Sigurnost i privatnost u okruženju pametnog grada

Stanić, Maja

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

SIGURNOST I PRIVATNOST U OKRUŽENJU PAMETNOG GRADA

Završni rad

Maja Stanić

Osijek, 2017.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 07.09.2017.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Maja Stanić
Studij, smjer:	Preddiplomski sveučilišni studij Elektrotehnika
Mat. br. studenta, godina upisa:	3960, 19.07.2014.
OIB studenta:	81432401462
Mentor:	Doc.dr.sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Sigurnost i privatnost u okruženju pametnog grada
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Predložena ocjena završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene mentora:	07.09.2017.
Datum potvrde ocjene Odbora:	11.09.2017.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 20.09.2017.

Ime i prezime studenta:	Maja Stanić
Studij:	Preddiplomski sveučilišni studij Elektrotehnika
Mat. br. studenta, godina upisa:	3960, 19.07.2014.
Ephorus podudaranje [%]:	2%

Ovom izjavom izjavljujem da je rad pod nazivom**: Sigurnost i privatnost u okruženju pametnog grada**

izrađen pod vodstvom mentora Doc.dr.sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj:

1. UVOD

Gradovi se već stoljećima smatraju važnim razvojnim centrima te ih povezujemo s inovacijama i bogatstvom. Imaju visok doprinos bruto domaćem proizvodu (BDP) svojih zemalja. Razvojem ekonomije i društvenih transformacija ljudi sve više migriraju iz sela u gradove, što za posljedicu ima veću urbanizaciju. Predviđa se da će se broj ljudi u gradovima povećavati, što će rezultirati većim mogućnostima života u gradu vezanih za ekonomiju i socijalni razvoj grada. Dakako naglo povećanje stanovnika u gradovima ima i neželjene efekte kao što su klimatske promjene, energetske promjene te promjene u načinu života ljudi. Javlja se sve više usluga koje omogućuju bolju informiranost ljudi o prometu, obrazovanju, zdravlju i dr. Da bi se smanjili troškovi, poboljšala učinkovitost i poboljšala kvaliteta života građana, gradovi sve više usredotočuju svoje studije na razvoj informacijskih i komunikacijskih tehnologija. Razvojem tehnologije i aplikacija koje nam olakšavaju život raste i briga o dostupnosti privatnih podataka. U završnom radu biti će predstavljene prijetnje koje se javljaju u pametnim gradovima te će se pojedinačno obraditi gradski sektori, problemi i rješenja.

1.1. Zadatak završnog rada

Okruženje pametnog grada (zahvaljujući primjeni velikog broja različitih naprednih informacijsko-komunikacijskih tehnologija) pruža svojim stanovnicima (stalnim i gostujućim) različite inteligentne usluge unutar različitih područja (transport, zdravstvena skrb, zabava, energetska učinkovitost...). Za pružanje ovih usluga neophodno je prikupljanje i razmjena velikih količina podataka, koji su često privatne i vrlo osjetljive prirode. Potrebno je sustavno i analitički istražiti problematiku sigurnosti i privatnosti unutar aplikacija i usluga pametnog grada. Potrebno je analizirati (i međusobno usporediti) postojeće metode kojima se u ovakvom okruženju rješavaju problemi sigurnosti i privatnosti korisnika usluga i njihovih podataka, kao i glavne smjernice budućeg razvoja ovih metoda. Također je potrebno prepoznati i istaknuti koji su glavni trenutačno otvoreni problemi u ovom području koje je u budućnosti nužno riješiti. Potrebno je specificirati i razraditi mogući sigurnosni okvir primjenjiv u ovakvom okruženju.

2. INFORMACIJSKA SIGURNOST

Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. I obuhvaća:

- privatnost,
- integritet,
- dostupnost.

Ta tri pojma definirat će se na sljedeći način:

- Privatnost- koncept privatnosti dopušta pristup podacima samo s točnom dozvolom.

Npr. ako se poruka šalje od A točke do B, a C točka je u mogućnosti prisluškivati poruku, poruka će biti privatna ako C točka nije u mogućnosti pročitati poruku.

- Integritet-koncept integriteta vezuje se za zadržavanje vrijednosti koja bi mogla biti podatak ili paket bez neovlaštenih promjena.

Npr. ako točka A šalje poruku točki B, a točka C mijenja poruku i šalje je ponovno na B točku, ova poruka će se smatrati integritetno neprekinuta ako točka B može otkriti da je nastala promjena i odbaciti poruku.

- Dostupnost-unatoč povezanosti sa hardware-ima i fizičkim poslužiteljima, ovo svojstvo svrstava se u sigurnosna pitanja kada osoba sa dozvolom može pristupiti podacima.

Npr. A točka šalje svoju poruku točki B, C točka ne može čitati poruka zato jer poruka ima svoju privatnost. B točka otkriva da je poruka nepromijenjena, tako da je integritet također provjeren. Konačno, kada B točka otključa poruku, može se reći da je dostupnost osigurana ako je sadržaj poruke na raspolaganju točki B.

U daljnjem dijelu rada predstavljena su glavna sigurnosna pitanja.

- Pristup informacijama iz aplikacija-uređaji mogu pristupiti paketu na različite načine i na različitim lokacijama. Stoga se za smanjenje latencije koriste lokalne kopije i predmemorijske vrijednosti tih paketa.
- Praćenje podataka- iznimno je važno da informacije koje koristi sustav B, a koje su izvorno iz sustava A ne mogu biti praćene natrag na svoj izvorni sustav.
- Praćenje građana – nijedna od informacija koje senzor sadrži ne smije se koristiti za praćenje građana, njihovih postupaka i dr.

- Gubitak podataka-pametni sustavi mogu dobiti pristup uređajima, kao što su pametni telefoni, tableti, gadgeti i dr. Ti uređaji omogućuju širok raspon podataka, kao što su slike, poruke, brojevi bankovnih računa i dr. Potrebno je spriječiti pristup takvim informacijama. Poželjno je upotrebljavati lokalne alate za pohranu ili API-je da bi se zadržali u uređajima..
- Prekoračeni pristup informacijama u podatkovnim centrima- ako se na bilo koji način krši sigurnost podataka bilo prilikom pohrane, analiziranja ili upravljanja, sustav može biti ugrožen. Npr. prilikom pristupa informacijama o studentu, korisnik može dobiti uvid u njegov policijski dosjee. Do toga može doći jer oba sustava imaju ista dopuštenja.
- Neovlašten pristup na strani klijenta- razmotrit će se informacije koje su promijenjene od A do B. Ako sustav A sprema studentove ocjene na pametni telefon, a sustav B koristi isti mehanizam za pohranu podataka o bankovnom računu, ako uređaj ne pruža izolaciju sustavima A i B, može doći do njihove zlouporabe.
- Nedostatak sigurnosti- jedan od glavnih rizika za WEB aplikacije odnosi se na injektiranje koda. Ovaj nedostatak odnosi se na sustave koji ne potvrđuju podatke na različitim slojevima i zaraženi su informacijama sa drugih uređaja.

3. POJAM PAMETNOG GRADA

Pametni grad se definira kao sustav koji koristi digitalne i komunikacijske tehnologije kako bi zadovoljio sve potrebe stanovništva te unaprijedio učinkovitost gradskih usluga, smanjio troškove i potrošnju energije. Također, vodi računa o okolišu i podiže životni standard građanstva. Pametni grad povezuje sve funkcije javnih usluga poput prometa, javne rasvjete i proizvodnje energije te na taj način povećava njihovu učinkovitost i smanjuje troškove električne energije. U radu će biti obrađeno nekoliko gradskih sektora (pametne zgrade, transportni sektor, gradska uprava, zdravstveni i financijski sektor) u kojima se primjenjuje tehnologija. Mnogobrojne usluge koje pružaju pametni gradovi navedene su na slici 3.1 [1].

Slika 3.1. Aplikacije pametnog grada[1]

3.1. Pametne zgrade

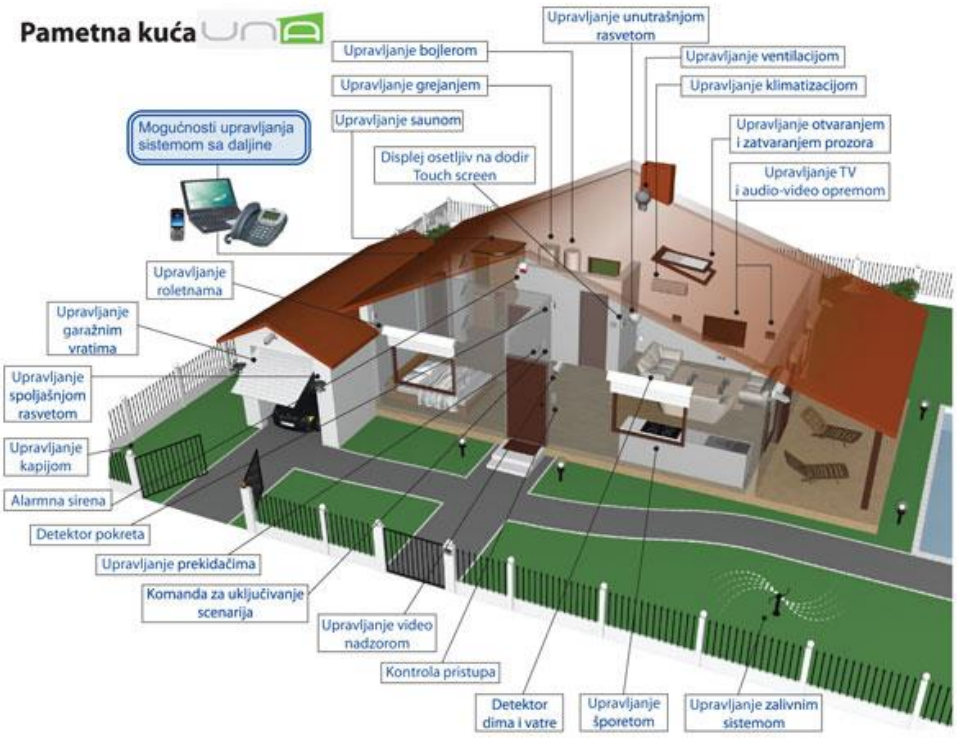
Pametni gradovi zahtijevaju inovativne i funkcionalne građevine zbog udobnosti, učinkovitosti rada sustava zgrade (dizala, vodovodne cijevi, plinske cijevi) i smanjenja potrošnje energije. U pametnim zgradama sustav automatizacije zgrada (*engl. Building Automation System – BAS*) automatski kontrolira grijanje, klimatizaciju, rasvjetu i druge sustave. Potrošnja energije za zgrade je oko 40% ukupne svjetske potrošnje, teži se da u budućnosti zgrade proizvode energiju koju konzumiraju, tj. da postanu nula energetske zgrade (*eng. zero-energy building -ZEB*). Postizanje

ZEB-a obuhvaća osim minimiziranja potrebne energije kroz učinkovite mjere i pokrivanje minimiziranih energetskih potreba usvajanjem obnovljivih izvora, niz optimiziranih i uravnoteženih operacija između potrošnje i proizvodnje zajedno s uspješnom integracijom mreže.

Informacijske i računalne tehnologije (ICT) i implementacija pametne mreže ključ su za postizanje ciljeva nulte energije . ICT za upravljanje energijom u zgradama znatno su se razvile posljednjih desetljeća što je dovelo do boljeg razumijevanja i prodiranja pojma "pametnih zgrada". Pametne građevine spremne za međusobno povezivanje s pametnim rešetkama moraju imati mogućnost pametnog mjerenja,mogućnost odgovora na potražnju, distribuiranu arhitekturu, interoperabilnost.

