Metode enkripcije u bežičnim lokalnim mrežama

Kolić, Domagoj

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

Stručni studij

METODE ENKRIPCIJE U BEŽIČNIM LOKALNIM MREŽAMA

Završni rad

Domagoj Kolić

Osijek, 2020.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Osijek, 17.09.2020.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Ime i prezime studenta:	Domagoj Kolić
Studij, smjer:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4476, 18.10.2019.
OIB studenta:	32601424172
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Prof.dr.sc. Drago Žagar
Član Povjerenstva 1:	Izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	Doc. dr. sc. Višnja Križanović
Naslov završnog rada:	Metode enkripcije u bežičnim lokalnim mrežama
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada	Zbog prirode bežičnog medija, adekvatno rješavanje problematike sigurnosti u bežičnim lokalnim mrežama od iznimne je važnosti. Potrebno je analizirati, objasniti i usporediti metode enkripcije koje se koriste u bežičnim lokalnim mrežama. Potrebno je u laboratorijskom okruženju implementirati bežičnu mrežu, u njoj testirati analizirane metode enkripcije, te prikazati i objasniti rezultate i zapažanja.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	17.09.2020.

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

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

IZJAVA O ORIGINALNOSTI RADA

Osijek, 13.10.2020.

Ime i prezime studenta:	Domagoj Kolić
Studij:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4476, 18.10.2019.
Turnitin podudaranje [%]:	12

Ovom izjavom izjavljujem da je rad pod nazivom**: Metode enkripcije u bežičnim lokalnim mrežama**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora

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

Potpis studenta:

Sadržaj

1. UVOD

Razvojem novih tehnologija dolazi do razvoja mreža i čovjekove želje za povezivanjem. Prvo se razvijaju žične mreže, dok se, zbog njihovih prednosti, u novoj povijesti fokus stavlja na razvoj bežičnih mreža. Razvojem mreža, pogotovo bežičnih dolazi do sigurnosnih problema.

Bežične mreže predstavljaju način komunikacije koji je posebno izložen napadima zbog samog načina rada bežičnih mreža. Bitno je posvetiti se osiguranju bežičnih mreža, jer sama bežična mreža predstavlja najslabiju kariku, a sam lanac je jak kao najslabija karika.

Što je mreža, što žična, što bežična veća i kompliciranija, to kroz nju prolazi više osjetljivih podataka. Takvim podacima je ključno osigurati siguran put.

Tijekom godina, od začetka ideje o bežičnim mrežama razvijaju se broji protokoli i algoritmi koji su tu da osiguraju bežične mreže te korisnike i njihove podatke na mreži.

Danas, iako nije najnapredniji, najkorišteniji je WPA2 protokol koji koristimo u bežičnim mrežama. U nastavku detaljnije je obrađena tema bežičnih mreža i metoda enkripcije u bežičnim lokalnim mrežama s posebnim osvrtom na WEP, WPA, WPA2 i WPA3 metode enkripcije, kao i njihove propuste. Rad također obuhvaća pregled vrsta napada te način osiguravanja bežičnih lokalnih mreža i penetracijsko testiranje.

2. BEŽIČNE MREŽE

Bežične mreže su vrsta komunikacijske mreže koje uz pomoć elektromagnetskih signala ili valova povezuju jedno ili više računala.

Wi-Fi predstavlja bežičnu mrežu kod koje se podaci između dva ili više klijenata razmjenjuju pomoću radio frekvencija. S Wi-Fi tehnologijom najčešće se susrećemo u lokalnim okruženjima, točnije u lokalnim bežičnim mrežama koje još poznate pod skraćenicom WLAN (engl. *Wireless local area network*). U posljednje vrijeme Wi-Fi ne susrećemo samo u lokalnim mrežama, već je i sveprisutniji u širokopojasnim mrežama – WAN (engl. *Wide Area Network*). Bežične lokalne mreže bazirane su na IEEE 802.11 obitelji standarda. Wi-Fi savez (engl. *Wi-Fi Alliance*) je neprofitna organizacija kojoj je cilj promoviranje Wi-Fi tehnologija i certificiranje Wi-Fi proizvoda, a Wi-Fi je zaštitni znak Wi-Fi saveza.

WLAN predstavlja lokalne računalne mreže gdje se komunikacija odvija bežično, koristeći RF (engl. *radio frequency*) spektar. U slučaju potrebe za postavljanje WLAN-a potrebno je imati pristupnu točku (*AP* – engl. *access point*) te jednog ili više krajnjih klijenata te je poželjno obratiti pažnju na sigurnost mreže. [1]

2.1 IEEE 802.11 standard

IEEE 802 je obitelj standarda nastalih za povezivanje u lokalnim i metropolitanskim mrežama. U ovu obitelj standarda spada i IEEE 802.11 koja specificira protokole za implementaciju bežičnih lokalnih mreža pri raznim frekvencijskim rasponima – 2.4 GHz, 5 GHz i 60 GHz.

Godine 1997. predstavljena je prva verzija 802.11 protokola i kroz godine je obitelj 802.11 doživjela brojne preinake i danas predstavlja najrašireniji standard za bežično povezivanje uređaja što u privatne, to u komercijalne svrhe. [1]

Kroz dugi niz godina nastaju mnoge inačice 802.11 standarda za različite namjene korištenjem raznih tehnologija. Ovo su neke od najbitnijih:

1. 802.11-1997: Predstavlja originalnu verziju 802.11 standarda koja se danas više ne koristi. Standard je radio na frekvenciji od 2.4 GHz s mogućim brzinama prijenosa 1 Mbit/s i 2 Mbit/s [2]

2. 802.11b: koristeći istu frekvenciju od 2.4 GHz ovaj standard može postići teoretsku brzinu od 11 Mbit/s, dok su realne oko 5 Mbit/s koje su postignute korištenjem CCK-a (engl. *Complementary Code Keying*) tehnologije. Uređaji s 802.11b standardom izlaze na tržište sredinom 1999. godine s *iBook*-om kao prvim osobnim računalom s 802.11b. Povećanje brzine kao i smanjenje cijene dovode do masovnog korištenja 802.11b standarda [2]
3. 802.11a: objavljen je 1999. te koristi isti *date layer* protokol, ali koristi OFDM (engl. *Orthogonal frequency-division multiplexing*) sučelje. Teoretska brzina iznosi 54 Mbit/s, dok realna brzina koju krajnji korisnik može postići iznosi oko 25 Mbit/s s radom na frekvenciji od 5 GHz, što je i mana samog standarda zbog veće cijene mrežne opreme koja radi na 5 GHz [3]
4. 802.11g: koristeći isti frekvencijski raspon od 2.4 GHz postiže maksimalnu teoretsku brzinu od 54 Mbit/s dok realna net brzina iznosi oko 31 Mbit/s koristeći CSMA/CA. 802.11g koristi OFMD modulacijsku shemu s brzinama prijenosa podatak 6, 9, 12, 18, 24, 36 ,48 i 54 Mbit/s, a za brzine od 5.5 i 11 Mbit/s koristi CCK shemu. 802.11g je u potpunosti unatrag kompatibilan s 802.11b hardverom i koristi iste kanale kao 802.11b [4]
5. 802.11n: poznat još kao i 802.11n-2009 predstavlja standard koji postiže veće brzine prijenosa koristeći više antena. Ovo je prvi standard koji podržava MIMO, *frame aggregtation* te pruža sigurnosne nadogradnje, a može se koristiti na 2.4 GHz i 5 GHz frekvencijskom području. Ovaj standard također donosi poboljšanje u brzini prijenosa podataka gdje maksimalna net brzina prijenosa podataka iznosi 600 Mbit/s uz korištenje kanala širine 40 MHz [5]
6. 802.11ac: ovaj standard objavljen je 2013. godine i Wi-Fi savez mu dodjeljuje oznaku „Wi-Fi 5“ (802.11n dobiva oznaku „Wi-Fi 4“). Radi na frekvencijskom rasponu od 5 GHz te podržava razne frekvencijske raspone te puno veće brzine – nešto manje od 7 Gb/s uz pomoć osam 160 MHz 256-QAM kanala što je veća teoretska brzina današnjeg SATA-3 protokola. S obzirom na to da u stvarnom svijetu ne možemo koristiti svih 8 kanala već samo dva ili tri, brzina opada u raspon od 1.7 Gb/s do 2.5 Gb/s. [6]

2.2 Sigurnost unutar bežičnih mreža

Bežična mreža predstavlja najslabiju kariku unutar cijele mreže. Analogno tome cijela mreža sigurna je kao i njezina najslabija karika. Bežična mreža je najslabija karika zbog samog načina rada. Podaci unutar nje se prenose koristeći radio frekvencije i podaci se prenose u cijelom radijusu dometa pristupne točke, što znači da bilo tko može probati presresti podatke ako je u dometu. Iako 802.11 obitelj standarda definira razne sigurnosne elemente to ne čini bežične mreže otporne na napad. U bežičnim mrežama za zaštitu podataka koji se prenose ključnu ulogu ima kriptografija koja nam omogućava kriptiranje podataka kao i sigurnosne elemente koji onemogućavaju naknadno mijenjanje podataka, lažiranje identiteta kao i poricanje slanja poruka.

Pri dizajniranju bilo koje mreže treba osigurati sljedeće:

1. Povjerljivost koja podrazumijeva da privatna informacija neće biti dostupna neovlaštenim osobama
2. Integritet koji podrazumijeva osiguranje da neovlaštena osoba neće moći izmijeniti podatke kao niti neovlašteno manipulirati sustavom
3. Dostupnost kojom se podrazumijeva osiguranje da će sustav i njegovi resursi u svakom trenutku biti dostupni svojim autoriziranim korisnicima
4. Autentičnost koja podrazumijeva osiguranje vjerodostojnosti ili istinitosti sudionika u komunikaciji
5. Odgovornost koja podrazumijeva se da se sve aktivnosti nekog entiteta mogu jednoznačno povezati s tim istim entitetom. [1]

3. METODE ENKRIPCIJE LOKALNIH BEŽIČNIH MREŽA

3.1. WEP

WEP (engl. *Wired Equivalent Privacy*) predstavlja sigurnosni algoritam koji je predstavljen kao dio originalnog 802.11 standarda 1997. godine. WEP je za cilj imao pružiti povjerljivost podataka jednaku onoj kod tradicionalnih, žičnih mreža. WEP je prepoznatljiv po svom ključu od 10 ili 26 heksadecimalnih znamenki (40 ili 104 bita) te je jedno vrijeme bio najkorišteniji standard.

WEP koristi RC4 (engl. *Rivest Cipher 4*) protočnu šifru za povjerljivost podataka i CRC-32 (engl. *Cyclic redundancy check*) kriptografsku kontrolnu sumu za integritet podataka. Standardni 64 bitni WEP koristi 40 bitni ključ (poznat još kao i WEP-40) koji se spaja s 24 bitnim inicijalizacijskim vektorom i zajedno tvore RC4 ključ.

Ograničenja postavljena od strane američke vlade ograničila su veličinu ključa, a kasnije, nakon što su ograničenja ukinuta proizvođači mrežne opreme implementirali su prošireni 128 bitni WEP, koristeći ključ veličine 104 bita (poznat još kao i WEP-104).

Kod standardnog WEP-a ključ se zapisuje kao niz od 10 heksadecimalnih znakova gdje svaki znak predstavlja 4 bita, čime dobivamo 40 bita. Na to dodajemo 24 bitni inicijalizacijski vektor te dobivamo 64 bitni ključ.

Kod proširenog WEP-a ključ se zapisuje kao niz od 26 heksadecimalnih znamenki, a svaka od njih je predstavljena s 4 bita, a kombinacija s 24 bitnim inicijalizacijskim vektorom dobiva 128 bitni ključ. [7]

Većina pristupnih točki dozvoljavala je krajnjim korisnicima unos ključa. Kod standardnog WEP-a korisnik bi unosio 5 ASCII znakova (0-9, a-z, A-Z), a svaki od znakova pretvarao se u 8 bitova. Kod proširenog WEP-a korisnici bi unosili 13 ASCII znakova. Koristeći ASCII znakove dolazi se do problema: svaki bajt mora biti ASCII znak, što je mali skup vrijednosti, te tako uvelike smanjujemo prostor mogućih ključeva.

