**UNIVERZITET SINGIDUNUM**

**FAKULTET ZA INFORMATIKU I RAČUNARSTVO**

# Analiza i primena kriptoanalitičkih metoda za potrebe penetracionog testiranja

**- diplomski rad -**

**Mentor:** **Kandidat:**

***prof. dr Mladen Veinović*** ***Marko Tmušić***

**Beograd, 2016.**



# FAKULTET ZA INFORMATIKU I RAČUNARSTVO

**UNIVERZITET SINGIDUNUM**

**FAKULTET ZA INFORMATIKU I RAČUNARSTVO**

**Beograd, Danijelova 32**

**Kandidat:** Marko Tmušić

**Broj indeksa:** 2012/200036

**Smer:** Informatika i računarstvo

**Tema:** Analiza i primena kriptoanalitičkih metoda za potrebe penetracionog testiranja

**Zadatak:**

MENTOR

Datum odobrenja rada:
Beograd, ___.___._____.

_____

DEKAN

_____

# Analiza i primena kriptoanalitičkih metoda za potrebe penetracionog testiranja

**Sažetak:**
U ovom radu predstavljeni su kriptoanalitički metodi za primenu u analizi saobraćaja bežičnih računarskih mreža sa aspekta penetracionog testiranja. Detaljnim uvidom u oblast istraživanja, predstavljene su najnovije kriptoanalitičke metode, kao i metode penetracionog testiranja koje podrazumevaju izviđanje i skeniranje, izvršavanje metoda, skrivanje i generisanje izveštaja. Takođe, polazeći od teorijskih osnova standarda bežičnih mreža IEEE 802.11, predstavljeni su svi sastavni elementi ove infrastrukture. Glavni doprinos ovog rada predstavlja kvalitetna studija slučaja koja prikazuje praktično korak po korak primenu kriptoanalitičkog metoda „Zli blizanac“. Na kraju je dat zaključak koji jasno ukazuje na trenutne teorijske i praktične okvire metoda za potrebe kriptoanalize i trenutno dostupni računarski resurs.

**Ključne reči:** kriptoanaliza, penetraciono testiranje, bežične mreže

# Analysis and usage of cryptanalytical methods for penetration testing purposes

**Abstract:**

In this paper we will dissect cryptanalytic methods applied in the field of traffic analysis of wireless computer networks. We are going to give a detailed overview of well-known cryptanalytic methods and an overview of different attack scenarios on a variety of cryptographic protection systems. Noted contribution for writing this paper and case study will encompass an exhibition and use of the “Evil twin” method, which is used for a direct attack on access points.

**Keywords:** cryptanalysis, penetration testing, wireless networks

# Sadržaj

- diplomski rad - ... - 1 -

**1 Uvod ... - 3 -**

1.1 Predmet istraživanja ... - 3 -

1.2 Doprinos rada ... - 3 -

1.3 Struktura rada ... - 4 -

**2 Pregled u oblasti istraživanja ... - 5 -**

2.1 Kriptoanaliza ... - 5 -

2.2 Savremeni kriptoanalitički metodi ... - 6 -

2.2.1 Najzastupljeniji napadi i pretnje ... - 7 -

2.3 Peneteracione testiranje ... - 8 -

2.3.1 Izviđanje i skeniranje ... - 9 -

2.3.2 Izvršavanje kriptoanalitičkog metoda ... - 9 -

2.3.3 Održavanje kontrole i sakrivanje ... - 10 -

2.3.4 Pravljenje izveštaja ... - 10 -

2.4 Okruženje za penetraciono testiranje – Kali Linux ... - 10 -

2.5 Open Web Application Security Project - OWASP ... - 11 -

2.5.1 Najzastupljeniji napadi prema OWASP statistici ... - 11 -

**3 Teorijske osnove istraživanja ... - 19 -**

3.1 Uvod u bežične mreže ... - 19 -

3.2 Fizičko ograničavanje propagacije signala ... - 19 -

3.3 Identifikator skupa usluga ... - 20 -

3.4 Povezivanje stanice sa pristupnom tačkom ... - 21 -

3.5 Standardi bežičnih mreža ... - 21 -

3.6 Standard bežičnih mreža IEEE 802.11 ... - 22 -

3.6.1 Infrastrukturni režim povezivanja BSS (Basic Service Set) ... - 22 -

3.6.2 Nezavisni način povezivanja IBSS (Independent Basic Service Set) ... - 22 -

3.6.3 Bežični distributivni sistemi ... - 22 -

3.6.4 Interakcija sa drugim IEEE 802 slojevima ..... - 23 -
3.7 Tipovi frejmova IEEE 802.11 standarda ..... - 23 -
3.8 Uvod u protokole bežičnih mreža ..... - 26 -
3.8.1 WEP ..... - 26 -
3.8.2 WEP2 ..... - 27 -
3.8.3 WPA ..... - 27 -
3.8.4 WPA2 ..... - 28 -
3.8.5 CCMP ..... - 29 -
3.9 Kriptoanalitički metod „Zli blizanac“ (engl. *Evil Twin*) ..... - 29 -
**4 Eksperimentalni rad – studija slučaja ..... - 31 -**
4.1 Primena kriptoanalitičkog metoda „Zli blizanac“ (engl. *Evil Twin*) ..... - 31 -
4.1.1 Metodologija napada ..... - 31 -
4.1.2 Potrebni uređaji ..... - 31 -
4.1.3 Potreban softver ..... - 31 -
4.2 Detaljan opis kriptoanalitičkog metoda „Zli blizanac“ ..... - 32 -
**5 Zaključak ..... - 37 -**
5.1 Predlog za budući rad ..... - 37 -
**6 Literatura ..... - 38 -**
**7 Appendix ..... - 39 -**

# 1 Uvod

## 1.1 Predmet istraživanja

Porastom popularnosti interneta, javio se problem obezbeđivanja sigurnosti računarskih, informacionih sistema i mreža. To postaje glavni problem preduzeća, organizacija i vladinih institucija, pa čak i pojedinaca. Oni koriste internet za elektronsko poslovanje, reklamiranje, širenje i veću dostupnost informacija, kao i za druge stvari. Ovde se javlja glavna briga da oni budu „uhakovani“. Kako bi ostvarili kontrolu nad ličnim i osetljivim informacijama, javila se potreba za angažovanjem stručnjaka za sigurnost koji će vršiti testove proboja (penetraciono testiranje) korišćenjem istih tehnika i alata kao i potencijalni napadač. Za razliku od napadača, on ne ugrožava sistem i ne krade informacije, već skreće pažnju na potencijalne ranjivosti sistema i kako se one mogu ukloniti, kako bi podaci bili što bezbedniji.

U ovom radu će biti predstavljen jedan od primera testiranja proboja u lokalnu bežičnu mrežu korišćenjem okruženja za penetraciono testiranje *Kali Linux*, gde je prikazano da uz poznavanje sistemske arhitekture i korišćenjem propusta u mrežnim protokolima lako možemo doći do poverljivih i privatnih podataka korisnika. Sa obzirom da sa sigurnošću ne možemo reći da se ovakvi napadi ne mogu u potpunosti izbegnuti, u ovom radu skrenuta je pažnja na neke od potencijalnih slabosti sistema bežičnih mreža i njihovo unapređenje. U potpunosti je prikazan kompletan kritoanalitički metod „Zli blizanac“, koji uz vešto zaobilaženje protokola zaštite dolazi do svog cilja. Cilj ovog metoda za proboj mreže jeste navođenje korisnika da se poveže na lažnu mrežu kako bi sa preciznom analizom saobraćaja mrežnih paketa došli do korisnikovih poverljivih podataka. Ovim se utvrđuje da svako može da postane meta napadača, pogotovo na javnim mestima gde su dostupne različite bežične mreže.

## 1.2 Doprinos rada

U ovom radu skrenuta je pažnja na osnovne propuste u sigurnosti bežičnih mreža koji se baziraju na standardu IEEE 802.11 i način njihovog funkcionisanja, što je ostavilo prostora za unapređenje sigurnosnih protokola. Prikazane su najčešće greške korisnika i njihova zloupotreba. Prikazan je postupak skeniranja i proboja u bežične mreže.

Na osnovu pomenutih propusta izvršen je i analiziran kompletan napad na bežične mreže „Evil Twin“.

Svrha ovog rada jeste da ukaže na neophodnost zaštite i podizanje svesti korisnika bežičnih mreža. Opisani kriptoanalitički napad „Evil Twin“ je sproveden i analiziran u edukativne svrhe i nije za cilj imao ugrožavanje bilo čije privatnosti. Napad je testiran u kontrolisanom okruženju i nikakva šteta nije načinjena.

## 1.3 Struktura rada

U prvom delu rada opisan je pregled u oblasti istraživanja osnovnih termina u oblasti kriptoanalize i opisani su savremeni kriptoanalitički metodi kao uvod u penetraciono testiranje. Izvršen je opis okruženja za penetraciono testiranje i predstavljena je statistika najzastupljenijih napada.

U drugom delu rada u teorijskim osnovama istraživanja napravljen je uvod u bežične mreže i opisani su standardi bežičnih mreža. Skrenuta je pažnja na protokole zaštite bežičnih mreža i njihove propuste. Predstavljen je kriptoanalitički metod „Zli blizanac“.

U trećem delu rada predstavljena je praktična primena kriptoanalitičkog metoda u vidu eksperimentalnog rada. Na kraju je dat predlog za budući rad u vidu unapređenja bezbednosti bežičnih mreža.

# 2 Pregled u oblasti istraživanja

## 2.1 Kriptoanaliza

Kroz istoriju informacija je oduvek imala najveću i najbitniju ulogu u životu svakog pojedinca, upravo se zbog toga javila potreba da se ona zaštiti. Pojava kriptologije napravila je pravu revoluciju u čovečanstvu.
Nastanak kriptografije, nauke koja se bavi zaštitom informacije, učinio je komunikaciju bezbednijom, a informacija je postala dosupna samo stranama koje su komunicirale i znale tajne parametre.
Cilj kriptografije jeste očuvanje tajnosti otvorenog teksta ili ključa od napadača ili neprijatelja. Prilikom komunikacije, smatra se da je komunikacioni kanal nebezbedan i da njemu pristup ima treća strana – napadač.

Upravo je kriptografija dovela do nastanka kriptoanalize, nauke koja bez ključa određuje otvoreni tekst na osnovu šifrata. Glavni cilj kriptoanalize jeste otkrivanje rada sistema, pronalaženje nedostataka i mana, njihovo iskorišćavanje i dolazak do željene informacije.
Iako je cilj ostao isti, metode i tehnike kriptoanalize su se vremenom drastično promenile. Uzrok tome jeste pokušaj kriptoanalitičara da se prilagode povećanoj kompleksnosti kriptografije.

Pokušaj kriptoanalize se naziva napad. Osnovnu postavku kriptoanalize prvi je objavio A.Kerkhof (A. Kerckhoffs) u 19. veku, navodeći da tajnost mora biti potpuno zasnovana na ključu. Upravo zbog toga što kriptoanalitičar poznaje sve pojedinosti kriptografskog algoritma i njegove primene.