Svaka pametna kuća ima središnju jedinicu iz koje je moguće kontrolirati sve radnje u kući. Na slici 3.2. je prikazana jedna kontrolna jedinica.

Slika 3.2. Kontrolna jedinica [2]



Slika 3.3. Prikaz pametne kuće[3]

Pametna kuća se može nadzirati na tri načina:

- sustav nadziran od strane vlasnika je tip sustava koji se u praksi rijetko primjenjuje jer vlasnici obično ne posjeduju dovoljno znanja za samostalno vođenje sustava,
- sustav nadziran izvana je tip sustava kod kojeg se briga o sustavu prepušta profesionalnim pružateljima ICT usluga ,
- više se sustava zajednički nadzire izvana. U ovakvom načinu nadziranja postoji pružatelj usluga preko kojeg ide sva komunikacija te se na taj način povećava sigurnost.

U pametnim gradovima, IT infrastruktura podupire projektiranje zgrada, upravljačke sustave, uključujući senzore svjetlosti i gibanja, grijače i hladnjače vode, stepenice, plin, detektore dima, propuštanja vode i dr. U pametnim zgradama prijetnja može biti poremećaj video nadzora, električna distribucija, rasvjeta, hitna pomoć, kontrola pristupa, dizalo, protupožarni sustavi, kontrola klime, itd. Svi povezani uređaji koji koriste neki softver su ranjivi, a napad može biti izveden na daljinu putem interneta. Napadač može pristupiti TV uređaju preko MITM (*eng. man-in-the-middle*) napada jer nema antivirusnog rješenja i softvera za otkrivanje malware-a za TV. U

pametnim zgradama se koriste različiti komunikacijski protokoli, od kojih su najčešći BACnet, KNX i FIP.

BACnet je standardizirani komunikacijski protokol od strane instituta američkih nacionalnih standarda (ANSI) i međunarodne organizacije standarda (ISO) (ISO 16484-5). Od 2003. godine se koristi za automatizaciju i kontrolu mreže zgrade. Određuje niz podataka na fizičkom ili sloju podatkovnog linka.

KNX je standardiziran prema normama EN 50090 i ISO / IEC 14543. To je međusobno povezivanje otvorenog sustava (OSI) mrežnim komunikacijama. KNX je protokol za inteligentne zgrade.

Factory Instrumentation Protocol (FIP) je europska norma (EN 50170-3) koja se koristi za međusobno povezivanje uređaja u automatiziranim sustavima. Određuje više aplikacija/podataka.

Međutim, ovi protokoli nemaju kibernetičke mjere sigurnosti kako bi zaštitili zgradu od napada. Računalne sigurnosne prijetnje su mnogobrojne. Sigurnosni sustav se može inficirati zlonamjernim softverom.

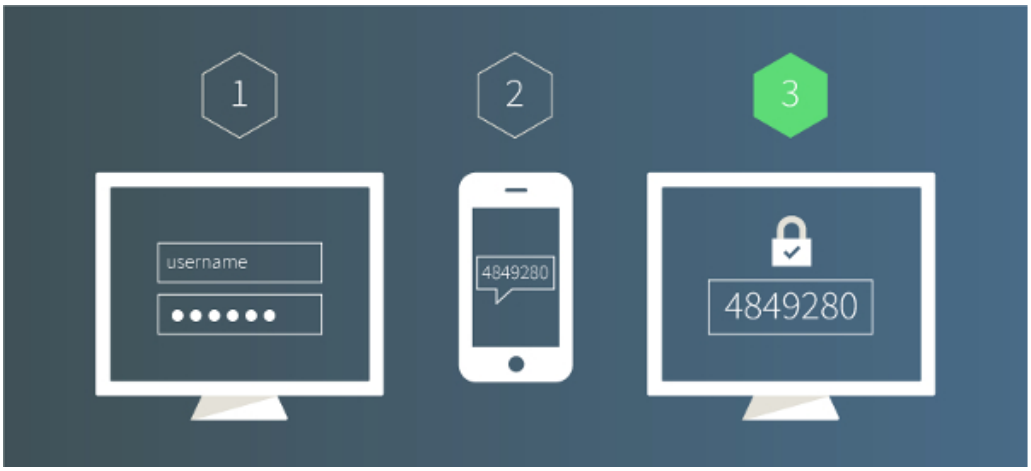
Zlonamjerni softveri (*eng.malware*) predstavljaju računalne programe koji se pokreću bez korisnikovog pristanka, te oštećuju program i podatke koji se nalaze u sustavu, šire se na druga računala, kradu podatke koji su uglavnom povjerljive prirode poput lozinki i bankovnih računa, omogućuju masovno slanje neželjenih poruka.

Prema načinu širenja zloćudni se programi mogu podijeliti na: računalne viruse, crve, trojanski konji. Prema načinu djelovanja i cilju zloćudni programi se dijele na: špijunske programe, programe za oglašavanje, fork bombe, ucjenjivački softver (softver koji traži otkupninu) .

3.1.1. Rješenja

Sustavi u pametnim kućama se nerijetko oštećuju, što uzrokuje nemogućnost opskrbe vodom i strujom, zaustavljanje korištenja obnovljivih izvora energije, probleme u radu klimatizacije ili grijanja što uzrokuje prekomjerno hlađenje ili zagrijavanje prostorija u kući. Pametni uređaji mogu biti i uzročnici nepogode kao što je poplava, koja se javlja uslijed pogreške u regulaciji navodnjavanja. Kako bi se spriječile nezgode i neželjene radnje postoje i protumjere koje štite pametne kuće. Česta je pojava dvostrukog unošenja autentifikacije i jednom zaporke. Najčešći oblik višestruke autentifikacije je SMS poruka (slika 3.4.) koju korisnik primi kada se pristupa korisničkom računu. U SMS poruci se dobije jednokratni kod koji se mora upisati na stranicu da bi se potvrdio identitet korisnika, postoje i dodatni oblici zaštite kao što je potvrdni link na e-mail

adresu, telefonski poziv (u kojem se izdiktira kod koji se upisuje u predviđenu formu na web stranici), tajno pitanje, dodatni PIN te sigurnosno kopiranje podataka i rješenje za oporavak kako bi se osigurala pouzdanost i rad usluga [2].



Slika 3.4. Dvostruka autentifikacija [4]

Da bi se osigurala privatnost korisnika i njegovih podatka potrebno je ograničiti kontrolu pristupa, čime se različitim subjektima dodjeljuju različite ovlasti.

Postupak autentifikacije i provjere identiteta korisnika koji se prijavljuje u sustav treba biti što jednostavniji, ali dovoljno siguran. Dugačke lozinke nisu najbolje rješenje. Jedno od boljih rješenja za kontrolu pristupa bi bio otisak prsta. Takav sustav zaštite nije idealan jer onemogućuje pristup kući iz daljine.

Jedna od metoda zaštite bi bila upotreba vatrozida. Vatrozidi kontroliraju mrežni promet te sprečava napade na mrežu. Vatrozidi se smatraju slabom zaštitom jer ne mogu zaštiti mrežu od naprednijih metoda napada. Da bi se zaštitila od zlućudnih programa, nužna je antivirusna zaštita. Nužno je osigurati povrat podataka nakon prekida rada sustava. Sustav mora imati mogućnost resetiranja jer neprestano radi i ponekad može doći do prekida rada ili greške u radu. Preporuka je često raditi backup podataka kako bi se po potrebi uvijek mogao napraviti uspješan povrat podataka i ponovno pokretanje sustava. Najvažnije je da svi ukućani razumiju potencijalnu sigurnosnu prijetnju te da savjesno rukuju sustavima pametne kuće.

Problemi u ovom području su mali broj studija koje bi istraživale sigurnost. Tehnologije koje se danas primjenjuju u pametnim kućama su relativno nove te se ne zna točno kolike bi štete mogući

napad mogao prouzročiti. Proizvođači tehnologija koje se koriste u kućama moraju biti veoma oprezni, jer ako se dogodi greška na nekom od proizvoda, štete bi mogle biti velike.

3.2. Transportni sektor

Mobilnost u gradovima dovodi do problema zagušenja prometa, onečišćenja okoliša i prevelike potrošnje energije. Da bi se smanjili ti problemi jedno od rješenja je inteligentni transportni sustav (ITS). ITS nudi više usluga, kao što su smanjenje mobilnosti olakšavajući transport, optimiziranje planiranja putovanja i upravljanja, otkrivanje vozača koji predstavljaju prijetnju u prometu, poboljšanje sigurnosti vozača i putnika, smanjenje CO_2, dostupnost parkirnih mjesta i praćenje automobila.

Javljaju se tri tipa pristupa automobilu: neizravan fizički pristup, bežični pristup kratkog dometa, bežični pristup velikog dometa.

- Neizravan fizički pristup- priključak OBD-II (*eng. On Board Diagnostics*) predstavlja najznačajnije automobilsko sučelje koje osigurava izravan pristup CAN (*eng.Controller Area Network*) sabirnici automobila i omogućuje dovoljan pristup kako bi se ugrozio velik broj automobilskih sustava. Navedeni priključak koristi se za povezivanje automobila s prijenosnim računalom najčešće u svrhu dijagnostike i servisa. Sve je češća primjena USB priključaka i Ipod-ova u automobilima. Napadač može iskoristiti upravo ova sučelja kako bi zlonamjerni kod ubacio na CD zajedno s podacima ili kao glazbenu datoteku.
- Bežični pristup kratkog dometa- u automobilima se koriste Bluetooth uređaji sa dosegom do 10m. Daljinsko otključavanje koje je uključeno u gotovo sve moderne automobile, omogućuje i dodatne opcije poput pokretanja motora. Primjenjuju se i radio frekvencijski identifikacijski ključevi koji onemogućuju korištenje automobila bez odgovarajućeg ključa, sustav nadziranja tlaka u gumama koji obavještava vozača o premalom ili prevelikom tlaku u gumama, te Wi-Fi . Usmjerene komunikacije kratkog dometa čija je namjena komunikacija između dva vozila. Za ovu skupinu napada postavlja se odašiljač na udaljenosti od 5-300m [10].
- Bežični pristup velikog dometa- u ovu skupinu ulaze GPS uređaji , satelitski radio, digitalni radio, sustav radio, kanal poruka o prometu.

Hakeri mogu doći do daljinskog pristupa upadom u Bluetooth, radio i Wi-Fi sistem automobila. Kritične su točke i sustav ulaska u vozilo i pokretanja motora automobila bez klasičnog ključa, ali

i sustav nadzora tlaka u gumama te interni dijagnostički sustav automobila. Hakerski se napadi na vozila mogu spriječiti osiguravanjem komunikacije između različitih sustava vozila, a vatrozidi mogu ograničiti mrežnu komunikaciju u slučaju da je jedan od sustava ugrožen. Pojednostavljeno, automobilska industrija treba razlučiti koji su sustavi sigurni, a koji nisu te bi trebala odijeliti jedne od drugih - staviti ih na zasebne ulaze i mrežne sustave, spriječiti komunikaciju između dvije vrste sustava.

Napadom na sustav moguće je i slanje lažnih hitnih poruka, upravljanje sustavom za kočenje u vozilu čime je ugrožen život vozača i ostalih sudionika prometa, zaustavljanje motora vozila, pokretanje pogrešnih zaslona na upravljačkoj ploči vozila čime se prikazuje lažno stanje goriva u rezervoaru, rastavljanje sustava za hitni slučaj vozila, promjena GPS signala, upravljanje brzinomjerom gdje se prikazuje proizvoljna brzina, a za takav napad se koristi presretanje na sporoj CAN sabirnici koja prenosi podatke o trenutnoj brzini i njihovu zamjenu sa zlonamjerno napisanim paketima u kojima se nalaze lažne brzine.