Kod WEP-a postoje dvije metode za autentifikaciju:

1. otvoreni sustav autentifikacija kod kojeg klijent ne pruža svoje vjerodajnice pristupnoj točki tijekom procesa autentifikacije
2. dijeljeni ključ autentifikacija gdje se koristi WEP ključ za autentifikaciju u 4 koraka.

Kod autentifikacije s dijeljenim ključem odvija se izazov-odgovor rukovanje u četiri koraka:

1. Klijent šalje autentifikacijski zahtjev pristupnoj točki
2. Pristupna točka odgovara uz *clear-text* izazov
3. Klijent enkriptira tekst koristeći WEP ključ i šalje enkriptirani tekst pristupnoj točki
4. Pristupna točka dekriptira odgovor te u slučaju da odgovara izvornom tekstu, pristupna točka šalje klijentu pozitivan odgovor.

Nakon autentifikacije WEP ključ koristi se i za enkripciju podatkovnih okvira uz pomoć RC4 protočne šifre. Korištenje RC4 protočne šifre predstavlja sigurnosni rizik zato što se isti ključ ne smije koristiti dva puta. Pri tome je uloga inicijalizacijskog vektora, koji se prenosi kao otvoreni tekst, da spriječi to ponavljanje. Međutim 24 bitni inicijalizacijski vektor nije dovoljno dug da osigura tu značajku u mrežama s puno prometa.

Način korištenja inicijalizacijskog vektora učinio je WEP standard ranjivim na napad povezanim ključem (engl. *related key attack*). Za 24 bitni inicijalizacijski vektor postoji 50% šanse da će se isti inicijalizacijski vektor ponoviti nakon 5000 paketa.

Iako je WEP standard doživio par inačica, ni jedna od verzija nije mijenjala duljinu vektora. Otkrivanjem mana, nedostataka u WEP protokolu nastala su pojedinačna rješenja koja adresiraju neke od nedostataka i mogućih točaka upada kod ove vrste enkripcije. Tu možemo izdvojiti WEPplus i dinamični WEP.

WEPplus, poznat kao i WEP+ predstavlja poboljšanje WEP-a razvijeno od strane *Agre Systems*. Poboljšanje se temelji na adresiranju slabog inicijalizacijskog vektora, ali ovo rješenje je efektivno samo ako ga koriste obje strane u bežičnoj komunikaciji. Iako WEPplus predstavlja poboljšanje, ovaj način enkripcije i dalje nije otporan na napad ponovnim slanjem i vrstama napada koje se ne temelje na slabosti inicijalizacijskog vektora.

Kod dinamičnog WEP-a koristi se kombinacija IEEE 802.1x tehnologija i EAP protokola. Dinamični WEP mijenja WEP ključeve dinamično, ali je ova verzija WEP-a bila dostupna samo kod određenih pružatelja usluga. [1]

WEP je bio jedini protokol dostupan na 802.11a i 802.11b mrežama prije WPA standarda. No s obzirom na sigurnosne propuste koji su otkriveni u radu WEP standarda, ratifikacijom 802.11i standarda, WEP standard zamjenjuje se WPA standardom.

3.2. WPA

WPA (engl. *Wi-Fi Protected Access*) predstavlja sigurnosni protokol razvijen od strane Wi-Fi saveza. WPA je nastao kao neposredni odgovor na ozbiljne sigurnosne mane koje su otkrivene kod prijašnjeg protokola dok ne dođe puna dostupnost 802.11i standarda.
WPA protokol bio je dostupan krajnjim korisnicima kroz nadogradnje softvera u slučaju da je mrežna oprema podržavala funkcije potrebne za WPA. U slučaju nadogradnje pristupne točke mogle su raditi u WEP/WPA načinu rada, pri čemu bi pružale samo WEP razinu zaštite za sve korisnike mreže.

WPA implementira veliki dio IEEE 802.11i standarda, gdje se fokus stavlja na TKIP (engl. *Temporal Key Integrity Protocol*). TKIP dinamički generira novi 128 bitni ključ za svaki paket te tako sprječava napade koji su se pokazali uspješni na prijašnjem WEP standardu. Kao sigurnosni standard, WPA korisni 48 bitni inicijalizacijski vektor i 64 ili 128 bitni enkripcijski ključ koji se ručno unosi u pristupnu točku i uređaje koji se spajaju na pristupnu točku.

WPA također implementira algoritam za autentifikaciju poruke – MAC (engl. *Message authentication code*) u zamjenu za CRC koji je korišten kod WEP-a. MAC algoritam dizajniran je za sprječavanje izmjene i ponovnog slanja podataka od strane napadača.

WPA standard je u konačnici zamijenjen WPA2 standardom koji u potpunosti implementira sve sigurnosne mjere definirane u 802.11i standardu. [8]

3.3. WPA2

WPA2 (engl. *Wi-Fi Protected Access II*) kao i njegov prethodnik temelji se na IEEE 802.11i standardu, a obuhvaća i sve mehanizme koje koristi WPA. No, uključuje i dodatna poboljšanja vezana za sigurnost pri čemu se posebno izdvaja CCMP enkripcija. Drugi naziv za WPA2 je i RSN (engl. *Robust Security Network*).

Za razliku od WEP standarda enkripcije koji je koristio RC4 protočnu šifru, WEP2 koristi AES[1] (engl. *Advanced Encryption Standard*) blok šifru. [8]

[1] AES- kriptografski algoritam koji podatke kriptira po blokovima od 128 bita, gdje ključ može biti veličine 128, 192, 256 bita. Algoritam se provodi u više koraka – ovisno o duljini ključa.

Kod 802.11i RSN-a sigurnosne specifikacije definiraju sljedeće usluge:

1. Autentifikacija pri kojoj se koristi protokol koji definira komunikaciju između korisnika i poslužitelja za provjeru autentičnosti. U tom postupku se generiraju privremene ključeve koji će se koristiti u bežičnoj komunikaciji između klijenta i pristupne točke
2. Kontrola pristupa kojom se primorava uporaba funkcije provjere autentičnosti, ispravno usmjeravanje poruke i olakšavanje razmjena ključeva
3. Privatnost uz integritet poruke pri čemu su podaci na MAC sloju. šifrirani zajedno s MIC[2] kodom. [1]

RSN sigurnosna specifikacija sastoji se od 5 funkcionalnih faza, a to su:

1. Otkrivanje- pristupna točka koristi kontrolne poruke za oglašavanje IEEE 802.11i sigurnosne politike uz pomoć kojih stanica identificira pristupnu točku kao WLAN na koji se želi priključiti
2. Autentifikacija– stanica i poslužitelj za provjeru autentičnosti međusobno dokazuju jedan drugom svoj identitet. Sve dok se ne završi postupak provjere autentičnosti, pristupna točka blokira sav promet između stanice i poslužitelja za provjeru autentičnosti
3. Generiranje i distribucija ključeva- pristupna točka i stanica generiraju kriptografske ključeve
4. Zaštićeni prijenos podataka – okviri koji se razmjenjuju između bežične stanice i krajnjeg odredišta idu preko pristupne točke, gdje se sigurni prijenos odvija samo od bežične stanice do pristupne točke
5. Prekid komunikacije – nakon razmijenjenih kontrolnih okvira sigurna veza se prekida. [9]

[2] MIC (engl. *Message Integrity Check*) drugo ime za MAC (engl. *Message Authentication Code*) koje se koristi u sektoru komunikacija kako ne bi došlo do zamjene s MAC (engl. *Media Access Control*) adresom.

3.3.1. Način rada protokola

WPA2 dolazi s implementacijom dva nova protokola: četverostruko rukovanje i rukovanje grupnim ključem.

WPA2 standard također implementira dva RSN-a protokola za integritet i povjerljivost podataka: TKIP i CCMP (engl. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). Implementacija CCMP-a je bila obavezna s obzirom na to da mehanizmi za povjerljivost i integritet podataka kod TKIP-a nisu toliko robusni kao kod CCMP-a, dok je implementacija TKIP-a bila nužna kako bi se osigurala kompatibilnost s prijašnjom verzijom standarda.

Početni proces provjere autentičnosti provodi se uz pomoć unaprijed dijeljenog ključa (engl. *PSK Pre Shared Key*) ili uz pomoć EAP[3] izmjene putem 802.1x koja zahtjeva prisutnost poslužitelja za autentifikaciju. Oba procesa osiguravaju da je krajnji klijent ovjeren s pristupnom točkom. Nakon procesa ovjere generira se tajni dijeljeni ključ koji se naziva upareni glavni ključ (engl. *Pairwise Master Key* – PMK). PMK izveden je od lozinke koja prolazi kroz PBKDF2-SHA1 kriptografsku hash funkciju[4]. U mrežama s unaprijed dijeljenim ključem (PSK) PMS je zapravo PSK (engl. *Pre Shared Key*). U slučaju da se koristi 802.1x EAP razmjena PMK je izveden iz EAP parametara koje daje poslužitelj za provjeru autentičnosti. [1]

3.3.1.1. CCMP

Uzimajući u obzir nedostatak TKIP enkripcije kod prijašnje verzije WPA protokola, kod WPA2 protokola uvodi se CCMP protokol (engl. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)*. On se temelji na AES protokolu i ulančanom šifriranju blokova. Uz AES, protokol CCMP koristi brojač i ulančano kriptiranje blokova u izradi autentifikacijske oznake poruke. Treba istaknuti da je kod ovog načina rada važno da se tekst dijeli na blokova nad kojima se prije kriptiranja izvodi logička operacija XOR s prethodno kriptiranim blokom što osigurava da za identične ulazne blokova imamo različit šifrat.

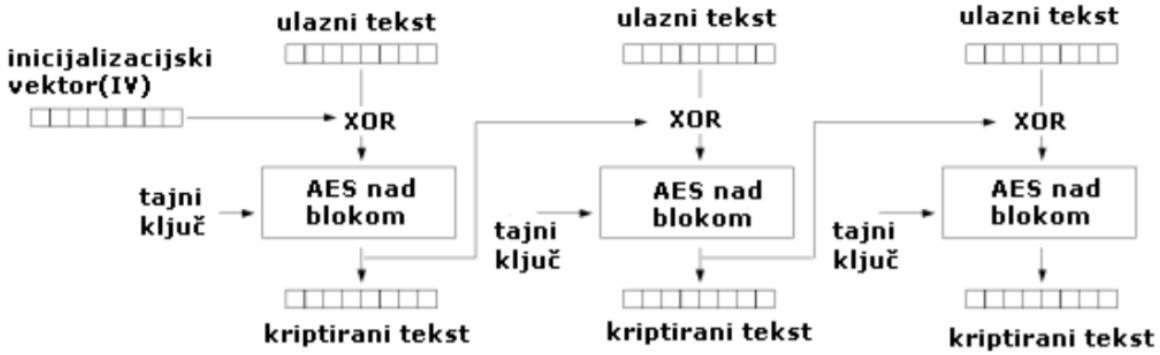
[3] EAP (engl. *Extensible Authentication Protocol*)- EAP definira format poruke koje se izmjenjuju prilikom bežične autentifikacije.

[4] Hash funkcija je funkcija h, koja zadovoljava iduća dva svojstva: 1. kompresiju – h ulazu x proizvoljne konačne duljine pridružuje se izlaz h(x) fiksne duljine m i 2. jednostavnost izračuna: zadani su h i ulaz x, h(x) je lako izračunati.

Kod CBC MAC (engl. *Cipher Block Chaining Message Authentication Code Protocol*) izrade autentifikacijske oznake inicijalizacijski vektor postavlja se na *nul-vektor,* odnosno, sve se vrijednosti u vektoru postavljaju na nula. MAC predstavlja izlaz zadnjeg kriptiranog bloka, gdje je broj blokova proporcionalan veličini same poruke. [1]

CCMP MPDU (engl. *Medium Access Control Protocol Dana Unit)* podatkovni paket sastoji se od pet dijelova:

1. MAC zaglavlje,
2. CCMP zaglavlje,
3. podatkovna jedinica,
4. MIC kod,
5. FCS (engl. *Frame Check Sequence*) za provjeru okvira.



