SIGURNOST BEŽIČNIH LOKALNIH MREŽA

Lukinec, Luka

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

SIGURNOST BEŽIČNIH LOKALNIH MREŽA

Luka Lukinec

Zagreb, veljača 2020.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, veljača 2020.

Predgovor

Glavnu svoju zahvalu dugujem mentoru, na njegovome strpljenju i pomoći u kasne noćne sate, te na njegovoj velikoj pomoći u stvaranju ovoga rada. Također želim zahvaliti svojoj majci i djevojci, što su vjerovale u mene i poticale me da završim ovaj preddiplomski studij. Hvala i svim djelatnicima Algebre, koji su sudjelovali u mojemu napretku, kako u profesionalnom tako i u ljudskome smislu, te se nadam da ćemo na isti način nastaviti i na diplomskome studiju.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Analizirano je stanje zaštite bežičnih lokalnih mreža na različitim područjima, počevši od kućanstva pa sve do poduzeća. Prema prikupljenim podacima vidljivo je, kako su korištene zaštite odnosno razina snage lozinke te vrsta enkripcije. Većina korisnika jedino ima zaštitu dobivenu od pružatelja usluga te su još uvijek nedovoljno upućeni u probleme zloupotrebe mreža. Sa pojavom novih tehnologija te sve većim korištenjem privatnih podataka putem mreža, potrebno je osvijestiti korisnike o posljedicama, koje mogu nastati korištenjem bežičnih mreža.

Ključne riječi: bežične lokalne mreže, lozinka, enkripcija, edukacija korisnika, nove tehnologije, zloupotreba

The state of protection of wireless computer networks in various areas, from households to enterprises have been analyzed. Based on the collected data, the used security, the power level of the password and the type of encryption are visible. Most users only have provider-provided protection and are still under-aware of network abuse issues. With the advent of new technologies, and the increasing use of private data through networks, it is necessary to gain awareness of the risky events that come with the use of wireless networks.

Keywords: wireless local area networks, password, encryption, user education, new technologies, abuse

Sadržaj

1. Uvod 1

2. Bežične mreže 2

2.1. Razvoj 2

2.1.1. Razlika između lokalne mreže i bežične lokalne mreže 2

2.2. Arhitektura 3

2.2.1. Osnovni servisni set (BSS) 3

2.2.2. Prošireni servisni set (ESS) 4

2.2.3. Nezavisni osnovni servisni set (IBSS) 5

2.3. Standardi 5

2.3.1. IEEE 802.11 6

2.4. Svrha korištenja 7

3. Sigurnost bežičnih mreža 8

3.1. Sigurnosni standardi 8

3.1.1. WEP 8

3.1.2. WPA 9

3.1.3. WPA2 9

3.1.4. WPA3 10

3.2. Sigurnosni propusti 11

3.2.1. Pasivni i aktivni napadi 12

4. Testiranje 14

4.1. Oprema 14

4.1.1. Softver 14

4.1.2. Hardver 16

4.2. Provođenje testiranja na lokacijama 16
4.3. Analiza rezultata 17
4.4. Definiranje izvještaja 18
5. Metode zaštite 20
5.1. Korištenje alata za zaštitu 20
5.2. Preporuka zaštite za kućanstva i manje javne prostore 20
5.3. Preporuka zaštite za manja poduzeća 21
6. Zaključak 23
Popis kratica 24
Popis slika 25
Popis tablica 25
Literatura 27

1. Uvod

Bežične mreže su u širokoj primjeni i njima se velik broj korisnika svakodnevno koristi. Pojavom novih tehnologija te modernih uređaja postale su neophodne za svakodnevni rad. Međutim mnogi se pitaju, koliko je korištenje bežičnih mreža ustvari sigurno. Prema istraživanju popularnog antivirusnog proizvođača Avasta, na globalnoj razini 40,8% kućanstava ima barem jedan ranjivi uređaj na bežičnoj mreži [1]. Samom pojavom jednoga ranjivoga uređaja u našoj mreži dovodimo u pitanje sigurnost svih uređaja te samim time cijele mreže.

Rijetki su pojedinci koji su postavili isto pitanje. Sigurnost bežičnih mreža je pojam koji se olako shvaća, a dovodi do ozbiljnih problema. Osnovna zaštita kod bežičnih mreža pokazala se nedovoljnom, korištenjem dostupnih alata isti se mogu probiti te dovesti u pitanje sigurnost vaših privatnih podataka, financijskih podataka te čak i krađe identiteta. Ovaj rad napravljen je s ciljem podizanja svijesti korisnika o negativnoj strani bežičnih mreža te kako na najlakše moguće načine pravovaljano zaštiti mrežu te tako zaštititi i sebe.

Analiza je provedena na običnim kućanstvima, mjestima okupljanja malog broja ljudi te u manjim poduzećima. Prikupljanjem konkretnih podataka o zaštiti te analizom iste provedeni su mjeseci. Prikupljanje je izvršeno uz privolu osoba uključenih u ovaj rad.

2. Bežične mreže

2.1. Razvoj

Bežične mreže možemo definirati kao više međusobno povezanih uređaja bez fizičkog dodira, povezanih preko radiovalova ili elektromagnetskih signala. Prva pojava bežičnih mreža bila je 1969. godine na Havajima, pod nazivom ALOHAnet, s radom je počela 1971. godine. Prva komercijalna bežična mreža bila je WaveLAN, razvijena od strane NCR-a 1986. godine [2].

Tijekom godina povećao se trend korištenja bežičnih mreža. Saznanjem da se više ne moraju fizički spajati na mrežne uređaje, korisnici su vrlo rado prihvatili novi način rada putem bežičnih mreža.

Današnje bežične mreže koriste se u kućanstvima, poduzećima, prostorima okupljanja te na mnogim drugim mjestima, gdje se uvelike olakšava komunikacija i prijenos podataka između sudionika.

2.1.1. Razlika između lokalne mreže i bežične lokalne mreže

S obzirom na današnje potrebe mobilnosti prilikom korištenja mrežnih resursa, bežične lokalne mreže su u velikom porastu prema lokalnim mrežama koje koriste žično spajanje. U prikazanoj tablici Tablica 2.1 – Usporedba lokalne mreže i bežične lokalne mreže objašnjene su osnovne razlike između lokalne mreže LAN (engl. *Local Area Network*) te bežične lokalne mreže WLAN (engl. *Wireless Local Area Network*).

Tablica 2.1 – Usporedba lokalne mreže i bežične lokalne mreže

	LAN	**WLAN**
Arhitektura	Žično te bežično povezivanje	Bežično povezivanje
Signal	Koristi električne signale za prijenos podataka	Koristi radiofrekvencijske valove za prijenos podataka
Sigurnost	Velika	Mala
Komunikacija	Full duplex	Half duplex
Pokretljivost	Ograničena	Proširena
Korištenje	Popularnost u padu	Popularnost u rastu

2.2. Arhitektura

Prilikom spominjanja arhitekture govori se o više zasebnih pojmova vezanih za lokalne bežične mreže. Međutim svi ti zasebni dijelovi tvore sustave koje se dijele na:

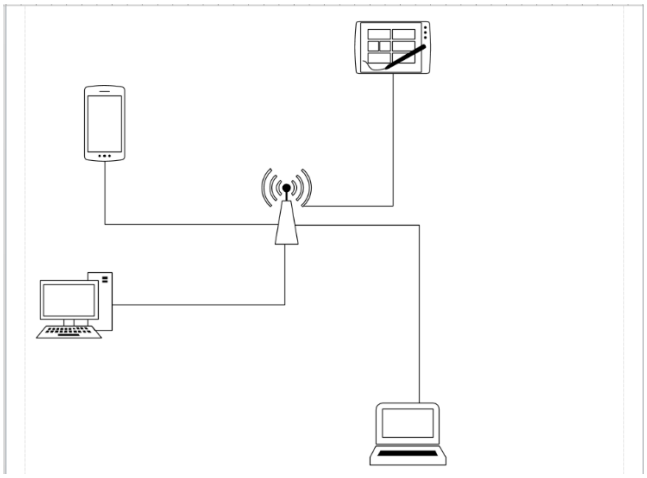
1. Osnovni servisni set (engl. *BSS – Basic Service Set*)
2. Prošireni servisni set (engl. *ESS – Extended Service Set*)
3. Nezavisni osnovni servisni set (engl. *IBSS – Independent Basic Service Set*)

Svaki od tih sustava ima svoj različiti način rada te različiti hardverski set opreme.

