Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Luka Pevec

Organizacija varne soseske

diplomsko delo

visokošolski strokovni študijski program
prve stopnje
računalništvo in informatika

Mentor: prof. dr. Aleksandar Jurišić

Ljubljana, 2018

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Osrednji cilj diplomskega dela naj bo študija varnosti stanovanjske soseske oziroma večstanovanjskega poslopja. Z uporabo najnovejših tehnologij skušajte izdelati predlog za izboljšavo varnosti stanovanjskih sosesk. Tradicionalno varovanje enega objekta razširite na celotno sosesko, kot to počne npr. sosedska straža, vendar z uporabo IoT tehnologije. Pri pooblaščanju sosedov za določene funkcije uporabite tudi kriptografsko shemo za deljenje skrivnosti.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
IoT	Internet of things	Internet stvari
AES	Advanced Encryption Standard	Standard za šifriranje podatkov
CBC	Cipher Block Chaining	Način za uporabo bločnega šifriranja
PIR	Passive Infrared	Pasivno infrardeč
UTP	Unshielded Twisted Pair	Neoklopljena sukana parica
FBI	Federal Bureau of Investigation	Zvezni preiskovalni urad ZDA
UV	Ultra violet	Ultravijolična (svetloba)
GPS	Global Positioning System	Globalni sistem pozicioniranja

Povzetek

Naslov: Organizacija varne soseske

Avtor: Luka Pevec

Projekt Varna soseska je varnostni sistem namenjen varovanju večih stanovanjskih enot. V diplomskem delu opišemo manj običajen pristop varovanja domov, kjer se ne osredotočimo na posamezen stanovanjski objekt, temveč na več geografsko povezanih objektov, ki uporabljajo skupen varnostni sistem. Ideje za naš projekt črpamo iz samo-organizacijskega varovanja prebivalcev, tj. sosedskih straž in iz modernih tehnologij, koncepta interneta stvari, združevanja novodobnih alarmnih sistemov ter senzorjev. Projekt Varna soseska povezuje ljudi v skupen boj proti kriminalu. Sosedje s pooblastili dobijo omejen nadzor nad našim varnostnim sistemom, ki jim je dostopen prek mobilne in spletne aplikacije. Varna soseska uporabnikom omogoča, da na učinkovit in varen način poskrbijo za varnost v lastnih soseskah.

Ključne besede: internet stvari, sosedska straža, varnost doma, varnost v soseskah, pametna soseska, pametno mesto, deljenje skrivnosti.

Abstract

Title: Organizing safe neighbourhood

Author: Luka Pevec

Our project Safe neighbourhood is a security system designed for our living neighbourhoods. We describe unordinary approach to home security where we do not focus on a single residential building but rather on multiple geographically linked homes that use common security system. Ideas for our project came from neighbourhood watch organizations and modern technology concepts like the internet of things, connected classical security systems and advanced sensors. The project Safe neighbourhood connects people to a common effort against crime. Authorized neighbours get limited control over our security system, which is accessible through mobile and web application. Our solution allows users to provide security in their own neighbourhoods in an effective and safe way.

Keywords: internet of things, neighbourhood watch, home security, neighbourhood security, smart neighbourhood, smart city, secret sharing.

Poglavje 1

Uvod

Samo v Sloveniji se je leta 2017 vsakih 35 minut zgodil nov vlom [25]. Kdor še ni bil žrtev vlomilcev, najprej pomisli na nastalo denarno škodo, ki obsega od nekaj sto do več tisoč evrov. Vendar, po številnih anketah, raziskavah in osebnih izpovedih žrtev, denarna škoda predstavlja manjšo težavo. Psihološki efekt, ki ga pusti vlom na žrtev, njeno družino in bližnje sosede, je nekaj, kar v vseh vpletenih pusti dolgotrajnejše posledice.

Raziskava zavarovalnice Allianz iz Velike Britanje [19] je razkrila, da v povprečju traja 8 mesecev preden se žrtve ponovno počutijo varne v lastnem domu. Manj kot polovica od njih se še kdaj doma počuti popolnoma varne. Nekateri so obsedeni z varnostjo domov, drugi živijo v večnem strahu pred ponovnim vlomom. Za enega od 10 je izkušnja celo tako travmatična, da zapustijo svoj dom in se preselijo na novo lokacijo.

Raziskava razkrije negativen vpliv tudi na otroke, celo tiste, ki niso bili doma v času vloma. Otroci, ki so bili v preteklosti pod to travmatično izkušnjo je v 40% primerih nikoli ne pozabijo in jih spremlja do konca življenja. Če ste bili prej mnenja, da so varnostne rešitve namenjene le bogatim ljudem, ki jih skrbi za svoje premoženje, ste zdaj morda dobili občutek, da gre za večji problem, ki bi se ga morali lotiti kolektivno, skupaj kot družba, soseska in ne le kot paranoičen posameznik.

Naša diplomska naloga opiše novo rešitev takega skupinskega boja pred

kriminalci. V naši rešitvi združimo zgodovinske in trenutne elemente sosedske straže in njej podobnih oblik samozavarovanja ljudi z moderno tehnologijo. V projektu Varna soseska bomo prikazali način, kjer se lahko vsaka soseska neodvisno bori proti kriminalu. To bomo dosegli z drugačnim načinom uporabe klasičnih alarmnih sistemov, ki jih bomo povezali v splet. V resnici bomo ustvarili dve povezavi, eno med vsemi vpletenimi napravami in drugo, med uporabniki teh naprav. Varna soseska omogoča višjo varnost sosesk in izboljša počutje ljudi. Skupnost pomaga ljudem, ki živijo v strahu, samoti in tesnobi pred posegom v njihov življenjski prostor, saj jim da večji nadzor nad bližnjim in domačim okoljem, ki ni omejen le na njihovo posest ampak tudi širšo sosesko. Hitro tudi ugotovijo, da niso bili edini.

V poglavju 4 bomo predstavili našo rešitev, projekt Varna soseska in v naslednjih treh poglavjih nadaljevali z opisom pravnih omejitev pri realizaciji tega projekta, si ogledali možne nadgradnje in podobne druge rešitve, ki so trenutno že v uporabi po svetu. V podpoglavju 6.3 bomo opisali kriptografski princip deljenje skrivnosti, ki je del predlaganih nadgradenj projekta. Preden začnete z branjem glavnega dela, ki se začne s poglavjem 4, si lahko v poglavju 2 in 3 preberete o konceptu sosedske straže iz katere črpamo veliko idej in o tehnologiji interneta stvari, ki je podlaga za izvedbo našega projekta. Problem, ki ga naš projekt Varna soseska rešuje, natančneje predstavimo v podpoglavju 3.2.

Poglavje 2

Sosedska straža

Razumevanje koncepta sosedske straže je za spoznavanje naše rešitve ključnega pomena. Sosedska straža je koncept za preprečevanje kriminalitete. Gre za državljansko samozavarovanje in samoorganizacijo prebivalcev v obliko neuradnega nadzorovanja. Sosedska straža ima pogosto dogovorjeno sodelovanje s policijo, ki se razlikuje pri posameznih organizacijah sosedske straže.

2.1 Kaj je sosedska straža

Sosedska straža je ena izmed najstarejših in najbolj poznanih oblik preprečevanja kriminala. Zanjo je značilno, da imajo aktivno vlogo prebivalci soseske, ki se zavzemajo za izboljšanje varnosti v njej. Člani sosedske straže sodelujejo s policijo in ji pomagajo pri ohranjanju varnosti v svojih soseskah. Sosedska straža torej povezuje uradno institucijo s predstavniki civilne družbe. Ključno je, da se prebivalci skupnosti, ki je pod okriljem sosedske straže, ne zanašajo zgolj na delo policije, ampak z njo sodelujejo in tudi sami pripomorejo k varnejši soseski.

Vsaka organizacija sosedske straže ima svoje unikatne značilnosti, saj je produkt okolja, časa in družbe v katerem nastane. Pravil za organizacijo ni, so le smernice in dobre prakse, ki jih lahko člani posameznih organizacij

spreminjajo in prilagajajo svojim potrebam. Za prikaz delovanja in organizacije sosedske straže bomo uporabili model iz ZDA, ki ga uporablja National Sheriffs' Asociation, glej Pšenica [18]

2.1.1 Model NNW

Pri modelu NNW (National Neighborhood Watch) [24] organizacijo sestavljajo prostovoljci, ki živijo v skupni soseski. Vsaka sosedska straža ima svojega koordinatorja (angl. coordinator) in vodjo (angl. Block Captain), kar je v manjših skupnostih pogosto ista oseba. V večjih skupnostih je vodij več, pogosto se ustanovi tudi izvršni odbor. Na strani policije je pooblaščena oseba, ki sodeluje s sosedsko stražo. V nadaljevanju bomo opisali posamezne položaje.

Člani sosedske straže

Ljudje lahko na lastno pobudo ali na pobudo policije ustanovijo sosedsko stražo. Glavni pobudnik navadno prevzame položaj koordinatorja sosedske straže. Člani so osnovni element vsake sosedske straže, saj je njihova primarna naloga aktivno sodelovanje in spodbuda drugih članov. Naj velja, da se od zdaj naprej z besedo"član", vedno sklicujemo na osnovnega pripadnika sosedske straže. Njihove ostale naloge so:

- nadzor soseske (videonadzor, patruljiranje, opazovanje itd.),
- označevanje lastnine,
- izpolnjevanje vprašalnikov o varnosti doma,
- urejanje okolice soseske, npr. odstranjevanje grafitov, čiščenje itd.,
- utrjevanje hiš in objektov (npr. protivlomna zaščita oken in vrat, senzorske luči, kamere, varnostni sistemi itd.)
- ozaveščanje drugih o delovanju sosedske straže,
- zbiranje sredstev za delovanje sosedske straže.

Koordinator sosedske straže

Pobudnik za nastanek nove sosedske straže ima navadno največ motivacije in veliko prostega časa, zato ta pogosto prevzame delo koordinatorja. Delo koordinatorja je najbolj pomembno in časovno zahtevno. Na začetku ustanovitve je naloga koordinatorja predvsem iskanje novih članov in vzpostavitev stika s policijo (če policija ni pobudnik za ustanovitev sosedske straže). Kasneje njegove naloge v organizaciji obsegajo:

- sodelovanje, komunikacija in podpora policiji,
- obveščanje članov in vodij sosedske straže,
- organizacija srečanj in izobraževanj,
- motivacija članov,
- sodelovanje z različnimi lokalnimi organizacijami,
- hranjenje liste članov in liste z lastnino članov, kar je lahko nevarno, glej podpoglavje 6.2.

Vodja sosedske straže

V večjih organizacijah (število gospodinjstev ni formalno določeno) se pojavi potreba po novem položaju, vodji sosedske straže. Vodja je zadolžen za območja, ki vsebujejo do 15 gospodinjstev, njihovo število je torej odvisno od velikosti organizacije. Člani vodje izvolijo oz. se lahko ti prostovoljno javijo na položaj. Zadolžitve vodje so:

- povezovanje, ozaveščanje in komunikacija,
- obveščanje članov; npr. o sestankih, dogodkih, delavnicah itd.
- pridobivanje novih članov.

Policijski pooblaščenec

Policijski pooblaščenec skrbi za ustanavljanje in podporo organizacijam posameznih sosedskih straž na geografsko omejenem območju. Udeležijo se

prvega srečanja sosedske straže, na katerem poda informacije o aktivnostih in njihovem poteku. Nadaljnjih srečanj se udeležijo le ob predhodnem povabilu koordinatorja. Pooblaščenec mora za učinkovito delovanje poznati okolje delovanja sosedske straže, kulturo in demografijo prebivalcev. Prav tako potrebuje dostop do podatkov o kriminalu na območju njegovega delovanja.