**Tipovi kriptoanalitičkih napada:**

1) **Napad „samo šifrat“** (engl. *ciphertext – only attack*)
   Kriptoanalitičar poseduje šifrate nekoliko poruka za čije šifrovanje je korišćen isti algoritam za šifrovanje. Cilj kriptoanalitičara jeste da rekonstruiše otvoreni tekst ili otkrije ključ, kako bi mogao da uspešno dešifruje sve poruke, šifrovane sa istim ključem.
2) **Napad „poznati otvoreni tekst“** (engl. *known – plaintext attack*)
   Kriptoanalitičar ima pristup šifratima, kao i otvorenim tekstovima koji pripadaju tim šifratima. Cilj kriptoanalitičara jeste otkrivanje ključa koji je korišćen za šifrovanje tih poruka.
3) **Napad „odabran otvoreni tekst“** (engl. *chosen – plaintext attack*)
   Kriptoanalitičar pored pristupa šifratima i njima odgovarajućim otvorenim tekstovima, poseduje i mogućnost da bira otvoreni tekst koji će se šifrovati. Na ovaj način je kriptoanalitičar u mogućnosti da odabere specifične blokove otvorenog teksta za šifrovanje i da izračuna ključ ili odredi algoritam koji je korišćen za šifrovanje.
4) **Napad „prilagodljiv odabrani otvoreni tekst“** (engl. *adaptive – chosen – plaintext – attack)*
   Kriptoanalitičar ne samo da može da odabere šifrovan otvoreni tekst, već je u mogućnosti i da modifikuje ono što je odabrao na osnovu rezultata prethodnih šifrovanja. Razlika između prethodnog napada i ovog je u tome što u napadu „odabran otvoreni tekst“ kriptoanalitičar može da izabere veliki blok otvorenog

teksta, dok kod napada „prilagodljiv odabrani otvoreni tekst“ kriptoanalitičar može da izabere manji blok otvorenog teksta, a zatim još jedan na osnovu rezultata prvog bloka i tako dalje.

5) **Napad „odabrani šifrat“** (engl. *chosen – ciphertext – attack* )
Kriptoanalitičar ima mogućnost da izabere šifrat za dešifrovanje, ima pristup dešifrovanom otvorenom tekstu. Njegov cilj je da dođe do ključa.
6) **Napad „odabrani ključ“** (engl. *chosen – key attack*)
Kriptoanalitičar mora da poseduje veliko znanje o ključevima i njihovom međusobnom odnosu, kako bi uspešno izvršio ovaj napad. Ne znači da kriptoanalitičar ima mogućnost odabira ključeva.
7) **Kriptoanaliza pretnjom, krađom ili ucenom** (engl. *rubber – hose cryptanalysis*)
Kriptoanalitičar preti, ucenjuje nekoga dok ne dobije ključ. Drugi naziv za ovakav tip napada jeste „kupovina ključa“. Predstavljaju veoma opasne napade.

## 2.2 Savremeni kriptoanalitički metodi

Postoje tri osnovna principa sigurnosti koji čine takozvano „veliko trojstvo“. To su: poverljivost (engl. *confideniality*), integritet (engl. *integrity*) i raspoloživost (engl. *availability*). Termin na engleskom jeziku je prestavljen skraćenicom **CIA**. Sigurnosni profesionalci moraju uzeti u obzir sva tri principa prilikom kreiranja plana zaštite sistema. Svaki napad se zasniva na napadanju jedne od strana „piramide sigurnosti“.
**Poverljivost** predstavlja pokušaj da se spreči neovlašćeno otkrivanje sadržaja poruke. Poverljivost se primenjuje na podatke bilo u slučaju skladištenja, obrade ili prenosa. Za neke sistema je na prvom mestu po važnosti poverljivost, dok je za većinu organizacija ona iza integriteta i raspoloživosti.
**Cilj očuvanja integriteta** jeste očuvanje celovitosti podataka tako da ukoliko napadač pokuša da izmeni podatke, to ne može ostati neprimećeno.
Postoje dve vrste integriteta:
Integritet podataka (engl. *data integrity*) – osigurava da podaci nisu izmenjeni na nedozvoljen način bilo u toku skladištenja, obrade ili prenosa.
Integritet sistema (engl. system integrity) – osigurava da sistem funkcioniše na način koji je oslobođen nedozvoljene manipulacije i da postoji određeni kvalitet dok sistem obavlja namenjenu funkciju.
**Raspoloživost** obezbeđuje pouzdanu i pravovremenu dostupnost podacima ili računarskim resursima. Sistem je aktivan i korisnik mu može pristupiti.




*Slika 1 – „Piramida sigurnosti“*

### 2.2.1 Najzastupljeniji napadi i pretnje

#### 2.2.1.1 Odbijanje usluga (engl. Denial of service)

Predstavlja napad koji izaziva prestanak rada servisa ili programa čime se onemogućava pristup korisniku tim servisima ili programima. Izvršava se na transportnom sloju slanjem velikog broja SYN paketa. Zaštita se ogleda u kontrolisanju broja SYN paketa u jedinici vremena.

#### 2.2.1.2 Lažiranje IP adresa (engl. Spoofing)

Napadač prati IP adrese u IP paketima i predstavlja se kao drugi računar. DNS ne proverava odakle dolazi informacija, omogućavajući napadaču da izvrši napad lažiranjem. Napad lažiranjem se ostvaruje tako što napač DNS servisu daje pogrešnu informaciju (ime računara od poverenja). Zaštita od ovakvog tipa napada jeste sprečavanje rutiranja paketa sa adresama izvorišta za koje se zna da su neispravni.

#### 2.2.1.3 Njuškanje (engl. Sniffing)

Napadač presreće TCP/IP pakete koji prolaze kroz određeni računar, a zatim pregleda njihov sadržaj. Ukoliko se kroz mrežu prosleđuju nazaštićeni podaci, napadač sa lakoćom može doći do poverljivih podataka.

#### 2.2.1.4 Trojanski konj (engl. Trojan horse)

Predstavlja ilegalan segment koda podmetnut u kod nekog programa. Cilj trojanskog konja jeste promena funkcije ili ponašanja originalnog programa.

#### 2.2.1.5 Crv (engl. Worm)

Predstavljaju samostalne zlonamerne programe koji se šire sa jednog računara na drugi. Metod prenošenja je elektronska pošta i internet servisi. Crv ekspolatiše ranjivost žrtve, koristi metode prevare i obmane (društveni inženjering), primoravajući korisnika da ga pokrene. Posledica je degradiranje preformansi ili dodatne štete.

#### 2.2.1.6 Virusi (engl. Virus)

Virusi nisu samostalni programi. Predstavljaju fragmente koda koji se ubacuju u druge legitimne programe. Zahtevaju nosioca u vidu izvršne datoteke. Nakon pokretanja, virus ponekada inficira i druge izvršne datoteke na sistemu. Destruktivni su i teško se uklanjaju. Zaštita od ovakvog tipa napada jeste upotreba anti-virusnih programa i podizanje svesti korisnika o opasnosti na internetu.

#### 2.2.1.7 Klopka (engl. Trapdoor)

Autor programa slučajno ili namerno ostavlja prazna mesta u svom kodu (klopku). Ukoliko uljez sazna za ta mesta, može podmetnuti svoj kod i time ostvariti svoj cilj. Autor programa može napraviti izmenu dela koda tako da se izmena ne može jednostavno primetiti. Klopke se teško otkrivaju, jer je potrebno uraditi detaljnu analizu celokupnog koda sumnjivog programa.

#### 2.2.1.8 Prekoračenje bafera (engl. Buffer overflow)

Najčešći mrežni napad pri pokušaju neovlašćenog pristupanju sistema. Napadač koristi grešku u programu, neogovarajuću kontrolu razdvajanja steka, podataka i koda. Napadač šalje više ulaznih podataka nego što program očekuje, prepunjava se bafer sve dok ne dođe

do steka. Zatim pomoću važeće adrese u steku upisuje adresu svog koda, puni deo steka svojim kodom. Posledica je izvršvanje ilegalnog koda.

#### 2.2.1.9 Fišing napadi (engl. Phishing attacks)

Fišing predstavlja oblik sajber kriminala zanovanog na tehnikama socijalnog inženjeringa i tehnikama prevare korisnika izgledom stranica.
Fišing (engl. *Phishing*) ili veb spufing (engl. *Web Spoofing*) napadi predstavljaju pokušaj napadača da prevari korisnika, podmetanjem lažnih sajtova ili stranica za prijavljivanje, veoma sličnih ili istih kao originalni. Cilj ovog napada jeste prevara ili „pecanje“ korisnika da dobrovoljno unesu poverljive podatke (brojeve kreditnih kartica, korisnička imena i lozinke, lične podatke,itd). Na ovaj način napadač sa lakoćom prikuplja poverljive informacije korisnika.

Fišing napadi se mogu distribuirati kroz elektronsku poštu, promenama u hosts fajlu (engl. *host file*) korisnika, preko društevnih mreža, sve što je potrebno jeste da korisnik klikne na predloženu veb stranicu i unese tražene podatke. Za razliku od spam poruka (engl. *spam message*), fišing poruke dolaze od poznatih kompanija, pojedinaca kojima se veruje. Za uspešnost ovog napada ključna je informacija koja potvrđuje validnost poruke, dobar razlog koji će ubediti korisnika u neophodnost unosa korisničkih podataka.

**Najbolji način zaštite** od fišing napada jeste opreznost korisnika, provera izvora zahteva, uveriti se da li je implementiran sigurnosni protokol (HTTPS,SSL) i ukoliko nije, ne unositi poverljive podatke.

## 2.3 Peneteracione testiranje

Penetraciono testiranje je legalan i autorizovan pokušaj pronalaženja propusta u računarskim sistemima i njihovo iskorišćavanje, sa ciljem unapređivanja zaštite ovih sistema. Obuhvata kompletnu analizu sistema – tehnički propusti, ranjivosti, propusti u korišćenim protokolima, implementaciji sistema, upravljanju bezbednosne politike sistema itd.
Prema količini znanja koje ispitivač ima, penetracioni testovi se mogu podeliti na:

- Testiranje crne kutije
- Testiranje bele kutije
- Testiranje sive kutije

**Testiranje crne kutije** predstavlja slučaj u kojem ispitivač ništa ne zna o sistemu ili infrastrukturi koju napada.

**Testiranje bele kutije** predstavlja slučaj u kojem je ispitivač dobio sve informacije koje su mu potrebne za izvršavanje napada na sistem ili infrastrukturu.

**Testiranje sive kutije** predstavlja kombinaciju prethodna dva slučaja.
Preporučuje se da se koristi najgori mogući scenario upravo zbog nemogućnosti predviđanja količine znanja koje napadač ima. Testiranje se završava kada se pronađeni nedostaci pronađu, iskoriste u svrhe testiranja, dokumentuju, predlože mehanizmi njihovog otklanjanja, prikaže plan održavanja sistema zaštite. Na ovaj način se u realnim uslovima prikazuju i rešavaju sigurnosni problemi sistema ali se vodi računa i o prevenciji i sprečavanju budućih napada na sistem.

Proces penetracionog testiranja se obavlja u nekoliko faza:

1) **Izviđanje i skeniranje** (*Reconnaissance and Scanning*)
2) **Izvršavanje kriptoanalitičkog metoda** ( *Exploitation*)
3) **Održavanje kontrole i sakrivanje** (*Maintaining Access and Hiding*)
4) **Pravljenje izveštaja (***Report making***)**

Ove procese možemo nazvati metodologijom penetracionog testiranja. Da bi se penetracioni test uspešno izvršio potrebno je da se procesi izvršavaju datim redosledom.
Preskakanje bilo koje faze sa sigurnošću vodi do neuspeha, cikličnost tj ponovni prolazak kroz faze je prihvatljiv.

### 2.3.1 Izviđanje i skeniranje

Prvi i veoma važan proces u penetracionom testiranju. Izviđanje predstavlja detaljno prikupljanje i dokumentovanje podataka o meti – identifikovanje mehanizma zaštite, sakupljanje informacija sa društvenih mreža i web sajtova, prikupljanje informacija o serverima, analiza saobraćaja itd. Svaka informacija koja je dostupna može biti ključna i upotrebljena sa ciljem pronalaženja propusta u sistemu. Ponekad se i na izgled nebitne informacije koje sistem daje pokažu kao ključni element u penetracionom testiranju.
Izviđanje se može podeliti na:

- Aktivno
- Pasivno

**Aktivno izviđanje** predstavlja direktnu komunikaciju sa metom, gde se IP adresa napadača može otkriti. Moguće je i komunicirati sa metom bez otkrivanja IP, korišćenjem *stealth* alata ali su naravno mogućnosti skeniranja ograničene.