2.2.1. Osnovni servisni set (BSS)

Set sastavljen od jedne pristupne točke te više stanica kao što je prikazano na **Error! Reference source not found.**a. Stanice su u principu uređaji poput mobitela, laptopa, tableta kojima se želimo spojiti na bežičnu mrežu. Pristupna točka (engl. *Access point*) kontrolira promet svih stanica te preko nje uređaji komuniciraju. Uređaji u ovakvoj topologiji ne mogu komunicirati zasebno jedni s drugima već je to moguće preko pristupne točke koja prosljeđuje okvire odredišnim stanicama. Pristupna točka funkcionira putem emitiranja signala te vlastitog identifikatora skupa usluga SSID (engl. *Service set identifier*). Svaki

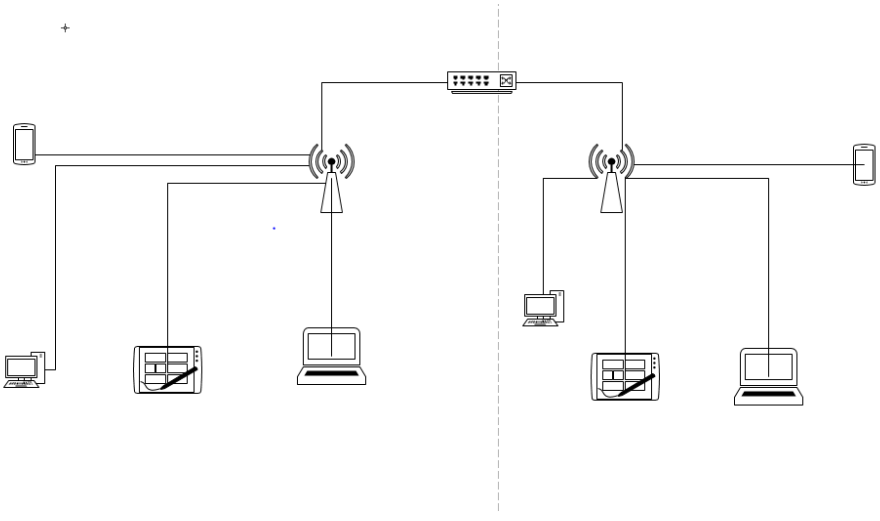
uređaj koji želi pristupiti prvo mora poslati zahtjev za pristupanjem te ispuniti kriterije poput autentifikacijskih podataka.



Slika 2.1 - Prikaz osnovnog servisnog seta

2.2.2. Prošireni servisni set (ESS)

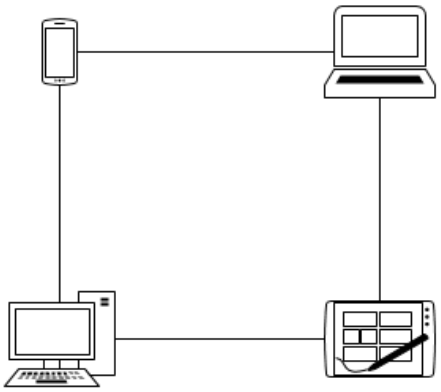
Prošireni servisni set je zapravo dvoje ili više spojenih osnovnih setova sa pripadajućim vanjskim uređajem, poput preklopnika spojenih na ožičenu mrežu prikazanih na **Error! Reference source not found.**. Stanice odnosno uređaji u zasebnim servisnim setovima koji se nalaze u proširenom servisnom setu mogu komunicirati te ne zahtijevaju identični SSID u svim pripadajućim setovima. Kod spominjanja proširenog servisnog seta potrebno je spomenuti i roaming, odnosno sposobnost prelaska iz jednog seta u drugi bez gubitka veze, pri čemu je veza između njih neprekidna.



Slika 2.2 - Prikaz proširenog servisnog seta

2.2.3. Nezavisni osnovni servisni set (IBSS)

Servisni set koji ne zahtjeva postojanje pristupne točke ili bilo kojeg drugog uređaja za mrežno spajanje kao što je moguće vidjeti na **Error! Reference source not found.**. Bilo koji uređaj, koji ima pristup mreži u dometu bilo kojeg drugog može komunicirati ukoliko se dogovore u nekoliko osnovnih parametara. Ukoliko jedan od tih uređaja također ima pristup ožičenoj mreži, može omogućiti isto i drugim uređajima. Takav način rada se najčešće naziva *Ad-Hoc* ili *Peer to Peer* način rada.



Slika 2.3 - Prikaz nezavisnog osnovnog servisnog seta

2.3. Standardi

Govoreći o bežičnim standardima oni se vežu za Institut električnih i elektroničkih inženjera IEEE (engl. *Institute of Electrical and Electronic Engineers*). IEEE objavljuje standarde za mnoge sisteme, počevši od energetskih sustava pa sve do glasačkih sustava. Međutim organizacija je poznata po svojim standardima o prijenosu podataka između računala. Standardi su odrađeni od strane volontera, odnosno eksperata zaposlenih u računalnoj industriji [3].

Standard koji se veže striktno za bežične mreže je standard IEEE 802.11 te on definira bitne parametre počevši od arhitektura pa sve do sigurnosnih algoritama.

2.3.1. IEEE 802.11

Standard 802.11 ima mnogo inačica, no ovdje su spomenuti samo oni, koji se smatraju bitnima te koji su donijeli određene promjene. Započinjemo sa standardom 802.11b, koji je prvi bio globalno prihvaćen među korisnicima. Odgovoran je za početak korištenja prvog vala kućne bežične mreže, kompanije s mrežnom opremom poput Linksys-a počele su s prodajom Wi-Fi routera uz žični internet [4].

Radi na frekvencijskom spektru od 2412 do 2484 MHz sa promjenjivim brojem kanala koji se preklapaju. Napravljen je da prenosi podatke brzinom do 11 Mbit/s, iako je realna brzina 40-50 Mbit/s sa dometom u prosjeku od 30 m. Pri prijenosu podataka 802.11b koristi CSMA/CA (engl. *Carrier Sense Multiple Access/Collision Avoidance*) tehniku definiranu u izvornom standardu 802.11, koristeći ovu tehniku kada čvor želi izvršiti prijenos, osluškuje čisti kanal te prenosi, ukoliko ne dobije potvrdu govora čekaju slučajno izabrano vrijeme i pokušava ponovno.

Pojavom 802.11g zamijenjen je standard 802.11b. Djelujući u istom frekvencijskom spektru podržavajući brzine prijenosa podataka do 54 Mbit/s te dometom od 45 m uvelike je prestignuta specifikacija od prijašnjih verzija. Napravljena tako da spaja najbolje od prijašnjih standarda u jedno, verzija 802.11g uvelike je zaživjela u tehnološkoj industriji.

