Aspekti kibernetičke sigurnosti u okruženju pametnog doma

Mišević, Antonio

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

Sveučilišni prijediplomski studij Računarstvo

ASPEKTI KIBERNETIČKE SIGURNOSTI U OKRUŽENJU PAMETNOG DOMA

Završni rad

Antonio Mišević

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P: Obrazac za ocjenu završnog rada na sveučilišnom prijediplomskom studiju

Ocjena završnog rada na sveučilišnom prijediplomskom studiju

Ime i prezime pristupnika:	Antonio Mišević
Studij, smjer:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	R4541, 27.07.2020.
JMBAG:	0165086481
Mentor:	prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Aspekti kibernetičke sigurnosti u okruženju pametnog doma
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	Brojni umreženi uređaji pretvaraju dom u pametno umreženo okruženje koje poboljšava kvalitetu življenja. Kibernetička sigurnost i privatnost su u ovakvom okruženju od iznimne važnosti. Potrebno je istražiti i analizirati sigurnosne prijetnje, izazove i ranjivosti u okruženju pametnog doma, te dati pregled mogućih rješenja za prevenciju.

Datum prijedloga ocjene završnog rada od strane mentora:	18.09.2024.
Prijedlog ocjene završnog rada od strane mentora:	Izvrstan (5)
Datum potvrde ocjene završnog rada od strane Odbora:	27.09.2024.
Ocjena završnog rada nakon obrane:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije završnog rada čime je pristupnik završio sveučilišni prijediplomski studij:	29.09.2024.

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

IZJAVA O IZVORNOSTI RADA

Osijek, 29.09.2024.

Ime i prezime Pristupnika:	Antonio Mišević
Studij:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R4541, 27.07.2020.
Turnitin podudaranje [%]:	1

Ovom izjavom izjavljujem da je rad pod nazivom**: Aspekti kibernetičke sigurnosti u okruženju pametnog doma**

izrađen pod vodstvom mentora prof. 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 pristupnika:

SADRŽAJ

1. UVOD

Svoje prve korake pametni domovi prate još tokom same industrijske revolucije koja donosi razne tehnološke napretke. Time se otvara prespektiva za napredovanje domova i načine kojima se može poboljšati sam dom, njegovo upravljanje i održavanje. Postepenim nastavkom razvoja tehnologije ovaj je koncept i njegovo viđenje samo napredovao. U današnje vrijeme oslanja i na sam internet te na Internet stvari (Internet of things). Internet stvari koncept je u kojemu se uređaji povezuju na internet ili neki drugi oblik umrežavanja. Za pametne domove to uvodi mogućnost upravljanja uređajima unutar doma ili sa puno većih udaljenosti kroz uporabu mobilnih aplikacija i interneta. Kao i kod drugih tehnoloških područja napredak je dobar, ali daje nove mogućnosti za napad i poteškoće s kojima se vlasnici ovakvih domova i tehnologija mogu susresti.

Ovaj rad bavi se konceptima pametnog doma i interneta stvari te njihovom sigurnosti. Kako bi se krenulo u dubinu i aspekte sigurnosti prvo treba definirati osnovne pojmove. Sigurnost je oduvijek bila poželjna nevezano sa digitalnim svijetom. Kada je riječ o ovakvom području gdje se radi o privatnosti ljudi i njihovim domovima, potreba za sigurnost još je veća. Osim same sigurnosti, rad se bavi i nekim od oblika napada koji su mogući te neki od mogućih pristupa za prevenciju ili borbu protiv napada. Na taj način poboljšavamo uvid u problem sa svrhom prevencije ili barem smanjenja rizika od njihove pojave.

1.1 Zadatak završnog rada

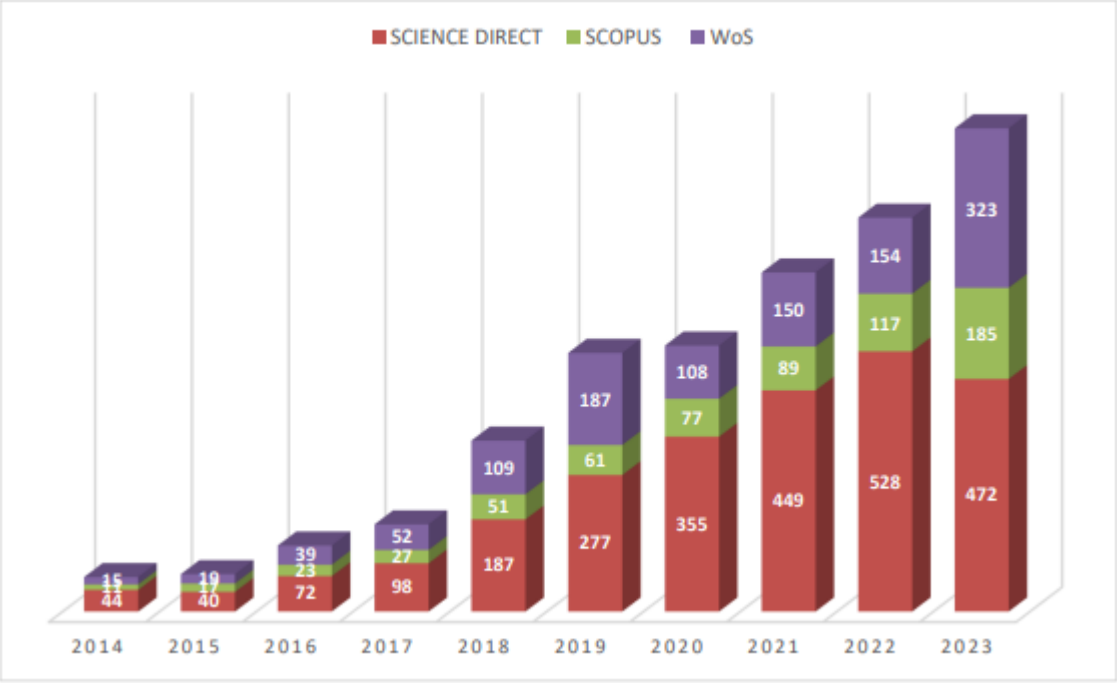
Brojni umreženi uređaji pretvaraju dom u pametno umreženo okruženje koje poboljšava kvalitetu življenja. Kibernetička sigurnost i privatnost su u ovakvom okruženju od iznimne važnosti. Potrebno je istražiti i analizirati sigurnosne prijetnje, izazove i ranjivosti u okruženju pametnog doma, te dati pregled mogućih rješenja za prevenciju.

2. INTERNET STVARI (INTERNET OF THINGS)

Internet stvari (engl. *Internet of Things, IoT)* jedan je od raširenijih termina i spada među najbrže rastuće tehnologije na svijetu te svoju primjenu ima u sve više različitih područja tehnologije i elektroničkih uređaja. Tehnologija se temelji na međusobnoj povezanosti i komunikaciji uređaja putem interneta ili neke druge mrežne strukture.

Sama ideja nastala je početkom 80-tih godina 20. stoljeća te je tokom godina imala razne napretke i počinje pronalaziti primjenu u raznim industrijama. Postepenim napretkom postaje pristupačnija, time počinje i komercijalna upotreba. Time se okoristio i sam pametni dom (engl. *Smart Home*), iako sam koncept nije obuhvaćen samo Internetom stvari i postojao je i prije.

Na temelju trendova i proučavanja razvitka u području Interneta stvari (slika 2.1). Predviđeno je da će se jedna u deset novih tehnologija oslanjati na IoT ili imati neki oblik IoT funkcionalnosti. U kontekstu pametnih domova i porasta proizvodnje senzora koji su veoma bitan faktor u pametnim domovima, u svrhu prikupljanja informacija iz samog doma. Forbes je 2014. godine objavio kako je IoT pretekao *big data* koji je također veoma bitan i aktualan segment u tehnološkom svijetu. Sve su ovo samo neki od pokazatelja uporabe i važnosti navadenih koncepata, što samo ukazuje na potrebu za adekvatnom sigurnosti.



Sl. 2.1. Graf trenda IoT istraživanja tokom proteklih godina [2]

Dodatan faktor koji je dobro uzeti u obzir je činjenica da razvoj 5G te u budućnosti 6G mreža također doprinosi samom IoT-u koji se temeljno oslanja na mreže za ostvarivanje svojih funkcija. Osim prijašnjih formata konekcije i umrežavanja IoT se tokom vremena oslanjao na različite formate uspostavljanja konekcije te se također kombinirao s raznim drugim tehnologijama kako bi se poboljšala njegova upotreba i sigurnost [2]. Neke tehnologije zajedno s kratkim opisom dane su u tablici 2.1.

Tablica 2.1. Tehnologije na koje se IoT oslanjao tokom vremena [2]

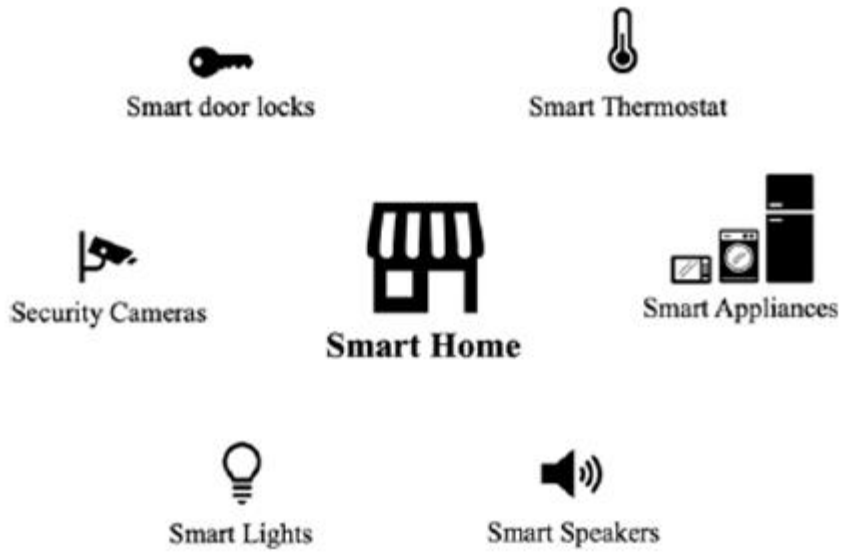
TEHNOLOGIJA	GODINA	OPIS
IDS	1986 do danas	Koristi se u strategijama kibernetičke sigurnosti. Dizajniran je za otkirvanje i reakcije na neovlaštene aktivnosti.
Wifi	1997 do danas	Automatizacija i opća upotreba
RFID	1998 do danas	Koristi radio signale za bežičnu komunikaciju među uređajima
Kvantno računarstvo	1998 do danas	Znanost o kvantnim tehnologijama proširenim na internet stvari
ZWave	1999 do danas	Automatizacija pametnog doma
Zigbee	2003 do danas	Niska potrošnja energije i podataka, kratki bežični domet
WSN/6LoWPAN	2005 do danas	Koristi AES-128 sigurnost sloja povezivanja definiranim u IEEE 802.15.4
CPS	2006 do danas	Integrira računalne procese u tehnologije interneta stvari
Blockchain	2008 do danas	Kombiniran s internetom stvari za neizmjenjivost, transparentnost i decentraliziranost
Računarstvo oblaka	2010 do danas	Sprema i analizira veliku količinu podataka generiranih od uređaja u oblak
Bluetooth 4.0LE	2010 do danas	Energetski efikasna komunikacija
NFC	2011 do danas	Komunikacija bez kontakta na kratke udaljenosti
SDN	2011 do danas	Komunikacija u mrežama s fleksibilnosti, programibilnosti i središnjim vodstvom
Bluetooth	2016 do danas	Bežična komunikacija unutar mogućeg dometa

Do sada je pažnja uglavnom bila na samoj tehnologiji i važnosti njezine sigurnosti, osim toga bitno je napomenuti kako komercijalizacija ovih uređaja ima bitan ekonomski značaj.