Slika 3.1. CBC način rada blokovnih šifri.

3.3.1.2. TKIP

TKIP je dizajniran tako da ga mogu koristiti i stariji uređaji, oni koji su koristiti WEP, uz odgovarajuću softversku nadogradnju. TKIP I CCMP služe za očuvanje povjerljivosti podataka i integritet poruke, samo ih postižu na različiti način.

Za osiguranje integriteta poruke TKIP dodaje MIC kod unutar 802.11 MAC okvira. MIC kod generira se uz pomoć *Michael* algoritma gdje se izračunava 64 bitna vrijednost na temelju izvorišne i odredišne MAC adrese, ključa i vrijednosti podatkovnog polja.

Tajnost podataka TKIP osigurava se RC4 algoritmom gdje se podatkovna jedinica kriptira zajedno s MIC kodom. Za razliku od CCMP-a TKIP nije zahtijevao dodatnu hardversku podršku. [10]

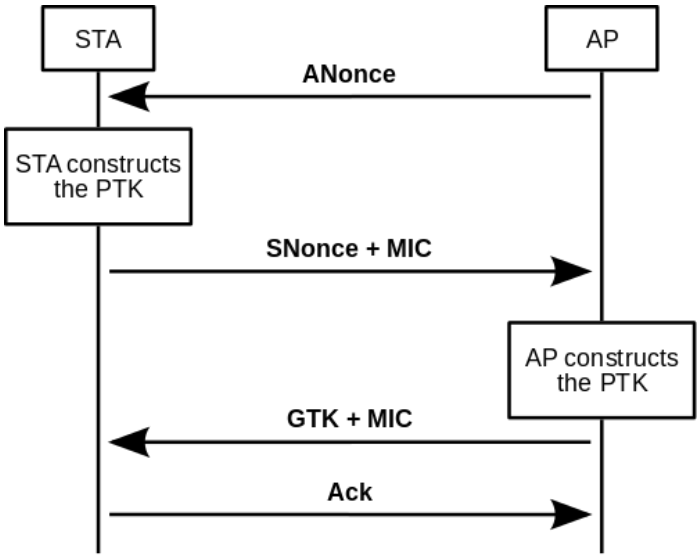
Tablica 3.1: Razlike u načinu postizanja integriteta i tajnosti poruke kod TKIP-a i CCMP-a.

	TKIP	CCMP
Integritet poruke	MIC kod unutar 802.11 MAC okvira	CBC-MAC
Tajnost poruke	RC4 algoritam	CTR način rada blokovnih šifri

3.3.1.3. **Četverostruko rukovanje**

Ovaj protokol dizajniran je tako da pristupna točka (ili autentifikator) i klijent mogu međusobno samostalno dokazati da poznaju PSK/PMK, a da nikad ne otkriju ključ. Umjesto otkrivanja ključa pristupna točka i klijent kriptiraju poruke jedno drugom koje je moguće dešifrirati samo uz pomoć PMK. Dokaz za poznavanje PMK leži u uspješnom dešifriranju poruke. PMK ostaje isti tijekom cijele sesije, zbog čega je za enkripciju prometa potrebno generirati nove, izvedene ključeve.

Četverostruko rukovanje koristi se kako bi se generirala još dva ključa – PTK (engl. *Pairwise Transient Key*) i GTK (engl. *Group Temporal Key*) koji se koristi za dešifriranje multicast i broadcast prometa. PTK se generira spajanjem više atributa: PMK, AP nonce[5] (ANonce), STA nonce (SNonce), MAC adrese pristupne točke i MAC adrese stanice. Vizualna reprezentacija vidljiva je na slici 3.2. [11]



Slika 3.2 Četverostruko rukovanje. [12]

[5] Nonce - u kriptografiji nonce je proizvoljan broj koji se može koristiti samo jednom u komunikaciji. Radi se o pseudo slučajnom broju koji se koristi u protokolu provjere autentičnosti kako bi se osiguralo da se stare komunikacije ne mogu ponovo upotrijebiti u napadima ponavljanja.

3.3.1.4. Rukovanje grupnim ključem

U mrežama koje zahtijevaju ažuriranje zbog isteka vremena koristi se privremeni ključ grupe (engl. *The Group Temporal Key- GTK*). Kada uređaj napusti mrežu grupni ključ se mora ažurirati. Ovo je sigurnosni mehanizam postavljen da spriječi daljnju razmjenu multicast ili broadcast poruka s pristupnom točkom.

Kada uređaj napusti mrežu potrebno je ažurirati privremeni ključ grupe, a za to je zadužen *Group Key Handshake* koji se sastoji od dvosmjernog rukovanja:

1. Pristupna točka koja šalje novi GTK svakoj stanici u mreži. Ključ je kriptiran koristeći KEK[6] ključ koji je dodijeljen svakoj stanici
2. Stanica priznaje novi ključ i šalje odgovor pristupnoj točki. [12]

Tablica 3.2: WPA2 ključevi za provjeru autentičnosti [1].

Naziv ključa	Uporaba ključa
Master key (MK)	Za izvođenje tajnog PMK ključa
Pairwise Master Key (PMK)	Za razmjenu PTK tajnog ključa
Pairwise Transient Key (PTK)	Za enkripciju, razmjenu GTK ključa, dokazivanje identiteta
Group Temporal Key (GTK)	Group Temporal Key (GTK)

[6] KEK (*engl. Key Encryption Key*) je ključ sesije za enkripciju ključeva.

3.3.2. Način korištenja protokola

WPA2 protokol može se koristiti na dva načina:

1. *Personal* koji podrazumijeva prethodnu razmjenu ključeva između svih klijenata i pristupne točke
2. *Enterprise* način rada koji uključuje zaseban ključ za svakog klijenta koji se želi spojiti na pristupnu točku.

Personal način rada naziva se još i PSK (engl. *Pre- shared key*) te je namijenjen privatnim (kućnim) mrežama i manjim poslovnim mrežama. Jednostavnije ga je implementirati od *Enterprise* načina rada jer ne zahtijeva poslužitelj za provjeru autentičnosti. Umjesto toga se definira jedinstveni 256 bitni ključ koji se koristi za komunikaciju u mreži. Ako uzmemo u obzir da za 256 bitni ključ postoji oko 1078 mogućih kombinacija, proizlazi da je ključ nemoguće izračunati iz hash vrijednosti, odnosno barem to nije moguće napraviti u razumnom vremenu.

Ovdje vrh hijerarhije može predstavljati sam PSK ključ koji dijele pristupna točka i stanica. PSK ključ implementira se mimo IEEE 802.11i standarda od strane krajnjeg korisnika.

Enterprise način rada omogućava i dodatnu razinu sigurnosti jer se svaki uređaj u mreži mora identificirati i potvrditi identitet lozinkom, a provjeru obavlja poslužitelj za provjeru autentičnosti. *Enterprise* rješenje je robusnije, međutim implementacija i održavanje takvog sustava zahtijeva znatno više posla. Prilikom provjere autentičnosti WPA2 *Enterprise* poslužitelji koriste RADIUS. [12]

RADIUS (engl. *Remote Authentication Dial In User Service*) označava mrežni protokol koji funkcionira na priključku (engl. *port*) 1812 te nam omogućuje centraliziranu provjeru autentičnosti, autorizaciju i upravljanje korisnicima koji se spajaju i koriste mrežu i mrežne usluge. [13]

3.4. WPA3

WPA3 predstavlja iduću generaciju Wi – Fi sigurnosnog standarda koji će pružiti vrhunske sigurnosne standarde te je dizajniran da pruži veću sigurnost unutar privatnih i javnih mreža. Uz veću sigurnost WPA3 nudi značajke za pojednostavljenje W-Fi sigurnosti, robusnija rješenja za autentifikaciju, te povećanje kriptografske zaštite za mreže s osjetljivim podacima to postiže uz pomoć SAE-a (engl. *Simultaneous Authentication of Equals*). [14]

3.4.1 Četiri područja nadogradnje

1. Sigurnije rukovanje: postiže se pomoću SAE protokola koji se još naziva *Dragonfly* rukovanje. Ovaj protokol zahtjeva novu interakciju svaki put kada uređaj zatraži enkripcijski ključ te se s time smanjuje količina napada te sprječava izvanmrežno dešifriranje podataka
2. Lakše povezivanje: WPA3 donosi lakše povezivanje na mrežu korištenjem Wi-Fi *Device Provisioning Protocol-a*. Ovaj protokol zamjenjuje zastarjeli WPS standard te nam omogućuje lakše i sigurnije povezivanje na mrežu pomoću QR koda ili zaporke
3. Zaštita na otvorenim mrežama: Wi-Fi *Enhanced Open* pruža bolju zaštitu na otvorenim, javnim *hotspot* mrežama nudeći zaštitu protiv pasivnog prisluškivanja bez zahtijevanja zaporke ili dodatnih koraka za pridruživanje bežičnoj mreži
4. Veći sesijski ključ: WPA3-*Enterprise* podržava veličinu ključa do 192 bita tijekom autentifikacije što u konačnici dovodi do veće otpornosti na neovlašteni ulaz i korištenje. [14]

3.4.2 Podjela u skupine

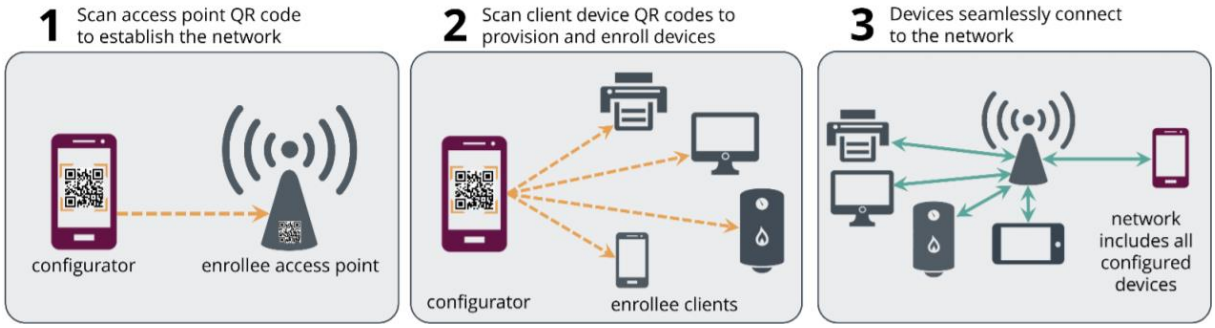
S obzirom na to da se bežične lokalne mreže razlikuju u uporabi i sigurnosnim potrebama WPA3 dijeli se u dvije skupina:

1. WPA3 – *Personal* – namijenjen za osobnu uporabu, koristi 128 bitnu enkripciju i donosi bolju zaštitu krajnjih korisnika pružajući robusniju autentifikaciju na temelju lozinki, čak i u slučaju ako korisnik odabere lozinku koja ne zadovoljava dogovorene preporuke o složenosti. Uz pomoć *Simultaneous Authentication of Equals* (SAE) ova verzija standarda otporna je na napade grubom silom. SAE predstavlja zamjenu za *Pre-shared key* (PSK) koji se koristi u WPA2 – *Personal* bežičnim lokalnim mrežama. WPA3 – *Personal* protokol donosi nova sigurnosne značajke u obliku generiranja novih setova enkripcijskih ključeva prilikom svakog povezivanja. Nova iteracija sigurnosnog protokola pruža višu razinu sigurnost uz olakšano korištenje i pristup bežičnoj mreži prosječnom korisniku
2. WPA3-*Enterprise* je standard namijenjen situacijama gdje je potrebna veća robusnost i veća zaštita podataka poput financijskih institucija i državnih agencija. Standard uključuje 192 bitnu zaštitu koja je u skladu sa zahtjevima američke vlade. Veća robusnost i zaštita postižu se kroz implementaciju novih protokola i algoritama:
    1. Za autentificiranje enkripcije koristi se 256 bitni *Galois/Counter mode* protokol (GCMP-256) koji tako štiti integritet poruke koja je poslana grupi krajnjih korisnika. U kriptografiji *Galois/Counter mode* je način izvođenja operacija za simetrične ključeve kriptografskih blok šifri
    2. Za izvedbu i potvrdu ključa koristi se eliptična krivulja *Diffie-Hellmanovog* protokola (ECDH) i algoritam digitalnog potpisa eliptične krivulje od 384 bita
    3. Zaštita okvira za upravljanje koristi 256-bitni *Broadcast/Multicast* protokol za integritet uz pomoć *Galoisovog* koda za provjeru autentičnosti poruke.

