Istraživanje ranjivosti terminalnih uređaja u okruženju pametnog doma

Gudiček, Dominik

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ISTRAŽIVANJE RANJIVOSTI TERMINALNIH UREĐAJA U OKRUŽENJU PAMETNOG DOMA

INVESTIGATING THE VULNERABILITY OF TERMINAL DEVICES IN A SMART HOME ENVIRONMENT

Mentor: dr. sc. Ivan Cvitić

Student: Dominik Gudiček

JMBAG: 0135241803

Zagreb, Studeni 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6417

Pristupnik: **Dominik Gudiček (0135241803)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Istraživanje ranjivosti terminalnih uređaja u okruženju pametnog doma**

Opis zadatka:

U okviru diplomskog rada potrebno je utvrditi principe rada uređaja unutar okruženja pametnog doma, zatim istražiti trenutno stanje sigurnosti IoT uređaja unutar okruženja pametnog doma sa svrhom povećanja svijest korisnika o mogućim sigurnosnim prijetnjama na IoT uređaje i podatke koji se prikupljaju. Nakon provedbe analize potrebno je sintetizirati dobivene rezultate i predložiti načine zaštite korisnika. Zaključno, potrebno je istaknuti otvorena pitanja i izazove sigurnosti u konceptu IoT.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

ISTRAŽIVANJE RANJIVOSTI TERMINALNIH UREĐAJA U OKRUŽENJU PAMETNOG DOMA

SAŽETAK

Rad daje pregled funkcionalnosti koncepta Interneta stvari (eng. *Internet of Things* - IoT), navodi i objašnjava princip rada komunikacijskih tehnologija koje se koriste u okruženju pametnog doma. Unutar rada se također navode i opisuju alati i metode koje napadači koriste prilikom izvođenja kibernetičkog napada. Za odabrane uređaje u radu izrađena je analiza ranjivosti za slučaj kada se napada prvo usmjerivač pa nakon toga IoT uređaji unutar mreže. Rezultat ispitivanja objašnjen je i analiziran, te su iznesene sigurnosne smjernice vezane uz IoT uređaje u okruženju pametnog doma.

KLJUČNE RIJEČI: IoT, okruženje pametnog doma, analiza ranjivosti

SUMMARY

The paper provides an overview of the functionality of IoT concept, it states and explains the working principle of communication technologies used in a smart home environment. The paper also lists and describes the tools and methods that attackers are using when performing a cyber-attack. For selected devices, an analysis of the vulnerability was performed in case when the router is attacked first and then the IoT devices within the network. The result of the examination was explained and analyzed, additionally, safety guidelines related to IoT devices in a smart home environment were presented.

KEY WORDS: IoT, smart home environment, vulnerability analysis

SAŽETAK:

1. Uvod

IoT tehnologija na velika vrata ušla je u naše živote. Sve je više uređaja koje posjedujemo u svojim domovima koji nam olakšavanju svakidašnje poslove. U još većoj mjeri IoT tehnologija zauzela je svoje mjesto u industrijskom okruženju, gdje omogućuje automatizaciju proizvodnje. Sve je češća uporaba IoT tehnologije unutar prometnih grana, razni vidovi prometa uvode sustave autonomnih vožnji koje omogućuje upravo IoT tehnologija uz ostale elemente sustava.

Pojavom senzorike i tehnika povezivanja, kako onih koji omogućuju komunikaciju na dugi dometa, a izričito onih koji omogućuju komunikaciju na kratki domet razvija se IoT tehnologija. Razvitak IoT tehnologije pruža se u smjeru smanjenja potrošnje baterija uređaja, te komunikacije sa cloud i fog tehnologijom. Isto tako pojava 5G tehnologije otvara nove mogućnosti unutar kojih će važnost IoT tehnologije zasigurno biti velika.

Naglim rastom broja uređaja, IoT uređaji postali su zanimljiva meta kibernetičkih kriminalaca. Razlog tome su slabiji zaštitni mehanizmi implementirani na same uređaje. Ali isto tako i autonomizacija koju pružaju iz razloga što većina korisnika niti ne primijete ukoliko njihovi uređaji obavljaju dodatne aktivnosti za vrijeme dok obavljaju ono za što su namijenjeni.

Također kada je riječ o korištenju IoT tehnologije unutar okruženja pametnog doma korisnici u velikoj mjeri nisu niti svjesni količine podataka koja se konstantno prenosi od uređaja do uređaja, te do mjesta gdje se ti podaci obrađuju, analiziraju i na kraju pohranjuju. Problem privatnosti ne misli se samo kada neovlašteni napadač ostvari kontrolu nad uređajem ili presretne promet te je u mogućnosti osluškivati informacije i podatke koji se prenose, već isto tako problem privatnosti predstavljaju i kompanije koje su proizvođači takvih uređaja. Prikupljanjem velike količine podataka proizvođači IoT uređaja stvaraju si uzorke kojima mogu odlučiti koje poslovne korake napraviti u budućnosti, te kojim inovacijama se okrenuti i u kojem smjeru nastaviti razvijati svoje uređaje i tehnologiju.

Seminarski rad sastoji se od sedam poglavlja:

1. Uvod

2. Pregled dosadašnjih istraživanja
3. Princip rada uređaja unutar okruženja pametnog doma
4. Analiza ranjivosti uređaja u okruženju pametnog doma
5. Sinteza rezultata istraživanja i prijedlog zaštite korisnika
6. Otvorena pitanja i izazovi sigurnosti u konceptu IoT
7. Zaključak

Unutar drugog poglavlja predstavljeni su neki od dosad već napravljenih radova na temu IoT koncepta, uređaja, te sigurnosti. Opisani su neki od prijedloga IoT arhitekture, te sigurnosnih sustava kojima bi se mogla povećati sigurnost IoT uređaja. Također navedena su i područja unutar koji se sve koristi IoT tehnologija, te je napravljeno istraživanje na temu velike raznolikosti i brojčanosti IoT uređaja.

Unutar trećeg poglavlja navedeni su i objašnjeni neki od osnovnih pojmova računalnih mreža kako bi se kasnije lakše razumjelo samo istraživanje. Također prikazane su i komunikacijske tehnologije korištene u konceptu IoT-a, te njihovi sigurnosni nedostaci. Zatim navedeni su i objašnjeni neki od vektora i vrsta mogućih napada, te je opisana kriptografija. Za kraj poglavlja prikazani su statistički podaci gdje se trenutno nalazi IoT tehnologija, te koja su predviđanja za nju gledano iz različitih stajališta.

Četvrto poglavlje predstavlja analizu ranjivosti testiranih uređaja. Za početak poglavlja opisan je proces penetracijskog testiranja. Zatim navedena je oprema koja je korištena unutar samog istraživanja, te su opisane karakteristike opreme. Za kraj poglavlja napravljeno je istraživanje ranjivosti usmjerivača i IoT uređaja u okruženju pametnog doma.

U petom poglavlju raspisani su rezultati napravljenog istraživanja. Te su opisani pojmovi koji omogućuje sprječavanje ili povećanje sigurnosti od napada kako u okruženju pametnog doma tako i u nekim većim korporacijskim okruženjima.

Šesto poglavlje rezervirano je za sigurnosne smjernice kojima se predlažu neki od koraka kako učiniti svoje kućno okruženje sigurnijim, te su također navedeni izazovi koji se tek trebaju riješiti vezani uz sigurnost IoT koncepta.

2. Pregled dosadašnjih istraživanja

IoT koncept spominje se već dugi niz godina te se velikom brzinom pronalaze brojne nove ideje i načini korištenja IoT uređaja. Unutar ovog poglavlja biti će opisana dosadašnja istraživanja na temu sigurnosti IoT uređaja, ali i cijelog IoT sustava u okruženju pametnog doma i ostalim okruženjima.

Prema [1] radu iz 2017. godine kroz različite poglede kao što su: korištenje IoT uređaja unutar industrijskog okruženja, kao osobna medicinska pomagala i kroz okruženje pametnog doma opisuju se sigurnosni zahtjevi koji je potrebno zadovoljiti kako bi se povećala sigurnost samih uređaja, ali i mreže.

IoT tehnologija koja se koristi u obliku osobnih medicinskih pomagala sve su češća i imaju sve veću primjenu. Sigurnosne prijetnje na takve vrste uređaja mogu imati direktan utjecaj na zdravlje i sigurnost ljudi, te je iz tog razloga posebno važno posvetiti više pažnje na sigurnost kod dizajniranja takvog sustava. Najčešće sigurnosne prijetnje koje se javljaju kada je riječ o IoT uređajima kao osobnim medicinskim pomagalima su: krađa osobnih podataka, napadi na pametne uređaje kojima se upravljaju medicinska pomagala, povećana potrošnja baterija. Napadom na pametne uređaje moguće je onemogućiti rad aplikacijama koje služe za monitoriranje rada medicinskog pomagala. Na taj način može se dogoditi da aplikacija korisniku prikazuje pogrešne podatke ili da u potpunosti prekine prikazivati informacije.

U nastavku rada opisane su sigurnosne prijetnje, napadi i moguća rješenja kada je riječ o okruženju pametnog doma. Neki od primjera prijetnji su: nezakonit ulaz, prikupljanje osobnih podataka, DoS (eng. *Denial-of-service*) i DDoS (eng. *Distributed Denial of Service*) napadi.

Napadi su podijeljeni u dvije kategorije: pasivne i aktivne napade. Pasivni napadi se smatraju oni kod kojih napadač nema fizički kontakt, dok se aktivni napad smatra napadom kod kojeg napadač ima fizički kontakt sa metom napada. Također napravljena je i podjela napada prema intenzitetu na četiri različita nivoa intenziteta napada.

Istraživanje [2] temelji se na troslojnoj IoT arhitekturi kroz koju se opisuju sigurnosni nedostaci kroz sva tri sloja. Tri sloja opisane arhitekture su: percepcijski sloj, mrežni sloj i aplikacijski sloj.

Percepcijski sloj smatra se sloj senzora unutar IoT arhitekture i glavni zadatak ovog nivoa je prikupljanje informacija iz okoline uz pomoć senzora. Osim prikupljanja podataka iz okoline ono što još spada pod percepcijski sloj je i obrada tih podataka te prijenos do mrežnog sloja. Sigurnosne prijetnje koje se javljaju unutar percepcijskog sloja podijeljene su na tri glavne prijetnje.

Prijenos podataka bežičnim putem prijetnja je koja se javlja jer se za prikupljanje i slanje prikupljenih podataka između senzora koriste bežični signali koji su podložni ranjivostima. Ranjivost senzora je također prijetnja koja se spominje iz razloga što se sami senzori često nalaze na udaljenim i otvorenim mjestima kojima napadač može imati direktan fizički pristup. Treća ranjivost koja se spominje je nedostatak memorije samih uređaja, kao i mogućnost ostanka bez napajanja te to ostavlja nove mogućnosti napadačima za provođenja napada.

Mrežni sloj ima zadatak prijenosa podataka putem Interneta do udaljenih IoT mreža, ali i komunikacija unutar mreže putem tehnologija povezivanja kao što su WiFi, LTE (eng. *Long-Term Evolution*), *Bluetooth*, 3G i Zigbee. DoS i *Man-in-the-middle* navedeni su kao najčešće vrste napada kojima je podložan mrežni sloj IoT arhitekture. Mogućnost prisluškivanja, ali i pasivnog monitoringa mrežne direktan su napada na povjerljivost i privatnost podataka koji se prenose mrežom. Kao moguće rješenje ovog problema predlaže se vrsta kriptografije, odnosno razmjene ključeva unutar same komunikacije.

Aplikacijskim slojem osigurava se autentifikacija, integritet i povjerljivost podataka. Nedostatak koji je naveden kao najveći problem je to što ne postoji standardiziranost unutar IoT okruženja. Brojni proizvođači proizvode svoje *software*-e i aplikacije koje koriste različite mehanizme autentifikacije i ostale sigurnosne mehanizme, te na taj način nestandardiziranost olakšava napadačima posao.

U daljnjem dijelu rada opisane su moguća rješenja kako bi se povećala sigurnost IoT uređaja. Jedno od rješenja je povećanje svijest korisnika o sigurnosnim propustima samih IoT uređaja. Velika većina korisnika IoT uređaja ili uopće ne koristi

lozinke za pristup samom uređaju ili ostavljaju unaprijed postavljenu lozinku koje se često mogu naći na Internetu prema modelu i proizvođaču uređaja.

U radu [3] autori navode prema njima „tipičnu“ IoT arhitekturu u okruženju pametnog doma. Arhitektura se sastoji od pametnog uređaja, *hub*-a, cloud dijela arhitekture i korisničkog sučelja. Pametni uređaji opisani su kao ključan dio cijele arhitekture iz razloga što se njima prikupljaju podaci iz okoline, odnosno pod pametne uređaje smješteni su razni senzori, ali i uređaji koji omogućuju komunikaciju nekom od komunikacijskih tehnologija, kao što su na primjer: Bluetooth, Wi-Fi, Zigbee, NB-IoT (eng. *Narrowband-Internet of Things*) i slično. Također navedeni su i aktuatori kao uređaji koji omogućuju izvršenje neke radnje, kao na primjer otključavanje vrata pomoću pametne brave.

Sljedeći dio navedene arhitekture je *Hub*. *Hub* ima funkciju prenošenja informacija od senzora prema cloud-u. Odnosno služi kao pristupnik prema cloud-u.

Dio arhitekture koji se nalazi u cloud-u obavlja funkciju logičkih radnji. Pretežito su te radnje usmjerene smanjenju potrošnje energije IoT uređaja koji su ograničeni kapacitetom energije. Kao primjer navedena je žarulja koja se pali, odnosno gasi ovisno o tome dali je osoba unutar prostorije.

Autori rada predstavili su WiVo sustav, odnosno dvo-faktorski autentifikacijski sustav koji koristi glas kao način autentifikacije. WiVo je sustav koji se prvenstveno koristi kako bi se onemogućio napada lažiranja glasovne autentifikacije. Način na koji to omogućuje je to što uzima u obzir faktor pokreta usana. Tehnologija koja se pritom koristi naziva se CSI (eng. *Channel state information*), odnosno procjena kanala.

Način rada WiVo sustava opisan je kroz četiri koraka. Prvo WiVo prikuplja glasovne uzorke i njegove odgovarajuće CSI podatke. Nakon toga WiVo neutralizira šumove i smetnje iz CSI podataka i segmentira slogove prikupljenog glasovnog uzorka. Treći koraka je odabir odgovarajućih značajki sa različitih nivoa. U zadnjem koraku WiVo razlučuje dali je glasovni uzorak autentičan ili se radi o napadu lažiranja.

U radu [4] autori su proveli istraživanje koje navodi raznolikost i veliku brojčanost IoT uređaja koji se koriste u okruženju pametnog doma, ali također i nekim drugi područjima. Tako su autori koncept Interneta stvari odlučili sagledati kao interakciju

između ljudi i objekata, ali kroz novu dimenziju koju omogućuje koncept Interneta stvari i to unutar tri glavna područja: industrija, okolina i društvo.

Područje industrije prema autorima podrazumijeva aktivnosti koje uključuju financijske i trgovačke transakcije između kompanija, organizacija i ostalih entiteta. Kao primjeri navedena je proizvodnja, logistika, sektora bankarstva, te brojne druge aktivnosti.

Pogled na koncept Interneta stvari kroz područje okoline prema radu odnosi se na aktivnosti koje su usredotočene na zaštitu, kontrolu i razvoj svih prirodnih resursa. Te se kao primjer navode aktivnosti agrokultura, recikliranje, te upravljanje energetskim resursima.

Područje društva smatra ju se aktivnosti koje su povezane sa razvojem kulture, gradova i ljudi. Kao primjeri navedeni su usluge državne službi prema građanima i ostalim socijalnim strukturama, te usluge koje su namijenjene prema starijim osobama i prema osobama sa invaliditetom.

Također se unutar rada navode i klasifikacija korištenja koncepta Interneta stvari kroz različite poglede. Pa tako ukoliko je riječ o široj slici postoje koncepti „pametnog grada“ unutar kojeg se nalaze brojena manja područja koja svaka ima svoju funkciju, ali međusobnom komunikacijom stvaraju cjelinu.

Isto tako navedena je i arhitektura koncepta „pametne građevine“. Koja kroz pet slojeva omogućuje upravljanje različitih aktivnosti kao što su: kontrola i upravljanje dizalima, upravljanje električnom energijom, upravljanje procesom zbrinjavanja otpada i brojni drugi procesi koji se konstantno monitoriraju. Na taj način omogućuje se veća količina podataka koja olakšava upravljanje potrošnjom kako bi se efikasnije iskoristili određeni resursi.

Unutar rada su također navedeni brojni statistički podaci koji prikazuju rast korištenja IoT uređaja unazad desetak godina, ali i trendove koji prikazuju daljnji još brzi rast. Osim statističkih podataka koji prikazuju rast broja IoT uređaja, također prikazana je statistika prednosti kompanijama koje su se odlučile na uvođenje koncepta Interneta stvari unutar svog poslovnog okruženja.

3. Princip rada uređaja unutar okruženja pametnog doma

Brojnim školama i fakultetima predavanja o IoT uređajima i cjelokupnom načinu rada okruženja postala su neizbježna. Unutar ovog poglavlja biti će opisan pojam IoT, općenit način rada IoT-a, te detaljnije opisan način rada IoT uređaja unutar okruženja pametnog doma.

Prema [5] IoT se definira kao mreža fizičkih uređaja koji se sastoje od senzora, *software*-a i komunikacijskih tehnologija koje omogućuju povezivanje i razmjenu podataka između sebe, ali i sa ostalim uređajima putem Interneta.

Dva pojma koja se od velike važnosti kada je riječ o IoT konceptu su senzori i aktuatori. Senzor predstavlja uređaj koji ima funkciju pretvorbe fizičkih parametara kao što su: temperatura, toplina, gibanje, vlažnost zraka, tlak i ostale slične parametre u električne signale. Mogli bismo reći kako senzori osluškuju našu okolinu i te podatke prikazuju kao električne signale. S druge strane aktuatori su uređaji pretvaraju električnu ili fluidnu energiju u mehaničku energiju. Tako za primjer aktuatora mogli bismo navesti zaslon i zvučnik koji kada prime električni signal pretvore ga ili u svjetlosni ili u zvučni [6].

Upravo ono što je vidljivo iz same definicije je da je ljudski faktor poprilično maknut iz samog načina rada IoT infrastrukture te je vrlo važan koncept M2M (eng. *Machine to Machine*) komunikacije. M2M komunikacija može biti bežična ili žična, a predstavlja automatiziranu razmjenu informacija između tehničke opreme, kao što je razna mehanizacija, strojevi, vozila ili mjerni uređaji koji mogu komunicirati međusobno ili sa centralnim sustavom za obradu podataka [7].

3.1 Osnovni pojmovi računalnih mreža

Kako bi bilo moguće opisati funkcionalnosti IoT uređaja i princip rada IoT uređaja potrebno je za početak navesti i objasniti neke osnovne pojmove iz područja računalnih mreža. Iako postoje brojni drugi pojmovi koji su krucijalni za poznavanje funkcionalnosti koncepta računalnih mreža unutar ovog poglavlja biti će opisani samo pojmovi koje će se pojavljivati i u nastavku rada prilikom opisa praktičnog dijela rada.

3.1.1 MAC i IP adresa

MAC (eng. *Media Access Control*) adresa je jedinstveni identifikator mrežne kartice uređaja pomoću koje uređaj komunicira. Sastoje se od 48 bit-a, te se još nazivaju i fizičke adrese. Za razliku od IP (eng. *Internet Protocol*) adresa, MAC adrese nisu promjenjive, te su dodijeljene uređaju od strane proizvođača. Kod procesa upravljanja mrežama i dijagnoze mrežnih problema, mrežni administratori često koriste MAC adrese upravo iz razloga što su nepromjenjive [8]. U nastavku rada identifikacija uređaja biti će potvrđena upravo pomoću MAC adrese.

Kako je već navedeno IP adrese nisu uvijek iste već su promjenjive. IP adresa također služi kao identifikator uređaja, te omogućuje komunikaciju između uređaja kako unutar određene mreže, tako i komunikaciju prema Internetu. Postoje dvije inačice IP adresa poznatije kao IPv4 i IPv6.

IPv4 adresa sastoji se od 32 bit-a podijeljena u četiri okteta, te je svaki oktet odijeljen točkom. Kako se radi o decimalnoj notaciji ukupan mogući broj različitih adresa je 4,294,967,296, odnosno 2^{32}. U vrijeme nastanka Interneta i počecima telekomunikacija smatralo se kako je količina od 4,294,967,296 jedinstvenih identifikatora uređaja sasvim dovoljna, danas znamo da taj broj nije dovoljan te je iz tog razloga nastao IPv6. IPv4 adresa podijeljena je u pet klasa koje se razlikuju ovisno o tome koji broj okteta označava mrežni identifikator, a koji broj okteta identifikator uređaja [9]:

- Klasa A se koristi kod mreža koje se sačinjavaju od velikog broja uređaja. Kod klase A samo je prvi oktet mrežni identifikator, što omogućava broj od 126 različitih mreža, a ostala tri okteta rezervirana su za identifikaciju uređaja unutar tih mreža.
- Klasa B se koristi za mreže srednjeg i velikog broja uređaja, te dozvoljava manji broj mreža u odnosu na klasu A iz razloga što prva dva okteta označavaju mrežni identifikator dok su zadnja dva okteta identifikatori uređaja.
- Klasa C najčešće je korištena kod malih LAN (eng. *Local Area Network*) mreža. Kod klase C prva tri okteta služe kao identifikator mreže, a posljednji četvrti oktet koristi se kao identifikator uređaja.

- Klasa D nema oktet dodijeljen identifikaciji uređaja, već služi kao višeodredišna adresa (eng. *multicasting)*
- Klasa E nije namijenjena općoj upotrebi, već isključivo služi za potrebe istraživanja [10].

IPv6 je novija generacija IP adresiranja nastala iz razloga što broj uređaja povezanih na Internet iz dana u dan raste te ponestaje slobodnih IPv4 adresa. Sama funkcionalnost je vrlo slična kao kod IPv4, no glavna razlika je što se kod IPv6 radi o heksadecimalnoj notaciji te omogućuje 2^{128} mogućih adresa.