Najveći pomak dogodio se pojavom 802.11n verzije koji donosi tehniku odašiljanja u više slojeva MIMO (engl. *Multiple Input Multiple Output*) tehnologiju, koja koristi istovremeno slanje i primanje sa nekoliko antena i prijemnika, odnosno odašiljača. Radeći na frekvencijskom spektru od 5 GHz uz prijašnjih 2,4 GHz te brzinom prijenosa podataka od 600 Mbit/s uvelike je odskakala od prijašnjih standarda.

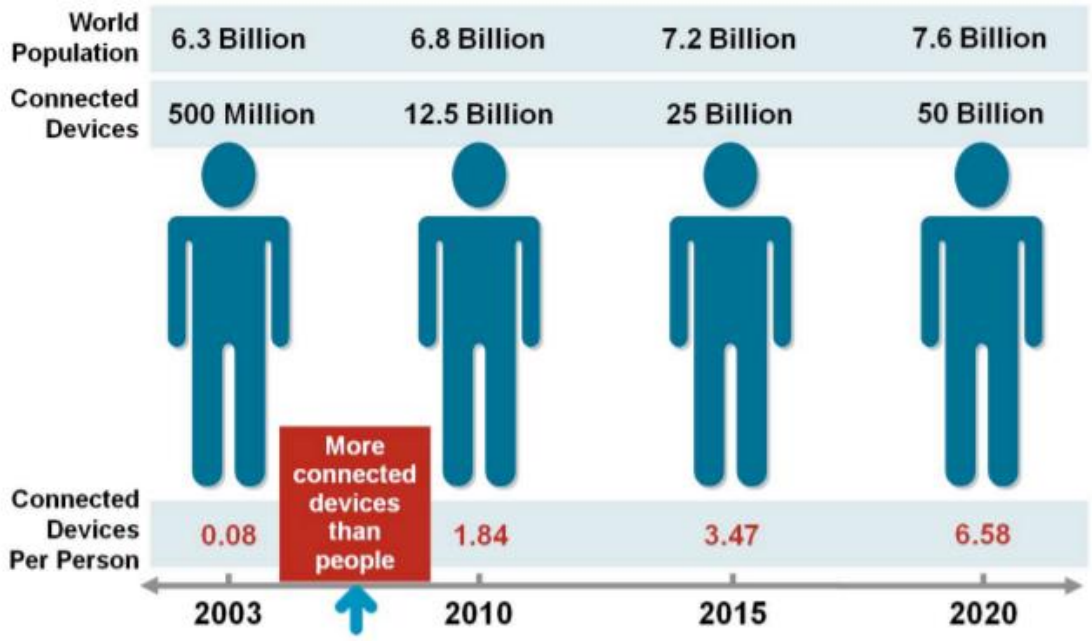
Svi noviji standardi kompatibilni su sa starijima, odnosno oprema koja podržava primjerice 802.11n podržava i starije poput 802.11b ili 802.11a. Govoreći o novijim standardima vrijedno je spomenuti i 802.11ac te standard, koji je posljednji izašao, 802.11ax sa brzinom prijenosa podataka do nekad nezamislivih 10 Gbit/s

Kada govorimo o bežičnim mrežama svima je opće poznat pojam pod nazivom Wi-Fi. Wi-Fi odnosno punog imena Wifi Alliance je neprofitna organizacija skupine proizvođača hardvera, koja se obvezala da će svoje uređaje podvrgnuti rigoroznim testovima kompatibilnosti i interoperabilnosti kako bi jamčila da oprema različitih proizvođača može funkcionirati i komunicirati međusobno [5]. Bazirani su na IEEE 802.11 standardima, no

unatoč tome nije svaki uređaj koji koristi IEEE 802.11 standarde Wi-Fi licenciran. Wi-Fi Alliance je zbog komplikacija duljine naziva IEEE standarda odlučio neke od tih naziva preimenovati u jednostavnije poput Wi-Fi 6 koji je zapravo 802.11ax, odnosno Wi-Fi 5 koji je 802.11ac.

2.4. Svrha korištenja

Zbog svojih prednosti bežičnog spajanja te samim time i mobilnosti, bežične lokalne mreže uvelike se koriste u raznim poduzećima, bolnicama, školama i ostalim ustanovama. Korištenjem više pristupnih točaka ta mobilnost se dodatno pospješuje te omogućuje korištenje s minimalnim ili nikakvim gubitkom podataka na većim područjima kao što su to zgrade. Prema nekim istraživanjima bežično spajanje prestiglo je žično u postocima korištenja te se na njemu razvijaju tehnologije za budućnost. Tehnološka kompanija Linksys navela je kako Wi-Fi tehnologija ubrzano raste te tako moraju i pametni uređaji kako bi držali korak s time [6]. Već ove godine broj spojenih uređaja prešao je brojku od 50 milijuna kao što vidimo po usporedbi na Slika 2.4 - Uređaji sa mogućnošću spajanja na bežične mreže [7].



Slika 2.4 - Uređaji sa mogućnošću spajanja na bežične mreže [7]

3. *Sigurnost bežičnih mreža*

Sigurnost bežičnih mreža jedan je od krucijalnih segmenata. Kada govorimo o korištenju istih, rijetko tko je ustvari svjestan svoje sigurnosti odnosno nesigurnosti. Nedovoljnom zaštitom i nepažnjom dovodimo svoje podatke u veliku opasnost. Najveći problem današnjice, kada govorimo o sigurnosti, je neupućenost. (Velika većina korisnika smatra kako je riješena njihova zaštićenost tako što dobiju potrebne uređaje i određene instalacije. Međutim sigurnost je puno više od jedne lozinke postavljene na uređaj. Za razliku od žičnih mreža, bežične je puno teže zaštititi te se ne mogu koristiti istim tehnikama zaštite.

Svaki uređaj koji ima nezaštićen ili slabo zaštićen izlaz na Internet je doveden u opasnost. Virusi i neželjene poruke su postali svakodnevni problem, no tu su i računalne prijevare, napadi uskraćivanjem pristupa te još niz mogućih napada.

3.1. Sigurnosni standardi

Sigurnosni standardi omogućavaju siguran prijenos podataka u bežičnoj mreži. Kada govorimo o sigurnosnim standardima vezanim za bežičnu komunikaciju, uglavnom govorimo o WEP (engl. *Wired Equivalent Privacy*) te WPA (engl. *Wi-Fi Protected Access*) standardima.

Usporedba sigurnosnih standarda prema njihovim specifikacijama prikazana je u Tablica 3.1 – Usporedba sigurnosnih standarda. Korisnici uglavnom nisu upućeni u važnost izbora sigurnosnog standarda te kao takvima još uvijek koriste standard, koji je pokazao svoje slabosti samo zbog njegove inicijalne pojave na usmjerniku.

3.1.1. WEP

WEP (engl. *Wired Equivalent Privacy*) standard napravljen je s ciljem onemogućavanja nedozvoljenog pristupa mreži. Kada se govori o žičnoj mreži napadač treba imati fizički pristup ethernet uređaju, dok kod bežične mreže je posao napada olakšan, jer nema potrebe za fizičkim pristupom. Upravo iz toga razloga, kako bi otežao napad na bežičnu lokalnu mrežu, napravljen je WEP. Standard koristi simetrični RC4 enkripcijski algoritam i glavna

karakteristika mu je korištenje istog ključa za enkripciju te dekripciju, kojega je lako probiti izravnim izračunom mogućih ključeva.

WEP je već bio daleko u uporabi kada su kriptografi i računalni eksperti otkrili njegove mane. Postalo je očito kako ne funkcionira onako kako je inicijalno osmišljen. Ovaj standard danas se još koristi iako je proglašen zastarjelim 2004. godine od strane IEEE. Koristi se u inicijalnim postavkama uređaja dobivenih od pružatelja mrežne usluge te u zastarjelim uređajima koji jednostavno nemaju mogućnost korištenja novijih standarda.