WPA3 dolazi s opcijama Wi-Fi *Easy Connect* i Wi-Fi *Enhanced Open*.

Wi- Fi *Easy Connect* pojednostavljuje i povećava korisničko iskustvo pri povezivanju uređaja na bežične mreže te istovremeno uključuje snažnu enkripciju kroz javni ključ te s time osigurava sigurnost i pouzdanost mreže pri dodavanju novih uređaja. Korisničko iskustvo vidljivo je i kroz upravljanje mrežom gdje se kroz jednostavne korake povezuje novi uređaj. Uređaji se mogu povezati skeniranjem QR koda, koji može biti ispisan ili digitalni, ili unosom niza u uređaj. [15]

Wi-Fi *Easy Connect* značajka treba pojednostaviti proces povezivanja Wi-Fi uređaja bez korisničkog sučelja (npr. IoT), dok Wi-Fi *Enhanced Open* pruža zaštitu podataka u otvorenim mrežama. Način funkcioniranja *Wi- Fi Easy Connect* načina rada vidljiv je na slici 3.3. [16]



Slika 3.3: Wi-Fi Easy Connect princip rada. [16]

Wi-Fi *Enhanced Open* bazira se na *Opportunistic Wireless Encryption* što znači da su podaci između klijenta i pristupne točke individualno kriptirani. Dakle, drugi klijenti mogu prisluškivati promet koji se odvija između klijenta i pristupne točke, ali ga ne mogu dekriptirati. Sam OWE je ekstenzija IEEE 802.11i veoma je sličan SAE-u. Migracija s otvorene mreže na Wi – Fi *Enhanced Open* moguća je bez ometanja mrežnih korisnika. [17]

3.4.2 *Dragonfly* rukovanje ili SAE

Dragonfly rukovanje, također je poznato i pod nazivom SAE (*Simultaneous Authentication of Equals)*. Oslanja se na *Zero Knowledge Proof*, metodu kojom dva korisnika mreže dokazuju jedan drugome da znaju vrijednost *x*, bez dijeljenja ikakve druge informacije, osim da znaju vrijednost *x*. *Zero Knowledge Proof* metoda zamijenila je rukovanje grupnim ključem koje se koristi u WPA2 standardu. *Dragonfly* protokolom se sprječava dijeljenje zaporki jer uređaj u mreži mora dokazati da ima znanje o zaporci, ali ne pokazuje i samu zaporku. Dakle, *Dragonfly* razmjena podataka sastoji se od razmjene dviju poruka. Prva faza protokola nosi naziv *Commit* razmjena i prilikom dijeljenja te poruke obije strane se obavezuju na samo jedno pogađanje zaporke. Druga faza nazvana je *Confirm*, u toj fazi oba uređaja potvrđuju znanje zaporke te se generira jedinstveni sesijski ključ.

Nadalje, pri svakom spajanju na bežičnu mrežu dolazi do *commit* i *confirm* razmjena, tako da ako napadač i razbije sesijski ključ ne može razbiti ostale. [18]

4. VRSTE NAPADA NA BEŽIČNE LOKALNE MREŽE

Nekoliko je načina na koji napadač može neovlašteno pristupiti WLAN mreži:

1. Slučajno povezivanje – riječ je o situaciji kada se u istom prostoru koristi više nezaštićenih mreža, a korisnik se slučajno spoji na pogrešnu mrežu i time ugrozi tuđi mrežni sustav
2. Zlonamjerno povezivanje – izvodi se tako da se mrežna kartica napadača predstavlja kao legitimna pristupna točka. Posljedica napada je da sav mrežni promet teče kroz napadačevu mrežnu karticu, to jest računalo [19]
3. *Ad - hoc* mreže - u kojima korisnici mogu komunicirati međusobno bez potrebe za postojanjem infrastrukture ili uređenih odnosa među korisnicima mreže. Zbog načina rada ovakve mreže često su nezaštićene što dovodi do mogućnosti lažnog predstavljanja i mnogih drugih vrsta napada [20]
4. Netradicionalne mreže - govori se o *Bluetooth* i sličnim tehnologijama. Ovim tehnologijama i sigurnosti ne pridodaje se puno značaja zbog njihovog kratkog dometa što ne znači da su mreže otporne na napade
5. Krađa identiteta - u situaciji kada podaci nisu kriptirani, napadač može saznati MAC adresu računala koje koristi određenu mrežu te uz pomoć različitih alata lažno se predstaviti kao ovlašteni korisnik mreže
6. Napadi posredovanjem u komunikaciji – (engl. *man in the middle*) – u ovim situacijama napadač prilikom uspješnog napada na tuđu mrežu može saznati osjetljive informacije koje potom može koristiti za posredovanje u komunikaciji. Posljedica ovakvog napada je da su krajnji korisnici nesvjesni napada na mrežu i prisluškivanja [19]
7. Mrežno ubacivanje – ovdje je za cilj izmjena postavki mrežnih uređaja kojima se iz WLAN-a pristupa pomoću pristupne točke.

4.1 Napadi vezani uz WEP

Glavne slabosti WEP protokola kriju se u dužini ključeva, u stvaranju niza ključeva, kao i u inicijalizacijskom vektoru. Iako je svrha inicijalizacijskog vektora stvaranje nasumičnog niza ključeva, sam inicijalizacijski vektor je ograničen na samo 24 bita. Dakle, nakon određenog vremena korištenja mreže, dolazi do ponavljanja inicijalizacijskog vektora. Poznatiji napadi na WEP protokol su FMS, PTW i ARP *Request replay* napadi. [21]

4.1.1 FMS napad

FMS napad nosi ime prema S. Fluhreru, I. Mantinu i A. Shamiru. Cilj napada bio je pronaći slabosti u kreiranju ključa te u RC4 protočnoj šifri. RC4 protočna šifra sastoji se od KSA algoritma za stvaranje ključeva te PRGA algoritma koji stvara nasumičnu sekvencu. Sam napad otkrio je dvije slabosti WEP protokola. Prva slabost povezana je s postojanjem velike količine slabih ključeva. Također, napad je otkrio da je moguće kroz mali dio tajnog ključa otkriti veliki broj bitova početne permutacije. Sama permutacija odvija se kroz KSA algoritam. Druga slabost WPA protokola očituje se kada je dio ključa koji prolazi kroz KSA algoritam vidljiv napadaču. [21]

4.1.2 PTW napad

Napad pod imenom PTW izvršili su Tews, Weinmann i Pyshkin 2007. godine. Umjesto isprobavanja svih mogućih kombinacija ključeva, ovaj napad se temelji na odabiru vjerojatnih ključeva, te provlačenju tih istih ključeva kroz RC4 algoritam. PTW napad temelji se na prijašnjem napadu nazvanom Klein napad iz 2005. godine. [21]

4.1.3 ARP *Request Replay* napad

Dok se prethodno navedeni napadi temelje na skupljanju velikog broja okvira, što može biti vremenski zahtjevno, ovakva vrsta napada generira mrežni promet ubacivanjem okvira u mrežu te time brže dolazi do inicijalizacijskog vektora. Upravo zbog potrebe za pojačanim mrežnim prometom, prilikom ovakvog napada koristi se *Address Resolution Protocol*[7] jer se njegovom upotrebom najbrže generiraju inicijalizacijski vektori koji se potom koriste za napad na mrežu zaštićenu s WEP ključem. Napad se izvršava tako da napadač prisluškuje ARP zahtjeve poslane na mrežu, a zatim ih ponovno odašilje na mrežu. Napadač to ponavlja sve dok ne prikupi dovoljnu količinu inicijalizacijskih vektora. [19]

[7] *Adress Resolution Protocol* se koristi za povezivanje IP mrežnih adresa s mrežnim uređajem

4.2 Napadi vezani uz WEP2

Ni jedna mreža niti jedan sigurnosni protokol nisu u potpunosti sigurni pa tako nije siguran niti WPA2. Neke od lakših tehnika za dobivanje pristupa WPA2 mrežama oslanjanju se na loše, kratke lozinke ili na socijalni inženjering. Ovo su neki od popularnijih napada na WPA2 mreže:

4.2.1 Napad preko WPS protokola

1. *Pixie Dust* - Ovo je offline vrsta napada koja radi samo na određenim uređajima. Sam napad fokusira se na manjak raznovrsnosti pri generiranju E-S1 i E-S2 tajnih nonce, to jest, iskorištava uređaje sa slabom ili nikakvom entropijom. Znajući te dvije varijable u vremenskom rasponu od nekoliko sekunda do nekoliko minuta može se lagano doći do WPS[8] PIN-a [22]
2. *Reaver* je jedan od prvih alata za napad grubom silom na WPS protokol. Napravljen je za dobivanje WPA/WPA2 ključa preko WPS protokola. Dizajniran je tako da radi s gotovo svim pristupnim točkama i konfiguracijama. U prosjeku *Reaver* će otkriti WPA2 ključ unutar 4 do 10 sati, pri čemu će polovicu vremena potrošiti na pogađanje WPS PIN-a, a drugu polovicu na otkivanje ključa [23]
3. Alat *Bully* veoma je sličan *Reaver-u,* radi na principu napada grubom silom na WPS protokol, ali dolazi s poboljšanjima poput manje ovisnosti o drugim programima, poboljšanjima u iskorištavanju glavne memorije (RAM) i procesora. *Bully* predstavlja robusnije rješenje naspram *Reavera,* te je također pogodan za gotovo sve pristupne točke. [24]

[8] WPS (engl. Wi – Fi Protected Setup) – predstavlja standard za bežično povezivanje između pristupne točke i krajnjeg uređaja. Cilj WPS-a bio je omogućiti kućnim korisnicima brzo postavljanje sigurnosnih postavki.

4.2.2. KRACK

KRACK – (*engl.* ***K****ey* ***R****einstallation* ***A****ttac****k****s*) – s obzirom na to da ovaj napad iskorištava manu unutar samog WPA2 protokola koji je danas najrašireniji sigurnosni protokol to čini veliki dio populacije ranjivim na ovu vrstu napada. KRACK napada četverostruko rukovanje koji se koristi za autentifikaciju korisnika pristupnoj točki. WPA2 protokol dizajniran je s privremenim prekidima veze između korisnika i pristupne točka na umu, te dozvoljava uporabu istih vrijednosti za treći korak u rukovanju prilikom ponovnog spajanje korisnika. KRACK napad to iskorištava i napadač može neprestano ponovo slati treće rukovanje nekog drugog uređaja i na taj način manipulirati ili poništiti WPA2 enkripcijski ključ.

Iako se kroz softversku nadogradnju ovaj problem popravio i dalje postoje načini da sustavi napadnu i budu kompromitirani od strane KRACK napada. [25]

4.2.3. PMKID napad

PMKID (engl. *Pairwise Master Key Identifiers*) za razliku od ostalih tehnika ova metoda ne zahtijeva uspostavu veze između korisnika i pristupne točke. Ovaj napad cilja na RSN-IE[9] (engl. *Robust Security Network Information Element*) element pojedinog EAPOL okvira. RSN – IE u sebi nosi informaciju o PMKID-u.
Prednosti ovog napada su što se ne mora čekati uspostava veze između korisnika i pristupne točke, kao ni čekanje da se izvrši četverostruko rukovanje. [26]

4.2.4 Napad grubom silom uz rječnik

Jedan od najlakših napada za implementaciju koji pogađa sve sigurnosne protokole je napad grubom silom uz rječnik. Radi se o napadu grubom silom uz korištenje rječnika (engl. *Dictionary*). Rječnik je ništa drugo nego tekstualna datoteka u koju su spremljene moguće lozinke. Program isprobava lozinku po lozinku dok ne nađe odgovarajuću. Rječnik možemo sastaviti sami ili preuzeti jedan od više dostupnih na internetu. Sam rječnik sastavlja se od popisa najčešće korištenih lozinki i njihovih permutacija. [27]

[9] RSN-IE predstavlja dodatna opcija koje se može pronaći u 802.11 upravljačkim okvirima.