Još jedna metoda napada je metoda umetanja i čuvanja zlonamjernog koda u neku od komponenata automobila. Postojeći napad moguće je proširiti u svrhu otežavanja forenzičke istrage. Tako primjerice zlonamjerni kod može izvesti akciju za koju je programiran i nakon toga izbrisati svaki trag svoga postojanja na tom uređaju. Na taj način se forenzičarima gotovo onemogućuje otkrivanje uzroka nesreće.

3.2.1. Rješenja

Napadi se mogu spriječiti upotrebom infrastrukture javnog ključa, digitalnim certifikatima, i rješenjima za enkripciju podataka.

Infrastruktura javnog ključa ili PKI (*eng. Public Key Infrastructure*) je skup uloga, pravila i postupaka potrebnih za stvaranje, upravljanje, distribuciju, korištenje i upravljanje šifriranjem ključnih riječi, objedinjuje certifikate, certifikacijsku ustanovu, bazu certifikata i opozvanih certifikata, korisnike certifikata, te sve njihove međusobne interakcije.

Svrha javnog ključa je olakšati siguran elektronički prijenos informacija za niz mrežnih aktivnosti kao što su e-trgovina, internetsko bankarstvo i povjerljiva e-pošta. Potrebno je za aktivnosti u kojima su jednostavne lozinke neadekvatna metoda provjere autentičnosti te su potrebni stroži dokazi za potvrđivanje identiteta stranaka uključenih u komunikaciju i potvrđivanje informacija koje se prenose [3]. Infrastruktura javnog ključa omogućuje smanjenje troškova obrade transakcijskih pristupa, smanjenje i odjeljivanje rizika, povećanje efektivnosti i performansa

sustava i mreža te smanjenje kompleksnosti sigurnosnih sustava, pruža podršku za B2B poslovanje itd. Osigurava cjelovitost elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom.

Digitalni certifikat sadrži podatke kao što su ime vlasnika certifikata, vlasnikov javni ključ, nadnevak do kada važi javni ključ, ime CA koji je izdao certifikat, jedinstveni serijski broj, ostale podatke za identifikaciju. Rješava problem dokazivanja autentičnosti. Certifikati koriste digitalne potpise za povezivanje javnih ključeva s podacima o identitetu vlasnika, kao što su ime osobe ili organizacije, adresa i sl., i time sprječavaju neovlašten pristup podacima objavljivanjem lažnog javnog ključa. Koriste se kod zahtjevnijih implementacija enkripcije. Digitalni certifikat se uvijek šalje potpisan digitalnim potpisom samog PKI poslužitelja.

Potrebno je precizno definirati sigurnosni problem koji PKI treba i realno može riješiti ,ne koristit PKI gdje nije potrebno, te ne koristiti PKI ako se nema namjeru paziti na svaku "kariku" u sustavu.

Problem pri korištenju PKI javlja se zbog X.509 standarda koji identificira certifikat putem DN-a (*eng. distinguished names*). Utvrđeno je da je DN poljima teško opisati ustroj stvari u stvarnome svijetu (npr. osoba se opisuje pripadnošću nekoj organizaciji), a postojanje globalnog javnog indeksa osoba razvrstanih prema mjestu zaposlenja postavlja i probleme privatnosti. Prema X.509 standardu, certifikati sadrže informacije koji su javni te ne jamče privatnost, a svaka izmjena podataka zahtijeva opoziv starih certifikata i izdavanje. Ako dođe do kompromizacije bilo kojeg privatnog ključa, kompromitirana je i valjanost svih certifikata koje je izdao određeni centar[16].

Neupitno je da će se automobilska tehnologija razvijati u budućnosti. Uređaji će pružiti još bolju informiranost o stanju na cestama, tlaku u gumama, mogućim kvarovima na automobilu, još lakšu komunikaciju sa drugim učesnicima prometa itd. Težit će se za postizanjem još bolje komunikacije kako bi se što bolje regulirale gužve u prometu. Računalna sigurnost automobila znatno će se povećati jer se kao prioritet svega stavlja sigurnost vozača i svakog sudionika prometa. Država bi trebala donijeti zakone koji bi pružili još veću zaštitu građana.

3.3. Sektor uprave

E-uprava koristi ICT (informacijsko-komunikacijsku tehnologiju) kako bi međusobno povezala državne i privatne institucije. Cilj je omogućiti građanima vladine usluge. Međutim, većina građana je zabrinuta za svoje privatne podatke prilikom korištenja e-uprave. Sigurnost e-uprave uključuje tradicionalne sigurnosne usluge (autentifikacija, povjerljivost , integritet i dostupnost).

Najveće prijetnje koje se javljaju u ovom sektoru su krađe identiteta , fiskalne prijevare, promjene podataka vezanih za pojedinca i njegovu imovnu. Prednosti e-uprave su smanjenje korupcije, povećanje transparentnosti, veća praktičnost, rast prihoda i smanjenje troškova.

3.3.1. Rješenja

Rješenja za sigurnosne probleme u ovom sektoru su Fortinet i Symantec.

Ova rješenja od prijetnji štite na dva načina:

- zaštita od poznatih prijetnji- izgrađeni sigurnosni stog uključuje dinamičan AV motor, vatrozid aplikacija, skener za ranjivost s automatskim popravljanjem i Web Filter koji radi zajedno kako bi se smanjila površina napada, sprečava napad zlonamjernog softvera.
- zaštita od nepoznatih prijetnji- omogućuje se provjera valjanosti nepoznate datoteke te se obavlja dinamička analiza kako bi se utvrdilo zlonamjerno ponašanje. Zlonamjerni softver je ublažen dijeljenjem inteligencije. Taj objekt se automatski izdvaja, te se imuniziraju sve ostale datoteke čime se proširuje zaštita.

Ova rješenja omogućavaju potpunu zaštitu mreže i integriraju sve servise potrebne za zaštitu poslovanja poduzeća u jedinstveno rješenje koje obuhvaća antivirusnu zaštitu, vatrozid, antispam, antispyware, detekciju i prevenciju upada u mrežu, kontrolu pristupa sadržajima na Internetu i VPN pristupa mreži.

Virtualna privatna mreža (VPN) je neophodna i gotovo sveprisutna za sve organizacije koje nude siguran daljinski pristup imovini. Korisnicima se omogućuje slobodan pristup s uvijek povezanim VPN klijentom koji podržava sigurnosni sloj utikača (SSL) i protokol internetske sigurnosti (IPSec), provjeru dvostruke autentičnosti i jednostruke prijave (SSO) . VPN ima ograničenja koja se odnose na:

• Pouzdanost (dostupnost i brzina) – VPN ovisi o kvaliteti usluge ISP-a (pružatelja Internet usluga). Također, ovisi o načinu primjene VPN veze (koji protokoli se koriste, autentifikacija, enkripcija, itd.).

• Nekompatibilnost opreme različitih proizvođača – što ima utjecaja prilikom primjene pojedinih standarda i protokola koji u tom slučaju neće raditi kako je predviđeno.

• Zahtijeva se vrhunsko poznavanje opreme koja se koristi u cilju ostvarivanja potpune zaštite privatne mreže od mogućih sigurnosnih prijetnji i napada. To uključuje poznavanje mrežnih

protokola, sigurnosnih mehanizama i pažljivo konfiguriranje postavki sustava. Slika 3.5. opisuje najčešće propuste u primjeni VPN tehnologije.

Opis	Iskorištavanje propusta
Hakerski napadi upućeni prema klijentu	Najčešće se izvode napadi krađe korisničkih sjednica (napadač preuzima postojeću korisničku sjednicu i postaje autorizirani korisnik na mreži) ili Man-in-the-Middle napad (pri čemu napadač prati pakete te ih može brisati, mijenjati ubacivati nove, itd.)
Autentikacija korisnika	Kod nekih ranije spomenutih protokola, kao što je primjerice PPTP, korisničko ime i lozinka se šalju mrežom bez enkripcije. Potencijalni napadač može tako vrlo jednostavno i brzo saznati sve bitne pristupne podatke te se spojiti na zaštićenu mrežu te tako otkriti osjetljive podatke. Isto tako treba pripaziti da se ti podaci čuvaju u datotekama koje nisu svakom dostupne.
Virusi	Ukoliko je korisnikovo računalo zaraženo virusom vrlo je vjerojatno kako će ga prenijeti i na mrežu na koju se spaja čime se povećava mogućnost curenja povjerljivih podataka kao što su podaci za pristup.
Pristupna prava i ovlasti	Potrebno je strogo kontrolirati tko sve ima pristup na mrežu, ali isto tako od velike je važnosti nadzirati kojim podacima, programima i ostalim resursima mogu pristupiti pojedini korisnici kako ne bi došlo do zlouporabe.
Nekompatibilnost proizvoda	Prilikom nabavke opreme bitno je voditi računa o tome jesu li uređaji različitih proizvođača međusobno kompatibilni za rad. U suprotnom mogući su problemi kod uspostave VPN veze ili ispravne primjene mehanizama koji doprinose zaštiti podataka

Slika 3.5. Najčešći načini zlouporabe VPN-a[17]

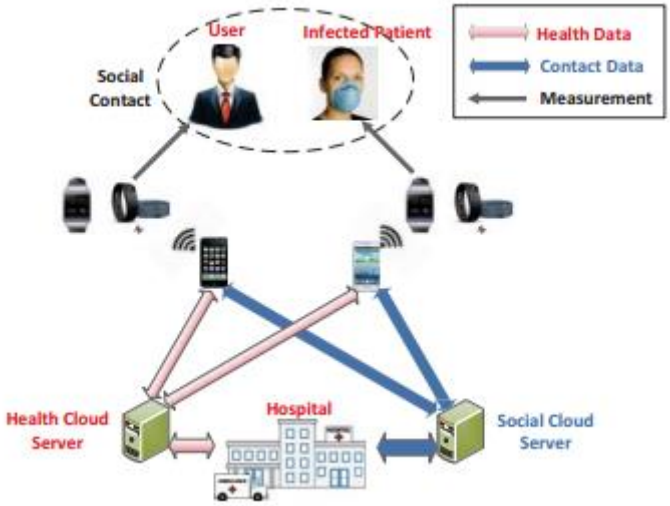
Tehnologije koje se primjenjuju za zaštitu računala su[14]:

- zaštita računala i poslužitelja s najučinkovitijim antivirusnim tehnologijama i softverima za otkrivanje malware-a (Endpoint Protection),
- stvaranje rezervnih kopija korporativnih podataka u mrežnim okruženjima (*NetBackup*),
- arhiviranje (*Enterprise Vault*),
- upravljanje poslužiteljima i uređajima za skladištenje podataka (*Storage Foundation, VERITAS Cluster Server, Command Central Storage*),
- sigurna poslovna rješenja kao što su *Brightmail Gateway, Web Gateway, Network Access Control, Endpoint Encryption, Control Compliance i Data Loss Prevention (DLP),*
- rješenja za zaštitu i nadzor kritičnih točaka sustav (*Altiris*).

Teži se a razvoju metoda koje bi jamčile sigurnost spremljenih podataka u bazama podataka. Veritas razvija inteligenciju koja će služiti za analizu rizika. Uvodi se tehnologija strojnog učenja te se ocjenjuje rizičnost korisnika i njegovih podataka, te se predlažu koraci za rješenje problema. Korištenjem umjetne inteligencije osigurava se sigurnost podataka.