3.1.2. WPA

Uvidjevši kako je WEP standard preslab, odnosno ne pruža više kvalitetnu zaštitu nastao je WPA standard sa ciljem eliminiranja svih sigurnosnih slabosti. Nastao je od strane Wi-Fi alliance udruženja kao privremena mjera za bolje očuvanje podataka. Standard koristi 256 bita za ključ i pokriva kompletnu komunikaciju. Postoje zapravo dvije pod- varijante WPA zaštite – WPA-PSK te WPA- Enterprise, koji zahtjeva primjenu RADIUS poslužitelja te ga je teže konfigurirati.

WPA kao i WEP koristi RC4 enkripcijski algoritam, no sada sa dinamičkim mijenjanjem ključeva za vrijeme korištenja sustava. Prednost WPA je mogućnost ugradnje u postojeću mrežnu opremu bez većih ulaganja. Ovaj standard eliminirao je slabosti prethodnog sustava uvođenjem dugačkog incijalizacijskog vektora (IV) i TKIP protokola radi obrane od napada kakvi se koriste za otkrivanje ključa u WEP protokolu [8].

3.1.3. WPA2

Kasnijim uvođenjem nadogradnje odnosno izbacivanjem WPA2, sustav je postigao kvalitetnu zaštitu. Prelazak na AES algoritam umjesto RC4 pokazao se pravim izborom. Promijenjen je i način rada sa ključevima koji sada nikada ne kolaju mrežom, nego se njihova ispravnost provjerava takozvanim četverosmjernim rukovanjem, sustavom koji osigurava da u četiri koraka oba sudionika u komunikaciji provjere zna li druga strana ispravni ključ.

WPA2 standard je uvelike otežao napade hakerima te samo oni s ozbiljnim hardverom i opremom mogu ugroziti sustav zaštićen navedenim standardom [9]. Osnovni nedostatak

WPA2 standarda je potrebito ulaganje u novu mrežnu opremu, koja može raditi na AES algoritmu bez padanja performansi.

3.1.4. WPA3

Standard objavljen početkom 2018. godine još nije definitivno zaživio u korisničkim usmjernicima te se čeka njegova zamjena prijašnjih standarda. Glavni cilj WPA3 je otežavanje probijanja mreža, što je moguće na do sada svim prijašnjim standardima. Jedan od poznatijih mrežnih proizvođača „*Cisco*“ glasi za jednog od većih zagovornika ovoga standarda te aktivno djeluje na uvrštavanju istog u svoju opremu.

Sa poboljšanim performansama zaštite poput SHA-2 integracije i povećane veličine ključeva, sigurnost kod ovoga standarda je zajamčena, no sada je sve na poslovnom sektoru, odnosno na pružateljima mrežne usluge kako bi zamijenili uređaje kod korisnika, koji su zastarjeli te nemaju tu mogućnost u svojim postavkama.

Tablica 3.1 – Usporedba sigurnosnih standarda

	WEP	WPA	WPA2	WPA3
Algoritam	RC4	RC4	AES	AES-CCMP
Integracija	CRC 32	MIC	CCM	SHA-2
Veličina ključa(bit)	40 ili 104	128	128	128 ili 256
Rotacija ključeva	Ne	Dinamička	Dinamička	Dinamička
Sigurnost	Loša	Srednja	Dobra	Izvrsna
Autentifikacija	Ne	802.1x, EAP/PSK	802.1x, EAP/PSK	SAE

3.2. Sigurnosni propusti

U današnje vrijeme bežične mreže su dostupne svima, ukoliko ne u domaćinstvu, onda u kafićima ili na ostalim mjestima okupljanja, koji imaju svoje mreže dostupne gostima. Sigurnosni propusti kod bežičnih mreža odnose se na nedovoljnu razinu zaštite. Samim spajanjem na neku nepoznatu mrežu dovodimo svoj uređaj u opasnost te mogućnost manipuliranja uređajem od strane osobe, koja ima nadzor nad mrežom.

Potpunu sigurnost je gotovo pa nemoguće ostvariti, no isto se može približno ostvariti čineći potrebne korake. Prije spomenuti sigurnosni standardi pomažu nam u očuvanju privatnosti podataka, no od velike važnosti su i faktori ljudske djelotvornosti. Pojedini segmenti poput promjene imena usmjernika i veličine zaporke čine se manje bitnima, no u široj slici itekako su važni. Primjerice promjenom inicijalnog naziva usmjernika dobivenog od pružatelja mrežne usluge možemo napadačima otežati saznavanje vrste usmjernika te potencijalno spriječiti napad na naše podatke i privatnost.

Naša privatnost i naši podaci trebali bi biti najvažnija stavka prilikom očuvanja sigurnosti, no korisnici unatoč tome rade greške poput slanja informacija putem javno dostupnih mreža kao što je prikazano na Slika 3.1 - Prijenos informacija putem javne mreže [10].

Slika 3.1 - Prijenos informacija putem javne mreže [10]

3.2.1. Pasivni i aktivni napadi

Napade na bežične mreže dijelimo na pasivne i aktivne. Razlika između njih je ta, da kod pasivnih napada napadač samo osluškuje signal te prikuplja informacije dok kod aktivnog napadač iskorištava isti taj signal i informacije kako bi ugrozili korisnika.

Pasivni napad bazira se na prikupljanju podataka o željenoj mreži izravnim slušanjem svih podataka koje sudionici u mreži odašilju u prostor. Naravno, takvi napadi imaju ograničenja te su znatno manje opasniji te sporiji od aktivnih napada. Pasivne napade je gotovo nemoguće otkriti, jer ne ostavljaju nikakve zapise niti tragove. Može se reći da takvi napadi služe za stvaranje slike napadnute mreže, kako je povezana te što se u njoj koristi.

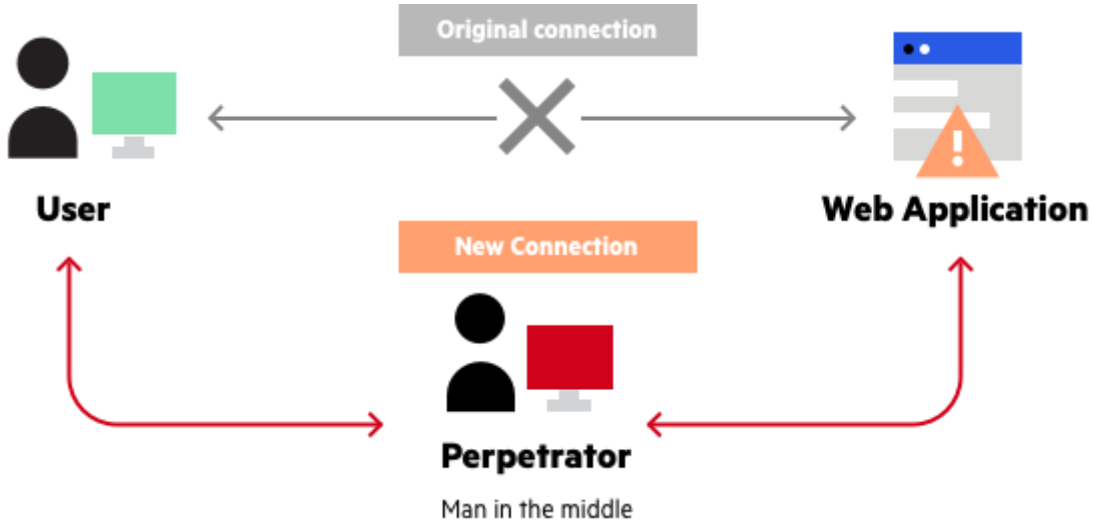
Za ovu vrstu napada dovoljna je antena, mrežna kartica i softver koji će analizirati veličinu i broj paketa. Jedini uvjet kako bi se ostvario pasivni napad je pristup signalu mreže gdje dolazi do izražaja fizička sigurnost mreže. Pasivnim napadom dolazi se do podataka o količini mrežnog prometa napadatnute mreže, lokaciji pristupnih točaka te vrsti protokola koji se na mreži koriste. Prilikom pasivnog napada na mrežu, u opasnosti je povjerljivost kao što je prikazano na Slika 3.2 - Pasivni napad na mrežu [11].

