Sigurnost bežičnih mreža

Belančić, Matija

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

«Dr. Mijo Mirković»

MATIJA BELANČIĆ

SIGURNOST BEŽIČNIH MREŽA

Završni rad

Pula, 2015.

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

«Dr. Mijo Mirković»

MATIJA BELANČIĆ

SIGURNOST BEŽIČNIH MREŽA

Završni rad

JMBAG: 2310-E, redoviti student

Studijski smjer: Informatika

Predmet: Računalne mreže

Mentor: Prof. dr. sc. Mario Radovan

Pula, srpanj 2015.

Sadržaj

Uvod 1
1. Općenito o bežičnim mrežama 3
1.1 Fleksibilnost bežičnih mreža 4
1.2. Standardi bežičnih mreža 6
1.3. Arhitektura bežičnih mreža 8
2. Općenito o sigurnosti 10
2.1 Sigurnosni standardi bežičnih mreža 13
2.1.1 WEP 13
2.1.2 WPA 14
2.1.3 WPA2 15
2.1.4 Identifikator skupa usluga (SSID) 16
2.1.5 802.1x standard 18
2.1.6 802.11i standard 21
3. Propusti i napadi na sigurnost bežičnih mreža 22
3.1 Propusti pri provjeri indetiteta korisnika 22
3.2 Propusti u WEP standardu 23
3.3 Napadi na WEP 25
4. Načini zaštite od napada na bežičnu mrežu 31
5. Probijanje WEP zaštite (praktični dio) 34
6. Zaključak 39
7. Literatura 40

Uvod

Svi koji računalo koriste čak i u najmanju svrhu (kao npr. za razonodu ili hobi) sigurno su se jednom susreli sa Wi-Fi mrežom (Wireless Local Area Network ili WLAN, odnosno bežičnom lokalnom mrežom). Bilo to u kafiću, na poslu, fakultetu ili jednostavno u svom vlastitom domu znaju da se tu odvija nekakva „zračna“ komunikacija odnosno prijem signala. Bežične mreže su svakako budućnost i sadašnjost povezivanja računala. Žične mreže imaju svojih prednosti, ali zato jednostavnost i brzina postavljanja bežične mrežne infrastrukture su na strani bežičnih mreža. Za prijenos informacija između spojenih uređaja, bežična mreža umjesto kabela koristi radio signal. Naravno kod bežičnih mreža signal koji putuje zrakom osjetljiv je na brojne interakcije i prepreke pa brzina uvelike ovisi i o kvaliteti veze, fizičkoj vidljivosti, zaprekama i slično. Radi toga bežične mreže su uglavnom sporije od žičnih mreža, tj. kabela, a osnovna oprema potrebna za postavljanje bežične mreže skuplja je od opreme za žičnu mrežu. Gotovo pa je nemoguće naći moderniji uređaj koji nema mogučnost bežičnog povezivanja. Imaju ga tableti, mobiteli, laptopi, fotoaparati čak i kamera, televizija i igraća konzola.

Praktičnost Wi-Fi mreža ima svoju negativnu stranu, a to je ozbiljno ugrožavanje privatnosti i sigurnosti. Gubitak povjerljivosti, integriteta, i prijetnje operacijskom sustavu najgore su značajke napada na bežične mreže. Neovlašteni korisnici, tj. napadači, mogu probiti i pristupiti pristupnoj točci (usmjerivaču) i korisničkovoj vlastitoj mreži i tako poremetiti podatke, trošiti samu dostupnost veze, spustiti mrežne performanse i pokrenuti napade koji bi autoriziranim korisnicima sprječavali pristup mreži ili jednostavno koristili njihovu mrežu kao napad na ostale mreže. Zato je od veoma velike važnosti dobro zaštiti vlastitu mrežu dobrim odabirom zaštite odgovarajuče enkripcije i lozinke.

Ovaj rad sadrži 5 cjelina koje će obuhvatiti opći pojam bežičnih mreža i načina njihovog rada, kao i standarda koji su vezani za bežične 802.11 mreže u koja je opisana u prvoj cjelini. Prva cjelina obuhvaća još i samu arhitekturu i način rada bežičnih mreža. Druga cjelina se odnosi na pojam sigurnosti, tj.sigurnosti u bežičnim mrežama, kao i standarde zaštite. Treća cjelina bazirana je na propustima WEP standarda, aktivnim i pasivnim napadima, i također propustima korisnika pri autentifikaciji.

U četvrtoj cjelini detaljno će se objasniti krađa indetiteta, kako se kradu indetiteti, te njihovo sprječavanje. Opisat će se značajnost lozinki, i prikazati one najučestalije kako bi ih mogli što manje koristiti radi sigurnosti naših podataka a i sprječavanja krađe indetiteta. Za kraj prikazan je napad na WEP zaštitu, i time kako se sa malo više računalnog znanja i sposbnosti može jako ugroziti naš sustav i naši podaci.

1. Općenito o bežičnim mrežama

Računalna mreža je grupa računala, na bližoj ili daljnoj lokaciji, povezanih prijenosnim medijem. Danas su računala i računalne mreže najbolji način prijenosa velikih količina informacija u vrlo kratkom vremenu i na velike udaljenosti. Razvojem informatičke opreme, posebno radnih stanica i osobnih računala, otvara se mogučnost stvaranja raznih informatičkih mreža. Informatičke mreže omogućuju da se s mnogih međusobno udaljenih lokacija ostvari pristup do največih nacionalnih instalacija.

Bežična mreža je mreža postavljena pomoću frekvencije radio signala za komunikaciju između računala i drugih mrežnih uređaja. Često se bežične mreže nazivaju Wi-Fi mreže ili WLAN (Wireless Local Area Network). Ova mreža postaje sve više popularna zbog jednostavnog postavljanja i bez kabela kojeg moramo provlačiti. Možemo povezati računala bilo gdje u našem domu bez potrebe za korištenjem LAN kabela. Bežične mreže obično imaju veliku fleksibilnost, koja se može prevesti na brzom raspoređivanju. Bežične mreže koriste niz baznih stanica za spajanje korisnika na postojeću mrežu. Infrastrukturna strana bežične mreže, međutim, je veoma kvalitetna bez obzira da li se spaja jedan korisnik ili milijun korisnika. Prvi su se bežični uređaji zasnovani na danas najraširenijem IEEE 802.11b standardu počeli pojavljivati na tržištu sredinom 1999. godine. S vremenom je broj proizvođača i zanimanje kupaca za ovakvu opremu toliko narastao da je bilo potrebno na neki način standardizirati cijeli koncept. U tu svrhu utemeljena je udruga proizvođača ovakve opreme – Wireless Ethernet Compatibility Alliance – koja je zadužena za brigu oko standardizacije opreme za bežične mreže. Jedna od posljedica postojanja ove udruge jest i udomaćivanje zajedničkog imena za različite standarde. Metoda kojom se mnoge današnje mreže služe – čak i one koje nemaju nikakve veze s umrežavanjem računala- naziva se spread spectrum. Takvom metodom uređaji upravljuju frekvencijom signala tako da različiti paketi podataka putuju na različitim frekvencijama između odašiljača i prijemnika. Postoje dvije vrste spread spectrum sistema: frequency hopping i direct sequence. U frequency hopping spread spectrum sistemu (FHSS) uređaji „skakuću“ između različitih frekvencija. Time se postiže sigurnija i pouzdanija komunikacija među uređajima. Direct sequence sustavi pouzadnost postižu emitiranjem u različitim, slučajno generiranim intervalima na jednoj frekvenciji.