Slika 4.1 Izgled jednog od online dostupnih rječnika

4.3 Napadi na WPA3

Iako stvoren da pruži najviši standard sigurnosti bežičnih mreža, WPA3 nije otporan na neovlašteni upad. Glavni problem leži u *Dragonfly* rukovanju koje se koristi prilikom spajanja uređaja u WPA3 mrežu. Dizajnirano protiv kriptografskih napada, *Dragonfly* rukovanje ipak posjeduje sigurnosne propuste. Upad je otkriven 2019. godine i povezan je s algoritmom za kriptiranje u protokolu *Dragonfly.* [28]

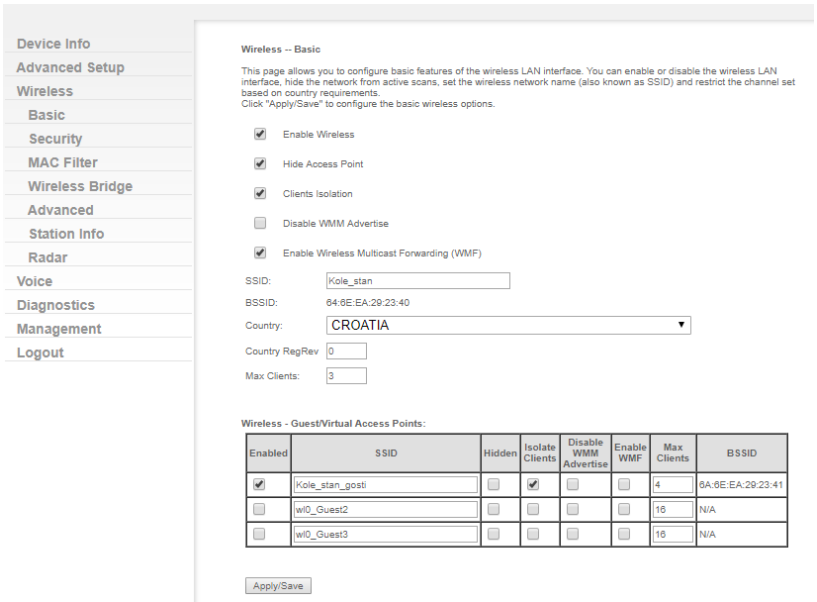
Nadalje, postoje sigurnosni propusti koji su pronađeni u WPA3 *Personal* standardu. Taj skup sigurnosnih propusta nosi ime *Dragonblood.* Jedan od napada koje je moguće izvršiti na WPA-3 *Personal* standard zove se *downgrade* napad. Taj napad vrši se na mreži koja istodobno podržava WPA2 i WPA3 standard. Prilikom napada, napadač koristi lažnu pristupnu točku koja podržava samo WPA2. Time se postiže da se žrtva spoji na mrežu koristeći četverostruko rukovanje u WPA2 standardu. Prije nego se prelazak s WPA3 na WPA2 primijeti, napadač je, koristeći četverostruko rukovanje, skupio dovoljno informacija kako bi mogao pokrenuti napad grubom silom uz rječnikom. [29]

5. ZAŠTITA LOKALNIH BEŽIČNIH MREŽA

Pri samim počecima lokalnih bežičnih mreža, bilo je dovoljno naći se u blizini određene mreže kako bi joj se pristupilo. Autentifikacija korisnika nije bila potrebna. No, rastom korisnika i broja lokalnih bežičnih mreža, postalo je nužno osigurati mrežu kako bi se zaštitili njeni korisnici kao i informacije koje se dijele. Iako ni jedna mreža nije sigurna moguće je poduzeti određene korake kako bi se maksimalno ogradili od mogućih napada.

1. MAC filtriranje: svaki mrežni uređaj određen je MAC adresom koja je definirana s 12 heksadecimalnih znakova. Većina današnje mrežne opreme omogućuje zaštitu pomoću filtriranja MAC adresa. Implementacija je jednostavna- korisnik ili administrator mreže jednostavno podesi parametre tako da samo određene MAC adrese imaju pravo pristupa. Iako je moguće lažirati MAC adresu, ova opcija predstavlja dodatan sloj sigurnosti [30]
2. Dinamično IP adresiranje – dinamične IP adrese imaju prednost pred statičnim zbog toga što se konstantno mijenjaju. Dakle, dok stalnost statične IP adrese pruža napadačima dovoljno vremena za napad na samo jednu adresu, trenutačna, dinamična IP adresa im otežava mogućnost napada. Nadalje, potrebno je naglasiti da su i statična i dinamična IP adresa vidljive napadačima. Ako korisnik želi, za trenutno skrivanje, može koristiti *Tor* preglednik ili javne Wi-Fi mreže [31]
3. Sakrivanje SSID-a što (engl. *Service Set Identifiers*) predstavlja pojam kojeg povezujemo uz identifikaciju mreže, a to je zapravo ime našeg WLAN-a. Ono se sastoji od 32 znaka koji mogu biti slova ili brojke. Prilikom spajanja na mrežu, korisnik vidi ime svoje mreže, kao i imena drugih korisnika mreže. Svako vidljivo ime je zapravo SSID te mreže. Iako skrivanje SSID ne pruža veliku sigurnost nije loša opcija za implementirati. Nadalje, i u vidljivoj SSID mreži, nužno je postaviti zaporku kako bi se ograničio pristup mreži [32]
4. Uporaba enkripcije – uporabom enkripcije poput WPA, WPA2 i korištenjem snažnih zaporki uvelike otežavamo posao napadačima što predstavlja prvu liniju obrane od napada. Nadalje, vezano uz enkripciju, na većini mrežnih usmjerivača nalazi se gumb pod nazivom WPS (*Wi-Fi Protected Setup).* WPS je povezan s WPA *Personal* i WPA2 *Personal* sigurnosnim protokolima. WPS se ne koristi na mrežama koje su spojene s WPA protokolom, s obzirom na njegovu zastarjelost i nedostatak sigurnosti. U WPS konfiguraciji, zaporka se generira nasumično [33]

5. Uporaba vatrozida - vatrozid predstavlja prvu liniju obrane od napada i većina mrežnih usmjerivača ima ga ugrađenog. Vatrozid nadgleda promet koji dolazi i odlazi te blokira sumnjive aktivnosti, većina vatrozida koristi filtriranje po paketima što znači da se pregledava zaglavlje paketa kako bi se odredilo polazište i odredište. Informacije od polazištu i odredištu se uspoređuju predefinirani pravilima koja određuju je li paket legitiman ili ne, točnije, hoće li vatrozid propustiti paket ili ne [33]
6. VPN – (engl. *Virtual Private Network*) predstavlja virtualnu kriptiranu mrežu. Ovakav sustav poznat je pod riječju *tunneling,* jer je kriptirani podatkovni tok poslan preko obične mreže. Prilikom upotrebe VPN-a dolazi do enkripcije podataka koji se šalju preko Wi-Fi mreže. Na taj način podaci postaju nečitljivi. Nadalje, VPN sakriva i povijest pretraživanja jer se samo pretraživanje povezuje s IP adresom VPN servera, a ne s IP adresom korisnika [33]
7. Odvojena mreža za goste – izradom odvojene mreže za goste uvelike se povećava sigurnost, gosti imaju pristup Internetu, ali nemaju pristup vašim podacima unutar lokalne mreže. Nadalje, odvojenom mrežom za goste sama mreža i mrežni uređaji se štite od vanjsko inficiranih uređaja. Dakle, posebna mreža za goste štiti ostatak mreže od zlonamjernog *softvera*. Kada su u pitanju IoT uređaji, također se preporučuje spajanje na odvojenu mrežu za goste zbog čestih ažuriranja IoT uređaja. Time se glavna mreža štiti od potencijalnih štetnih ažuriranja ili od napada preko IoT uređaja. Postoje brojni načini za zaštitu bežičnih mreža, a kombinacijom više načina zaštite uvelike možemo otežati posao napadačima. [34]



Slika 5.1: Postavke bežične mreže.

U primjeru sa slike radi se o vlastitoj bežičnoj mreži gdje je ograničen broj klijenata na osobno računala te dva mobilna telefona kojima su adrese statičke. Za goste su dozvoljena 4 uređaja koja su na odvojenoj mreži te imaju pristup Internetu, ali nemaju pristup lokalno spojenim uređajima.

Tablica 5.1 Popis najkorištenijih lozinki 2018. godine. [35]

Top 20 lozinki 2018			
1	123456	**11**	princess
2	password	**12**	admin
3	123456789	**13**	welcome
4	12345678	**14**	666666
5	12345	**15**	acb123
6	111111	**16**	footbal
7	1234567	**17**	123123
8	sunshine	**18**	monekey
9	qwerty	**19**	654321
10	iloveyou	**20**	!@#$%^&*

6. PENETRACIJSKO TESTIRANJE

Penetracijsko testiranje vrsta je etičkog hakiranja. Samo etičko hakiranje koristi se za sprječavanje mrežnog kriminala i zaštitu mreža od napada. Cilj etičkog hakiranja je primijetiti sigurnosne propuste na vrijeme, kao i predložiti načine na koje se može podići razina sigurnosti cjelokupnog sustava. Kako bi se procijenila razina sigurnosti, nužno je provesti penetracijsko testiranje. Takva vrsta testiranja simulira pravi hakerski napad na sustav. Na taj način provjerava se svaka komponenta testiranog sustava te se otkrivaju njegove slabosti i mane. [36]

Pri penetracijskom testiranju najčešće se koristi *Kali Linux*. Sam program nastao je kao preinaka *Backtrack Linux-a*, programa koji se također koristi za penetracijsko testiranje. *Kali Linux* temelji se na *Debian* standardu te je prvi put pušten u javnost 2013. godine. Popularnost programa temelji se na tome što je besplatan i dolazi uz mnogo alata vezanih uz mrežnu sigurnost [37]. Uz *Kali Linux* potrebna je i mrežna Wi-Fi kartica koja podržava *monitor mode.*

Monitor mode predstavlja način rada gdje mrežna kartica prelazi u *listening mode* i na taj način možemo zabilježiti sve tipove mrežnih paketa koji su nam potrebni za napad na bežične mreže.