2.2 Sosedska straža v Republiki Sloveniji

Sosedske straže v podobni obliki, kot je opisana v poglavju 2.1.1 v Republiki Sloveniji ni in ni nikdar bilo. V Sloveniji so delovale in delujejo organizacije, ki imajo skupne elemente s sosedsko stražo. Ena najstarejših oblik samoorganizacije prebivalcev na slovenskem ozemlju je obramba pred Turki v petnajstem stoletju. Kmetje so gradili utrjena naselja (tabore), ki so bili navadno na hribih, okrog cerkva. V tem času se je pojavila tudi obveščevalna mreža, ki je s prižiganjem kresov (grmad) na hribih opozarjala na bližajočo se nevarnost. Našteli bomo tudi nekaj podobnih organizacij iz 19. in 20. stoletja, ki so delovale na slovenskem ozemlju: orožniki, narodna "brana" (slo. obramba), mestna policijska straža, narodna zaščita in narodna milica. Poleg teh lahko omenimo tudi prostovoljna gasilska društva, lovska društva in Gorsko reševalno zvezo, ki imajo v slovenski zgodovini že dolgo tradicijo.

Vse naštete organizacije so način delovanja črpale iz francoskega načina izvajanja policijske dejavnosti, sosedska straža pa je način delovanja črpala iz angleškega. Zato se tudi pri nas verjetno ni nikoli zares razvila. V današnjem času globalizacije vsi aktivno iščemo učinkovite načine za povečanje varnosti vsepovsod, kar je tudi glavni razlog za nastanek naše obravnavane rešitve. V Sloveniji za ustanovitev sosedske straže ni potrebno ustanoviti organizacije ali je registrirati pri državnih organih. Za sodelovanje s policijo imamo tudi zakonsko podlago, ki je zapisana v 4. in 5. členu 435. Zakona o nalogah in pooblastilih policije, ki je del Uradnega lista Republike Slovenije. Omogočeno je sodelovanje s posamezniki, skupnostjo in organizacijami. Posamezniki imajo pri sodelovanju s policijo tudi zakonsko zaščito v primeru

škode, poškodb in smrti [26].

2.3 Posledice sosedske straže na okolico

Ustanovitev sosedske straže ima poleg večje varnosti tudi druge pozitivne učinke na okolico; krepitev skupnosti, boljša komunikacija med sosedi, sodelovanje s drugimi organizacijami, bolj urejena okolica, boljša pripravljenost ljudi v primeru nesreč ali katastrof. Višja je tudi nacionalna varnost, saj člani sosedske straže prijavljajo sumljive dogodke, ki so lahko del terorističnih dejanj.

Poleg vseh pozitivnih, obstajajo tudi negativna plat izvajanja sosedske straže. Gre za vprašanje zasebnosti. Strah pred zmanjšano stopnjo zasebnosti ljudi v soseski je upravičen, saj dejavnost sosedske straže upravičuje oprezanje in opazovanje v zameno za zagotovitev boljše varnosti v soseski. Pomembno je, da se v organizaciji vedno držimo zakonov o varovanju osebnih podatkov in ustavne osebnostne pravice.

Slika 2.1: Primer znaka, ki ga uporabljajo sosedske straže v ZDA.

Poglavje 3

IoT in problem, ki ga rešujemo

Za razumevanje naše varnostne rešitve je pomembno poznavanje pojma "internet stvari" za katerega bomo od zdaj naprej uporabljali kratico IoT (angl. Internet of Things). Predstavili bomo štiri ključne elemente IoT, ki sestavljajo "veliko sliko" (angl. big picture). Namen tega poglavja ni predstaviti IoT z inženirskega ali razvojnega vidika, ti so dobro opisani v knjigi *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things* [11]. Poleg IoT bomo v tem poglavju tudi natančneje predstavili problem, ki nas je pripeljal do razvoja in zasnove projekta Varna soseska. Našo rešitev bomo podrobneje predstavili v poglavju 4.

3.1 Osnove področja interneta stvari

Pojem internet stvari oz. IoT v letu 2018 ni več nov, saj se je prvič pojavil leta 1999. Opredelitev IoT je kljub temu za večino ljudi še vedno težavna, saj smo v času izredno hitrega razvoja tehnologije. V naših vsakdanjih življenjih smo obdani z "inteligentnimi", med seboj povezanimi napravami (stvarmi), ki se povezujejo v internet stvari. Ta povezava nam omogoča številne, pred tem nepredstavljive oz. mogoče možnosti v našem vsakdanjem življenju. Pametni mobilni telefon je primer take naprave, ki je spremenila življenje ljudi. Internet stvari definiramo kot uporabo standardiziranih komunikacij-

skih protokolov in omrežne infrastrukture, ki razširi navidezne meje interneta na neenotne samostojne (imajo možnost samostojne konfiguracije) naprave, ki lahko med seboj tudi sodelujejo. Gre za razširitev interneta v fizični svet. V posameznih razdelkih, ki sledijo bomo predstavili štiri ključne elemente, ki nam bodo pomagali razumeti IoT in našo rešitev:

1. zaznavanje,
2. komunikacija,
3. zajemanje in konsolidacija,
4. dostava informacij.

Zaznavanje

Za vsak IoT sistem je pomembno zajemanje podatkov iz našega vsakdanjega sveta, na mestu aktivnosti (angl. point of activity). Podatke zajemamo na različne načine, s statičnimi senzorji ali gibljivimi senzorji, npr. s pomočjo nosljivih naprav (angl. wearable device). Senzorji lahko zajemajo biometrične, biološke, okoljske, vidne ali slišne podatke. Zelo pogosto se uporablja kombinacija naštetih načinov zajema, saj so senzorji cenovno ugodni. Naša rešitev lahko uporablja od nekaj deset do nekaj sto povezanih senzorjev. Več o senzorjih sledi v podpoglavju 4.2.

Komunikacija

Mnoge nove IoT naprave, ki jih videvamo v našem življenju, niso načrtovane za optimalno komunikacijo z oblačnimi storitvami. Kaj so strežniki in oblačne rešitve, si lahko ogledate v podpoglavju 4.3. Te naprave potrebujejo način prenosa zaznanih informacij do strežnika oz. oblačne storitv, kjer se dobljene informacije procesirajo naprej. Prav v procesiranju teh informacij se skriva prava vrednost IoT sistemov. Za prenos informacij potrebujemo WiFi/LAN ali WAN komunikacije, glej pod razdelki 4.1.2. Odvisno od posameznega primera lahko potrebujemo tudi druge vrste komunikacij (npr. GPS, Bluetooth,

ZigBee itd.) vendar jih v naši rešitvi zaenkrat ne uporabljamo, zato jih ne bomo natančneje obravnavali.

Zajemanje in konsolidacija

Zajeti podatki so posredovani na strežnik, kjer se podatki iz različnih IoT naprav agregirajo. Tako zbrani podatki zagotavljajo koristne informacije za končnega uporabnika. Konsolidacija podatkov lahko vključuje tudi informacije iz drugih virov (drugi IoT sistemi, spletni viri, itd.). V večini IoT sistemov se na tem mestu dogaja tudi procesiranje zbranih podatkov. Procesiranje teh surovih podatkov nam lahko iz na videz nejasnih in nekoristnih podatkov prinese uporabne rezulate ter iskane informacije za katere so kupci včasih pripravljeni plačati ogromno denarja.

Dostava informacij

Zadnji korak za katerega je zadolžen sistem IoT je dostava uporabnih informacij končnim uporabnikom. Končen uporabnik je lahko potrošnik ali industrijski uporabnik, lahko pa je tudi druga naprava, npr. v modelih naprava napravi (angl. Machine to Machine, kratica M2M). Naša rešitev je usmerjena na potrošnika zato drugih končnih uporabnikov ne bomo obravnavali. Cilj pri potrošniško usmerjenih sistemih je zagotoviti informacijo na kar se da enostaven in transparenten način. Pomembno je premišljeno načrtovanje uporabniških vmesnikov, ki prinesejo optimizairano poenoteno izkušnjo prek različnih naprav in platform (npr. kombinacija telefon - tablica - osebni računalnik) ali prek različnih operacijskih sistemov (Windows, Linux, Mac OS, Android, iOS itd.). V naši rešitvi informacije dostavimo uporabniku prek mobilne aplikacije, ki je opisana v podpoglavju 4.4 in prek spletne aplikacije, ki jo obravnavamo v podpoglavju 4.5.

3.2 Opredelitev našega problema

Leta 2017 je bilo v Sloveniji 8752 vlomov, kar pomeni, da se pri nas zgodi približno 42 vlomov na dan [25]. Za primer lahko vzamemo ZDA s približno 327 milijoni prebivalcev, kjer se jih je leta 2016 zgodilo 1 515 096, kar je približno 4150 vlomov vsak dan [9]. Vlomilci pogosto oropajo več hiš v neki soseski, preden se premaknejo na drugo lokacijo [4]. Cilj naše rešitve je zaščita sosesk pred vlomilci s trajno in učinkovito varnostjo rešitvijo, ki deluje na osnovah sosedske straže, ki smo jo predstavili v poglavju 2 in IoT tehnologije, ki smo jo opisali v poglavju 3. Naša "varna soseska" je običajno na področju varnosti samozadostna in ne potrebuje nobenega stika z varnostno službo, vse temelji na zaupanju in sodelovanji s sosedi in drugimi družinskimi člani. Naša rešitev uporablja pristope, ki jih leta 2018 v Republiki Sloveniji najverjetneje še ni v uporabi. Po prestopu meje naše države so podobne rešitve v začetnih fazah, kar pomeni, da je razvoj take rešitve pomemben korak na področju varnosti prebivalcev po vsem svetu. Z dosedanjimi rešitvami se ukvarjamo v poglavju 7. Raziskava Koehlerja in Wortmanna [13] je pokazala, da so ljudje izredno pozitivno naravnani v neinvazivne varnostne rešitve, pri katerih sodelujejo njihovi družinski člani in njihovi sosedje. V anketi so rezultati presenetljivo pokazali, da bi ljudje raje omogočili dostop do varnostnega sistema tistim, ki jih poznajo kot policiji (dostop omogoča pomoč pri varovanju objekta). Ta raziskava nas je dodatno spodbudila v razvoj varnostne rešitve pri kateri lahko aktivno sodelujejo naši sosedje in drugi družinski člani, brez da bi pri tem ogrožali svojo varnost in našo zasebnost.

Poglavje 4

Varna soseska

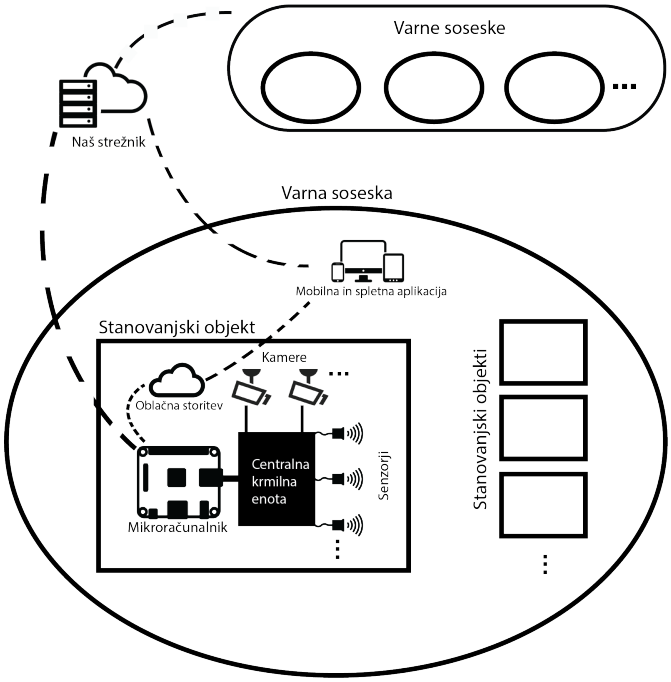
Cilj našega projekta Varna soseska je z uporabo najnovejših tehnologij izboljšati varnost v stanovanjskih soseskah in večstanovanjskih objektih. Ideje in inspiracijo črpa iz sosedske straže in novodobnih alarmnih sistemov, ki so namenjeni varovanju enega objekta. Od zdaj naprej bomo našo varnostno rešitev imenovali Varna soseska, skrajšano VS. Projekt VS torej povezuje več stanovanjskih objektov ali stanovanj, če gre za večstanovanjski objekt. Vsi objekti v VS imajo skupen, modularen varnostni sistem (elemente je možno dodajati ali odstranjevati po potrebi). Senzorji in njihovo število je odvisno od posameznega objekta. Vsi stanovanjski objekti so povezani z mobilno aplikacijo in spletno aplikacijo, ki pooblaščene uporabnike obveščata o morebitnih varnostnih incidentih.