**Pasivno izviđanje** se bavi prikupljanjem dostupnih informacija o meti.
Sastavni deo procesa izviđanja je skeniranje.
Postoji više različitih nivoa skeniranja:

- Horizontalno
- Vertikalno
- Dubinsko

**Horizontalno skeniranje** predstavlja proces u kome se ispituje koji se mrežni uređaji nalaze u računarskoj mreži, ispituje se i topologija računarske mreže.
**Vertikalno skeniranje** predstavlja proces u kome se ispituju otvoreni portovi i mrežni servisi na njima.
**Dubinsko skeniranje** predstavlja proces u kome napadač dolazi do veoma vrednih informacija kao što su informacije o sistemskom i korisničkom softveru.

### 2.3.2 Izvršavanje kriptoanalitičkog metoda

Kada isiptivač poseduje potrebne informacije o sistemu koji testira, dolazi do druge faze u penetracionom testiranju – pravljenje i izvršavanje kriptoanalitičkog metoda (exploit-a).

Korišćenjem alata za penetraciono testiranje, mnoštvo različitih tehnika i pisanjem skripti ispitivač pravi specijalno dizajniran exploit za pronađen propust u sistemu, imajući u cilju da iskoristi pronađen propust u svoju korist.
Cilj izvršavanje exploit-a jeste dobijanje privilegija u administratora sistema.

#### 2.3.2.1 Razlike izmedju pojma exploit-a i payload-a

**Eksploit (engl. *Exploit*)** predstavlja napad na određeni deo računarskog sistema, koristeći propuste u sistemu, sa ciljem „probijanja“ zaštitnih mehanizama bez aktiviranja “alarma” odnosno bez znanja administratora sistema.
Alarm može predstavljati IDN sistem (*Intrusion Detection System*) koji ima ulogu da administratora sistema obavesti o detektovanom napadu, nedozvoljenom pokušaju autentifikacije, autorizacije ili eskalacije privilegija.
**Pejload (engl. *Payload*)** predstavlja mehanizam kontrole već “probijenog” sistema koji ispitivač koristi kako bi mogao da uspešno upravlja sistemom ili izvede željene akcije i promene na sistemu.

### 2.3.3 Održavanje kontrole i sakrivanje

U trećem koraku penetracionog testiranja akcenat je na pravljenju i aktiviranju payload-a. Pomoću njega ispitivač dobija kompletnu kontrolu nad sistemom. Mana većine payload-a je ograničeno trajanje, zbog čega napadači koriste privilegije adiministratora kako bi instalirali maliciozni softver, softver za sprečavanje detektovanja instaliranog malicioznog softvera i akiviraju alate za brisanje log fajlova i na ovaj način se “kriju” od administratora.
Upravo ovaj korak razlikuje napadača i penetracionog testera. Osoba koja testira sistem ne zloupotrebljava privilegije administratora, već samo dokumentuje i dokazuje pravom administratoru sistema neophodnost promene bezbednosne politike i potrebu za unapređenjem zaštite sistema.

### 2.3.4 Pravljenje izveštaja

Upravo se u poslednjem koraku ispitivač bavi dokumentovanjem svake faze penetracionog testiranja Detaljno se opisuje kako su testovi izvođeni, šta je urađeno u svakoj fazi testiranja, kao i rezultat svake faze. Izveštaj se deli u dva dela – deo sa detaljnim opisima kriptoanalitičkih metoda i deo bez tehničkih opisa. Veoma je bitno da je izveštaj razumljiv i osobi koja nema tehnička znanja.

## 2.4 Okruženje za penetraciono testiranje – Kali Linux

Kali Linux je naslednik popularnog Backtrack Linux-a, sa preko 300 programa za penetraciono testiranje i Linux operativnim sistemom, predstavlja jedinstveno integrisano rešenje. Osnovna namena ovog okruženja jeste testiranje sistema zaštite, monitoring, pronalaženje propusta i njihovo otklanjanje, rad na prevenciji i unapređenju sigurnosnih politika.
Alati se mogu podeliti u više kategorija:

- Alati za prikupljanje informacija (engl. *Information Gathering*)
- Alati za analizu propusta (engl. *Vulnerability Analysis*)
- Exploit alati (engl. *Exploitation Tools*)

- Alati za testiranje bežičnih mreža (engl. *Wireless Attacks*)
- Forenzički alati (engl. *Forensics Tools*)
- Alati za testiranje web aplikacija (engl. *Web Applications*)
- Stres testiranje (engl. *Stress Testing*)
- Alati za prisluškivanje i obmanu (engl. *Sniffing and Spoofing*)
- Alati za testiranje lozinki (engl. *Password Attacks*)
- Alati za održavanje pristupa (engl. *Maintaining Access*)
- Alati za testiranje hardvera (engl. *Hardware Hacking*)
- Alati za reverzno inženjerstvo (engl. *Reverse Engineering*)
- Alati za pravljenje izveštaja (engl. *Reporting Tools*)

Tvorac Kali Linux-a je *Offensive security*[1], čija je vizija da se bezbednosti sistema pristupi na potpuno drugačiji način. Potrebno je testirati sopsvene mehanizme zaštite iz uloge napadača. Kali Linux je *open source* operativni sistem, zasnovan na Debian distribuciji. Prva verzija Kali Linux-a je predstavljena 13.03.2013. na „*Black Hat*“ konferenciji u Amsterdamu, druga verzija se pojavljuje 11.08.2015. pod nazivom Kali Sana, dok Rolling distribucija 21.1.2016. predstavlja aktuelnu verziju Kali Linux-a.
Kali Rolling distribucija obogaćena je novim alatkama i novim sistemom ažuriranja softvera. Rolling distribucija koristi Debian testing distribuciju, omogućavajući konstantno unapređivanje softvera novim verzijama i upotrebu najnovijih funkcionalnosti.

## 2.5 Open Web Application Security Project - OWASP

**OWASP** je neprofitna organizacija i otvorena zajednica koja nastoji da osigura bezbednost aplikacija bez sumnje u njihov integritet.
Organizacija je osnovana su u Sjedinjenim Američkim Državama 2004-te godine.
Zaslužni su za održavanje i implementaciju zaštitnih mehanizama kao i za postojanje velikog foruma za pomoć pri zaštiti internet aplikacija.
Njihove ključne vrednosti su: otvorenost, inovacije, dostupnost i integritet.

### 2.5.1 Najzastupljeniji napadi prema OWASP statistici

1) **Napad ubacivanja** (engl. *Injection*)

**Ko može biti napadač?**
Treća lica, korisnici sistema i administratori.
Razmatra se da svako ko može da šalje neproverene podatke sistemu.
Napadač šalje jednostavne tekstualne napade i ubacuje kod u nezaštićeni sistem i menja tok izvršavanja. To se najčešće dešava u slučajevima zastarelih kodova npr u SQL-u, LDAP[2]-u, Xpath[3]-u ili NoSQL[4]-u.

[1] Offensive security predstavlja tim IT stručnjaka za bezbednost, čija je glavna ekspertiza testiranje sistema.
[2] Lightweight Directory Access Protocol predstavlja standardni aplikacioni protokol za pristupanje i održavanje informacionih servisa distribuiranih direktorijuma.
[3] Xpath je sintaksa za definisanje delova XML dokumenta. Koristi "path expression" princip za navigaciju kroz XML document.
[4] NoSQL podrazumeva širok dijapazon različitih tehnologija baza podataka.Veoma korisni za situacije u kojima se radi sa velikim brojem struktuiranih, polu-struktuiranih i nestruktuiranih podataka.

**Posledice napada**
Može da nastupi gubitak ili korupcija podataka ili nemogućnost pristupa podacima. Ponekad se može desiti potpuno preuzimanje *host*-a. Teške posledice mogu biti u poslovnom okruženju gde se čak i reputacija može ugroziti.

**Da li je aplikacija ranjiva?**
Najbolji način da se proveri ranjivost je da se potvrdi da li kod jasno odvaja neproverene podatke od komande ili upita.Veoma su korisne alatke za analizu kodova.
Stručnjaci veoma brzo mogu da naprave napade kojima proveravaju integritet kodova. Ponekad se mogu koristiti i automatizovani skeneri, koji pokušavaju da pronađu propust, ali ne mogu da daju potpunu sliku u svakom slučaju.

**Kako da se sprečava napad ubacivanja?**
Najbolji način je da se koristi bezbedan interfejs aplikacije koji podrazumeva izbegavanje korišćenja *interpreter*[5]- a. Ako ovakav interfejs nije dostupan treba pažljivo ograničiti korišćenje specijalnih karaktera. Za ovu svrhu poželjno je koristiti sintaksu za ograničavanje. OWASP poseduje listu velikog broja takvih sintaksi.
Poželjno je napraviti listu dozvoljenih unosa kako bismo ograničili unos nedozvoljenih podataka.

2) **Napad kompromitovanja autentifikacije i menadžmenta sesije**
*(*engl. *Broken Authentication and Session Management)*

**Ko može biti napadac?**
Treća lica i korisnici sistema.
Napadač koristi propuste u autentifikaciji ili u funkcijama menadžera sesija npr. u nalozima, šiframa, ID sesija, u cilju preuzimanja identiteta korisnika. Programeri često prave sopstvene šeme autentifikacije, što može biti veoma zahtevno. Iz tog razloga često dolazi do pojave grešaka u šemama, pogotovo u delu kao što je odjavljivanje (*logout*).

**Posledice napada**
Može se desiti da dođe do napada na neke ili čak na sve naloge. Posle uspešnog napada, napadač može raditi sve što je dozvoljeno i samom korisniku. Nalozi sa dodatnim privilegijama se često napadaju. U poslovnim okruženjima potrebno je posebno razmotriti uticaj na poslovanje i odavanje tajni javnosti.

**Da li je aplikacija ranjiva?**
Potrebno je proveriti da li su zaštićeni poverljivi podaci korisnika (npr korisničko ime i lozinka), kao i identifikatori sesija.

**Kako se sprečava ovaj napad?**
Najbolje je načiniti dostupnim programerima set dobrih kontrola za autentifikaciju i menadžment sesija. Takođe treba uložiti veće napore za izbegavanje XSS propusta.

[5] Interpreter predstavlja program koji izvršava instrukcije (kod) napisan u programskom jeziku višeg nivoa.

### 3) Cross-site scripting (XSS)

**Ko može biti napadač?**
Treća lica, korisnici ili čak administratori.
Svako ko može da šalje neproverene podatke sistemu.
Napadač šalje tekstualne skripte u cilju eksploatacije interpretera u internet pretraživaču. Skoro svaki podatak može da se koristi za napad uključujući podatke iz interne baze podataka. XSS je jedan od najzastupljenijih napada. Ovi propusti se dešavaju kada aplikacija ubaci podatke koje šalje korisnik, u stranicu poslatu pretraživaču bez pravilne validacije.

**Posledice napada**
Može doći do krađe korisničkih sesija, narušavanje izgleda web sajta, ubacivanje spoljnih podataka, preusmeravanje korisnika itd.

**Postoje tri vrste XSS napada:**
Svaka od nabrojanih vrsta XSS napada se može pojaviti i na strani klijenta i na strani servera.