3. PAMETNI DOM (SMART HOME)

Uz oslonac koji pruža tehnologija Interneta stvari te njegovo konstantno poboljšanje i napredak sve je istaknutija pojava pametnih okruženja, konkretnije pametnih domova. Pod terminom pametni dom misli se na kućanstvo ili okruženje koje se oslanja na pametne uređaje i sustave automatizacije sa svrhom poboljšanja i olakšanja života i životnih uvjeta [3].

Pametni domovi nisu oduvijek obuhvaćali umreženost samih uređaja koji se koriste (npr. termostat može regulirati temepraturu doma na temelju praćenja trenutne temperature, zadane željene temperature i po potrebi željenog trajanja), međutim u današnje vrijeme umreženost i „pamet“ doma veoma su usko povezani i često idu jedno s drugim. Kao i u primjeru termostata koji se ne oslanja na povezivanje u neki oblik sustava ili mreže. Svejedno se oslanja na jedan od najbitnijih elemenata pametnog doma, a to su senzori. Senzor omogućuje praćanje neke vanjske informacije i kao rezultat ima neki oblik reakcije ili baratanja informacijom. Složenost i količina senzora daje raznolike mogućnosti kako se pametni uređaji mogu koristiti. S obzirom da je u današnje vrijeme veoma prisutno i strojno učenje, veliki broj podataka koje senzori prikupljaju daje mogućnost modeliranja navika korisnika unutar kućanstva te time još bolju optimizaciju i automatizaciju samog okruženja tj. doma. [4]



Sl. 3.1. Tipovi uređaja koji se nalaze unutar pametnog doma [4]

Pet kategorija uređaja koji zastupaju pametni dom (slika 3.1) :

1) Sigurnost – pod sigurnost se misli na sami dom. Uglavnom se radi o kamerama, senzorima, alarmima i drugim oblicima osiguravanja okruženja.

2) Regulacija temperature – razni oblici regulacije temperature: ako se radi o što manjem ljudskom sudjelovanju riječ je o modelima strojnog učenja koji „pamte“ navike ili pod utjecajem korisnika putem aplikacija ili nekih drugih sučelja. Važan aspekt ove kategorije je i samo očuvanje energije koje se postiže izučavanjem korisničkih navika što nije bilo prisutno kod običnih termostata.

3) Osvjetljenje – kako i sama kategorija kaže radi se o samo osvjetljenju prostora, ali i ova kategorija ima mogućih kompleksnosti i proširenja. Uz razne moguće metode i načine reguliranja, mogući su i razni oblici osvjetljenja, u ovisnosti o tome koje je doba dana, aktivnosti kojima se korisnik bavi i slično.

4) Kućanski uređaji – svi dosadašnji uređaji unutar doma na ovaj način dobivaju dodatne funkcije i poboljšanja. Jedan od prvih uređaja u ovoj domeni bio je hladnjak s mogućnosti obavještavanja stanovnika kada su namjernice pri kraju. Aspekt koji dodatno ističe samu „pamet“ je umrežavanje uređaja i uporaba nekog od pomoćnih alata (npr. Alexa kompanije Amazon). Pomoćni alati dodatno olakšavaju posao, moguće je baratanje većim brojem uređaja preko jednog sučelja. Kod Alexe radi se o kontroli pomoću govora.

5) Zabava – Televizori, sustavi za ozvučenje te ostali oblici zabave unutar doma također dobivaju proširenje i lakši pristup i baratanje sadržajima.

Termin koji se još povremeno koristi u ovom kontekstu je sustav sustava (engl. *System of systems*). Uglavnom se odnosi na umrežavanje manjeg, užeg sustava u cijelokupni, obuhvatniji sustav okruženja. Razlog tome je još bolja sistematizacija uređaja i olakšavanje njihovim baratanjem [4].

Mogućnost očuvanja energije koja je napomenuta pod kategorijom Regulacije temperature veoma je bitan i tražen segment pametnih domova. Veliku važnost ima i ekološki aspekt doma u smislu da je dom pogodan i korista za okolinu ili da joj barem ne nanosi dodatnu štetu. Osim ova dva tremina bitna je i ekonomičnost koji je jedan od vodiča za razvoj ovakvih okruženja, sam termin nalaže što bolji sustav koji obavlja neku funkciju što je efikasnije moguće [3].

4. SIGURNOST PAMETNOG DOMA

Kao i u svakoj drugoj tehnološkoj domeni i u kontekstu pametnog doma njegovih uređaja veoma je bitna sigurnost. Sigurnost u ovom kontekstu ima dodatno veliki značaj i važnost upravo iz razloga što se radi o domovima koji su i dalje glavni oblik privatnosti koju svaki pojedinac želi i treba. Međutim kao i u drugim područjima napadi su ponekad neizbježni te uvijek prate i sam razvitak i napredak uređaja kao i metoda koje su povezane uz njih.

Jedan od problema koji se nameće je kako bi osobe koje nisu adekvatno informirane u ovome području trebale donijeti informirane odluke pri odabiru uređaja koje će kupiti i koristiti u svom domu, iako postoji osnovna razina sigurnosti koju svaki uređaj mora garantirati. Jedan od pristupa bavi se tom tematikom te se kao osnovna metoda za donošenje odluka zasnovanih na više različitih kriterija nameće *Analytic Hierarchy Process* (AHP) [5]. Metoda se koristi za donošenje odluka kod kojih je prisutna hierarhija prioriteta. U našem konkretnom primjeru radi se o sigurnosnim aspektima koje želimo da naš uređaj obuhvaća. Navedena metoda prikazuje rezultat koji mogu shvatiti čak i ljudi koji nisu znalci o područjima koje uređaj obuhvaća.

4.1 Područja napada uređaja

Temeljni aspekti svakog uređaja unutar pametnog doma mogu se podijeliti u četiri kategorije: sam uređaj, mreža koja se koristi, *cloud* i aplikacija.

1. Uređaj – odnosi se na konkretne fizičke uređaje te direktne napade na njih i slabosti kod njihove realizacije i upotrebe

2. Mreža – odnosi se na protokole i metode koji se koriste za umrežavanje

3. *Cloud* – dio uređaja može se oslanjati na *cloud* tehnologije u svrhu skladištenja informacij i događaja vezanih uz sam uređaj

4. Aplikacije – aplikacije koje se koriste za udaljeno baratanje i kontrolu uređaja

Količina radova za svako područje nalazi se u tablici 4.1.

Svako od navedenih područja napada ima svoje specifične probleme i napade vezane uz njihovu realizaciju i strukturu, ali naravno niti jedan od njih nije manje vrijedan ili bitan. Kada je u pitanju sigurnost i privatnost ne bi trebalo biti mjesta za kompromis.

Tablica 4.1. Prikaz radova za svaku od kategorija u svrhu boljeg uvida kojim područjima se pridaje veća količina pažnje [5]

Područje	Digitalna biblioteka	Broj objavljenih radova
Sigurnost uređaja	IEEE Xplore Science Direct Engineering Village ACM Digital Library	652 5465 840 1965
Mrežna sigurnost	IEEE Xplore Science Direct Engineering Village ACM Digital Library	627 6585 1081 3021
Sigurnost oblaka	IEEE Xplore Science Direct Engineering Village ACM Digital Library	179 2686 280 1454
Sigurnost aplikacija	IEEE Xplore Science Direct Engineering Village ACM Digital Library	136 3787 215 4686

Na početku ovog poglavlja (4.1) spomenuta je sigurnost pametnog doma kao i područja na osnovu kojih se onda granaju kategorije napada, bitno je napomenuti kako je ta podjela više bazirana iz perspektive interneta stvari te iako je internet stvari usko povezan sa pametnim domovima oni nisu jedno te isto. Naime u drugim literaturama moguće je pronaći drugačiju kategorizaciju i imenovanje područja koja mogu biti mete. Recimo u [6] se u jednom od odlomaka govori upravo o tome: kroz prizmu Pametni kućni sustavi (engl. *Smart Home Systems*, SHS) što je zapravo još jedan od termina za pametne domove. U današnje vrijeme zbog raznolikosti i količine pametnih uređaja koji se koriste, mogu biti promatrani kao sustav. U kontekstu SHS-a sigurnosne prijetnje granaju se u 3 kategorije: fizička ili perceptivna, mrežna i aplikacijska. Za razliku od prijašnje kategorizacije vidljivo je da *cloud* nije naveden. Razlog tome je što *cloud* sam po sebi nije nužan dodatak svakom uređaju, a osim toga *cloud* je sam po sebi također veliki tehnološki segment koji također raste samostalno tako da sigurnost i napredak u tom području samo prenosi i na pametne uređaje.