3.1.2 Funkcionalnosti i korištenje ARP protokola

ARP (eng. *Address Resolution Protocol*) je protokol kojemu je glavna zadaća povezivanje IP adresa uređaja i MAC adresa uređaja unutar LAN mreže. Iako je MAC adresa pojedinog uređaja fiksna, IP adresa je promjenjiva te kako bi se mogla odvijati komunikacija potreban je netko tko će pratit te promjene i omogućiti komunikaciju, te upravo zato služi ARP. Prema OSI (eng. *Open Systems Interconnection*) referentnom modelu ARP protokol se nalazi i djeluje između podatkovnog i mrežnog sloja. Kako uistinu ARP odrađuje svoje zadatke moguće je objasniti primjerom. Kada se novo računalo ili neki drugi uređaj poveze na LAN mrežu on dobiva IP adresu koja mu služi za identifikaciju i komunikaciju. Jednom kada paketi stignu na pristupnik LAN mreže, recimo da se radi o usmjerivaču, tada usmjerivač pogleda u svoju ARP tablicu dali se u njoj nalazi IP adresa za koju je namijenjen paket, te dali je uparena sa svojom MAC adresom kako bi znao kojem uređaju unutar LAN mreže proslijediti navedeni paket. Ukoliko se u ARP tablici već nalaze potrebne IP i MAC adrese, usmjerivač samo prosljeđuje poruku bez potrebnih dodatnih zadataka. No ukoliko se u ARP tablici usmjerivača ne nalazi potreban par IP i MAC adresa, tada usmjerivač prvo šalje ARP zahtjev (eng*. ARP Request*) poruku do svih uređaja u mreži. Uređaj koji ima traženu IP adresu odgovara porukom (eng. *ARP Reply*) na kojoj MAC adresi se nalazi tražena IP adresa. Tada si usmjerivač te podatke zapisuje u svoju ARP tablicu te nastavlja sa procesom prosljeđivanja poruke prema uređaju sa traženom IP adresom. ARP tablica ne postoji samo kod usmjerivača već i ostali uređaji u mreži sadržavaju svoju ARP tablicu kako bi mogli komunicirati međusobno [11].

ARP tablica ima unaprijed postavljeno koliku količinu podataka može sadržavati. Nakon zapunjenja najstariji podaci se brišu kako bi se oslobodilo mjesto za nove podatke. Kako uopće ne bi došlo do zapunjenja ARP tablice, unaprijed je određen i vremenski rok nakon kojeg uređaji brišu svoje ARP tablice te je kod nove komunikacije potrebno ponovno proći kroz ranije naveden postupak kako bi se omogućila komunikacije i ponovno popunjavanje ARP tablica. Osim zapunjenja još jedan razlog čestog brisanja ARP tablica je mogućnost napada takozvanog trovanja ARP predmemorije (eng. *ARP cache poisoning*). Iako brisanje ARP tablica usporava komunikaciju, također poveća sigurnosti i smanjuje mogućnost napada trovanja ARP predmemorije [11].

Napad trovanja ARP predmemorije je napad kod kojeg napadač šalje lažnu ARP poruku te na taj način „tjera“ uređaj da mijenja svoju ARP tablicu. Sve poruke koje su bile namijenjene tom određenom uređaju tada dolaze do napadača. Na taj način napadač može doći do brojnih povjerljivih informacija što može imati velike posljedice. Napad je moguć iz razloga što sam ARP nema sigurnosne mehanizme pomoću kojih bi se takva vrsta napada detektirala i spriječila [11].

ARP protokol koristi se i prilikom istraživanja ranjivosti terminalnih uređaja u nastavku rada. Svoju ulogu ima kod aktivnosti kao što je pronalazak IP i MAC adrese pojedinog uređaja unutar testne mreže.

3.2 Komunikacijske tehnologije i izazovi razvoja IoT uređaja

Prilikom izrade IoT uređaja proizvođačima mnogi parametri predstavljaju izazov. Ti parametri također određuju i same funkcionalnosti uređaja. Iz razloga što većina IoT uređaja mora biti poprilično malih dimenzija smanjuje se mogućnost ugradnje većih baterija, ali i ostalih komponenti koje bi učinile uređaje efikasnijima. Iz tog razloga izrazito je bitno obratiti pažnju kako omogućiti što dulje trajanje baterija, a jedan od načina je i odabir komunikacijske tehnologije koja će se koristiti prilikom slanja prikupljenih podataka.

Komunikacijske tehnologije koje se koriste većim dijelom su poznate po svojim karakteristikama potrošnje male količine energije. Neke od tehnologija koje se koriste biti će ukratko opisane u nastavku poglavlja.

3.2.1 Radio frekvencijska identifikacija

RFID (eng. *Radio-frequency identification*) je komunikacijska tehnologija koja se sastoji od RFID čitača, antene, sustava za obradu podataka i RFID transponder (eng. *transmitter/responder*) - tag koji je nositelj informacija za identifikaciju i praćenje objekta. RFID tehnologija omogućava funkcioniranje sustava bez izravne optičke vidljivosti i po bilo kakvim vremenskim uvjetima kao i istovremeno očitavanje više tagova. Velika raznolikost RFID sustava omogućuje izrazito velik broj primjena, koji s vremenom i tehnološkim napretkom sve brže raste [12].

Mogućnosti korištenja RFID tehnologije su brojne, od industrijskih pogona i proizvodnje, skladišta, pa isto tako i unutar pametnih kuća. RFID u okruženju pametnog doma može se koristit kao sustav koji se služi kod identifikacije osoba prilikom ulaska u prostorije. Osobe sa sobom u nekom obliku nose čitače, to može biti privjesak za ključeve ili nešto slično, prilikom ulaska u prostoriju, osoba prisloni čitač na tag te sustav zna dali da otvori vrata, upali svijetlo ili obavi neku drugu aktivnost. Već ovdje moguće je za primjeriti kako postoje sigurnosni nedostaci takvog sustava.

Zbog nedostatka autentifikacijskih mehanizama u velikom broju RFID oznaka omogućava neovlašteni pristup sadržaju prometa koji se generira putem tih oznaka. Česti napadi kada je riječ i RFID oznakama su DoS napadi. Samim neovlaštenim pristupom napadač može potencijalno dobiti uvid u privatne informacije vlasnika kao što su brojevi telefona i kućne adrese [13].

3.2.2 ZigBee

ZigBee je standardizirani bežični komunikacijski protokol koji se koristi za povezivanje uređaja u IoT mrežama. Često se koristi kao komunikacijska tehnologija unutar okruženja pametnog doma. ZigBee se temelji na IEEE (eng. *Institute of*

Electrical and Electronics Engineers) 802.15.4 standardu. Glavna prednost ZigBee-a nad konkurentima je standardizacija između različitih proizvođača IoT uređaja koji koriste ZigBee tehnologiju komunikacije. Osim toga iz razloga što ZigBee komunikacijska tehnologija nema veliki domet, produljuje se vijek trajanja baterije uređaja [14].

Unutar ZigBee mreže postoje tri vrste uređaja: Koordinator, Usmjernik (eng. *Router*) i krajnji uređaj. Koordinator se ponaša kao administrator mreže, te je u većini slučajeva dovoljno jedan koordinator unutar ZigBee mreže. Najčešće *Hub* kao mrežni uređaj preuzima ulogu koordinatora, te on omogućuje povezivanje ostalih uređaja na Internet, ali i povezivanje ZigBee uređaja sa uređajima koji ne koriste ZigBee komunikacijski protokol [14].

Osim Koordinatora postoje i usmjernici, uređaji koji za svoje napajanje ne koriste baterije. Usmjernici komuniciraju sa svim ostalim uređajima unutar ZigBee mreže koji se nalaze u njihovom dosegu. Također unutar ZigBee mreže svaki uređaj koji se ne napaja na bateriju ima ulogu pojačivača signala te se na taj način širi ukupni doseg ZigBee mreže [14].

Posljednji uređaji ZigBee mreže su krajnji uređaji. To su uređaji koji za svoje napajanje koriste bateriju, oni nemaju mogućnost prosljeđivanja signala, te oni ne komuniciraju međusobno. Jedina komunikacija krajnjih uređaja je sa usmjernicima, te sa koordinatorima [14].

Neke od poznatih prijetnji sigurnosti ZigBee tehnologije su neovlašteno prikupljanje prometa, dekodiranje paketa i manipulacija sadržajem. Primjerice, neovlašteni pristup jednom senzorskom čvoru unutar ZigBee mreže daje pristup dijeljenom tajnom ključu mreže, a time i prometu unutar mreže. Uz poznate prijetnje pojavljuju se nove, poput sabotiranja krajnjih uređaja u ZigBee mreži s ciljem iscrpljivanja kapaciteta baterije te iskorištavanje procesa razmjene ključeva [13].

3.2.3 Bluetooth Low Energy

BLE (eng. *Bluetooth Low Energy*) je komunikacijska tehnologija koja se koristi za komunikaciju na kratkim udaljenostima, te pritom koristi malu količinu energije. Kao i

kod ranije spomenute ZigBee tehnologije, BLE se koristi u situacijama kada je važnije trajanje baterije od količine i brzine prijenosa podataka.

Jedna od prednost BLE tehnologije nad „klasičnom“ *Bluetooth* tehnologijom se može pronaći u situacijama kada nije potrebno konstantan prijenos podataka, već u nekim periodičnim intervalima. U tom slučaj krajnji rezultat je ponovo manja potrošnja energije, odnosno dulje trajanje baterija. Također prednost BLE-a nad *Bluetooth*-om je i ta što je kod BLE moguće ostvarenje do 20 simultanih konekcija dok *Bluetooth* ima mogućnost do sedam. To je moguće zbog prijenosa manje količine podataka. Upravo iz navedenih razloga moguće je primijetiti zašto se BLE koristi unutar IoT okruženja, bilo to industrijski pogoni ili okruženje pametnog doma [15].

Kada je riječ o BLE tehnologiji važno je za spomenuti BLE *Beacon* kao uređaj koji odašilje malu količinu podataka putem BLE komunikacijske tehnologije. Sam naziv „*Beacon*“ može se poistovjetiti sa svjetionikom iz razloga što konstantno odašilje signal koji je vidljiv ostalim uređajima u blizini. Način na koji se uređaji poput pametnih telefona povezuju sa *Beacon*-om je pomoću aplikacije. BLE *Beacon* odašilje identifikacijski broj koji pametni telefon u njegovoj blizini primi, te ukoliko već im instaliranu odgovarajuću aplikaciju dobiti će informacije koje mu Beacon pruža. Kao neke od primjera najčešće uporabe BLE *Beacon*-a možemo navesti: marketinške svrhe u šoping centrima i ostala oglašavanja, unutarnja navigacija koja se može koristiti primjerice unutar dućana za navođenje kupaca, ali isto tako i na kolodvoru [15].

3.2.4 6LoWPAN

6LoWPAN (eng. *IPv6 over Low-Power Wireless Personal Area Network*) predstavlja bežičnu komunikacijsku tehnologiju koja naglasak stavlja na nisku potrošnju energije, te svaki čvor u mreži posjeduje IPv6 adresu. To omogućuje da svi čvorovi mreže imaju mogućnost komuniciranja putem Internet protokola. Također kao i kod ZigBee komunikacijske tehnologije čvorovi su povezani u isprepletenu (eng. *Mesh*) mrežnu topologije što znači da je jedan čvor povezan sa više ili sa svima čvorovima unutar mreže te se na taj način omogućuje funkcionalnost cijelog sustav i u slučaju kada neki od čvorova prestanu raditi [16].

Neka od područja rada 6LoWPAN komunikacijske tehnologije su: područja automatizacije, monitoriranja unutar proizvodnje ili tvornica, unutar okruženja pametnog doma, te također i unutar okruženja pametnih gradova.

Kada je riječ o sigurnosti 6LoWPAN koristi AES (eng. *Advanced Encryption Standard*)-128 enkripcijski standard koji osigurava autentifikaciju i enkripciju. AES koristi simetričnu kriptografiju kako bi zaštitio prijenos podataka, što znači da koristi isti ključ i za kriptiranje i za dekriptiranje. Oznaka 128 označava da je riječ o duljini enkripcijskog ključa od 128 bita, odnosno broj mogućih kombinacija. Sam AES razvijen je početkom 21. stoljeće od strane NIST-a (eng. *The National Institute of Standards and Technology*) prvenstveno za Američku vladu, ali se kasnije standard počeo koristiti u svakodnevne svrhe, te danas AES standard koristimo pri povezivanja VPN-om (eng. *Virtual Privat Network*), kod Wi-Fi povezivanja, te različite aplikacije koriste AES kao način zaštite podataka [17].

3.3 Metode i alati napadača

Prilikom izvođenja samog napada napadaču su potrebni alati s kojima izvršava proces napada. Osim programskih alata potrebna je i ljudska aktivnost kako bi napadač došao do svog cilja bio on prikupljanje osjetljivih informacija, stjecanje neovlaštenog pristupa sustavu ili umetanje malicioznog koda unutar sustava [13].

Kada je riječ o alatima napadača važno je definirati dva pojma, a to su: vektori i vrste napada. Vektori napada predstavljaju kategorije unutar kojih se klasificiraju vrste napada, kao što je vidljivo u tablici 1.

Tablica 1: Vektori i Vrste napada

Vektori napada	Vrste napada
Umetanje malicioznog koda	• Virusi • Trojanski konji • Crvi
Web temeljeni	• *Cross-site scripting* (XSS) • *SQL injection*
Mrežno temeljeni	• Napad uskraćivanja usluga (DoS) • Distribuirani napada uskraćivanja usluga (DDoS) • Presretanje zaporki i osjetljivih informacija
Socijalni inženjering	• Lažno predstavljanje • *Phishing* • *Spear Phishing*

Izvor: [13]

3.3.1 Mrežno temeljeni napadi

Prema [18] napad uskraćivanja usluga, odnosno DOS napad možemo definirati kao napad, odnosno maliciozne aktivnosti napadača koje rezultiraju na način da onemoguće legitimnom korisniku dolazak do željenih podataka bilo da se radi o nekoj vrsti Internetske usluge, pristupu nekoj vrsti uređaja ili nekom drugom mrežnom resursu. Uskraćivanje usluga legitimnog korisnika omogućuju procesi kao što su preplavljivanje dijela mreže ili servera kako bi došlo do pada cijelog sustava ili kako bi se jednostavno spriječila mogućnost korištenja napadnutog sustava od strane legitimnog korisnika**.**

Napad uskraćivanja usluga nije uvijek krajnji cilj napadača. Postoje slučajevi kada je napad uskraćivanja usluga bio samo jedna komponenta cjelokupnog napada. Također poznati su takozvani simptomi DoS napada koje možemo podijeliti na [19]:

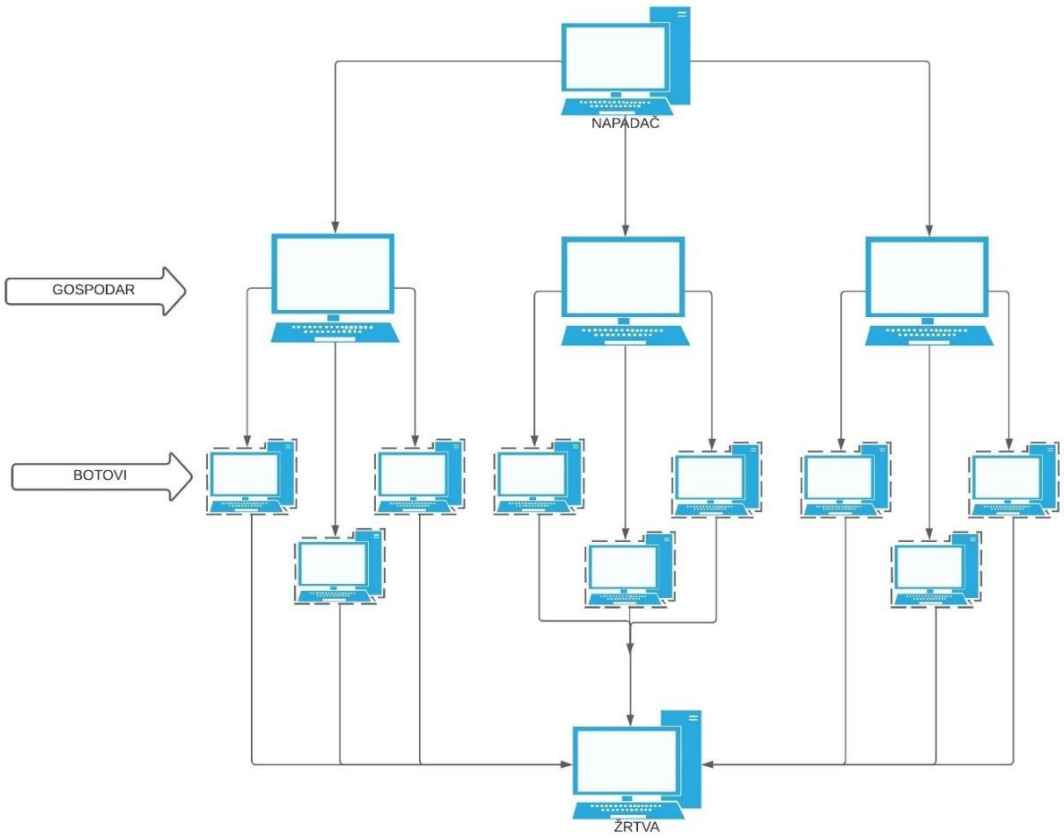
- Neuobičajena sporost mreže,

- Nedostupnost određene web stranice,
- Nemogućnost pristupa bilo kojoj web stranici,
- Drastično povećanje broja primljene neželjene elektroničke pošte.

Konstantnim razvijanjem tehnologije napadači pronalaze i nove načine izvođenja računalno kriminalnih radnji, među njima su i novi načini izvođenja DoS napada. Iako je nemoguće sve vrste napada detaljno okarakterizirati prema [19] postoje pet osnovnih tipova napada:

1. Potrošnja računalnih resursa, kao što su komunikacijski kapacitet, diskovni prostor ili procesorsko vrijeme,
2. Poremećaj konfiguracijskih podataka, kao što je usmjeravanje informacija,
3. Poremećaj informacija o stanju (eng. *state information*), kao što je neželjeno ponovno postavljanje TCP veze,
4. Poremećaj fizičke komponente mreže,
5. Prekid komunikacije između legitimnih korisnika, tako da oni više ne mogu komunicirati na odgovarajući način.

Distribuirani napad uskraćivanja usluga, odnosno DDoS napad nastaje kada više kompromitirani sustava poplavljuju resurse ciljanog sustava [19]. Slika 1 prikazuje glavnu razliku između DDoS i DoS napada koja je upravo u tome što kod DoS napada jedan kompromitirani sustav služi za napad na žrtvu, dok se kod DDoS napada na neki način kontroliraju brojni kompromitirani sustavi koji tada mogu generirati puno veću količinu prometa prema žrtvi. U današnje vrijeme kada je riječ o napada uskraćivanja usluga govori se upravo o DDoS napadu.



Slika 1. Prikaz arhitekture DDoS napada

Najčešći način na koji se odvija DDoS napada je da napadač pronalazi ranjivosti jednog sustava i iskorištava te ranjivosti kako bi preuzeo kontrolu nad tim sustavom. Tada taj sustav predstavlja gospodara (eng. *master*). Nakon tog koraka započinje komunikacija sa ostalim sustavima koji su ranjivi te se na njih učitavaju određeni alati pomoću kojih dobiva kontrolu za daljnje napade. Za te ostale kompromitirane uređaje u mreži postoje brojni nazivi, a neki od njih su „zombiji“ ili „botovi“. Također mreža koji ti uređaji zajedno sa gospodarom kreiraju naziva se „botnet“.

Česta meta DDoS napada su ranjivi poslužitelji, odnosno oni koji sadrže operacijske sustave i sistemske programe s poznatim ranjivostima, ne sadrže antivirusne programe, sadrže antivirusne programe, ali starijih inačica ili oni koji nisu na neki način ispravno konfigurirani.

Isto tako upravo su IoT uređaji česta meta DDoS napada razlog tome su upravo sigurnosni nedostaci IoT uređaja, ali isto tako i količina IoT uređaja. Jednom kada

napadač preuzme kontrolu nad velikim brojem IoT uređaja daje mu se mogućnost generiranja velike količine podataka prema željenoj meti.

MIRAI je primjer zlonamjernog softvera koji skenira mrežu tražeći IoT uređaje kao što je na primjer pametna žarulja. Ukoliko pronađeni IoT uređaji imaju tvornički konfigurirane pristupne podatke, MIRAI preuzima kontrolu nad njima i pretvara ih u „botove“ koje koristi za DDoS napad [20].

Pomoću MIRAI zlonamjernog softvera 2016. godine proveden je napad na „OVHcloud“ francusku kompaniju čija je temeljna djelatnost pružanje usluga računalstva u oblaku. Procjenjuje se da je u napadu korišteno otprilike 145 tisuća kompromitiranih IoT uređaja koji su generirali veliku količinu prometa. Sam napad trajao je sedam dana. Taj podatak prikazuje nepredvidivost i sofisticiranost MIRAI softvera [21].

Iz razloga čestih DDoS napada uzrokovanih IoT uređajima, ta tema postaje sve zanimljivija znanstvenicima u pronalasku rješenja detekcije DDoS napada. Tako je iz znanstvenog rada [22] moguće vidjeti ideju o klasifikaciji IoT uređaja unutar okruženja pametnog doma ovisno o tome koliko je predvidljiv promet kojeg ti uređaji generiraju prilikom svog svakodnevnog rada. Unutar rada različiti modeli detekcije koriste se ovisno o klasi IoT uređaja. Također rad dokazuje važnost prepoznavanja klase unutar koje se nalazi IoT uređaj radi što lakšeg uočavanja anomalija mrežnog prometa kojeg ti uređaji generiraju, te se na taj način može detektirati DDoS napad. Rad dokazuje predviđanje generiranog prometa u točnosti višoj od 99% što uvelike olakšava uočavanje anomalija, te samim time i detekciju DDoS napada.

3.3.2 Brute-force metoda

Brute-force metoda je poprilično jednostavna, ali i poprilično uspješna metoda koju koriste napadači kako bi saznali pristupničke podatke korisnika. Temelji se na metodi pokušaja i pogreške, što znači da napadači pokušavaju sa brojnim kombinacijama korisničkog imena i lozinke sve dok ne ostvare pristup sustavu. Metoda ne uključuje napadača koji ručno upisuje moguće kombinacije, već napadač koristi unaprijed sastavljene liste ili skripte lozinka. Liste su sastavljene od najčešće korištenih lozinka, ali i lozinke koje se često postavljaju kao tvornički postavljane od strane proizvođača.

Prilikom napada uspoređuju se lozinke unutar datoteke sa lozinkom mete napada sve dok se ne pronađe prava. *Brute-force* metoda ovisno o kompleksnosti lozinke može vrlo dugo potrajati, te iz tog razloga nije primjerena za sve situacije [23]. U nastavku rada pomoću *brute-force* metode pokušati ćemo ostvariti pristup testnom usmjerivaču pomoću kojega ćemo si pokušati omogućiti pristup LAN mreži.

3.5 Kriptografija

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Osnovna zadaća kriptografije je omogućiti komunikaciju između pošiljatelja i primatelja na način da se očuva tajnost sadržaja od entiteta, koji može biti: osoba, razni procesi i aplikacije, koji imaju mogućnost nadziranja promatranog komunikacijskog kanala [13].

Kriptografija ima široku uporabu u svakodnevnom životu iako ljudi koju ju i koriste nisu niti svjesni važnosti koju kriptografija ima. Kriptografski algoritmi dijele se na simetrične i asimetrične kriptografske algoritme koji će biti detaljnije opisani u nastavku poglavlja.