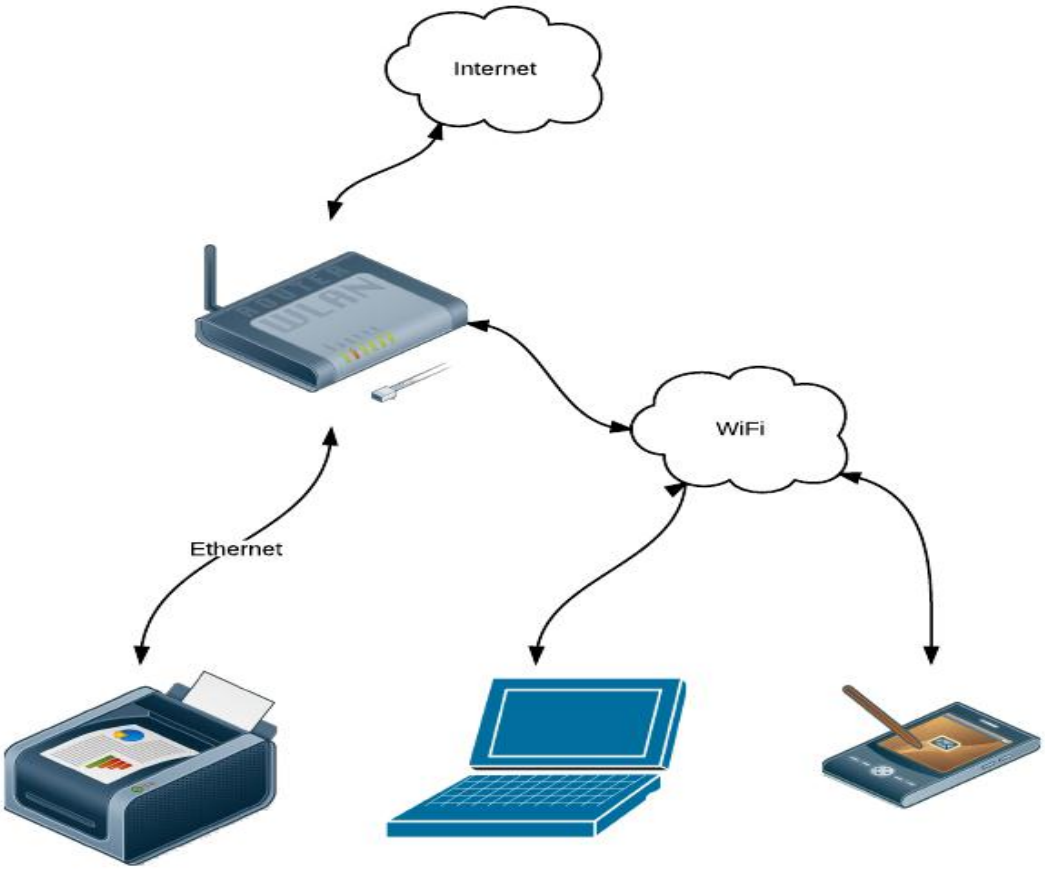
Skup tehnologija koje zajednički nazivamo WLAN tehnologije definirane su skupom IEEE 802.11 standarda. Preciznije, WLAN tehnologije kriju se pod oznakama 802.11b, 802.11a i 802.11g. U usporedbi sa Ethernetom brzine ovih mreža nisu velike. Štoviše, teoretska brzina najpopularnije od bežičnih tehnologija – 802.11b – od 11 Mbps zamalo je deset puta manja od najpopularnijeg 100 Mbps Etherneta.

„Bežična komunikacija u ovim mrežama ostvaruje se predajom signala od jednog do drugog primopredajnika (komunikacijski uređaj sposoban primati i odašiljati signale). Komunikacija u bežičnom LAN-u može obavljati unutar kruga određenog dometom primopredajnika. Ovisno o pojedinom standardu, maksimalno se može komunicirati na daljinama od 350 metara na otvorenom prostoru bez prepreka.“ (Ilišević 2005., str. 80)

1.1 Fleksibilnost bežičnih mreža

Bežične mreže dijele nekoliko važnih prednosti, bez obzira kako su protokoli dizajnirani, ili koje vrste podataka s njima dolaze. Najveća prednost mobilnih mreža je svakako mobilnost. Korisnici bežičnih mreža mogu se spojiti na postojeću mrežu i dozvoljeno im je da mogu biti spojeni bez obzira u kojem dijelu stana, kuće, kafića, fakulteta ili bilo kojeg mjesta oni bili sve dok je signal na dovoljno jakoj razini. Sa boljom opremom, dobrim terenom bez puno prostora koji bi odbijao signal, tj. radio valove, možemo proširiti raspon 802.11 mreže do nekoliko kilometara. Da bi signal i pristup u određenom prostoru bili dostupni, potrebno je imati pristupnu točku (usmjerivač) i antene. Jednom kad je infrastruktura napravljena, dodavanje korisnika u bežičnu mrežu je uglavnom stvar autorizacije. Infrastrukutra se mora konfigurirati tako da se prepozna i daje pristup novim korisnicima. Sama fleksibilnost je važan atribut za pružatelje usluga.

Jedno od 802.11. rješenja na tržištu za koju se dosta dobavaljača zainteresirano je takozvani hotspot. Hotspot je područje koje je pokriveno bežičnom mrežom koji omugućuje da se korisnik besplatno spoji i surfa na toj bežičnoj mreži. Njega koriste zračne i željezničke luke radi boljeg ugođaja njihovih putnika dok čekaju svoj let ili liniju da se u bilo kojem trenutku mogu spojiti na mrežu. U mnogim kafićima i restoranima je poželjno imati pristup mreži. Fleksibilnost može biti od izmine važnosti u starijim zgradama jer smanjuje potrebu za većom konstrukcijom (Gast, 2002). Bežične mreže se mogu vrlo brzo rasporediti u takvim ustanovama i sredinama jer postoji samo mala žična mreža koja treba biti instalirana.



Slika 1. Prikaz rada bežičnih mreža u vlastitom domu (Izvor: Autor)

1.2. Standardi bežičnih mreža

Bežične mreže su definirane u standardu IEEE 802.11 koje donio IEEE.[1] U standardu se definiraju najniža dva sloja OSI modela: fizički i podatkovni sloj veze. Početna verzija standarda IEEE 802.11 formirana je sredinom 1997, tako što je za rad bežičnih Ethernet sistema određena radna frekvencija od 2,4 Ghz i dvije brzine prijenosa podataka – od 1 i 2 Mb/s . Ponuđene su i dvije tehnologije prijenosa radio-signala: FHSS (Frequency Hopping Spread Spectrum) i DSSS (Direct Sequence Spread Spectrum). FS označava Frequency Hopping (skakanje po frekvencijama), a DS Direct Sequence (niz skokova), dok SS na kraju ovih skraćenica označava Spread Spectrum, tehnologiju prijenosa signala sa ispod nivoa šuma (razmazani spektar).

Ubrzo po objavljivanju standarda određene su sljedeće radne grupe:

- grupa "A", zadužena za unaprijeđenje inicijalnog standarda,
- grupa „B", zadužena za izradu bržeg DSSS prijenosa na 2,4 GHz,
- grupa „D", zadužena za usklađivanje međunarodnih pravilnika o slobodnim radio-frekvencijama,
- grupa „E", koja obrađuje kvalitetu servisa (QoS),
- grupa „F", koja razrađuje podršku za roming, i
- grupa „G" zadužena ta rad na 54 Mb/s za zahtjevne korisnike standarda 802.11b.

Standardi 802.11a, 802.11b i 802.11g razlikuju se prema fizičkom sloju (frekvencijama rada). Sloj veze jednak je u sva tri standarda i sastoji se od podsloja pristupa medijumu (MAC) i podsloja logičke kontrole toka (LLC). MAC podsloj se malo razlikuje o takvog sloja u 802.3 koji definira žičane lokalne mreže. Umjesto CSMA/CD, za standard 802.11 karakterističan protokol CSMA/CA.[2]

[1] Engl. Institute of Eletrical and Eletronics Engineers – udruga koja razvija standarde za gotvo sve što ima veze s elektronikom. IEEE pokriva područja od automobliske industrije do neuralnih meža i supervodiča.
[2] Engl. Carrier Sense Multiply Access/ Collison Avoidance – stanica koja želi da pošalje podatke, prvo osluškuje medijum i ukoliko je on zauzet tj. ako netko već šalje podatke, stanica poštuje to i povlači se. Ukoliko je medijum slobodan određeno vrijemem setanica smije započeti slanje svojih podataka.