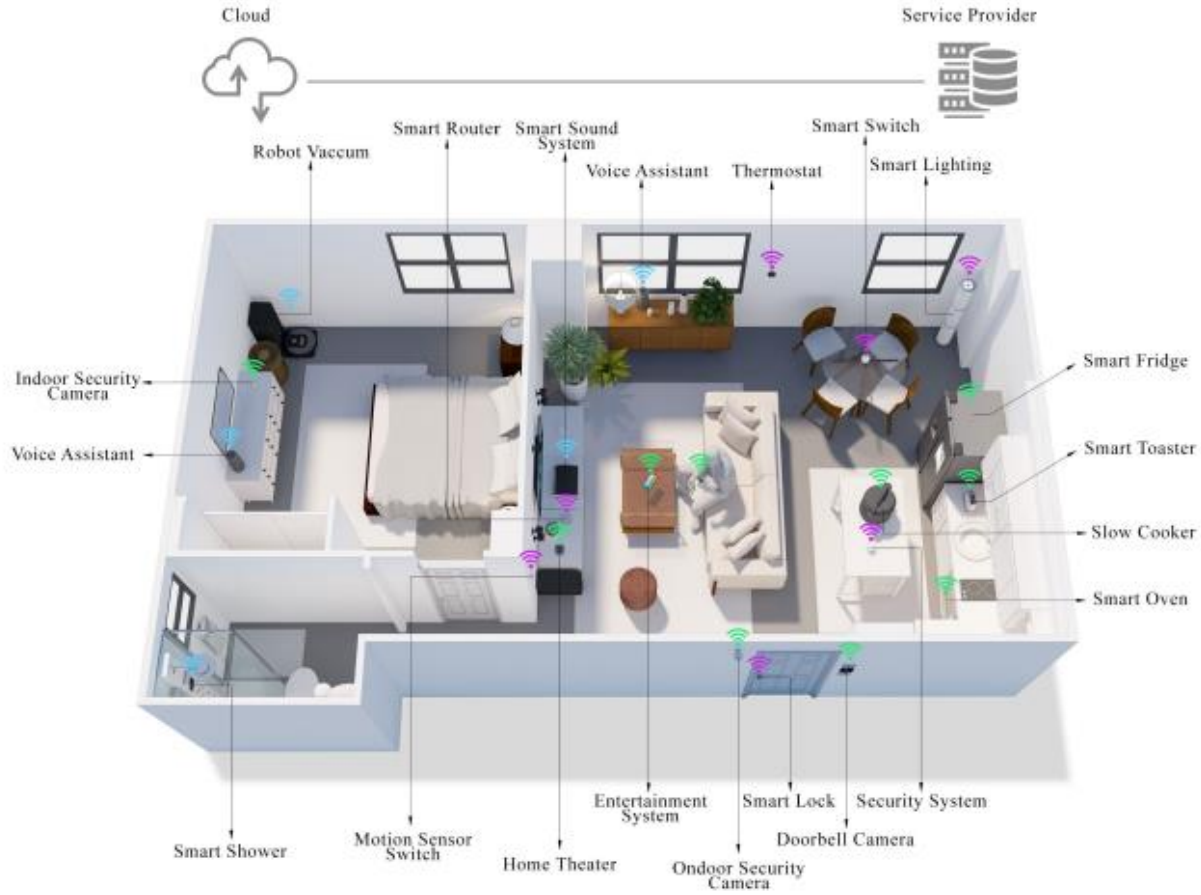
4.2 Moguće vrste i oblici napada

Poglavlje 4.1 govori o samim metama na koje napadi mogu ciljati. Ovaj segment baviti će se napadima direktno: koji su generalni pristupi koji se koriste za napade, koje konkretne metode i tehnologije se koriste za realizaciju napada. U kontekstu načina na koji se napadi realiziraju moguće ih je podijeliti u četiri kategorije: ignoriranje, smanjenje, zlouporaba i proširenje. Osim ove četiri kategorije bitno je napomenuti kako postoje i neke specifične metode koje se koriste samo u kombinaciji sa nekim specifičnim uređajima, zbog moguće specifičnosti funkcije ili načina na koji se ti uređaji realiziraju. Prva tri tipa napada uvelike su bazirana na samom uređaju i njegovim već postojećim funkcijama, dok četvrti – proširenje kako i naziv nalaže proširuje mogućnosti samog uređaja sa svrhom nanošenja dodatne štete. Prijašnja kategorizacija gleda više iz perspektive samog napada i kako napad koristi ometeni uređaj. S druge strane [7] kategorizira napad ne temelju sigurnosnog aspekta koji se pokušava narušiti te se po tom kriteriju napadi dijele na: izmišljanje (engl. *fabrication*) koja cilja na autentikaciju, presretanje (engl. *interception*) za povjerljivost, izmjene (engl. *modification*) za integritet, prekidanje (engl. *interruption*) za dostupnost. Također su moguće kombinacije ovih kategorija, drugim riječima napadi koji ciljaju na više od samo jednog aspekta sigurnosti. Aspekte sigurnosti kao i konkretne tehnike napada i slabosti koje napadi koriste za realizaciju obuhvatiti će poglavlje 5.

5. SLABOSTI I NAPADI

Poglavlje 4 ukazalo je na postojanje različitih područja pametnog doma te njegovih uređaja baziranih na internetu stvari koji mogu biti meta napada. Ovo poglavlje baviti će se svakim od navedenih područja, navesti neke od primjera i meta koje se koriste za raznolike oblike napad te ih objasniti kako u generalnom smislu tako i konkretnije u samom kontekstu pametnog doma.

Uz same tehnološke i sigurnosne slabosti koje uređaj posjeduje jedan od faktora koji utječe na napade je sama činjenica kako se proizvođači takvih uređaja razlikuju pa time i njihova kvaliteta, koje se tehnologije i protokoli koriste. Raznolikosti u protokolima umrežavanja (slika 5.1)



Sl 5.1. Prikaz raznolikosti u načinima umrežavanja koje uređaji koriste [5]

Ljubičasta – ZigBee, Plava – Bluetooth i Zelena – Wi-Fi

Kao i u svim ostalim područjima kibernetičke sigurnosti poznati su te veoma važni osnovni koncepti i očekivanja, ima ih 7 a oni su:

1) Autentikacija (engl. *authentication*) mehanizam koji omogućuje potvrđivanje izvora neke informacije u smislu da je poznat izvor informacije kako bi znali da je pouzdan

2) Autorizacija (engl. *authorization*) ovaj koncept se odnosi na ovlasti koje svaki korisnik ima za izvršavanje nekih akcija

3) Povjerljivost (engl. *confidentiality*) podrazumijeva da će pristup informacijama kao i činjenica kojim osobama one pripadaju tj. koji je njihov izvor biti zaštićene i ograničenog pristupa

4) Integritet (engl. *integrity*) podrazumijeva da informacije neće promijeniti svoj sadržaj u procesu prijenosa ili rukovanja

5) Odgovornost (engl. *accountability*) obuhvaća mehanizam za određivanje vršitelja/izvora neke radnje u sustavu kako bi se uvijek znalo tko je odgovoran za izmjene ili radnju

6) Dostupnost (engl. *availability*) odnosi se na samu dostupnost sustava ili uređaja te koliko je on zapravo na raspolaganju svojim korisnicima

7) Neporecivost (engl. *non-repudiation*) omogućuje da izvor neke poruke ili informacije u sustavu bude poznat te da korisnici ne mogu odbiti prijem poruka

Svaki od ovih sedam kocepata ima svoj oblik slabosti i meta za napad u kontekstu pametnog doma, ali naravno neki od njih su u većoj opasnosti i rizičniji su kao meta napada nego ostali. U kontekstu opasnosti ističe par raznih izvora koji iskazuju svoje viđenje kritičnih područja u kontekstu pametnog doma [4]. Konačni zaključak kao rezultat daje četiri elementa: integritet, povjerljivost, autentikacija, autorizacija.

Gore navedenih sedam koncepata generalno su vezani uz kibernetičku sigurnost, osim njih kroz uporabu AHP metode pronalazi i ističe važnost i još nekih sigurnosnih aspekata koji su veoma bitni za uređaje u kontekstu interneta stvari pa time i samog pametnog doma (slika 5.2) [5].

Sl 5.2. Rezultat AHP metode važnosti sigurnosnih aspekata [5]

Vidljivo je kako ih je većina sa slike upravo neka od onih sedam te se osim toga preklapaju s istaknutim točkama rizika koje su prije navedene. Osim navedenih sedam koncepata na slici su prisutni i još neki koji su važni za područje kojim se rad bavi.

Pristup (engl. *Access*) slično kao i prošli odnosi se na pristup informacijama, ali ovaj aspekt se više odnosi na korisničku perspektivu i njihov pristup, a ne organizaciju sustava i informacija.

Fizička kontrola (engl. *Physical control*) vezana je uz našu temu i Internet stvari, a odnosi se na uređaje koji se koriste za sigurnost u stvarnom svijetu (npr. kamere, senzori i slično)

Ovaj odlomak objasnit će načine na koje se napadi mogu realizirati te neke od učestalih načina napada koji se koriste kao i njihova objašnjenja. Poglavlje 6 baviti će se konkretnim napadima za svako od prije navedenih područja, uz svaki napad navesti će se predloženi oblici borbe ili prevencije navedenog napada.

Tehnike i tehnologije koje se koriste su:

Napad sporednim kanalom (engl. *Side-channel attack*) – sami po sebi ovakvi tipovi napada koriste se informacijama od strane samih uređaja te na osnovu njih dobivaju sve što je potrebno za napad.

Fizički napad (engl. *Physical/hardware attack*) – oslanjaju se na fizičke aspekte uređaja za realizaciju napada. Neke verzije napada sporednim kanalom također se oslanjaju na ovaj tip napada iako je kod njih više naglasak na podatke, dok ovi tipovi napada ciljaju na sam uređaj i njegovu strukturu.

Društveni inžinjering (engl. *Social engineering*) – ova metode se ne oslanja direktno na tehnologije i uređaje. Zasniva se na zlouporabi ljudske psihologije kako bi naveli korisnika da vam omogući pristup važnim informacijama ili omogući instalaciju zlonamjernih programa.

Pretvaranje (engl. *Spoofing attack*) jedna je od metoda napada koja bi se mogla svrstati unutar ovog područja, korisnika se zavarava na načine da se napadač pretvara da je ovlaštena osoba te na taj način dobiva pristup važnim informacijama.

Energetski napadi (engl. *Energy attacks*) – koriste analizu energije ili neki drugi oblik napada te neovlaštenim pristupom uređaju. U kontekstu pametnog doma i IoT uređaja istaknuti su napadi sa svrhom krađe energije, pogotovo kada se radi o pasvinim uređajima s kojima korisnici nemaju učestalu interakciju te je tako manja šansa da uoče odstupanja.