**1) Trajni** (engl. *Persistent*) - skripta se trajno ubacuje u ciljanoj aplikaciji
**2) Reflektovani** (engl. *Reflected*) - napadač postavlja skriptu na server i izvršavanje se dešava na korisničkoj strani.
**3)DOM-zanovani** (engl. *DOM based*) - skripte korisnika u aplikaciji se upisuju u DOM [6]. Aplikacija zatim čita podatke iz DOM-a i ispisuje u pretraživaču.

**Da li je aplikacija ranjiva?**
Potrebno je da se proveri da li su zabranjeni svi upisi korisnika ili da su određeni upisi korisnika bezbedni. Automatizovane alatke mogu pronaći XSS propuste, ali ih je najbolje koristiti u kombinaciji sa ručnom proverom koda.

**Kako se sprečava XSS napad?**
Potrebno je sprečiti nedozvoljene korisničke unose**,** napraviti dozvoljenu listu korisničnih unosa**,** razmotriti korišćenje biblioteka koje automatski vrše saniranje npr. AntiSamy [7] ili Java HTML**[8],** razmotriti korišćenje Content Security Policy (CSP)[9].

### 4) Napad na nezaštićene direktne reference objekata
*(*engl. *Insecure Direct Object References)*

**Ko može biti napadač?**
Razmotriti sve tipove korisnika sistema. Da li imaju parcijalni pristup nekim od tipova podataka na sistemu? Napadač, koji je korisnik, menja vrednost koja direktno utiče na objekat u sistemu za koji korisnik nema autorizaciju. Aplikacije često koriste ime ili vrednost objekta kada generišu web stranice. Aplikacije često ne proveravaju da li je korisnik autorizovan za pristup ciljanom objektu.

---

[6] DOM (engl. *Document Object Model*) predstavlja programerski API za HTML i XML dokumenta. Definiše logičku strukturu dokumenata, način na koji se dokumentu pristupa i manipuliše.
[7] AntiSamy je biblioteka koja omogućava filtriranje HTML-a, CSS-a i JavaScript-a onemogućavajući napadaču izvršavanje XSS napada.
[8] Java HTML je biblioteka koja omogućava filtriranje HTML koda.
[9] Content Security Policy daje instrukcije internet pretraživacu sa kojih lokacija i/ili koje vrste resursa su dozvoljene za učitavanje.

**Posledice napada**
Ovakvi propusti mogu da kompromituju podatke koji se oslanjaju na napadnuti parametar. Osim ako objekat referenciranja nije nepredvidljiv, napadaču je jednostavno da pristupi svim dostupnim podacima određenog tipa.

**Da li je aplikacija ranjiva?**
Najbolji način da se sazna da li je aplikacija ranjiva je da se proveri da li su svi referencirani objekti propisno zaštićeni.
Razmotriti da li je korisnik autorizovan da pristupa podacima u slučaju direktnih referenci kod podataka sa ograničenim pristupom. U slučaju indirektnog referenciranja podataka, proveriti da li direktna referenca ne ograničava pristup trenutnom korisniku.

**Kako se sprečava Insecure Direct Object References napad?**
Koristiti sesijski indirektne reference objekata za svakog korisnika. Ovo sprečava napadaču da pristupa nedozvoljenim resursima. Takođe proveriti svako korišćenje direktne reference od neverifikovanog izvora. Takav izvor mora da uključuje kontrolu pristupa da proverava li je korisnik autorizovan da zahteva objekat.

5) **Loše podešavanje bezbednose konfiguracije**
*(*engl. *Security Misconfiguration)*

**Ko može biti napadač?**
Treća lica i korisnici sistema.
Napad se sastoji od nedozvoljenog pristupa inkorporisanim nalozima, nekorišćenim stranicama, nezaštićenim fajlovima i direktorijumima od strane napadača. Na svakom nivou aplikacije se mogu desiti ovakvi propusti, uključujući platformu,bazu podataka i kod. Programeri i administratori sistema moraju sarađivati u cilju osiguranja bezbednosti celokupnog sistema. U ovome od pomoći mogu biti skeneri propusta.

**Posledice napada**
Može doći do kompromitovanja celokupnog sistema bez znanja administratora.
Može doći do krađe ili izmene svih podataka.

**Da li je aplikacija ranjiva?**
Proveriti da li aplikaciji nedostaje zaštita na bilo kom nivou. Da li je verzija programa najnovija? Ovo podrazumeva operativni sistem, server i biblioteke kodova. Da li su uključene nepotrebne opcije? Ovo uključuje portove, servise, stranice, naloge i privilegije.
Da li su inkorporisani nalozi i njihove lozinke još u upotrebi ili nisu promenjeni? Da li poruke o greškama odaju informacije o aplikaciji? Da li su sigurnosne opcije u razvojnom okruženju pravilno podešene?

**Kako se sprečava Security Misconfiguration napad?**
Potrebno je napraviti proces koji čini brzim i jednostavnim postavljanje drugog sistema koji je propisno obezbeđen. Ugrađivati najnovije verzije programa i biblioteka kodova u kratkom roku. Napraviti dobro zaštićenu arhitekturu aplikacije, koja pruža odvojenost komponenti. Razmotriti skeniranje i ručne provere za nove verzije programa u cilju sprečavanja budućih napada.

6) **Izlaganje poverljivih podataka**
*(*engl. *Sensitive data exposure)*

Najveći propust je izbegavanje šifrovanja osetljivih podataka. Kada se koristi kriptografija, problemi su: loše generisani ključevi, loši algoritmi, pogotovo loše tehnike heširanja lozinki. Slabosti u pretraživaču su lake za otkrivanje, ali se teško vrši napad na njih u slučaju velikih aplikacija. Napadač teško može otkriti koje su slabosti na strani servera zbog ograničenog pristupa i takvi napadi su teški za implementaciju.

**Ko može biti napadač?**
Napadač može biti svako ko ima pristup osetljivim podacima i svim kopijama tih podataka. Razmotriti sve spoljne i unutrašnje pretnje. Napadači često ne napadaju šifrovane podatke direktno, već npr. kradu ključeve, izvode „čovek u sredini" napade, ili kradu podatke iz tekstualnih fajlova.

**Posledice napada**
Posledica se sastoji u tome što dolazi do kompromitovanja poverljivih podataka, što može obuhvatiti osetljive podatke kao npr. zdravstveni podaci, brojevi kreditnih kartica i drugi lični podaci.

**Da li je aplikacija ranjiva?**
Prvo je potrebno utvrditi koju su podaci veoma osetljivi. Da li su ti podaci sačuvani u tekstualnim fajlovima duže vreme? Da li se vrši njihov prenos u tekstualnim fajlovima interno i eksterno? Da li se koriste zastareli ili loši kriptografski algoritmi? Da li su loše generisani kriptografski ključevi?

**Kako se sprečava Sensitive data exposure napad?**
Proveriti da li su dobro šifrovani svi poverljivi podaci. Ne skladištiti osetljive podatke bespotrebno. Koristiti dobar standard za algoritme i jake ključeve. Osigurati da postoji dobar menadžment ključeva. Osigurati da su lozinke skladištene sa algoritmima koji su posebno dizajnirani za lozinke. Onemogućiti keširanje stranica sa osetljivim podacima.

7) **Napad na privilegovane funkcije sa nedostatkom kontrole pristupa**
*(*engl. *Missing Function Level Access Control)*

**Ko može biti napadač?**
Treća lica ili autorizovani korisnici.
Napadač menja URL ili parametar za pristup privilegovanim funkcionalnostima.

**Posledice napada**
Korišćenje funkcija namenjenih samo za privilegovane korisnike, obično administratore sistema.
"Curenje" poverljivih poslovnih informacija koje se obrađuju.

**Da li je aplikacija ranjiva?**
Ukoliko postoji mogućnost da neautorizovani korisnik pristupi funkcionalnostima ili stranicama namenjenim autorizovanim korisnicima.
Ispitati svaku funkcionalnost pojedinačno, proveriti da li nedostaje navigacija
za privilegovane funkcionalnosti, autentifikacija i autorizacija od strane server i da li se serverska strana oslanja samo na informaciju dostavljenu od napadača.

Koristeći proxy pokrenuti aplikaciju kao administrator,a zatim stranice za privilegovane korisnike ponovo posetiti. Ukoliko su odgovori servera slični, postoji izloženost ovom napadu.
Potrebno je detaljno proveriti kod modula za kontrolu pristupa, pokrenuti neku od privilegovanih funkcija a zatim analizirati autorizacioni modul i pronaći delove u kojima je on izostavljen.

**Kako se sprečava ovaj napad?**
Autorizacioni modul mora biti konzistentan, prilagodljiv i lak za izmenu.
Podrazumevana podešavanja moraju zabraniti sve funkcionalnosti, zahtevajući dodatne parametre koje korisnik ili treća strana moraju uneti kako bi dobili pristup određenoj funkcionalnosti.
Nije dovoljno samo onemogućiti pristup privilegovanim funkcijama na prezentacionom nivou, već je potrebno i omogućiti proveru u kontroleru i biznis logici.

8) **Pravljenje malicioznih stranica sa mogućnošću falsifikovanja zahteva** (engl. *Cross-site request forgery*)

Ovaj napad koristi to što većina veb aplikacija dozvoljava napadačima da predvide detalje određene aktivnosti. S obzirom da pretraživaci šalju korisničke podatke automatski kao sesijske kolačiće, napadači mogu da naprave maliciozne stranice koje generišu falsifikovane zahteve. Ovakvi zahtevi ne mogu se razlikovati od pravih. Detekcija ovakvog napada je uglavnom jednostavna putem analize koda.

**Ko može biti napadač?**
Razmotriti ko sve može da učita sadržaj u pretraživač korisnika, što korisnika prisiljava da pošalje zahtev aplikaciji. Napadač kreira lažirani HTTP zahtev i prevari žrtvu da pošalje takav zahtev kroz tag slike,XSS itd.

**Posledice napada**
Napadač može da prevari žrtvu da uradi bilo koju od aktivnosti za koju je autorizovana, što može ostaviti ozbiljne posledice na sistem.

**Da li je aplikacija ranjiva?**
Proveriti da li bilo kom linku i formi nedostaje nepredvidivi cros-site request forgery token. Takođe treba osigurati transakcije sa više koraka. Napadač lako može da lažira seriju zahteva korišćenjem više tagova ili javascript.

**Kako se sprečava cross-site request forgery napad?**
Prevencija se najčešće vrši ubacivanjem nepredvidivog tokena u svaki HTTP zahtev. Takvi tokeni moraju da budu jedinstveni za svakog korisnika. Poželjno je takve tokene ubaciti u skriveno polje. Ovo sprečava inkluziju tokena u URL. Alternativno, može se tražiti od korisnika da dokažu da žele da izvrše određenu aktivnost kroz reautentifikaciju, ili npr. CAPTCHA test.

9) **Korišćenje komponenata sa poznatim propustima**
(engl. *Using Components with Known Vulnerabilities*)

**Ko može biti napadač?**
Treća lica ili korisnici sistema. Komponente sa propustima (biblioteke aplikacije, okruženja itd) mogu biti pronađene i napadnute od strane automatizovanih alata napadača. Napadač prilagođava podešavanja *exploit*-a prema potrebi i izvršava napad. Propusti mogu biti iskorišćeni kako bi se uspešno izvršili i druge vrste napada (*Injection, Broken Access Control, XSS*).

**Posledice napada**
Kompromitovanje poverljivih podataka, preuzimanje kontrole nad sistemom.

**Da li je aplikacija ranjiva?**

Skoro svaka aplikacija ima propuste upravo zbog toga što razvojni timovi ne vode računa o verzijama i ažuriranosti komponenata i biblioteka.