Na tem mestu si oglejmo ključne elemente vsakega stanovanjskega objekta, ki je del VS:

- centralna krmilna enota,
- mikroračunalnik,
- senzorji gibanja,
- senzorji za zaznavanje razbitja stekla,
- senzorji za zaznavanje odprtih vrat in oken,
- sirena z bliskavico,

- kamere s senzorji gibanja.

Za administracijo omrežij uporabljamo strežnik s spletnim portalom, ki je namenjen administratorjem projekta VS in ne nujno končnim uporabnikom.



Slika 4.1: Shema projekta VS.

Primer 1. Delovanje projekta VS si bomo ogledali na enostavnem primeru. V stanovanjski soseski so tri stanovanjske hiše, ki uporabljajo VS. Skrbniki teh hiš so Timotej, Ana in Lucija. Timotej dela izmenično, Ana je vsako dopoldne v službi, Lucija pa dela od doma. Ker vlomilec X že ve, da je Ana vsak dan od 7:30 do 17:00 v službi, se kljub napisu *Pozor, objekt je varovan!* na njenih vratih odloči vlomiti v njeno hišo. Vlomilec želi hišo oropati prej kot v 15 minutah. Povprečen reakcijski policijski čas za nujne interventne dogodke je bil leta 2017 v Republiki Sloveniji 11 minut in 51 sekund [25]. Vlomilec X sklepa, da policija ne bo prišla dovolj hitro, saj bi jih nekdo moral poklicati takoj po sprožitvi alarma. Varnostne službe imajo prometne omejitve in so zato lahko še počasnejše od policije. Vlomilec X

se odloči vlomiti skozi zadnje kletno okno Anine hiše. V trenutku, ko X iz torbe vzame kovinsko palico, se sproži sirena (več o tem v nadaljevanju) in X se odloči zapustiti kraj, saj ne želi, da bi ga opazil kdo od sosedov med vlamljanjem.

Naš projekt VS je vlomilca zaznal takoj, ko je stopil na prednje dvorišče s pomočjo visoko tehnološke kamere, ki ima vgrajen sistem za zaznavanje gibanja. V času, ko je vlomilec hodil proti zadnjemu oknu in začel s postopkom vloma so Ana, Timotej in Lucija prejeli obvestilo na telefon, da se nekaj dogaja na Anini posesti. Ana in Lucija sta bili zasedeni in nista opazili obvestila na telefonu. Timotej je obvestilo opazil in skozi kamere spremljal vlomilca na Aninem dvorišču. Takoj, ko je videl kovinsko palico za vlamljanje je vedel, da gre za vlomilca in ne pogodbenega delavca. Preko mobilne aplikacije je lahko sprožil alarm v Anini hiši in poklical policijo. ◊

V našem primeru 1 smo vlomilca odgnali, še preden je ta povzročil škodo. Če se na obvestila mobilne aplikacije nihče ne bi odzval, bi se takoj ob vlomu sprožil alarm. Lucija, ki je bila v času vloma doma, bi alarm slišala in lahko ukrepala. Na mobilni aplikaciji bi preko posnetka najprej preverila, da gre res za vlom v Anino hišo in nato poklicala policijo. Če posnetka ne bi videl nihče, bi vlom (razbitje okna ali odpiranje okna) zaznali s senzorji na oknih, ki bi sprožili sireno in javili vsem uporabnikom VS prek spletne in mobilne aplikacije, da gre za vlom v kletne prostore Anine hiše. V obeh primerih je reakcijski čas hitrejši kot predvideva vlomilec X, saj v realnosti nihče ne pokliče policije takoj, ko zasliši sosedov alarm. Po Irski anketi 87% ljudi ob slišanem alarmu policije sploh ne bi klicali [12]. To je tudi pomemben problem, ki ga projekt VS rešuje, saj je odziv na alarm zagotovljen.

V danem primeru so obvestilo na mobilni aplikaciji prejele tri osebe. V realni postavitvi je teh oseb več, saj v posameznem stanovanjskem objektu lahko živi več oseb, ki so uporabniki tega sistema. Vpletenost večjega števila oseb izboljša varnost in odzivnost, saj je verjetnost, da nekdo opazi obvestilo mobilne aplikacije oz. sliši alarmno sireno, večja.

4.1 Centralna krmilna enota

V tem podpoglavju si bomo najprej ogledali delovanje klasičnega žičnega varnostnega sistema in nato opisali našo nadgrajeno alarmno centralo Bosch AMAX 2100, ki je povezana na mikroračunalnik. Skupaj tvorita "možgane" posamezne stanovanjske enote, ki je nato povezana v celoto, projekt VS. Našo centralno enoto in senzorje natančneje opisuje Bečić [3].

4.1.1 Klasičen žičen varnostni sistem

Nedolgo nazaj so bili glavna zaščita objektov ljudje, fizično varovanje z varnostniki. Danes so vsi varovani objekti zavarovani tudi s tehnološkimi napravami, ki zaznavajo, beležijo in opozarjajo na incidente. Osredotočili se bomo na varovanje domov in predstavili delovanje klasičnega žičnega varnostnega sistema. Zakaj uporabljamo žični sistem, je opisano v razdelku 4.1.2. Sestavni elementi tega sistema so alarmna centrala, v kateri je vsa logistika sistema. V njej je telefonski ali radijski pozivnik, ki obvešča in prenese dogodek naprej (npr. varnostnemu podjetju Sintal). Vsaka alarmna centrala ima vsaj eno tipkovnico, ki uporabniku omogoča interakcijo s sistemom. Na centralo so priklopljeni senzorji za zaznavanje vloma in sirena, ki zvočno ter svetlobno opozarja na incident. V primeru incidenta ima uporabnik (na njegovo nesrečo tudi vlomilec) navadno od 30 do 60 sekund časa, da onemogoči varnostni sistem. V nasprotnem primeru se vklopi sirena, centrala pa pošlje dogodek varnostni službi, ki ukrepa z intervencijo. V našem projektu VS uporabljamo več povezanih in nadgrajenih varnostnih sistemov, ki namesto varnostni službi, dogodke pošljejo drugim uporabnikom VS.

4.1.2 Zakaj žičen alarmni sistem

Izbira centralne enote sistema VS je bila najpomembnejša arhitekturna odločitev, saj so vse strojne komponente VS odvisne od nje. Pri zasnovi varnostnega sistema imamo na voljo dve tehnologiji - brezžično (angl. wireless) ali žično (angl. wired), možna pa je tudi kombinacija obeh. Obe imata različne pred-

nosti in šibkosti zato izbira ni enostavna. Brezžična tehnologija ima dve glavni prednosti: je cenovno ugodnejša in bolj prilagodljiva (angl. scalable). Zaradi vse večjega števila novih proizvajalcev na trgu brezžičnih IoT naprav in poceni priklopa, brez velikih stroškov montaže, je to cenejša možnost. Za priklop ne potrebuje dodatne opreme (npr. žic), kar omogoča dobro razširljivost, saj je dodaten (nov) senzor enostavno priklopiti na že obstoječ sistem. Nekateri novejši senzorji uporabljajo tehnologijo "avtomatskega odkritja" (angl. auto-discovery), ki še dodatno zniža čas montaže.

Kljub pozitivnim lastnostim ima brezžična tehnologija tri ključne ranljivosti zaradi katerih smo za našo uporabo v VS izbrali žično tehnologijo. Žičen sistem je zanesljivejši, saj je v uporabi 21 let dlje. To se kaže predvsem pri ohranjanju stalne in kvalitetne povezave. Brezžična omrežja imajo s povezavo pogosto težave zaradi interference (angl. interference), ki privede do manj kvalitetne povezave, lahko tudi izpadov iz omrežja, ki je lahko tudi posledica namernih motenj nepridipravov. Naslednja težava brezžičnih senzorjev je, da za delovanje uporabljajo baterije, ki jih je potrebno redno menjati, čas delovanja je namreč odvisen od pogostosti uporabe in senzorja. Število senzorjev se glede na posamezen objekt razlikuje. Na sliki 4.3 je prikazan primer stanovanjskega objekta z 48 senzorji. Ni si težko predstavljati obremenitve končnih uporabnikov, ki bi morali redno preverjati, da imajo vsi senzorji dovolj napolnjene baterije, ki se lahko izpraznejo prav v njihovi odsotnosti od doma, kar predstavlja visoko tveganje uporabe baterijskih senzorjev in drugih varnostnih naprav. Zadnja šibkost je varnost, vendar za projekt VS, najpomembnejša. Odločilno vlogo je imel članek Fernandesa, Junga in Prakasha [10], v katerem so prikazali ranljivost sodobnih brezžičnih alarmnih sistemov. Izkoristili so zasnovo ogrodja (angl. framework design) in prikazali štiri napade:

1. podtikanje kod za odpiranje vhodnih vrat,
2. krajo obstoječih kod,
3. razorožitev alarma,

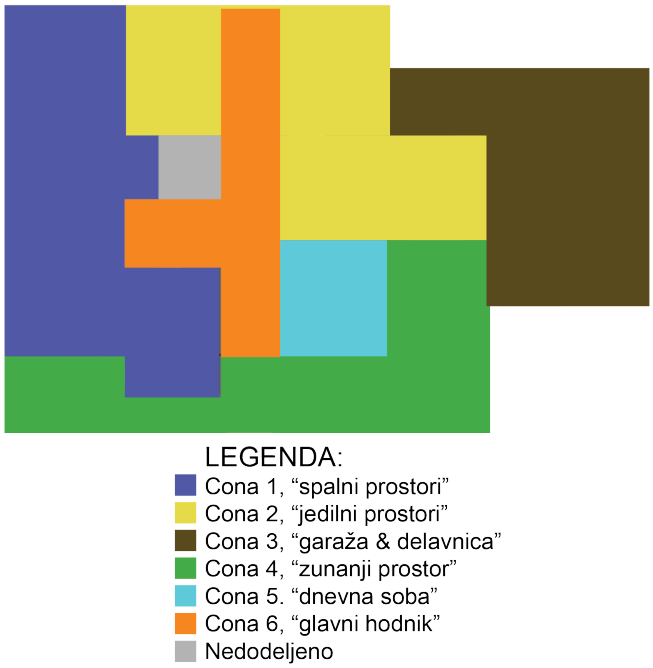
4. sprožitev lažnega požarnega alarma.

V članku so prikazali da je vse našteto mogoče sprožiti na daljavo, kar predstavlja nedopustno ranljivost naše varnostne rešitve, ki bi uporabljala podobno tehnologijo. Žične povezave so običajno zaščitene s požarnim zidom (angl. firewall) na lokalnem omrežju (angl. Local Area Network, LAN), kar nam omogoča skoraj popolno kontrolo komunikacijskega sistema in zgoraj našteti napadi zaradi enostavnejših komunikacij med senzorji in centralno enoto niso mogoči.