Podjela standarda

- **Standard 802.11a.** Fizički sloj ovog standarda definira rad na frekvenciji 5GHz (frekvencija koju je po međunarodnim standardima dopušteno koristiti bez posebnih dozvola i naknada) sa OFDM (Orthonogal Frequency Division Multiplexing) multipleksiranjem kanala. Standard omogućava brzine od 6, 9, 12, 18, 24, 36, 48 i 54 Mb/s. Iako mreže rađene po ovom standardu omogućavaju najveće brzine, one imaju jednu ogromnu manu – domet je ograničen na 15 m što je neprikladno za većinu korisnika.
- **Standard 802.11b.** 802.11a je propisao prijenos podataka brzinama od 6 do 54 Mb/s, a 802.11b je inicijalni standard pomjenio sa 1, na 5,5 i 11 Mb/s. Fizički sloj radi na frekvenciji od 2,4 Ghz, koristi DSSS tehnologiju za odašiljanje signala i omogućava maksimalnu propusnost od 11 Mb/s. DSSS tehnologija se upotrebljava zbog velike pouzdanosti i propusnosti jer se koristi širi frekvencijski opseg. Ovaj standard danas dominira na tržištu ponajviše zbog relativno niske cijene implementacije i zadovoljavajučih performansi.
- **Standard 802.11g.** Ovaj standard omogućava maksimalnu propusnost od 54 Mb/s (kao 802.11a) na frekvenciji od 2,4 Ghz (kao 802.11b). Bitno je naglasiti da je ovaj standard kompatibilan i sa 802.11a i sa 802.11b. Fizički sloj se u standardu 802.11g naziva Extendet Rate PHY (ERP). Sloj veze isti je kao i u standradima 802.11a i 802.11b.
- **Standard 802.11n.** Ovaj standard nadovezuje se na predhodne 802.11 standarde dodavanjem višestrukih unosa i izlaza (MIMO).[3] Dodatni odašiljač i prijemnik antene omogućuju veću propusnot podataka kroz prostore multipleksiranja i povećanog raspona. Brzina je 450Mb/s što je čak 4-5 brže od 802.11g, a uređaji rade na frekvencijama od 2,4 i 5 GHz 802.11n također nudi bolju radu udaljenost od sadašnjih mreža.
- **Standard 802.11ac.** Ovo je i zadnji standard na tržištu, pojavio se 2013. godine. Postoje 2 verzije. U prvoj verziji omogućava brzinu prijenosa do 1,3 Gb/s i radi isključivo na 5 GHz. A u drugoj verziji koja je izašla 2014, također radi na frekvenciji od 5 GHz, no s maksimalnom brzinom prijenosa od 6, 93 Gb/s.

[3] Engl. Multiple-Input/Multiple-Output – Tehnologija koja omogućava istovremeno slanje više streamova prema više klijenata

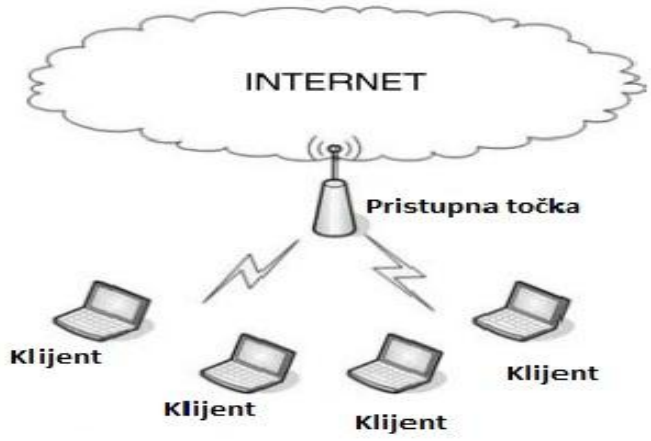
1.3. Arhitektura bežičnih mreža

Postoje dva osnovna načina ostvarivanja bežičnih mreža, od kojih korisnik odabire jedan, shodno svojim potrebama i mogućnostima. To su infrastrukturni i ad - hoc način rada.

Infrastrukturni način rada

Većina bežičnih LAN-ova rade u takozvanom infrastrukturnom načinu rada u kojemu pristupne točke osiguraju vezu bežičnih klijenata s LAN mrežom. Standard definira ovaj tip mreže kao Basic Service Set (BSS).

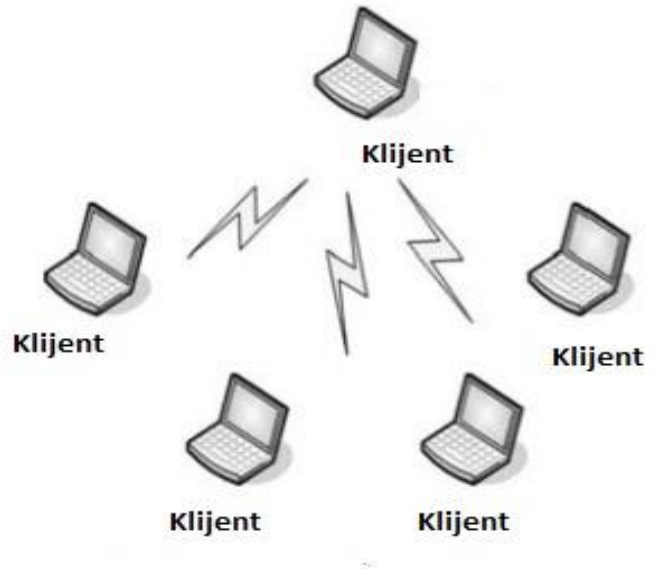
Pristupne točke (engl.access points) jesu uređaji preko kojih klijenti mogu dobiti pristup mreži. Prednost ovoga rješenja leži u tome što dopušta veću fleskibilnost u radu, veće domete signala i bolju kvalitetu. Osnovno područje rada pristupne točke je prostor koji je pokriven signalom, a često se naziva i mikroćelija. 802.11 uređaji tipično pokrivaju rastojanja od oko 100 m u zatvorenom prostoru, sa standradnim neusmjerenim antenama. Suština problema dometa bežičnih uređaja leži u slabljenju signala pri prolasku kroz zrak i prepreke. Pri izradi dobrog bežičnog sistema potrebno je dobro poznavati uzrok slabljenja signala. Veća rastojanja se pokrivaju s više pristupnih točaka povezanih u Ethernet mrežu, ili primjenom antena s većim pojačanjem. (Pleskonjić, Maček, Đorđević, Carić, 2007). Ukoliko s područja pokrivaju s više pristupnih točaka, preporučuje se da proširenja uključuju 10-15% preklapanja, kako bi korisnici bez gubljenja signala, mogli preizlaziti iz jedne ćelije u drugu.



Slika 2. Infrastrukturni način rada (http://www.pcekspert.com/)

Ad - hoc način rada

Kod ovog načina rada, bežične mrežne kartice rade nezavisno od pristupne točke. Također jednostavnije je spajanje nego kod infrastrukturnog načina ako želimo spojiti dva uređaja međusobno bez potrebe za pristupnom točkom. Na primjer, recimo da imamo dva prijenosna računala, i nalazimo se u sobi bez Wi-Fi-a. Možemo ih povezati direktno pudem ad-hoc načina rada da se formiraju u privremenu bežičnu mrežu bez potrebe za pristupnom točkom, tj. routerom. Tako uređaji mogu razmjenjivati datoteke, ili napraviti radnu grupu bez ikakvih instaliranih kablova i druge mrežne opreme. Standard definira ovaj način povezivanja kao IBSS.[4] „Ali ad – hoc ima nedostatke, takav način rada zahtijeva više sistemskih resursa kako se izgled fizičke mreže mijenja dok se uređaji izmjenjuju, tj. nadopunjuju, dok u infrastrukturnom načinu pristupna točka ostaje statična. Maksimalno se može spojiti 9 korisnika na mrežu ali opet ako su mnogi korisnici spojeni na ad - hoc mreže tu će biti više smetnji jer svako računalo, tj. korisnik mora uspostaviti izravnu vezu sa drugog računala, umjesto da ide preko jedne pristupne točke“ (How-To Geek, 2014). Ako je računalo izvan dometa drugog računala koji se želi spojiti, proći će kroz sve podatke drugih uređaja na putu, a prolazak kroz podatke drugih računala u mreži je dosta sporije nego kad se prolazi kroz samo jednu pristupnu točku.