**Kako se sprečava cross-site request forgery napad?**

Potrebno je često proveravati da li je za određenu komponentu pronađen propust. Postoje baze pronađenih propusta (CVE, NVD) koje su relevantne i dostupne svima.
Neophodno je redovno ažurirati softver, identifikovati koje komponente, verzije komponenata i zavisnosti između komponenata postoje. Obezbediti monitoring bezbednosti ovih komponenata, uspostaviti bezbednosnu politiku i omogućiti bezbednosne module koji će isključivati nekorišćene funkcionalnosti i obezbediti slabe delove komponenti.

10) **Neproverena preusmeravanja i prosleđivanja**
*(*engl. *Unvalidated Redirects and Forwards)*

**Ko može biti napadač?**
Svako ko može da prevari korisnika da pošalje zahtev ka web sajt-u. Napadač menja URL od stranice za preusmeravanje kako bi korisnike preusmerio na maliciozni ili *phishing* sajt. Vrši izmenu parametara stranice za prosleđivanje ka drugoj stranici u okviru istog sajta, uspešno prolazi proveru kontrole pristupa i izvršava eskalaciju privilegija [10] u administratora sistema.

**Posledice napada**
Gubitak poverenja korisnika u sistem, zbog nasilnog preusmeravanja na maliciozni ili *phishing* sajt od napadača.

**Da li je aplikacija ranjiva?**
Proveriti kod za preusmeravanje i prosleđivanje na druge stranice unutar web sajta. Testirati da li se svako preusmeravanje i prosleđivanje vrši po parametrima koje je zadao administrator.

[10] Eksalacija privilega predstavlja korišćenje propusta u programiranju i dizajnu sistema zaobilazeći autorizacione provere, omogućavajući korisniku sistema veće privilegije, sa ciljem dobijanja privilegija administratora.

**Kako se sprečava cross-site request forgery napad?**

Izbegavati korišćenje preusmeravanja i prosleđivanja na web sajtu. Ukoliko se koristi, izbegavati korišćenje parametara korisnika u računanju destinacije. Proveriti da li je korisnik autorizovan za preusmeravanje, upotrebiti mapirane vrednosti a ne kompletan ili delimičan URL jer će server prevesti mapiranu vrednost u URL.

# 3 Teorijske osnove istraživanja

## 3.1 Uvod u bežične mreže

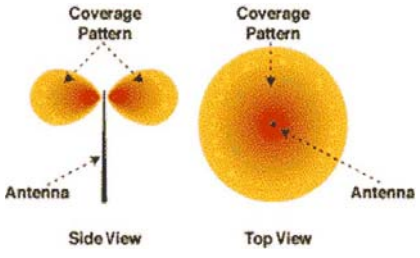
U standardima bežičnih računarskih mreža definisani su različiti elementi sigurnosti. Neupotrebljenost određenih elemenata, nepravilna konfiguracija i upotreba dovode do sigurnosnih propusta. Nedostaci u okviru samog standarda, koji nisu pravovremeno uočeni, mogu znatno uticati na nivo sigurnosti bežične računarske mreže.
Propuste u standardu predstavljaju:

- propusti pri proveri identiteta korisnika mreže
- propusti pri šifrovanju između pristupne tačke i korisnika

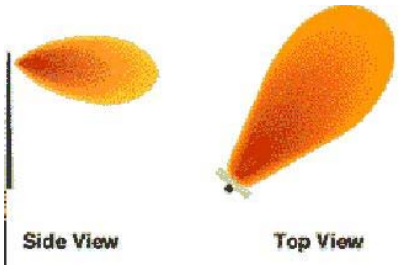
IEEE je ostavio otvorena pitanja o sigurnosnim elementima – raspodeli ključeva i robusnom načinu provere identiteta korisnika.
Iako se teži ka usavršavanju standarda, standardi ne uspevaju da zadovolje sve aspekte piramide sigurnosti (pouzdanu proveru identiteta korisnika, zaštitu privatnosti, autorizaciju korisnika). Upravo je cilj napadača penetracija u jednu od strana piramide sigurnosti (poverljivost, integritet, dostupnost).

## 3.2 Fizičko ograničavanje propagacije signala

Prilikom projektovanja bežične mreže, neophodno je pregledati lokaciju na kojoj je potrebno postaviti mrežnu opremu, odrediti optimalnu vrstu antena i dovoljnu snagu signala. U upotrebi su najzastupljenije omnidirekciona, panel(ravna) i direkciona(usmerena) antena.
**Omnidirekciona antena** ima izotropni oblik zračenja u datoj ravni, usmeren u ortogonalnoj ravni. Kako bi signal stigao do korisnika, antena emituje signal višesmerno, podsećajući na kružno talasanje u vodi. Snaga se zrači jednako u svim pravcima horizontalne ravni. U slučaju velikog broja korisnika može doći do interferencije signala, upravo zbog signala koji promaše željenog korisnika, a koji zatim postaju smetnja.
**Direkciona(usmerena) antena**
Zračenje signala se koncentriše u određenom smeru ili ugaonoj oblasti. Koriste se za rastojanja od tačke do tačke, ponekad i za *multipoint* sisteme. Upotreba u klijentskom režimu je česta. Zna se gde je pristupna tačka i lokacije baze, pa je samo potrebno usmeriti antenu prema bazi, kako bi se dobio što bolji i kvalitetniji signal.
**Panel (ravna) antena**
Spadaju u grupu direkcionih antena. Koriste se u unutrašnjoj i spoljašnjoj sredini, mogu se koristiti za mrežnu arhitekturu tipa od tačke do tačke kao i za *multipoint* sisteme.




*Slika 2- Dijagram zračenja omnidirekcione antene*




*Slika 3- Dijagram zračenja direkcione antene*

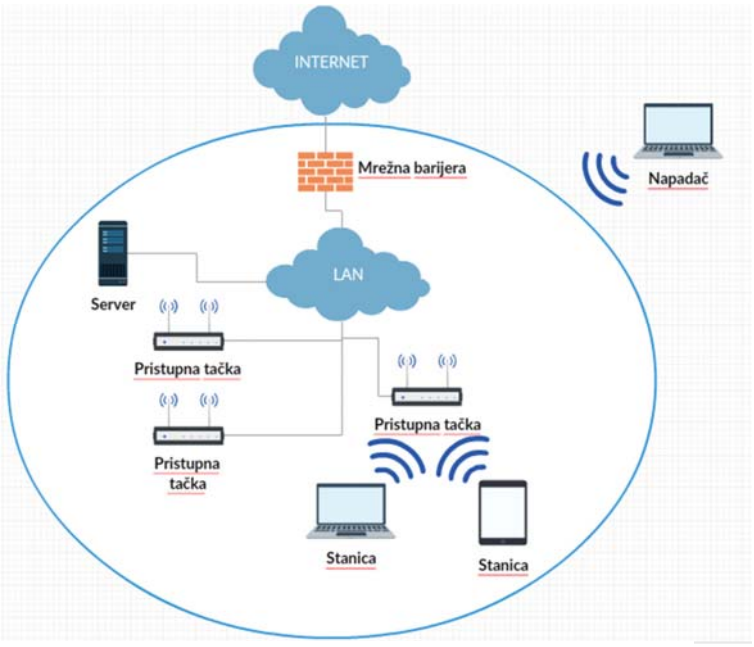
Nelicencirane frekvencije od 2.4 GHz, koje koriste bežične mreže po standardima 802.11b i 802.11g mogu dovesti do interferencije signala sa drugim uređajima (bežičnim telefonima, uređajima koji rade na frekvenciji od 2,4GHz) i nastanka uskraćivanje usluge DoS. Napadač može imati znatno bolju opremu, koja znatno može proširiti domet mreže, otvarajući sebi mogućnost za izvršenje mnogih napada.
Kao preventivne mere, mogu se navesti tehnike za ograničavanje propagacije signala. Koristeći antene sa usmeravanjem i neke od tehnika interferencije, koje znatno utiču na signal i čine ga nerazumljivim u pojedinim područjima, ograničava se propagacija signala.

## 3.3 Identifikator skupa usluga

Standard bežičnih mreža IEEE 802.11 definiše drugi način ograničavanja pristupa, što jeste identifikator skupa usluga engl. SSID (Service Set Identifier).
Identifikator skupa usluga predstavlja ime mreže koju pokriva jedna ili više pristupnih tačaka. Postoje dva načina upotrebe identifikatora skupa resursa:

1) SSID se koristi kao identifikator mreže. Pristupna tačka šalje SSID u signalnom upravljačkom okviru. Pomoću njega klijent može odlučiti kojoj će se mreži pridružiti.
2) SSID se koristi kao sigurnosni faktor. Pristupne tačke se mogu konfigurisati na način da ne šalju SSID kontrolnog okvira. U ovom slučaju klijent mora imati isti SSID kao i mreža kojoj pristupa. Ukoliko ga ne poseduje, stanica odbacuje sve kontrolne okvire i postupak pridruživanja je onemogućen.

Propust u ovakvom načinu kontrole pristupa ogleda se u tome da se svi kontrolni okviri ne šalju u šifrovanom obliku. Kontrolni okviri se šalju od strane pristupnih tačaka, prilikom komunikacije sa stanicama. Moguće je izvršiti napad osluškivanja saobraćaja, gde napadač sa lakoćom može uhvatiti kontrolne okvire, saznati SSID mreže i neovlašćeno pristupiti mreži (“Napad sa parkirališta”). Mehanizam zaštite zasnovan na ograničenju da je dozvoljeno da mreži pristupaju samo stanice čije MAC adrese su zabeležene u evidenciji bazne stanice se pokazao neuspešnim, upravo zbog toga što je moguće lažirati MAC adresu mrežnog adaptera.




*Slika 4- " Napad sa parkirališta"*

## 3.4 Povezivanje stanice sa pristupnom tačkom

Kako bi se stanica uspešno povezala na postojeću pristupnu tačku, potrebno je dobiti informaciju o sinhronizaciji pristupne tačke.
Ova informacija se može dobiti na dva načina:

1) **Pasivno skeniranje**
   Stanica čeka da primi *beacon* okvir od strane pristupne tačke. Pristupna tačka šalje *beacon* okvir periodično, sa svim informacijama o sinhronizaciji.
2) **Aktivno skeniranje**
   Stanica pokušava da pronađe pristupnu tačku, tako što emituje *probe request* okvire i čeka *probe response* okvir od pristupne tačke.

Pre nego što stanica postane član mreže, neophodno je da uspešno prođe proveru identiteta.
Postoje dva tipa provere identiteta:

1) **Provera identiteta otvorenog sistema (*Open System Authentication*)**
   Stanica šalje zahtev za autentifikaciju, koji sadrži ID stanice, što je uglavnom MAC adresa stanice. Pristupna tačka šalje odgovor na autentifikaciju koji sadrži poruku o uspešnosti ili neuspešnosti autentifikacije. Ovakav sistem omogućava pristup mreži svakome ko zatraži.

2) **Provera identiteta zasnovana na deljenoj tajni (*Shared Key Authentication*)**
   Stanica koristi WEP protokol kako bi se povezala sa stanicom. Ovakav sistem podrazumeva da obe strane poseduju isti deljeni ključ. Pristupna tačka šalje izazov stanici, zatim stanica šifruje izazov deljenim ključem i vraća šifrat pristupnoj tački. Pristupna tačka dešifruje primljenu poruku svojim deljenim ključem. Ukoliko pristupna tačka dobije isti tekst koji je poslala stanici, provera identiteta se smatra uspešnom.