3.5.1 Simetrična kriptografija

Simetrična kriptografija je starija metoda kriptografije, ali i dalje korištena u velikoj mjeri. Simetrična kriptografija koristi jedan ključ za kriptiranje podataka i za dekriptiranje podataka. Prema tome i pošiljate i primatelj moraju imati ključ kako bi mogli komunicirati. Pošiljatelj prije slanja poruku kriptira, te se poruka šalje nesigurnim kanalom do primatelja. To je moguće iz razloga što ukoliko netko i presretne poruku neće ju moći pročitati bez ključa. Iz tog razloga je također vrlo važno da se sam ključ ne šalje istom porukom ili istim kanalom. Ključ se šalje drugim sigurnim kanalom do primatelja kako bi mogao dekriptirati poruku, te vidjet tekst u izvornom obliku [24].

Prema načinu kriptiranja simetrične kriptografske algoritme dijelimo na [24]:

1. Algoritme koji rade s blokovima (eng. *block cipher*) podataka – ulazni podaci kriptiranju se blok po blok. Često korištene duljine blokova su: 128, 192 ili 256 bita.

2. Algoritmi koji rade s tokovima (eng. *stream cipher*) podataka – ulazni podaci kriptiraju se bit po bit.

Primjeri algoritama koji koriste simetričnu kriptografiju su: *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES), *Transport Layer Security* (TLS) i *Secure Sockets Layer* (SSL).

DES algoritam spada pod algoritme koji rade s blokovima, te kriptira ulazne podatke u blokovima veličine 64 bita. DES se zbog svojih poznati mana, te slabosti u današnje vrijeme više gotovo pa i ne koristi [25].

Za razliku od DES algoritma AES je napredniji enkripcijski algoritam koji se smatra iznimno učinkovitim i sigurnim. AES također spada pod algoritme koji rade s blokovima, ali za razliku od DES-a koji koristi blokove duljine 64 bita, postoje više inačica AES algoritma ovisno o duljini ulaznog bloka. Pa tako postoji AES - 128, AES - 192 i AES – 256 [26].

TLS algoritam najčešće se koristi za enkripciju podataka komunikacije između poslužitelja i web aplikacija. Svoju primjenu pronašao je i kod email komunikacije i *Voice over IP* (VoIP) komunikacije. Predložen je od strane IEFT (eng. *Internet Engineering Task Force)* internacionalne standardizacijske organizacije 1999. godine, te danas se koristi treća inačica TLS algoritma, TLS 1.3, koji je objavljen 2018. godine [27].

TLS je nastao na primjer SSL kriptografskog algoritma koji se danas slabije koristi, a glavna zadaća mu je bila osigurati privatnost i cjelovitost podataka, te omogućiti autentifikaciju.

Implementacijom TSL algoritma na HTTP (eng. *Hypertext Transfer Protocol*) protokol nastaje sigurni HTTPS (eng. *Hypertext Transfer Protocol Secure*) protokol koji je danas u širokoj upotrebi. Većina korisnika kada pretražuje Internet ne obraća pažnju na to dali stranica koju posjećuju koristi HTTP ili HTTPS protokol, ali taj jednostavan način može korisniku odgovoriti na pitanje koliko su njegovi privatni podaci koje je ostavio na toj Internetskoj stranici sigurni.

Način na koji TSL omogućuje sigurniju komunikacije započinje na način da web stranica ili aplikacija koja želi koristiti TSL mora najprije imat TLS certifikat. Certifikat

izdaje se od autorizirane strane koja na taj način garantira pouzdanost korisnicima stranica.

TLS konekcija uspostavlja se takozvanim TSL rukovanjem (eng. *TLS handshake*). Proces TLS rukovanja započinje kada korisnik, odnosno uređaj sa kojim pristupa web stranici koja koristi TLS algoritam. Pomoću TLS rukovanja uspostavlja se komunikacija, te se pritom dogovaraju detalji, kao na primjer koji će se enkripcijski ključ koristiti tijekom komunikacije [27]. Proces TLS rukovanja biti će objašnjen također i na primjeru u praktičnom dijelu rada.

3.5.2 Asimetrična kriptografija

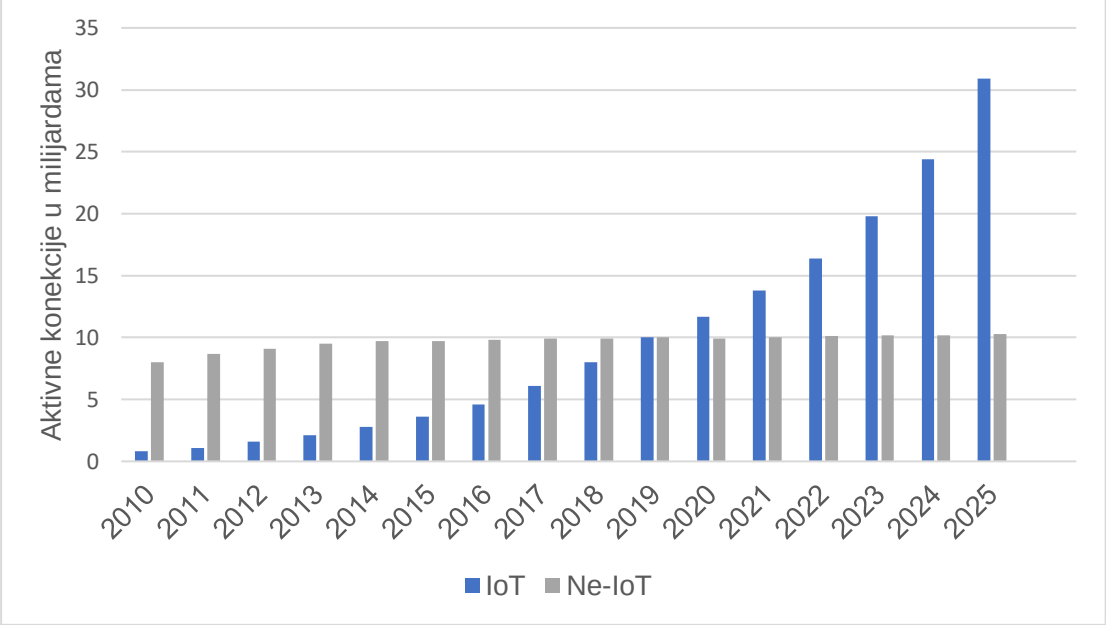
Za razliku od simetrične kriptografije koja koristi jedan ključ i za enkripciju osjetljivih podataka i za dekripciju tih istih podataka, asimetrična kriptografija koristi dva ključa koji se nazivaju privatni i javni ključevi. Način na koji se odvija komunikacija pomoću asimetrične kriptografije može se objasniti primjerom. Ukoliko imamo korisnika A i korisnika B koji međusobno žele komunicirati, podijeliti će si međusobno javne ključeve. Korisnik A kada želi poslati kriptiranu poruku korisniku B, poruku koju želi poslati kriptira pomoću javnog ključa korisnika B. Korisnik B pomoću svojeg privatnog ključa kojeg zna samo on može dekriptirati poruku. Jednom kada je korisnik A kriptirao poruku, čak niti on ju više ne može dekriptirati, već samo korisnik B sa svojim privatnim ključem.

Asimetričnom kriptografijom riješen je problem osiguravanja sigurnog kanala koji je potreban kod simetrične kriptografije za slanje ključa. Ali zbog veće duljine ključeva koji se koriste kod asimetrične kriptografije sam proces duže traje nego kod simetrične kriptografije.

3.5 Statistički pokazatelji sadašnjosti i budućnosti Interneta stvari

Broj IoT uređaja povezanih na Internet proteklih godina u eksponencijalnom je rastu, a jednaka su očekivanja i za budućnost. Grafikon 1 prikazuje omjer IoT uređaja i prema [28] takozvanih „ne IoT uređaja“. Pod IoT uređaje svrstani su uređaji povezani na Internet, te su podijeljeni u pojedine skupine: uređaji u automobilskoj industriji, uređaji koji se koriste u proizvodnoj industriji vezani uz proces robotizacije i autonomizacije. Isto tako pod IoT uređaje svrstani su i uređaji koji se koriste u okruženju pametnog doma koji će biti detaljnije opisani u nastavku rada. Kao predstavnici „ne IoT uređaja“ svrstani su pametni telefoni, prijenosna i stolna računala.

Grafikon 1. Omjer i rast IoT uređaja



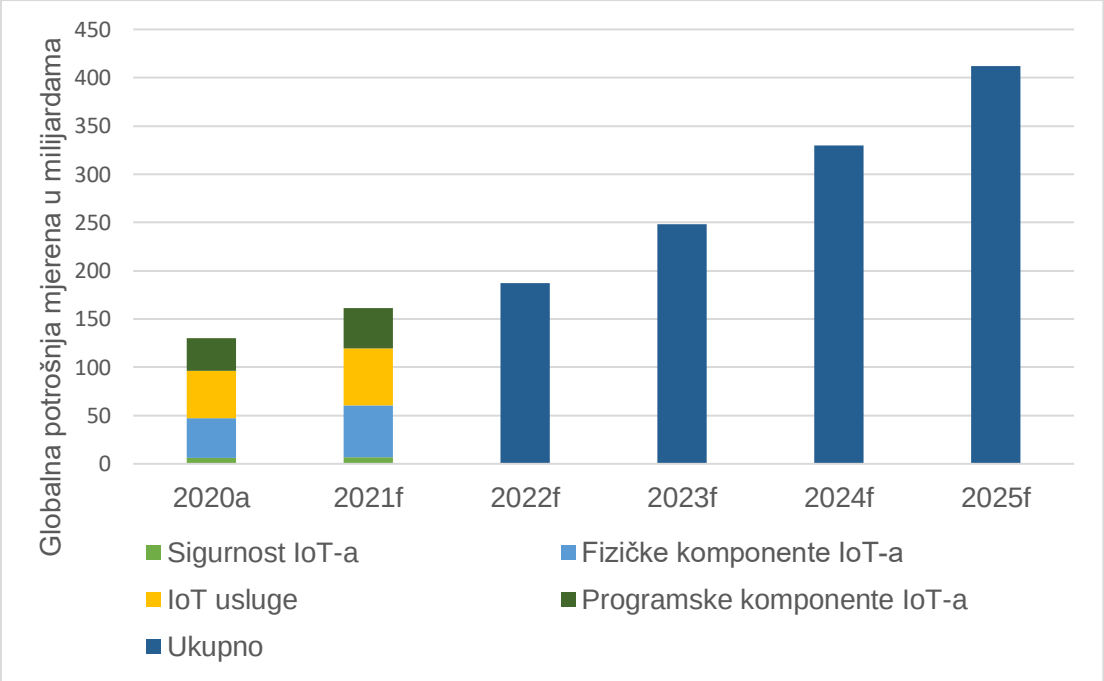
Izvor: [28]

Također je na grafikonu 1 vidljivo predviđanje da će do 2025 godine na Internet biti povezano čak 30.9 milijarde IoT uređaja. Još bržem rastu IoT uređaja doprinosi i širenje 5G mobilne mreže koja omogućuje manju latenciju te se to rezultira točnijim stvarnovremeni podacima.

Prema [29] ulaganje u IoT industriji raste unatoč pandemiji COVID-19. Grafikon 2 prikazuje u ulaganja proizvođača od 2020. godine do 2025. godine u milijardama dolara. Također za godine 2020. i 2021. prikazano je ulaganje prema segmentima:

sigurnost, hardware, razvoj budućih rješenja i software. Za budućnost predviđa se linearan rast ulaganja. Neki od segmenata kao što su ulaganje u cloud infrastrukturu i sigurnost u području IoT-a unatoč pandemiji COVID-19 nastavili su rast. Na poteškoće je naišao segment proizvodnje fizičkih uređaja zbog nedostatka sirovine. Iako je u porastu ulaganje u sigurnosni aspekt, još uvijek su ta ulaganja daleko manja nego u ostale aspekte pokrivene ovim istraživanjem.

Grafikon 2. Prikaz istraživanja ulaganja kompanija vezana za IoT tehnologiju



Izvor: [29]

Kada je riječ o statističkim podacima vezanih uz sigurnosni aspekt Interneta stvari prema [30] 2018. godine 813 milijuna IoT uređaja bila je meta malicioznih incidenata. Te brojke narednih godina su u velikom porastu, te tako već 2019. godine broj je narastao na dvije milijarde i 900 milijuna IoT uređaja koji su bili meta bilo kakvih malicioznih napada.

Prema istom izvoru navedeno je kako su upravo Usmjerivači najčešća meta napadnutih uređaja iz razloga što usmjerivači imaju funkciju pristupnika, te se pomoću njih IoT uređaji povezuju na Internet.

Unutar područja sigurnosti IoT uređaji ne spominju se samo kao mete napadača. IoT uređaji imaju i svoju ulogu kao uređaji pomoću koji se provode sigurnosne mjere kako bi se sustavi učinili što sigurnijima. Prema [31] 7.7% od ukupnog broja IoT uređaja koriste su unutar sigurnosnih sustava. Sigurnosni sustavi današnjice u potrebi su stvarnovremeno komunicirati jedini sa drugima, te iz tog, ali i drugih razloga koriste se IoT uređaji. Brojni senzori, brave i razni biometrički uređaji samo su neki od IoT uređaja koji se svakodnevno koriste u sigurnosnim sustavima.

4. Analiza ranjivosti uređaja u okruženju pametnog doma

Unutar ovog poglavlja biti će opisan pojam penetracijskog testiranja, te biti će navedene faze penetracijskog testiranja. Isto tako raspisana je metodologija analize i konfiguracija uređaja koji će biti korišteni unutar samog istraživanja. Također praktičnim primjerima biti će opisani neki od postupaka iskorištavanja ranjivosti IoT uređaja.

4.1 Penetracijsko testiranje

Penetracijsko testiranje definira se kao tehnika procijene sigurnosti računalnog sustava ili mreže koja se temelji na oponašanju stvarnog napada. Prilikom testiranja, ovlašteni ispitivač provjerava metu izvodeći različite vrste napada jednakim tehnikama koje bi koristio i da je stvarni napadač. Cilj mu je uočiti bilo kakvu ranjivost koju je moguće iskoristiti za ostvarenje neovlaštenog pristupa [32].

Brojne kompanije prilikom dizajniranja samog sustava nisu obraćale dovoljno pažnje na sigurnost, te je penetracijsko testiranje rješenje koje im omogućuje informacije koliko je njihov sustav siguran. Pronalazak sigurnosnih mana prije nego što se dogodi neočekivani i neželjeni sigurnosni propust vrlo je važno za kompanije u današnjem svijetu. Izvedba penetracijskih testiranja pronalazi slabosti sustava, te također izvođači testiranja pružaju informacije koje dijelove sustava je potrebno nadograditi i na koji način. Osim što kompanije dobivaju uvid u stanje sigurnosnog sustava, također prikazuje im se i moguća šteta koja nastaje prilikom stvarnog napada. Na temelju financijske magnitude koju neovlašteni napad može prouzročiti kompanije donose odluke koliko financijskih sredstava uložiti u poboljšanje sigurnosnih sustava. Nije dovoljno samo ulaganje u sigurnosnu infrastrukturu sustava, već je vrlo važno i ulaganje u edukaciju samih zaposlenika te uvođenje sigurnosnih pravila kojih se zaposlenici moraju pridržavati kao što su na primjer:

- promjena zaporki unutar određenog vremenskog perioda,

- zabrana donošenja privatnih prijenosnih medija iz razloga mogućnosti kompromitiranja sigurnosti sustava, ali isto tako i kopiranja podataka koji su u vlasništvu kompanije,
- korištenje poslovnih mobilnih uređaja na kojima su obuhvaćene određene mjere zaštite, te nemogućnost povezivanja privatnih mobilnih uređaja na korporacijsku mrežu.

Ovisno o željenom rezultatu testiranje postoje tri osnovne vrste penetracijskog testiranja [33]:

- *Black box* testiranje – ispitivači kod ovog načina testiranja nemaju nikakve informacije o samom sustavu nad kojim se vrši testiranje. Ponašanju se u potpunosti kao napadači, te se takva vrsta testiranja prvenstveno bavi istraživanjem vanjskih mogućih prijetnji koje bi napadači potencijalnog mogli iskoristiti prilikom stvarnog napada.
- *Gray box* testiranje – ispitivači kod ovog načina testiranja imaju određene podatke o samom sustavu. Kao što su pristupnički podaci, dijelove koda i algoritme sustava.
- *White box* testiranje – ispitivači kod ovog načina testiranja već imaju pristup cijelom sustavu nad kojim se vrši testiranje iz razloga kako bi u što kraće vremenskom periodu mogli dati što je moguće veći set podataka o trenutnom stanju sigurnosti cijelog sustava, ali isto tako i mogućnosti poboljšanja.

Ispitivači prilikom izvršavanja testiranja prolaze kroz određene faze. Iako je te faze moguće modificirati, te nisu jednake niti za sve izvođače niti za sve projekte u nastavku će biti navedena jedna od podjela faza penetracijskog testiranja [34]:

1. Izviđanje (eng. *Reconnaissance*) – izviđanje je faza unutar koje se prikuplja što je više moguće informacija vezanih uz metu napada. Načini na koje se prikupljaju podaci su raznoliki: pretraživanje Internet-a, informacije prikupljene putem DNS (eng. *Domain Name System*) poslužitelja, *social engineering*, pretraživanje mreže koje nije vidljivo meti napada, također je moguće pronaći vrijedne informacije metodom koja se naziva *Dumpster diving* odnosno pretraživanje „smeća“.

2. Identifikacija sustava (eng. *Scanning*) – identifikacija sustava je faza koja slijedi nakon što smo prikupili što je moguće više podataka vezanih uz metu napada. Penetracijskih testeri koriste razne alate kojima skeniraju sustav mete u potrazi za slabostima.
3. Ostvarenje pristupa (eng. *Gaining access*) – ostvarenje pristupa sustavu mete napada napadaču omogućuje razne mogućnosti. Sve ovisi o samom sustavu koji se napada, ali i do vrsti pristupa koji je tester ostvario. Tako na primjer testeri ukoliko ostvare potpun pristup sustavu imaju mogućnost brisanja, te izmjene podataka koji se nalaze unutar sustava.
4. Održavanje pristupa (eng. *Maintaining access*) – završna faza napadača prilikom gotovo svakog napada je omogućiti si ponovni ulaz na neprimjetan način.

Unutar istraživanja koje slijedi u nastavku primijenjena je vrsta *Grey box* testiranja iz razloga što je napadač prilikom istraživanja ranjivosti usmjerivača imao saznanja o MAC i IP adresi mete napada. Kod istraživanja Wi-Fi kamere je također napadaču bila poznata informacija naziva pristupne točke, ali ne i MAC adresa niti koji su sve uređaji bili u trenutku istraživanja povezani na pristupnu točku.

Od navedenih faza penetracijskog testiranja prve tri faze su korištene također u nastavku rada na samom istraživanju ranjivosti terminalnih uređaja u okruženju pametnog doma. U dijelu rada „sinteza rezultata istraživanja“ biti će detaljnije objašnjena pojedina faza.

4.2. Metodologija istraživanja

Istraživanje se provodilo unutar okruženja kućne LAN mreže pri čemu je korišten usmjerivač „INNBOX v45“ čija je konfiguracija vidljiva iz tablice 2.

Tablica 2. Konfiguracija usmjerivača „INNBOX v45“

Lokalno sučelje	• 1 port „Gigabit Ethernet 10/100/1000Base-TX (RJ-45)“ korišten kao LAN ili WAN • 4 porta „Fast Ethernet 10/100Base-TX (RJ-45)“ • 2 porta „FXS (RJ-11) za POTS konekciju“ • 2 porta USB 2.0
Wireless	• 802.11b/g/n 2×2 MIMO *access point*, 2.4 GHz • *Wi-Fi protected setup* (WPS) • WEP sa 64- ili 128-bita duljinom ključa • WPA/WPA2 u PSK modu • Kontrola pristupa ovisno o MAC adresi
Fizičke veličine	• 190 mm × 143 mm × 27 mm • 0.28 kg (bez strujnog adaptera)
Sigurnost i QoS	• URL filtriranje • NAT vatrozid • DMZ • VPN • Rezervacija *bandwidth*-a • Prioritiziranje glasovnog prometa

Izvor: [35]

Usmjerivač je korišten i kod analize ranjivosti samog usmjerivača, ali i kod analize ranjivosti pametne utičnice i analize Wi-Fi kamere iz razloga što su ti uređaji bili povezani putem usmjerivača na LAN mrežu u okruženju pametnog doma unutar kojeg se vršilo istraživanje.

Osim usmjerivača u istraživanju korišteno je i stolno računalo. Specifikacije računala vidljive su iz tablice 3.

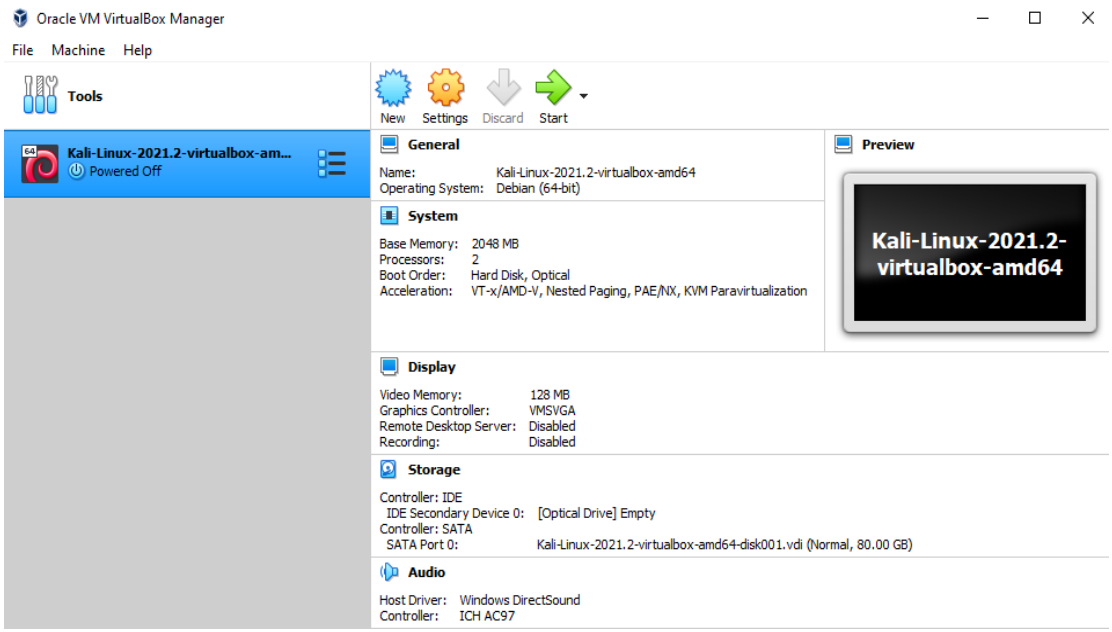
Tablica 3. Konfiguracija stolnog računala

Operativni sustav	• Windows 10 Pro • OS build: 19043.1165
Procesor	• Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz
RAM	• 12 GB
Grafička kartica	• NVIDIA GeForce GTX 760
Mrežna kartica	• Realtek PCLe GbE Family Controller

Stolno računalo također je korišteno i prilikom analize ranjivosti usmjerivača, kao i prilikom analize ranjivosti pametne utičnice i Wi-Fi kamere. Iako je operativni sustav stolnog računala „Windows 10 Pro“, prilikom analize korišten je drugi operativni sustav „*Kali Linux*“.