Slika 3. Ad – hoc način rada (http://www.pcekspert.com/)

[4] Engl. Independent Basic Service Set - set svih stanica, klijenata koji koji komuniciraju svatko sa svakim

2. Općenito o sigurnosti

Pleskonjić, Maček, Đorđević i Carić (2007) navode da je sigurnost proces održavanja prihvatljive razine rizika. U skladu s time, sigurnost je proces, a ne završno stanje, tj. nije konačni proizvod. Organizacija ili institucija ne može se smatrati „sigurnom“ ni u jednom trenutku poslje izvršene posljednje provjere usklađenosti s vlastitim sigurnosnim pravilima. Sigurnost kao proces zasniva se na četri osnovna koraka: procjena, zaštita, otkrivanje i odgovor.

1. **Procjena** (engl. assesment). Procjena je priprema za ostale tri komponente. Smatra se posebnom akcijom, zato što je u vezi s pravilima, procedurama, pravnom i drugom regulativom, određivanjem budžeta, i tehničkom procjenom stanja sigurnosti. Greška u procjeni bilo kojeg od ovih elemenata, može naškoditi svim operacijama koje slijede.
2. **Zaštita** (engl. protection). Zaštita, tj. sprječavanje ili prevencija, podrazumjeva primjenu protumjera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primjenjuje se sljedeći korak – otkrivanje.
3. **Otrkivanje** (engl. detection). Otkrivanje, ili detekcija predstavlja proces indetifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost.
4. **Odgovor** (engl. response). Odgovor ili reakcija predstavlja proces oporavka. U novije vrijeme sve češće se koriste pravna sredstva (sudski proces protiv onoga koji ugrožava sigurnost).

Problem sigurnosti

Problem sigurnosti na internetu i općenito, možemo usporediti sa svojim automobilom. Svaki put kada ga vozimo prihvačamo određene rizike: naš automobil može se pokvariti, možemo doživjeti prometnu nezgodu, pa čak i smrtno nastradati. Takve rizike prihvačamo zato je nam je automobil neophodan. Svaki put kada koristimo računalo, pa tako i internet, također prihvačamo određene rizike: krađu indetiteta, viruse, spam, spyware i tako dalje. Čak i bezazelne lokacije poput popularnih odredišta za e- trgovinu ili online zabavu mogu poplaviti naše računalo softverom koji generira oglašavanje (i usporava rad računala) ili prati naše korištenje interneta. Velik je broj korisnika koji, međutim, koriste Interenet ne poduzimajući nikakve korake za ublažavanje rizika: nemaju vatrozid, ni antivirusni softver, ni

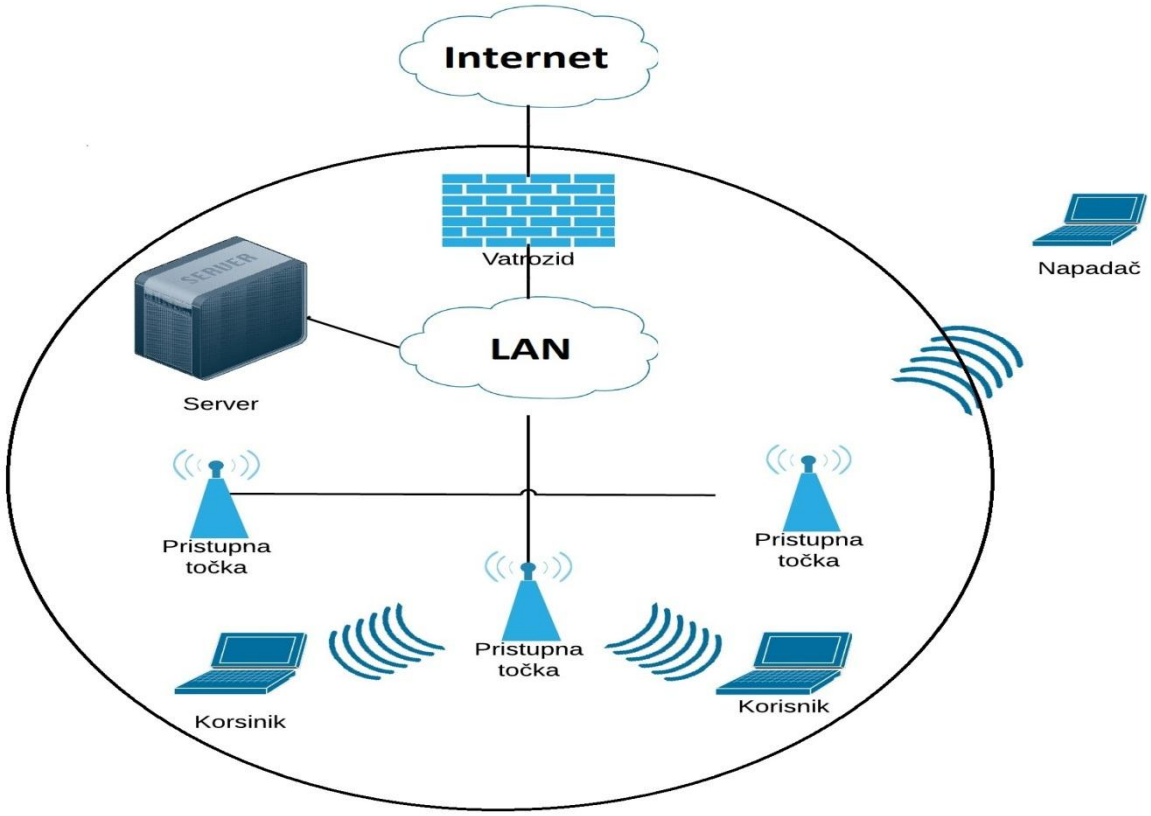
ikakve ideje o tome da prevaranti i otmičari aktivno „plaze“ Internetom u potrazi za novim žrtvama.

Praktičnost Wi-Fi mreža ima svoju cijenu: ozbiljno narušavanje privatnosti i sigurnosti. Bežična kartica ili čip u našem računalu i naša pristupna točka su zapravo radio prijemnici, doduše mali koji koriste različite frekvencije od tradicionalne AM/FM vrste. Signale koje šalju naši bežični uređaji mogu uloviti bilo koji uređaj unutar dometa, a ne samo naša pristupna točka. Napadači to znaju, pa koriste softverske programe koji se nazivaju prisluškivači i koji im omogućuju „prisluškivanje“ nešifirirane bežične veze. Ovi prisluškivači su bežično ekvivalenti prislušnim uređajima na telefonskim linijama, osim što oni mogu ugrabiti e-poštu, naše poruke prilikom dopisivanja pomoću IM-a i naravno svaku lozinku ili brojeve računa koji koriste tijekom bežičnog prijenosa.

„Bežični alati za prisluškivanje ažurirane su verzije žičanih prislušnih alata, koji mogu nadzirati prijenos na ožičenim mrežama. Međutim, bežične je prisluškivače mnogo lakše koristiti jer se ne trebamo spajati na žicu niti tražiti praznu mrežnu utičnicu“ (Murray i Weafer, 2005., str. 176). Najučestaliji rizik kod kučnih bežičnih mreža je taj da naš susjed može gledani naš promet ili besplatno koristiti Internet vezu. Također, neki bi se entuzijalist za bežičnu mrežu mogao provozati kvartom koristeći poseban softver za traženje bežičnih mreža. To se zove war driving.[5] Prilikom projektiranja bežične mreže u nekom području, potrebno je detaljno pregledati to područje i utvrditi optimalnu vrstu antena koje će se koristiti i dovoljnu snagu, a uz to treba voditi računa o svim ograničenjima. Frekvencije koje koriste mreže po standardima 802.11b i 802.11g, od 2,4 GHz su nelicencirane, što dovodi do smetnji drugih uređaja koji koriste tu istu frekvenciju, a samim time dolazi do uskraćivanja usluge.

[5] Napadačka tehnika s automatiziranim računalnim programom koji poziva telefonske brojeve s dugačkog popisa u potrazi s računalnim modemima. Druga riječ za to je war dialnig.