3.4. Zdravstveni sektor

Inteligentna zdravstvena zaštita koristi spoj biomedicinskih senzora, zdravstvenih podataka za pohranu i obradu te pruža preventivne, kurativne i palijativne zdravstvene usluge. Može prikupiti širok raspon zdravstvenih podataka o korisniku, analizira zdravstvene probleme diljem grada, poput širenja zaraznih bolesti. Zarazne bolesti, npr. ebola, gripa i akutne respiratorne infekcije, brzo se šire među stanovništvom fizičkim kontaktom. Ljudi imaju česte kontakte ili snažne društvene veze s pacijentom (npr. studenti koji studiraju u istoj učionici i obitelji koje žive u istoj kući) obično se smatraju osjetljivim iz biomedicinske i sociološke perspektive. Staromodan pristup prevencije je izolirati osjetljive ljude za određeno razdoblje. Međutim, ovaj pristup ima niz negativnih utjecaja, uključujući trošak tako velike zdravstvene zaštite, ekonomski gubitak izoliranih ljudi i paniku te anksioznost u društvu. Da bi se riješio problem širenja zaraze, inteligentna zdravstvena zaštita pružit će učinkovitu dijagnozu i hitno upozorenje u realnom vremenu što se postiže analizama infektivnosti [1].



Slika 3.6. Umreženost u pametnom zdravstvu [1]

Razvijene su mnoge zdravstvene aplikacije koje povećavaju zdravstvenu sigurnost građana. Na primjer Wechat program može pronaći korisnike u fizičkoj blizini i bilježiti društvene interakcije; prepoznavanje govora može otkriti ako neki ljudi kašlju ili imaju kihavicu. S druge strane, nosivi uređaji i medicinski senzori omogućuju uvid u pacijentovo zdravstveno stanje . Međutim, prikupljaju se podaci o zdravlju od strane više neovisnih pružatelja usluga, kao što su bolnica i društvene mreže (npr. Facebook i Wechat). Suradnja tih davatelja usluga omogućuje poboljšanje analize infekcije, i predstavlja niz sigurnosnih pitanja. Za očuvanje podataka korisničke privatnost i dostupnosti podataka, homomorfno šifriranje može se usvojiti kako bi se napravili i podaci s društvenih mreža i podaci o zdravlju nevidljivi nepouzdanim poslužiteljima u oblaku. Suradnja s različitim nepouzdanim oblak poslužiteljima postiže se preko ovlaštenog entiteta (tj. bolnice ovlaštene od strane korisnika). Međutim, kada bolnica upita za podatke o zaraženom pacijentu na društvenom poslužitelju za oblak, poslužitelj može zaključiti da je korisnik zaražen iako je sadržaj upita i dalje nevidljiv. Osim toga, bilo koji entitet bez autorizacije vlasnika podataka ne bi trebao imati mogućnost upita u korisničke podatke. Najsuvremenija sigurnosna i privatna zaštita je bitna za inteligentnu zdravstvenu zaštitu. Bez učinkovite zaštite, korisnici možda neće biti spremni podijeliti svoje socijalne i zdravstvene podatke s drugima.

U tu svrhu zaštite podataka razvijen je protokol prijenosa za upit o zaštiti privatnosti. S jedne strane, omogućuje ovlaštenom entitetu, kao što su liječnici, pristup pacijentovim društvenim i zdravstvenim podacima iz oblaka društvenog poslužitelja, s druge strane, on sprečava pristupanje podacima neovlaštenim poslužiteljima i zaključivanje svih podataka o upitu, kao što je identitet

pacijenta. Korisnici ili vlasnici podataka moraju odobriti pristup autoriziranom entitetu. Svaki entitet bez ovlaštenja korisnika ne može pristupiti podacima. Osim toga koristi se i kriptiranje homomorfnom enkripcijom za sprečavanje pristupa bilo kojeg nepouzdanog zdravstvenog oblaka koji želi citati bilo koje privatne i društvene, te zdravstvene podatke.

Širenjem takvih podataka imamo uvid u zdravstveno stanje građana. Mnoga istraživanja usredotočena su na korištenje bežičnih medicinskih mreža za područje tijela (WBAN) kako bi poboljšali kvalitetu njege kod udaljenog medicinskog nadzora. Primjerice, u medicinskom polju pacijent može biti opremljen bežičnom mrežom za područje tijela koja se sastoji od senzora koji kontinuirano mjere specifične biološke funkcije, kao što su temperatura, krvni tlak, puls, elektrokardiogram (EKG), disanje i dr. Prednost je da pacijent ne mora ostati u krevetu i može se slobodno kretati po sobi ili čak napustiti bolnicu na neko vrijeme. Time se poboljšava kvaliteta života pacijenta i smanjuju troškovi bolnice. Osim toga, podaci prikupljeni tijekom duljeg razdoblja i u prirodnom okruženju pacijenta nude više korisnih informacija, što omogućuje točniju i ponekad bržu dijagnozu.

Takve mreže velik su izazov u smislu sigurnosti i privatnosti. Prenošenje elektrokardiograma (EKG) bez šifriranja imalo bi velik utjecaj na privatnost pacijenta. Uobičajene metode koriste diskretnu cosinusnu transformaciju (DCT), valnu transformaciju, adaptivnu Fourierovu dekompoziciju (AFD).

3.4.1. Rješenja

Sigurnost podataka se može osigurati upotrebom osiguranih Wi-Fi mreža kojima se garantira siguran rad sa povjerljivim podacima učinkovita rješenja su AirTight mreže i Aerohive sigurnosna rješenja. Procjena rizika bitan je faktor za sigurnost, a metode koja se primjenjuju za procjenu su Rapid7 rješenja, rješenja za zdravstvenu sigurnost, SafeNetova rješenja za sigurnost podataka, rješenja za sigurnost tvrtke Stanley, Intelova sigurnosna rješenja za zdravstvenu zaštitu.

AiRTight mreže redefiniraju modernu Wi-Fi platformu. Korisnik mora kupiti bežične senzore (mali dodatak hardvera plug-n-playa) i priložiti ih odgovarajućim strojevima u svojoj tvrtki, odgovoriti na nekoliko pitanja o bežičnom podešavanju. U roku od nekoliko dana počinju primati izvješća o bežičnoj sigurnosti. Nema poslužitelja ili softvera za kupnju, konfiguriranje ili administriranje jer se sve analize podataka i generiranje izvješća nalaze na AirTightovim poslužiteljima putem interneta.

Aerohive rješenja nemaju kontrolera u obliku fizičkog uređaja te jedinstven, originalan su sustav kofiguracije sustava putem centralnog mjesta mrežnog upravljanja i konfiguracije. Aerohive mrežna struktura radi bez prekida i utjecaja na rad krajnjih korisnika.

Metode za procjenu rizika transformiraju podatke, osnažujući IT i sigurnosne stručnjake da napreduju i štite svoje organizacije. Rješenja su omogućena naprednom analitikom i razumijevanjem napadačeva razmišljanja. To olakšava prikupljanje podataka, pretvara ih u prioritetan i djelotvoran uvid i dolazi do ljudi koji mogu raditi s njima. Koriste kritične informacije bitne za unapređenje i zaštitu najboljih interesa organizacije. Olakšava se unificiranje operativnih podataka diljem sustava, a napredna analitika otključava informacije potrebne za sigurno razvijanje i upravljanje današnjim sofisticiranim aplikacijama i uslugama [12].

Zdravstvena industrija, poput ostalih vertikala, posjeduje poslovno-poslovne (B2B) i poslovno-privatne (B2C) komponente. Ta područja zahtijevaju siguran pristup aplikacijskim API-jima kako bi pružili potrebnu razinu usluga klijentima i partnerima. Sigurno izlaganje API-jima zahtijeva najbolje prakse u sigurnosti i zaštiti od prijetnji, uključujući enkripciju, virtualizaciju i zaštitu od SQL injekcija i uskraćivanja usluge (DOS napada). Pristup informacijama koje pružaju API-ji imaju dvije provjere:

- provjeru autentičnosti
- provjeru autorizacije

Provjera autentičnosti osigurava da je strana koja traži zahtjev točno ta za koju tvrdi da je. Provjera autorizacije osigurava da vlasnik informacija pristane na davanje informacija koje se objavljuju i da stranka koja traži pomoć ima odgovarajuću ovlast za pristup. Na njoj se upravlja na nekoliko načina, uključujući, ali ne ograničavajući se na, korisničko ime/zaporku, potvrde ili autentifikaciju na temelju tokena kao što su SAML ili OAuth. U mnogim slučajevima, kao što su mobilne aplikacije, autentifikacijski entitet je aplikacija sebe. Za autentifikaciju u B2B scenariju, autorizacija se obično upravlja putem podataka iz baze podataka gdje je zabilježen prethodni pristanak pacijenta. Za B2C slučajeve, pristanak je često u stvarnom vremenu interaktivno odobrenje pacijenta da aplikaciji dopusti pristup njihovim podacima.

SafeNet osigurava siguran pristup osjetljivim podacima i zaštitu identiteta korisnika. Omogućuje dijeljenje informacija s mogućnošću prijenosa sigurnih podataka između dvije ili više različitih interesnih zajednica ili sigurnosnih domena.

Intel Core procesori su idealni za zdravstveni sektor, javni sektor i industrijske primjene jer sadrže značajke ključne za napredne internetske (IoT) dizajne, kao što su podrška za ECC (memoriju kodova za ispravljanje pogreškama) memoriju i tehnologija Intel vPro [11].

- Intel Trusted Execution tehnologija mjeri vatrozid, BIOS i hipervisiju i uspoređuje vrijednosti.
- Intel virtualizacijska tehnologija omogućuje otkrivanje, blokiranje i uklanjanje sofisticiranih zlonamjernih programa kao što je kernel mod Rootkita, čak i izvan operacijskog sustava u sigurnosti kao što su McAfee Deep Defender i McAfee DeepSAFE tehnologija.
- Intel OS Guard štiti operacijski sustav od aplikacija koje su napadnute sprečavanjem izvršenja napada iz aplikacijske memorije.

U budućnosti se teži za još većom sigurnošću pacijenata i njihovih podataka. Razvijene su e-uputnice i e-naručivanje na preglede čime se štedi vrijeme i novac pacijenata i zdravstvenih radnika, s tom namjerom razvijene su mnogobrojne aplikacije koje su dostupni pacijentima i medicinskom osoblju. Tehnologija koja se razvija u zdravstvu bi trebala pridonijeti učinkovitijem rješavanju zdravstvenih problema. Zbog dostupnosti velike količine podataka uvode se , među ostalim, načela „smanjenja količine podataka", „integrirane zaštite podataka", i „zadane zaštite podataka" kako bi se osiguralo da se mjere za zaštitu podataka uzimaju u obzir u fazi planiranja postupaka i sustava.