Korisnički podatci i napadi privatnosti (engl. *User-credentials and privacy attacks*) – meta ovakvih napada su korisničke informacije za pristup računima i informacijama vezanim uz privatnost korisnika. Slabosti i greške sigurnosnih protokola mogu pomoći za pristup informacijama o uređaju korisnika sa svrhom probijanja lozinke.

Analiza prometa (engl. *Traffic analysis*) – koristi se analizom mrežnog prometa za identifikaciju uređaja i njihovih stanja kako bi se dobile informacije o privatnosti korisnika.

Uskraćivanje usluge (engl. *Denial of Service, DoS*) jedan je od čestih tipova napada koji je zasnovan upravo na mrežnom prometu, u kontekstu pametnog doma preuzeti uređaj se može se koristiti za distribuirano uskraćivanje usluge (engl. *Distributes Denial of Service, DDoS*)

Napadi zbunjivanja strojnog učenja (engl. *Adversarial Machine Learning, AML*) – u današnje vrijeme strojno učenje (engl. *Machine learning, ML*) koristi se u sustavima za otkrivanje neovlaštenog pristupa (engl. *Intrusion Detection System, IDS*), strojno učenje koristi se za kreiranje modela koji izučavaju korisničke navike i ponašanja u sustavu te se na temelju odstupanja prepoznaje da se radi o neovlaštenom korisniku. Meta ovog tipa napada su modeli strojnog učenja koji se koriste za uočavanje odstupanja od normalnog ponašanja. Napad se realizira unosima i pristupima koji onda postepeno ublažavaju reakcije i kriterije modela i daju mogućnost za lakši pristup.

Osim ovih gore navedenih tehnologija postoje još neki tipovi unutrašnjih napada gdje se dobiva pristup uređaju u sklopu pametnog doma i na osnovu toga započinje napade iznutra. Još jedan tip napada je Posrednički napad (engl. *Man-in-the-middle attack*) gdje osoba promatra komunikaciju među uređajima u svrhu dobivanja bitnih ili korisnih informacija.

Uz sve gore navedene metode i tehnologije bitno je napomenuti kako se veliki broj metoda i tehnika napada ne koristi samo jednistvenom metodom iz jedne od ovih kategorija nego je često kombinacija više različitih napada. Gornja kategorizacija bazira se na pametni dom i tehnologije na koje se on oslanja.

6. MJERE SIGURNOSTI I PREVENCIJE NAPADA

Ovo poglavlje bavi se konkretnim primjerima napada koji su se pojavili. Osim toga obuhvatiti će predložene ili već implementirane ideje za borbu ili prevenciju navedenog napada. Svaki napad će također biti opisan područjem na koje cilja u kontekstu aspekata uređaja za pametni dom kao i aspekt kibernetičke sigurnosti na koji cilja.

Jedan od faktora koji se često spominje u kontekstu pametnog doma te njegovih uređaja je činjenica da ga koriste ljudi. S jedne strane korisnici imaju veću slobodu kontrole i baratanja tim uređajima, s druge strane postoji veća šansa za napadom. Prosječan čovjek nije informiran o uređajima, protokolima, sigurnosti i svim ostalim aspektima. Također ljudi mogu jedni drugima prosljeđivati uređaje i uređaj na razne načine može promijeniti vlasnika što također može biti loše. Još jedan od faktora je sama sigurnosna kompanija koja se bavi uređajem, zaštitu može preuzeti neko drugi te se dotadašnji uređaji ne poboljšavaju, nema nove podrške niti proširenja što definitivno nije poželjno. Traganje za adekvatnim rješenjem za uređaje, korisnike i njihove domove još uvijek traje. Predložene opcije su periodično testiranje takvih uređaja u svrhu ponovne evaluacije sigurnosti ili s druge strane garancija od strane prodavača uređaja da će podrška postojati u nekom određenom vremenu.

6.1 Fizički napadi

Osluškivanje (engl. *Eavesdropping*) jedan je od tipova napada na koji su uređaji slabi, u ovom napadu zlonamjerna osoba osluškuje promet koji prolazi kroz uređaj. Preuzimanje čvorova (engl. *Node capture attack*) konkretno preuzima uređaj te se koristi informacijama koje pristižu u čvor za nastavak i širenje napada na druge uređaje i potencijalno cijelu mrežu. Napadi ponavljanjem (engl. *Replay attacks*) ponavljaju poslane poruke i na osnovu tog nanose štetu obavljajuću željenu radnju više puta. Napadi uskraćivanjem sna (engl. *Sleep deprivation attacks*) ciljaju na čestu funkcionalnost uređaja da prelazi u efikasan način rada pri maloj količini zahtjeva, ovaj napad onemogućuje tu funkciju konstantnim slanjem zahtjeva u vremenskim intervalima potrebnim da uređaj nikad ne uđe u „štedljivi“ način rada. Zadnji napad može se svrstati u oblik energetskog napada, dok svi prije tog kombiniraju razne oblike napada navedene u prošlom poglavlju. Bitno je ponovo istaknuti kako napadi rijetko koriste samo jednu tehnologiju i područje za napad. Osim toga fizički uređaji pružaju samu uslugu i njihova povezanost s mrežom i svime ostalim na taj način pruža mogućnost napada sa svih strana. Jedan od tih problema leži i u samim

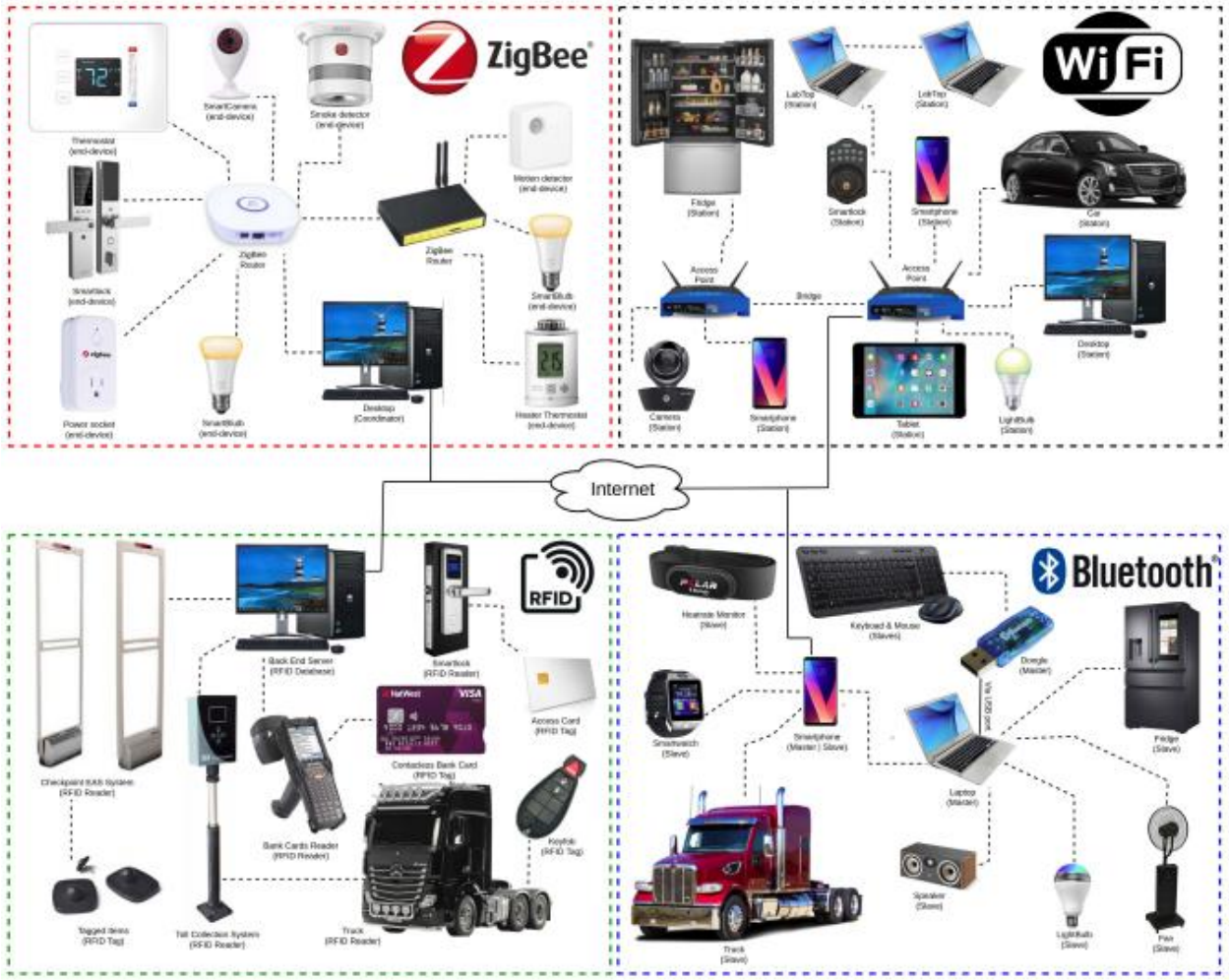
aplikacijama koje se koriste u kombinaciji s uređajem radi lakšeg pristupa i baratanja. [8] Ističe kako je jedan od glavnih razloga i problema aplikacija njihova uska povezanost i činjenica da aplikacije u startu imaju velike razine pristupa uređaju što olakšava napad. Jedan od razloga je manjak pažnje i „održavanja“ uređaja u obliku lozinki i protokola na koje se oslanja. [9] Prikazuje kako je i pomoću jednostavnog napada rječnikom (engl. *Dictionary attack*) moguće dobiti pristup uređajima zbog jednostavnih ili čak početnih lozinki. Činjenica da je uređaj povezan na mrežu također igra ulogu u njegovoj slabosti, povezanost na internet ili neki od mrežnih protokola na koje se uređaj oslanja. Kada se radi o samoj fizičkoj realizaciji uređaja postoji veliki raspon mogućih napada. U kontekstu arhitekture sistema, neki od primjear su napad na proces paljenja (engl. *Boot attack*) i ugrađeni napad *(engl. Firmware attack*), ali to su samo neki od napada.