Osim toga dobro je pretpostaviti da potencijalni napadač može imati bolju i osjetljiviju opremu od one koja je propisana standardima, što praktično proširuje domet mreže (van fizičkih granica organizacije kojoj mreža pripada). Zbog toga se može javiti potencijalna opasnost jer se omogućava „napad s parkirališta“ (engl. parking lot attack). U novije vrijeme često koristimo različite tehnike za ograničavanje propagacije signala, zasnovane na antenama sa usmjeravanjem, ali i ometanjem signala nekom od tehnika interferencije, kako bi se signal u pojedinim područima učinio nerazumljivim.



Slika 4. „Napad s parkirališta“ (Pleskonjić i sur., 2007. str. 377)

2.1 Sigurnosni standardi bežičnih mreža

Od 1990. godine kada su bežične mreže postale popularne, postavljala su se veoma dobra pitanja a tako i sumnje u vezi sigurnosti. Zbog takvih problema i rizika koje one predstavljaju dosta ljudi je prije mislilo da se one uopče ne bi trebale koristiti. No zbog svoje jednostavnosti korištenja i praktičnosti, jasno je da bežične mreže moraju ostati pa samim time moramo ih i zaštititi kako bi bili sigurni. Postoje 3 glavna mehanizma, tj. standarda koji služe za zaštitu WLAN prometa: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) i WPA2 (ažurirana verzija WPA koji koristi jači algoritam za zaštitu i teško je probiti takav mehanizam).

2.1.1 WEP

WEP (Wired Equivalent Privacy) je sigurnosni protokol naveden od strane IEEE 802.11 standarda koji je dizajniran da pruža bežičnoj lokalnoj mreži određenu sigurnost i privatnost usporedivo s onom šta pruža LAN kabel. LAN je obično zaštičen fizičkim sigurnosim mehanizmima koji su učinkoviti kada je u pitanju kontrolirana fizička okolina, ali može biti neučinkovita za bežični rad mreža jer radiovalovi ne moraju nužno probiti zidove koje sadrže mrežu. WEP nastoji uspostaviti sličnu zaštitu kao mjera fizičke sigurnosti žične mreže pomoću slanja enkripcije podataka bežične mreže. Enkripcija podataka štiti ranjivu bežičnu povezanost između klijenata i pristupnih točaka, jednom kad je takva mjera poduzeta, ostali tipični LAN sigurnosni mehanizmi, kao što su zaštita lozinkom, E2EE[6], virtualne privatne mreže (VPN), te provjere autentičnosti mogu se staviti na svoje mjesto kako bi se osigurala privatnost.

Cilj WEP-a je da se osigura sljedeće:

- povjerljivost poruka - osnovna namjena je sprječavanje prisluškivanja mrežnog prometa
- kontrolu pristupa – pristupne točke mogu zabraniti klijentima pristup mreži ukoliko ne zadovoljavaju provjeru indetiteta

[6] Engl. End-to-end encryption – metoda koja se koristi kako bi se osigurao prijenos šifriranih podataka koji se kreću od izvora do određenog odredišta. Cilj end- to-end enkripcije je šifriranje podataka na web razini i to dešifrirati u bazu podataka ili aplikacijski server

- integritet poruka – dodatno polje u okviru koje služi za provjeru integriteta samog okvira

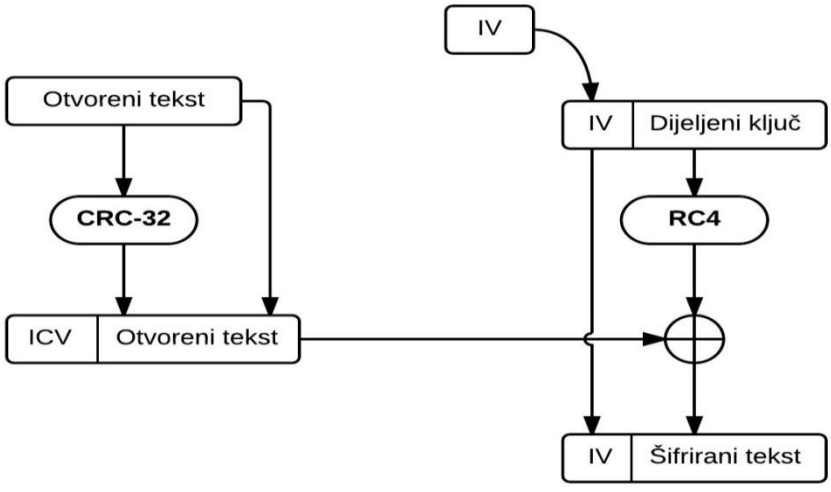
WEP se koristi radi zaštite podataka na sloju veze OSI modela. Sigurnost WEP-a je zasnovana na tajnosti ključa pomoću kojeg se tijelo okvira poruke šifrira na relaciji pristupna točka – klijent. Šifriranje se vrši u slijedećim koracima:

1. Zaštitno kodiranje

Integritet poruke osigurava se operacijom zaštitnog kodiranja algoritmom CRC-32, čime se dobija kontrolni zbroj koji se dopisuje na kraj podataka koji se žele zaštititi. U osnovi algoritma je 32-bitni polinom, 0x04C11DB7 (zapisan heksadecimalno). Osnovna namjena algoritma CRC-32 je očuvanje integriteta podataka u komunikacijskom kanalu sa smetnjama i šumom. CRC-32 je loš izbor ukoliko se primjenjuje u kriptografske svrhe jer ne štiti u potpunosti integritet poruke (moguće promijeniti određene bitove tako da se to ne detektira na prijemnoj strani). Otvoreni tekst koji predstavlja ulaz za šifriranje dobija se kao P=(M, CRC-32(M)) gdje je M originalni podatak, a CRC-32(M) kontrolni zbroj.

2. Šifriranje

Za šifriranje tijela okvira koristi se simetričan protočni algoritam RC4. Algoritam generira veliki broj pseudoslučajnih bitova kao fukciju ključa *k* i inicijalizacionog vektora IV. Ovaj niz bitova označava se sa RC(IV, *k*). Poslije toga se vrši operacija ekskluzivno ILI nad bitovima otvorenog teksta i nad dobijenim nizom pseudoslučajnih bitova kako bi se dobio šifrovani tekst.



Slika 5. Shematski prikaz WEP šifriranja i dobijanja WEP okvira (Pleskonjic i sur., 2007. str. 380)

2.1.2 WPA

Organizacija Wi-Fi Alliance projektirala je WPA (Wi-Fi Protected Access) u namjeri da otkloni nedostatke uočene u WEP standardu, a da se pritom zadrži kompatibilnost s postojećom mrežnom opremom. WPA nudi poboljšanje zaštite podataka i kontrole pristupa za WLAN sustave. Isplativiji je od današnjih IPSec rješenja, jer radi na drugom sloju OSI modela. WPA koristi:

- protokol TKIP (Temporal Key Integrity Protocol) za šifriranje,
- standard 802.1x i neki od uobičajnih EAP protokola za provjeru identiteta,
- MIC (Message Integrity Check, pominje se i pod imenom „Michael“) za sprječavanje lažiranja paketa

WPA predviđa mogućnost provjere identiteta pomoću dijeljenih ključeva, što je pogodno za manje mreže, i pomoću RADIUS servera, što je pogodno za veće bežićne mreže. Prednost je da se može, bez većih troškova, ugraditi i u sadašnju mrežnu opremu. Dovoljno je instalirati nove pogonske programe u pristupnim točkama i klijentskim mrežnim karticama kako bi se prešlo na novi standard. Ukoliko se kupuje nova oprema važno je da ona podržava WPA.

2.1.3 WPA2

WPA2 je nova generacija Wi-Fi sigurnosti u kojoj je Wi-Fi Alliance uveo 2004. godine. WPA2 provodi Nacionalni institut za standarde i tehnologiju (NIST). Ona u odnosu na sami WPA koristi algoritam AES[7] umjesto RC4 u CBC[8] načinu rada. „AES je mnogo jača enkripcija nego TKIP koji koristi WPA. Ključevi šifriranja koji koji se koriste za svakog korisnika na mreži su jedinstveni i specifični za tog korisnika. U konačnici, svaki paket koji je poslan preko „zraka“ je šifriran s jedinstevnim ključem. Međutim, osnovni nedostatak WPA2 je neophodno ulaganje u novu mrežnu opremu koja se može osigurati funkcioniranjem algoritma AES bez većeg degradiranja performansi (Cisco, 2008).