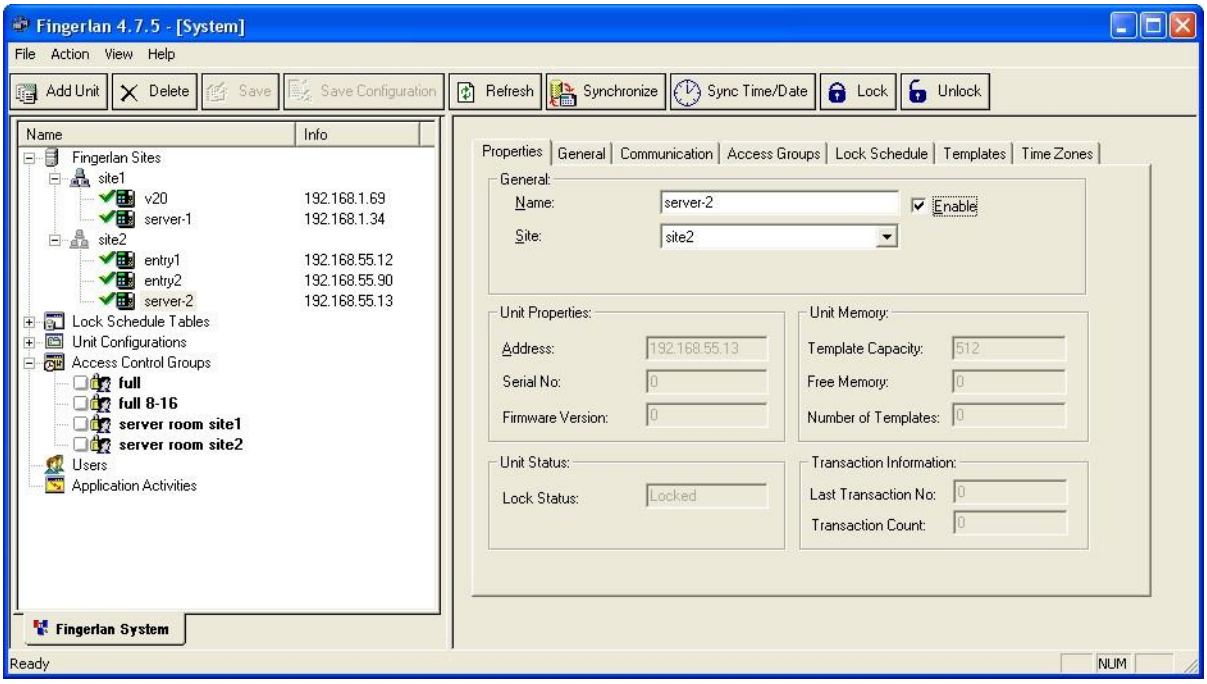
Moraju se pronaći još bolji načini za učinkovitu uporabu velike količine zdravstvenih podataka prikupljenih s mobilnih uređaja te za osiguranje sigurne obrade takvih podataka. Potrebno je financirati nove projekte čiji bi cilj bio zaštita podataka.

Računalstvo u oblaku osigurava mogućnost pristupanja podacima u bilo koje vrijeme i na bilo kojem mjestu. Cilj omogućiti brže donošenje sigurnih rješenja za računalne oblake u Europi, čime bi se podržala sigurna pohrana zdravstvenih podataka internetom.

3.5. Financijski sektor

Imajući na umu da su naši privatni podaci dostupni javnosti , jedan od većih problema predstavlja gubitak privatnosti u financijskom sektoru, gdje gotovo svi djelatnici imaju uvid u naše financijsko stanje, velika prijetnja su i računovodstvene prijevare koje se događaju u ovom sektoru.

Pri internetskoj kupnji potrebno je ograničiti pristup podacima , kao što je vidljivo na slici 3.8., gdje se različitim slojevima dodjeljuju različite mogućnosti za pristup podacima te se time sprečava nepotreban uvid u korisnikove podatke.



Slika 3.8. Kontrola pristupa [9]

Čest slučaj su i računovodstvene prijevare gdje su najčešći oblici prijevara:

- protupravno prisvajanje novca ili imovine od strane osobe kojoj je povjerena na čuvanje ili upravljanje,
- krađa novca (različiti oblici krađe novca nakon njegovog evidentiranja), najčešće se radi o krađi gotovine iz blagajne,
- pranje novca (nelegalno stečen novac se prenosi u legalne tijekove),
- lažiranje ponuda (pobjeda na natječajima zbog posjedovanja povlaštenih informacija te mogućnosti davanja najjeftinije ponude), a na naknadnim se aneksima ugovora povećava iznos isporuka,
- skimming (krađa čiji je objekt neevidentirani novac),

- fiktivna potraživanja (služe za prikrivanje fiktivne prodaje), najčešće su to prikrivanja krađe na zalihama,
- lažna prodaja (podrazumijeva neevidentiranu prodaju), podcijenjenu prodaju,
- fiktivnu prodaju, povećanje cijena radi povećanja provizije,
- lažna plaćanja (podrazumijeva višestruka plaćanja jednom dobavljaču),
- fiktivna potraživanja,
- fiktivne troškove i slično.

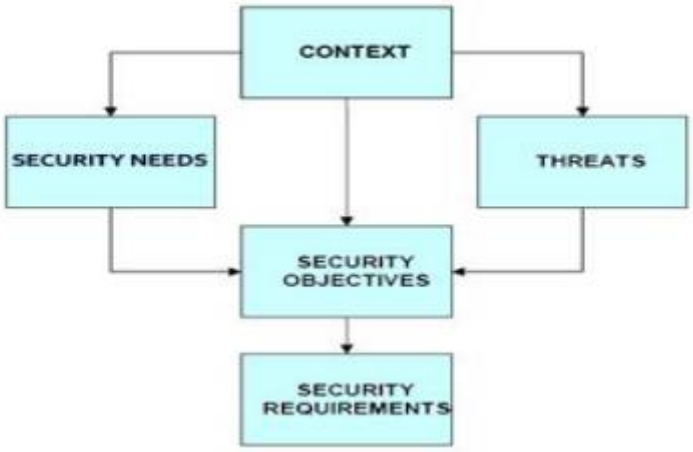
Nedovoljnim provjerama daje se pristup povjerljivim informacijama o tvrtki te pristup povjerljivim informacijama o klijentima, i na taj način se oštećuje reputacija tvrtke. Česti su i DOS napadi i krađe identiteta. Neke od češćih prijetnji su SQL ubrizgavanje i trojanski konj.

3.5.1. Rješenja

Za analizu rizika koriste se MEHARI i EBIOS metode.

3.5.1. EBIOS

Metoda uključuje 5 koraka (kontekst, sigurnosne potrebe, analiza prijetnji, identifikacija sigurnosnih ciljeva i identifikacija sigurnosnih zahtjeva) kao što je prikazano na slici 3.9.



Slika 3.9. Metodologija EBIOS-a [8]

3.5.2. MEHARI

MEHARI za cilj ima pomoći upraviteljima (operativnim menadžerima, CISO, CIO, upraviteljima rizika, revizorima) u njihovim nastojanjima da upravljaju sigurnošću informacija i IT-a resursima te smanjiti povezane rizike. Metodologija MEHARI-a je opisana na slici 3.10. [8] :

Slika 3.10. Metodologija MEHARI [8]

MAHARI sadrži osnove znanja o rizicima, pravila za konsolidaciju dobivene analize rizika u optimalnom planu akcijskih planova, analiziranje glavne uloge, analiziranje ranjivosti, smanjenje i upravljanje rizicima, nadziranje sigurnosti informacija, revizijske baze podataka.

Postoje mnogi softveri za otkrivanje malware-a, najčešće primjenjivani su McAfee, Symantec. Sve tehnike pružaju proizvode i usluge za sprječavanje financijskog kriminala, usklađenost i upravljanje rizikom u industriji financijskih usluga. Pružaju u stvarnom vremenu prevenciju unakrsnih kanala, otkrivanje pranja novca i rješenja za nadzor trgovanja koja se bave takvim problemima kao što su prijevara s plaćanjem, virtualnog kriminala, zlouporaba tržišta, dubinsku analizu kupaca. U tablicama 3.11. i 3.12. je prikazana usporedba metoda za analizu rizika, gdje su pored MAHARI i EBIOS, uspoređivane i druge metode poput Cramm, Octave i Cobra.

No.	Comparison criteria	*Weight*	Mehari	Cramm	Ebios	Octave	Cobra
1	Cost	*5*	2	0	5	5	0
2	English documentation	*2*	2	2	2	2	2
3	National standard	*2*	0	0	0	0	0
4	International standard	*4*	0	0	0	0	0
5	Declared compliance with standards	*3*	2	1	3	0	1
6	Target group	*5*	5	1	5	1	1
7	Sophistication of usage/implementation	*5*	3	1	3	3	5
8	Popularity	*2*	2	2	2	0	0
9	Flexibility	*3*	2	1	3	3	3
10	Method's scope of action	*5*	3	3	5	5	3
11	Method of risk identification	*2*	1	1	2	1	1
12	Risk completeness verification	*3*	0	0	3	1	3
13	Number of standard "scenarios"	*2*	2	2	2	2	2
14	Analysis of "scenarios" dependencies	*4*	4	4	4	2	4
15	Data gathering method	*3*	1	1	3	1	1
16	Data verification	*3*	3	3	3	2	3
17	Basis for risk calculation	*2*	2	0	2	2	2
18	Number of risk levels	*2*	2	0	2	2	2
19	Basis for probability estimation	*2*	2	2	2	2	2
20	Number of probability levels	*2*	2	0	2	2	2
21	Basis for cause estimation	*2*	2	0	2	2	2
22	Number of cause levels	*2*	2	0	2	2	2
23	Cause metric	*1*	1	0	1	1	1
24	Probability metric	*1*	1	1	1	1	1
25	Risk metric	*1*	1	0	1	1	1
26	Choice of countermeasures	*2*	2	2	2	2	2
27	Analysis of countermeasures' dependencies	*3*	1	3	1	1	0
28	Analysis of countermeasures' influence	*3*	3	3	3	1	3
29	Estimation of risk treatment efficiency	*4*	0	0	0	2	0
30	Risk monitoring	*2*	0	0	0	1	0
31	Detection of new risks	*2*	0	0	1	1	1
32	Adaptability	*4*	2	0	2	2	4
33	Automatic correction of dependant risk	*2*	1	0	0	0	2
34	Support for security policy framework generation	*5*	0	0	5	5	2
35	Procedures generation support	*5*	0	0	5	5	2
	Total:	***100***	**56**	**33**	**79**	**63**	**60**

Tablica 3.11. usporedba metoda za analizu rizika [18]

Generic ISRM phase and its output	CRAMM phase	NIST SP 800-30 phase	OCTAVE phase	EBIOS phase	ISO 27005 phase
System Characterization Output:: inventory list of assets to be protected, including their acceptable risk level	Asset Identification	System Characterization	Identification of Critical Assets and Corresponding Security Requirements Identification of Current Security Practices	Study of the Organization Study of the Target System Determination of the Security Study Target Expression of Security Needs	Identification of Assets
Threat and Vulnerability Assessment Output: list of threats and corresponding vulnerabilities endangering the identified assets	Threat Assessment Vulnerability Assessment	Threat Identification Vulnerability Identification Control Analysis	Identification of Threats and Organizational Vulnerabilities Identification of Current Technology Vulnerabilities	Study of Threat Sources Study of Vulnerabilities Formalization of Threats	Identification of Threats Identification of Vulnerabilities
Risk Determination Output : quantitative or qualitative risk figures/levels for identified threats (input: threat probability and magnitude of impact)	Asset Valuation Risk Assessment	Likelihood Determination Impact Analysis Risk Determination	Risk Determination for Critical Assets	Comparison of Threats with Needs (Risk Determination)	Identification of Impact Assessment of Threat Likelihood Assessment of Vulnerability Likelihood Risk Estimation
Control Identification Output: list of potential controls that can mitigate the risks to an acceptable level	Countermeasure Selection	Control Recommendations	Identification of Risk Measures	Formalization of Security Objectives	Evaluation of Existing and Planned Controls
Control Evaluation and Implementation Output: list of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level	Countermeasure Recommendation	Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation	Protection Strategy Development Risk Mitigation Plan Development	Determination of Security Levels Determination of Security Requirements Determination of Security Assurance Requirements	Information Security Risk Treatment (Risk Avoidance, Risk Transfer, Risk Reduction, or Risk Retention

Tablica 3.12. usporedba metoda za analizu rizika [8]

Zaključuje se da nijedna od metoda procjene rizika nije savršena, pa ni ona koja je dobila najveće ocjene prilikom analiziranja. Kao najveći problem smatra se manjak automatizacije te činjenica da kod metoda analiziranja nema podrške za potrebne procese.