Kali Linux je distribucija Linux operativnog sustava temeljen na Debianu, te je prvenstveno namijenjen digitalnoj forenzici, penetracijskom testiranju i ostalim aktivnostima usko vezanih uz sigurnost informacijsko–komunikacijskih sustava. Kali Linux pojavio se 2013. godine te se od tada razvija sa novim alatima i mogućnostima [36].

U našem istraživanju „podizanje“ virtualne mašine Kali Linux operativnog sustava omogućeno je pomoću hipervizora „*Oracle VM VirtualBox*“, pritom je korištena verzija „6.1.22 r144080 (Qt5.6.2)“. *Oracle VM VirtualBox* je virtualizacijski *software* koji omogućuje korisnicima pokretanje više različitih ili istih operativnih sustava na istom fizičkom računalu. Pri tom procesu dijele se resursi tog fizičkog računala kako bi svi operativni sustavi mogli obavljati svoje funkcije. Sama konfiguracija koliko je određenih resursa dodijeljeno određenoj virtualnoj mašini postavlja se manualno te je na izbor korisnika. Slika 2 prikazuje grafičko sučelje *Oracle VM VirtualBox* hipervizora.



Slika 2. Izgled sučelja Oracle VM VirtualBox hipervizora

Također vrlo važan uređaj koji je korišten prilikom istraživanja je TP-LINK(TL-WN722N) USB (eng. *Universal Serial Bus*) Wi-Fi adapter.

USB Wi-Fi adapter je uređaj potreban za istraživanje iz razloga što je tijekom istraživanja bio konfiguriran na način da omogućuje komunikaciju između Kali Linux operativnog sustava sa ostalim uređajima putem Wi-Fi bežične mreže. Bitna stavka kod odabira USB Wi-Fi adaptera za izvođenje ovakve vrste testiranja je da podržava „*Monitor mode*“, odnosno način rada koji omogućuje prikupljanje i monitoriranje prometa koji se prenosi bežičnom mrežom koja se u tom trenutku osluškuje [37]. Primjena monitor moda biti će prikaza u nastavku rada. Slika 3 predstavlja usmjerivač i USB Wi-Fi adapter korišteni tijekom istraživanja.

Slika 3. Usmjerivač i USB Wi-Fi adapter korišteni u istraživanju

Za dio istraživanja vezan uz analizu ranjivosti pametne utičnice korištena je Smart Plug model: SM-PW734E pametna utičnica. Slika 4 prikazuje pametnu utičnicu koja je korištena u svrhu istraživanja.

Slika 4. Pametna utičnica korištena u istraživanju

Pametna utičnica koristi Wi-Fi tehnologiju povezivanja, te pritom koristi 2.4GHz frekvencijski pojas. Sa korisničke strane upravljanje samom pametnom utičnicom omogućeno je pomoću mobilne aplikacije koju je potrebno preuzeti na pametni telefon. Pametna utičnica omogućuje funkcionalnosti kao što su na primjer: paljenje i gašenje uređaja koji je uključen u pametnu utičnicu iz daljine bez da je potrebno doći fizički skroz do nje, također postoji i vremenska odgoda kada će se pametna utičnica upaliti, odnosno ugasiti.

Završni dio praktičnog dijela istraživanja odvijao se na Wi-Fi kameri proizvođača Xiaomi. Kamera koja je korištena proizvedena je u svrhu korištenja unutar vlastitog doma za osobne potrebe.

Postavljanje kamere temelji se na povezivanju sa kućnim usmjerivačem putem Wi-Fi IEEE 802.11 tehnologije, te se pritom koristi 2.4GHz frekvencijski pojas. Osim povezivanja sa usmjerivačem, odnosno povezivanja na kućnu mrežu, pokretanje i upravljanje kamerom obavlja se putem mobilne aplikacije koju je potrebno instalirati na vlastit pametni telefon.

Kamera ima mogućnost lokalne pohrane u obliku SD (eng. *Secure Digital*) memorijske kartice na koju može pohranjivati snimke. Također unutar kamere postoji i mikrofon koji omogućuje komunikaciju u dva smjera.

Slika 5 prikazuje Xiaomi „*Mi Home Security Camera Basic 1080P*“ koja je korištena u nastavku rada u svrhu istraživanja ranjivosti IoT uređaja na DoS napad.

Slika 5. Prikaz Xiaomi Wi-Fi sigurnosne kamere

4.3 Analiza ranjivosti Wi-Fi usmjerivača

Postupkom istraživanja sigurnosnih nedostataka Wi-Fi usmjerivača započinje testiranje ranjivosti terminalnih uređaja u okruženju pametnog doma iz razloga što ukoliko napadač uspješno izvede napad na usmjerivač kućne mreže te dobije pristup mreži, poprilično si je olakšao posao samog napada na terminalne uređaje unutar same mreže.

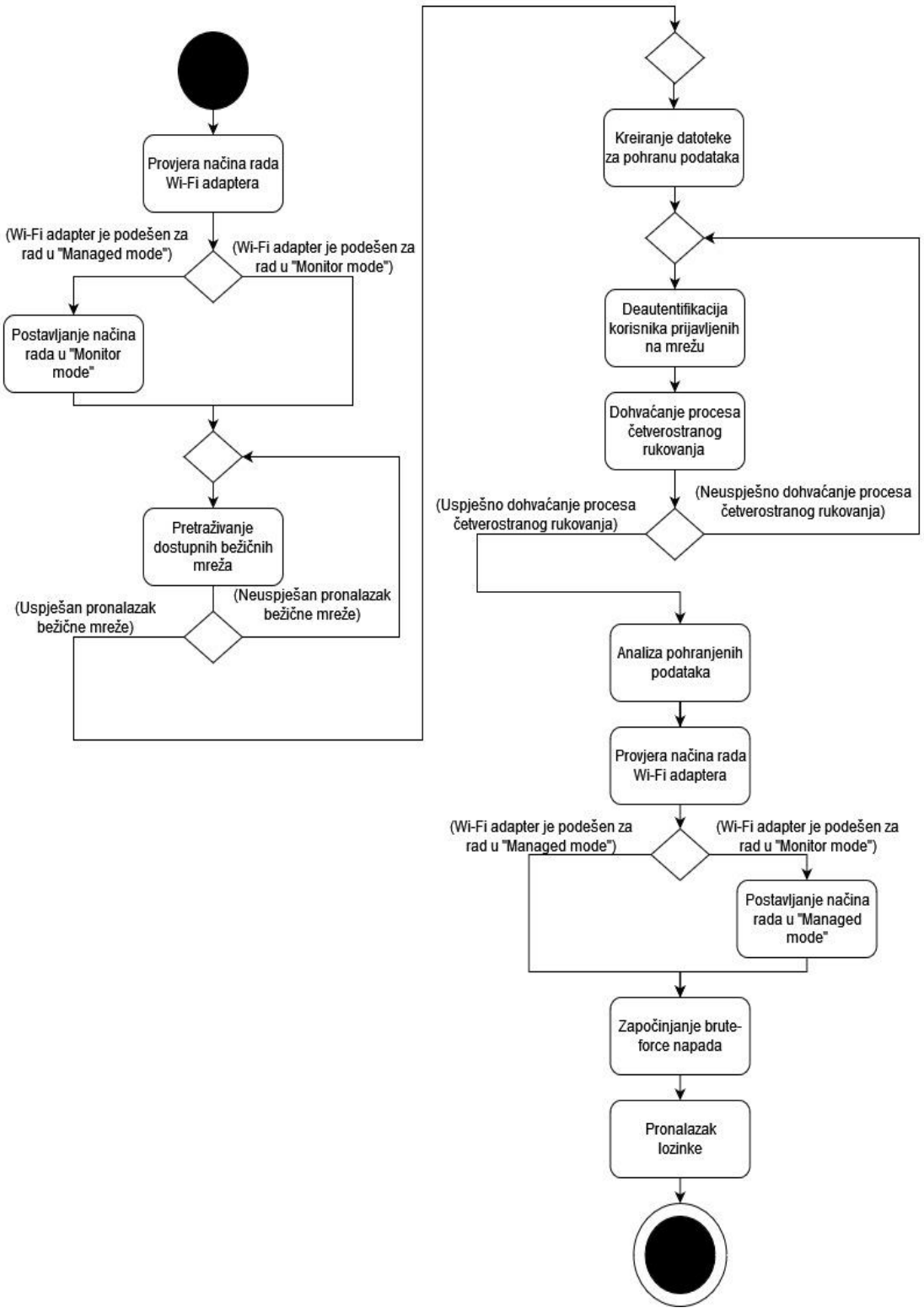
Proces koji će u nastavku biti detaljno opisan samo je jedan od načina kako je moguće pridobiti pristup privatnoj mreži putem Wi-Fi tehnologije. Proces se sastoji od nekoliko glavnih koraka koje je potrebno izvršiti, a oni su:

1. Pretraživanje dostupnih bežičnih mreža koje se nalaze u blizini.
2. Deautentifikacija korisnika koji su već prijavljeni na bežičnu mrežu koja je meta napada.
3. Dohvaćanje metode četverostranog rukovanja (eng. *Four-way handshake*).
4. Korištenje metode *Brute force* napada kako bi se pristupilo bežičnoj mreži.

Za potrebe testiranja promijenjena je lozinka usmjerivača kako bismo pokušali dokazati važnost snažnih lozinka. Isto tako iz razloga dokazivanja važnosti ispravo postavljenih sigurnosnih postavki, algoritam sigurne komunikacije unutar 802.11 komunikacijskog protokola maknut je sa WAP2 i postavljena je na WAP koji je zastario, te kod kojeg postoje određene sigurnosne mane. Također u testnom scenariju napadač prilikom pretraživanja dostupnih bežičnih mreža već unaprijed zna IP i MAC adresu mreže koja će biti meta, te naziv mreže.

Slika 6 prikazuje dijagram aktivnosti kojim se grafički prikazuju koraci analize. Proces napada započinje pretraživanjem bežičnih mreža u blizini WiFi adaptera. Jednom kada je pronađeno nekoliko bežičnih mreža, napadač identificira željenu mrežu i odabire ju kao metu napada. Slijedi proces identifikacije uređaja povezanih na odabranu pristupnu točku. Nakon identifikacije povezanih uređaja započinje se sa procesom deautentifikacije tih istih uređaja. Prije procesa deautentifikacije unaprijed je odrađena priprema kojom se žele prikupiti pristupni podaci jednom kada se ti uređaji pokušaju ponovno povezati na mrežu. Nakon dohvaćanja pristupnih podataka, podaci

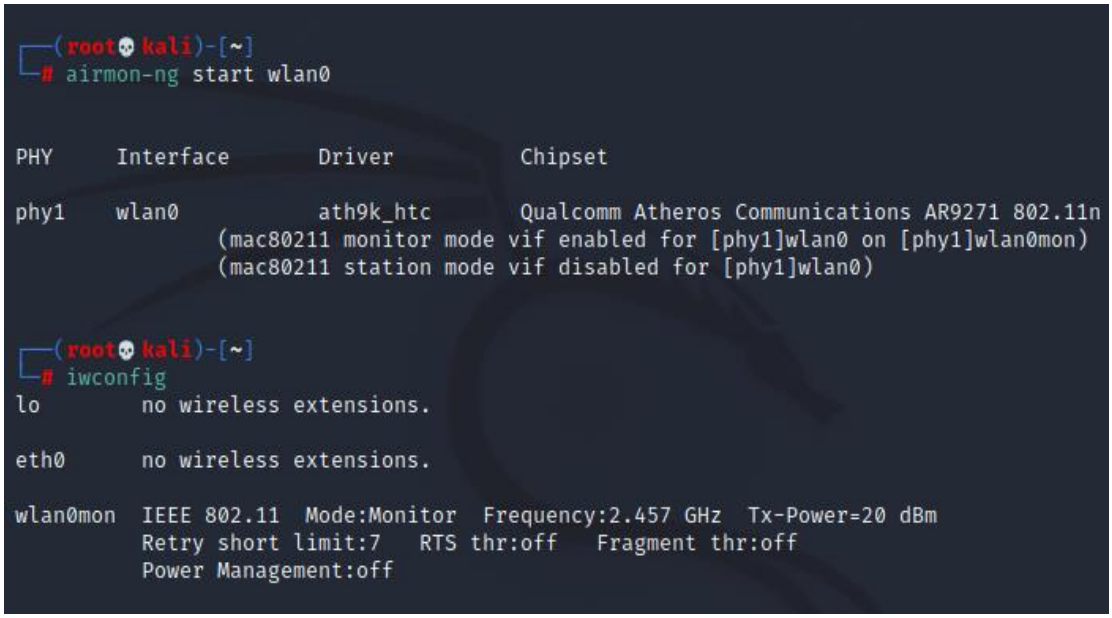
se analiziraju, te se *brute-force* metodom napada pokušava pridobiti pristup meti napada. Unutar nastavka poglavlja svi koraci biti i detaljnije opisani.



Slika 6. Dijagram aktivnosti analize ranjivosti usmjerivača

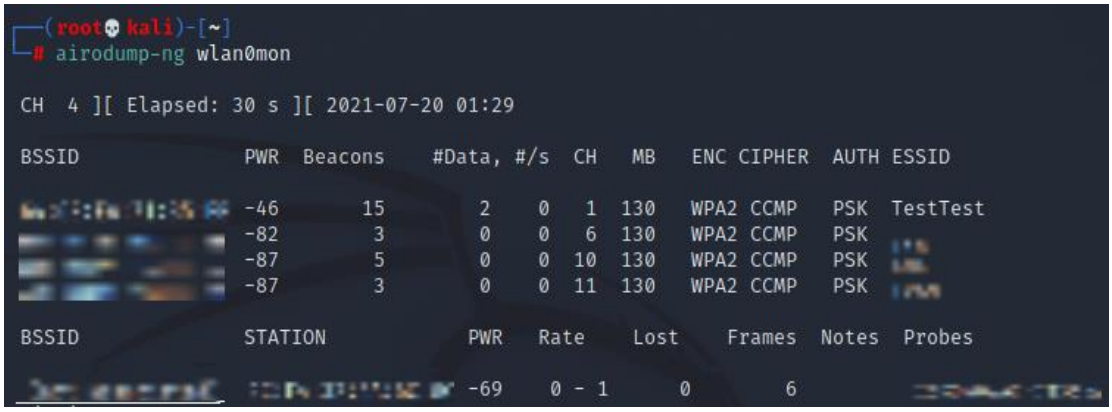
Prvi korak navedenog istraživanja bio je pretraživanje dostupnih bežičnih mreža koje se nalaze u blizini USB Wi-Fi adaptera. Prilikom konfiguriranja Kali Linux virtualnog okruženja USB Wi-Fi adapter podešen je za radu u „*Managed Mode*“ koji omogućuje njegovu osnovnu funkciju, odnosno komunikaciju sa uređajima koji se nalaze u blizini putem Wi-Fi bežične komunikacijske tehnologije.

U svrhu pretraživanja dostupnih bežičnih mreža u neposrednoj blizini potrebno je USB Wi-Fi adapter postaviti na *Monitor* način rada. Unutar Kali Linux Terminala upise se naredba „*airmon-ng start wlan0*“, te se na taj način pokreće *Monitor* način rada wlan0 mrežnog adaptera kao što je vidljivo na slici 7. Postavljanjem USB Wi-Fi adaptera u *Monitor* način rada onemogućuje mu se funkcija komunikacije sa drugim uređajima unutar mreže, te on sam se ponaša kao da više nije dio mreže unutar koje se nalazi. Iz tog razloga je moguće ovu simulaciju nastaviti kao da se napadač ne nalazi unutar mreže već napadač započinje napad prikupljanja pristupnih podataka usmjerivača.



Slika 7. Postavljanje mrežnog adaptera wlan0 u Monitor način rada

Nakon što je USB Wi-Fi adapter postavljen u *Monitor* način rada započinje proces pretraživanja bežičnih mreža koje se nalaze u blizini. Naredba koja to omogućuje je „*airdump-ng wlan0mon*“. Moguće je primijetiti kako je sada za wlan0 mrežni adapter potrebno dodati i sufiks „*mon*“ iz razloga što se nalazi u načinu rada monitoriranja. Slika 8 prikazuje pronađene bežične mreže.

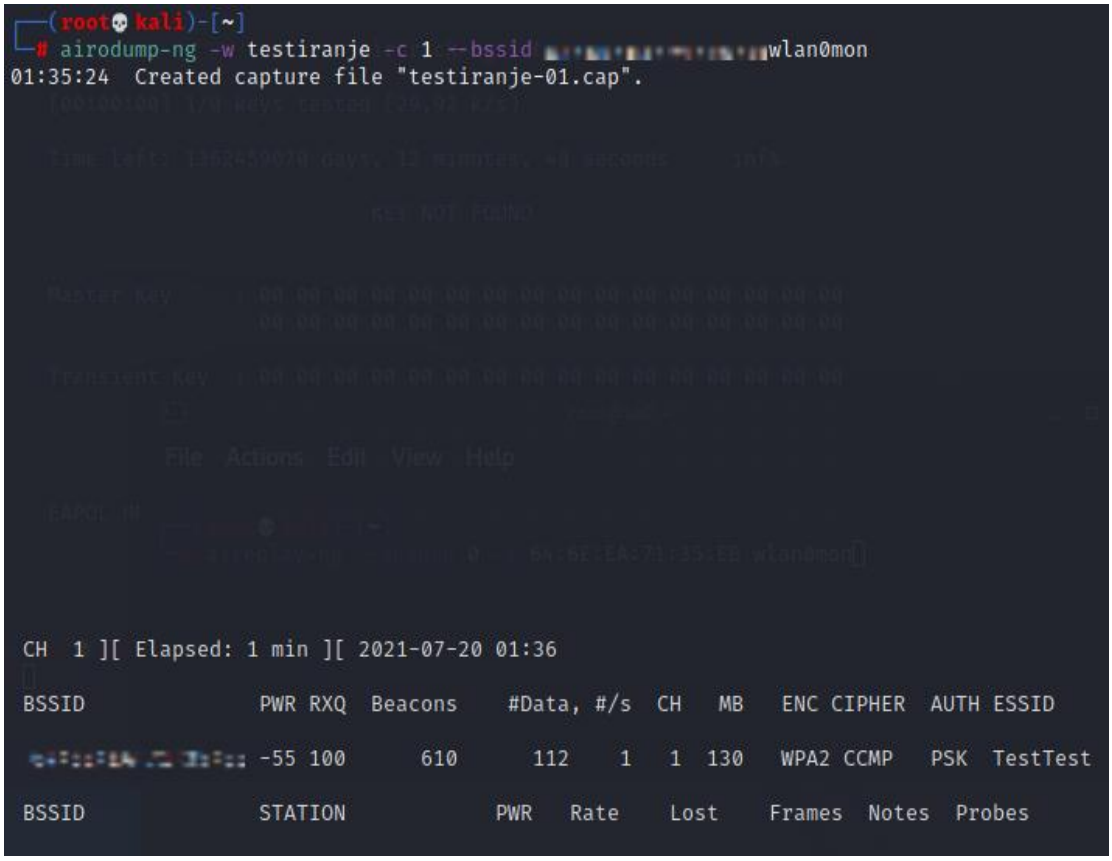


Slika 8. Prikaz pronađenih bežičnih mreža

Podaci koji su potrebni za nastavak testiranja su BSSID (eng. *Basic Service Set Identifier*), odnosno identifikator pristupne točke i kanal na kojem se odvija komunikacija. Uz BSSID važan pojam je i SSID (eng. *Service Set Identifier*), odnosno identifikator mreže. SSID ili ESSID (eng. *Extended Basic Service Set Identifier*) kao što je prikazan na slici 8 upravo je ono što korisnik vidi, kada se na primjer sa svojim pametnim telefonom želi povezati na bežičnu mrežu. Jedan WLAN (eng. *Wireless Local Area Network*) može biti sastavljen od više pristupnih točaka ovisno o veličini i konfiguraciji prostora, također materijala od kojih je sam prostor napravljen ili materijala predmeta koji se nalaze u prostoru. Ukoliko se korisnik fizički pomiče unutar WLAN mreže sa više pristupnih točaka njegov će se uređaj povezivati na bližu pristupnu točku bez da to korisnik primijeti u svom radu [38].

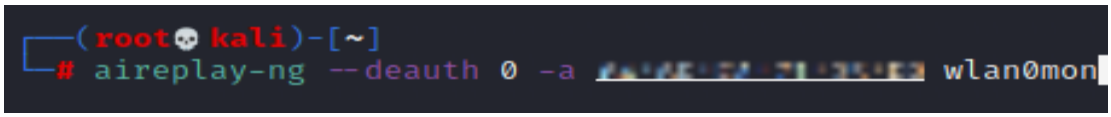
Također iz slike 8 moguće je vidjeti kako postoji uređaj pod poljem „*station"* koji je povezan na pristupnu točku za koju je cilj prikupiti pristupne podatke.

Sljedeći korak analize je deautentifikacija trenutno povezanih uređaja na pristupnu točku koja je meta napada. Razlog zbog kojeg se izvršava postupak deautentifikacije je taj što prilikom ponovnog pokušaja prijave uređaja doći će do procesa koji se naziva metoda četverostranog rukovanja kojom uređaji uspostavljaju komunikaciju. Također bitna stvar prije samog procesa deautentifikacije je kreacija datoteke unutar koje će se pospremati prikupljeni podaci pokušaja ponovne prijave uređaja na pristupnu točku. Naredba kojom se kreira datoteka unutar koje će se zabilježiti bitan promet izgleda „airodump-ng -w testiranje -c 1 –bssid [MAC adresa usmjerivača] wlan0mon". -W dio naredbe označava naziv datoteke unutar koje će zabilježiti promet kao što je vidljivo na slici 9.