[7] Engl. Advanced Encryption Standard – spesifikacija za šifriranje podataka koje je utemeljio Nacionalin institut za standarde i tehnologiju (NIST)
[8] Engl. Chiper Block Chaining – način rada za ulančavanje blokova šifri (šifra od predhodnog bloka otvorenog teksta koristi se za „zamagljivanje“ otvorenog teksta sljedečeg bloka, prije nego li se promijeni algoritam za šifriranje.

Ona također pruža međusobnu autentifikaciju sa Pre-Shared Key (PSK; osobni način rada) i EAP (način rada za korporacije). One se jednostavnije nazivaju WPA2-Enterprise i WPA2-Personal. Jednosmjernom autentifikacijom, korisnički uređaj šalje svoja uvjerenja i ako je pristup ovlašten, korisnički uređaj je spojen na mrežu. Međusobnu autentifikaciju zahtijeva korisnikov uređaj za provjeru mrežnog uvjerenja prije uspostavljanja veze, da bi se spriječilo povezivanje neovlaštenog korisnika. Uz WPA2, bežična tehnologija je dosegla stanje zrelosti koja omugućuje da se pruži vrhunska sigurnost za sve Wi-Fi korisnike.

WPA2-Enterprise i WPA2-Personal

WPA2 djeluje na dva načina, poslovni i osobni, ovisno o zajtevima mreže. One se nazivaju WPA2 - Enterprise i WPA2 - Personal. Jednosmjernom autentifikacijom, korisnički uređaj šalje svoja uvjerenja i ako je pristup ovlašten, korisnički uređaj je spojen na mrežu. Podrška za WPA2- Personal je obavezna u svim ovlaštenim bežičnim korisničkim uređajima i pristupnim točkama. Podrška za WPA2-Enterprise je opcija, ali preporučena je za uređaje koje rade u velikim mrežama. Posebni sigurnosni zahtjevi diktiraju način koji način rada će se koristiti u mreži. Stambene i male uredske mreže obično koriste WPA2-Personal, jer se ne zahtijeva bilo kakva oprema izvan ovlaštenih bežičnih pristupnih točka i uređaja od strane Wi-Fi CERTIFIED ™.[9]

U WPA2-Personal ključ zaštite je izveden sa mreže SSID-a i lozinkom koji unio korisnik. Potrebno je izabrati jaku lozinku kako bi se u potpunosti iskoristila zaštita WPA2 standarda. Duge, složene i slučajne zaporke su ključne za dobru sigurnost, kao i česte promjene istih. Poslovne mreže koriste više od softicirane fukcionalnosti koju pruža WPA2-Enterprise, što uključuje mogučnost za pračenje i upravljanje prometom, definicijom specifično-korisniče autentifikacije, te anonimni pristup. WPA2-Enterprise omogućuje bežični pristup da bude integriran s kontrolom ukupnog pristupa putem mreže. (Wi-Fi Alliance, 2012)

[9] Međunardoni priznati pečat odobrenja za proizvode koji ukazuju da su se upoznali i složili sa standardima za interperabilnosti, sigurnosti, i nizom primjene posebnih protokola.

2.1.4 Identifikator skupa usluga (SSID)

Standardi defirniraju i drugačiji način ograničavanja pristupa, a to je identifikator skupa usluga (engl. Service Set Identifitier, SSID). On je zapravo ime mreže koju pokriva jedna ili više pristupnih točaka. Moze sadržavati najviše 32 znakovna simbola. Svaki uređaj koji se želi povezati na našu pristupnu točku mora znati SSID. „U najčešče korišćenom načinu, pristupna točka šalje SSID u signalnom upravljačkom okviru pomoću kojega klijent može odlućiti kojoj će se mreži pridružiti“ (Pleskonjić i sur., 2007., str. 376). U drugom načinu, SSID se može iskoristiti kao sigurnosni faktor, jer se pristupne točke mogu konfigurirati tako da ne šalju SSID unutar kontrolnog okvira

Ukoliko klijet nema ispravan SSID, pristupna točka odbacuje sve kontrolne okvire koje šalje klijent i on ne može proći postupak spajanja. Iako opisani način kontrole pristupa teoretski izgleda dobro, u praksi ima značajnih problema. Naime, kako se svi kontrolni okviri ne šalju u šifriranom obliku, napadač može osluškujući komunikaciju unutar mrže – točnije, hvatajući kontrolne okvire koje šalju sve pristupne točke u komunikaciji s drugim valjanim korisnicima mreže – saznati SSID mreže i tako se neovlašteno pridružiti mreži.

2.1.5 802.1x standard

Glavni cilj 802.1x je unaprijeđenje mehanizma provjere indetiteta, čime se rješava dobar dio trenutnih problema sa sigurnošću bežičnih mreža. 802.1.x radi na MAC podsloju drugog sloja OSI modela. Osmišljen je s ciljem da omogući nadzor pristupa lokalnoj mreži kroz proces autentikacije. Podržali su ga doslovno svi proizvođači mrežne opreme i softvera. „Nije primjenjiv u WAN okruženju ili za kontrolu udaljenog pristupa, ali često se koristi u okruženju gdje je potreban javni pristup mreži putem ethernet sučelja, a posebno za autentikaciju klijenata koji se spajaju bežičnim tehnikama.“ (Nerandžić, 2005)

Klijenti se pridružuju mreži preko portova koji u okvirima standarda označavaju pridruživanje klijenata pristupnoj točki. Standard 802.1x odvaja tri etinteta: klijenta, autentifikatora i server za provjeru identiteta. Klijent (mrežna kartica klijenta) koristi usluge autentifikatora (pristupne točke) koje mu on nudi preko portova. Klijent se posredstvom autentifikatora predstavlja serveru za provjeru indetiteta (bilo koji EAP server, najšešće RADIUS) koji se nalaže autentifikatoru da moliocu dozvoli pristup mreži. Pretpostavka je da svi autentifikatori komuniciraju sa istim centralnim servisom za provjeru indentiteta.

EAP

EAP (Extensible Authentication Protocol) najvažniji je dio standarda 802.1x i služi za osnovnu primjenu različitih mehanizma za provjeru identiteta. Budući da su zahtjevi na sigurnost s vremenom povećavani, potreba za novom metodom autentikacije je postajala sve izraženija pa je kao posljedica te težnje nastao EAP protokol. On se nadograđuje na PPP protokol[10] i osigurava podlogu za implementaciju različitih autentikacijskih metoda. Kada se on kod udaljenog pristupa koristi kao autentikacijski protokol, udaljeni autentikacijski poslužitelj ne mora poznavati metodu i parametre autentikacije na lokalnom računalu. Sve potrebne podatke može dobiti kroz izmjenu EAP poruka i kroz intepretiraciju njihova sadržaja. Ovo svojstvo bitno umanjuje posao administratora pri konfiguraciji, jer podatke o postavkama lokalnih računala nije potrebno zapisivati na poslužitelj.

[10] Engl. Point-to-Point Protocol - protokol podatkovnih veza koji se koristi za izravnu vezu između dva čvora. Može osigurati autentifikaciju veze i prijenos enkripcije.

U EAP protokolu postoje četri vrste poruka:

- EAP Request – izazov koji autentifikator šalje klijentu,
- EAP Response – odgovor klijenta autentifikatoru,
- EAP Success – autentifikator prihvača klijenta,
- EAP Failure – autentifikator odbija klijenta.