Važno je spomenuti inteligenciju internetskog kriminala (*RSA CyberCrime Intelligence Service, ThreatMetrix Advances Cybercrime Prevention, SurfWatch VC-Suite, analiza IBM Enterprise Insight*).

Inteligencije internetskog kriminala služe za obavještavanje o prijetnjama, pružaju analize veza i uvide kako bi se proaktivno riješile eventualne internetske prijetnje korisnicima i poslovanju. Spoznaja o pojavi cyber prijetnje pomaže nam osigurati zaštitu podataka o klijentima.

Kako bi to postigla zaštita, korisnik mora steći neka znanja o računalima te primijeniti preporučene mjere zaštite. Neke od njih su:

- zaobilaženje otvaranja poveznica (*eng. link*) sumnjivih poruka elektroničke pošte (to su obično one poruke u kojima se traži odavanje osobnih podataka, PIN-ova i slično),
- upotreba filtra za neželjenu elektroničku pošti (*eng. spam filter*),
- upotreba antivirusnih programa,
- upotreba vatrozida (*eng. firewall*),
- primjena najnovijih zakrpa i instalacija inačica programa u kojima su ispravljeni sigurnosni propusti,
- korištenje antispyware programa,
- česte provjere stanja bankovnih računa te
- edukacija o sigurnosti.

Edukacija o sigurnosti možda je i najvažniji savjet jer broj Internet prijevara svakodnevno raste i korisnici moraju biti svjesni opasnosti koje vrebaju, kao i načina na koje se mogu zaštititi.

4. PRIVATNOST

Važnost privatnosti će se objasniti pomoću registracijskih oznaka vozila. Svaku registracijsku oznaku možemo povezati sa identitetom vlasnika vozila. Putanja vozila se može pratiti iako su svi podaci između korisnika i infrastrukture šifrirani. Ovo se protivi ljudskoj privatnosti, čime im se onemogućuje nesmetana kretnja bez javnog nadzora. Uređaji povezani u vozili spremaju veliku količinu osobnih podataka te međusobno imaju različite mogućnosti komunikacije. U pametnim gradovima, broj međusobno povezanih uređaja može biti jako velik, a podaci koji su prikupljeni preko interneta omogućuju drugim korisnicima podataka uvid u vlasnikove navike.

4.1. Modeli privatnosti

U informacijskim sustavima tri su glavne operacije: prijenos podataka, obrada i pohrana. Zabrinutost zbog privatnosti može se pojaviti tijekom bilo koje od ovih operacija što može utjecati na ponašanje korisnika. Usluge mogu biti povezane s lokacijom korisnika što može predstavljati problem privatnosti. Spominje se više modela sigurnosti, neki od njih su :

- Gdje, tko, što model (W3) privatnosti za usluge temeljene na lokaciji (LBS),
- troslojni model privatnosti,
- pristup koji se temelji na linearnim algebarskim operacijama (kao što su množenja matrica) za rješavanje linearnih sustava i izračun korelacije između distribuirane skupine podataka.

Nažalost, tehnike očuvanja privatnosti ne rješavaju ograničenja kao što su česte promjene članova i nepouzdane treće strane. Zato očuvanje privatnosti ostaje značajan izazov koji zahtijeva daljnju istragu.

Sustav se može ugroziti na mnogo načina. Neki od glavnih su zlćudni softveri (*eng. malware*). hoax-i, uskraćivanje usluga i loše lozinke.

Hoax predstavlja prevaru čiji se sadržaj nalazi u neželjenoj e-mail poruci (*eng. spam*) [13]. S ciljem zastrašivanja ljudi i slanja dezinformacija. Oblici kroz koje se manifestira su upozorenja o štetnim programima i virusima, lanci sreće i zaraze, lažni zahtjevi za pomoć ,prijetnje…

Uskraćivanje usluge ne uzrokuje gubitak informacija, ali stvara poteškoće u radu sustava. Oblici su smuf-ping, SYN-uspostava enormno velikog broja konekcija i fragmentacija paketa.

Lozinke imaju prednost zbog jednostavne implementacije, ali su laka meta za hakere , budući da se 40% lozinki može pogoditi jer obično ne koristimo komplicirane lozinke koje je teže pogoditi, često stavljamo datume rođenja ili lozinke od samo nekoliko znakova.

Sustavi se mogu zaštititi raznim antivirusnim programima, vatrozidima i kriptografijom. Mnogobrojni antivirusni programi mogu se besplatno preuzeti na uređaje. Rade na principu prepoznavanja, neutralizacije i eliminacije zlućudnih softvera .

4.2. Problemi privatnosti

Najčešće prijetnje za privatnost predstavljaju kolačići, neželjena pošta, mrežna krađa identiteta, pretraživači, elektronička trgovina.

Kolačići su tekstualne datoteke koje web poslužitelj pohranjuje na disk klijenta. Kolačići bilježe sve prijave i prijavljuju ih tamo gdje je dizajner kolačića to odredio. Ukoliko glavno računalo prepozna kolačić na pregledniku svaki put kada se učita oglas ili stranica, ono može poslati evidenciju vašeg posjeta i preciznije vam odrediti oglase prilikom vašeg sljedećeg posjeta. Tako će vam se, primjerice, neki oglasi obratiti imenom i spomenuti vašu lokaciju.

Neželjena poruka je poruka koja se šalje primatelju bez korisnikovog dopuštenja, a koja vrlo često sadrži i prijevaru. Postoje i druge vrste neželjenih poruka, poput onih na na blogu, wikijima ili u sobama za razgovore, a može biti riječ i o e-mail neželjenoj poruci. Oko 80% ukupnih poruka su neželjene.

Mrežna krađa identiteta predstavlja vrstu prijevare na način da korisnika navode da otkrije svoje podatke (OIB, ime, prezime, PIN-ove i dr.). Korisniku koji je postao žrtva krađe identiteta može pomoći promjena lozinke ili PIN za pristup na svoj korisnički, odnosno bankarski račun ili u krajnjem slučaju da zatvori račun kod davatelja usluge.

Elektronička trgovina plaća se putem formulara upisom broja kreditne kartice, tako upisani podatak putuje mrežom i vidljiv je svima koji imaju ovlasti za pristup. Podaci se prenose protokolom HTTP, adresa počinje s http://. Sigurnost se može postići šifriranjem podataka aplikacije.

4.3. Najčešće metode za zaštitu privatnosti podataka:

Tri najčešće metode za zaštitu privatnosti podataka su:

1. k-anonimnost
2. l-raznolikost
3. t-bliskost

Metoda k-anonimnosti razvijena je s namjerom rješenja problema narušavanja privatnosti zbog povezivanja većeg skupa podataka. Pretpostavlja se da organizacija sadrži strukturiran skup podataka koji predstavljaju privatne i osjetljive podatke o korisnicima, te mogućnost objave podataka s garancijom da se subjekti ne mogu identificirati iz podatka koji su objavljeni, ali da je ipak i time omogućena potrebna analiza i istraživanje koje se vrši. Objava podataka zadovoljava svojstvo k-anonimnosti (k>1), ako se zapisi pojedinca koji se nalaze u objavi ne razlikuju od najmanje (k-1) pojedinaca čije se informacije također pojavljuju u objavi. U tom slučaju vjerojatnost pravilne identifikacije pojedinca bit će (1 / k) .

Prikazana je tablica 4.1. od n redaka i m stupaca koji se sastoje od privatnih, osjetljivih podataka pojedinaca. Tablica 4.1. sadrži informacije o bolesti jedanaest osoba. Tablica 4.1. sadrži 6 stupaca i 11 redaka. Pojedinci u tablici mogu se identificirati njihovim imenima i dobi. Kombinacija atributa kao što su "Ime", "Dob", "Spol" i "Država " mogu se koristiti za prepoznavanje pojedinaca. Skup podataka nije anoniman.

Name	Age	Sex	State	Religion	Disease
Sarika	38	Female	Maharashtra	Hindu	Cancer
Padama	33	Female	Goa	Hindu	Viral infection
Salima	37	Female	Maharashtra	Muslim	TB
Monty	36	Male	Punjab	Parsi	No illness
Anna	33	Female	Goa	Christian	Heart-problem
Ranvir	32	Male	Punjab	Buddhist	TB
Rakesh	28	Male	Goa	Hindu	Cancer
Aakash	38	Male	Punjab	Hindu	Heart problem
Jon	26	Male	Goa	Christian	Heart-problem
Faiz	28	Male	Goa	Christian	Viral infection

Tablica 4.1. Prikaz podataka pojedinaca [5]

Uobičajene metode za postizanje k-anonimnosti za bilo koju vrijednost k:

1. Suzbijanje- u ovoj metodi, vrijednosti prepoznavanja atributa u svim ili nekim redovima zamjenjuju se simbolom "*". U slučaju da se atribut "Ime" potisne, osoba koja gleda tablicu će znati bolest, ali ne i ime osobe koja ima tu bolest.

2. Generalizacija-u ovoj metodi vrijednosti atributa su zamijenjene rasponom ili širom kategorijom. Kao primjer, kada se u obzir uzme atribut "dob", ako je osoba u dobi od 18 godina, može se zamijeniti s "15 <dobi<20" ili zamijeniti kategoričnom varijablom "mlad".

Tablica dobivena nakon primjene ovih dvaju koraka prikazanih u tablici 2.

Name	Age	Sex	State	Religion	Disease
*	30<Age ≤ 40	Female	Maharashtra	*	Cancer
*	30<Age ≤ 40	Female	Goa	*	Viral infection
*	30<Age ≤ 40	Female	Maharashtra	*	TB
*	30<Age ≤ 40	Male	Punjab	*	Heart Problem
*	30<Age ≤ 40	Female	Goa	*	Heart-problem
*	30<Age ≤ 40	Male	Punjab	*	TB
*	Age ≤ 30	Male	Goa	*	Cancer
*	30< Age ≤ 40	Male	Punjab	*	Heart-problem
*	Age ≤ 30	Male	Goa	*	Heart-problem
*	Age ≤30	Male	Goa	*	Viral infection

Slika 4.2. Anonimizirana tablica [5]

Dva najčešća napada na k-anonimnost su :

1. Homogenost napada: Ovaj napad može se pojaviti kada su sve vrijednosti za osjetljive atribute unutar skupa podataka k zapisa identične. Primjer takvog slučaja može biti tamo gdje je vrijednost atributa "bolesti" identična kao kod "godine", "spol" i "država".

2. Pozadinska znanja: U ovom slučaju, prethodno poznavanje povezanosti jedne ili više vrijednosti kvazinidentifikacijskih atributa koristi se za smanjenje skupa mogućih vrijednosti za osjetljivi atribut.

Model l-raznolikosti može se smatrati produženjem modela k-anonimnosti i može pružiti zaštitu od već opisanih napada na k-anonimnost. Glavna ideja za l-raznolikosti je da su vrijednosti osjetljivih atributa dobro zastupljene u skupini. Pokazano je da se postojeći algoritmi k-anonimnosti mogu proširiti kako bi se dobili skupovi podataka sa svojstvom l-raznolikosti. U modelu l-raznolikosti koriste se tehnike generalizacije i supresije za smanjenje granularnosti prikazivanja podataka. U nekim slučajevima napadač može upotrijebiti poznavanje rijetkog pozitivnog pokazatelja bolesti za zaključivanje vrijednosti. Takav pokazatelj može pružiti više informacija nego zajednički negativni pokazatelj. Osjetljive informacije mogu se zaključiti iz anonimnog skupa podataka koji zadovoljavaju svojstvo l-raznolikosti.