Uz opširan spektar opasnosti i napada potrebne su adekvatne protumjere, mjere prevencije i zaštite stalno se razvijaju i predlažu jednako kao što i sami napadi napreduju. Jedan od predloženih tehnoloških okvira (engl. *framework*) : ProvThings, zasniva se na pračenju podrijetla informacija sa svrhom otkrivanja grešaka i potencijalnih napada te je treniran na skupu od 26 mogućih IoT napada [10].

Jedna od metoda pomoći u kontekstu aplikacija s prevelikim ovlastima je SmartAuth koji analizira sigurnosne pretpostavke i informacije od aplikacije i generira sučelje sa svrhom povezivanja mogućnosti koje su predstavljene korisniku i stvarnih mogućnosti aplikacije. Oslanja se na procesiranje prirodnog jezika (engl. *Natural language processing, NLP*), koje je jedno od područja umjetne inteligencije, što samo dodatno ukazuje korist koju si različita područja tehnologije mogu uzajamno pružiti [11].

6.2 Mrežni napadi

Što se tiče uređaja i njihove mrežne povezanosti jedan od već spomenutih problema je mrežna raznolikost koja je prisutna zbog raznih načina povezivanja uređaja (slika 6.1). Jedno od intuitivnih rješenja problema bilo bi stvaranje i uporaba jedinstvenog mrežnog sustava, ono naravno ne bi u potpunosti omogućilo sigurnost, a i sama realizacija i kordiniran prijelaz je teško izvediv. U kontekstu povezivanja ne internet potrebno je obratiti pažnju i na same usmjerivače s kojima se cijelo kućanstvo povezuje na internet, njegova nezaštićenost također može pružiti prilike za napad. Jedan od uočenih problema je jednostavnost lozinki, činjenica da ih korisnici rijetko mijenjaju te da i same platforme nemaju učestala poboljšanja.



Sl 6.1. Prikaz čestih uređaja i njihovih načina povezivanja na kreće relacije [12]

Temeljit prikaz i usporedbu napada baziranih na ovim metodama umrežavanja kao i predložene i moguće metode borbe i prevencije za svaku od njih već je obrađeno u jednom radu. Glavni zaključak je problematičnost protokola za autentikaciju, ponovno se ističe problem raznolikosti metoda na koje se oslanjaju kućanski uređaji što daje raznolike slabosti i mogućnosti napada. Iako je glavni utvrđeni problem autentikacija rad daje odličan uvid i ispis napada i prevencija napada za sva četiri tipa umrežavanja na području svih koncepata kibernetičke sigurnosti. Vidljiv je manjak povjerljivosti i integriteta u protokolima na koje se oslanjaju uređaji interneta stvari. Jedan od primjera toga su senzori za pokret i kamere kod kojih je uočeno da podatci koji se šalju uopće nisu enkriptirani što u potpunosti olakšava posao napadača. Takvi problemi su očigledno jasni i već sama enkripcija sadržaja poboljšala bi sigurnost. Teško je dovoljno istaknuti važnost kvalitetne zaštite i sigurnosti ovog područja, pogotovo kada su u pitanju korisnici i njihova privatnost. Navedeni primjer je savršen pokazatelj koliko prostora za napredovanje ima [12].

Prikaz kako i protokoli koji su dugo i opširno korišteni također imaju svoje probleme i slabosti. Rad predstavlja protokolni oblik napada nazvan DROWN koji daje primjer napada na TCP/IP (*Transmission Control Protocol/Internet Protocol*) zasnovan na TLS (*Transmission Layer Safety*). Napad koristi SSLv2 (*Secure Sockets Layer*) kako bi dešifrirao TLS veze. Rezultat istraživanja ukazuje kako je 26% HTTPS servera nezaštićeno od posredničkog napada i kako je SSL loš i nesiguran u kontekstu TLS-a [13].

Bitan detalj za napomenuti u ovome području je kako iako se radi o kibernetičkoj sigurnosti uređaja ona se veoma lako može pretvoriti u oblik nesigurnosti u stvarnom svijetu. Uređaj je umrežen te je meta kibernetičkog napada, ali ako napad uspije problem prelazi u stvarni svijet i kućanstvo korisnika. Jedan od primjera toga je i sam promet uređaja koji može biti pokazatelj trenutnog stanja kućanstva, ako je recimo promet uređaja malen veoma je vjerovatno da se uređaj ne koristi aktivno što preko dužeg perioda može ukazati na odsutnost ukućana i otvoriti opcija i za napade u stvarnom svijetu. Tako da sama enkripcija i kvaliteta enkripcije prometa nije dovoljna da bi se postigla opsežna privatnost.

Što se tiče borbe i prevencije na području mrežnog dijela pametnog doma i interneta stvari postoji puno prijedloga i ideja za povećanje sigurnosti. Po uzoru na dosadašnje oblike sustava za otkrivanje neovlaštenog pristupa (IDS) predložen je sličan sustav kao i u drugim područjima kibernetičke sigurnosti. Radi se o sustavu koji bi se oslanjao na strojno učenje za izučavanje i prepoznavanje odstupanja u ponašanju. Sustav bi imao dva sloja: jedan bi bio lokalni i on bi se bavio promatranjem i donošenjem odluka na lokalnoj razini, a osim njega postojao bi i globalni sustav na razini svih kućanstava koji se oslanjaju na navedenu uslugu. Što se tiče spomenutog TLS-a, jedan od prijedloga je pronalazak i kreiranje neke kompaktnije alternative, jedan od razloga tome je što je količina resursa u uređajima ograničena kao i okruženje u kojemu funkcionira naspram dosadašnjih uređaja. SecIoT jedna je od mogućih metoda borbe, ovdje se radi o okruženju koje je usmjereno prema problemima vezanim uz autentikaciju, uz mogućnost autentikacije na kvalitetan način omogućuje komunikaciju među potvrđenim korisnicima uz moguć prikaz rizika. Oslanjao bi se na Petu Generaciju (5G) i uz autentikaciju pružio bi i olakšao komunikaciju među uređajima u bilo kojem trenutku [14]. Jedano od mogućih rješenja za raznolikost načina umrežavanja u kontekstu doma što je već ranije spomenuto jedan od problema koji otvara vrata za raznolike oblike napada. Prijedlog je pristup temeljen na pravilima koji bi nove uređaje automatski pripremio i zaštitio od raznolikosti uređaja i protokola unutar interneta stvari [15].

6.3 Napadi putem aplikacije

Prijašnja poglavlja dotakla su se kako je jedan od temeljnih problema koji aplikacije pružaju u kontekstu pametnog doma i interneta stvari razina ovlasti i pristupa koju aplikacije imaju nad uređajem što iako namjenjeno lakoći i jednostavnosti uporabe vrlo lako može postati problem sigurnosti i privatnosti. Jedan rad spominje generalnu sigurnost mobilnih uređaja, ali osim toga dotiče se i već spomenute problematike koju pristup i priprema uređaja može imati na sigurnost i kako te aplikacije također pružaju platformu za napad koji je onda proširiv i na druga područja [16]. Dosad je spomenuta autentikacija i protokoli te i sama ograničenost uređaja zbog okruženja i načina rada. To je također dio problema, protokoli i konfiguracije kao i načini na koje aplikacija surađuje s ostalim aspektima tehnološki su određeni tokom godina te u slučaju novog područja s novim potrebama i mogućnostima. Problem postaje: kako novinu ususstaviti bez problema i potreba za glomaznim izmjenama. Jedan od mogućih napada gdje se imitira uređaj interneta stvari pomoću potrebnih aplikacija te prevari aplikaciju da pruži potreben podatke za pristup Wi-Fi-u kao i pristup privatnim informacijama [17]. Proširenje na problematiku neovlaštenog pristupa privatnim podatcima, utvrđeno je da većina okruženja koja se koriste za moblinu sigurnost rade na principu odobrenja za pristup podatcima, što omogućuje zlouporabu te neovlašteni pristup na temelju odobrenja [18].

Predložena rješenja imaju par pristupa iz različitih prespektiva: [19] ističe kako bi implementacija sigurnosti aplikacije, usmjerivač (engl. *router*) i pametnog uređaja tražila izmjene u nekom od tri navedena područja što bi dovelo do dodatnih troškova u bilo kojem od tri područja. HanGuard pruža rješenje bez potreba za proširenjima u prijašnja tri područja, rješenje je slično (engl. *Software Defined Network, SDN*) pristupu gdje se programski kreira mreža radi lakoće i kontrole, svaki uređaj ima aplikaciju pomoću koje se identificira te definira uređaj kojem želi pristupiti unutar pametnog doma, odluka se preusmjerava ruteru te ruter provodi pravo pristupa ne temelju odluke. Osim toga moguč je i drugačiji pristup sustavu za detekciju neovlaštenog pristupa zasnovanom na Skrivenom Markovljevom Mehanizmu (engl. *Hidden Markov Machines, HMM*), koji je ukratko jedan od modela koji statistički opisuje prijelaze iz ulaza u izlaze, na temelju dosadašnje promjene stanja, razlika naspram Markovljeva lanca je prisutnost nepoznatog faktora koji potiče izmjene stanja na način na koji se odvijaju. Kao i u drugim oblicima sustava za detekciju neovlaštenog pristupa ovaj sustav koristi navedeni statistički modela za izučavanje korisnika i njegovih navika te moguće prijelaze i promjene u ponašanjima [20].