4.1.3 Bosch AMAX 2100

Torej, odločili smo se, da bomo izbrali žičen alarmni sistem. Na izbiro imamo več centralnih enot, ki jih lahko izberemo za osnovo našega sistema. Po pogovoru s strokovnjakom (A. Jurkovnik) smo izbrali centralno alarmno enoto "Bosch AMAX 2100", ki ponuja vse trenutne in prihodnje željene funkcionalnosti. O prihodnjih nadgradnjah pišemo v poglavju 6. AMAX je nato povezan na mikroračunalnik (npr. Raspberry Pi). Centrala deluje kot klasična alarmna centrala povezana z varnostno službo, ki je opisana v podpoglavju 4.1.1. V našem primeru vlogo varnostne službe prevzamejo uporabniki projekta VS. Na centralno alarmno enoto sta povezani vsaj dve tipkovnici, zunanja in notranja. Zunanja je namenjena pooblaščenim sosedom za izklop sirene, ki je na daljavo iz varnostnih razlogov ni mogoče izklopiti. Zunanji dostop do tipkovnice ne vpliva na varnost VS, saj brez varnostne kode vlomilec sirene ne more izklopiti. Notranja tipkovnica je enaka zunanjim, le da je zaradi uporabniške izkušnje locirana v stanovanjski objekt. Poleg tipkovnice so na centralo povezani še drugi senzorji, ki jih bomo natančneje opisali v podpoglavju 4.2. Centralna enota senzorsko zabeležene incidente pošlje na mikroračunalnik, ki je priključen preko IP naslova in omogoča nadaljno komunikacijo s strežnikom in oblačno storitvijo. Slednji so namenjene komunikaciji z ostalimi člani VS in hrambi videoposnetkov. Varnostni sistem AMAX uporablja 1-8 con, ki so namenjene lažjemu prepoznavanju lokacije

incidenta. Vsaka cona pokriva območje, ki ji ga dodeli uporabnik. Primer: incident razbitja okna se je v našem primeru zgodil v jedilnici, ki ji je dodeljena cona 2 z oznako "jedilni prostori". Na spodnji sliki 4.2 je prikazan opisan primer v katerem je uporabnik dodelil 6 od 8 con v svojem stanovanjskem objektu (ni nam potrebno dodeliti vseh). ID senzorja na oknu je centralni enoti neviden, kar je za naše potrebe dobrodošlo, saj je uporabniška izkušnja pri uporabi boljša. V primeru vloma ni pomembno specifično razbito okno, za uporabnika je pomembno le, približna lokacija vlomilca. Za varnost komunikacijskih povezav, centrala uporablja 256 AES (angl. Advanced Encryption Standard) šifriranje v CBC načinu (angl. Cipher Block Chaining), ki veljata za mednarodni standard na področju kriptografije za zagotavljanje varnih povezav [14], [2].



Slika 4.2: Primer razdelitve con v stanovanjskem objektu.

4.2 Senzorji

Projekt VS trenutno uporablja 5 različnih vrst senzorjev. Število vseh senzorjev v posameznem stanovanjskem objetku je odvisno od velikosti, tlorisa, števila nadstropij, oken in vrat. Kot smo omenili v razdelku 4.1.2 je teh senzorjev več deset, kar si lahko ogledamo tudi na sliki 4.3. Senzor je vsaka naprava, ki zaznava ali meri fizikalne lastnosti in se na njih odziva. V tem podpoglavju jih bomo natančeje opisali. Običajno so senzorji na centralno enoto povezani z žicami.

4.2.1 Senzorji premikanja

Za pokritje večjih notranjih prostorov in hodnikov je najbolj smiselna uporaba senzorjev premikanja. Njihov glavni namen v VS je zaznavanje vlomilca in pošiljanje alarma centralni enoti, vendar lahko služijo tudi drugim namenom, s katerimi se trenutno projekt VS ne ukvarja. Delujejo samo, če jih uporabnik vključi, praviloma to stori, pred odhodom iz varovanega objekta ali pa že pri ohodu iz določene cone. V VS uporabljamo senzorje premikanja PIR (angl. Passive Infrared), ki so najpogosteje uporabljeni v domačih alarmnih sistemih. Zaznava toploto in gibanje v okolici s pomočjo mreže (angl. grid), ki se na nenadne spremembe infrardeče energije odzove s pošiljanjem signala centralni enoti, podrobneje so to opisali v članku Song, Choi in Lee [21]. Senzor, ki ga uporabljamo v projektu VS je neobčutljiv na male živali (tudi otroke), ki ne presegajo 20kg. Število senzorjev je odvisno od posameznega objekta. Vsak pokriva 12m $\times$ 12m veliko območje v prostorih brez ovir, saj senzorje gibanja blokirajo stene in drugi visoki objekti. Senzorji gibanja so najučinkovitejši v večjih in odprtih prostorih (brez ovir).

4.2.2 Senzorji na oknih in vratih

FBI je v svojem poročilu razkril, da se 23% vseh vlomov v ZDA zgodi skozi okno v pritličju. Zato je pomembno, da so vsa okna, ki so lahko dostopna dobro fizično zavarovana (npr. z kovinskimi mrežami). Pri oknih je največja

težva to, da lahko skozenj vlomilci pridejo na dva načina, razbijejo oziroma razrežejo steklo ali ga s silo odprejo in stekla ne poškodujejo. Odločili smo se, da projekt VS pokrije oba primera ne glede na statistiko pogostejšega pristopa vlomilcev. Na oknih torej uporabljamo senzorje, ki zaznavajo razbitje stekla in senzorje, ki zaznavajo odprtje oken. Izbrali smo detektorje razbitja stekla, ki sprožijo alarm v primeru detekcije zvoka razbitja stekla. Te senzorji lahko pokrivajo več oken hkrati in so v kombinaciji z ostalimi seznorji dovolj učinkoviti. Za zaznavanje odprtega okna uporabljamo magnetne senzorje, ki sprožijo alarm ob prekinitvi stika med magnetoma.

4.2.3 Sirena

V primeru sprožitve senzorjev (vseh razen kamere) se takoj sproži alarmna sirena z bliskavico. Sirena ima dve glavni nalogi: preplašiti vlomilca in opozariti sosede o sproženem alarmu. Sirena je zunanja in notranja ter oddaja svetlobne signale z bliskavico. Če vlomilca bliskanje in glasen zvok ne odžene iz objekta, mu ta vsaj oteži delo in zmanjša koordinacijo in oslabi sluh in vid. V prihodnosti bi lahko sistem nadgradili z uporabo pametnih luči v objektu, ki bi se v primeru vloma vklopile. V primeru sprožitve sirene dobijo vsi člani VS opozorila prek mobilne aplikacije in incident, ki je sprožil alarm. Opozorilo vsebuje le, kateri senzor in na kateri lokaciji (coni) je prišlo do incidenta. Opozorilo vsebuje tudi posnetek s kamere, če ima uporabnik za to ustrezno pooblastilo. Naloga uporabnikov, ki prejmejo in opazijo opozorila je, da presodijo ali gre za lažen alarm ali ne. V primeru lažnega alarma lahko pooblaščeni sosedje izklopijo sireno le prek zunanje tipkovnice, v primeru pravega alarma pa morajo nemudoma poklicati policijo in ji posredovati vse koristne podatke.

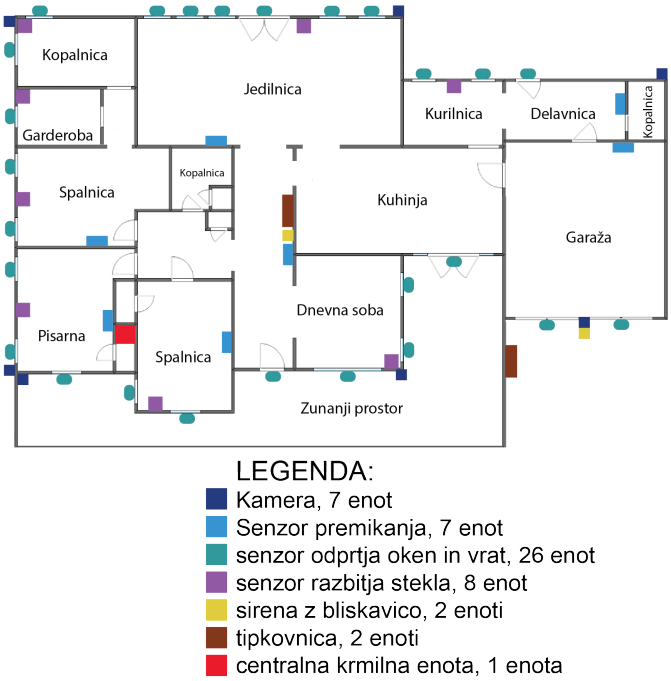
4.2.4 Kamere z zaznavanjem gibanja

V interesu uporabnikov projekta VS je, da imajo do kamer v njihovi odsotnosti dostop tudi njihovi zaupanja vredni pooblaščeni sosedje. Ti lahko

v primeru sproženega alarma lažje ocenijo situacijo in primerno ukrepajo. Kamere zmanjšajo število lažnih alarmov, saj lahko s posnetki preverimo ali gre za vdor ali ne. Izbira kamer je široka, zato smo na podlagi priporočil strokovnjaka izbrali kamere "Hikvision DS-2CD1043G0-I", ki imajo visoko resolucijo (2560 x 1440) in snemajo z 20 sličicami na sekundo (angl. frames per second). Vanje so vgrajeni PIR senzorji premikanja s 30m dosegom. To pomeni, da kamera ne snema ves čas ampak samo v primeru zaznanega gibanja, kar pripomore k nižji porabi energije in prostora za shranjevanje posnetkov. Omogoča pogled v živo preko lastnega programa, ki je na volju tudi kot mobilna aplikacija. Kamera je na internet povezana preko UTP kabla ali Wi-FI omrežja, če je mogoče izberemo žično povezavo zaradi zanesljivosti povezave, opisane v razdelku 4.1.2. Kamera posnetke pošlje centralni enoti, ki jih nato posreduje na mikroračunalnik. Ta shrani posnetke direktno na oblačno storitev (angl. cloud service), ki jo izbere uporabnik in ne naš strežnik. S tem se razbremenimo odgovornosti hrambe občutljivih osebnih podatkov (videoposnetkov), glej podpoglavje 5.2 in prihranimo prostor na strežniku, s čimer rešimo težave z razširljivosto projekta VS. Uporabniki imajo tudi popoln nadzor in dostop do svojih posnetkov.

4.3 Strežnik

Namen strežnika je distribucija podatkov in storitev (angl. services) med odjemalce (angl. clients). Posamezen strežnik lahko služi več odjemalcem in posamezen odjemalec lahko uporablja več strežnikov hkrati. V projektu VS so odjemalci naši uporabniki, ki uporabljajo dva strežnika. Prvi je oblačna soritev za hrambo in ogled posnetkov s kamer in drugi je strežnik, ki smo ga razvili prav za potrebe VS. Oblačna storitev pomeni zakup računske moči, prostora, aplikacij in drugih IT virov prek interneta. Strežnik je preko interneta povezan na vse mikroračunalnike, ki se uporabljajo v določeni soseski, ki so del projekta VS. Zasnovan je tako, da lahko upravlja z več logično ločenimi soseskami. Namen strežnika je, da omogoča distribucijo podatkov



Slika 4.3: Primer razporeditve strojnih elementov v stanovanjskem objektu.

in povezavo uporabnikov, objektov, mobilne ter spletne aplikacije. V podatkovni bazi shranjuje le najnujnejše podatke o uporabnikih in ne shranjuje posnetkov iz videokamer, le povezave na te posnetke uporabnikom, ki so za to pooblaščeni. Strežnik je ključen za opozarjanje drugih uporabnikov na varnostne incidente, saj prenaša informacije o proženju alarma od enega objekta do drugega, ki ima za to pooblastilo. Natančnejše specifikacije našega strežnika opisuje Ž. V. Dragan [8].