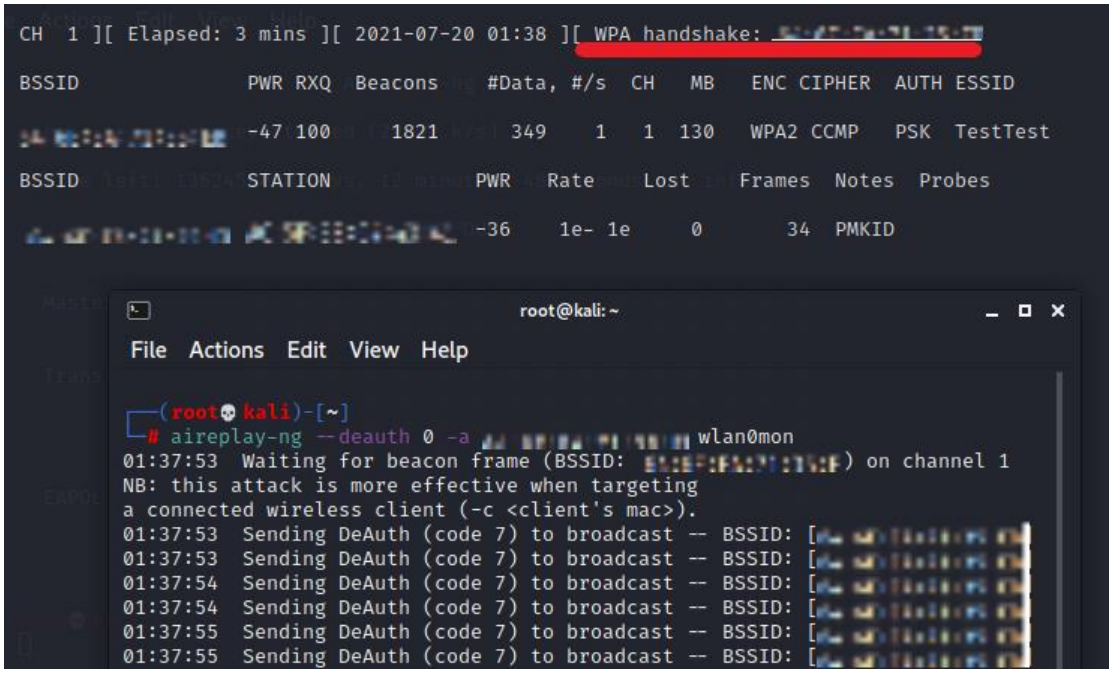
Slika 9. Prikaz naredbe za kreiranje datoteke „testiranje“

Nakon što je kreirana datoteka „testiranje“ započinje proces deautentifikacije trenutno povezanih korisnika. Naredba kojom se deautentificiraju korisnici je „aireplay-ng –deauth 0 -a [MAC adresa usmjerivača] wlan0mon“ kao što je vidljivo na slici 10.



Slika 10. Naredba deautentifikacije korisnika

Sljedeći korak je dohvat četverostranog rukovanja. Upravo nakon izvršenja naredbe deautentifikacije, čekajući da se uređaji ponovno pokušaju povezati se na pristupnu točku dohvaća se proces četverostranog rukovanja. Prikaz iz Linux terminala vidljiv je na slici 11.

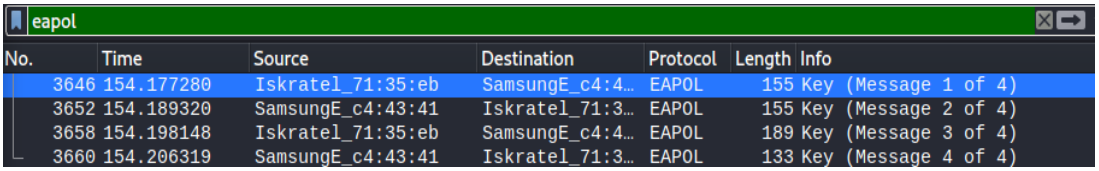


Slika 11. Prikaz da je uhvaćen WPA handshake

Korak koji slijedi je analiza promatranog prometa kroz alata koji se naziva „*Wireshark*“. Wireshark je alat koji se koristi za prikupljanje i analizu mrežnog prometa. Promet prikuplja u stvarnom vremenu, pohranjuje ga, te omogućuje daljnju analizu prikupljenog prometa.

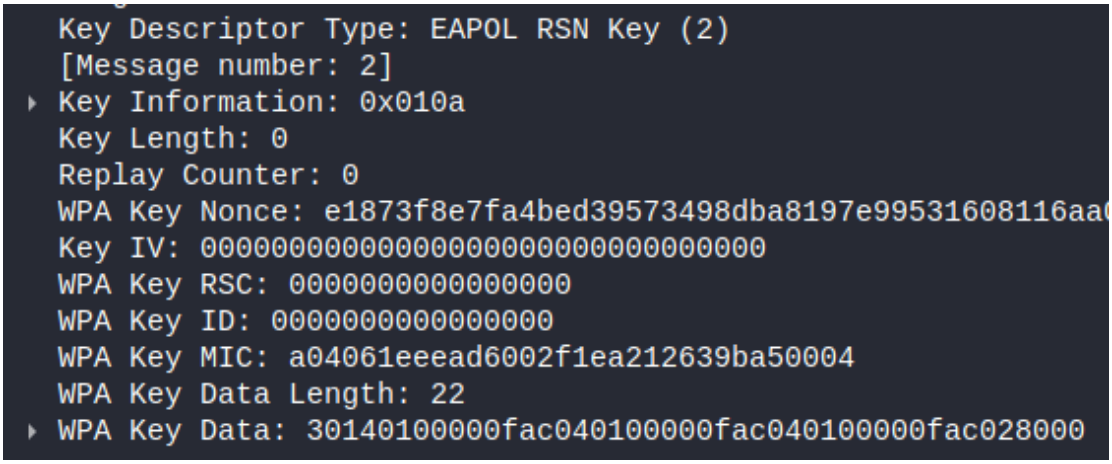
Prikupljeni promet potrebno je filtrirati kako bi se što je brže moguće pronašao željeni dio prometa, odnosno proces četverostranog rukovanja. Način na koji je moguće brzo pronaći željeni promet je filtriranje po protokolu EAPoL (eng. *Extensible Authentication Protocol over LAN*). EAPoL je protokol koji se koristi kod autentificiranja putem mrežnog porta [39].

Slika 12 prikazuje izgled Wireshark rezultata filtriranja prikupljenog prometa po EAPoL protokolu. Moguće je vidjeti da se radi o četiri koraka iste komunikacije, odnosno metodi četverostranog rukovanja.



Slika 12. Prikaz filtriranja prema EAPoL protokolu unutar alata Wireshark

Unutar druge od ukupno četiri razmijenjene poruke nalazi se „*WPA Key Data*“ odnosno autentifikacijska poruka poslana od uređaja koji želi pristup prema pristupnoj točci kako bi se izvršila autorizacija. Slika 13 grafički prikazuje izgled detalja druge od četiri poruke četverostranog rukovanja.

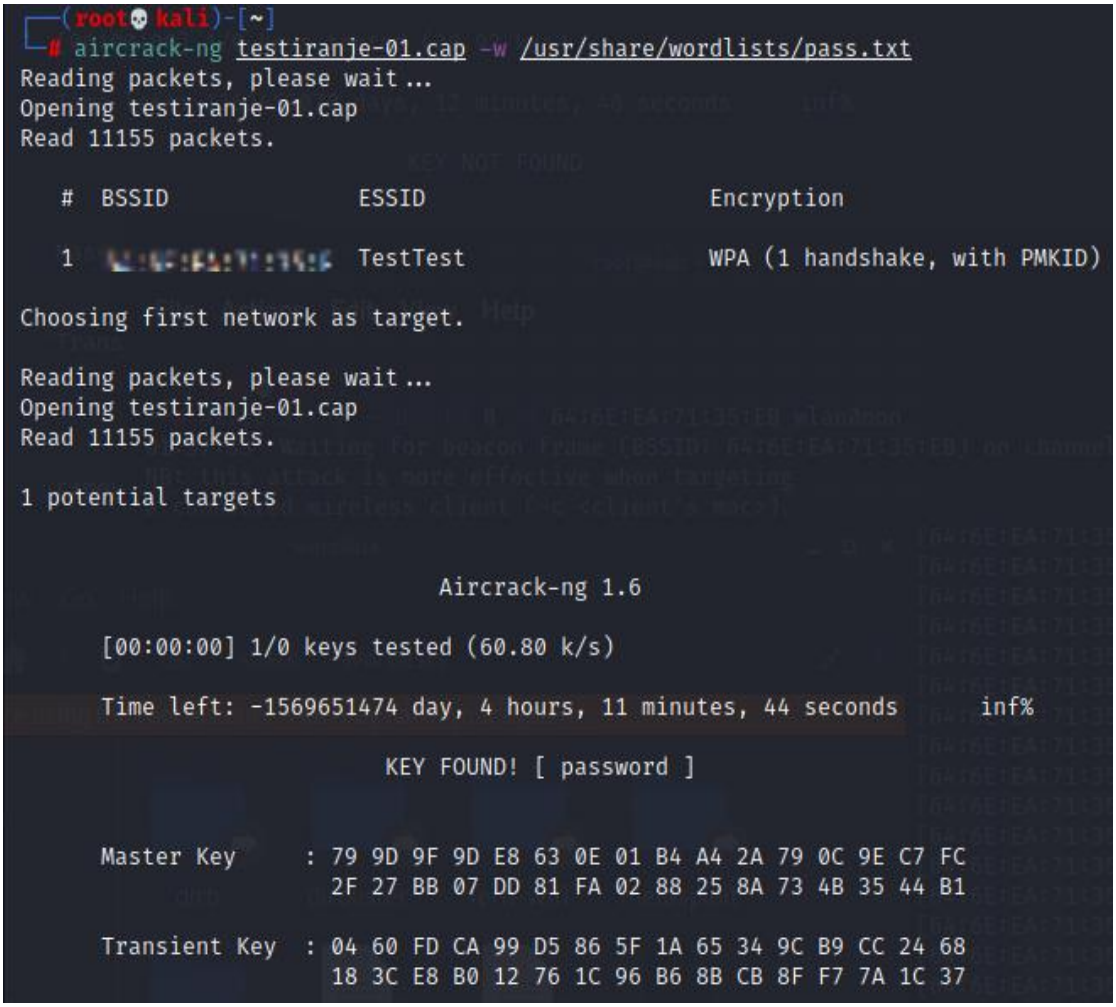


Slika 13. Grafički prikaz detalja poruke

Wireshark alat omogućuje dekriptiranje WPA (eng. *Wi-Fi Protected Access*) protokola. Na taj način moguće je ostvariti željeni pristup pristupnoj točki. Unutar istraživanja korištena je metoda *brute force* napada.

Prije početka *brute force* napada potrebno je Wi-Fi mrežni adapter vratiti iz *monitor* načina rada u *managed* način rada iz razloga što kada je Wi-Fi mrežni adapter postavljen u monitor način rada njegova zadaća je monitoriranje prometa, te nije u mogućnosti povezivanja na Internet ili ostale uređaje.

Naredba kojom se započinje *brute force* napad je „aircrack-ng testiranje-01.cap -w /usr/share/wordlists/pass.txt“, odnosno uz pomoć već unaprijed sastavljene liste najčešćih lozinka unutar dokumenta „pass.txt“ pokušava se pronaći lozinka koja je postavljena kao zaštita za povezivanje na pristupnu točku. Slika 14 prikazuje sam napad, te rezultat da je pronađena lozinka „password“.



Slika 14. Prikazuje pronađenu lozinku „password“

Nakon što je otkrivena lozinka napadač ima mogućnost potpunog pristupa Wi-Fi mreži, ali i mnogo više od toga. Svi uređaji povezani na istu napadnutu mrežu su u potencijalnoj opasnosti, te ostvarenje pristupa napadaču otvara brojne mogućnosti, a sve ovisi o prvenstvenom cilju napadača.

4.4 Analiza ranjivosti pametne utičnice

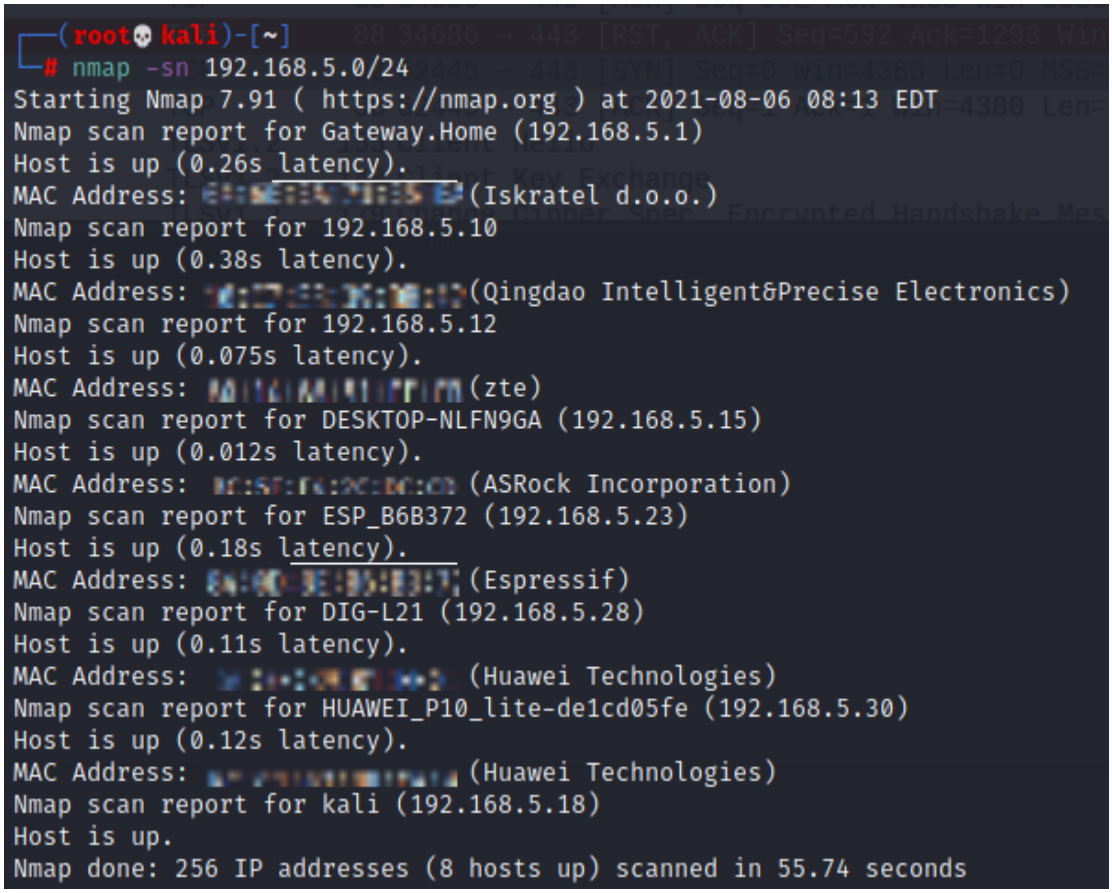
Analiza ranjivosti pametne utičnice nastavak je na prethodno poglavlje, te se simulacija nastavlja na scenarij kada napadač već ima pristup Wi-Fi mreži na koju je povezana pametna utičnica.

Napadaču je posao poprilično olakšan jednom kada već ima pristup mreži unutar koje se nalazi IoT uređaj koji je meta napada. U prvom koraku napada cilj je doći do IP i MAC adrese IoT uređaja koji je meta napada, u ovom slučaju pametne utičnice. Jednostavnom naredbom „ifconfig“ unutar Linux Terminala moguće je doći do IP adrese mrežnog adaptera povezanog na istu bežičnu mrežu na kojoj je i pametna utičnica. Na taj način dobiva se raspon IP adresa potrebnih za ovo istraživanje, iz razloga što se radi o IP adresi razreda C promatraju se prva tri okteta iz razloga što su oni rezervirani kao mreži identifikator. Kao rezultat toga identificirana je mreža koju je potrebno skenirati kako bi se otkrila informaciju koji se sve uređaji nalaze povezani na tu mrežu, pa tako i pametna utičnica.

Pronalaskom IP adrese mreže koju je potrebno skenirati koristeći alat „*Nmap*“ započinje proces skeniranja mreže u potrazi za svim povezanim uređajima na tu mrežu. Nmap je besplatan mrežni alat koji je dostupan za Windows, Linux i Mac operativne sustave. Glavne funkcije za koje se koristi alat Nmap su mrežno administriranje i skeniranje portova, ali postoje i ostale mogućnosti koje nudi alat Nmap [40].

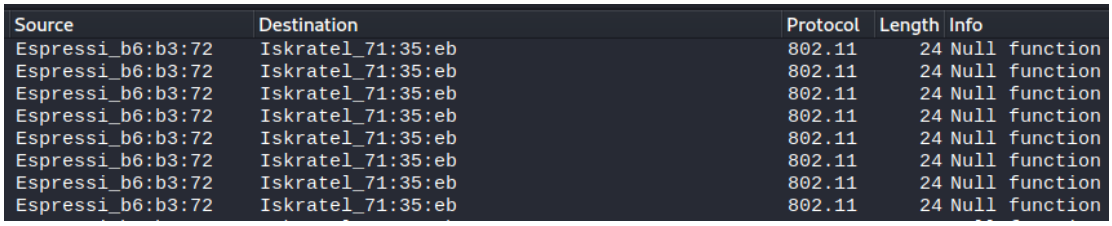
U provedenom istraživanju unutar Kali Linux Terminala naredbom nmap -sn, te mrežni dio IP adrese, odnosno mrežni identifikator, zatim na kraju dodajemo 0/24. Kao rezultat skeniranja dobivaju se svi uređaji povezani na mrežu kao što je prikazano na slici 15.

Slika 15 prikazuje sve uređaje koji su u trenutku skeniranja bili povezani na pristupnu točku mreže unutar koje se provodi istraživanje. Iz sigurnosnih razloga na slici su „zamućene“ MAC adrese uređaja.



Slika 15. Prikaz skeniranja mreže u potrazi za IP adresom mete napada

Nakon prikupljenih informacija o IP i MAC adresa mete napada, provodi se skeniranje mreže korištenjem Wireshark programskog alata. Skeniranje započinje sa također otprije poznatom naredbom „airodump-ng -w powersocket2 -c 1 –bssid [MAC adresa usmjerivača] wlan0mon“ koja skenira sva promet unutar testne mreže, te ga posprema unutar datoteke koja se naziva „powersocket2“. Alatom Wireshark omogućuje otvaranje navedene datoteke te je na slici 16 moguće vidjeti tko je pošiljatelj, a tko primatelj određenih podataka, ali je također vidljivo da je promet kriptiran.

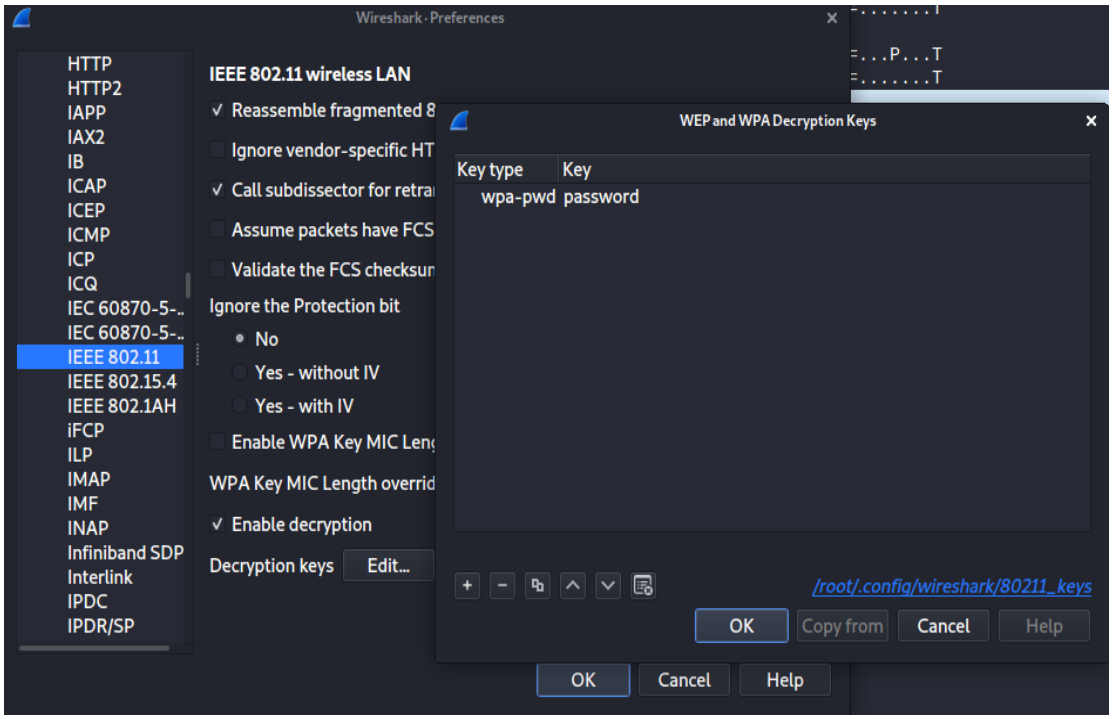


Source	Destination	Protocol	Length	Info
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function
Espressi_b6:b3:72	Iskratel_71:35:eb	802.11	24	Null function

Slika 16. Prikaz kriptiranog prometa

Kriptirani promet zadaje poteškoće kod očitavanja i analize prometa, te ga je potrebno dekriptirati. Slika 17 prikazuje konfiguraciju na koji način alat Wireshark omogućuje dekriptiranje. Prvo je bilo potrebno pronaći o kojem se protokolu radi, unutar ovog istraživanja riječ je o IEEE 802.11 što ujedno označava skupinu standarda za bežične mreže. Nakon pronalaska navedenog protokola potrebno je odabrati o kojoj je vrsti ključa riječ, odnosno koja vrsta ključa je rabljena prilikom proces kriptiranja. Istraživanjem pronađeno je kako je riječ o wpa-pwd (eng. *Wi-Fi Protected Access - password*) vrsti ključa koja kriptira promet prilikom metode četverostranog rukovanja.

Odabirom wpa-pwd ključa, potrebno je znati i pristupnu lozinku mreže. Taj podatak je poznat prethodnog poglavlja te ga napadač ima mogućnosti iskoristiti u ovom koraku kako bi si olakšao proces dekriptiranja prometa.



Slika 17. Prikaz Wireshark konfiguracije vezan uz dekriptiranje prometa

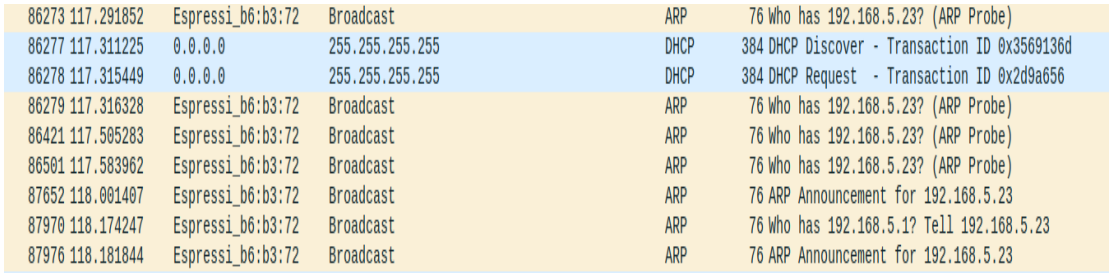
Jednom kada je promet dekriptiran napadač ima uvid u sve pakete koji se nalaze unutar promatrane mreže. Velike su mogućnosti na koji način napadač može zloupotrijebiti informacije koje su mu dostupne, te mogućnosti ovise prvenstvenom o samom cilju napadača.