Model t-blizine proširuje model l-raznolikosti uzimajući u obzir raspodjelu osjetljivog atributa u tablici i u klasi. T -blizina uključuje da je raspodjela osjetljivog atributa u bilo kojoj klasi ekvivalencije blizu distribucije osjetljivog atributa u ukupnoj tablici. Ova metoda može pružiti zaštitu od otkrivanja osjetljivog atributa, ali ne i protiv otkrivanja identiteta.

4.3.1. Ostale metode zaštite privatnosti

Agregacija

U ovoj tehnici granularnost podataka se smanjuje. Ova se tehnika koristi za smanjenje rizika otkrivanja podatka pretvaranjem potencijalno osjetljivih zapisa (koji imaju visok rizik od otkrivanja) u evidencije s nižim rizikom objavljivanja. Kao primjer, promatra se slučaj u kojem postoji samo jedna osoba s određenom kombinacijom demografskih značajki u gradu, ali mnoge osobe s tim karakteristikama u nekoj državi. U takvom se slučaju podaci mogu objaviti na državnoj razini, a ne na gradskoj razini. To će smanjiti rizik od otkrivanja.

Suzbijanje

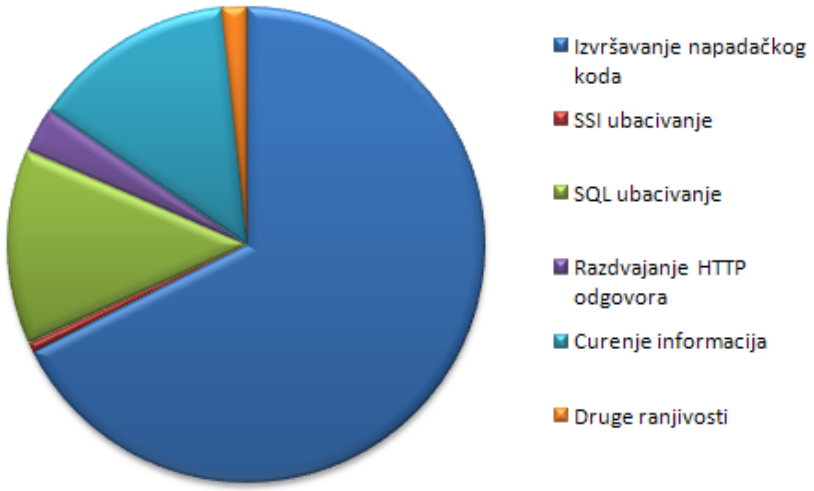
Organizacije koje objavljuju podatke mogu izbrisati osjetljive vrijednosti iz objavljenog skupa podataka. Ako su vrijednosti određenih atributa suprimirane, skup podataka s nedostajućim vrijednostima bit će stvoren. U nekim slučajevima možda neće biti moguće analizirati takav skup podataka. Kao primjer, konus može uzeti u obzir slučaj u kojem se potiskuju prihodi iznad određenih vrijednosti praga. Zatim će svaka procjena raspodjele dohotka temeljena na objavljenim podacima biti pristrana i prosječna i srednja vrijednost bit će znatno niža od stvarnih vrijednosti.

Zamjena podataka

U ovoj tehnici organizacije koje objavljuju podatke postavljaju swap vrijednosti podataka za određene odabrane zapise, a zatim puštaju skup podataka. Skup podataka se može otpustiti nakon prebacivanja vrijednosti atributa poput dobi, rase i spola za evidenciju s višom razinom rizika otkrivanja s odgovarajućim vrijednostima zapisa s nižom razinom rizika otkrivanja. Organizacije koje koriste ovu tehniku ne otkrivaju broj izmijenjenih vrijednosti i algoritme koji se koriste.

5. RANJIVOST APLIKACIJA

Zbog nedovoljnih provjera ulaznih podataka softver postaje ranjiv. U ovom dijelu rada biti će obrađene najčešćih ranjivosti koje se pojavljuju, a prikazane su na slici 5.1.



Slika 5.1. Najčešće ranjivosti aplikacija [6]

Izvršavanje napadačkog koda jedna je od najčešćih ranjivosti koje se pojavljuju na internetu. Ranjivost se pojavljuje kada neki od ulaznih parametara aplikacije postaje sastavni dio HTML dokumenta koji se prikazuje posjetiteljima. Žrtve ovih napada su korisnici aplikacija , a ne aplikacije ,te se zlonamjerni sadržaj isporučuje se pomoću JavaScript-a.

SSI ubacivanje iskorištava slabost servera na način da napadač šalje kod u web aplikaciju. Podaci u aplikaciji nisu dovoljno filtrirani prije ubacivanja u HTML datoteku koju interpretira serverska strana. Najpoznatiji alati za provjeru ovakve vrste napada su Webscarap, Burp Suite,W3af,Wapiti,Paros.

SQL ubacivanje vrši napade na baze i SQL upite. Time se napadačima omogućuje izvršavanje SQL upita nad bazom podataka te su svi korisnički podaci koji se tamo nalaze vidljivi napadaču.

Razdvajanje HTTP odgovora se javlja kada su podaci uneseni iz nepouzdanog izvora. Podaci koji su uključeni u http zaglavlje se šalju korisniku bez provjere zlonamjernosti. Napad se smatra vrlo

jednostavnim .Napadač prenosi zlonamjerne podatke ranjivoj aplikaciji, a aplikacija sadrži podatke u zaglavlju HTTP odgovora

Curenje informacija i davanje informacija vanjskom svijetu koji nema ovlašten pristup od kako su informacije prikupljene, poslane i procesuirane predstavlja veliki problem . Postoje razni načini zaštite podataka kako bismo omogućili sto bolju sigurnost kao sto su enkripcija, anonimnost te kontrola pristupa [8].

5.1. Mjere zaštite podataka

Informacijska sigurnost postiže se primjenom odgovarajućeg skupa kontrola, uključujući politike, procese, procedure, organizacijske strukture i softverske i hardverske funkcije. Mjere zaštite informacijskih sustava mogu se podijeliti na zaštitu na razini države, zaštitu samih podataka, programsku zaštitu, organizacijsku zaštitu, te fizičku i tehničku zaštitu.

Kako bi se osigurala što bolja zaštita podataka potrebno je obratiti pažnju na:

- fizičke metode zaštite,
- programske metode zaštite i zaštite podataka ,
- organizacijske metode zaštite

5.1.1. Fizičke metode zaštite

Fizičku sigurnost čine tri aspekta:

- zaštita informacijske opreme i uređaja
- zaštita okoline
- kontrola fizičkog pristupa

Fizička zaštite informacijske opreme se odnosi na opremu i uređaje kojima se služe zaposlenici unutar određenog sustava[9]. na slici 5.2. je prikazan primjer fizike zaštite računala , gdje se računalo odvaja od ostalih uređaja i onemogućuje se neovlašten pristup.

Slika 5.2. Primjer fizičke zaštite računala[7]

Fizička zaštita okoline informacijskog sustava objedinjuje sve mjere i metode potrebne za zaštitu informacijskih sustava od vanjskih čimbenika. Najsigurnije je ograničiti pristup računalu i spremiti ga u metalno kućište koje će ograničiti pristup, potrebno je osigurati toplinsku regulaciju i vodootpornost samog računala. Pristup prostoriji bi trebao biti zaštićen posebnim ulaznim vratima koja je moguće otvoriti jedino posebnim ključem ili digitalnom lozinkom, potrebno je osigurati videonadzor prostorije , te zaštitu alarmnim sustavima[9].

Za postizanje fizičke sigurnosti se koriste razni uređaji, poput:

- posebnih magnetskih kartica za zaposlenike koje omogućuju pristup samo određenim podacima
- Nadzornih infracrvenih kamera
- Alarmni sustava u slučaju neovlaštenog pristupa

5.1.2. Programske mjere zaštite

U najčešće programske mjere zaštite spadaju:

- Zaštita na razini operacijskog sustava
- Zaštita na razini korisničke programske podrške
- Kriptiranje podataka u komunikaciji
- Antivirusni alati
- Antispyware alati
- Zaštitni zid (Firewall)

Na razini operacijskog sustava izvršena je podjela na administratore i korisnike. Administratori svakom korisniku određuju:

- korisničko ime
- lozinku

Za svakog korisnika ili grupu korisnika mogu se odrediti različite ovlasti. Svako računalo može imati više administratora i korisnika[14].

Zaštitu na razini korisničke podrške čine ograničenja pri korištenju aplikacija i podataka unutar operacijskog sustava te je regulirana od strane mrežnog administratora. Ograničenja se dijele na tri razine te se najčešće provode lozinkom za pristup ili jednostavno zabranom pristupa određenim dijelovima operacijskog sustava.

1. razina – korisnicima je dozvoljeno čitanje određenih podataka iz baze podataka

2. razina –korisnicima omogućava izmjenu pojedinih podataka i unos novih podataka

3. razina –omogućuje brisanje podataka iz operacijskog sustava

Kriptiranje je postupak kojim se razumljiv tekst po određenom principu pretvara običnom korisniku u nerazumljiv tekst. Kriptiranje je najvažnije sredstvo programske zaštite osjetljivih i povjerljivih podataka. Koriste se simetrična i asimetrična kriptografija[15].

- Simetrična kriptografija je vrsta kriptografije kod koje postoji samo jedna vrsta transformacije podataka koja se obrnuto transformira sa samo jednim ključem, te joj je glavni nedostatak što obje osobe u komunikaciji moraju imati isti ključ. Simetrična kriptografija se deklarira kao slabija vrsta zaštite i rijetko je u upotrebi.

- Asimetrična kriptografija je vrsta kriptografije kod koje se koriste javni i tajni ključ. Javnim ključem se poruka s podacima transformira i kao takva vidljiva je svim sudionicima u komunikaciji, dok je tajni ključ samo kod jednog primatelja te je samo on u mogućnosti obrnuto transformirati poruku i pristupiti podacima.

Simetrični algoritmi su računski jednostavniji od asimetričnih algoritama. U praksi, asimetrični algoritmi su stotine do tisuće puta sporiji od simetričnih. Nedostatak simetričnog kriptiranja je postojanje kopije ključa kod svakog sugovornika. Da bi se osigurala komunikacija potrebno je mijenjati ključeve.

Antivirusni alati su računalni softveri koji se koriste za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih štetnih programa koji mogu uzrokovati probleme u korištenju

računala ili oštetiti podatke. Bitna funkcija antivirusa je automatsko obnavljanje, odnosno ažuriranja baze podataka o potencijalnim novim prijetnjama.

Spyware je vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole. Ono što ga razlikuje od virusa i crva je u tome što se obično ne replicira. Kao jedino sredstvo za prevenciju od malicioznih programa napravljeni su anti-spyware alati koji ih uklanjaju ili blokiraju. Najpoznatiji i najčešće korišteni besplatni alati su Ad-Aware SE, Spybot-Search & Destroy te Windows Defender.

Zaštitni zid (*engl. firewall*) je mrežni uređaj čija je namjena filtriranje mrežnog prometa tako da se stvori sigurnosna zona. Program koji želi pristupiti Internetu treba imati dopuštenje od vatrozida.

5.1.3. Organizacijske mjere zaštite

Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu[14].