Slika 3.2 - Pasivni napad na mrežu [11]

Kod aktivnog napada prelazi se na uplitanje u napadnutu mrežu odnosno slanje paketa ili okvira u komunikaciji sa odabranom mrežom. Također napad se koristi lažnim predstavljanjem kao sudionik mreže tako prikupljajući potrebne podatke. Cilj aktivnog

napada je promijeniti specifikacije određene mreže kako bi pridobili željene podatke. Međutim aktivni napadi su puno lakši za uočiti od pasivnih zbog njihovog djelovanja, no kod loše konfiguriranih mreža mogu prouzročiti puno štete. Prilikom aktivnog napada uvijek se prouzroči neka šteta na mreži te ugrozi intergritet i dostupnost iste.

Jedan od najpoznatijih aktivnih napada naziva se čovjek u sredini (engl. *Man in the middle*), koji se koristi za čitanje i modifikaciju podataka. Napadač se u ovom slučaju postavlja u komunikacijski kanal između korisnika i pristupne točke gdje presreće komunikaciju te izvodi napad. Izvršavanjem napada ne dopušta korisniku ponovno spajanje s pristupnom točkom. Umjesto spajanja na pristupnu točku, korisnik zapravo uspostavlja vezu sa napadačevim računalom nakon kojeg se napadač predstavlja pristupnoj točki kao napadnuti korisnik te uspostavlja vezu s njom. Napad je grafički prikazan na Slika 3.3 - Man in the middle napad [12].



Slika 3.3 - Man in the middle napad [12]

4. Testiranje

Radi otkrivanja koliko su korisnici zapravo sigurni u svojem korištenju bežične lokalne mreže, napravljeno je testiranje na osnovu korištenog sigurnosnog standarda kako bi se dokazala sigurnost odnosno nesigurnost ljudi. Nakon testiranja istim ispitanicima predloženi su određeni savjeti kako bi se pravovaljano zaštitili te kako ne bi imali neovlaštenih upada na mrežu.

4.1. Oprema

Oprema odnosno resursi korišteni za ovaj rad sastoje se od softverskog i hardverskog dijela. Oprema kao takva pretežito je besplatna za korištenje, izuzev hardverskog dijela. Softverski dio sastoji se od:

- Oracle VM VirtualBox
- Operacijski sustav Kali Linux
- Wireless alati sustava Kali Linux, posebice aircrack-ng
- Wireshark

Hardverski dio sastoji se od:

- Laptop Dell Vostro 3580
- Wireless adapter TP-Link TL-WN722N

4.1.1. Softver

Oracle VM VirtualBox je računalni softver za virtualizacijsko okruženje, koji je izabran usprkos velikom izboru kvalitetnih softvera. Isprobane su i druge inačice poput VMware Horizon Clienta te Hyper-V hypervisora, no zbog komplikacija izazvanih verzijama podržavanja potrebnih uređaja te nemogućnosti pravovaljanog očitavanja izbor je ostao na VirtualBoxu.

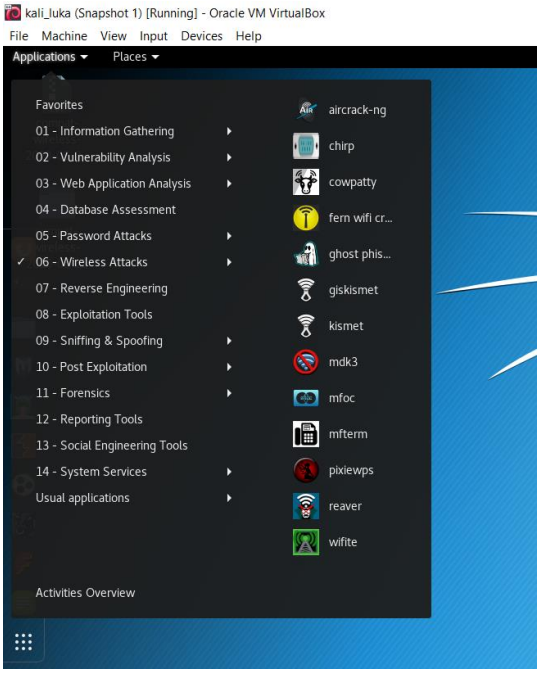
Navedeni softver se može legalno te potpuno besplatno preuzeti sa njihove službene stranice [13]. Instalacija istog potpuno je jednostavna te ne stvara nikakve komplikacije. Unutar

spomenutog softvera potpuno jednostavno može se spremiti trenutno stanje pomoću korištenja snimka (engl. *snapshot*), što je od velike koristi zbog potreba praćenja pojedinih stanja.

Kali Linux operacijski sustav pokrenut je unutar VirtualBoxa. Svrha mu je korištenje za penetracijsko testiranje te etičko hakiranje. Njegovi alati iskorištavaju se za nalaženje mana sustava, međutim isti se svejedno iskorištavaju u ilegalne svrhe te hakiranje u svrhe napada te krađe podataka. Kali Linux odabran je radi poznatog okruženja te prijašnjeg korištenja. Zadovoljava potrebe rada te omogućava sve potrebno kako bi rad bio ostvaren kvalitetno.

Instalacija samog sustava pretežito je jednostavna ukoliko se izabere putem grafičkog sučelja, prije same instalacije jedino je potrebno dodati datoteku instalacije preuzetu sa njihove službene stranice u virtualnu mašinu. Potrebni resursi za instalaciju sastoje se od: minimalno 3GB tvrdog diska(engl. *hard disk*) te minimalno 512MB RAM-a (engl. *Random Access Memory*) što u principu imaju sva računala unutar zadnjih 10-15 godina.

Kao što je navedeno Kali sadrži alate za prikupljanje informacija u svrhu otkrivanja slabosti prikazane na **Error! Reference source not found.**, za ovaj rad korišteni su samo wireless alati te wireshark, alat za „snifanje“ prometa.



Slika 4.1 - Prikaz dostupnih alata Kali inuxa

Glavni alat korišten u radu naziva se aircrack-ng. To je u principu kodirani program unutar terminala gdje se putem naredbi dolazi do željenih rezultata. Navedeni program pretražuje bežične mreže u okolici te otkriva podatke o njima. Ukoliko su mreže slabo zaštićene, primjerice WEP sigurnosnim standardom lako ih je probiti te otkriti pristupne podatke za ulaz u mrežu. Od softverskih alata koristili smo još Wireshark , alat isključivo korišten za analizu paketa na određenim mrežama koje smo u ovom radu analizirali.

4.1.2. Hardver

Od hardverske opreme korišteno je privatno prijenosno računalo marke Dell, koje ima sve potrebne specifikacije za kvalitetno pokretanje potrebnih alata bez ikakvih poteškoća ili eventualnih prekida rada. Uz prijenosno računalo kupljen je wireless adapter marke TP-Link kako bi uspješno bile pronađene mreže u blizini te kako bi pojačali signal za lakše dohvaćanje željenih mreža. Navedeni adapter bilo je potrebno dodati ručno unutar virtualne mašine te instalirati ga u skladu sa trenutnom verzijom.