   Nakon završavanja procesa provere identiteta, započinje se proces asocijacije, što predstavlja razmenu informacija o mogućnostima stanice i pristupne tačke. Asocijacija omogućava pristupnoj tački da zabeleži svaku stanicu, tako da se okviri mogu pravilno proslediti. Stanica može da izvrši asocijaciju sa samo jednom pristupnom tačkom u određenom trenutku. Stanica šalje zahtev za asocijaciju pristupnoj tački. Pristupna tačka šalje odgovor na asocijaciju koji sadrži informaciju o statusu asocijacije i ID asocijacije, ukoliko je asocijacija uspešna. ID asocijacije se koristi za identifikaciju stanice, za prosleđivanje baferovanih okvira ukoliko je omogućen režim čuvanja energije. U slučaju neuspešne asocijacije zahtev asocijacije sadrži samo status asocijacije i procedura se završava. Nakon uspešnog procesa asocijacije, transfer podataka može da započne.

## 3.5 Standardi bežičnih mreža

Institut inženjera elektrotehnike i elektronike engl. IEEE (*Institute of Electrical and Electronics Engineers*) je najveća tehnička neprofitna organizacija koja je posvećena razvoju različitih tehnologija u oblasti inženjerstva, kompjuterske tehnike i informacionih tehnologija.
Standard IEEE 802.11 spada u porodicu srodnih 802 standarda, koji se bave razvojem lokalnih (LAN) i gradskih (MAN) računarskih mreža. Postoji više standarda u okviru 802.11 standarda, od kojih su osnovni: IEEE 802.11a, 802.11b, 802.11g, 802.11n.

Razlike između ovih standarda ogledaju se u brzini prenosa podataka i frekvenciji na kojoj rade. Frekvencija na kojoj se komunikacija obavlja je takozvani ISM (*Industrial*, *Scientific*, *Medical*) opseg frekvencija.
ISM sadrži tri opsega frekvencija: 902 – 928 MHz, 2400 – 2483,5 MHz, 5728 – 5750 MHz**.** Najčešće korišćeni opseg je 2400 – 2483,5 MHz.

## 3.6 Standard bežičnih mreža IEEE 802.11

Standard bežičnih mreža IEEE 802.11 podržava fiksirane, mobilne i portabilne stanice. Mobilne stanice pristupaju lokalnoj mreži dok su u pokretu. Portabilne stanice mogu menjati svoj položaj ali pristupaju lokalnoj mreži stacionarno dok se nalaze na jednom mestu.

Razlika između tradicionalnih lokalnih računarskih mreža i bežičnih lokalnih računarskih mreža (*WLAN*) je u tome što kod bežičnih lokalnih računarskih mreža pretpostavljamo da adresa na koju dostavljamo poruku ne predstavlja fizičku lokaciju koja se adresira. Kod bežičnih lokalnih računarskih mreža uređaj koji se adresira predstavlja stanicu (*Station – STA*). Termin stanica predstavlja krajnje odredište poruke.

**BSS** (*Basic Service Set*) predstavlja osnovu 802.11 bežičnih lokalnih mreže. Može se predstaviti kao područje u okviru koga stanice mogu komunicirati. Drugi naziv za ovo područje je BSA (*Basic Service Area*). Ukoliko stanica napusti ovo područje više nije u mogućnosti da komunicira sa drugim stanicama koje se nalaze u BSA.

### 3.6.1 Infrastrukturni režim povezivanja BSS (Basic Service Set)

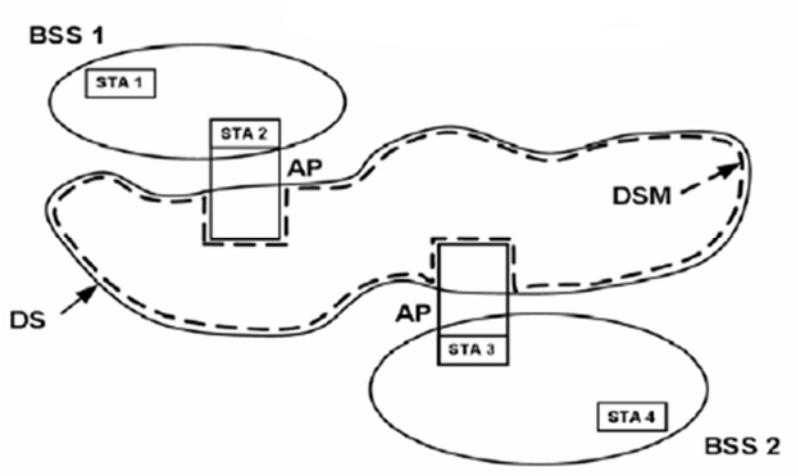
Infrastrukturni režim povezivanja sadrži pristupnu tačku i stanice koje ne komuniciraju direktno već preko pristupne tačke. Kako bi stanica uspešno pristupupila BSS-u vrši se procedura za sinhronizaciju definisana u 802.11 standardu. Stanica započinje transmisiju *beacon* frejmova i vrši proceduru za održavanje sinhonizacije. Nakon toga, stanica postaje član mreže.

### 3.6.2 Nezavisni način povezivanja IBSS (Independent Basic Service Set)

Nezavisni način povezivanja predstavlja najjednostavniji način povezivanja, koji sadrži minimum dve stanice. Stanice komuniciraju direktno, što znači da ne postoji pristupna tačka. Mreža postoji sve dok postoji potreba za komunikacijom, ovakav tip mreže se smatra *ad hoc* mrežom.

### 3.6.3 Bežični distributivni sistemi

Nasuprot postojanju koncepta odvojenih BSS-ova koji imaju ograničen opseg komunikacije, distributivni sistemi omogućavaju povezivanje dva BSS-a što se naziva ESS (Extended Service Set). Ovim se postiže povećanje opsega delovanja bežične mreže ili spajanje dve ili više bežičnih mreža.




*Slika 5 – Bežični distributivni sistem*

### 3.6.4 Interakcija sa drugim IEEE 802 slojevima

Standard IEEE 802.11 zahteva da se višem podsloju LLC[11] u okviru sloja veze podataka prikaže kao žični IEEE 802 LAN. Zbog toga je neophodno da IEEE 802.11 mreža reši pitanje mobilnosti stanica u okviru MAC podsloja na sloju veze podataka. Povodom toga neophodno je da IEEE 802.11 standard ugradi funkcionalnost koja je atipična za MAC podsloj.

## 3.7 Tipovi frejmova IEEE 802.11 standarda

Frejmovi predstavljaju enkapsulaciju podataka sa viših slojeva OSI modela.
Okviri IEEE 802.11 standarda su podeljeni u tri kategorije:

- **Menadžment okviri (*Management frames*)**

  Menadžment okviri se koriste kako bi izvršili nadzor kompletnog procesa, pristupanje i napuštanje bežičnih mreža.

  Postoji 12 podtipova menadžment okvira:

  1) **Zahtev za povezivanje** *(*engl. *Association Request)* – omogućava pristupnoj tački da izvrši sinhronizaciju sa stanicom. Stanica šalje zahtev za sinhronizaciju pristupnoj tački, okvir sadrži informacije o stanici i SSID mreže kojoj želi da pristupi. Nakon prijema zahteva za sinhronizaciju, pristupna tačka razmatra da li da izvrši asocijaciju sa stanicom i ukoliko prihvati rezerviše prostor u memoriji, uspostavlja identifikacioni broj asocijacije za stanicu.
  2) **Odgovor na zahtev za povezivanje** *(*engl. *Association Response)* – pristupna tačka šalje okvir za odgovor na asocijaciju, koji sadrži obaveštenje o prihvatanju ili odbijanju asocijacije. Ukoliko je asocijacija prihvaćena ovaj okvir sadrži identifikacioni broj asocijacije.
  3) **Zahtev za ponovno povezivanje** ***(***engl. *Reassociation Request)* – ukoliko se stanica udalji od pristupne tačke na koju je povezana i pronađe drugu pristupnu

[11] *Logical Link Control* (LLC) je viši podsloj unutar sloja veze podataka koji vrši obradu grešaka, kontrolu toka, frejmovanje i MAC adresovanje.

tačku koja ima jači beacon signal, stanica će poslati okvire reasocijacije toj pristupnoj tački.

4) **Odgovor na zahtev za ponovno povezivanje** *(*engl. *Reassociation Response)* – pristupna tačka šalje okvir sa odgovorom za reasocijaciju, koji sadrži poruku o prihvatanju ili odbijanju zahteva za reasocijaciju, ovaj okvir sadrži iste podatke kao i okvir za asocijaciju
5) ***Probe* zahtev** *(*engl. *Probe Request)* – stanica šalje Probe Request okvir kada je potrebno pribaviti informaciju od druge stanice npr. stanica šalje Probe zahtev kako bi odredila koja je pristupna tačka dostupna
6) ***Probe* odgovor** *(*engl. *Probe Response)* – stanica odgovara sa Probe Response okvirom kada primi Probe Request okvir
7) ***Bikon*** *(*engl. *Beacon)* – pristupna tačka periodično šalje beacon okvir kako bi oglasila svoje prisustvo i prenela informacije npr. SSID.
   Stanice kontinuirano skeniraju sve 802.11 radio kanale i osluškuju prisustvo beacon signala. Na osnovu ovoga vrše izbor na koju će se pristupnu tačku povezati.
8) ***Poruka o potvrdi saobraćaja*** *(*engl. *Announcement Traffic Indication Message)* – koristi se u ad hoc ili IBSS mrežama kako bi oglasili prisustvo frejmova u baferu. Ove poruke se šalju između stanica kako bi se sprečio ulazak stanica u sleep režim i naglasilo da slede podaci.
9) ***Deasocijacija*** *(*engl. *Disassocation)* – stanica šalje drugoj stanici okvir deasocijacije ukoliko želi da prekine asocijaciju
10) ***Autentifikacija*** *(*engl. *Authentication)* – autentifikacija je process kroz koji pristupna tačka prihvata ili odbija identitet stanice. Stanica započinje process tako što šalje okvir autentifikacije koji sadrži identitet stanice.
    U sistemu otvorene autentifikacije stanica šalje samo jedan autentifikacioni frejm i pristupna tačka odgovara sa jednim autentifikacionim okvirom koji označava prihvatanje ili odbijanje.
    U sistemu autetifikacije sa razmenom ključa, stanica šalje inicijalni autentifikacioni okvir a pristupna tačka odgovara sa autentifikacionim frejmom koji sadrži tekst izazova. Stanica mora poslati enkriptovan tekst izazova pristupnoj tački, koristeći bezbednosni WEP ključ, u autentifikacionom okviru. Pristupna tačka proverava da li stanica ima odgovarajući bezbednosni WEP ključ tako što proverava da li je dešifrovan tekst identičan tekstu izazova. Na osnovu toga pristupna tačka šalje odgovor u autentifikacionom okviru koji sadrži prihvat ili odbijanje stanice.
11) ***Deautentifikacija*** *(*engl. *Deauthentication)* – stanica šalje deautentifikacioni okvir stanici sa kojom želi da prekine komunikaciju.
12) ***Akcija*** *(*engl. *Action)* – ovaj tip okvira služi da se pokrene akcija u ćeliji.

- **Kontrolni okviri (*Control frames*)**

Kontrolni okviri se koriste zajedno sa okvirima podataka, kako bi izvršili akviziciju kanala, funkcije podrške nosioca, potvrdu o prijemu podataka. Koriste se zajedno kako bi obezbedili pouzdan prenos podataka između stanica.
Postoji više podtipova kontrolnih okvira:

1) ***Okvir za čuvanje energije*** *(*engl. *Power Save (PS) Poll)* – koristi se za uštedu energije tokom transmisije podataka. Stanica šalje pristupnoj tački ovaj okvir što označava da je stanica ušla u režim čuvanja energije i da ukida putanju za prijem podataka. Pristupna tačka šalje podatke tek na zahtev stanice.
2) ***Zahtev za slanje*** *(*engl. *Request to Send (RTS))* – sprečava koliziju okvira u slučaju postojanja skrivenih stanica koje su povezane na istu pristupnu tačku.