4.4 Mobilna aplikacija

Na primeru 1 je prikazano delovanje projekta VS. Iz njega je tudi razvidno, da ima mobilna aplikacija poleg sirene, ključno vlogo pri obveščanju uporabnikov o varnostnih incidentih. Naša mobilna aplikacija uporabnikom omogoča:

- prikaz dogodkov,

- trenutno varnostno stanje po nastavljenih conah, glej 4.1.3,
- pregled preteklih dogodkov,
- deljenje dogodkov,
- klicanje na različne intervencijske številke,
- proženje sirene (izklop sirene ni mogoč iz varnostnih razlogov),
- spremljanje kamer v živo (povezava do aplikacije kamere).

Glavna naloga mobilne aplikacije je nadzor in pregled stanja naše varnostne rešitve na daljavo. Mobilna aplikacija nam omogoča tudi omejen vpogled in nadzor varnostnega sistema drugih (pooblaščenih) uporabnikov (sosedov). Pooblaščeni uporabniki imajo na voljo naslednje funkcionalnosti:

- trenutno stanje po vseh osmih conah,
- prikaz naših tekočih dogodkov, brez prikaza zgodovine,
- hitro klicanje na različne intervencijske številke,
- proženje naše sirene,
- ogled zajetega posnetka ob dogodku z možnostjo hitrega ukrepanja (vklop sirene in klicanje policije oziroma potrditev, da gre za lažen alarm).

Trenutno je mobilna aplikacija razvita le za operacijski sistem Android, kar predstavlja težavo, ki jo opišemo v poglavju 6.1. Več o mobilni aplikaciji si lahko preberete v diplomskih nalogah V. Šemrova oz. T. Špeharja [27], [28].

4.5 Spletna aplikacija

Če je glavna naloga mobilne aplikacije obveščanje in pregled nad trenutnim stanjem, nam spletna aplikacija omogoča delno administracijo projekta VS. Ključne funkcije spletne aplikacije so:

- upravljanje s pooblaščenimi uporabniki, glej podpoglavje 4.4,

- pregled vseh vpletenih v VS (pooblaščenih in nepooblaščenih uporabnikov),
- zgodovina dogodkov,
- izvoz dogodkov,
- trenutno stanje po vseh osmih conah,
- možnost vklopa sirene,
- povezava z oblačno storitvijo, kjer uporabniki hranijo svoje videoposnetke.
- upravljanje s senzorji (dodajanje / odvzemanje).

Namen spletne aplikacije je torej določanje pravic drugim uporabnikom in administracijo, sem štejemo upravljanje s senzorji. Pomembno je, da moramo za pooblastitev drugega uporabnika dobiti njegovo potrditev, saj s tem, ko pooblastimo drugega uporabnika tudi on dobi nadzor nad našim sistemom, za več informacij o pravicah pooblaščenih uporabnikov glej podpoglavje 4.4.

Poglavje 5

Omejitve pri realizaciji

Za uspešno realizacijo projekta VS je pomembno upoštevanje zakonov Republike Slovenije, primerna skrb za osebne podatke in varnost naše rešitve. V sledečem podpoglavju si bomo ogledali najpomembnejše omejitve projekta VS.

5.1 Zakoni na področju izvajanja videonadzora v Republiki Sloveniji

Informacijski pooblaščenec je v dokumentu Smernice glede izvajanja videonadzora [17] podal odgovore na najpogostejše zastavljena vprašanja glede videonadzora z vidika Zahtev zakona o varstvu osebnih podatkov. Omenili bomo nekaj najpomembnejših zakonov glede izvajanja videonadzora, ki zajemajo videonadzor v zasebnih stanovanjskih objektih in posestvih. Videonadzor je sistematično snemanje, prenos in shranjevanje žive slike z ene lokacije na drugo. Sem spada tudi prenos žive slike brez snemanja (t.i. podaljšano oko). Med videonadzor ne štejemo video domofona, saj ima ta povsem drugačno funkcijo. Najpomembnejši zakoni, ki se jih mora držati vsak uporabnik projekta VS, ki uporablja videonadzor:

- videonadzor je dovoljen le na posesti posameznika,

- predpis ukrepov za zavarovanje osebnih podatkov,
- določiti osebe, ki so odgovorne za evidenco nadzornega sistema,
- zagotoviti evidenco, iz katere je mogoče ugotoviti, kdaj so bili posamezni osebni podatki iz evidence videonadzornega sistema uporabljeni ali drugače obdelani in kdo je to storil,
- snemanje sosednjih in javnih zemljišč je dovoljeno samo z ustreznim dovoljenjem.

Izvajanje videonadzora je najstrožji v večstanovanjskih objektih, saj je zakonodajalec ocenil, da gre v tem primeru za hujši poseg v zasebnost posameznikov. Poleg prej naštetih moramo pri izvajanju videonadzora večstanovanjskih objektov upoštevati še:

- pisna privolitev solastnikov o uvedbi videonadzora,
- objaviti obvestilo o izvajanju videonadzora,
- nadzor vhodov/izhodov stavb in skupnih prostorov,
- dostop imajo lahko le pooblaščeni stanovalci ali osebe pogodbenega obdelovalca,
- celovitost in zaupnost,
- odgovornost.

Prepovedan je videonadzor vhodov stanovanj, dvigal in delavnice hišnika.

5.2 Osebni podatki

Osebni podatek pomeni katero koli informacijo, ki je povezana z določenim ali določljivim posameznikom. Slednji predstavlja osebo, ki jo je mogoče neposredno ali posredno določiti. V nadaljnjem besedilu je to končni uporabnik projekta VS.

V interesu uporabnikov projekta VS je, da v podatkovni bazi hranimo le najnujnejše osebne podatke uporabnikov. Občutljivi podatki uporabnikov so

dostopni le njim. Občutljivi podatki so na primer posnetki iz njihovih video kamer, zgodovina sprožitev senzorjev, informacija o tem, komu so dodeljeni dostopi do njegovega sistema itd. Dostop do občutljivih podatkov lahko uporabniki po potrebi omogočijo tudi drugim, saj s tem povečajo funkcionalnost projekta VS.

5.2.1 Obdelava osebnih podatkov

Obdelava osebnih podatkov je vsako dejanje, ki se izvaja v zvezi z osebnimi podatki z avtomatiziranimi sredstvi ali brez njih. To vključuje zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje, ki so zapisani v uradnem list EU, člen 4 [16]. V projektu VS se držimo vseh 6 načel v zvezi z obdelavo osebnih podatkov, ki jih podaja Uradni list EU člen 5(1)[16].

- zakonitost, pravičnost in preglednost,
- omejitev namena,
- najmanjši obseg podatkov,
- točnost,
- omejitev shranjevanja,
- celovitost in zaupnost,
- odgovornost.

Obdelava uporabniških podatkov je zakonita po točki (b) člena 6(1)[16], kjer izpolnjujemo pogoj, da je obdelava osebnih podatkov potrebna za izvajanje pogodbe, katere pogodbena stranka je uporabnik projekta VS. Obdelava osebnih podatkov je torej v skladu z zakonodajo Republike Slovenije. V projektu VS trenutno obdelujemo in hranimo naslednje osebne podatke: ime in

priimek, naslov, telefonsko številka, elektronska pošta. Tipi obdelave podatkov vključujejo shranjevanje, omogočanje dostopa, spreminjanje, zbiranje in uničenje podatkov.

5.3 Varnost

Za uspešno izvedbo projetka VS je pomembno, da je ta varno zasnovan. Poleg logične varnosti je pomembno tudi ustrezno fizično zavarovanje občutljivih elementov varnostne rešitve. Varnost je pomembna tako iz pravnega vidika varovanja osebnih podatkov, kot zagotavljanja varnosti projekta iz praktičnega vidika. V mislih imamo nepooblaščene dostope in onemogočenje delovanja sistema. Varnostni sistem, ki ni ustrezno zaščiten v praksi ni uporaben. Naloga vsakega zasnovalca varnostnih sistemov je, da varnost postavi na prvo mesto.

Pri projektu VS za varnost poskrbimo s sledečimi ukrepi:

- dostop do posnetkov ima le uporabnik, ki si ga s sledenjem naših navodil ustrezno logično zavaruje,
- dostop do posnetkov je organiziran preko programskega vmesnika,
- vsak dostop do posnetkov se evidentira,
- za osnovo uporabljamo varen in zanesljiv žičen alarmni sistem,
- podatke šifriramo,
- uporaba žičnih senzorjev.

Poglavje 6

Nadgradnje projekta VS

Projekt VS je v začetni fazi razvoja. Poleg rednega vzdrževanja in odpravljanja varnostnih lukenj lahko projekt VS nadgradimo tudi na popolnoma druge načine. Omenili bomo aplikacijo z listo premoženja uporabnikov, nadgradnjo projekta VS z družabnim omrežjem, ki pripomore k boljši komunikaciji s sosedi, grajenju skupnosti in k dobrim sosedskim odnosom. Nazadnje bomo omenili nadgradnjo, ki posploši koncept VS v VPS - Varna Pametna Soseska (Smart Safe Neighbourhood, SSN). V naslednjem podpoglavju bomo nadgradnje razdelili na nujne in izbirne ter jih na kratko opisali.

6.1 Nujne nadgradnje VS

Nekatere nadgradnje in izboljšave projekta VS so nujne. Za projekte v začetni fazi je pričakovano večje število nepričakovanih napak in hroščev zato bomo najprej omenili nujnost rednega vzdrževanja in odpravljanja varnostnih lukenj ter drugih programskih napak. Pričakovane so tudi druge vrste težav (programske in strojne), ki se lahko pojavijo pri vsakodnevni uporabi naše varnostne rešitve. Ne smemo pozabiti tudi na morebitne težave s strojno opremo (npr. vandaliziranje izpostavljenih elementov). Naslednja nujna nadgradnja je implementacija novih preverjenih rešitev na področju varnosti, ki v času nastanka projekta VS še niso obstajale. Cilj je, da je Varna soseska "v

koraku s časom" in preprečiti zastaranje tako na področju varnosti, kot tudi uporabniške izkušnje (angl. User experience design) in oblikovanja aplikacij (angl. application design).

Naslednja pomembna nadgradnja je izdelava in podpora mobilne aplikacije za mobilne telefone in tablične računalnike podjetja Apple. Njihovi tablični računalniki (iPad) po podatkih iz leta 2017 zavzemajo največji tržni delež s 26.8% [5], na trgu mobilnih naprav imajo prav tako najvišji tržni delež z 19.7% (glede na posamezne proizvajalce) v letu 2017 [6]. Dokler ne omogočimo podpore Applovim mobilnim napravam, ne moremo pričakovati masovne uporabe naše rešitve, saj je mnogo ljudi sploh ne bi mogla uporabljati - Apple je februarja 2018 v svojem četrtletnem poročilu zapisal, da imajo skupaj več kot 1.3 miljarde aktivnih naprav [1].

6.2 Izbirne nadgradnje projekta VS

Izbirne nadgradnje niso nujno potrebne za učinkovito delovanje, bi pa z njihovo pomočjo naš projekt občutno izboljšali ali povsem spremenili. Med delom na projektu VS so se pojavile številne možne izboljšave, predstavili bomo tri najbolj zanimive za potencialno realizacijo. Vsaka od nadgradenj je zase večji projekt in je natančnejši opis izven obsega te diplomske naloge.

Družabno omrežje

Najprej naj omenimo razvoj družabnega omrežja za potrebe projekta VS kot samostojno mobilno in spletno aplikacijo, ki ima možnost intergacije s trenutnim sistemom. Glavni cilj tega "sosedskega družabnega omrežja" je boljša povezanost uporabnikov, ki so že del VS in ni mišljeno kot orodje za iskanje novih uporabnikov. Vsaka posamezna instanca projekta VS bi tako imela ločeno zaprto in navzven anonimno skupino znotraj tega omrežja. Uporabniki bi torej lahko videli le člane svoje soseske, druge organizacije bi bile nevidne. Povezovanje med soseskami bi vsaj sprva onemogočili, saj bi lahko prišlo do zlorab in ogrozitve varnosti in učinkovitosti projekta VS. V

mislih imamo predvsem potencialne kriminalce, ki bi vohunili po omrežju z lažno identiteto in tako iskali primerne tarče in žrtve. Družabno omrežje bi omogočalo varno in šifrirano medsosedsko komunikacijo, pregled nad dogodki v soseski, deljenje sumljivih dogodkov z drugimi uporabniki. Z uporabo družabnega omrežja bi okrepili medsosedske odnose in tako pripomogli k boljšemu in varnejšemu življenju v soseski.