4.2. Provođenje testiranja na lokacijama

Testiranje je provedeno na lokacijama pojedinih kućanstava, mjestima okupljanja manjeg broja ljudi, u ovom slučaju kafića te u manjim poduzećima. Testiranje je provedeno u vremenskom razdoblju od 4 mjeseca uz privolu nadležnih osoba. Cilj je analiziranje sigurnosti mreže navedenih lokacija, te po potrebi predlaganje kako se bolje osigurati u svrhu zaštite.

Testirane lokacije nisu izabrane slučajno, već u dogovoru sa vlasnicima. Lokacije se nalaze na više mjesta područja grada Zagreba, pretežito u istočnom dijelu grada radi lakše dostupnosti. Na slici Slika 4.2 - Prikaz geografskih lokacija testiranja označene žutom bojom vidljive su lokacije ispitanih na području grada. Testiranje se provodilo unutar objekata uz maksimalan pristup signalu pomoću hardverske opreme.

Slika 4.2 - Prikaz geografskih lokacija testiranja

4.3. Analiza rezultata

Prilikom korištenja ranije navedenih alata analizirani su željeni podaci bežične sigurnosti. Primarni cilj ove analize je otkrivanje mogućnosti ulaska u mrežu. Pomoću alata aircrack-ng očitavane su dostupne mreže u blizini te pronađene mreže objekta u kojem se nalazimo te nad kojim je izvršeno testiranje.

Analizom je definiran izvještaj, koji služi za procjenu razine sigurnosni testiranih lokacija. Analiza je provedena nakon svakog testiranja zasebno, odnosno nakon svake lokacije koja je testirana. Iako je ovakav način testiranja u principu ilegalan, od iznimne je koristi za dobivanje podataka potrebnih za analizu te je proveden uz dozvolu. Analiza je provođena uz prisutnost testiranih kako bi uživo vidjeli vlastite rezultate sigurnosti.

Navest ćemo primjer naredbi za probijanje mreže odnosno dobivanja podataka za spajanje na istu:

airmon-ng start wlan0 – Pokrećemo alat te te sučelje na kojem se nalazi bežična kartica.

airodump-ng wlan0mon – Putem navedene naredbe očitavamo aktivne mreže u blizini. Željena mreža prikazana je na Slika 4.3 - Odabrana korisnička mreža

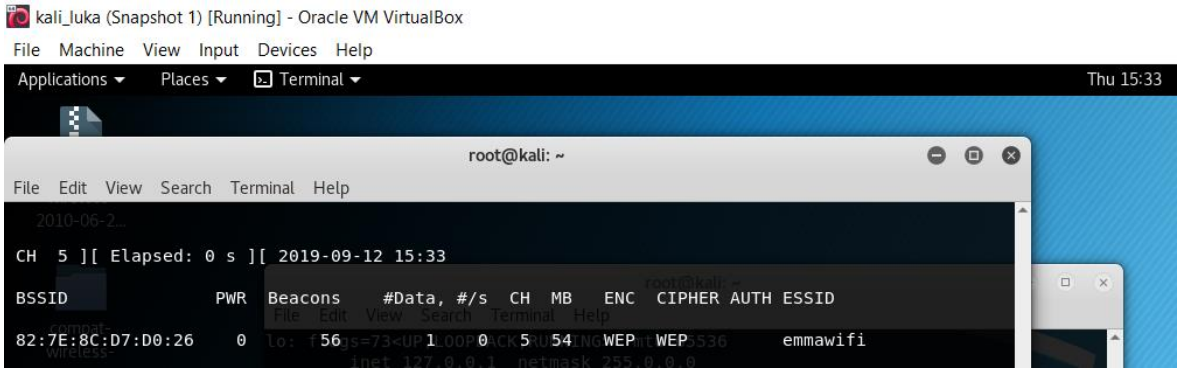
airodump-ng -c 5 –bssid 82:7E:8C:D7:D0:26 –write Emma wlan0mon – Slovo c označava kanal na kojem pristupna točka rada, u ovom slučaju radi se o 5. kanalu. Bssid označava MAC (engl. *Media Access Control*) adresu analiziranog uređaja, dok stavka write označava željeni naziv datoteke gdje spremamo podatke o paketima. Ovom naredbom se fokusiramo samo na željenu mrežu te nju nadziremo.

aireplay-ng -0 1000 –a bssid 82:7E:8C:D7:D0:26 -e emmawifi wlan0mon – Nadalje se odrađuje takozvani *deauth* napad, odnosno napad kojima se isključuju svi uređaji do tada spojeni na mrežu. Broj 0 označava *deauth* napad, 1000 označava broj paketa koji se šalju. Naredbom -a se označava MAC adresu dok naredbom -e se zapisuje ESSID odnosno naziv mreže.

Nakon odrade *deauth* napada dobiveni su podaci o WEP *handshake*-u, gdje se također može raditi o WPA te WPA2 *handshake*-u, no kod njih je vrijeme za dobivanje lozinke puno veće. Sada možemo otkriti šifru navedene mreže.

aircrack-ng 1-01.cap –w /usr/share/passwords.txt – Završnim korakom otvara se datoteka(1-01.cap) gdje su pohranjeni uhvaćeni podaci te uspoređuje sa datotekom sa učestalim lozinkama koja je preuzeta sa interneta.

Odradom ovoga napada uspješno smo došli do šifre koja je u ovom slučaju bila 87654321.

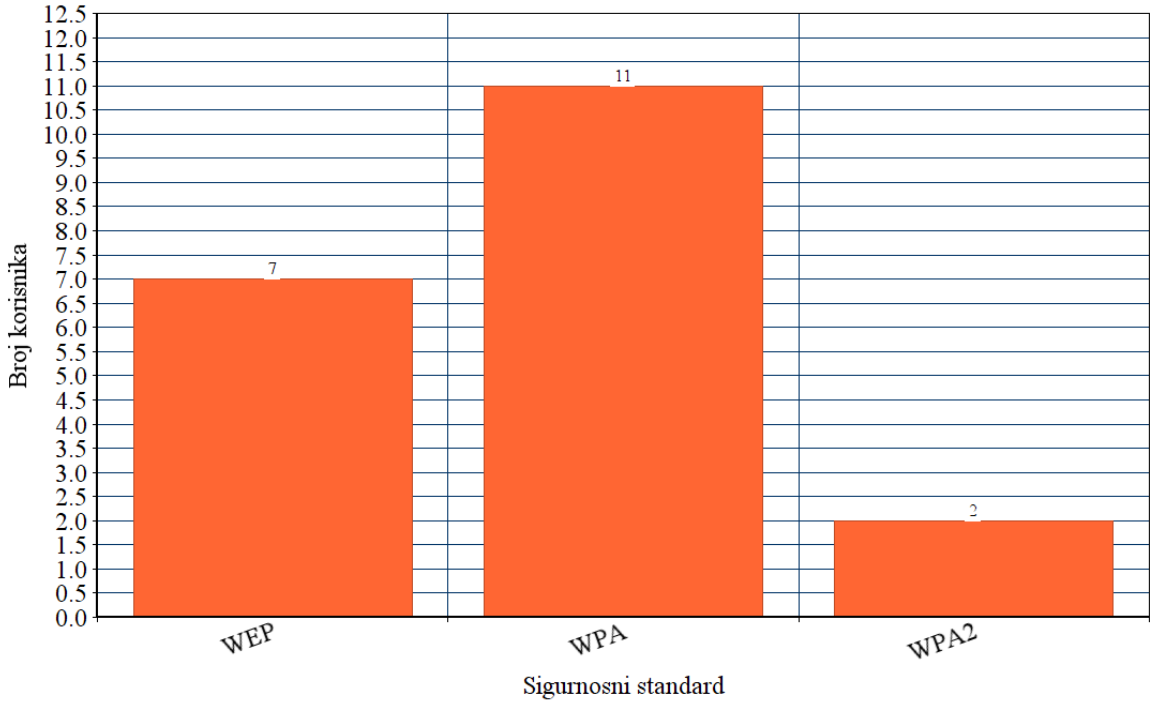


Slika 4.3 - Odabrana korisnička mreža

4.4. Definiranje izvještaja

Na početku je važno napomenuti kako nijedna od osoba nad kojima je izvršeno testiranje nije znala koji sigurnosni standard ima na bežičnoj mreži. Prilikom testiranja rezultati tih istih sigurnosnih standarda su također porazni. Na dvadeset korisnika samo dvoje su imali nužni WPA2 standard kao što je prikazano na **Error! Reference source not found.**