EAP protokol omogućava implementaciju različitih metoda autentikacije. Čak štoviše, EAP standardom su definirane i različite metode autentikacije koje udovoljavaju specifičnim zahtjevima bežičnih mreža. Podijeljene su u dvije grupe:

Metode autentikacije temeljene na digitalnim certifikatima i TLS (engl. Transport Layer Security) protokolu:

- EAP-TLS (engl. Transport Layer Security). TLS nudi veoma siguran način provjere indetiteta; umjesto lozinke, koriste se sertifikati i infrastrukturna javnih ključeva. TLS podržava obostranu provjeru indetiteta i dinamičke WEP ključeve.
- EAP-TTLS (eng. EAP Tunnelled Transport Layer Security) TTLS proširuje TLS-a koje otklanja potrebu za klijentskim sertifikatima. Ovo je jedan od dva protokola koji podržavaju sigurni tunel preko mreže. Klijent pomoću WEP ključa s pristupnom točkom – stvara sigurnosni tunel.
- PEAP (eng. Protected Extensible Authentication Protocol). PEAP je drugi protokol koji se se koristi za za provjeru identita klijenta. Kao i TTLS, i PEAP stvara sigurnosni tunel između klijenta i pristupne točke. PEAP ne dozvoljava stare metode provjere indetiteta, već samo EAP metode.

Metode autentikacije temeljene na metodi jake zaporke ZKPP (eng. Zero Knowledge Password Proof)

- LEAP (engl. Lightweight Extensible Authentication Protocol). LEAP je razvio Cisco, za svoje proizvode su usklađeni sa standardom 802.11. Cisco je vlasnik LEAP-a i taj protokol se može ugrađivati samo u Ciscove uređaje.
- SPEAK (engl. Strong Password Exponential Key Exchange) SPEAK je autentikacijska metoda temeljena na zaporci i korisničkom imenu (kao i LEAP), ali se smatra znatno sigurnijom jer je gotovo nemoguće otkriti zaporku iz poruka koje se razmjenjuju između klijenta i poslužitelja.

EAP protokol vodi računa o nekim greškama u prijenosu i implementira mehanizam ponavljanja poruke, ali ne može ukloniti pogrešku uzrokovanu krivim redoslijedom poruka pa od transportnog sloja zahtjeva očuvanje redoslijeda poslanih i primljenih poruka. Također, EAP podržava slanje samo jednog paketa, tj. ne podržava fragmentaciju i defragmentaciju podataka, pa autentikacijske metode koje zahtijevaju prijenos podataka čija je veličina veća od one podržane EAP standardom moraju same osigurati pravilnu fragmentaciju i defragmentaciju. EAP autentikacija je inicirana od strane poslužitelja (Autentikatora) što je razlika u odnosu na većinu autentikacijskih metoda kod kojih autentikaciju inicira klijent. Za implementaciju takvih autentikacijskih metoda posredstvom EAP protokola potrebno ih je proširiti dodatnim porukama (jednom ili najviše dvije). (CARNet, 2006)

Ukoliko se EAP-om ostvaruje autentikacija temeljena na certifikatima, broj interakcija, tj. EAP poruka može biti povećan zbog potrebe fragmentacije. To može dovesti do problema u slučaju implementacije EAP-a povrh transportnog protokola koji zahtijeva ponavljanje slanja poruka jer će u tom slučaju broj poruka biti značajno povećan. U dosadašnjem razmatranju EAP je kao potporu u prijenosu podataka koristio PPP protokol, ali to nije nužan preduvjet njegovog rada.

Zbog svojih karakteristika EAP se može implementirati pored proizvoljnog transportnog protokola. Ovo svojstvo iskorišteno je za ostvarenje EAP-a u žicnim ili bežicnim LAN mrežama, gdje se komunikacija ostvaruje pored Ethernet protokola. Standard koji opisuje ovakvu realizaciju nosi oznaku 802.1x, a buduci se odnosi na EAP u LAN mrežama, još se naziva i EAP Over LAN (EAPOL).

2.1.6 802.11i standard

802.11i zaštitni standrad je zapravo omot oko 802.11 standarda. Sastoji se od komponente koje se šire u dva sloja. Najniži sloj sastoji se od dvaju poboljšanih algoritama za šifriranje:

- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
- TKIP (Temporal Key Integrity Protocol).

CCMP protokol

CCMP je protokol za šifiranje, a temelji se na AES algoritmu (Advanced Encryption Standard) i koristi takozvani CCM režim rada (Counter Mode Encryption with CBC-MAC Data Origin Authenticity). CCMP se smatara odličnim i dugotrajnim rješenjem u vezi problema zaštite podataka u bežičnim mrežama. Upotreba CCMP-a je obavezna u svim implementacijama standarda 802.11i.

Za šifriranje i zaštitu integriteta podataka u CCM režimu rada koristi se 128- bitni vremenski ključ (engl. temporal key), poznat klijentu i pristupnoj točki. CCM je specijalno dizajnirani standard 802.11i i predviđen je samo za blokovsko šifriranje, trenutno ne postoje planovi da se prilagodi protočnom šifriranju, tj. tokovima podataka.

TKIP protokol

TKIP protokol se već ranije bio spominjao, a on je osmišljen kako bi se riješili svi poznati problemi i nedostatci u WEP standardu ali i da i dalje bude kompatibilan s postoječim uređajima. To znači da bude kompaktan i da se provodi ili kao hardverska ili kao softverska nadogradnja na postoječe uređaje. Postoje tri dijela TKIP protokola a ona su: šifriranje, ponovni unos i poruke integriteta. On dinamički mijenja ključeve za vrijeme korištenja sustava. Kombinacijom dugačkog inicijalizacijskog vektora (IV) i TKIP protokola sustav se može lagano obraniti od napada kakvi se koriste za otkrivanje ključeva. Danas, uređaji koji su pod standardom zaštite 802.1i ne moraju osigurati provedbu TKIP-a.

CCMP značajno povečava nivo sigurnosti s uporedbom prema TKIP-u. Jedini nedostatak CCMP-a je to što se nemože implementirati u postojeću mrežnu opremu, nego se mora zamijenti novijom opremom, koja će biti dovoljno sposobna da pokreće AES algoritam bez značanog pada preformansi.

3. Propusti i napadi na sigurnost bežičnih mreža

Onaj tko namjerno ometa rad računalne ili bežične mreže, proces komunikacije i integritet sadržaja u mreži, nazivamo napadačem. Napadač može prisluškivati tuđu komunikaciju i time ometati povjerljivost mrežne komunikacije. Prisluškivanje obično znači kopiranje podatkovnih i upravljačkih sadržaja (paketa) koji se prenose mrežom, a takvo kopiranje može se izvoditi na usmjerivačima kroz koje ti sadržaji prolaze. Napadač može preuzimati (zaustavljati, skretati s puta) poruke koje se prenose mrežom, mijenjati njihove sadržaje i prosljeđivati poruke na adresu primatelja kojem su one izvorno upućene. Posao i cilj sustava sigurnosti i zaštite bežičnih mreža je da se spriječi nastanak problema i propusta, a za sve one vrste napada koje taj sustav ne može spriječiti, taj sustav onda to treba otkrivati.

3.1 Propusti pri provjeri indetiteta korisnika

Klijent koji želi da pristupi mreži osluškuje signal u svim frekvencijiskim opsezima i čeka upravljačke okvire koje šalju pristupne točke iz negovog dometa. Klijent bira kojoj se pristupnoj točci želi pridružiti, sa njom razmjenjuje nekoliko upravljačkih okvira i ulazi u proces pridruživanja. Ukoliko prođe kroz provjeru identiteta, klijent prelazi u drugo stanje i šalje upravljački okvir kojim zahtjeva da se pridruzi mreži. Tek kada mu pristupna točka odgovori drugim upravljačkim okvirom, on prelazi u treće stanje i konačno dobija pristup mreži. Dakle, da bi se pristupilo mreži, klijent mora prvo proći provjeru indetiteta, a to se može napraviti kroz dva načina:

- **Provjera indetiteta otvorenog sistema (engl. Open System Authentication)**

Ovaj način autentifikacije je podrazumijevani u standardu 802.11. Kako samo ime sugerira on dopušta pridruživanje mreži svakome tko to zatraži. Dakle on ne predstavlja nikakvu metodu autentifikacije.