Sljedećih nekoliko slika prikazati će samo neke od podataka u koje napadač ima uvid jednom kada se prikupljeni promet dekriptira. Slika 18 prikazuje razmjenu poruka prilikom četverostranog rukovanja. Napadač na taj način ima uvid ukoliko novi uređaj pristupa mreži.

Slika 18. Prikaz poruka četverostrukog rukovanja

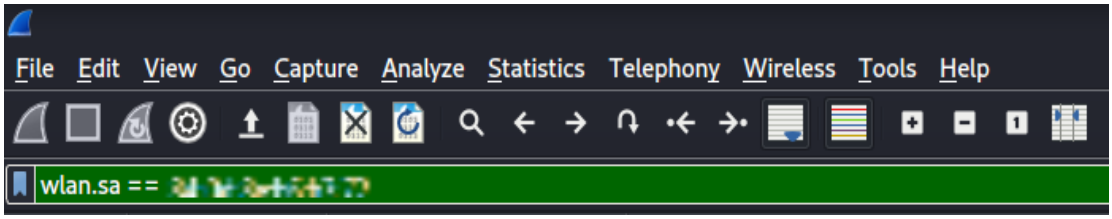
Zatim slika 19 prikazuje izmjenu ARP poruka. Kao što je ranije navedeno zadaća ARP protokola je povezivanje IP i MAC adresa uređaja te na taj način omogućuje komunikaciju. Na slici 19 je također vidljivo kako pametna utičnica šalje četiri *ARP Probe* poruke, te na taj na sve uređaje u mreži pita dali itko već koristi navedenu IP adresu. Ukoliko nitko ne odgovori, pametna utičnica će poslati *ARP Announcement* poruku također prema svima uređajima u mreži i naglasiti kako se ona od sada nalazi iza te IP adrese.

Isto tako moguće je vidjeti kako nakon što je naglasila svima da se ona nalazi iza IP adrese 192.168.5.23, zatražuje tko se nalazi iza IP adrese 192.168.5.1 kako bi dobila MAC adresu pristupnika, te kako bi mogla započeti komunikaciju.



Slika 19. Prikaz razmjene ARP poruka

Prilikom analize mrežnog prometa alatom Wireshark velik dio tog prometa nije toliko potreban napadaču prilikom napada, već u daljnjoj analizi pomoću tog prometa napadač može doći do raznih saznanja. Iz razloga što kada se analizira mrežni promet, u većini slučajeva je riječ o velikom broju paketa, Wireshark omogućuje filtriranje prometa koji služi bržoj i jednostavnijoj analizi. Slika 20 prikazuje način filtriranja prometa prema izvorišnoj adresi koja je od koristi za ovo istraživanje, za potrebe filtriranja korištena je MAC adresa pametne utičnice.



Slika 20. Prikaz filtriranja po izvorišnoj adresi unutar alata Wireshark

Nakon filtriranja prometa prema izvorišnoj MAC adresi pametne utičnice moguće je vidjeti razne poruke koje se prenose od strane mete napada. Na primjer na slici 21 vidimo kako pametna utičnica započinje komunikaciju sa uređajem IP adrese 18.185.182.159 porukom „*Client Hello*“ koja služi kao inicijalna poruka TLS rukovanja. Zatim slijedi razmjena ključeva kako bi se komunikacija kriptirala to je moguće vidjet porukom „*Client Key Exchange*“. Nakon što je završen proces TLS rukovanja slijedi prijenos podataka vidljivo porukama „*Application Data*“.

Source	Destination	Protocol	Length	Info
192.168.5.23	18.185.182.159	TLSv1.2	155	Client Hello
192.168.5.23	18.185.182.159	TLSv1.2	148	Client Key Exchange
192.168.5.23	18.185.182.159	TLSv1.2	179	Change Cipher Spec, Encrypted Handshake Message
192.168.5.23	18.185.182.159	TLSv1.2	429	Application Data
192.168.5.23	18.185.182.159	TLSv1.2	381	Application Data
192.168.5.23	18.185.182.159	TCP	88	23292 → 443 [ACK] Seq=853 Ack=637 Win=3744 Len=0
192.168.5.23	18.185.182.159	TCP	88	23292 → 443 [RST, ACK] Seq=853 Ack=637 Win=4380 Len=0

Slika 21. Prikaz TLS rukovanja i razmjene podataka kroz alat Wireshark

4.5 Analiza ranjivosti Wi-fi kamere

Cilj ovog istraživanja je dokazati da nije uvijek slučaj da se IoT uređaji koriste kao „pomagači“ kada je riječ o DDoS napadu, već i da sami mogu postati meta DoS napada.

Sljedećim koracima pokušati će se dokazati mogućnost onemogućavanja osnovne funkcije kamera, snimanja, pomoću DoS napada. Generiranjem prometa pokušati će se onemogućiti povezivanje kamere na mrežu, te na taj način i onemogućavanje prijenosa snimke.

Za razliku od već ranije provedenog istraživanja unutar kojeg se testirala sigurnost usmjerivača, te je sigurnosna postavka enkripcije bila postavljena na WPA, sada su

postavke postavljene na WPA2. Na taj način će se pokušati dokazati kako ni postavljanje enkripcijskog standarda neće biti u mogućnosti zaustaviti DoS napad.

Još jedan razlog zašto je spomenuto istraživanje provedeno na usmjerivaču je taj što se i unutar ovog istraživanja koristi Kali Linux operativni sustav. Ali i alati koje Kali sadržava, te su već korišteni u ranijim istraživanjima.

Tijek ovog napada možemo navesti kroz tri glavne faze:

1. Pronalazak dostupnih bežičnih pristupnih točaka,
2. Pronalazak uređaja povezanih na bežičnu pristupnu točku,
3. Slanje deautentifikacijskih poruka prema meti napada.

Ovo istraživanje također je analizirano pomoću virtualne mašine Kali Linux koja je pokrenuta pomoću hipervizora „Oracle VM VirtualBox“ na Windows 10 operativnom sustavu računala koji služi kao „domaćin“.

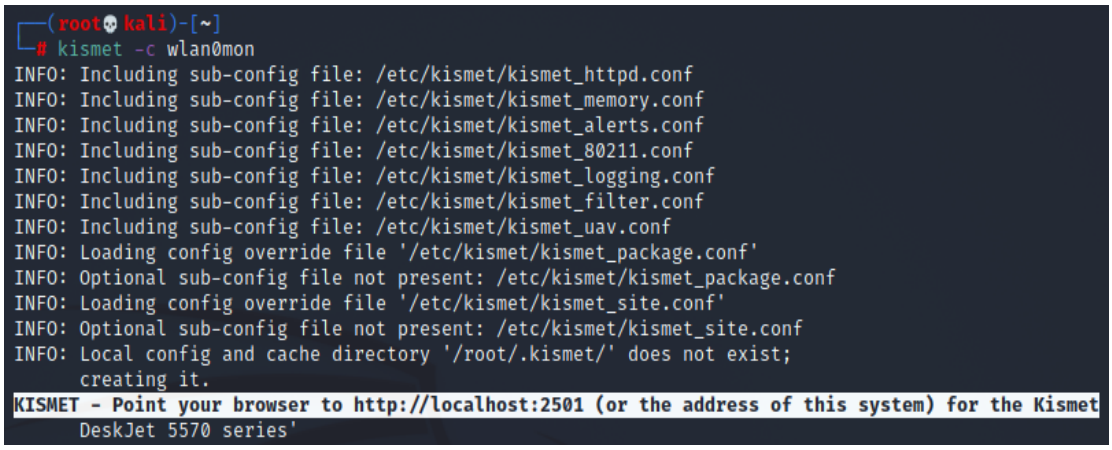
Osim Kali Linux-a i njegovih alata korišten je ponovno i Wi-Fi USB adapter pomoću kojeg se pretražuju pristupne točke, uređaji povezani na njih, ali i odašilje promet kojim se ometa normalan rad kamere.

Prva faza ove analize je pronalazak dostupnih bežičnih pristupnih točaka. Faza započinje na način da se Wi-Fi USB adapter postavlja u *Monitor* način rada iz razloga što je cilj ovog istraživanja simulirati napad kad napadač nema pristup mreži unutar koje se nalazi kamera koja je meta napada. Sama naredba postavljanja adaptera u *Monitor* način rada je već prikazana ranije. Isto tako i naredba airodump-ng kojom se pomoću alata „Aircrack“ pretražuju bežične mreže prikazana je prilikom istraživanja ranjivosti usmjerivača. Iz tog razloga tijekom izvedbe ove simulacije korišten je drugi alat iz ponude Kali Linux alata koji se naziva „Kismet“.

Kismet je alat koji omogućuje detekciju bežičnih mreža i uređaja povezanih na njih. Osim Wi-Fi načina komunikacije ima mogućnost rada i sa *Bluetooth* i SDR (eng. *Software defined radio*) komunikacijskim tehnologijama [41].

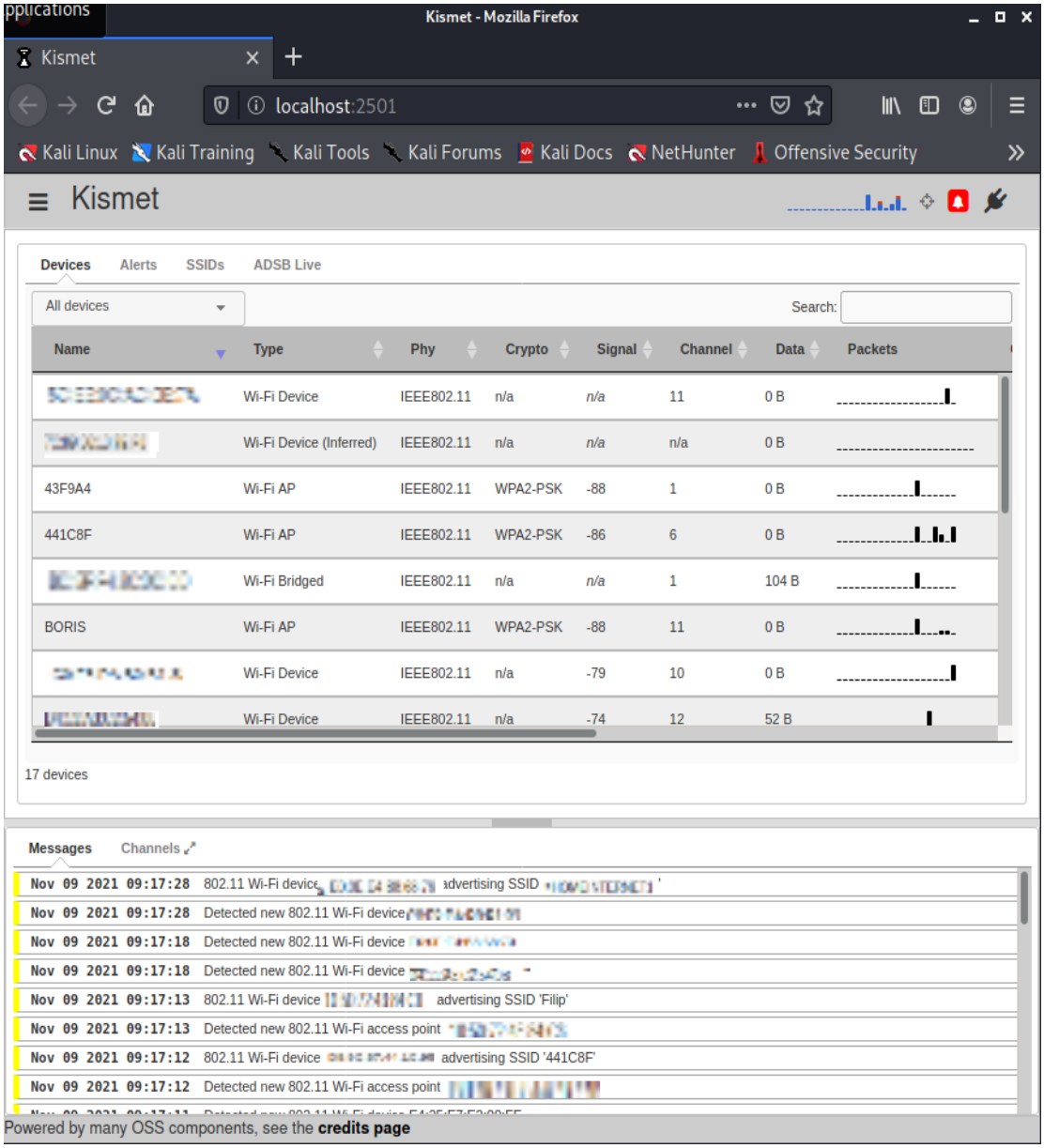
Kismet omogućuje i grafičko sučelje uz mogućnost pisanja naredbi kroz Kali terminal. Unutar ove demonstracije mogli bismo zaključiti kako se faze pronalaska bežičnih pristupnih točaka i faza pronalaska uređaja povezanih na te pristupne točke preklapaju. Iz razloga što alat Kismet naredbom koja je vidljiva na slici 22 „kismet -c

wlan0mon“ započinje traganje za bežičnim pristupnim točkama i ostalim uređajima u blizini USB Wi-Fi adaptera wlan0mon.



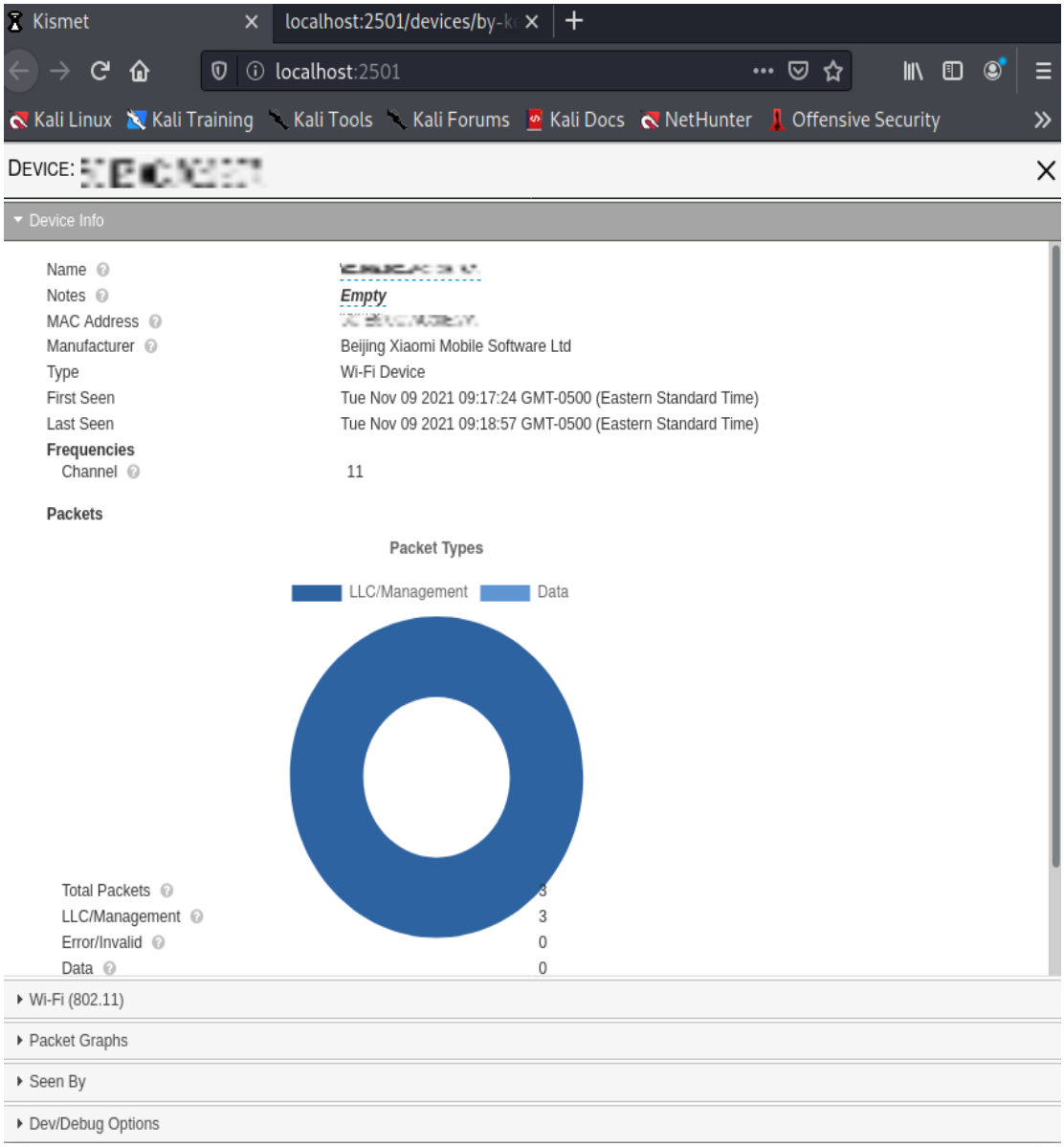
Slika 22. Prikaz pretraživanja bežičnih pristupnih točaka pomoću alata „Kismet“

Nakon što je alat Kismet pronašao pristupne točke i ostale uređaje u blizini adaptera, alat nudi i grafičko sučelje kroz web preglednik kao što je također vidljivo na slici 22. Slika 23 prikazuje grafičko sučelje alata Kismet. Za razliku od alata Aircrack, Kismet prikazuje još neke dodatne informacije o samim uređajima koje pronađe. Pa je tako moguće vidjeti imena uređaja, MAC adrese uređaja, komunikacijska tehnologija kojom uređaj komunicira, kanal na kojem uređaj komunicira, grafički prikazuje gustoću slanja paketa odnosno količinu razmjene paketa pojedinog uređaja, te još neke od dodatnih mogućnosti.



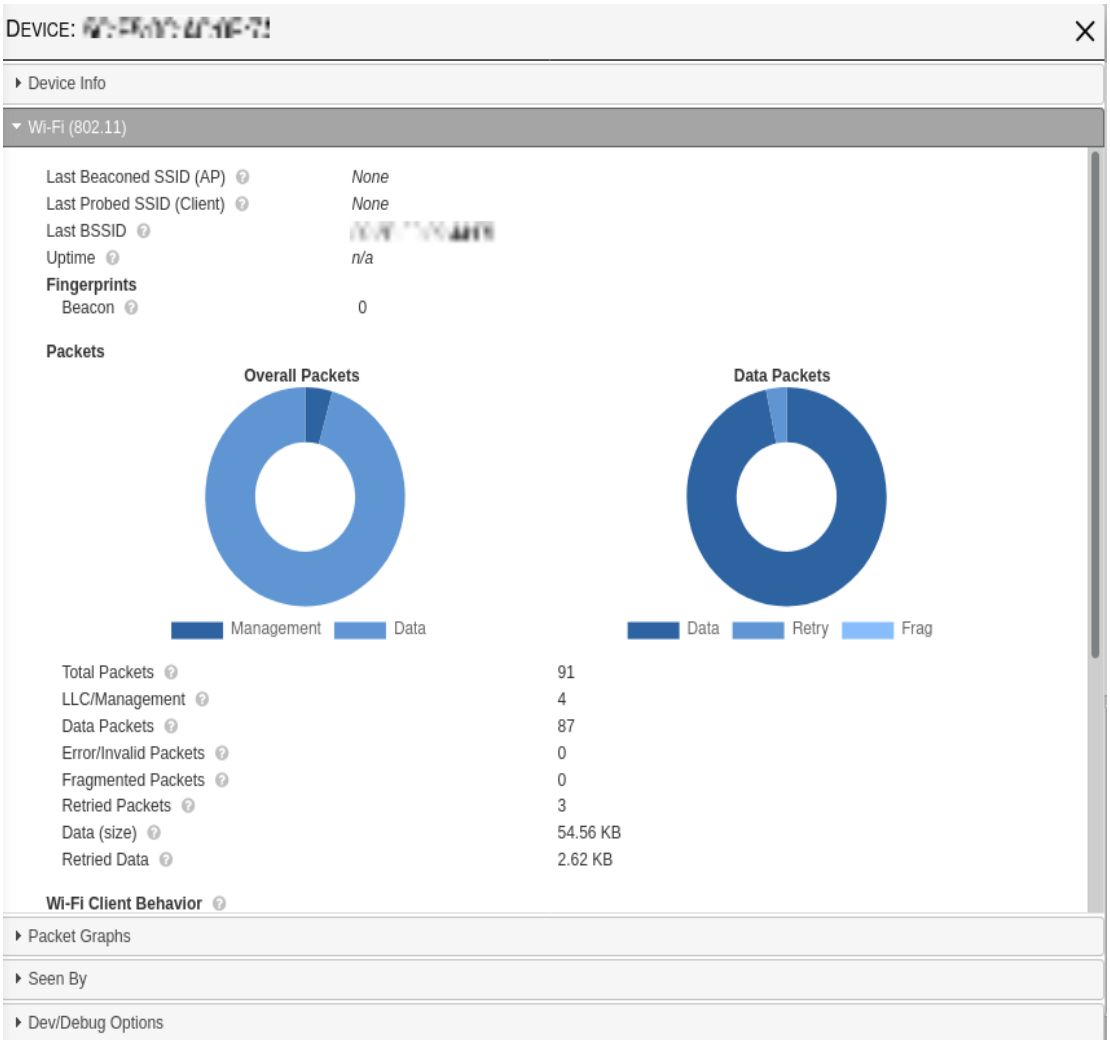
Slika 23. Grafički prikaz rezultat pretraživanja uređaja alatom Kismet

Unutar grafičkog sučelja metu napada moguće je najčešće pronaći pomoću naziva samog uređaja ukoliko naziv nije jednak MAC adresi ili pomoću dodatnih detalja koje nam nudi alat Kismet. Slika 24 prikazuje detalje uređaja koji je odabran iz glavnog dijela grafičkog sučelja te je moguće vidjeti pod stavkom proizvođač da je riječ o Xiaomi uređaju što dodatno potvrđuje kako je riječ o željenoj meti napada.



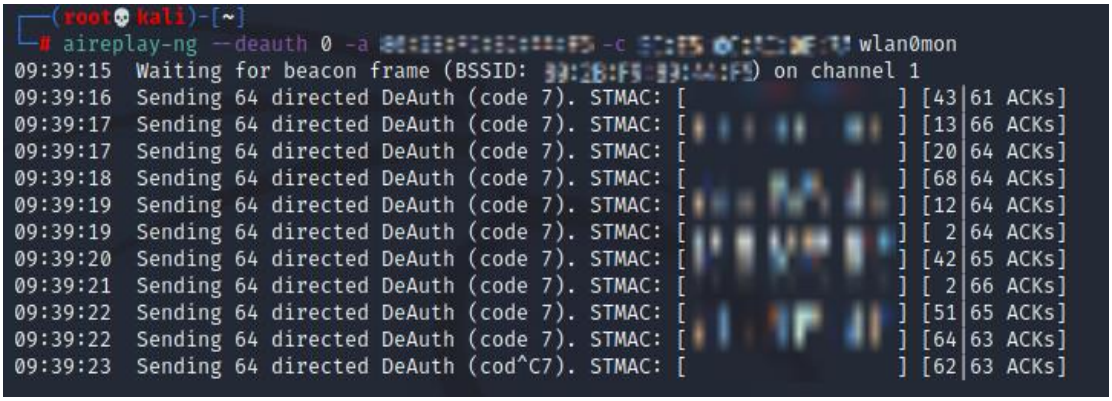
Slika 24. Prikaz dodatnih detalja o uređaju pomoću alata Kismet

Osim nekih osnovnih podataka o uređaju, alat omogućuje i informacije o paketima koje uređaj odašilje kao što je vidljivo na slici 25.