Stanica šalje RTS okvir drugoj stanici kao prvu fazu u postupku „dvostrukog rukovanja“ (*two-way handshake*), koja je neophodna pre slanja podataka.

3) ***Potvrda za slanje*** *(*engl. *Clear to send (CTS)* – stanica odgovara na RTS okvir sa ovim okvirom, što predstavlja zahtev drugoj stanici da pošalje okvir podataka. CTS okvir sadrži vremensku vrednost koja prouzrokuje da ostale stanice sačekaju sa transmisijom podatka dok stanica koja je poslala RTS okvir ne prosledi okvir podatka.
4) ***Potvrda o prijemu*** *(*engl. *Acknowledgement (ACK))* – nakon prijema okvira podataka, stanica koja prima takav okvir pokreće proceduru za proveru grešaka. Prijemna stanica će poslati ACK okvir ako ne postoje greške. U slučaju da ACK okvir nije stigao na odredište, stanica koja šalje ACK okvir ponovo posle određenog vremena.
5) ***Contention-Free*** **okvir** (engl. *Contention-Free (CF)* – End**)** – služi za indikaciju contention-free perioda (CFP). To znači da pristupna tačka funkcioniše u režimu koordinacije funkcije tačke (PCF). Tokom CFP-a pristupna tačka šalje upite o nameri da se proslede okviri podataka samo stanicama koje funkcionisu u PCF režimu. Ova metoda se koristi za prioritizaciju stanica.
6) ***CF-kraj+CF-potvrda*** (engl. *CF-End+CF-Ack)* – služi za indikaciju CFP i potvrđuje se prijem okvira koji se redovno koriste u PCF režimu
7) ***Crna potvrda*** *(*engl. *Black-Ack)* – okviri se šalju dok funkcioniše režim hibridne koordinacije funkcije tačke (HCF). HCF je slična PCF, ali za razliku od PCF u kom je interval između dva beacon okvira podeljen na CFP i *Contention* period, HCF dozvoljava da CFP bude pokrenut tokom celog *Contention* perioda.
8) ***Crni potvrdni zahtev*** *(*engl. *Black Ack request)* – koristi se u HCF-u za zahtevanje različitih parametara transmisije

- **Okviri podataka (*Data frames*)**

Okviri podataka predstavljaju glavne nosioce podataka, sadrže protokol višeg sloja. Postoji 15 tipova okvira podataka:

1) ***Data*** – ovaj okvir sadrži podatak koji se šalje
2) ***Data+CF-Ack***
3) ***Data+CF-Poll***
4) ***Data+CF-Ack+CF-Poll***
5) ***Null*** – označava da se ne šalju podaci i da stanica ulazi u režim čuvanja energije.
6) ***CF-Ack***
7) ***CF-Poll***
8) ***Data+CF-Ack+CF-Poll***
9) ***QoS data***
10) ***QoS Null***
11) ***QoS data+CF-Ack***
12) ***QoS data+CF-Poll***
13) ***QoS data+CF-Ack+CF-Poll***
14) ***QoS CF-Poll***
15) ***QoS CF-Ack+CF-Poll***

## 3.8 Uvod u protokole bežičnih mreža

Međunarodne organizacije za standardizaciju su uvidele nedostatke standarda za bežične mreže kao i neophodnost da se on unapredi. Kao rezultat, nastaju dva nova standarda WPA (engl. Wi-Fi Protected Access) i 802.11i.

### 3.8.1 WEP

WEP (engl. *Wired Equivalent Privacy*) je protokol bežičnih mreža, koji se koristi kako bi obezbedio zaštitu podataka na sloju veze OSI modela.
Protokol je detaljno definisan u standardu bežičnih mreža IEEE 802.11, u nastavku je detaljno opisan princip rada ovog protokola. Cilj WEP protokola jeste da ostvari poverljivost podataka, kontrolu pristupa i integritet poruka.

**Poverljivost podataka** se ostvaruje šifrovanjem tela okvira uz pomoć simetričnog protočnog algoritma RC4. Generiše se veliki broj pseudoslučajnih bitova kao funkcija ključa k i inicijalizacionog vektora IV. Ovaj niz bitova je označen kao RC(IV,k).
Nakon toga se vrši operacija ekskluzivno ILI nad bitovima otvorenog teksta (P) i nad dobijenim nizom pseudoslučajnih bitova, rezultujući dobijanje šifrata $C = P \oplus RC(IV, k)$.
Sigurnost WEP protokola je zasnovana na tajnosti ključa, uz pomoć kojeg se vrši šifrovanje tela okvira poruke.

**Integritet poruka** se ostvaruje operacijom zaštitnog kodovanja algoritmom CRC-32. Dobija se kontrolni zbir koji se dopisuje na kraj podataka koje je potrebno zaštiti. Osnovna namena ovog algoritma jeste očuvanje integriteta podataka u komunikacionom kanalu sa smetnjama i šumom, služi za detekciju grešaka. Algoritam CRC-32 nije namenjen za kriptografsku upotrebu, jer ne štiti u potpunosti integritet podataka. Otvoreni tekst predstavlja ulaz za šifrovanje i dobija se na sledeći način: $P = (M, \mathrm{CRC32(M)})$, gde M predstavlja originalni podatak, a $\mathrm{CRC32(M)}$ kontrolni zbir.

**Sigurnosni propusti WEP protokola**

- Prilikom komunikacije između stanice i pristupne tačke, zaglavlja kontrolnih okvira nisu šifrovana, napadač sa lakoćom može doći do inicijalizacionog vektora koji se koristi za šifrovanje. Napadač može uhvatiti dva šifrata koji su šifrovani istim inicijalizacionim vektorom, dobijajući informacije o porukama.
$$C_1 \oplus C_2 = \big(P_1 \oplus RC4(v,k)\big) \oplus \big(P_2 \oplus RC4(v,k)\big) = P_1 \oplus P_2$$
Ukoliko otvoreni tekst sadrži dovoljno metainformacija, napadač može doći do $P_1$ i $P_2$ , poznavajući samo $P_1 \oplus P_2$. Za uspešnost ovog napada je potrebno da napadač poseduje podatke šifrovane istim inicijalizacionim vektorom, mora barem delimično poznavati otvoreni tekst.
- U arhitekturi WEP protokola postoji propust koji rezultuje ponovnom upotrebom ključa, što je neprihvatljivo sa stanovišta sigurnosti. Dužina ključa je 40 bitova, polje koje sadrži vrednost inicijalizacionog vektora dugačko je 24 bita, što daje $2^{24}$ = 16.777.216 različitih vrednosti. S obzirom da prosečna stanica koja šalje okvire veličine 1500 bajtova pri prosečnoj brzini od 5 Mb/s, iskoristi sve vektore za manje od pola dana, jasno je da će se ponovo upotrebiti isti inicijalizacioni vektor za

širovanje, što predstavlja veliki propust. Analizom mrežnog saobraćaja napadač čeka da se ponovi isti inicijalizacioni vektor, dolazeći do $P_1 \oplus P_2$.

- **Napad ponavljanjem inicijalizacionog vektora** (engl. *IV replay attack*)
  Napadač preko interneta šalje poruku osobi koju želi da napadne. Zatim prisluškuje mrežu, čekajući da prisupna tačka pošalje korisniku poruku sa poznatim tekstom. Napadač „skida" kriptografsku zaštitu sa poruke, upravo zbog toga što mu je poznat inicijalizacioni vektor šifrovane poruke. Nakon ovoga, napadač može dodavati svoje podatke u šifrovane pakete. Osnovna pretpostavka je da se inicijalizacioni vektor i WEP ključ mogu ponavljati sve dok mreža ne prihvati da je u pitanju ispravan paket. Kada napadač dobije niz bitova kojima je paket šifrovan, dobijeni niz koristi kako bi uspešno šifrovao druge podatke koje ubacuje u mrežu.

- **Napad obrtanjem bitova** (engl. *bit-flipping attack*)
  Koristi slabost vektora integriteta poruke, moguće je predvideti elemente paketa, koji se nalaze na fiksnim pozicijama, iako šifrovan paket nije fiksne dužine. Napadač prisluškuje mrežu, uzima jedan okvir i menja vrednosti nekoliko slučajnih odabranih bitova unutar polja IP paketa koji sadrži poruku. Menja sadržaj polja vektora integriteta poruke (ICV) a zatim izmenjeni paket šalje na mrežu.
  Korisnik prima paket, računa vektor integriteta poruke pomoću podataka koji se nalaze u paketu. Upoređuje se izračunata i dobijena vrednost vektora integriteta poruke, ukoliko su vektori isti, prihvata se paket, skida se enkapsulacija i prosleđuje se višem sloju OSI modela. S obzirom da je napadač zamenio bitove IP paketa, provera integriteta nije uspešna i generiše se predvidljiv izveštaj o grešci.
  Napadač prisluškuje mrežni saobraćaj, tražeći predvidljiv šifrovani odgovor. Po prijemu odgovora, napadač dolazi do niza bitova ključa.

### 3.8.2 WEP2

Naslednik WEP protokola, nasledio je fundamentalne slabosti u dizajnu iako je osnovni cilj IEEE standarda bio da se poveća sigurnost WEP protokola. Promenjena je dužina ključa na 128 bita, prošireno je polje inicijalizacionog vektora na 128 bita. Kompatibilan je sa WEP protokolom i podržava Kerberos V protokol. Algoritam za šifrovanje i način upravljanja ključevima nisu unapređeni, ne donoseći nikakav napredak na polju sigurnosti.
Promena dužine ključa i polja inicijalizacionog vektora nije rešila brojne sigurnosne propuste WEP protokola.

### 3.8.3 WPA

WPA je projektovan od strane Wi-Fi alijanse (engl. *Wi-Fi Alliance*). Nastao je kao potreba da se otklone nedostaci WEP standarda, a da se pri tome ne naruši kompatibilnost sa postojećom mrežnom opremom. WPA radi na sloju veze OSI modela, koristi TKIP protokol (engl. *Temporal Key Integrity Protocol*) za distribuciju ključa i RC4 algoritam za šifrovanje, standard 802.1x i neki od uobičajenih EAP protokola za proveru identiteta i MIC (engl. *Message Integrity Check*) za sprečavanje lažiranja paketa.
Provera identiteta se vrši pomoću deljenih ključeva i RADIUS servera za veće bežične mreže. Uz instalaciju novih drajvera u pristupnim tačkama i korisničkim mrežnim karticama, biranjem tipa EAP protokola za proveru identiteta sa lakoćom se može implementirati u postojeću mrežnu opremu.

### 3.8.4 WPA2

WPA2 predstavlja nadogradnju WPA protokola. Koristi AES algoritam u CBC režimu rada za šifrovanje paketa. Za servis autentifikacije koristi Kerberos protokol, koji vrši verifikaciju identiteta korisnika na mreži na bazi tiketa.
Ulančavanje omogućava blokovskim šiframa mehanizam povratne sprege. Rezultati šifrovanja prethodnih blokova predstavljaju ulazne vrednosti za šifrovanje trenutnog bloka. Svaki blok šifrata zavisi i od odgovarajućeg bloka otvorenog teksta, kao i od prethodnih blokova otvorenog teksta.