6.1 Penetracijsko testiranje u laboratorijskim uvjetima

U svrhu ovog završnog rada odrađeno je penetracijsko testiranje bežične mreže s WEP enkripcijom. Pri testiranju korišteno je:

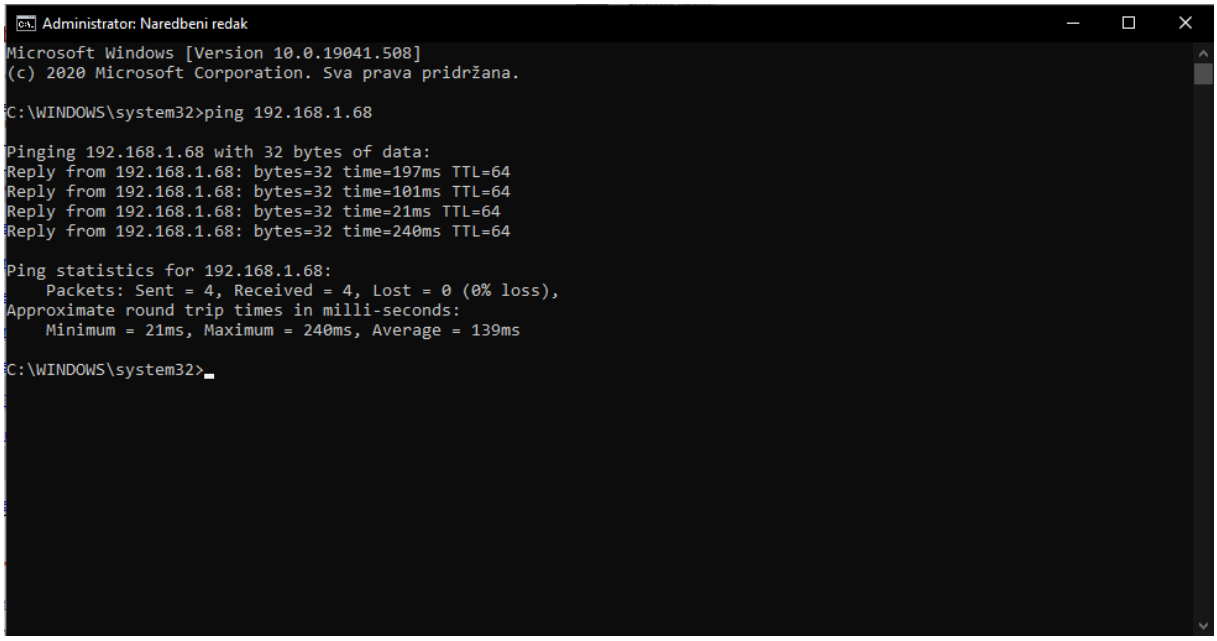
1. Mrežni usmjerivač marke *Thomson*, model ST780i WL za kreiranje pristupne točke
2. *Kali Linux* distribuciju za izvršavanje penetracijskog testiranja
3. Mrežnu karticu marke Tp-Link, model TL-WN722N za pristup mreži.

Penetracijsko testiranje započelo je kreiranjem bežične mreže na mrežnom usmjerivaču. U postavkama mrežnog usmjerivača postavljena je Wi-Fi mreža s imenom *PenTesting* sa 64bit-nom WEP enkripcijom i WEP enkripcijskim ključem „1234567890“.

Slika 6.1: prikaz primijenjenih postavki lokalne bežične mreže.

Na slici 6.1. vidljive su prethodno spomenute postavke koje su bile temelj penetracijskog testiranja.

Nakon postavljanja postavki uslijedilo je spajanje uređaja na lokalnu bežičnu mrežu kako bi se provjerila ispravnost i funkcionalnost mreže. Nakon spajanja uređaja testirana je komunikacija između njih to je postignuto koristeći *ping* naredbu uz IP adresu jednog od spojenih uređaja, kao što je vidljivo na slici 6.2.



Slika 6.2: prikaz komunikacije dva uređaja na mreži.

Po završetku postavljanja mreže započinje se s kreiranjem uvjeta za penetracijsko testiranje što uključuje instalaciju *Linux* distribucije *Kali*. Za instalaciju korišten je dodatni prijenosnik iako je moguće koristiti i virtualni stroj za instalaciju gore spomenutog operacijskog sustava.

Prilikom instalacije operacijskog sustava dovoljno je pratiti uputstva od strane proizvođača.

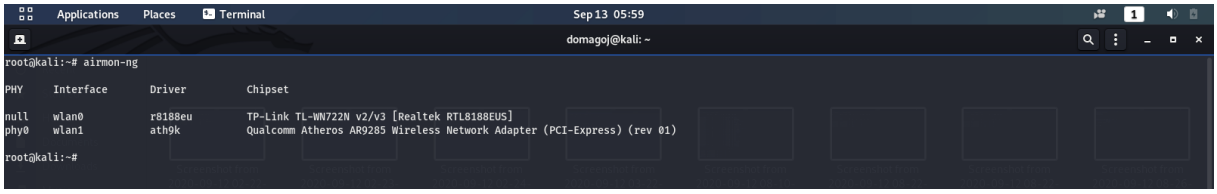
Nakon dovršetka instalacije bilo je potrebno ažurirati sve pakete u svrhu postizanja funkcionalnosti odabrane mreže kartice.

S obzirom na to da odabrana mrežna kartica nije automatski podržana potrebno je bilo preuzeti i instalirati upravljački program za nju. Naredbe potrebne za preuzimanje i instalaciju upravljačkog programa vidljive su na slici 6.3.

```
git clone https://github.com/lwfinger/rtl8188eu.git
cd rtl8188eu
make
make install
modprobe 8188eu
```

Slika 6.3: postupak preuzimanja i instalacija upravljačkih programa.

Slika 6.4. prikazuje mrežna sučelja što uključuje i mrežnu karticu koja će koristiti za napad na mrežu.



Slika 6.4: prikaz mrežnih sučelja.

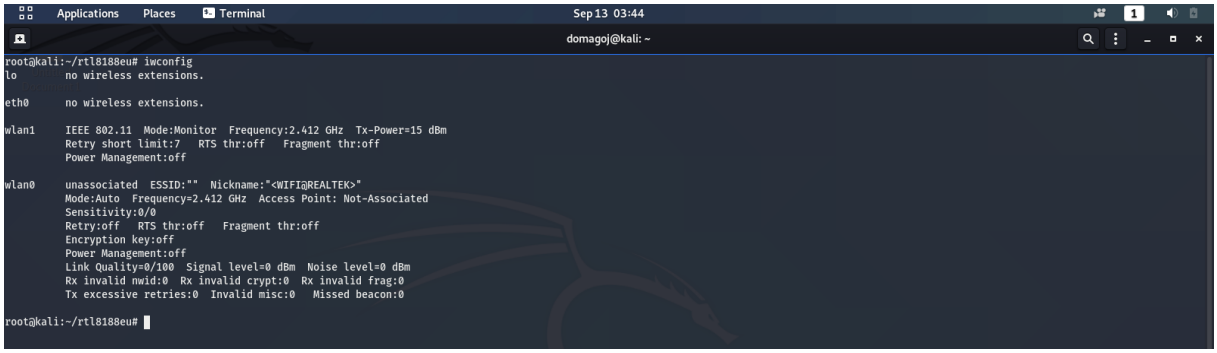
S obzirom na to da je mrežna kartica vidljiva operacijskom sustavu može se započeti s penetracijskim testiranjem.

Potrebno je bilo prebaciti mrežnu karticu iz *Managed mode-a* u *Monitor mode*. To se postiže na sljedeći način; gašenje *wlan0* sučelja, terminiranje svih procesa koji ometaju rada alata, prebacivanje *wlan0* sučelja u *monitor mode*, te ponovo podizanje sučelja, što je vidljivo na slici 6.5.

```
ifconfig wlan0 down
airmon-ng check kill
iwconfig wlan0 mode monitor
ifconfig wlan0 up
```

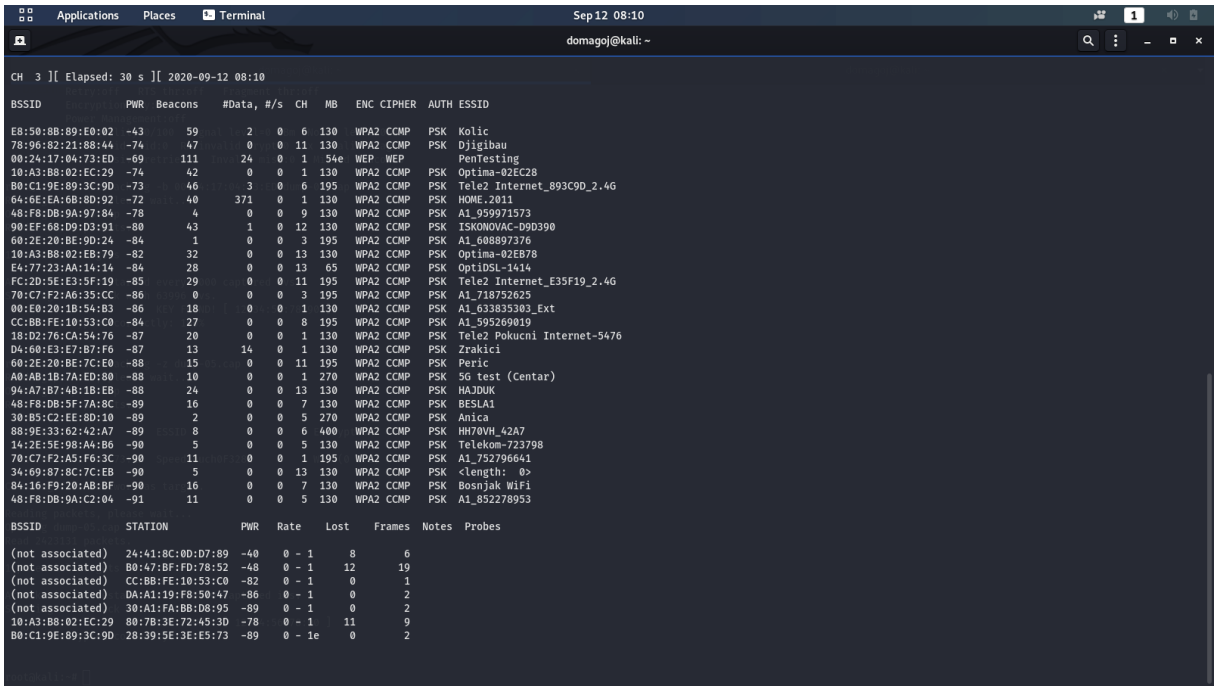
Slika 6.5: naredbe potrebne za prelazak mrežne kartice u monitor mode.

Radi provjere uspješnosti procesa moguće je koristiti naredbu *iwconfig*, što je vidljivo na slici 6.6., koja prikazuje mrežna sučelja i detalje o njima, između ostalog i informaciju o tome u kojem stanju se nalazi mrežna kartica.



Slika 6.6:prikaz mrežnih sučelja i njihovih stanja.

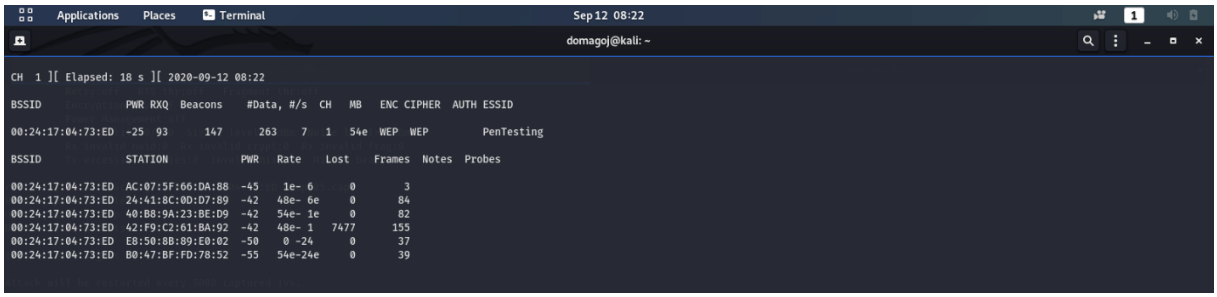
Kako bi odabrali mrežu koju želimo napasti prvo je potrebno koristiti naredbu *airodump-ng* uz priklano mrežno sučelje, u ovom slučaju radi se o *wlan0* sučelju. Ova naredba skenira sve kanale i prikazuje sve pristupne točke koje odašilju. Prikaz ispisa *airodump-ng* naredbe vidljiv je na slici 6.7.



Slika 6.7:prikaz mreža u blizini.

Uz pomoć ove naredbe dobivamo informacije o: MAC adresi pristupne točke, jačini signala, broju *beacon* okvira, vrsti enkripcije i imenu bežične mreže.

Sa slike 6.7. vidljiva je *PenTesting* mreža s MAC adresom: 00:24:17:04:73:EB i WEP razinom enkripcije na prvom kanalu. Ove informacije potrebne su za nastavak procesa.



Slika 6.8: prikaz hvatanja inicijalizacijskih vektora.

Uz informacije iz prethodne naredbe: MAC adresa mreže, broj kanala možemo započeti hvatanje inicijalizacijskih vektora.

```
airodump-ng -c 1 --bssid 00:24:17:04:73:EB  -w dump wlan0mon
```

Slika 6.9: prikaz airodump-ng naredbe.