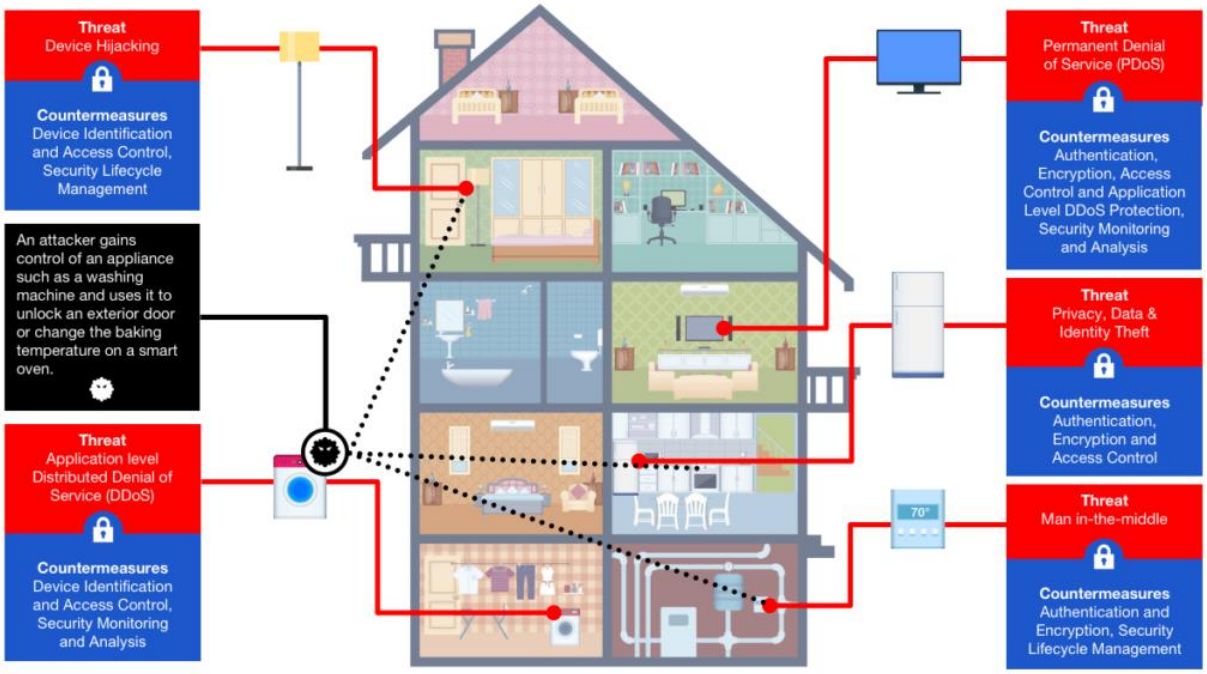
6.4 Cloud napadi

Pametni uređaji koji se nalaze u pametnom domu u zadnje vrijeme često se oslanjaju na *cloud* i njegove usluge. Iako su prednosti i privilegije koje *cloud* donosi poželjne zbog ograničenosti resursa od strane pametnih uređaja za dom, s druge strane i *cloud* otvara mogućnosti za napade preko njega. Kod oslanjanja na *cloud,* informacije veoma često putuju u dva smjera, prvo se šalju na *cloud* gdje ih se sprema i obavlja ostatak radnji koje su potrebne te se u nekom trenutku vraćaju nazad do uređaja. Kao i do sad taj postupak prijenosa može biti nesiguran ili biti direktna meta napada. Uočeno je kako je čest problem kod ovakvih situacija autentikacija. Problem također može ležati i u samim *cloud* sustavim i u njihovim platformama. [21] Ističe slabosti programiranja krajnih korisnika (engl. *end-user-programming, EUP*), *IFTTT(*engl. *if-true-then-that)* koristi koncept recepta, autor ističe moguće slabosti i probleme koji mogu nastati kada se koriste recepti, te je uočeno kako u kombinaciji s uređajima interneta stvari postoji velika mogućnost za napade bilo konkretno širenje virusa ili preuzimanja računala sa svrhom napada distribuiranog uskraćivanja usluge. Analiza pravila za okidanje popularnog i javno dostupnog sustava za automatizaciju doma kako je učestala pojava prekomjernog okidanja što također može dovesti do slabosti i napada. Sama platforma na koju se usluga oslanja također može biti slabost, jedan od uočenih problema je mogućnost napada na platforme za uvođenje *clouda,* na taj način otkrivaju korisnikov OAuth žeton. Žeton se koristi za davanje ovlasti i informacija preko različitih platformi bez dijeljenja lozinke, što ukazuje na problem u privatnosti.

Jedno od predloženih rješenja vezano uz napade preslušavanja predlaže dodavanje mogućnosti za dinamički odabir puta kojim će podatci ići kako bi se zaobišle točke na koje se sumnja da osluškuju podatke. [22] Predložio je necentralizirano okruženje koje bi funkcioniralo na osnovu okidača za određene događaje i omogućuje kreiranje platformi zvanih: decentralizirana platforma bazirana na radnji i reakciji (engl. *Decentralized Trigger-Action Platform, DTAP*) te platforme služile bi kao poveznica *cloud* paltformi i korisničke lokalne mreže. Glavna zamisao su žetoni za prijenos (engl. *transfer tokens, XTokens*) koji bi služili za pristup pametnom uređaju, ali su napravljeni na način da ih napadači teško mogu zlouporabiti.

6.5 Primjer pametnog doma

Dosadašnja potpoglavlja bavila su se područjima napada te je uz svaku generalnu metodu napada predložen i neki oblik sučelja ili metoda za prevenciju ili borbu protiv napada. Ovo poglavlje kao svrhu će imati ususstaviti sve dosada spomenuto u jedan mogući primjer pametnog doma sa svojim uređajima. Kućanstva, uređaji i potrebe kao i ukućani mogu varirati tako da primjer neće ići u krajnost potpuno automatiziranog pametnog doma nego će više biti usmjeren obraćanju pažnje na moguće probleme te njihovu prevenciju i zaštitu. Slika 6.2. može poslužiti kao dobar vizualni pokazatelj jednostavnog pametnog doma sa svojim uređajima i mogućim slabostima i problemima koje uređaji mogu imati.



Sl. 6.2. Primjer pametnog doma, uređaja i njihovih slabosti

Kako je i dosad spomenuto napadi se mogu promatrati iz perspektive napada na internet stvari, ali također ih je moguće promatrati iz perspektive pametnog doma kao sustava. Pošto ovdje konkretno govorimo o samom pametnom domu kao sustavu, analizirat ćemo napade, njihovu prevenciju i obranu isključivo iz perspektive pametnog doma. To znači da ćemo se baviti perceptivnim tj. fizičkim, mrežnim i aplikacijskim napadima.

Što se tiče perceptivnog oblika napada veliki problem proizlazi iz već spomenute resursne ograničenosti samih uređaja, dosadašnji oblici sigurnosti nisu imali zahtjeve ovakvog tipa kao ni ograničenost pa je zato primjena loša i u većini slučajeva se za sigurnost oslanjaju na neke dodatne platforme, što i dalje ne uklanja slabosti samog uređaja. Ograničenost se također prenosi i na tu interakciju s okolinom što onda može dovesti i do slabosti u servisima na koje se oslanja. U korist ovome ne ide ni činjenica kako potražnja za funkcijama ovih uređaja postepeno raste, a stari problemi se ne mogu tako lako riješiti što samo stvara nove probleme i slabosti. Uz to i sami postupci autentikacije koje uređaji koriste nisu pretjerano dobri što olakšava napade pretvaranja gdje napadač osluškuje komunikaciju te vrlo lako dobiva informacije o uređaju, pretvara se da je pravi uređaj i dobiva dodatne informacije za proširenje napada. Osim toga korisnici su često skloni ostaviti početne lozinke uređaja što ne pomaže već početno lošoj situaciji. Konkretan primjer ovakvih uređaja i njihovih problema su sigurnosne kamere i ostali oblici senzora. Lakoća pristupa i preuzimanja kontrole ovakvih uređaja može biti problem i za samo kućanstvo, ali se zbog lakoće preuzimanja vrlo lako može kreirati i *botnet* sa svrhom distribuiranog napada za uskraćivanje usluge. Još jedan od čestih uređaja sa velikim rasponom slabosti su uređaji bazirani na govoru korisnika kao što je Alexa tvrtke Amazon. Svrha takvih uređaja je pružiti sučelje koje onda omogućuje lagano baratanje sa svim ostalim uređajima. Zbog stalnog napretka tehnologije i umjetne inteligencije ljudi su pod dojmom kako je teško poremetiti „pametne“ uređaje, ali i sama Alexa mora na neki način biti umrežena kako sa svim uređajima često i sa internetom. Rizik uređaja koji kontrolira ostatak sustava pametnog doma je očit, a uz velike napretke strojnog učenja i rekonstrukcije ljudskog govora napadi takvog oblika postaju još jedan od problema.

Dosad navedene slabosti ukazuju na problem autentikacije, ovdje se radi o autentikaciji i potvrdi uređaja okolini na koje se oslanjaju. Očito rješenje je poboljšanje sigurnosnog standarda, ali uz već navedene ograničenosti takvo rješenje nije veoma lagano. Osim toga predloženo je promatranje okoline, podataka i navika korisnika kao jedno od rješenja. Problem toga je opet dodatna potreba za analizom velike količin podataka. Još jedno od nametnutih rješenja je smanjiti opseg funkcija uređaja, na taj način kada dođe do napada opseg problema koji može nastati je manji. Kao i dosad ni ovo nije optimalno iz razloga što ubija svrhu uređaja: automatizacija i jednostavnost kontrole kućanstva. Potreba za kontrolom i provjerom uređaja je jasna, ali zbog same prirode situacije i uređaja ne postoji direktno i jednostavno rješenje. Nešto što se može učiniti je usmjeriti pažnju korisnika uređaja na važnost izmjene lozinki, praćenja stanja u kojem se tehnologija nalazi i redovno održavanje uređaja i njihove podrške.

Kada je u pitanju mrežni ili komunikacijski aspekt, problemi opet poprimaju nove oblike, neki od problema međusobne interakcije uređaja preko mreže već su navedeni: preslušavanje, pretvaranje, preuzimanje uređaja, ponovno slanje itd. No u ovom području to nije jedini problem, veliki broj kamera i senzora se počinje koristiti u kućanstvu: senzori vlage, temperature, svjetlosti, zvuka kao i kamere. Stoga se ovo može razdvojiti na mrežne probleme, ali i fizičke probleme u komunikaciji. Sve te informacije od senzora koriste se za donošenje odluke koje se također prenose mrežom. Napadač može omesti rad senzora te time oštetiti rad cijelog sustava, jedan od primjera napada je povećanje smetnje u signalu kojim se prenose informacije, na taj način se otežava prijem signala. Kanali za prijenos informacija time gibe svoju efikasnost što može utjecati na ukupnu kvalitetu mreže i sustava. Moguća borba bila bi ograničenje opsega mrežnog prometa koji uređaj može zauzeti kako jedan ometeni uređaj nebi naštetio cijeloj mreži. Razni oblici smetnje u komunikaciji mogu imati razne rezultate, jedan od mogućih rezultata su neželjene radnje od uređaja u pametnom domu, ovisno o uređaju te radnje mogu imate i teže posljedice na uređaj ili dom. Jedan od već spomenutih problema je loša konfiguracija protokola, neki od primjera su slabo ili čak nepostojeće šifriranje sadržaja. Ovakvi problemi većinski su bazirani na senzore i ostale oblike uređaja koji dobijaju informacije iz okoline, ali sve je češća praksa kod današnjih uređaja da imaju barem neki oblik umreženosti.