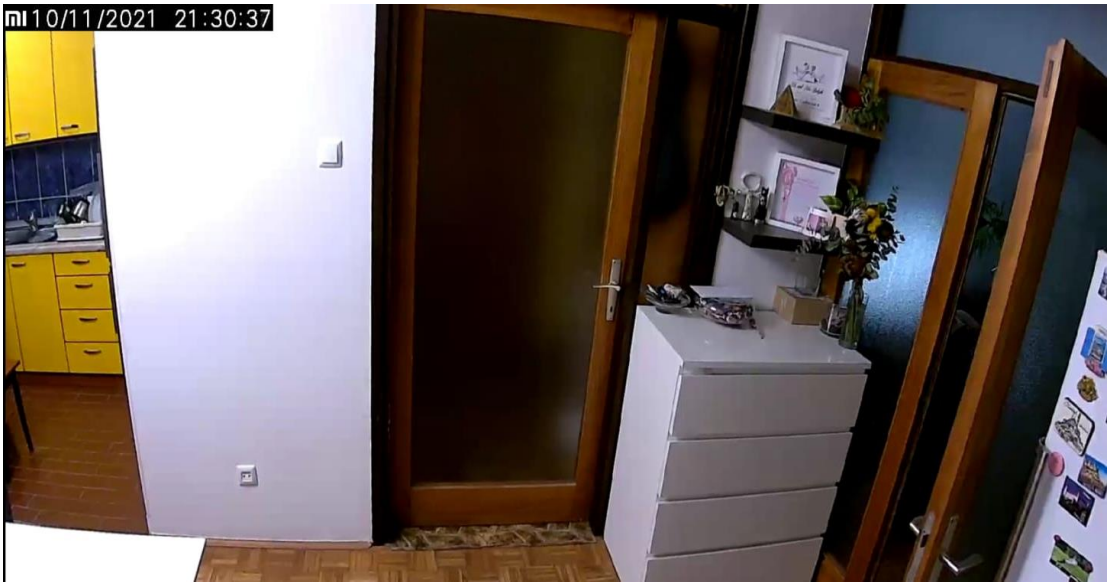
Slika 25. Informacije o Wi-Fi prometu mete napada

Jednom kada je napadač utvrdio da je pronašao svoju metu napada dostupne su mu sve informacije koje su mu potrebne kako bi započeo generiranje deautentifikacijskih paketa prema kameri. Odnosno MAC adresa usmjerivača na koji je povezana kamera, te MAC adresa kamere. Slika 26 prikazuje naredbu koja je također već od prije poznata te je u sličnom obliku korištena prilikom analize usmjerivača, ali je tada korištena za deautentifikaciju svih uređaja povezanih na pristupnu točku dok je sada cilj napad samo na jedan uređaj. Razlog tome je smanjena mogućnost primjećivanja samog napada.



Slika 26. Prikaz naredbe deautentifikacije mete napada

Naredbom „aireplay-ng –deauth 0 -a [MAC adresa usmjerivača] -c [MAC adresa kamere] wlan0mon“ započinje se napad na kameru. Slike u nastavku imaju cilj prikaza kako žrtva napada vidi svoju kućnu kameru za vrijeme napada. Slika 27 prikazuje situaciju kada napad započinje, te je sve do tada vrijeme u gornjem desnom kutu teklo normalnim tokom.



Slika 27. Prikaz snimke kamere za vrijeme napada

Ta ista slika bila je vidljiva žrtvi napada sve dok napad nije završio. Žrtva prilikom napada nije na svom pametnom telefonu dobila obavijest kako kamera u tom trenutku ne komunicira sa svojim usmjerivačem, već je slika ostala zamrznuta. Ukoliko žrtva nije pomno pratila vrijeme koje se prikazuje na snimci poprilično je teško za uvidjeti da se u tom trenutku odvijao DoS napad.

Slika 28 prikazuje završetak napada. Snimka je ostala identična jedino što se promijenilo je vrijeme koje se vratilo na stvarno vrijeme. Napad iz primjera trajao je oko minute, no stvarni napad može trajati i duže. No iako kamera nije bila povezana na lokalnu mrežu iz razloga što ima mogućnost lokalne pohrane u obliku SD memorijske kartice lopov bi u ovo slučaju bio snimljen. U slučaju da SD kartica nije bila umetnuta snimku ne bi bilo moguće vratiti. Isti je slučaj i sa nestankom električne energije, ukoliko dođe do nestanka struje kamera nije u mogućnosti snimanja je nema vlastito dodatno napajanje.

Slika 28. Prikaz snimke završetka napada

5. Sinteza rezultata istraživanja i prijedlog zaštite korisnika i organizacija

Iako IoT uređaji olakšavaju ljudsku svakodnevicu ovim istraživanje prikazano je da kada je riječ o sigurnosnom aspektu potrebno je uložiti još napora i od strane proizvođača i od strane regulatora, ali također i od strane samih korisnika u smislu obrazovanja kako bi se povećala sigurnost samih IoT uređaja.

5.1 Sinteza rezultata istraživanja

Ovim istraživanjem na primjeru smo prikazali virtualizaciju pomoću *Oracle VM VirtualBox* hipervizora i Kali Linux operativnog sustava. Iako se simulacija mogla odviti i na Windows operativnom sustavu, Kali Linux sa svojim već unaprijed instaliranim alatima bio je pogodniji za ovo istraživanje.

Prilikom istraživanja ranjivosti terminalnih uređaja aktivnosti koje su se provodile prolazile su kroz pojedine faze penetracijskog testiranja. Slika 29 prikazuje aktivnosti prema fazama.

	Faza izviđanja	Faza identifikacije sustava	Faza ostvarenja pristupa
Istraživanje ranjivosti usmjerivača	Detekcija dostupnih pristupnih točaka	Prikupljanje informacija o usmjerivaču kao što su detekcija enkripcijskog standarda i detekcija broja uređaja povezanih na pristupnu točku	Pristup je ostvaren pomoću *Brute-force* napada
Istraživanje ranjivosti pametne utičnice		Pronalazak IP i MAC adrese mete napada	Enkripcijom prometa ostvario se pristup podacima
Istraživanje ranjivosti Wi-Fi sigurnosne kamere	Detekcija dostupnih pristupnih točaka i uređaja povezani na nju	Prikupljanje informacija pomoću alata Kismet kao štu su naziv i proizvođač uređaja	

Slika 29. Tablični prikaz faza penetracijskog testiranja napravljenog istraživanja

Istraživanjem prikazane su neke od slabosti usmjerivača i IoT uređaja. Iako je prikazana metoda napada univerzalna za sve vrste usmjerivača i IoT uređaja, ovisno o proizvođaču i modelu postoje različite ranjivosti. Te ranjivosti napadači detaljno istražuju jednom kada saznaju koju opremu koristi meta napada.

Cilj istraživanja sigurnosti usmjerivača bio je dokazati važnosti pravilno postavljanje snažne lozinke. Kao što je već unutar rada naglašeno sigurnosna lozinka koja nije postavljena prema preporukama struke, odnosno njezina kompleksnost i duljina ne zadovoljavaju kriterije koju su preporučeni, slabe su karike kada se nađu na meti kibernetičkog kriminalca. Tako za svrhu istraživanja lozinka usmjerivača bila je „password“, te je dokazano kako je takvu lozinku moguće „probiti“ uz pomoć već sastavljenih lista. Liste su javno dostupne, te je prilikom postavljanja lozinka na bilo

kojem uređaju ili sustavu potrebno je izbjegavati takve lozinke koje su česte i ponavljajuće upravo iz dokazanog razloga.

Također cilj istraživanja je bio prikazati važnost obrazovanja korisnika o uređajima koje koriste svakodnevno unutar svog doma. Te kako jednostavnim postupcima mogu znatno povećati sigurnost vlastitih uređaja. Iako je prvi dio istraživanja analizirao sigurnost usmjerivača, jednom kada napadač dobije pristup usmjerivaču u velikoj mjeri mu je olakšan put prema ostalim uređajima unutar mreže, te je upravo to i dokazano u nastavku istraživanja.

Daljnje istraživanje odvijalo se na pametnoj utičnici kao IoT uređaju koji se nalazio na istoj mreži kao i usmjerivač na kojeg je napadač uspješno dobio pristup.

Cilj istraživanja napada na pametnu utičnicu bio je dokazati mogućnosti napadača koji je ostvario pristup mreži unutar koje se nalaze IoT uređaji. Također cilj je bio analizirati mogućnost probijanja kriptiranih podataka. Unutar analize korišten je način kriptiranja korištenjem wpa-pwd kriptografskog ključa. Sam sustav je zastario, te cilj bio prikazati kako nije dovoljno samo kriptirati podatke, već je potrebno poznavanje samog sustav kojim se podaci kriptiraju.

Istraživanje je dokazalo da je korištenjem besplatnih mrežnih alata moguće prikupljati podatke uređaja jednom kada imamo pristup istoj mreži unutar koje se nalazi i uređaj koji se analizira. Isto tako dokazano je da iako su podaci koji su se prenosili mrežom bili kriptirani, postoje načini dekriptiranja podataka. Za sve to su korišteni alati koji su u potpunosti besplatni, te to dodatno stavljana na važnost da gotovo bilo tko može pristupati našim podacima ukoliko naše sustave ne zaštitimo na odgovarajući način.

Iako se metoda napada istraživanja temeljila na pristupu LAN mreži preko usmjerivača, te si na taj način napadač omogućuje olakšano iskorištavanje ranjivosti ostalih uređaja unutar mreže. Također postoje i drugi načini na koji napadač može usmjeriti svoj napad. Na primjer pristupom napada izvan LAN mreže, unutar koje se nalaze mete napada. Na taj način omogućuje si bolje prikrivanje tragova, ali su mogućnosti ograničene i sam postupak napada zahtjeva naprednija znanja i opremu napadača.

Završni dio praktičnog dijela rada bio je istraživanje ranjivosti Wi-Fi sigurnosne kamere. Cilj ovog dijela rada bio je dokazati kako napadač ne mora imat pristup mreži unutar koje se nalaze IoT uređaji kako bi omeo njihov rad. Također cilj je bio dokazati da se IoT uređaji kada je riječ o kibernetičkim napadima ne koriste samo u svrhe „pomagača“ odnosno u svrhu generiranja velike količine prometa sa različitih geografskih lokacija. Već mogu i sami postati meta takvog napada.

Istraživanje je dokazalo da korištenjem Kali Linux operativnog sustava, te besplatnih alata koje Kali omogućuje moguće je onesposobiti sigurnosnu kameru na neki određeni vremenski period. Također dokazano je da samim time funkcionalnost kamere nije u potpunosti onemogućena iz razloga što posjeduje lokanu memoriju, te ima mogućnost pohrane snimke na nju za vrijeme kada nema mogućnost povezivanja sa drugim uređajima.

Provedenim istraživanjem postignut je rezultat kojim je vidljivo kako postoje sigurnosne mane terminalnih uređaja nad kojima je provedeno istraživanje. Opasnosti koje se kriju iza rezultata ovog istraživanja mogu se smatrati veoma opasnima. Privatni podaci korisnika kompromitirani su jednom kada napadač ostvari pristup lokalnoj mreži, te količina podataka do kojih tada napadač ima mogućnosti doći ovise o samoj sposobnosti napadača. Iako unutar istraživanja pristup snimci sigurnosne kamere nije omogućen, prikazana je mana onesposobljavanja prenošenja trenutne snimke na način da je sigurnosnoj kameri na vremenski period od jedne minute prekinuta povezanost sa lokanom mrežom. Kada bismo to sagledali iz kuta stvarno napada, vremenski period napada može se produžiti, te može biti dovoljan za lopova da provede pljačku bez da ga sigurnosne kamere snime ili dovoljan da pronađe izvor napajanja kamere te si zasigurno omogućio da ga kamera ne snimi.

Slika 30 prikazuje tabličan prikaz rezultata istraživanja kojim je cilj na jednostavniji i praktičniji način objediniti rezultate provedenog istraživanja.

	Istraživanje usmjerivača	Istraživanje pametne utičnice	Istraživanje Wi-Fi sigurnosne kamere
Cilj istraživanja	Prikaz važnosti postavljanja sigurne lozinke, te analiza sigurnosnog aspekta usmjerivača na *brute-force* napad.	Prikaz količiine podataka o uređajima unutar lokalne mreže kojoj napadač ima pristup jednom kada ostvari pristup lokalnoj mreži.	Istraživanje ranjivosti terminalnog uređaja na napad uskračivanja usluga.
Vrsta napada	*Brute-force*		Napad uskraćivanja usluga
Korišteni alati (*Hardware*)	Stolno računalo USB Wi-Fi mrežni adapter	Stolno računalo USB Wi-Fi mrežni adapter	Stolno računalo USB Wi-Fi mrežni adapter
Korišteni alati (*Software*)	Oracle VM VirtualBox Kali Linux AirCrack	Oracle VM VirtualBox Kali Linux AirCrack	Oracle VM VirtualBox Kali Linux AirCrack Kismet
Dobiveni rezultati	Analizirani usmjerivač ranjiv je na brute-force napad u slučaju kada je sigurnosna lozinka jednostavna, te se nalazi na listi često korištenih lozinka.	Dokazano je da iako su podaci koji su se prenosili mrežom bili kriptirani, postoje načini dekriptiranja podataka.	Napadom uskraćivanja usluga moguće je onesposobiti sigurnosnu kameru na neki određeni vremenski period.
Moguća sigurnosna rješenja	Postavljanje kompleksnije lozinke, te konfiguriranje sigurnosnih aspekta usmjerivača svela bi mogućnost da ovakva vrsta napada uspije.	Korištenje novijih enkripcijskih standarda smanjila bi mogućnost dekripcije povjerljivih podataka.	Većina lokalnih mreža u okruženju pametnog doma nema mogućnost jednosvatnog rješenja za obranu od DoS napada. Rješenja koja postoje su skupa, te se koriste unutar većih korporacija i kompanija.

Slika 30. Tablični prikaz rezultata istraživanja

5.2 Sredstva zaštite informacijsko komunikacijskog sustava

Iako postoje brojna sredstva zaštite informacijsko komunikacijskog sustava, nisu sva namijenjena za uporabu unutar okruženja pametnog doma. Kompanije kada razvijaju napredne sustave zaštite, svoje proizvode prvenstveno razvijaju za velike kupce. Iz tog razloga takvi sustavi se i naplaćuju znatne svote novaca pa i iz tog razloga nisu čest odabir kada je riječ o sigurnosti okruženja pametnog doma. Isto tako postoje i određena sredstva zaštite koja je moguće primijeniti unutar okruženja pametnog doma, ta sredstva imaju određenih mana, ali se svejedno preporučuju kao način zaštite vlastitog doma.

5.2.1 Osnovni modeli zaštite informacijsko-komunikacijskog sustava

Postoje dva osnovna modela zaštite informacijsko-komunikacijskog sustava bez obzira dali je riječ o IoT uređajima, računalnim mrežama ili drugim uređajima koji ostvaruju neku vrstu komunikacije. Riječ je o *Lollipop* modelu i slojevitom modelu (eng. *Defense-in-depth model*).

Lollipop model iako se još uvijek koristi, smatra se vrlo nesigurnim. Kod *Lollipop* modela, imovinu korisnika, odnosno ulazak u sam sustav brani samo jedna vrsta zaštite, na primjer korisničko ime i lozinka. Ukoliko napadač na neki način dođe do saznanja o korisničkom imenu i lozinki ima otvoren put prema imovini koja se nalazi unutar sustava. Moguće ga je prikazati na još jedan način, a to je kao da imamo zid koji štiti od ulaska napadača, no jedno kada napadač prođe prepreku zida unutra ga više ništa ne sprječava u njegovim namjerama [42].

Za razliku od *Lollipop* modela, slojeviti model ne temelji se na jednom sloju, odnosno granici zaštite, već se temelji na mnogo slojeva zaštite, te napadač kako bi došao do imovine informacijsko-komunikacijskog sustava potreban je proći sve slojeve zaštite. Slojevi su promjenjivi te ovise o samoj konfiguraciji sustava, što opet ovisi o tome što se nalazi unutar samog sustav, te koliko je novaca i vremena potrebno uložiti kako bi se imovina tog sustava učinila sigurnijom.

Prema [42] slojevi koji se navode su: vatrozid, IDS (eng. *Intrusion Detection Systems*) i IPS (eng. *Intrusion Prevention Systems*) o kojima će nešto više biti napisano u nastavku, proces autentifikacije, proces autorizacije i kriptografija. Naravno da bi se na ove slojeve mogli nadodati još poneki kao što je fizička zaštita sustava ili redoviti nadzor sustava, ali i ovako je lako za primijetiti kako se radi o sigurnijem modelu zaštite od *Lollipop* modela.

5.2.2 Vatrozid

Vatrozid (eng. *Firewall*) možemo definirati kao fizičko ili programsko rješenje koje obavlja funkciju monitoriranja dolaznog i odlaznog prometa prema lokalnoj mreži, ali i od lokalne mreže prema Internetu, te sprječavanje prolaska malicioznog prometa. Vatrozidi se najčešće nalaze na rubnim dijelovima lokalnih mreža, a način na koji se određuje koji promet spada pod maliciozni, a koji ne, su unaprijed konfigurirana pravila. Najčešće se pregledava izvorišna IP adresa, te kome je paket poslan, odnosno odredišna IP adresa, te port. Iz razloga što danas nije dovoljno samo filtriranje prometa po izvorišnoj i odredišnoj IP adresi nastaju različiti tipovi vatrozida kako bi se analiza prometa vršila prema većem broju parametara. Iz tog razloga nastaju novi tipovi vatrozida, a neki od njih su [43]:

- Proxy vatrozid,
- *Next Generation Firewall*,
- NAT vatrozid .

Proxy vatrozid je vatrozid koji svoju analizu ne ograničava samo na mrežni i transportni sloj OSI referentnog modela, već promet analizira na svih sedam slojeva OSI referentnog modela. Koristi se kao *gateway* vatrozid, no iz razloga što ne analizira samo IP adrese, već i brojne druge protokole Proxy vatrozidi čine kvalitetniju zaštitu [44].

Next Generation Firewall smatra se vatrozid koji uz osnovne funkcionalnosti vatrozid kombinira i još neke dodatne funkcionalnosti kao što je dekripcija kriptiranog prometa kako bi se mogla napraviti analiza paketa, te utvrditi dali se radi o malicioznom prometu ili ne. Sama analiza paketa se razlikuje od vatrozida starijih

generacija iz razloga što uključuje dubinsku inspekciju paketa (eng. *Deep Packet Inspection* - DPI) [45]. To znači da kada se radi sama analiza paketa ne analizira se samo zaglavlje paketa, odnosno odredišna i izvorišna IP adresa i broj porta, već analiza uključuje i podatke koji se šalju samim paketom. Na taj način moguće je pronaći skrivene prijetnje [46].

NAT (eng. *Network address translation*) vatrozidi pretvaraju privatne IP adrese uređaja u javne IP adrese pomoću koji se odvija komunikacija sa ostalim uređajima van lokalne mreže. Na taj način privatna IP adresa ostaje skrivena za napadače [45].

5.2.3 IDS i IPS

IDS ili sustav detekcije neovlaštenog upada je pasivni alat koji monitorira i analizira mrežni promet, te detektira potencijalne maliciozne aktivnosti prema unaprijed postavljenim pravilima. Nakon što IDS detektira potencijalnu malicioznu aktivnost on ne zaustavlja promet niti sam reagira na nju, već pomoću upozorenja obavještava osobu koja je zadužena za praćenje takvih upozorenja [47].

IPS ili sustav zaštite od neovlaštenog upada je također alat za monitoriranje i analiziranje mrežnog prometa, ali za razliku od IDS-a nije pasivan što znači da ukoliko detektira potencijalnu prijetnju na nju automatski reagira. Odnosno paket koji se smatra potencijalnom prijetnje neće se propustit te je na taj način moguće spriječiti napade [47].

Iako se IPS čini dominantnijim i sigurnijim rješenjem od IDS, IPS nije pravo rješenje za sve vrste sustava. IDS je bolje rješenje kod sustava kojima je dostupnost na prvom mjestu i gdje podaci korisnicima moraju biti dostupni u svakom trenutku pa čak i pod cijenu smanjene sigurnosti sustava. IPS se smatra boljim rješenjem kod sustava koji sadrže vrijedne podatke i informacije. Isto tako sustava koji si mogu dopustiti kratkotrajne nedostupnosti za cijenu poboljšane sigurnosti [47].

5.2.4 Mjere zaštite od DDoS napada

Kada je riječ o DDoS napadima postoje načini i prakse kako se pripremiti i kako postupati u slučaju aktivnog DDoS napada. Jedan od načina je poprilično jednostavan i u većini slučajeva vatrozid sprječava napade tog. Riječ je o napadima manjeg volumena bez da žrtva napada primijeti da se napad uopće i odvijao. To je vrsta napada kada su IP adrese botova, odnosno uređaja pomoću kojih se izvodi napada po nekim karakteristikama prepoznatljive. Na primjer ukoliko su sve IP adrese uređaja sa kojih se izvodi napada iz pojedine države, žrtva, odnosno njen vatrozid prepoznaje tu karakteristiku, te jednostavno onemogućuje dolazni promet iz tog „bazena“ (eng. *scope*) IP adresa.

Također IDS i IPS su sustavi koji mogu primijetiti DDoS napada, te reagirati na njega. Naravno da postoje i vrste napada nad kojima IDS i IPS sustavi ne prepoznaju anomalije, te napad može napraviti određene štete prije nego se reagira na njega.

Uz IDS i IPS način na koji je moguće smanjiti ranjivost sustava je filtriranje prometa kroz više slojeva zaštite prije nego dospije unutar mreže ili do dijela mreže kojeg može zagušiti. Također kompanije kao mjeru zaštite koriste i način povećanja mrežnog *bandwidth-a* i veći broj mrežnih uređaja kao redundanciju, iako im za normalno poslovanje nisu potrebni. Na taj način sustav može podnijeti veću količinu mrežnog prometa ukoliko dođe do DDoS napada [48].

Još jedan način zaštite koji je vezan uz *bandwidth* je *cloud* poslovanje. Prebacivanje poslovanja ili dijela poslovanja na *cloud* također može poslužiti kao mjera zaštite od DDoS napada upravo iz razloga što pružatelji *cloud* usluga osiguravaju veliki *bandwidth* kompanijama, te se brinu za sigurnost njihovog poslovanja [48].