Računajući da su ti korisnici manja poduzeća, dok kafići i ostala manja mjesta javnog okupljanja imaju pretežito WPA zaštitu, a kućanstva nažalost WEP.



Slika 4.4 - Sigurnosni standardi kod ispitanih korisnika

Nadalje samo petero ispitanika je izmjenilo šifru nakon dobivanja usmjernika od pružatelja mrežne usluge te samo istih tih petero je promijenilo i inicijalni naziv. Prikupljene lozinke bile su ili inicijalno dobivene ili pretežito sastavljene od imena i brojeva, ponegdje i samo brojeva.

Prema istraživanju provedenom na području grada Zagreba dokazano je da korisnici rijetko mijenjaju ono što im operater postavi kao ime mreže te da broj korisnika bez zaštite ili onih sa WEP zaštitom dolazi do brojke od 20% po čemu se da zaključiti da je broj nezaštićenih prevelik [14]. Utvrđeno je da korisnici jednostavno nisu dovoljno upućeni, mrežni operatori nisu ponudili nikakvu pomoć po tome pitanju te korisnici nisu znali koliko su u principu slabo zaštićeni.

5. Metode zaštite

Kada govorimo o sigurnosti moramo znati da je apsolutnu sigurnost nemoguće ostvariti, te da sigurnost nije proizvod već proces na koji je potrebno učestalo paziti. Prilikom zaštite potrebno je ostvariti pouzdanu autentifikaciju korisnika, zaštitu privatnosti i autorizaciju korisnika. Objašnjeno je kako se kvalitetno zaštititi na razini kućanstava i manjih javnih prostora te na razini manjih poduzeća.

5.1. Korištenje alata za zaštitu

Iako nema pretežito mnogo alata koji se mogu koristiti za zaštitu, važno je znati kako se može zaštititi već izmjenom inicijalnog naziva te šifre. Pomoću pristupnih podataka moguće je spojiti se na korisničko sučelje dobivenog usmjernika te podesiti željene parametre poput već spomenutih naziva, lozinki, kanala, sigurnosnih standarda.

Lozinka koju je potrebno koristiti mora biti snažna te treba se sastojati od:

- Minimalno 12 znakova
- Sadrži slova, brojeve, barem jedno veliko slovo te posebnih znakova poput $
- Nije povezana sa našim imenom
- Ne mjenja slova za očite brojeve, poput O i 0

Preporuča se također i isključivanje bežične mreže dok nismo u dometu iste. Kroz vatrozid (engl. *firewall*) mogu se napraviti određena pravila što može biti dostupno, a što ne može, kako bi se još bolje zaštitili od nepoželjnih napada.

5.2. Preporuka zaštite za kućanstva i manje javne prostore

Zaštita kućanstva i manjih javnih prostora zasniva se na privatnoj zaštiti, zaštiti koja se može provesti bez dodatnih ulaganja i hardvera. Prvi korak zaštite je prelazak na WPA3 enkripciju

ukoliko je to moguće, ukoliko nije zbog učestale zastarjele opreme onda na WPA2-PSK (AES) koju je trenutno teško probiti.

Promjena lozinke i inicijalnog naziva u druge nazive i sigurnije jače lozinke također su jedne od važnijih stavki kod zaštite. Vrijeme probijanja lozinke zasniva se na kompleksnosti složene lozinke. Što je lozinka kompleksnija te duža, vrijeme probijanja se povećava. Na razini kućanstva moguće je ograničiti spajanje uređaja prema njihovoj fizičkoj adresi, što nažalost radi svakodnevnih novih korisnika nije moguće na manjim javnim prostorima poput kafića.

Gašenjem bežičnog uređaja po izlasku iz doma smanjuje se mogućnost neovlaštenog napada tokom našeg odsustva, također štitimo i uređaj od mogućih oštećenja izazvanih prekidom električne energije. Iako možda nije od prevelike koristi u javnim prostorima, u kućanstvima je pozicija usmjernika bitna stavka, kako bi imali što bolji signal, sredina stana/kuće najbolja je pozicija, dok pozicija bliže prozorima na rubnim dijelovima kuće omogućava bolji vanjski signal te lakši pristup napadačima.

Prilikom slaganja mrežnih postavki koristi se administratorsko sučelje, koje najčešće dolazi sa inicijalnim korisničkim imenom te lozinkom, koja najčešće bude kombinacija poput admin, password. Iste je potrebno promijeniti u nešto složenije

Ažuriranje usmjernika je isto tako bitna stavka, iako većinom kod uređaja u našem domu ili prostorima to nije moguće, kontaktiranjem pružatelja mrežne usluge to možemo zatražiti kako bi to napravili. Ukoliko postoji mogućnost vatrozida, isti je potrebno aktivirati u mrežnim postavkama kako bi unaprijed bili odbijeni potencijalni napadi. Svi ti koraci nužni su za pravovaljanu zaštitu, iako izgledaju na prvi pogled komplicirano te da uzimaju previše vremena, ukoliko želimo sigurnost svojih podataka vrijedni su implementacije.

5.3. Preporuka zaštite za manja poduzeća

Prilikom zaštite poduzeća uz sve gore navedene korake potrebni su ipak još neki dodatni zbog vjerojatne dodatne mrežne opreme. Poduzeća su mete stalnih hakerskih napada kako kroz pretraživanja otvorenih portova tako kroz napade uskraćivanjem usluge. Svako poduzeće trebalo bi koristiti privatnu mrežu VPN (engl. *Virtual Private Network*) kako bi

osigurali nesmetano spajanje sa udaljenih lokacija. Sama konfiguracija takve mreže nije pretežito kompliciranа te se sastoji od svega par koraka.

Nadalje preporuča se korištenje *SSH* protokola kod spajanja umjesto popularnog *Telnet* spajanja, jer kod *Telnet* spajanja lakše je neautoriziranim korisnicima upasti u mrežu radi prisutnih mana tog protokola. Kod poduzeća, kako velikih tako i manjih većinom se dodatno kupuje i dodatna mrežna oprema uz postojeću od mrežnog poslužitelja. Na navedenoj opremi poput Ciscove, HP-ove moguća je konfiguracija sigurnosnih aspekata mreže.

Primjer tipa konfiguracije je uspostavljanje IPsec (engl. *Internet Protocol Security*) protokola kada smatramo da je mreža nesigurna. Konfiguracijom IPsec-a uspostavljaju se tuneli sigurne komunikacije, prije no što se korisnik prilikom spajanja na bežičnu mrežu, putem tunela prvo se spaja na žičnu mrežu i samo kroz taj sigurni tunel komunicira sa drugim korisnicima u mreži.