Zbog svih gore navedenih problema, ali i mnogih drugih evidentna je potreba za pouzdanim i sigurnim komunikacijskim kanalima. Protokoli manje složenosti kao: WiFi i ZigBee pogodni su za ograničenost, ali opet otvaraju prostor za razne napade. Kada je u pitanju enkripcija protokoli poboljšavaju sigurnost, ali otežavaju pristup informacijama dodatnim platformama što otežava mogućnost analize i regulacije prometa u sigurnosne svrhe. Fizički kanali za interakciju također trebaju bolji pristup kako bi se smanjila mogućnost smetnje sustavu. Sve ovo nas dovodi do potrebe za novim oblikom komunikacijskih kanala koji bi obuhvatili sve potrebe uređaja pametnog doma što kao ni do sad nije lagana zadaća.

Na kraju dolazimo do aplikacija koje također viđaju sve veću uporabu u uređajima s obzirom na to da su mobilni uređaji u današnje vrijeme postali norma. Jedan čestih problem aplikacija koje se koriste u pametnom domu je prevelika razina ovlasti koju aplikacije imaju što ih često čini metom napada, osim toga često je prisutan i pozadinski ulaz (engl. *back-door*) što također može biti sredstvo napada i na kraju može omogućiti pristup privatnim podatcima o korinisku. Jednom od relativno sigurnih metoda zaštite od takvih oblika napada smatra se vatrozid (engl. *firewall*). Međutim postoje metode koje se oslanjaju na uređaje pametnog doma koje mogu zaobići tu zaštitu. Jedna od takvih metoda oslanja se upravo ne često korišteni pametni uređaj, a

riječ je o pametnim televizorima, kompanija GeoEdge tvrdi kako se televizori mogu koristiti kao sredstvo za napade [28]. Napad radi na način da se kreira zlonamjerni kod koji koristi reklame za unos navedenog zlonamjernog programa u mrežu i na taj način dolazi u kontakt s uređajem povezanim na WiFi mrežu. Još jedan zanimljiv oblik obilaska vatrozida oslanja se na još jedan danas veoma čest uređaj, riječ je o pametnim svjetlima, program radi na način da u vremenu koje nije vidljivo ljudskom oku mijenja razinu osvjetljenja i na taj način vizulanim senzorima razašilje bitne ili privatne informacije te vatrozid na to ne može reagirati, a ljudi nisu u stanju uočiti [29]. Kada je riječ o prevelikim ovlastima aplikacije moguće je kreirati napada koji se oslanja na taj višak ovlasti te izvesti radnju koja ne bi trebala biti moguća. Jedan od primjera je mogućnost otključavanja pametnih vrata, iako bi svrha aplikacije trebala biti zaključavanje vrata u ovisnosti o zadanim pravilima. Jedno od istraživanja obavljeno na 940 android aplikacija ustanovilo je kako trećina ima prevelike ovlasti što može dovesti do sličnih problema kao i navedeni napad s vratima [30].

Sreća je što se kod ovakvih problema većinski radi o samim aplikacijama i načinu na koji su one organizirane tako da se veliki dio problema može popraviti boljim aplikacijama, reguliranjem njihovih ovlasti i slično. Jedna od već spomenutih metoda SmartAuth ima svoje prednosti, no međutim ima slabost na napade zavaravanja u slučaju kada se kreira stvarni promet [11]. Kada je riječ o učestalo korištenim radnjama koristan je WHYPER koji se također oslanja na NLP (engl. *Natural Language Processing*), no kada se radi o rijetkim radnjam model nije dovoljno sposoban [25]. IoTGuard koristan je sustav koji tjera uređaje na točne akcije i ponašanja na temelju stvarnih potreba i okolnosti kućanstva [26]. Kada je riječ o preslušavanju i zavaravanju postoji HoMotion koji promatra ponašanje aplikacija bez donošenja promjena na sustav pametnog doma [27].

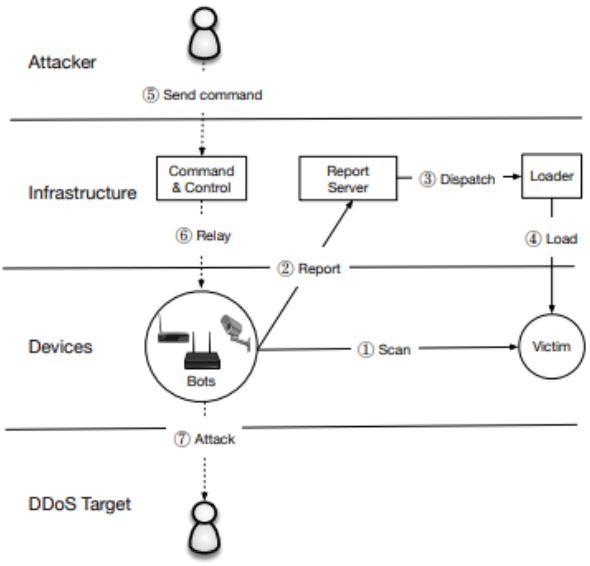
Sve u svemu jasno je kako pametni dom i njegovi uređaji imaju svoje probleme čiji se popravak ne može očekivati preko noći. Iako ga česta korist čini poželjnom metom za napade, s druge strane postoji osjećaj nade s obzirom da je ovo područje veoma bitno i istaknuto u današnjem tehnološkom svijetu. Iz tog razloga mogu se očekivati poboljšanja i napredak iako zasad stvarn ne izgledaju bajno. [31]

7. ZABILJEŽENI INCIDENTI

Po uzoru na dosadašnje sadržaje vidljivo je kako sigurnost domova te uređaja koji ga popunjavaju ima svoje slabosti i problem u raznim područjima, što opravdava pažnju koju dobiva u tehnološkom svijetu zadnjih par godina. Incidenti manjeg opsega prisutni su zbog slabosti i pružaju mogućnost za lakše napade, uglavnom se radi o provalama i krađama iz domova temeljenih na manjkavostima u sigurnosti pametnih vrata i lokota. [23] Prema prošlogodišnjem istraživanju u prosjeku 8 pametnih domova bude napadnuto. Međutim tu se većinski radi o javno dostupnim uređajima. Ovaj segment rada obuhvatit će incidente malo većeg opsega koji su kao metu imali uređaje interneta stvari ili domova.

7.1 Mirai botnet

U ovom napadu se radi o botnet tipu napada koji je zapravo skup uređaja nad kojim se napadom stekla mogućnost upravljanja te ih se koristilo za izvođenje napada distribuiranog uskraćivanja usluge (DDoS). Botnet je bio sačinjen od skupa uređaja interneta stvari, kao metoda širenja koristio se program sličnog oblika crvu (engl. *worm*), radi se o obliku napada koji pomoću mreže dobiva pristup još više uređaja. Raspon preuzetih uređaja bio je veoma velik, jedan od razloga tome je već spomenuta činjenica da su uređaji raznoliki po pitanju protokola koje koriste. Mete DDoS napada bile su razne kompanije koje pružaju razne oblike internetskih usluga.



Sl 7.1. Prikaz strukture napada [9]

Širenje je radilo na način da su botovi skenirali IPv4 adrese za uređaje koji se koriste telnet ili SSH protokolom za povezivanje, nakon pronalaska uređaja aktivirao bi se postupak pokušavanja probijanja šifre grubom silom koristeći napad rječnikom. Ako napad uspije bot šalje IP adresu i sve potrebne informacije poslužitelju zaduženom za osluškivanje koji bi zatim okinio funkciju za preuzimanje uređaja. Svaki preuzeti uređaj imao je mogućnost nastavka traženja novih uređaja ili izvođenja DDoS napada po potrebi. (1) Korak je proučavanje koji je radio na način da uređaj šalje TCP SYN zahtjeve na pseudoslučajne IPv4 adrese, ako je pronađen uređaj koji bi mogao biti potencijalna žrtva prelazi su pokušaj pristupa grubom silom, nakon toga se pokušava uspostaviti konekcija korištenjem nasumičnih deset imena i lozinki od mogućih 62 u imeniku. Nakon uspješnog logiranja izvodi se (2) koje obuhvaća kombinaciju koja se koristila za pristup uređaju. (3) Nepovezani uređaj za učitavanje pristupio bi uređaju, pronašao detalje o uređaju i sustavu te zatim učitao zlonamjerni program (engl. *malware*) ovisno o utvrđenoj strukturi (4). Po dovršetku procesa krenuo bi postupak prikrivanja postojanja. Struktura i rad botneta vidljivi su na slici 7.1. Detaljnija analiza i uvid u Mirai incident dostupan je na [9].

7.2 Verkada incident

Riječ je o napadu koji se dogodio 2021. godine, meta napada bili su uređaji istoimenog proizvođača. Verkada se uglavnom bavi prodajom kamera koje se oslanjaju na cloud tehnologiju i ističe se njihova lakoća instalacije i održavanja kao i mogućnost udaljene kontrole i mogućnost uporabe *clouda* za spremanje podataka. Iako meta napada jesu bile kamere, u ovom konkretnom slučaju razlog napada bila je slabost u samom sustavu kompanije Verkada. Napadači su se koristili poznatim slabostima u mrežnom sustavu i načinu implementacije te su na temelju slabosti dobili pristup dostupnim informacijama o administratorskom računu što im je pružilo pristup. Kao rezultat toga napadači su dobili pristup velikoj količini sadržaja snimljenih sa uređaja od korisnika kao i informacije o korisnicima. Grupa hakera tvrdi kako je cilj bio ukazivanje na slabosti ovakvih sustava i uređaja u kontekstu sigurnosti i privatnosti.