5.3 Prijedlog zaštite korisnika

Kada je riječ o zaštiti korisnika u informacijsko-komunikacijskom svijetu vrlo je važan faktor obrazovanje samih korisnika. U današnje vrijeme korisnici pametnih telefona, ali i drugih uređaja koji se povezuju na Internet nisu u potpunosti svjesni

prijetnji koje su moguće. Razlog tome je djelomično i to što djeca već vrlo rano počinju koristiti pametne telefone. Dok sa druge strane velik broj starije populacije također koriste pametne telefone i društvene mreže također u velikoj većini bez velikih saznanja na koji način se informacije koje tamo ostavljaju mogu upotrijebiti protiv njih.

Sredstva zaštite koja su spomenuta u prijašnjem poglavlju nisu uobičajena u okruženju pametnog doma. Razlozi tome su prvenstveno ti što brojna slična sredstva se naplaćuju po znatnim svotama. Samim proizvođačima takvih sredstava krajnji korisnici kao pojedinci nisu niti na meti kao kupci, već se okreću prema većim kompanijama kojima su takva rješenja potrebnija pa samim time su i spremni platit veću novčanu sumu. Osim financijskog aspekta još jedan od razloga je i sama edukacija korisnika. Kako bi se navedena rješenja implementirala i koristila na pravi način potrebno je određeno informacijsko znanje i vještine.

Iako je već kroz rad navedena smjernica koja je vrlo važna kada je riječ o sigurnosnom aspektu IoT uređaja unutar okruženja pametnog doma je postavljanje i promjena lozinke. Promjena lozinke na usmjerivaču, te postavljanje kompleksne lozinke uvelike može otežati posao napadaču, a u neki slučajevima i spriječiti uspješnost napada. Također postavljanje i promjena tvornički postavljenih lozinka i na IoT uređajima u velikoj mjeri otežati će posao napadaču. Velik broj IoT uređaja koji su bili meta DDoS napada, proces promjena lozinke i postavljanje kompleksnije lozinke mogao je spriječiti napade.

Također još jedna sigurnosna smjernica prihvatljiva za okruženje pametnog doma su sigurnosne postavke usmjerivača. Vrlo je važno sigurnosne postavke usmjerivača konfigurirati prema takozvanoj „najboljoj praksi“ iz razloga što kao što je prikazano u istraživanju koristeći WPA umjesto WPA2 enkripcijskog standarda rezultiralo je lakšim uspješnim provođenjem napada. Također postoje i brojne druge sigurnosne postavke koje je potrebno pažljivo konfigurirati kako bi se okruženje pametnog doma učinilo što sigurnijim.

Analiza vlastite mreže također je vrlo važan sigurnosni faktor unutar okruženja pametnog doma. Redovitim analiziranjem mrežnog prometa moguće je uočiti anomalije koje su potencijalni pokazatelj ugroženosti cjelokupne mreže pa tako i IoT uređaja unutar nje.

6. Otvorena pitanja i izazovi sigurnosti u konceptu IoT

Rastom broja IoT uređaja koji su povezani na Internet, rastu i mogućnosti napadača na koje sve načine mogu doći do željenih podataka ili nekog drugog zlonamjernog cilja. U današnje vrijeme često se spominje sigurnost IoT uređaja, ali isto tako česte su informacije o brojnim kibernetičkim napadima unutar kojih su u nekom dijelu napada iskorištene sigurnosne slabosti IoT uređaja. U nastavku poglavlja biti će navede neke od smjernica kako učiniti vlastite IoT uređaje sigurnijima, što ujedno znači i učiniti i cjelokupnu vlastitu računalnu mrežu sigurnijom.

6.1 Sigurnosne smjernice korisnicima IoT uređaja

Smjernice koje su vezane uz sigurnost IoT uređaja su brojne upravo iz razloga što se dogodio već dovoljan broj kibernetičkih napada na IoT uređaje te je moguće napraviti uzorak slabih točaka samih uređaja. Postavlja se pitanje iz kojeg razloga i dalje već postojeće i poznate sigurnosne mane, proizvođači uređaja ne otklone pri samoj proizvodnji. Veliku ulogu ima cijena samih uređaja, proizvođači pokušavaju napraviti uređaj cjenovno što prihvatljivijim za kupce, te se pri tom ne ulaže dovoljno u sigurnost. Također kao što je već naglašeno unutar rada velika odgovornost leži na edukaciji korisnika IoT uređaja iz razloga što korisnici sami mogu doprinijeti sigurnosti vlastite lokalne mreže.

Neke od smjernica koje su upućene samim korisnicima kako mogu učiniti svoje IoT uređaje sigurnijima su [49]:

- Poznavanje vlastitih uređaja,
- Promjena pristupnih podataka,
- Redovita instalacija zakrpa,
- Redovita monitoriranja LAN mreže.

Već i prije kupnje samog uređaja potrebno je napraviti analizu uređaja. Pri tom se misli na provjeru kojim protokolima komunicira, dali proizvođači redovito izdaju sigurnosne zakrpe za taj uređaj, te dali podržava enkripciju podataka [49].

Vrlo je važno kao što je dokazano i u praktično dijelu rada promijeniti pristupne podatke. Korisničko ime i lozinku potrebno je promijeniti, te je poželjno pratit savijete takozvane „najbolje prakse“. Iako to nije čest slučaj, prema preporukama lozinka bi morala biti različita za svaki račun koji korisnik koristi. Pa tako na primjer nije preporučljivo koristiti istu lozinku za pristup vlastitoj LAN mreži i za pristup jednoj od društvenih mreža. Lozinka bi trebala biti različita od imena i prezimena, te također preporučljivo je da se koristi lozinka koja sadržava velika i mala slova, brojeve, te specijalne znakove [50].

Problem sa redovitom instalacijom sigurnosnih zakrpa može predstaviti ukoliko sam proizvođač jednostavno ne izdaje redovite zakrpe. Zakrpe je potrebno redovito instalirati iz razloga što upravo pomoću zakrpa proizvođači rješavaju neke od poznatih problema i sigurnosnih nedostataka zbog kojih je i njihov uređaj ranjiv [49].

Redovito monitoriranje vlastite LAN može uvelike povećati sigurnost cjelokupne LAN mreže, pa tako i IoT uređaja koji se nalaze unutar nje. Redovitim monitoriranjem moguće je vidjeti koji su sve uređaji povezani na LAN mrežu, te dali postoje neka neočekivana ponašanja određenih uređaja koja bi mogla prouzročiti štetu svim uređajima povezanim na mrežu [49].

6.2 Izazovi IoT sigurnosti

Kao što je vidljivo iz prošlog poglavlja brojni su načini na koje bismo mogli IoT koncept sigurnijim. Nalazimo se na prekretnici kada se sve češće spominje IoT sigurnost, ali još uvijek u praksi nije na željenom nivou.

Unutar ovog poglavlja biti će navedeni neki od izazova koje će biti potrebno riješiti u budućnosti kako bi se IoT koncept učinio sigurnijim.

Za početak važno je naglasiti da će se unatoč limitacijama koje današnji uređaji sa svojom veličinom i cijenom predstavljaju morati ići korak dalje u smjeru sigurnosti. Bitna stavka je i pronalazak načina na koji će se moći efikasno upravljati velikim brojem uređaja koji nas već i danas preplavljuju, te će se taj broj u budućnosti samo povećavati [51].

Jednako tako, jasno će se morati odrediti zadaće i zaduženja proizvođača, vlasnika, ali i korisnika uređaja. Bez ovog koraka ukoliko se od proizvođača na primjer ne zahtjeva ugradnja minimalnih sigurnosnih standarda, te redovito izdavanje sigurnosnih zakrpa, nemoguće je postići željenu razinu sigurnosti. Sa druge strane sami korisnici, odnosno osobe zadužene za održavanje uređaja morati će snositi i svoju odgovornost ukoliko se korištenje uređaja nije obnašalo po sigurnosnim standardima, primjerice namjerno izbjegavanje instaliranja sigurnosnih zakrpa, te na taj način „otvaranje vrata“ napadaču pri izvođenju napada [51].

Upravo zbog navedenog, ali i brojnih drugih slučajeva od regulatornih agencija zahtjeva se nove upotpunjene smjernice i zaduženja svih entitetima koji se nalaze u sustavu kako bi svatko znao i obnašao svoje zadaće [51].

7. Zaključak

Pomoću naznaka koje prikazuju istraživanja o rastu broja korištenja IoT uređaja, moguće je zaključiti kako će se i broj napada na te uređaje povećati. Pogotovo ukoliko se linija ulaganja u sigurnosni dio IoT koncepta ne poveća, mogući su novi napadi čak i većih razmjera nego što su do sada zabilježeni.

Broj pametnih kuća također se povećava, pa i u tom segmentu postoje brojne nove opasnosti. Pozitivan element je taj što se pojam sigurnosti IoT uređaja sve češće spominje te i sami korisnici takvih uređaja poduzimaju određene mjere kako bi učinili svoje domove, ali i svoju privatnosti što sigurnijom.

Iako je istraživanje ovog rada ukazalo na određene mane predmeta istraživanja, uz manje preinake sigurnosnih postavka, ali i redovitim monitoriranjem moguće je izbjeći ovakve vrste napada. To ne znači da, ukoliko se pridržavamo svih savjeta nećemo biti žrtva napada i da smo u potpunosti sigurni. Potpuna sigurnost ne postoji koliko god neki sustav učinili sigurnim, uvijek postoji mogućnost kompromitiranja sustava, pa makar taj način ugroze danas još niti ne postoji.

Najbolji način na koji možemo svoje kućno okruženje učiniti što sigurnijim je samostalno obrazovanje. Potrebno je konstantno slijediti napredak tehnologije kako bismo bili u korak sa njom. Vjerujem da će zanimanje za računalnom sigurnosti u naredno vrijeme postati sve veće, iako napadači otkrivaju nove načine prelaženja preko sigurnosnih prepreka, imati će sve teži posao iz razloga što će šira populacija imati veća saznanja o tehnologiji i računalnoj sigurnosti.

Svjesnost od mogućih prijetnji je pozitivna stvar, te nema potrebe za strahom od nove tehnologije koja ima mogućnosti pomoći na brojne načine ljudima u njihovim uobičajenim poslovima. Iako funkcionalnosti nekih uređaja ne razumijemo u potpunosti, poželjno je informirati se, a ne odbaciti pomoć koja nam se pruža na dohvat ruke. Novom tehnologijom omogućene su stvari koje ljudi unazad 50 godina nisu mogli niti zamislit. Iz tog razloga sa pozitivnom dozom straha zašto ne iskoristiti nešto što svakodnevni život može učiniti mnogo lakšim?

LITERATURA

[1] Razzaq, A, M. Gill, H, S. Qureshi, A, M. Ullah, S.: Security Issues in the Internet of Things (IoT): A Comprehensive Study, Vol. 8, No. 6, 2019 Preuzeto sa: https://www.researchgate.net/publication/318096417_Security_Issues_in_the_Internet_of_Things_IoT_A_Comprehensive_Study [Pristupljeno: svibanj 2021.]

[2] Vignesh, R., Samydurai, A., Security on Internet of Things(IOT) with Challenges and Countermeasures. 2017 IJEDR | Volume5, Issue 1| ISSN: 2321-9939.Preuzeto sa:https://thesai.org/Downloads/Volume8No6/Paper_50-Security_Issues_in_the_Internet_of_Things.pdf [Pristupljeno: svibanj 2021.]

[3] Meng, Y. Zhang, W. Zhu, H. Shen, S, X.: Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures, 2018Preuzeto sa: https://ieeexplore.ieee.org/document/8600778 [Pristupljeno: svibanj 2021.]

[4] Cvitić, I., Peraković, D., Periša, M., Krstić, M. & Gupta, B. (2021) Analysis of IoT Concept Applications: Smart Home Perspective. U: Peraković, D. & Knapcikova, L. (ur.)Future Access Enablers for Ubiquitous and Intelligent Infrastructures, FABULOUS 2021, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering doi:10.1007/978-3-030-78459-1_12.Preuzeto sa: https://www.bib.irb.hr/1132646 [Pristupljeno: studeni 2021.]

[5] URL: What is IoT? Preuzeto sa: https://www.oracle.com/internet-of-things/what-is-iot/ [Pristupljeno: lipanj 2021.]

[6] URL: STEM. Senzori i Aktuatori. Preuzeto sa: https://www.stem.ba/arduino-elektronika/tutorijali/item/319-senzori-i-aktuatori [Pristupljeno: lipanj 2021.]

[7] HAKOM - Javne konzultacije M2M komunikacija – regulatorni pregled. Preuzeto sa:https://www.hakom.hr/userdocsimages/javnaRasprava/M2M_komunikacija_javne%20konzultacije-20141216.pdf [Pristupljeno: lipanj 2021.]

[8] URL: WhatIsMyIPAddress. What is a MAC Address? Preuzeto sa: https://whatismyipaddress.com/mac-address [Pristupljeno: kolovoz 2021.]

[9] URL: IBM Documentation. Internet Protocol Version 4 (IPv4). Preuzeto sa: https://www.ibm.com/docs/en/zos/2.4.0?topic=ipv6-internet-protocol-version-4-ipv4 [Pristupljeno: kolovoz 2021.]

[10] URL: MERIDIANOUTPOST. The Five IPv4 Classes - Quick Reference. Preuzeto sa: https://www.meridianoutpost.com/resources/articles/IP-classes.php [Pristupljeno: kolovoz 2021.]

[11] URL: Fortinet. What is Address Resolution Protocol (ARP)? Preuzeto sa: https://www.fortinet.com/resources/cyberglossary/what-is-arp [Pristupljeno: kolovoz 2021.]

[12] Ristov, P. Mrvica, A. Tomas, V. Komadina, P.: Informacijski sustav podržan RFID tehnologijom u procesu prodaje i kontrole karata u brodskom putničkom prometu, 2015. Preuzeto sa: https://www.scribd.com/document/495423769/9-Ristov-Mrvica-Komadina-Tomas [Pristupljeno: kolovoz 2021.]

[13] Peraković, D. Cvitić, I.: Sigurnost i zaštita informacijsko komunikacijskog sustava, 2020Preuzeto sa: https://moodle.srce.hr/2019-2020/pluginfile.php/3428278/mod_resource/content/2/P01_P02_S01_S02_P03_S03_P04_P05_P06_S04_P07_S05_P08_P09.pdf [Pristupljeno: kolovoz 2021.]

[14] URL: Homey. What is Zigbee? Explaining the World's Most Popular Smart Light Network Technology. Preuzeto sa: https://homey.app/en-au/wiki/what-is-zigbee/ [Pristupljeno: lipanj 2021.]

[15] URL: Beaconstac. Bluetooth Low Energy (BLE) Beacon Technology Made Simple: A Complete Guide to Bluetooth Beacons. Preuzeto sa: https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/ [Pristupljeno: lipanj 2021.]

[16] URL: Radiocrafts. What is 6LoWPAN? Preuzeto sa: https://radiocrafts.com/technologies/6lowpan/ [Pristupljeno: lipanj 2021.]

[17] URL: Cybernews. What is AES encryption and how does it work? Preuzeto sa: https://cybernews.com/resources/what-is-aes-encryption/ [Pristupljeno: lipanj 2021.]

[18] URL: us-cert.cisa.gov. Security Tip (ST04-015) Understanding Denial-of-Service Attacks. Preuzeto sa: https://us-cert.cisa.gov/ncas/tips/ST04-015 [Pristupljeno: srpanj 2021.]

[19] URL: CARNet. DDoS napad CCERT-PUBDOC-2008-09-240. Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf [Pristupljeno: srpanj 2021.]

[20] URL: Cloudflare. What is the Mirai Botnet? Preuzeto sa: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ [Pristupljeno: srpanj 2021.]

[21] URL: A10networks. Five Most Famous DDoS Attacks and Then Some. Preuzeto sa: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/ [Pristupljeno: srpanj 2021.]

[22] Cvitić, I., Peraković, D., Gupta, B. & Choo, K. (2021) Boosting-based DDoS Detection in Internet of Things Systems. Prihvaćen za objavljivanje u *IEEE Internet of Things*. [Preprint] doi:10.1109/JIOT.2021.3090909. Preuzeto sa: https://www.bib.irb.hr/1137291 [Pristupljeno: studeni 2021.]

[23] URL: Fortinet. Brute-force attack. Preuzeto sa: https://www.fortinet.com/resources/cyberglossary [Pristupljeno: kolovoz 2021.]

[24] URL: Trenton systems. Symmetric vs. Asymmetric Encryption: What's the Difference? Preuzeto sa: https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption [Pristupljeno: kolovoz 2021.]

[25] URL: GeeksforGeeks. Data encryption standard (DES) | Set 1. Preuzeto sa: https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/ [Pristupljeno: kolovoz 2021.]

[26] URL: NFON. AES. Preuzeto sa: https://www.nfon.com/hr/servis/baza-znanja/baza-znanja/aes [Pristupljeno: kolovoz 2021.]

[27] URL: Cloudflare. What is TLS (Transport Layer Security)? Preuzeto sa: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ [Pristupljeno: kolovoz 2021.]

[28] URL: Statista. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. Preuzeto sa: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ [Pristupljeno: lipanj 2021.]

[29] URL: IoT-Analytics. Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security. Preuzeto sa: https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/ [Pristupljeno: lipanj 2021.]

[30] URL: Pareteum. 32 IoT Stats to Know in 2021. Preuzeto sa: https://www.pareteum.com/internet-of-things-iot-stats-2021/ [Pristupljeno: studeni 2021.]

[31] URL: Safeatlast. 80 Insightful 'Internet of Things' Statistics (Infographic). Preuzeto sa: https://safeatlast.co/blog/iot-statistics/ [Pristupljeno: studeni 2021.]

[32] URL: CARNet. Metodologija penetracijskog testiranja CCERT–PUBDOC–2008–02–219. Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-219.pdf [Pristupljeno: srpanj 2021.]

[33] URL: Synopsys. Penetration Testing. Preuzeto sa: https://www.synopsys.com/glossary/what-is-penetration-testing.html [Pristupljeno: srpanj 2021.]

[34] URL: Imperva. Penetration Testing. Preuzeto sa: https://www.imperva.com/learn/application-security/penetration-testing/ [Pristupljeno: kolovoz 2021.]

[35] URL: Iskratel. INNBOX V45 High-Performance VDSL2 Home Gateway. Preuzeto sa: https://www.iskratel.com/si/files/default/Documents/Data-Sheet/Iskratel-Innbox-V45-Datasheet-EN.pdf [Pristupljeno: rujan 2021.]

[36] URL: KALI. What is Kali Linux? Preuzeto sa: https://www.kali.org/docs/introduction/what-is-kali-linux/ [Pristupljeno: kolovoz 2021.]

[37] URL: Latest Hacking News. What is monitor mode in wifi? Preuzeto sa: https://latesthackingnews.com/2017/07/19/what-is-monitor-mode-in-wifi/ [Pristupljeno: kolovoz 2021.]

[38] URL: Juniper. Understanding the Network Terms SSID, BSSID, and ESSID. Preuzeto sa: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.7/topics/concept/wireless-ssid-bssid-essid.html [Pristupljeno: kolovoz 2021.]

[39] URL: VoCAL. EAPoL – Extensible Authentication Protocol over LAN. Preuzeto sa: https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/ [Pristupljeno: kolovoz 2021.]

[40] URL: Varonis. How to Use Nmap: Commands and Tutorial Guide. Preuzeto sa: https://www.varonis.com/blog/nmap-commands/ [Pristupljeno: kolovoz 2021.]

[41] URL: Kismetwireless. Kismet. Preuzeto sa: https://www.kismetwireless.net/ [Pristupljeno: studeni 2021.]

[42] URL: GeeksforGeeks. Introduction To Security Defense Models. Preuzeto sa: https://www.geeksforgeeks.org/introduction-to-security-defense-models/ [Pristupljeno: kolovoz 2021.]

[43] URL: Norton. What is a firewall? Firewalls explained and why you need one. Preuzeto sa: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html [Pristupljeno: kolovoz 2021.]

[44] URL: Fortinet. What Is a Proxy Firewall? Preuzeto sa: https://www.fortinet.com/resources/cyberglossary/proxy-firewall [Pristupljeno: kolovoz 2021.]

[45] URL: Forcepoint. What is a Firewall? Preuzeto sa: https://www.forcepoint.com/cyber-edu/firewall [Pristupljeno: kolovoz 2021.]

[46] URL: Fortinet. Deep Packet Inspection (DPI). Preuzeto sa: https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection [Pristupljeno: kolovoz 2021.]

[47] URL: Check Point. Intrusion Detection System (IDS) Vs Intrusion Prevention System (IPS). Preuzeto sa: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/ [Pristupljeno: kolovoz: 2021.]

[48] URL: Computer World. How to defend against DDoS attacks. Preuzeto sa: https://www.computerworld.com/article/2564424/how-to-defend-against-ddos-attacks.html [Pristupljeno: kolovoz 2021.]

[49] URL: Datamation. IoT Security: 10 Tips to Secure the Internet of Things. Preuzeto sa: https://www.datamation.com/networks/iot-security-10-tips-to-secure-the-internet-of-things/ [Pristupljeno: kolovoz 2021.]

[50] URL: Microsoft Docs. Password must meet complexity requirements. Preuzeto sa: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements [Pristupljeno: kolovoz 2021.]

[51] URL: Tulane. IoT Security Challenges and Threats. Preuzeto sa: https://sopa.tulane.edu/degrees-programs/programs-study/information-technology/iot-security-challenges-and-threats [Pristupljeno: kolovoz 2021.]

POPIS KRATICA

IoT – Internet of Things

DoS - Denial-of-service

DDoS - Distributed Denial of Service

LTE – Long-Term Evolution

NB-IoT – Narrowband-Internet of Things

CSI - Channel state information

SMS - Systematic mapping study

M2M - Machine to Machine

IP - Internet Protocol

MAC - Media Access Control

ARP - Address Resolution Protocol

DNS - Domain Name System

LAN - Local Area Network

OSI - Open Systems Interconnection

RFID - Radio-frequency identification

IEEE - Institute of Electrical and Electronics Engineers

BLE - Bluetooth Low Energy

6LoWPAN - IPv6 over Low-Power Wireless Personal Area Network

AES - Advanced Encryption Standard

NIST - The National Institute of Standards and Technology

VPN - Virtual Privat Network

DES - Data Encryption Standard

TLS - Transport Layer Security

SSL - Secure Sockets Layer

VoIP - Voice over IP

IEFT - Internet Engineering Task Force

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

USB - Universal Serial Bus

SD - Secure Digital

BSSID - Basic Service Set Identifier

SSID - Service Set Identifier

ESSID - Extended Basic Service Set Identifier

WLAN - Wireless Local Area Network

EAPoL - Extensible Authentication Protocol over LAN

WPA - Wi-Fi Protected Access

WPA-PWD - Wi-Fi Protected Access – password

IDS - Intrusion Detection Systems

IPS - Intrusion Prevention Systems

NAT - Network address translation

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Istraživanje ranjivosti terminalnih uređaja u okruženju pametnog doma** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 11/20/2021

(potpis)