Lista z vredno lastnino uporabnikov

V 2.1.1 podpoglavju govorimo o listi vredne lastnine uporabnikov (angl. Valuable Property Record), ki jo po modelu NNW hrani koordinator sosedske straže, nekatere druge oblike sosedskih straž pa priporočajo, da listo hrani vsak posameznik zase [7]. Lista vsebuje naslednje podatke: ime lastnine, ime proizvajalca/model/serijska številka, mesto označbe, številka lastnika (angl. operation ID) - to je številka, ki jo lastnik zapiše na svojo lastnino za identifikacijo v primeru kraje. Tako označena lastnina je manj privlačna za tatove, saj ima nižjo vrednost na črnem trgu in lahko pripomore k prijetju kriminalca. Če imamo sklenjeno zavarovanje v primeru vloma moramo pri prijavi škode posredovati seznam odnešenih stvari, ki vključuje (navedbo posameznih stvari, količino, nabavna vrednost, leto nabave, amortizacijo in dejansko vrednost v EUR). Hramba liste z vredno lastnino nam celoten proces poenostavi.

Naša ideja je, da bi razširili spletno/mobilno aplikacijo in dodali novo funkcijo, ki omogoča kreiranje liste z lastnino, ki je varno shranjena in njena vsebina šifrirana. Za dostop do liste bi uporabnik potreboval enak dostop kot ga ima za prijavo v trenutno aplikacijo. Izdelava take aplikacije se nam zdi smiselna predvsem iz praktičnega in varnostnega vidika, saj uporabnikom na enostaven in varen način omogočimo kreiranje in hranjenje liste z lastnino. Poleg vseh prej omenjenih podatkov bi dodali še možnost dodajanja fotografij in avtomatsko dodajanje datuma sprememb. Taka lista z vredno lastnino nam pomaga tudi pri dokazovanju matrialne škode pri zavarovalnicah. Morda je rešitev hranjenja take liste najbolj elegantna s pomočjo

tehnologije veriženja blokov (angl. block chain), vendar je obravnavanje in analiza omenjene rešitve izven obsega naše diplomske naloge.

Pametna Varna Soseska

Do leta 2020 bo v Evropi in ZDA 91 milijonov pametnih domov [22]. Naša ideja je, da funkcionalnost Varne soseske razširimo s funkcionalnostjo pametnih domov in tako dobljeno rešitev poimenujemo Pametna Varna Soseska, krajše PVS. Posamezni objekti bi imeli vso trenutno funkcionalnost pametnih domov, npr. razsvetljava, energetika, senčila, varnost (poplava, požar, plin), zaklep vrat itd. Poleg teh bi imeli vse funkcionalnosti projekta VS. Nov projekt PVS bi omogočal medsosedsko komunikacijo in pomoč ob različnih negativnih dogodkih npr. požar, poplava, vlom, teroristični napad itd. V PVS sodijo tudi pametna parkirišča, ki bi sporočala prebivalcem o trenutni zasedenosti in o morebitnih nedovoljenih parkiranjih na njihovih parkiriščih. Potreba po PVS vsekakor je, funkcionalnosti in "pamet" se lahko glede na potrebe posamezne soseske dodaja ali odvzema.

6.3 Deljenje skrivnosti

Nadgradnja s konceptom deljenje skrivnosti spada v področje kriptografije in je namenjena povečanju varnosti projekta VS. Najprej si bomo ogledali dva primera v katerih so prikazane ranljivosti našega sistema in potreba po izboljšavi.

Primer 2. Ljudje v bežigrajski soseski živijo več stanovanjskih blokih. V enem izmed blokov v tej stanovanjski soseski so se na zboru stanovalcev odločili za našo varnostno rešitev. Vendar se kmalu pojavi težava z zaupanjem. Nekateri ljudje se med seboj dobro poznajo, vendar se številni prebivalci tudi pogosto menjajo in težko bi rekli, da v splošnem večina ljudi resnično zaupa novim posameznikom. Stanovalcem zato ponudimo dodatno razširitev varnostnega sistema (nadgradnjo, ki jo opisujemo v tem podpoglavju), ki omogoča, da sistema en sam pooblaščen stanovalec, ne more

izključiti brez drugih dveh pooblaščenih sosedov. Vsi stanovalci dobijo pametno kartico, ki je zaščitena s prstnim odtisom in geslom, na njej se namreč nahaja pomembna "skrivnost", del pooblastila. Če se sproži alarm, so stanovalci pooblaščeni da ga lahko izklopijo tako, da se zberejo poljubni trije pooblaščeni sosedje, ki svojo pametno kartico prislonijo na čitalnik. Ta iz posameznih deležev skrivnosti izračuna ključ s katerim se lahko alarm izklopi. Edini osebi, ki lahko alarm samostojno izklopita, sta lastnik stanovanja in morda še hišnik stanovanjskega bloka. ◊

Primer 3. Sosedje v Gorenji vasi, so med sabo res dobro povezani in se poznajo že celo življenje. Drug drugemu resnično zaupajo. Vomilca X in Y poznata delovanje varnostnega sistema in imata idejo, na katero nihče od uporabnikov VS ni niti pomslil. Najprej morata ugotoviti, v kakšnih odnosih so sosedje in kdo komu zaupa. Po nekaj dnevnem opazovanju soseske, je to hitro jasno, saj imajo ljudje bolj ali manj očitne prijateljske odnose. Naslednji korak je izbira dveh najbolj primernih tarč. Ena je hiša v katero bosta vlomila, druga pa najšibkejši pooblaščeni uporabnik A, ki ima možnost izklopa alarma v izbrani hiši. Cilj enega vlomilca X je, da z grožnjo prepriča pooblaščenega soseda, da ob vlomu alarm izklopi, drugi vlomilec Y pa lahko medtem nemoteno vlomi v hišo. Preden na kraj dogodka prispe policija, sta kriminalca že pobegnila. ◊

Iz zgornjega primera 2 lahko opazimo, da kadar sosedom ne moremo popolnoma zaupati, ne želimo, da imajo omogočen samostojen nadzor nad našim varnostnim sistemom. Pomanjkanje zaupanja lahko bistveno zmanjšano, če zahtevamo, da morajo biti prisotni vsaj trije pooblaščeni sosedje, za izklop našega alarmnega sistema. Varnost celotnega sistema smo s tem ukrepom občutno izboljšali. Na drugem primeru 3 lahko vidimo, da je tudi takrat, ko si ljudje popolnoma zaupajo, koncept z deljenjem skrivnosti dobrodošla nadgradnja. V ekstremnih primerih lahko s takšnim ukrepom zaščitimo svoje najbližje pred ugrabitvijo, izsiljevanjem in nasiljem.

Realizacijo nadgradnje s konceptom deljenja skrivnosti lahko izvedemo s čitalnikom pametnih kartic, ki je del zunanje tipkovnice. Vsak uporabnik projekta VS dobi svojo pametno kartico, ki je šifrirana in zaščitena z biometričnim testom (npr. prstnim odtisom) ali geslom (npr. PIN). Na njej se nahaja del skrivnosti, ki je v resnici le neko število (podrobneje bomo delovanje opisali v naslednjem razdelku). Število potrebnih pooblaščenih uporabnikov, ki se morajo zbrati za izklop alarmnega sistema (lahko tudi drugih varnostnih akcij), lahko poljubno določamo. Število oseb je odvisno od gostote naseljenosti in želj uporabnikov. Po našem mnenju je občutek in zaupanje, ki ga nadgradnja prinese uporabnikom, ki imajo pretekle travmatične izkušnje, ki so povezane z izdajo, vlomom, ugrabitvijo itd. oz. so ti le izredno previdni, neprecenljiv. Tega jim zagotavlja dejstvo, da nas ena sama oseba ne more izdati in da so vsi pooblaščeni uporabniki veliko varnejši pred nasiljem (vlomilca iz primera 3, bi izredno težko prisilila 3 neodvisne ljudi v sodelovanje).

6.3.1 Matematično ozadje deljenja skrivnosti

V kriptografiji ne radi računamo s približnimi vrednostmi (ne moremo si predstavljati, da bi nam bankomat odvrnil, da ste PIN vpisali približno pravilno), zato si za računanje izberemo končne obsege. Uporabljali bomo obseg števil, ki je podoben tisti množici s številčnice ure ($0, 1, \ldots, 11$, kjer je $12 = 0$). Števila si lahko predstavljamo na krogu, saj smo v nekem smislu sklenili začetek in konec intervala. V tej strukturi je $7 +_{12} 8 = 7 + 8 \mod 12 = 3$, saj gredo števila okrog, kot kazalec na uri. Temu načinu računanja pravimo modularna aritmetika.

Definicija 1. Naj bo $n \geq 2$ neko naravno število. Za modularno seštevanje $+_n$ in množenje $*_n$ velja:

$$a +_n b := a + b \bmod n, \quad a *_n b := a * b \bmod n.$$

V kolobarju $\mathbb{Z}_n = (\{0, 1, \ldots, n-1\}, +_n, *_n)$, torej računamo čisto običajno, nato pa rezultat zreduciramo po modulu n. Za celi števili a in b pišemo

$a \equiv b \pmod{n}$ in rečemo, da sta kongruentna po modulu n, gre torej za neko relacijo.

Trditev 1. Naj bo polinom $p(x) = \sum_{i=1}^{n} p_i x^i$ stopnje n. Če je $p(\alpha) = 0$ za nek $\alpha \in \mathbb{R}$, potem je $p(x) = (x - \alpha)q(x)$, kjer je $q(x)$ polinom stopnje $n - 1$.

Dokaz: $p(x) = p(x) - p(\alpha) = \sum_{i=1}^{n} p_1(x^i - \alpha^i)$. Izraz $x^i - \alpha^i$ lahko razstavimo in izpostavimo člen $(x - \alpha)$:

$$x^i - a^i = (x - \alpha)(x^{i-1} + \alpha x^{i-2} + \cdots + \alpha^{i-2}x + \alpha^{i-1}) \quad (1 \leq i \leq n).$$

Sledi, da je naša trditev resnična. □

Zdaj bomo definirali še shemo za deljenje skrivnosti.

6.3.2 Shema za deljenje skrivnosti

Definicija 2. Naj velja, da sta $n, t \in \mathbb{N}$, $2 \leq t \leq n$ in naj bo k skrivnost (npr. ključ), ki jo želimo nekako razdeliti med n oseb. Če velja:

1. skrivnost k lahko iz svojih deležev ključa izračuna poljubna skupina oseb velikosti t,
2. skupina z manj kot t osebami ne more izračunati nobene informacije o skrivnosti k, kljub temu, da imajo svoje deleže,

rečemo, da gre za **$(\mathbf{t}, \mathbf{n})$-stopenjsko shemo za deljenje skrivnosti**.

Želimo poiskati takšno shemo, za katero bo veljala **popolna varnost**. Opredelimo ta pojem najprej za simetrično šifro.