Reakcija kompanije na napad bila je korektna te je također pružila uvid u važnost nekih aspekata kibernetičke sigurnosti. Kada je napad otkriven ugašeni su svi uređaji i oduzet je pristup preuzetim računima. Verkada je također samostalno, ali i uz pomoć dodatne kompanije za kibernetičku sigurnost obavila istraživanje sustava kako bi se poboljšala sigurnost i smanjila mogućnost od budućih napada. Dodatno obavljen je postupak jačanja sigurnosnih mjera kao i metoda reakcije u svrhu bolje sigurnosti od budućih napada. Također je usmjerena pažnja prema

korisnicima i važnosti održavanja uređaja i programske podrške te iznimna važnost „jakih“ lozinki, također su omogućili autentikaciju s dva faktora. Sve u svemu opseg i šteta napada nije bila ogromna te je dodatno usmjerila pažnju na važnost sigurnosti u općenitom smislu kao i važnost educiranosti i upućenosti korisnika. Evidencija i analiza incidenta od strane same Verkade dostupna je na [24]

7.3 Napad na termostate

Ovaj napad slične je prirode kao i prije spomenut Mirai incident, naime radi se o botnet obliku napada koji je također prouzrokovao DDoS tip napada. Nasuprot dosad spomenutih napada ovaj je malo problematičniji. Meta napada bili su termostati u minimalno dvije zgrade u Finskoj te su kao pokušaj reakcije na napad zapeli u beskonačnoj petlji pokušaja ponovnog paljenja što je efektivno onemogućilo njihovu funkciju, problem leži u lokaciji napad gdje temperature zimi znaju biti veoma niske te su u ovom konkretnom slučaju mogle imati posljedice na zdravlje ili čak život korisnika. Na sreću vrijeme je u tom periodu bilo podnošljivo tako da nije bilo ozbiljnijih posljedica. Reakcije kompanije koja je za to zadužena također je bila adekvatna. Sustav je ugašen i vraćen je nazad na ručnu kontrolu temperature, a u svrhu zaštite i prevencije budućih napada uvedena je granica za mrežni promet kao i dodatak vatrozida. Iako posljedice nisu bile kobne ovo služi kao samo jedan od bezbroj primjera koji ukazuju na važnost što bolje i temeljitije sigurnosti ovakvih uređaja.

8. ZAKLJUČAK

Tema završnog rada bila je usmjerena prema pametnom domu te aspektima njegove sigurnosti, kao uvod objašnjeni su koncepti i tehnologije koje se danas koriste u pametnim domovima. Rad započinje sa osnovnim pojmovima i informacijama vezanim uz područja kojima će se rad baviti, objašnjeni su koncepti interneta stvari i pametnog doma. Bitan zaključak je: iako su koncepti usko povezani definitivno nisu ista stvar. Nakon osnovnih informacija prelazimo na pravu problematiku koja je kibernetička sigurnost kako samih uređaja tako i pametnog doma kao sustava. Navedeni su aspekti i područja kibernetičke sigurnosti samostalno te područja napada za same uređaje. Također su dani primjeri nekih tipova napada te uz njih i neke od mogućih metoda prevencije ili čak borbe protiv napada.

Kako i kroz rad tako i na internetu i drugim oblicima sadržaja koji se bave ovom tematikom evidentna je manjkavost ovog područja i potreba za proširenjem i poboljšanjem sigurnosti u većini aspekata. Jedan od faktora koji se također često spominje je činjenica da je u kontekstu doma i uređaja prisutan i ljudski faktor. Manjak tehnološkog znanja na području kibernetičke sigurnosti čini ljude lakšim metama za napad, uz već postojeće sigurnosne nedostatke. Jedan od problema leži i u specifičnosti i zahtjevima uređaja u domu, teško je dosadašnje standarde i metode obrane uklopiti u drugačiji i često resursno ograničen sustav.

Utjehu je moguće pronaći u činjenici da napredak i razvoj ovog područja pa time i pažnja koja mu se pridaje kontinuirano raste iz godine u godinu. Uz ljudsku želju za privatnost i sigurnost neophodno je kretanje u smjeru da se to zadovolji, apsolutnu sigurnost teško je garantirati, ali to ne treba značiti da ju treba zapostaviti. Uz neprestano ulaganje i poboljšavanje uređaja pa time i pametnog doma, vjerujem da bi dodatnu pomoć pružilo i povećanje svjesti i informiranosti korisnika pošto je vidljivo da uređaji sve više i više postaju dio naše svakodnevice.

LITERATURA

[1] S. Obadić, IoT i Pametna kuća, dostupno na:

https://dabar.srce.hr/islandora/object/etfos%3A1651

[2] Internet Of Things (IOT): Origin, Embedded Technologies, Smart Applications and its Growth in the Last Decade (IEEE), dostupno na: https://ieeexplore.ieee.org/document/10570411

[3] Ž. Juric, Smart House - Moderni sustavi upravljanja za primjenu u obiteljskoj kući, dostupno na: https://dabar.srce.hr/islandora/object/etfos%3A2513

[4] R. Khatoun, Cybersecurity in Smart Homes, dostupno na:

https://www.oreilly.com/library/view/cybersecurity-in-smart/9781789450866/f01.xhtml

[5] Ranking Security of IoT-Based Smart Home Consumer Devices (IEEE), dostupno na: https://ieeexplore.ieee.org/document/9698229

[6] A Comprehensive Survey of Security Issues of Smart Home System: „Spear“ and „Shields,“ Theory and practice (IEEE), dostupno na: https://ieeexplore.ieee.org/document/9963917

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, dostupno na: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf

[8] Security Implications of Premission Models in Smart-Home Application Frameworks (IEEE), dostupno na: https://ieeexplore.ieee.org/document/7891524

[9] M. Antonakakis, Understanding the Mirai Botnet, dostupno na: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[10] Q. Wang, Fear and Logging in the Internet of Things, dostupno na: https://www.ndss-symposium.org/wp-content/uploads/2018/03/NDSS2018_01A-2_Wang_Slides.pdf

[11] Y. Tian, SmartAuth: User-Centered Autohrization for the Internet of Things, dostupno na: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tian

[12] Attacks and Defenses in Short-Range Wireless Technologies for IoT (IEEE), dostupno na: https://ieeexplore.ieee.org/document/9090905

[13] N. Aviram, DROWN: Breaking TLS Using SSLv2, dostupno na: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/aviram

[14] X. Huang, SecIoT: a security framework for the Internet of Things, dostupno na:

https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1259

[15] M. Serror, Towards In-Network Security for Smart Homes, dostupno na: https://dl.acm.org/doi/10.1145/3230833.3232802

[16] S. Grzonkowski, Smartphone Security: An overview of emerging threats, dostupno na: https://ieeexplore.ieee.org/document/6914660

[17] H. Liu, Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem, dostupno na: https://ieeexplore.ieee.org/document/8730685

[18] E. Fernandes, FlowFence: Practical Data Protection for Emerging IoT Application Frameworks, dostupno na: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fernandes

[19] S. Demetriou, HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps, dostupno na: https://dl.acm.org/doi/10.1145/3098243.3098251

[20] M. Yamauchi, Anomaly Detection in Smart Home Operation From User Behaviots and Home Conditions, dostupno na: https://ieeexplore.ieee.org/document/9040414

[21] M. Surbatovich, Some Recipes Can DO More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes, dostupno na:

https://dl.acm.org/doi/10.1145/3038912.3052709

[22] E. Frenandes, Decentralized Action Integrity for Trigger-Action IoT Platforms, dostupno na: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-3_Fernandes_paper.pdf

[23] Bitfinder, The 2023 IoT Security Landscape Report, dostupno na:

https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

[24] Verkada, March 9, 2021 Security Incident Report, dostupno na:

https://www.verkada.com/security-update/report/

[25] R. Pandita, X. Xiao, W. Yang, W. Enck, and T. Xie, “WHYPER: Towards automating risk assessment of mobile applications,” in Proc. USENIX Security Symp., 2013, pp. 527–542. dostupno na:

https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_pandita.pdf

[26] Z. B. Celik, G. Tan, and P. D. McDaniel, “IoTGuard: Dynamic enforce ment of security and safety policy in commodity IoT,” in Proc. Netw. Distrib. Syst. Security Symp. (NDSS), 2019, pp. 1–15. dostupno na: https://patrickmcdaniel.org/pubs/ctm19b.pdf

[27] W. Zhang, Y. Meng, Y. Liu, X. Zhang, Y. Zhang, and H. Zhu, “HoMonit: Monitoring smart home apps from encrypted traffic,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), 2018, pp. 1074–1088. dostupno na: https://dl.acm.org/doi/10.1145/3243734.3243820

[28] “Your security partner for ad quality.” GeoEdge. 2022.

dostupno na: https://www.geoedge.com/

[29] E. Ronen and A. Shamir, “Extended functionality attacks on IoT devices: The case of smart lights,” in Proc. IEEE Eur. Symp. Security Privacy, 2016, pp. 3–12.

dostupno na: https://eyalro.net/pdf/EyalShamirLed.pdf

[30] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. A. Wagner, “Android per missions demystified,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), 2011, pp. 627–638. dostupno na: https://dl.acm.org/doi/10.1145/2046707.2046779

[31] Z. Wang, D. Liu, Y. Sun, X. Pang, „A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses“, dostupno na: https://ieeexplore.ieee.org/document/9869705

SAŽETAK

Završni rad usmjeren je ka sigurnosti pametnog doma kao koncepta koji postaje sve češći i poznatiji tokom prijašnjih godina, dio zasluge za to ima koncept interneta stvari na koji se pametni domovi većinski oslanjaju. Nakon uvodnog poglavlja prolazimo osnovne informacije o internetu stvari i pametnom domu. U nastavku se spominju generalne informacije vezane za kibernetičku sigurnost od općenitih opasnosti i problem, koncepata i usluga. Zatim se pristupa kibernetičkoj sigurnosti u kontekstu doma sa područjima, vrstama i oblicima napada. Uz istaknute probleme priložene su neke od predloženih metoda poboljšanja navedenog područja. Na kraju su navedeni neki incidenti i situacije koje su također vezane uz ovo područje i dodatno potvrđuju važnost napretka kibernetičke sigurnosti u ovome području.

Ključne riječi: internet stvari, kibernetička sigurnost, pametni dom

ABSTRACT

The Bachelor thesis talks about the security of smart homes, the concept of smart homes itself is becoming more known and frequent over the past few years, one of the reasons for that is the concept Internet of Things (IoT), since smart homes mostly make use of those devices. After the introduction we give the definition of the two concepts as well as some general information about them. The upcoming chapters talk about cybersecurity from general information to concepts and services that are expected from it. Lastly the thesis gives a look at cybersecurity from the perspective of smart homes and IoT, types of attacks, issues and vulnerabilites are given. Then we go over some concrete attacks from ceratin categories with proposed solutions or improvements. Lastly we go over some bigger incidents that occured giving more understading for the need in improvement of cybersecurity in the domain.

Keywords: cybersecurity, internet of things, smart home