Razlika između zadnjih dviju naredbi je u tome što zadnja naredba ima dodatne parametre. S obzirom na skeniranje kanala nije moguće uhvatiti sve potrebne pakete ciljane mreže te s toga uz dodatne parametre možemo slušati samo jedan kanal i njegov promet spremiti na uređaj za pohranu.

Tablica 6.1: definicije korištenijih parametara.

-c	Parametar za odabir kanala
--bssid	Parametar za odabir MAC adrese
-w	Parametar za spremanje podataka na disk

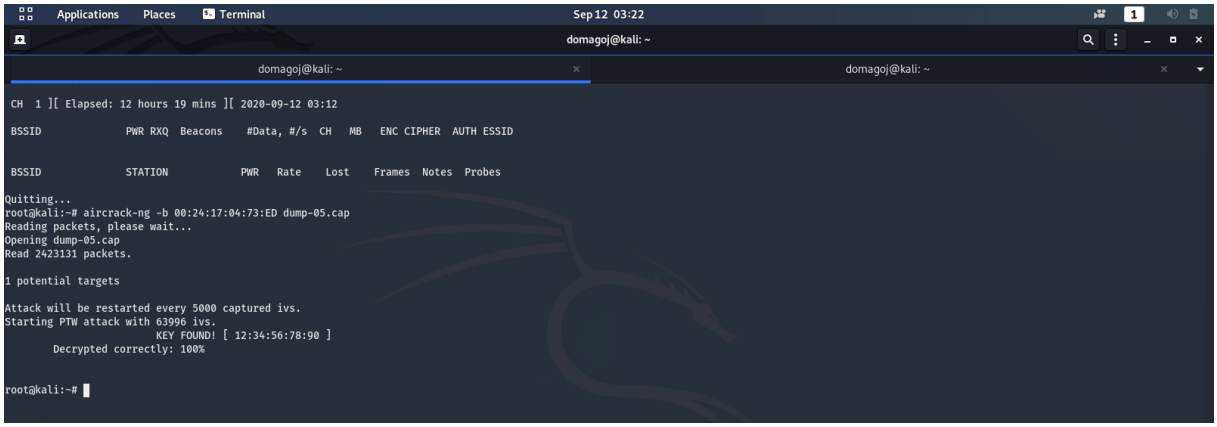
Napad na mrežu moguć je tek nakon što se skupi određena količina inicijalizacijskih vektora. Potrebno je sakupiti najmanje 40 000 vektora. U slučaju nepostojanja dovoljne količine mrežnog prometa sakupljanje dovoljnog broja inicijalizacijskih vektora može potrajati, jedan od načina ubrzavanja procesa je *ARP* napad.

Nakon skupljana dovoljnog broja inicijalizacijskih vektora može se pokušati probiti WEP ključ.

```
aircrack-ng -b 00:24:17:04:73:EB dump-05.cap
```

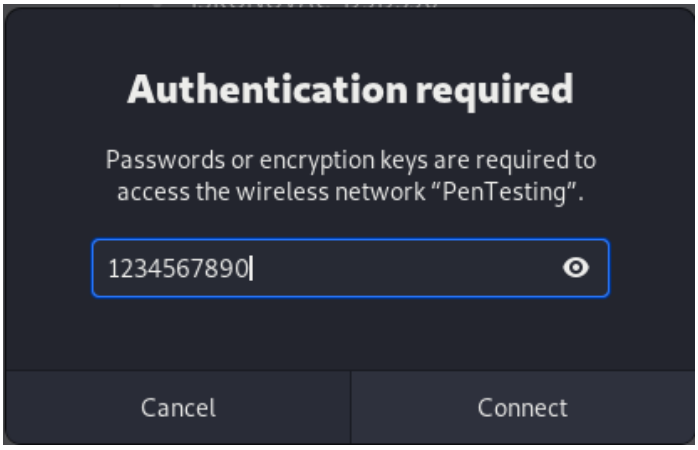
Slika 6.10: naredba za pokretanje probijanja.

Naredba sa slike 6.10. služi za probijanje mrežnog ključa, potrebno je u njoj definirati MAC adresu pristupne točke i datoteku u kojoj je sadržan uhvaćeni mrežni promet.



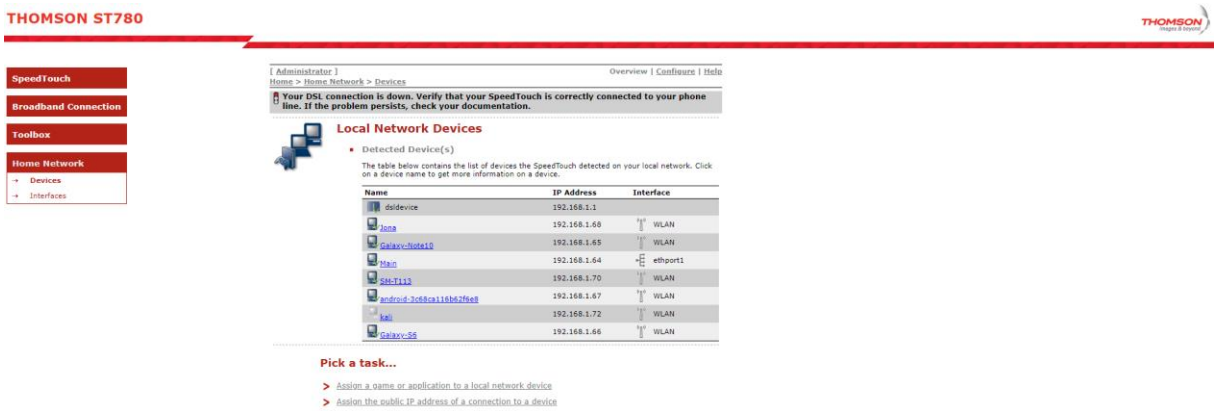
Slika 6.11: prikaz pronalaska ključa.

Slika 6.11. prikazuje trenutak kada je ključ pronađen. Ključ se nalazi u heksadecimalnom formatu te je potrebno samo ukloniti dvotočje pri unosu ključa prilikom spajanja na mrežu.



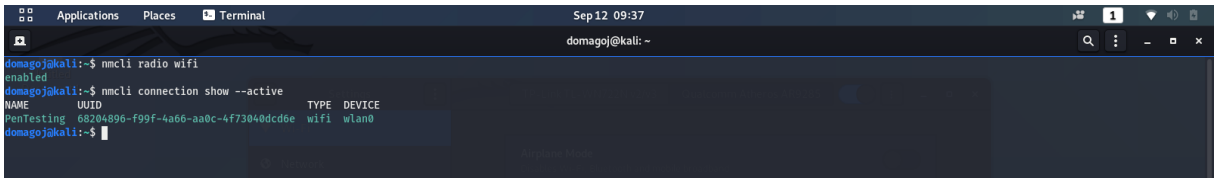
Slika 6.12: unos ključa bežične mreže

Slika 6.12 prikazuje pokušaj prijava na bežičnu mrežu.



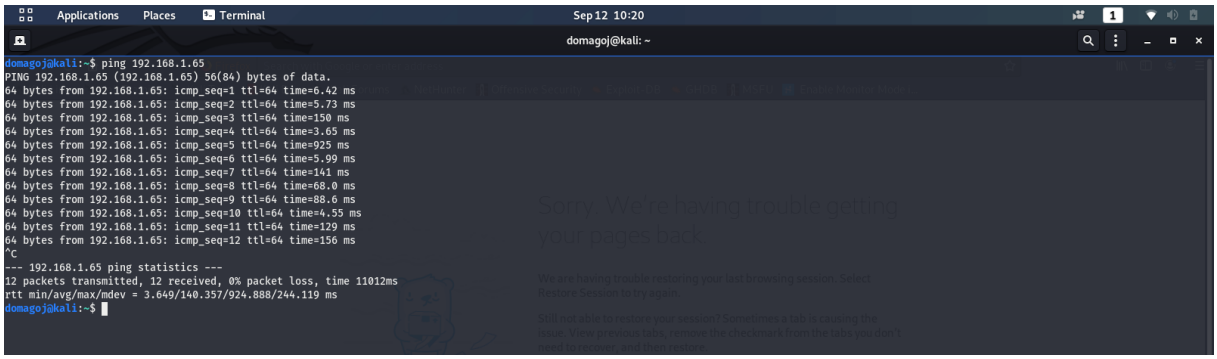
Slika 6.13:prikaz spojenih uređaja

Sa slike 6.13 je vidljivo da se na mrežu pridruži novi uređaj koristeći pronađeni ključ.



Slika 6.14: prikaz aktivne veze s napadačeva računala.

Slika 6.14 prikazuje korištenje naredbe *nmci radio wifi* s kojom se prikazuju detalji o mrežnom sučelju kao i povezanosti na bežičnu mrežu.



Slika 6.15:prikaz komunikacije dva uređaja na mreži

Slika 6.15. prikazuje komunikaciju između napadačeva računala i računala od prije povezanog na lokalnu bežičnu mrežu.

7. ZAKLJUČAK

Naš svakodnevni život danas je teško zamisliv bez bežičnih mreža, bilo da je riječ o poslu ili privatnoj upotrebi. Upotrebljavamo ih u vlastitim kućama i stanovima, očekujemo ih i susrećemo se s njima na fakultetima, gradskim trgovima, trgovinama, bankama i mnogim drugim mjestima

Bežične mreže nude veću slobodu kretanja, a s time i brži, lakši pristup informacijama, gdje više nije potrebno naći slobodno računalo u knjižnici kako bi potražili neke informacija. Sada je dovoljno da se spojimo na bežičnu mrežu i sami potražimo informaciju na našim uređajima.

S obzirom na način funkcioniranja bežičnih mreža i njihovu opću sveprisutnost bitno se pobrinuti i osigurati određena sigurnosna svojstva kako korisnici koji koriste bežičnu mrežu zajedno s njihovim podacima ne bi bili ugroženi.

Tijekom godina razvijeni su brojni sigurnosni protokoli koju su nastali kako bi osigurali sigurnost u bežičnim mrežama.

Godine 1997. pojavio se prvi standard za enkripciju nazvan WEP, a cilj je bio da pruži istu razinu sigurnosti kao kod žičanih mreža. Međutim, tijekom godina pronađeni su sigurnosni propusti kod WEP protokola te je on zamijenjen prvo WPA, a kasnije WPA2 protokolom.

WPA2 protokol nastao je da riješi sve probleme i ranjivosti WEP-a i danas je najrašireniji sigurnosni protokol u bežičnim mrežama. Za bolju sigurnost, osiguranje integriteta i osiguranje tajnosti poruke koristi značajno naprednije algoritme nego prijašnji protokoli. Za osiguranje integriteta poruke koristi CBC- MAC način rada, dok za tajnost poruka koristi blokovne šifre s CTR (*engl. Counter*) načinom rada.

WPA2 dolazi s TKIP I CCMP sigurnosnim protokolima, od kojih je CCMP napredniji. TKIP je implementiran kako bi se pružila bolja sigurnost, kroz softversku nadogradnju starijim uređajima koji su koristili WEP. Za razliku od CCMP-a, TKIP nije zahtijevao dodatna hardverska rješenja.

WPA2 protokol može se koristiti na dva načina: WPA2 PSK i WPA2 Enterprise, gdje WPA2 predstavlja rješenje za privatne i male poslovne korisnike te se lagano implementira jer ne zahtijeva poslužitelja za provjeru autentičnosti. Krajnji korisnik definira PSK ključ koji se koristi za spajanje na pristupnu točku.

Kod WPA2 Enterprise protokola koristi se zaseban ključ za svakog klijenta koji se spaja na pristupnu točku. Enterprise način rada pruža još jedan dodatan sloj sigurnosti jer se svaki uređaj u mreži mora identificirati i ovjeriti identitet lozinkom.

