.]

[36] Techtarget. *Firewall*. Preuzeto s: https://www.techtarget.com/searchsecurity/definition/firewall [Pristupljeno: kolovoz 2022.]

[37] NetMotion Software. *How does a mobile firewall work?.* Preuzeto s: https://www.netmotionsoftware.com/blog/security/mobile-firewall [Pristupljeno: kolovoz 2022.]

[38] eSecurity Planet. *Data Encryption Protocols & Software*. Preuzeto s: https://www.esecurityplanet.com/networks/encryption/ [Pristupljeno: kolovoz 2022.]

[39] Spiceworks. *What Is Multi-Factor Authentication? Definition, Key Components, and Best Practices.* Preuzeto s: https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-multi-factor-authentication/ [Pristupljeno: kolovoz 2022.]

[40] Geekflare. *14 Security Apps to Protect Your Android Devices*. Preuzeto s: https://geekflare.com/android-security-apps/ [Pristupljeno: kolovoz 2022.]

[41] Avast. *Avast Mobile Security for Android*. Preuzeto s: https://www.avast.com/en-au/free-mobile-security#block-threats [Pristupljeno: kolovoz 2022.]

[42] Malwarebytes. *Cybersecurity. For every one.* Preuzeto s: https://www.malwarebytes.com/ [Pristupljeno: kolovoz 2022.]

[43] Google Play. *VIPRE Android Security.* Preuzeto s: https://play.google.com/store/apps/details?id=com.ssd.android.vipre&hl=hr&gl=US [Pristupljeno: kolovoz 2022.]

[44] Google Play. *Nox Security, Antivirus, Clean*. Preuzeto s: https://play.google.com/store/apps/details?id=com.noxgroup.app.security [Pristupljeno: kolovoz 2022.]

[45] Google Play. *Safe Security - Antivirus, Booster, Phone Cleaner*. Preuzeto s: httpgs://play.google.com/store/apps/details?id=com.qihoo.security [Pristupljeno: kolovoz 2022.]

[46] Google Play. *Bouncer - Temporary App Permissions*. Preuzeto s: https://play.google.com/store/apps/details?id=com.samruston.permission [Pristupljeno: kolovoz 2022.]

[47] Moz://a. *Firefox Focus*. Preuzeto s: https://www.mozilla.org/en-US/firefox/browsers/mobile/focus/ [Pristupljeno: kolovoz 2022.]

[48] Google Play. *Sophos Intercept X for Mobile*. Preuzeto s: https://play.google.com/store/apps/details?id=com.sophos.smsec&hl=en [Pristupljeno: kolovoz 2022.]

[49] Google Play. *Secure Call.* Preuzeto s: https://play.google.com/store/apps/details?id=com.securecallapp&hl=en [Pristupljeno: kolovoz 2022.]

[50] Google Play. *Google pronađi moj uređaj*. Preuzeto s: https://play.google.com/store/apps/details?id=com.google.android.apps.adm [Pristupljeno: kolovoz 2022.]

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____**završni rad**_____
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu **završnog rada** pod naslovom _____**Sigurnosni izazovi pametnih mobilnih i nosivih uređaja**_____, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, _____9/6/2022_____

MIHAELA RIPLI, Mihaela Ripli
(ime i prezime, *potpis*)