5.2. Problemi u području zaštite

Klasične metode enkripcije same ne mogu zaštititi neki sustav već se rabe skupa s protokolima i uređajima za zaštitu podataka. Korisnici i uređaji su najslabija točka za napade. Jedno od mogućih rješenja za zaštitu je kvantna distribucija ključa, koja iako u praksi nesavršena i podložna napadima na fizičke uređaje pruža mogućnost otkrivanja napadača pomoću zakona kvantne fizike koji su kao takvi nepromjenjivi te služe kao osnova svakog kvantnog algoritma. Dodatna mogućnost je metoda tagiranja, koja iako neprimjenjiva u klasičnom okruženju, omogućuje da se razmjena ključa „izbaci“ iz jednadžbe te da se umjesto ključa koristi lokacija kao identifikator i ključ te se na taj način izbjegava gore navedene metode napada na klasične sustave[16].

5.3. Sigurnosni okvir

Mogući sigurnosni okvir koji bi se upotrebljavao za zaštitu podataka i korisnika, sastojao bi se od 9 ključnih dijelova:

1. Unaprijed određenih pravila i normi za sigurnost,

2. Procjene rizika,

3. Nadogradnje sustava,

4. Upravljanja imovinom,

5. Organizacije informacijske sigurnosti,

6. Operacijske sigurnosti koju čine procedure i odgovornosti, zaštita od zlonamjernog softvera, sigurnosna kopija, snimanje i praćenje, kontrola operativnog softvera,

7. Komunikacije i upravljanja operacijama,

8. Kontrole pristupa

9. Razvoj i održavanje informacijskih sustava

Pristup korisnika IT sustavima, mrežama, aplikacijama i informacijama mora se kontrolirati u skladu sa zahtjevima za pristup koji su određeni od strane relevantnih vlasnika informacijskih sredstava, obično prema ulozi korisnika. Generički ili testni ID-ovi ne smiju se izraditi niti omogućiti na proizvodnim sustavima, osim ako nakon unaprijed definiranog broja neuspjelih pokušaja prijave, unosi sigurnosnih zapisa i (ako je potrebno) sigurnosna upozorenja moraju se generirati i korisnički računi te se blokirati ako to nalaže vlasnik informacija.

Lozinke moraju biti duge i složene, te se sastojati od mješavine slova, brojki i posebnih znakova koji bi bili komplicirani za pogađanje. Informacije o autentifikaciji kao što su lozinke, sigurnosni zapisi, konfiguracije sigurnosti i slično moraju biti na odgovarajući način osigurane od neovlaštenog ili neprikladnog pristupa, izmjene, korupcije ili gubitka. Privremena prava pristupa koja se obično zahtijevaju za administriranje, konfiguriranje, upravljanje, sigurnost i nadzor nad informacijskim sustavima moraju se redovito pregledavati. Korisnici se moraju odjaviti ili blokirati zaporku prije nego što odlaze bez nadzora.

Preporučuje se izrada sigurnosnih kopija kako bi podaci ostali sačuvani u slučaju mogućeg napada. Ažuriranje sustava neophodno je za održavanje sigurnosti na mreži. Te se preporučuje uključivanje opcije automatskog ažuriranja.

6. ZAKLJUČAK

Glavni cilj pametnog grada je poboljšati kvalitetu usluga koje se pružaju te poboljšati kvalitetu života građanstva. Razvojem tehnologije u gradovima raste i težnja za povećanjem sigurnosti. Važno je nastaviti razvijati gradove, te pronaći još bolja rješenja vezana za očuvanje energije, stvaranje održivog okoliša, povećanje javne sigurnosti, te povećati sigurnost u prometu. Gledajući prema budućnosti, privatnost i javna sigurnost ostaju središnja briga za koju je potrebno više pravnih, znanstvenih i političkih razmatranja.

U uvodnom dijelu rada opisan je pojam pametnog grada i ukratko objašnjena njegova svrha. U glavnom dijelu rada opisane su zgrade sa visokom tehnologijom i mogućnostima koje nam pružaju poput ušteda energije i osiguranja imovine, te načini upravljanja uređajima u takvi zgradama i prijetnjama koje se javljaju u njima, obrađen je transportni sektor gdje je vidljivo da povećanjem tehnologije u automobilskoj industriji rastu i sigurnosni problemi koji mogu ugroziti živote sudionika prometa, predstavljeni su neki od mogućih napada i rješenja. U sektoru gradske uprave svaki zaposlenik koji obrađuje osobne podatke korisnika ima značajnu ulogu u održavanju privatnosti. Zaposlenici nikada ne smiju zaboraviti da je zaštita privatnih informacija u opisu njihovog poslova te treba raditi na osvještavanju zaposlenika o važnosti osobnih podataka pojedinca. U zdravstvenom sektoru zaštita privatnosti korisnika je ključna jer pacijenti ne bi pristali podijeliti svoje osobne podatke sa drugim ljudima, i u tom sektoru je nužno osigurati podatke, što se postiže protokolom za privatnost koji omogućuje ovlaštenom entitetu, kao što su liječnici, pristup pacijentovim društvenim i zdravstvenim podacima i sprečava neovlašten pristup. U financijskom sektoru neophodno je ograničiti dostupnost podataka, čime različiti slojevi imaju drugačiju mogućnost uvida u podatke i time se ograničava nepotreban uvid u korisničke podatke. Nabrojane su mogućnosti računovodstvenih prijevara i rješenja. U svakom sektoru vidljivi su mnogobrojni problemi koji ugrožavaju ljudske živote i njihovu imovinu.

Potrebno je proširiti svijest o prijetnjama koje su danas među nama, educirati veći broj stručnjaka koji će osmisliti nova rješenja za zaštitu, te nastaviti s razvojem tehnologije koja će olakšati život i riješiti probleme. S pravnog gledišta stvoriti zakone koji će osigurati korisnika i njegovu imovinu.

LITERATURA

1.K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X.Shen, Security and Privacy in Smart City Applications: Challenges and Solutions, 2017.

Dostupno na : https://ece.uwaterloo.ca/~k52zhang/papers/sapfsc.pdf

2. Aautomatizacija- inteligentna kuća, napredne elektroinstalacije

Dostupno na : http://novidom.blogspot.hr/p/napredne-elektronistalacije-domotika.html

3. Doel, O pametnim kućama, Pazin

Dostupno na:
https://www.google.hr/search?q=prikaz+pametne+kuce&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiF3qju0fLVAhWH1hQKHbe3A1kQ_AUICigB&biw=1366&bih=662#imgdii=7wHAjebtNND8sM:&imgrc=lnQgtOlqgE_e5M:

4. B.P., Zašto biste trebali koristiti dvostruku autentifikaciju? PCCHIP, 2017.

Dostupno na: http://pcchip.hr/helpdesk/zasto-biste-trebali-koristiti-dvostruku-aute7ntifikaciju/

5. P. Nicopolitidis, M. S. Obaidat, Smart Cities and Homes, Morgan Kaufmann,2016

Dostupno na: https://www.safaribooksonline.com/library/view/smart-cities-and/9780128034637/#toc

6. M. K., Automatizirano određivanje vrste Web aplikacije,2007.

Dostupno na: http://sigurnost.zemris.fer.hr/ns/websec/2007_kozina/

7. Nacionalni CERT, fizička zaštita informacijskih sustava,2010.

Dostupno na : http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf

8. M. Ghazouani, S. Faris, H. Medromi, A. Sayouti, Information Security Risk Assessment, A Practical Approach with a Mathematical Formulation of Risk, International Journal of Computer Applications, broj časopisa 8, broj sveska 103,str.37, 8.10.2014.

Dostupno na: http://research.ijcaonline.org/volume103/number8/pxc3899155.pdf

9. Edge group, softver za kontrolu pristupa

Dostupno na: https://www.edge-group.info/hr/softver-za-kontrolu-pristupa/

10. CIS, Sigurnost automobila, Centar informacijske sigurnosti, 2012.

Dostupno na: http://www.cis.hr/files/dokumenti/CIS-DOC-2012-01-036.pdf

11. D. Houlding, R. Samani, N. Vuckovic, Healthcare Security: User Experience, Compliance, and Risk,Intel, 2012.

Dostupno na: http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/healthcare-security-user-experience-compliance-and-risk.pdf

12. CA technologies, Healthcare Security Solutions: Protecting your Organization,Patients, and Information, 2014.

Dostuno na: http://www3.ca.com/~/media/Files/SolutionBriefs/healthcare-security-solutions.pdf

13. G. Gledec, Sigurnost i privatnost, FER

Dostupno na : https://www.fer.unizg.hr/_download/repository/Sigurnost-i-privatnost.pdf

14. Sigurnost informacijskih sustava, zlouporaba informacijskih tehnologija, etički izazovi primjene informacijskih tehnologija

Dostupno na: http://www.unizd.hr/portals/1/Primjena_rac/Brodostrojarstvo/predavanje_6.pdf

15. T. Besjedica, Metode zaštite i enkripcije u informacijskim sustavima, Kvantna distribucija ključa

Dostupno na: https://www.fer.unizg.hr/_download/repository/KDI_Toni_Besjedica.pdf

16. K. Nesek, Infrastruktura javnih ključeva i certifikacijski centar , 2017.

Dostupno na: http://sigurnost.zemris.fer.hr/pki/2004_nesek/seminar.pdf

17. Hrvatska akademska i istraživačka mreža, Usporedba VPN poslužitelja CCERT-PUBDOC-2008-11-246,

Dostupno na: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-11-246.pdf

18. L. Fabisiak, T. Hyla, T. Klasa, Comparative analysis of information security assessment and management methods,2012.

Dostupno na:
http://www.pszw.edu.pl/images/publikacje/t060_pszw_2012_fabisiak_hyla_klasa_-_comparative_analysis_of_information_security_assessment_and_management_methods.pdf

SAŽETAK

Razvojem tehnologije raste i briga za sigurnosti i privatnosti korisnika. U radu je opisan pojam pametnog grada, kao grada koji je prilagođen potrebama svojih stanovnika i koji je opskrbljen velikim brojem senzora i pametnih uređaja omogućujući lakši i sigurniji život stanovnika. Svaki sektor obrađen je kao zasebna cjelina i sadrži opis problema i rješenja vezana za probleme koji se u tom sektoru javljaju. Nakon analiziranja svakog od njih može se shvatiti važnost sigurnosti i privatnosti. Mnogi sigurnosni propusti ugrožavaju ljudske živote i imovinu.

Potrebno je upoznati korisnike usluga o prijetnjama koje u njima vladaju te ponuditi učinkovitija rješenja koja će još bolje osigurati korisničke podatke, svaku službenu osobu koja radi s osobnim podacima korisnika educirati o važnosti osobnih podataka pojedinca.

Ključne riječi: pametni grad, sigurnost, privatnost, integritet, dostupnost.

ABSTRACT

Security and Privacy in the Smart City Environment

Techology development requires better security and privacy for the user. The paper describes the concept of a smart city which is tailored to the needs of its inhabitants and equipped with a large number of sensors and smart devices, enabling easier and safer life for the inhabitants. Each sector is treated as a separate entity and contains a description of problems and solutions related to the problems that occur in that sector. After analyzing each entity , it is possible to understand the importance of security and privacy. Many security failures endanger human lives and property.

It is necessary to introduce users with the threats, offer more sophisticated solutions that will provide better security of user data, and warn each official person who works with personal information on their importance.

Key words: smart city, security, privacy, integrity, accessibility.

ŽIVOTOPIS

Maja Stanić rođena je 23.12.1995. u Slavonskom Brodu. Živi u Gunji gdje je završila OŠ ,, Antuna i Stjepana Radića". Nakon osnovne škole upisuje Opću gimnaziju ,,Vaso Pelagić" u Brčkom. Nakon završene srednje škole upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, te se odlučuje za smjer komunikacije i informatika.

_____

(potpis)