Kroz dugi niz godina od začetka WPA2 protokola pronađeni su brojni načini za napade na WPA2 mreže od kojih su neki više, a neki manje učinkoviti. Najznačajniji napad kod WPA2 protokol je KRACK napad koji iskorištava treći korak u četverostrukom rukovanju u svoju korist.

Wi- Fi savez predstavio je novu verziju WPA protokola – WPA3 koji bi trebao riješiti sve manje i ranjivosti WPA2 protokola, ali nedavno je pronađen ozbiljan sigurnosni propust i u WPA3 protokolu. Radi se o takozvanom *Dragonblood* napadu koji iskorištava manu na *Dragonfly* protokolu.

U ovom završnom radnu odrađeno je penetracijsko testiranje lokalne bežične mreže sa svrhom dobivanja pristupa lokalnom mreži i uređajima na njoj.

Širenjem bežičnih mreža i opće povezanosti doći će do razvoja novih, još boljih protokola, a s dolaskom novih protokola doći će i do otkrivanja novih sigurnosnih propusta.

Reference

[1] CARNet, »Centar Informacijske Sigurnosti,« Lipanj 2009. [Mrežno]. Available: www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-06-267.pdf. [Pokušaj pristupa 17 Rujan 2020].

[2] Wikipedia, »IEEE 802.11,« Wikipedia, 17 Rujan 2020. [Mrežno]. Available: en.wikipedia.org/wiki/IEEE_802.11#endnote_80211ns_sgiB6. [Pokušaj pristupa 17 Rujan 2020].

[3] Wikipedia, »IEEE 802.11a-1999,« Wikipedia, 6 Svibanj 2020. [Mrežno]. Available: en.wikipedia.org/wiki/IEEE_802.11a-1999. [Pokušaj pristupa 17 Rujan 2020].

[4] Wikipedia, »IEEE 802.11g-2003,« Wikipedia, 25 Srpanj 2020. [Mrežno]. Available: https://en.wikipedia.org/wiki/IEEE_802.11g-2003. [Pokušaj pristupa 17 Rujan 2020].

[5] Wikipedia, »IEEE 802.11n-2009,« Wikipedia, 31 Kolovoz 2020. [Mrežno]. Available: https://en.wikipedia.org/wiki/IEEE_802.11n-2009. [Pokušaj pristupa 17 Rujan 2020].

[6] Wikipedia, »IEEE 802.11ac,« Wikipedia, 6 Kolovoz 2020. [Mrežno]. Available: en.wikipedia.org/wiki/IEEE_802.11ac. [Pokušaj pristupa 17 Rujan 2020].

[7] Wikipedia, »Wired Equivalent Privacy,« Wikipedia, 15 Kolovoz 2020. [Mrežno]. Available: en.wikipedia.org/wiki/Wired_Equivalent_Privacy. [Pokušaj pristupa 17 Rujan 2020].

[8] Wikipedia, »Wi-Fi Protected Access,« Wikipedia, 28 kolovoz 2020. [Mrežno]. Available: en.wikipedia.org/wiki/Wi-Fi_Protected_Access. [Pokušaj pristupa 17 Rujan 2020].

[9] S. Frankel, B. Eydt, L. Owens i K. Scarfone, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Gaithersburg: National Institute of Standards and Technology, 2007.

[10] C. Chaplin, E. Qi, H. Ptasinski, J. Walker i S. Li, »IEEE 802 LAN/MAN Standards Committee,« 9 Veljača 2005. [Mrežno]. Available: http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf. [Pokušaj pristupa 17 Rujan 2020].

[11] G. Weildman, Penetration Testing: A Hands-On Introduction to Hacking, San Francisco: No Starch Press, 2014.

[12] Wikipedia, »IEEE 802.11i-2004,« Wikipedia, 5 Travanj 2020. [Mrežno]. Available: en.wikipedia.org/wiki/IEEE_802.11i-2004. [Pokušaj pristupa 17 Rujan 2020].

[13] Wikipedia, »RADIUS,« Wikipedia, 4 Rujan 2020. [Mrežno]. Available: en.wikipedia.org/wiki/RADIUS. [Pokušaj pristupa 17 Rujan 2020].

[14] C. Hoffman, »What Is WPA3, and When Will I Get It On My Wi-Fi?,« How-To Geek, 21 Listopad 2018. [Mrežno]. Available: www.howtogeek.com/339765/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi/. [Pokušaj pristupa 17 Rujan 2020].

[15] Wi-Fi Alliance, »Discover Wi-Fi: Security,« Wi-Fi Alliance, 2018. [Mrežno]. Available: www.wi-fi.org/discover-wi-fi/security. [Pokušaj pristupa 17 Rujan 2020].

[16] S. Scrivens, »Android Q's Wi-Fi Easy Connect is a more secure replacement for WPS authentication,« Android Police, 10 Lipanj 2019. [Mrežno]. Available: www.androidpolice.com/2019/06/10/android-qs-wi-fi-easy-connect-is-a-more-secure-replacement-for-wps-authentication/. [Pokušaj pristupa 17 Rujan 2020].

[17] Wi-Fi Alliance, »Wi-Fi CERTIFIED Enhanced Open™ delivers data protection in open Wi-Fi® networks,« Wi-Fi Alliance, 5 Lipanj 2018. [Mrežno]. Available: www.wi-fi.org/news-events/newsroom/wi-fi-certified-enhanced-open-delivers-data-protection-in-open-wi-fi-networks. [Pokušaj pristupa 17 Rujan 2020].

[18] Humboldt University Berlin, »WPA3 Dragonfly Handshake,« Humboldt University Berlin, 20 Studeni 2018. [Mrežno]. Available: sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake. [Pokušaj pristupa 17 Rujan 2020].

[19] Georgia Southern University, »Wireless Network Attacks Simulator,« Georgia Southern University, [Mrežno]. Available: www.infotech.armstrong.edu/katz/wireless_attacks/wireless_attacks.html. [Pokušaj pristupa 17 Rujan 2020].

[20] IONOS by 1&1, »WLAN security: how to make your wireless network into a fortress,« IONOS by 1&1, 14 Kolovoz 2019. [Mrežno]. Available: www.ionos.com/digitalguide/server/security/wlan-security-the-best-protection-for-your-network/. [Pokušaj pristupa 17 Rujan 2020].

[21] Wireless Network Security, »Wireless Security Attacks,« Wireless Network Security, Siječanj 2013. [Mrežno]. Available: wirelessnetworkssecurity.blogspot.com/2013/01/wireless-security-attacks.html. [Pokušaj pristupa 17 Rujan 2020].

[22] Kali, »Pixiewps: wps pixie dust attack tool,« Kali, 4 Ožujak 2015. [Mrežno]. Available: forums.kali.org/showthread.php?25018-Pixiewps-wps-pixie-dust-attack-tool. [Pokušaj pristupa 17 Rujan 2020].

[23] KALI, »Reaver Package Description,« KALI, [Mrežno]. Available: tools.kali.org/wireless-attacks/reaver. [Pokušaj pristupa 17 Rujan 2020].

[24] Kali, »Bully Package Description,« Kali, [Mrežno]. Available: tools.kali.org/wireless-attacks/bully. [Pokušaj pristupa 17 Rujan 2020].

[25] M. Vanhoes, »Key Reinstallation Attacks,« KrackAttacks, 2017. [Mrežno]. Available: www.krackattacks.com/. [Pokušaj pristupa 17 Rujan 2020].

[26] Hackers- Arise, »Wi-Fi Hacking, Part 11: The PMKID Attack,« Hackers- Arise, 12 Ožujak 2019. [Mrežno]. Available: www.hackers-arise.com/post/wi-fi-hacking-part-11-the-pmkid-attack. [Pokušaj pristupa 17 Rujan 2020].

[27] B. Vigliarolo, »Brute force and dictionary attacks: A cheat sheet,« TechRepublic, 17 prosinac 2018. [Mrežno]. Available: www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/. [Pokušaj pristupa 17 Rujan 2020].

[28] D. Fisher, »New Weaknesses Found in WPA3,« Decipher, 5 Kolovoz 2019. [Mrežno]. Available: duo.com/decipher/new-weaknesses-found-in-wpa3. [Pokušaj pristupa 17 Rujan 2020].

[29] T. Foltýn, »WPA3 flaws may let attackers steal Wi-Fi passwords,« Welivesecurity, 11 Travanj 2019. [Mrežno]. Available: www.welivesecurity.com/2019/04/11/wpa3-flaws-steal-wifi-passwords/. [Pokušaj pristupa 17 Rujan 2020].

[30] V. Bajaj, »MAC Filtering in Computer Network,« GeeksforGeeks, 9 Kolovoz 2019. [Mrežno]. Available: www.geeksforgeeks.org/mac-filtering-in-computer-network/. [Pokušaj pristupa 17 Rujan 2020].

[31] WhatIsMyIPAddress, »Your IP Address Can Change without Notice. Should You Be Concerned?,« WhatIsMyIPAddress, [Mrežno]. Available: whatismyipaddress.com/dynamic-static. [Pokušaj pristupa 17 Rujan 2020].

[32] B. Mitchell, »What Is a Service Set Identifier (SSID)?,« Lifewire, 17 Travanj 2020. [Mrežno]. Available: www.lifewire.com/definition-of-service-set-identifier-816547. [Pokušaj pristupa 17 Rujan 2020].

[33] Norton, »Keep your home Wi-Fi safe in 7 simple steps,« Norton, [Mrežno]. Available: us.norton.com/internetsecurity-iot-keep-your-home-wifi-safe.html. [Pokušaj pristupa 17 Rujan 2020].

[34] H. Aver, »What's a guest Wi-Fi network, and why do you need one?,« Kaspersky, 17 Rujan 2018. [Mrežno]. Available: www.kaspersky.com/blog/guest-wifi/23843/. [Pokušaj pristupa 17 Rujan 2020].

[35] M. Ehrenkranz, »The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius,« Gizmodo, 13 Prosinac 2018. [Mrežno]. Available: gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705. [Pokušaj pristupa 17 Rujan 2020].

[36] EC- Council, »What is Ethical Hacking?,« EC- Council, [Mrežno]. Available: www.eccouncil.org/ethical-hacking/. [Pokušaj pristupa 17 Rujan 2020].

[37] Kali, »What is Kali Linux?,« Kali, 25 Studeni 2019. [Mrežno]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Pokušaj pristupa 17 Rujan 2020].

SAŽETAK

Ovaj završni rad obrađuje teme sigurnosti unutar bežičnih lokalnih mreža. Kroz godine, razvojem tehnologije dolaze novije i poboljšane metode zaštite lokalnih mreža. Kao prvi standard za enkripciju pojavio se WEP, a otkrivanjem njegovih nedostataka dolazi do privremenog rješenja – WPA koji je bio namijenjen za upotrebu dok ne dođe puna implementacija IEEE 802.11i standarda. Standard WPA2 koji je danas najpopularniji i najkorišteniji standard, dolazi s mnogim poboljšanjima. Standard WPA2 u službi je već 15 godina, no nije savršen te su otkriveni propusti. Svjesna propusta koji su otkriveni, organizacija Wi – Fi Alliance predstavila je 2018. godine novi i poboljšani standard – WPA3.

Kroz završni rad opisani su pojedinačni sigurnosni standardi, a odrađeno je i penetracijsko testiranje WEP protokola.

Ključne riječi: WEP, WPA, WPA2, WPA3, PENETRACIJSKO TESTIRANJE

ABSTRACT

This paper deals with security issues within wireless local area networks. Throughout the years, technology development has come up with newer and improved methods of protecting local networks. The WEP standard appeared as the first encryption standard, and the discovery of its shortcomings led to a temporary solution -WPA, that was intended for use until the full implementation of the IEEE 802.11i standard. The WPA2 standard, today's most popular and most used standard, comes with many improvements. The WPA2 standard has been in use for 15 years, but it's not perfect, and flaws have been discovered. Aware of the failures that have been discovered, the Wi-Fi Alliance organisation introduced a new and improved standard - WPA3 in 2018.

Through this paper, individual security standards were described, and WEP protocol penetration testing was performed.

Keywords: WEP, WPA, WPA2, WPA3, PENETRATION TESTING