Definicija 3. Naj bo M množica čistopisov, C množica tajnopisov in K množica ključev. Velja, da je $E : M \times K \to C$, kjer je E šifrirna funkcija (enkripcija). S ključem $k \in K$ zašifriramo sporočilo $m \in M$ v šifrirano besedilo $c \in C$, tj. na kratko $E_k(m) = c$. Simetrična šifra z množico ključev

K in množico tajnopisov C je **popolno varna**, če za vsako porazdelitev ključev K, vsak $k \in K$ in $c \in C$, ki se pojavi z verjetnostjo $P(C = c) > 0$, drži:

$$P(K = k \mid C = c) = P(K = k).$$

Za deljenje skrivnosti bomo uporabili shemo, ki sta jo leta 1979 neodvisno odkrila **Berkley** in **Shamir**. V grobem je ključna ideje $(2, n)$–stopenjske sheme, da za določitev premice (skrivnosti) zadostujeta vsaj dve točki te premice, ki predstavljata deleža vsake osebe. To si lahko tudi sami intuitivno predstavljamo, saj vemo, da lahko skozi eno točko potegnemo "neskončno" število različnih premic[1], skozi dve točki, pa gre natanko ena premica. V primeru $(3, n)$–stopenjske sheme premico zamenjamo s parabolo. Iz primerov, za $t = 2$ in $t = 3$, je razviden "vzorec", za katerega velja, da za določitev krivulje stopnje $t - 1$, potrebujemo vsaj t točk, skozi katere gre iskana krivulja.

Preden podamo algoritem za iskano shemo, vpeljemo interpolacijski polinom za poljubno množico točk $\{T_i(x_i, y_i)\}_{i=1}^{t}$, stopnje $t - 1$, ki je ključen za razumevanje predlagane sheme.

Definicija 4. Interpolacijski polinom definiramo s polinomi:

$$p_i(x) = (x - x_1)(x - x_2) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_t),$$

tj. produkt faktorjev $(x - x_j)$ za $j \neq i$, z naslednjo formulo:

$$p(x) = y_1 \frac{p_1(x)}{p_1(x_1)} + \cdots + y_t \frac{p_t(x)}{p_t(x_t)}. \tag{6.1}$$

Trditev 2. Vse točke $T_i(x_i, y_i) \quad (1 \leq i \leq t)$, ležijo na grafu funkcije $y = p(x)$, tj. na interpolacijskem polinomu.

Dokaz: V polinom, ki ga predstavimo nekoliko bolj nazorno:

$$p(x) = y_1 \frac{(x - x_2)(x - x_3) \cdots (x - x_t)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_t)} + y_2 \frac{(x - x_1)(x - x_3) \cdots (x - x_t)}{(x_2 - x_1)(x_2 - x_3) \cdots (x_2 - x_t)} + \cdots +$$

[1] V resnici jih je, ko delamo v $\mathbb{Z}_l$, le končno mnogo, glej sliko 6.1, vendar preveč, da bi lahko preverili vse možnosti.

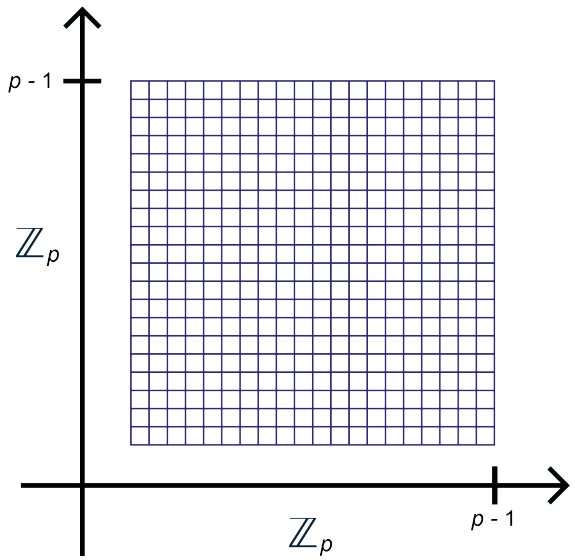
$$+y_t \frac{(x-x_1)(x-x_2)\cdots(x-x_t)}{(x_t-x_1)(x_t-x_2)\cdots(x_t-x_{t-1})}$$

vstavimo vrednost x_i $(1 \leq i \leq t)$. Ugotovimo, da imajo vsi ulomki, razen enega, en faktor 0 in posledično vrednost 0. Ulomek $p_i(x)/p_i(x_i)$ zavzame po vstavljanju $x = x_i$ vrednost 1. Torej je res,

$$p(x_i) = y_i \qquad (1 \leq i \leq t).$$

□

Algoritem 1. Za dan $n \in \mathbb{N}$ izberimo dovolj veliko praštevilo p (glej sliko 6.1), tako da velja $p \geq n+1$. Skrivnost $k \in \mathbb{Z}_p$. Naj bo $\mathcal{P} = \{P_1, \ldots, P_n\}$ množica oseb. Neodvisen delivec D, tj. $D \notin \mathcal{P}$, izbere natanko n različnih elementov $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p \backslash \{0\}$ in osebi P_i dodeli x_i $(1 \leq i \leq n)$.



Slika 6.1: Prikazan je primer množice v kateri računamo. Pomembno je, da je p dovolj velik, npr. 2^{80}.

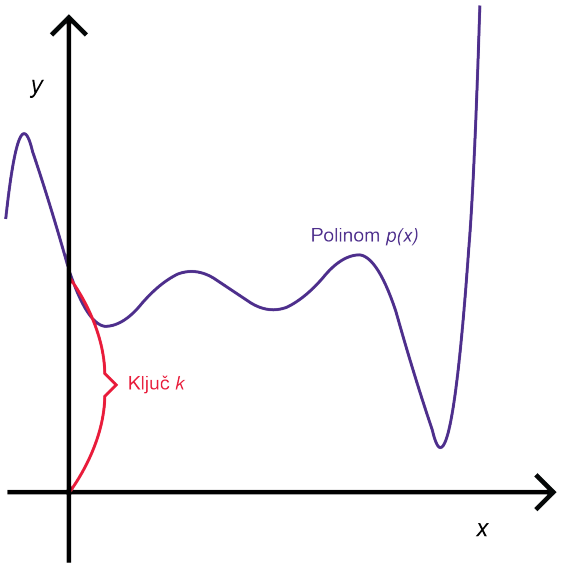
Nato izbire naključno $t-1$ elementov $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$, izračuna:

$$y_i := a(x_i) \qquad (1 \leq i \leq n),$$

kjer je

$$a(x) = k + a_1 x + \cdots + a_{t-1} x^{t-1} \tag{6.2}$$

in vrednost y_i izroči osebi P_i. Opozorimo, da v resnici ključ ni dejansko sam polinom, pač pa je $k = a(0)$, tj. ključ je y-koordinata točke, ki predstavlja presek y-osi in grafa polinoma $a(x)$, glej sliko 6.2.



Slika 6.2: Grafični prikaz ključa na grafu polinoma $p(x)$.

Trditev 3. V (t, n)–shemi za deljenje skrivnosti (algoritem 1) lahko ključ k izračuna poljubna množica oseb velikosti t. Z drugimi besedami, v algoritmu 1 smo definirali shemo, ki ima lastnost 1 iz definicije 2.

Dokaz: Predpostavimo, da gre za osebe $P_1, \ldots, P_t$. Naj bo $p(x)$ interpolacijski polinom za točke $T_1, \ldots, T_t$, glej definicijo 4. Iz definicije 6.2 y_i velja $a(x_i) = y_i$. Po trditvi 2 velja $y_i = p(x_i)$. Polinoma stopnje $t - 1$, ki se ujemata v t točkah sta enaka po trditvi 1, torej je $p(x) = a(x)$ in je zato $k = a(0) = p(0)$.

Polinoma stopnje $t - 1$, ki se ujemata v t točkah (kar je očitno iz $a(x_i) = y_i = p(x_i)$ — slednji enačaj velja po trditvi 2, prvi pa iz definicije y_i), sta

dejansko enaka, torej je $p(x) = a(x)$ in je zato $k = a(0) = p(0)$. □

Opomba: ključ torej izračunamo kot linearno kombinacijo delov y_i.

$$k = b_1 y_1 + b_2 y_2 + \cdots + b_t y_t,$$

kjer koeficiente $b_i \quad (1 \leq i \leq t)$ izračunamo z $b_i = p_i(0)/p_i(x_i)$.

Trditev 4. Berkley-Shamirjeva (t, n)–shema za deljenje skrivnosti ima lastnost 2 iz definicije 2, tj. oseb $t - 1$ oseb ne more priti do ključa.

Dokaz: Kaj se zgodi, kadar skupina udeležencev $t - 1$ želi izračunati skrivnost k? Dobili bodo sistem $t - 1$ enačb s t neznankami. Recimo, da izberejo vrednost y_0 za ključ. Potem je $k = a(0)$. Sklepamo lahko, da za vsako predpostavljeno vrednost za skrivnost y_0, obstaja natanko določen polinom $p(x)$.

Naj bo $x_0 = 0$. Predpostavimo, da je naših $t - 1$ oseb ravno $P_1, \ldots, P_{t-1}$. Označimo s $p(x)$ interpolacijski polinom stopnje $t - 1$ za točke $\{T(x_i, y_i)\}_{i=0}^{t-1}$, tj. $p(x_i) = y_i \quad (0 \leq i \leq t - 1)$.

Vidimo lahko, da nobena vrednost skrivnosti (ključa) ne more biti izločena oz. so vsi ključi enako verjetni. Zato skupina $t - 1$ udeležencev ne more pridobiti nobene informacije o skrivnosti k. □

Poglavje 7

Podobne druge rešitve

V tem poglavju bomo opisali podobne rešitve na področju varovanja sosesk. Leta 2018 v Republiki Sloveniji rešitve kot je naša najverjetneje ni. V Sloveniji je za varovanje sosesk zadolžena le policija, ki po naseljih izvaja občasne patrulje. Varovanje domov je omejeno na posamezne objekte in je v celoti prepuščeno posameznikom, ki nosijo odgovornost, da je njihova izbrana zaščita ustrezna. Pogosto je v praksi je tudi pogodbeno fizično varovanje, ki ga izvajajo varnostne službe. V tem poglavju želimo predstaviti visoko tehnološke varnostne rešitve, ki zajemajo varnost večjih območij, sosesk, mest itd.

7.1 Tehnološka samoorganizacija

V ZDA se pojavlja trend samoorganizacije prebivalcev, ki s pomočjo kamer in spleta sodelujejo s policijo ter tako pripomorejo k zmanjšanju kriminala. Posnetke kaznivih ali sumljivih dejanj objavijo na spletu, kjer jim ostali pomagajo z indentifikacijo posameznikov. Zdaj bomo prikazali enega izmed takih primerov.

Primer 4. V članku, ki ga je objavil Chitwood leta 2016 je zapisan dogodek, ki se je zgodil v Georgiji (ZDA) [4]. Policija je objavila obvestilo na Facebook skupini "Historic District Neighborhood Watch" v katerem so za-

pisali (povzemam), da iščejo posameznika, ki je vlamljal in kradel po soseski Historic District ter prosijo člane skupine za njihovo pomoč. Poleg obvestila so pripeli posnetek iskanega moškega, ki se je potikal po dvorišču in oprezal po domovih. Policija je moškega že prej identificirala in zaslišala, vendar ga zaradi pomanjkanja dokazov niso mogli zadržati. Po objavi policije na družabnem omrežju so ljudje delili svoje posnetke z videokamer, kjer se je pokazalo, da je na vseh posnetkih isti človek. Policija je nato vlomilca lahko aretirala na podlagi deljenih videoposnetkov iz družabnega omrežja. ◊

Pomoč policiji

Ljudje so z deljenjem posnetkov policiji v veliko pomoč, kar je razvidno tudi iz prej opisanega primera 4. Težava nastopi takrat, kadar ljudje kaznivih dejanj ne prijavijo policiji. Pogosto posnetek le delijo na družabnih omrežjih ali drugih internetnih straneh. Policija brez prijave kaznivega dejanja ne more ukrepati tudi, če posnetek nekega kaznivega dejanja opazijo na spletu. V primeru 4 je prikazan pogost pojav, kadar kriminalec oropa veliko število stanovanjskih objektov na nekem območju in se nato premakne drugam. Zato je izredno pomembno, da vsaka žrtev kaznivo dejanje prijavi, saj lahko detektivi ujamejo storilca z analizo pridobljenih informacij.