**CBC** (engl. *Cipher Block Chaining*) režim rada, pre šifrovanja obavlja XOR operaciju nad blokom otvorenog teksta i prethodnim blokom šifrata. Nakon šifrovanja bloka otvorenog teksta, dobijeni šifrat se upisuje u registar sa povratnom spregom. Pre šifrovanja sledećeg bloka otvorenog teksta, obavlja se XOR operacija nad tim blokom i registrom s povratnom spregom, a rezultat ovog koraka postaje sledeći ulaz rutine za šifrovanje. Dobijeni šifrat se zatim ponovo upisuje u registar sa povratnom spregom, kako bi se ponovo primenila operacija XOR sa sledećim blokom otvorenog teksta, i tako do kraja poruke.
Matematički gledano, šifrat se dobija na sledeći način: $C_i = E_k(P_i \oplus C_{i-1})$
Blok šifrata se dešifruje i upisuje u registar sa povratnom spregom. Nakon dešifrovanja sledećeg bloka, obavlja se operacija XOR sa rezultatima registra sa povratnom spregom. Sledeči blok šifrata se upisuje u registar sa povratnom spregom i tako do kraja poruke. Proces dešifrovanja se obavlja na sledeći način: $P_i = C_{i-1} \oplus D_k(C_i)$

WPA2 je upotrebljiv i u IBSS režimu rada bežičnih mreža. Osnovni nedostatak ovog protokola jeste neophodnost ulaganja u novu mrežnu opremu, koja može da podrži funkcionisanje AES algoritma, bez značajnog gubitka performansi.

Pokušaj da se prevaziđu ograničenja kod WEP-a ostvaren je implementacijom TKIP protokola, koji je doneo brojna poboljšanja:

- Povećava se polje inicijalizacionog vektora sa 24 na 48 bita
  Ovim se sprečava mogućnost šifrovanja dva paketa istim inicijalizacionim vektorom
- Generiše se 128-bitni ključ koji se koristi za šifrovanje samo jednog paketa RC4 algoritmom, dok je kod WEP-a bila praksa da se jedan ključ koristi za šifrovanje više paketa, što je sa kriptološke strane neprihvatljivo

Ključ za šifrovanje podataka se generiše mešanjem u dva koraka vremenskog ključa, MAC adrese klijenta i inicijalizacionog vektora
Ukoliko se vremenski ključ ne obnovi ili ukoliko se brojač paketa iscrpi a stanica i pristupna tačka se ne dogovore oko novog vremenskog ključa komunikacija se prekida
CRC-32 funkcija je zamenjena MIC algoritmom. MIC algoritam definiše efikasan mehanizam za sprečavanje aktivnih napada. Pretpostavka je da paketi stižu na prijemnu stranu po redu. Nakon prijema paketa koji se ne očekuje, prijemna strana odbacuje paket, menja vremenski ključ i inicijalizacioni vektor postavlja na nulu. Iako bi upotreba heš funkcija bila mnogo ispravnija u kriptografskom smislu, njihova upotreba za zaštitu integriteta podataka bi negativno uticala na performanse mreže.

### 3.8.5 CCMP

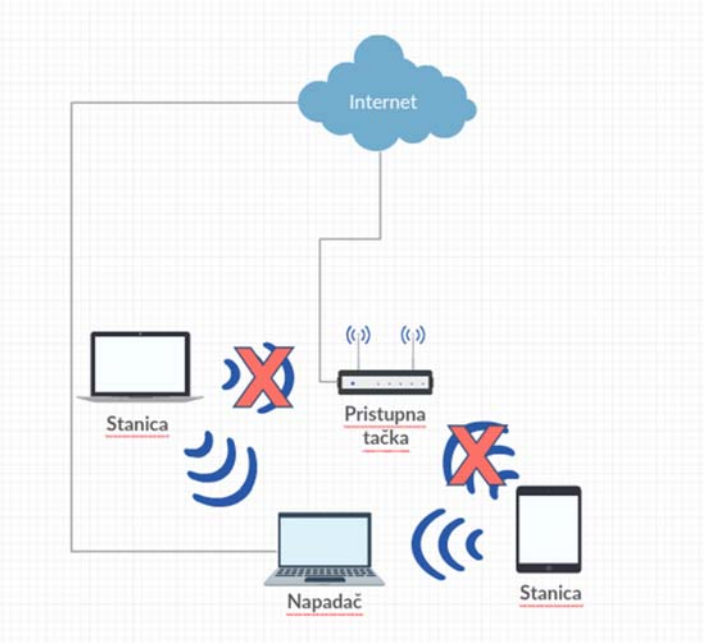
**CCMP** (engl. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) protokol za šifrovanje je sastavni deo 802.11i standarda bežičnih mreža. Njegova upotreba je obavezna u svim implementacijama ovog standarda, predviđen je samo za blokovsko šifrovanje. Predstavlja bolje i trajnije rešenje brojnih problema zaštite bežičnih računarskih mreža. Koristi AES algoritam u CCM režimu rada (engl. Counter Mode Encryption with CBC – MAC Data Origin Authenticity).

Šifrovanje i zaštita integriteta podataka obezbeđeni su uz pomoć vremenskog ključa (engl. Temporal Key), koji je poznat samo stanici i pristupnoj tački. CCM režim koristi 128-bitne blokove podataka. Najpre se u CBC-MAC režimu generiše MIC koji služi za zaštitu integriteta paketa. Zatim se korisni podaci šifruju AES algoritmom koristeći CTR režim rada (engl. counter mode). Proizvoljno odabrana vrednost - brojač se šifruje AES algoritmom. Nakon toga se nad dobijenim rezultatom i blokom podataka koji se šifruje izvodi operacija ekskluzivno ILI. Nakon svakog šifrovanog bloka, brojač se inkrementira. Prilikom šifrovanja bitova zaštite integriteta uzima se 0 kao vrednost brojača. CTR režim rada poseduje funkciju zaštite privatnosti podataka (poverljivost).

CCMP značajno povećava nivo sigurnosti u odnosu na TKIP i WEP. Jedini nedostatak predstavlja nemogućnost implementacije u postojeću mrežnu opremu, osim ukoliko ona ne poseduje dovoljne performanse za pokretanje AES algoritma.

## 3.9 Kriptoanalitički metod „Zli blizanac“ (engl. *Evil Twin*)

„Zli blizanac“ (engl. *Evil Twin*) predstavlja vrstu napada čovek u sredini (engl. man-in-the-middle). Ovakav napad se može koristiti za čitanje i izmenu podataka korisnika određene mreže.
Napad se izvodi tako što napadač pravi lažnu pristupnu tačku koja izgleda kao prava pristupna tačka, sa ciljem da se korisnik poveže na nju, što rezultuje kompromitovanjem integriteta korisničkog uređaja. Napadač koristi uređaj koji ima mogućnost povezivanja na internet (pametni telefon, kompjuter itd.) i alatke konstruisane u ovu svrhu. Napadač postavlja svoj uređaj u blizini prave pristupne tačke, kako bi prikupio imena prave pristune tačke i radio frekvencije na kojoj ona radi. Nakon toga šalje svoj radio signal, pritom koristi isto ime kao prava pristupna tačka.
Sledi nasilni prekid komunikacije korisnika i pristupne tačke od strane napadača, koji ujedno klijentu ne dopušta ponovno povezivanje na pravu pristupnu tačku. Klijent zatim pokušava da pristupi pravoj pristupnoj tački, ali sa obzirom da napadač ne dozvoljava, klijent se povezuje na lažnu pristupnu tačku tj. napadačev uređaj.
Takva konekcija se može desiti tako što se korisnik svesno poveže na lažnu pristupnu tačku, jer uočava da ova pristupna tačka ima dobar signal i povezanost sa internetom. Moguće je podesiti da se korisnikov uređaj povezuje automatski ukoliko je podešen promiskuitetan režim, što znači da se uređaj povezuje automatski na otvorenu mrežu, u ovom slučaju na „zlog blizanca“.




*Slika 6 – Kriptoanalitički metod „Zli blizanac“*

# 4 Eksperimentalni rad – studija slučaja

## 4.1 Primena kriptoanalitičkog metoda „Zli blizanac“ (engl. *Evil Twin*)

Prednost ovog kriptoanalitičkog metoda jeste zaobilaženje klasičnih kriptoanalitičkih metoda za „razbijanje“ kriptografski zaštićenih sistema bežičnih mreža, ušteda resursa potrebnih za njihovo otkrivanje i „nasilno“ preusmeravanje korisnika na napadačevu pristupnu tačku. Za primenu ovog kriptoanalitičkog metoda koristi se Kali Linux distribucija.

### 4.1.1 Metodologija napada

1) **Skeniranje dostupnih bežičnih mreža**

   Skeniranje dostupnih mreža radi pronalaženja mete napada.

2) **Skeniranje ciljane pristupne tačke**

   Posmatranje aktivnih uređaja povezanih na pristupnu tačku koja predstavlja metu napada.

3) **Pravljenje “zlog blizanca”**

   Napadač uzima parametere originalne pristupne tačke u cilju pravljenja kopije, koja ima isti naziv (ESSID[12]) i broj kanala (CH) kao i originalna pristupna tačka.

4) **Skeniranje “zlog blizanca”**

   Napadač skenira napravljenu pristupnu tačku, kako bi video da li postoje uređaji koji su se povezali.

5) **Podešavanje IP adrese, subnet maske i firewall pravila zlog blizanca**

6) **Napad deautentifikacije na originalnu pristupnu tačku** podrazumeva korišćenje alata za deautentifikaciju uređaja povezanih na originalnu pristupnu tačku. Cilj ovog napada je onemogućavanje povezivanja korisnika na originalnu pristupnu tačku.

### 4.1.2 Potrebni uređaji

1) **Laptop računar**
2) **Mrežna kartica** koja poseduje režim skeniranja (engl. *monitor mode*) i mogućnost ubacivanja paketa (engl. *packet injection*)
3) **Ruter (**mobilni telefon sa mogućnošću kreiranja režima pristupne tačke)

### 4.1.3 Potreban softver

1) **Kali Linux 2.0**
2) **Set alata za penetraciono testiranje**
   (Airmon-ng, airodump-ng, airbase-ng, aireplay-ng)
3) **isc-dhcp server**

[12] ESSID (engl. *Extended Service Set Identification*) predstavlja naziv bežične mreže.

4) **IP tables**
5) **Apache, MySQL**

## 4.2 Detaljan opis kriptoanalitičkog metoda „Zli blizanac“

### Korak 1 – instalacija dhcp servera

DHCP (engl. *Dynamic Host Configuration Protocol*) je klijent/server protokol koji automatski dodeljuje internet protokol (IP) adresu *host*-u i druge informacije kao što je subnet maska i podrazumevani mrežni prolaz (engl. default gateway).

Instalacija dhcp servera se postiže sledećom komandom:

**apt-get install isc-dhcp-server**

### Korak 2 – konfigurisanje dhcp servera

Konfiguracija dhcp servera se obavlja unošenjem sledećih komandi u fajl pod nazivom dhcpd.conf. Otvaranje ovog fajla se postiže sledećom komandom u terminalu:

**nano /etc/dhcp/dhcpd.conf**

Nakon otvaranja se na početak fajla unosi sledeći kod:

```
authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0
{
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8;
    range 192.168.1.5 192.168.1.100;
}
```

### Korak 3 – razrešavanje konflikta između airmon-ng i Network Manager–a

Razrešavanje konflikta je potrebno uraditi kako ne bi bilo potrebno gasiti pristup internetu pre stavljanja kartice u monitor mode. Potrebno je uneti sledeću komandu u terminal:

**nano /etc/NetworkManager/NetworkManager.conf –** pristupanje konfiguracionom fajlu (engl. *config file)* network manager-a

Uneti sledeći kod na kraj fajla:

**[keyfile]**

**unmanaged-devices=interface-name:wlan0mon;interface-name:wlan1mon;interface-name:wlan2mon;interface-name:wlan3mon;interface-name:wlan4mon;interface-name:wlan5mon;interface-name:wlan6mon;interface-name:wlan7mon;interface-**