Također se koristi i *RADIUS* server koji služi za autentifikaciju korisnika putem žične ili bežične mreže. Putem njega odobravamo korisnike koji mogu pristupiti mreži sa svojim korisničkim imenom i šifrom te raditi izmjene i vršiti komunikaciju. Ukoliko imamo više uređaja spojenih na glavni mrežni uređaj bilo bi dobro odvojiti ih u druge mreže odnosno *VLAN-ove*. Bežične uređaje poput pristupnih točaka bi stavili u zasebni *VLAN*, da ukoliko dođe do fizičkog spajanja napadač bi morao točno znati u kojem *VLANU* se oni nalaze.

Zaštita poduzeća varira do razine i količine mrežne opreme, na temelju tih podataka može se odrediti i klasificirati kvalitetna razina zaštite. Prema mojem mišljenju svako poduzeće bi trebalo imati vlastitog informatičara upoznatog u sigurnosne aspekte, no iz vlastitog radnog iskustva nažalost takve stvari nisu česte te tek nakon što se problem dogodi i mreža već bude napadnuta poduzimaju se koraci. Tada većinom bude već prekasno te se radi samo na spašavanju mogućih podataka.

6. Zaključak

Provedenim istraživanjima u sklopu ovoga rada ustanovljeno je da korisnici nisu dovoljno upućeni u problematiku sigurnosti korištenja bežičnih mreža. Koliko god to izgledalo kao propust korisnika, smatram da je to zapravo propust nadležnih regulatornih državnih agencija (HAKOM) i pružatelja usluge u kontekstu nedovoljne brige o tom važnom sigurnosnom aspektu. Pod brigom mislim na nedovoljnu edukaciju i senzibilizaciju šire javnosti, koja treba započeti u obrazovnim ustanovama vrlo rano jer djeca kao najranjivija skupina i digitalne usluge počinju koristiti vrlo rano. Tehnologija stalno napreduje te se sve više prelazi u digitalno doba gdje se sve više naših osobnih osjetljivih i povjerljivih podataka i zapisa nalazi na nekom od digitalnih medija, pa je stoga važno i potrebnu pažnju posvetiti zaštiti tih podataka.

Nedovoljno zaštićenom mrežom dovodimo se u veliki rizik od uspješnog zlonamjernog napada na naše podatke. Da zaključimo, potrebno je na vrijeme i pravovaljano educirati ljude na svim razinama, kako bi bilo što manje *cyber* zločina te kako bi internet postao sigurnije mjesto. Kao što štitimo svoj dom protiv fizičkih provala zaključavanjem, na isti način moramo imati zaključan svoj digitalni dom. Kada govorimo o bežičnim lokalnim mrežama, onda govorimo o efikasnim zaštitnim WPA2 i WPA3 ključevima.

Popis kratica

BSS	*Basic Service Set*	Osnovni servisni set
ESS	*Extended Service Set*	Prošireni servisni set
IBSS	*Independent Basic Service Set*	Nezavisni osnovni servisni set
SSID	*Service set identifier*	Identifikator servisnog seta
CSMA/CA	*Carrier Sense Multiple Access/Collision Avoidance*	Višestruki pristup/izbjegavanje sudara u smislu nosača
MIMO	*Multiple Input Multiple Output*	Više prijemnika / predajnika
WEP	*Wired Equivalent Privacy*	Privatnost ekvivalentna žičanoj
WPA	*WiFi Protected Access*	Bežično zaštićeni pristup
TKIP	*Temporal Key Integrity Protocol*	Vremenska zaštita integriteta ključa
PSK	*Pre Shared Key*	Unaprijed dijeljeni ključ
AES	*Advanced Encryption Standard*	Napredni standard šifriranja
VPN	*Virtual Private Network*	Virtualna privatna mreža
SSH	*Secure Shell*	Sigurnosni pristup
VLAN	*Virtual LAN*	Virtualna lokalna mreža
MAC	*Media Access Control Address*	Fizička adresa uređaja

Popis slika

Slika 2.1 - Prikaz osnovnog servisnog seta 4

Slika 2.2 - Prikaz proširenog servisnog seta 4

Slika 2.3 - Prikaz nezavisnog osnovnog servisnog seta 5

Slika 2.4 - Uređaji sa mogućnošću spajanja na bežične mreže [7] 7

Slika 3.1 - Prijenos informacija putem javne mreže [10] 11

Slika 3.2 - Pasivni napad na mrežu [11] 12

Slika 3.3 - Man in the middle napad [12] 13

Slika 4.1 - Prikaz dostupnih alata Kali inuxa 15

Slika 4.2 - Prikaz geografskih lokacija testiranja 17

Slika 4.3 - Odabrana korisnička mreža 18

Slika 4.4 - Sigurnosni standardi kod ispitanih korisnika 19

Popis tablica

Tablica 2.1 – Usporedba lokalne mreže i bežične lokalne mreže 3

Tablica 3.1 – Usporedba sigurnosnih standarda 10

Literatura

[1] Antivirusni program Avast, *How secure is your wi-fi network*, 1 stranica [online], citirano 03.02.2020, dostupno na: https://blog.avast.com/how-secure-is-your-wi-fi-network

[2] Besplatna online enciklopedija, wikipedia, *Wireless network*, 1 stranica [online], citirano 03.02.2020. dostupno na: https://en.wikipedia.org/wiki/Wireless_network

[3] Krishna Sankar, Sri Sundaralingam, Andrew Balinsky, Darrin Miller; Cisco Wireless LAN Security;(2007); ISBN: 978-1-58705-154-8

[4] Lifewire online portal za tehničke savjete i informacije, *History of wireless standard 802.11b*, 1 stranica [online], citirano 04.02.2019, dostupno na: https://www.lifewire.com/history-of-wireless-standard-802-11b-816555

[5] Neprofitna udruga wi-fi alliance, *About us*, Portal [online] citirano 04.02.2020, dostupno na: https://www.wi-fi.org/

[6] Proizvođač mrežne opreme Linksys, *Home wifi internet speed evolution*, 1 stranica[online], citirano 07.02.2020 dostupno na: https://www.linksys.com/us/home-wifi-internet-speed-evolution/

[7] Proizvođač mrežne opreme Cisco, *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*, 11 stranica [online], citirano 12.02.2020, dostupno na: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[8] Levente Buttyan, Jean-Pierre Hubaux; Security and Cooperation in Wireless Networks; Cambridge; (2007); ISBN: 9780521873710

[9] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić; Sigurnost računarskih sistema i mreža; Mikro knjiga; (2007); ISBN: 978-86-7555-305-2

[10] Portal HelpNetSecurity, *Public Wi-Fi; Users' habits and perceptions of risk*, 1 stranica [online], citirano 12.02.2020, dostupno na: https://www.helpnetsecurity.com/2016/10/19/public-wi-fi-users-habits-risk/

[11] Portal Techdifferences, *Differnce between Active and Passive Attacks*, 1 stranica [online], citirano 12.02.2020, dostupno na: https://techdifferences.com/difference-between-active-and-passive-attacks.html

[12] Kompanija za mrežnu sigurnost "Imperva", *Man in the middle attack*, 1 stranica [online], citirano 12.02.2020, dostupno na https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[13] VirtualBox, *Download VirtualBox*, Portal [online], citirano 12.02.2020, dostupno na: https://www.virtualbox.org/wiki/Downloads

[14] Završni rad, Visoko Učilište Algebra, Jasmin Redžepagić, *Otvorenost i zaštita bežičnih mreža na području Republike Hrvatske;(2016)*