7.2 Varnostni sistem NNW

Organizacijo "National Neighborhood Watch", ki je v lasti in jo vodi "National Sheriff's Organization" [24] smo omenili že v podpoglavju 2.1.1, kjer je opisan njihova organizacija sosedske straže. Na tem mestu si bomo ogledali njihov projekt, ki je od vseh, ki smo jih našli najbolj podoben našemu varnostnemu sistemu. Njihov varnostni sistem ima podobne cilje kot projekt VS, s pomočjo moderne tehnologije izboljšati varnost sosesk. V njihovem primeru tudi učinkovitejše izvajanje že obstoječih sosedskih straž. Varnostni sistem NNW za delovanje potrebuje **vozlišče** (angl. hub), ki je priklopljeno na in-

ternetni usmerjevalnik in brezžične notranje ter zunanje kamere, ki imajo senzorje gibanja. Brezžične kamere napajajo baterije in so enostavne za namestitev v uporabnikovo okolje. Kamere za prenašanje podatkov uporabljajo šifrirane radijske signale na istih frekvencah, ki jih uporablja policija in drugi reševalci. Radijska frekvenca je zanesljivejša in ima večji doseg kot tehnologija WiFi, kar smo že natančneje opisali v podpoglavju 4.1.2. Uporabniki za nadzor uporabljajo mobilno aplikacijo, ki omogoča vklop ali izklop sistema, pregled videoposnetkov in pošiljanje alarma. Ko kamere zaznajo gibanje, pošljejo kratek videoposnetek o dogajanju uporabniku na njegov pametni telefon. Uporabnik ima nato na voljo tri možne akcije:

1. odpošiljanje (angl. dipatch) - pošiljanje alarma s posnetkom v centralno postajo (angl. Central Monitoring Station) na katerega se odzove policija,

2. razorožitev (angl. disarm) - izklop varnostnega sistema in nadaljnjih opzoril,

3. zavrnitev (angl. dismiss) - arhiviranje posnetka, sistem deluje naprej brez drugih sprememb.

Uporabnik vsako opozorilo s kamer ročno filtrira, kar zmanjša potrato časa policije zaradi lažnih alarmov. Opisani varnostni sistem se od našega razlikuje v nekaj ključnih točkah:

- uporaba brezžične tehnologije,
- ni drugih senzorjev poleg kamer,
- direktna povezava s policijo,
- ni medsosedskega sodelovanja,
- zaprt sistem, brez možnosti nadgradnje.

Težav pri opisanem sistemu NNW je več. Najprej naj omenimo varnost brezžičnih sistemov in drugih problemov, ki smo jih opisali v podpoglavju 4.1.2, naslednji problem je v primeru, da uporabnik ne opazi opozorila na telefonu pravočasno, da bi lahko ukrepal. V takem primeru lahko vlomilec nemoteno oropa "varovan" objekt, saj na oknih in vratih ni dodatnih senzorjev, ki bi takoj sprožili sireno. Vseeno pa je sistem NNW pokazatelj, da potreba po takih sistemih je in da se tudi v praksi ponekod že uporabljajo.

7.3 Pametna mesta

Dotaknili se bomo še zadnjega primera, ki z našim projektom VS nima veliko skupnih točk, vendar je vseeno tesno povezan z varnostjo na večjih območjih (npr. celotna mesta). Govorimo o "pametnih" mestih, ki uporabljajo **napreden nadzorni sistem** (angl. smart city surveillance). Pametna mesta temeljijo na masivnih podatkih (angl. big data). Mesta uporabljajo **omrežne kamere** (angl. network video cameras) s senzorji, ki zbirajo raznovrstne podatke. Našteli bomo nekaj primerov uporabe takih sistemov:

1. povečana varnost,
2. spremljanje gibanja za namen zmanjšanja zastojev in gneče,
3. mikrofon za zaznavanje strelov, ki takoj samostojno o tem obvesti policijo [23],
4. mikrofon za zaznavanje hrupa,
5. merjenje kakovosti zraka,
6. merjenje UV žarkov.

7.3.1 Varnost v pametnem mestu

Oglejmo si točko 1 iz podpoglavja 7.3, saj se direktno dotika problema varnosti na večjem območju, se ukvarja tudi naš projekt VS. Ostale točke z našo

primarno idejo nimajo skupnih lastnosti in jih ne bomo natančneje obravnavali. Glavni cilj pametnih kamer je večji nadzor, ki vsaj v teoriji prinese večjo varnost na nadzorovanem območju. O'Brien v svojem članku [15] zaključi, da je potrebnih več raziskav, ki bi potrdile, da prisotnost uličnih kamer zares vpliva na zmanjšano stopnjo kriminala. Iz članka lahko ugotovimo, da prisotnost kamer izboljša občutek varnosti pri ljudeh in morda večjo negotovost pri kriminalcih. Vsekakor nadzorne kamere pripomorejo k lažji identifikaciji in priprtju zločincev v primeru kaznivih dejanj. Z razvojem umetne inteligence kamere omogočajo identifikacijo obrazov in tako v realnem času obvestijo oblasti. To predstavlja tudi veliko težav, ki jih taka tehnologija prinese. Solon v svojem članku [20] omeni napake algoritmov, ki jih je približno 15% in skrb za vdor v zasebnost. Poleg obrazov kamere omogočajo tudi prepoznavanje registrskih tablic, ki jih primerjajo s podatkovno bazo lokalnih policijskih postaj, kar omogoča lociranje vozil, ki jih išče policija. Sistemi, ki skrbijo za varnost na večjih površinah (npr. mestih, mestnih četrtih, cestah itd.) so po svetu že v uporabi. Vendar so te rešitve v večini primerov uporabne šele "post mortem", torej, ko se neko kaznivo dejanje že zgodi. V realnem času imajo pogosto le psihološki učinek, ki je odvisen od vsakega posameznika.

Poglavje 8

Zaključek

Vsako leto vlomi in druge oblike kriminala po vsem svetu prizadanejo na milijone ljudi. Tega trenutno še ne znamo popolnoma preprečiti, vendar je projekt VS pomemben korak, ki bo pripomogel k razvoju varnejših in medesbojno bolj povezanih skupnosti ljudi.

Poleg večje splošne varnosti, naš projekt pomaga k boljšemu občutku posameznikov, da se ti res lahko počutijo varneje v svojem domačem okolju. Naša varnostna rešitev uporabnikom omogoča vpogled v njihov varnostni sistem v realnem času in svojo sosesko tudi kadar so daleč od doma. Poleg večje varnosti nam projekt VS odpira nova vrata, ki omogočajo številne nadgradnje domov in okolja v katerem živimo. Nadgrajen sistem bi lahko spremenil trenutno interakcijo z našim domačim okoljem in tako pomagal izboljšati naše vsakdanje življenje ter hkrati pripomogel k manjši porabi energije in drugih dragocenih virov.

Z novo tehnologijo se pojavljajo tudi številne nove možnosti, ki jih je potrebno raziskati in preučiti v praksi. Pomembno je tudi ugotoviti kakšne posledice bi imele na življenje posameznikov, ki bi živeli v takem tehnološko naprednem prostoru.

Morda se nam zdi, da je naše okolje v katerem živimo res varno, vendar ne smemo pozabiti, da je to le iluzija, ki izgine za vedno, v trenutku, ko tudi sami postanemo žrtev.

Literatura

[1] Apple. Apple reports first quarter results. Dostopno 30. 6. 2018 na: https://www.apple.com/newsroom/2018/02/apple-reports-first-quarter-results/.

[2] M. Bellare, J. Kilian, and P. Rogaway. The security of cipher block chaining. Springer Berlin Heidelberg, 1994.

[3] D. Bečić. Varna soseska: Senzorji in centralna enota, 2018. Osnutek diplome, UL Fakulteta za računalništvo in informatiko.

[4] T. Chitwood. Dostopno 5. 8. 2018 na: http://www.govtech.com/social/Columbus-Ga-Residents-Use-Social-Media-in-Neighborhood-Crime-Prevention.html.

[5] International Data Corporation. Detachable tablets return to growth during the holiday season as slate tablet decline continues, according to idc. Dostopno 28. 6. 2018 na: https://www.idc.com/getdoc.jsp?containerId=prUS43549518m.

[6] International Data Corporation. Smartphone vendor. Dostopno: 28. 6. 2018 na: https://www.idc.com/promo/smartphone-market-share/vendor.

[7] Gainesville Police Department. Gpd neighborhood watch program. Dostopno 10. 5. 2018 na: http://www.gainesville.org/fullpanel/uploads/files/gpd-nhw-packet.pdf.

[8] Ž. V. Dragan. Varna soseska: Strežnik, 2018. Osnutek diplome, UL Fakulteta za računalništvo in informatiko.

[9] FBI. Burglary. Dostopno 4. 8. 2018 na: https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/burglary.

[10] E. Fernandes, J. Jung, and A. Prakash. Security analysis of emerging smart home applications. Objavljeno v IEEE Symposium on Security and Privacy, 2016.

[11] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry. *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press, 2017.

[12] The Journal. Do you ignore ringing burglar alarms? Dostopno 2. 6. 2018 na: http://www.thejournal.ie/most-people-ignore-burglar-alarms-666818-Nov2012/.

[13] M. Koehler and F. Wortmann. Making effective home security available to everyone-towards smart home security communities. Springer, 2014.

[14] F. P. Miller, A. F. Vandome, and J. McBrewster. *Advanced Encryption Standard*. Alpha Press, 2009.

[15] A. O'Brien. Is there empirical evidence that surveillance cameras reduce crime? Dostopno 7. 8. 2018 na: https://www.mtas.tennessee.edu/knowledgebase/there-empirical-evidence-surveillance-cameras-reduce-crime.

[16] Evropski parlament. Uredba 2016/679 evropskega parlamenta in sveta. Dostopno 11. 7. 2018 na: https://publications.europa.eu/sl/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-sl.

[17] Informacijski pooblaščenec. Smernice glede izvajanja videonadzora.

[18] M. Pšenica. Sosedska straža kot oblika varnostnega samoorganiziranja prebivalcev. 2015. Diplomsko delo, Univerza v Mariboru, Fakulteta za varnostne vede.

[19] Allianz SE. The emotional impact of burglary. Dostopno 12. 7. 2018 na: `https://www.allianz.com/en/press/news/business/insurance/`.

[20] O. Solon. Facial recognition database used by FBI is out of control, house committee hears, 2017.

[21] B. Song, H. Choi, and H. S. Lee. Surveillance tracking system using passive infrared motion sensors in wireless sensor network. Jan 2008. V knjigi *International Conference on Information Networking*.

[22] J. Svanberg. Smart homes and home automation. Dostopno 5. 8. 2018 na: `http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh4-ps.pdf`.

[23] Seattle Times The. Seattle mayor pushes for gunshot-detection system. Dostopno 4. 8. 2018 na: `https://www.seattletimes.com/seattle-news/crime/seattle-to-test-gunshot-locator-technology-in-rainier-valley-central-district/`.

[24] National Neighborhood Watch. About neighborhood watch. Dostopno 5. 5. 2018 na: `https://www.nnw.org/`.

[25] Ministrstvo za notranje zadeve. Letno poročilo o delu policije za 2017. Dostopno 10. 5. 2018 na: `https://www.policija.si/index.php/en/statistika`.

[26] Državni zbor Republike Slovenije. Zakona o nalogah in pooblastilih policije, uradni list republike slovenije. Dostopno 6. 7. 2018 na: `https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/111944`.

[27] V. Šemrov. Varna soseska: Mobilna aplikacija, 2018. Osnutek diplome, UL Fakulteta za računalništvo in informatiko.

[28] T. Špehar. Varna soseska: Mobilna aplikacija, 2018. Osnutek diplome, UL Fakulteta za računalništvo in informatiko.