- **Provjera indetiteta zasnovana na dijeljenoj tajni (engl. Shared Key Authentication)**

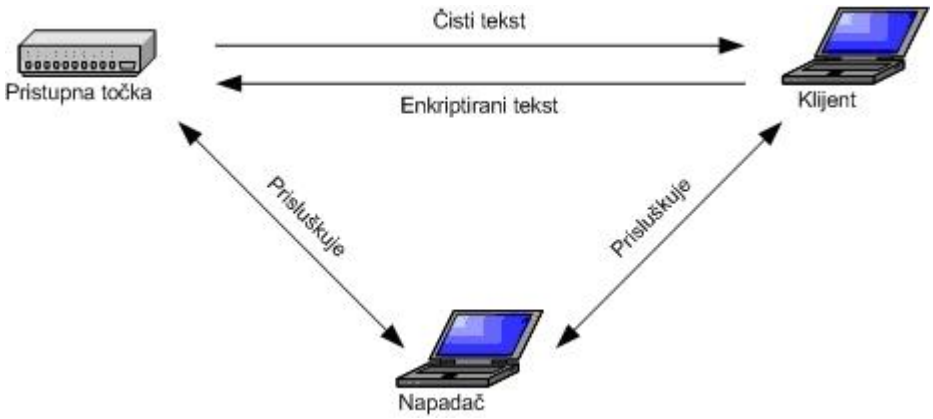
Temelji se na činjenici da obje strane u procesu autentifikacije imaju jednak dijeljeni ključ (Shared Key). Pretpostavlja da je taj ključ prenesen klijentu i pristupnoj točci sigurnim

kanalom. Pristupna točka šalje klijentu izazov koji klijent enkriptira svojim tajnim ključem i šalje natrag pristupnoj točci. Pristupna točka dekriptira primljenu poruku sa svojim tajnim ključem, koji je isti kao i kod klijenta, te ukoliko se radi o istom tekstu koji je i poslala tada je klijent prošao proces autentifikacije te se može pridružiti mreži. Ukoliko klijent želi provjeriti pristupnu točku tada on čini isto samo u obrnutom smjeru.

Ovaj način autentifikacije se nikako ne preporučuje i smatra se da je bolje koristiti otvorenu kontrolu pristupa. Razlog tome je ponovno slanje upravljačkih okvira u nekriptiranom obliku preko nesigurnog medija. Naime napadač može uhvatiti upravljačke okvire sa čistim tekstom kao i sa enkriptiranim istim tekstom i na taj način doći do ključa koji se koristio.

Napad „čovjek u sredini“

Napad „čovjek u sredini“ (engl. man-in-the-middle attack) zasnovan je na propustu u provjeri identiteta klijenta i pristupne točke. On se može iskoristiti za čitanje ili modifikaciju podataka. Napadač se postavlja između klijenta i pristupne točke i blokira njihovu komunikaciju, a zatim izvodi napad. Glavni čimbenici ovog napada su ti da napadač kada prekine komunikaciju klijenta i pristupne točke, ne dopušta da se tu ponovno uspostavi veza s pristupnom točkom, i kada klijent nastoji da uspostavi vezu, pošto ne uspijeva, postavalja vezu s napadačevim računalom koji glumi pristupnu točku. Napadač se predstavlja pristupnoj točki kao klijent i uspostavlja vezu s njom. I na takav način napadač uspostavlja dva tunela: napadač – klijent i napadač - pristupna točka.



Slika 7. Napad „čovjek u sredini“ (www.cis.hr)

3.2 Propusti u WEP standardu

Pri komunikaciji klijenta i pristupne točke podaci se šalju u obliku okvira. Sami okviri nisu enkriptirani pa je napadač u mogućnosti doći do inicijalizacijskog vektora koji je korišten u enkripciji. Poznata zamka svih enkripcijskih algoritama koji rade sa tokom podataka (stream ciphers) je to da enkripcija dviju različitih poruka istim inicijalizacijskim vektorom (IV)[11] daje informacije o samim porukama. „Ukoliko je napadaču poznata samo jedna riječ otvorenog teskta, drugu riječ može dobiti automatski. Ako otvoreni teskt sadži dovoljno metainformacija, napadač može otkriti P_1 i P_2, poznajući samo $P_1 \oplus P_2$. Za ovo postoji nekoliko tehnika. Jedna tehnika je otkrivanje tekstova koji XOR-ovanjem daju $P_1 \oplus P_2$“ (Stjepanović, Prlina, 2010.) Ukoliko imamo *n* poruka koje su kriptovane istim keystream-om, imamo problem dubine *n*. Čitanje teksta u dubinu postaje lakše kako se n povećava, pošto se XOR svakog para čistog teksta može izračunati. Za rješavanje ovih problema postoje mnoge klasične tehnike kao što je anliza frekvencije i sl.

Također što je veći broj poznatih šifriranih riječi, veća je vjerojatnost da će napadač otkriti podatke. Znači da bi napad uspio, napadač mora imati podatke šifrirane istim inicijalizacionim vektorom i mora barem dijelomično poznavati otvoreni tekst. Da bi se izbjegli ovi napadi, WEP za svaki paket koji se šifrira koristi drugi IV. Taj IV se šalje u nešifriranom obliku u sastavu podataka koji se šalju, što znači da je on poznat i napadačima. „Međutim WEP ne osigurava sigurnost od napada koji su bazirani na ponovnoj upotreni keystream-a. Jedan od razloga za ponavljanje upotrebe keystream-a je nepravilno upravljanje IV-ovima. WEP standard predlaže (ali ne zahtjeva) da se IV mijenja sa svakim paketom, ali ništa ne govori o načinu njihova izbora. U praksi se pokazalo da je kod mnogih bežičnih kartica upravljanje IV-om jako loše. Ozbiljniji propust WEP standarda su veoma kratki IV-ovi u svim implementacijama WEP standarda. Dužina IV je 24 bita, što znači da će se on sigurno ponavljati“ (Stjepanović, Prlina 2010.). Ako pretpostavimo da prosječna pristupna točka šalje pakete dužine 1500 bajtova pri prosječnoj brzini od 5Mbps, dolazi se do zaključka da će potrošiti svi IV-ovi za manje od pola dana. Ovaj propust je fundamentalan za sve WEP implementacije i ne može se izbjeći. Kada se otkriju dva šifrirna paketa koja koriste isti IV, mogu se iskoristiti mnogi napadi za otkrivanje čistog teksta, a ako je sadržaj jednog čistog teksta poznat, drugi se lako otkriva.

[11] Inicijalizacijski vektor (IV) - proizvoljan broj koji se može koristiti zajedno s tajnim ključem za šifriranje podataka.

3.3 Napadi na WEP

Postoje dvije vrste napada na WEP stanard a to su:

- **Pasivni napadi** – napadač samo prisliškuje komunikaciju korisnika s mrežom. U ove napade spadaju analiza mrežnog prometa i pasivno prisluškivanje.
- **Aktivni napadi** – napadač aktivno utječe na promet na mreži. On to može činiti na više načina primjerice može ubacivati svoje podatke, lažirati komunikaciju klijenta i pristupne točke, zagušivati promet na mreži, neovlašteno koristiti mrežne resurse. Aktivni napadi su općenito zahtjevniji za napadača jer mora uložiti veći trud, više vremena i materijalnih sredstava nego što bi trebao za pasivni napad.

Pasivni napadi

Kao što se prije navelo u pasivni napad spadaju **analiza mrežnog prometa** koja je najednoostavniji pasivni napad gdje napadač prisluškuje mrežu i prati broj i veličinu paketa u mreži. Za ovu vrstu napada napadaču je potrebna zadovoljavajuća antena, mrežna kartica koja radi u modu za slušanje i programska podrška koja će vršiti analizu veličine i broja paketa.

Ovim napadom napadač može saznati tri osnovne informacije: količinu prometa u mreži, fizičku lokaciju pristupnih točaka te vrste protokola koji se koriste na mreži. Pojava naglog povećanja prometa na mreži može poslužiti kao indikator nekog bitnog događaja. Uz usmjerenu antenu (Yagi antena) i u kombinaciji sa GPS (Global Positioning System) sustavom napadač metodom triangulacije može doći do fizičke lokacije pristupne točke ili centra bežične mreže. Informaciju o vrsti protokola napadač može dobiti brojeći pakete u vremenskom intervalu.

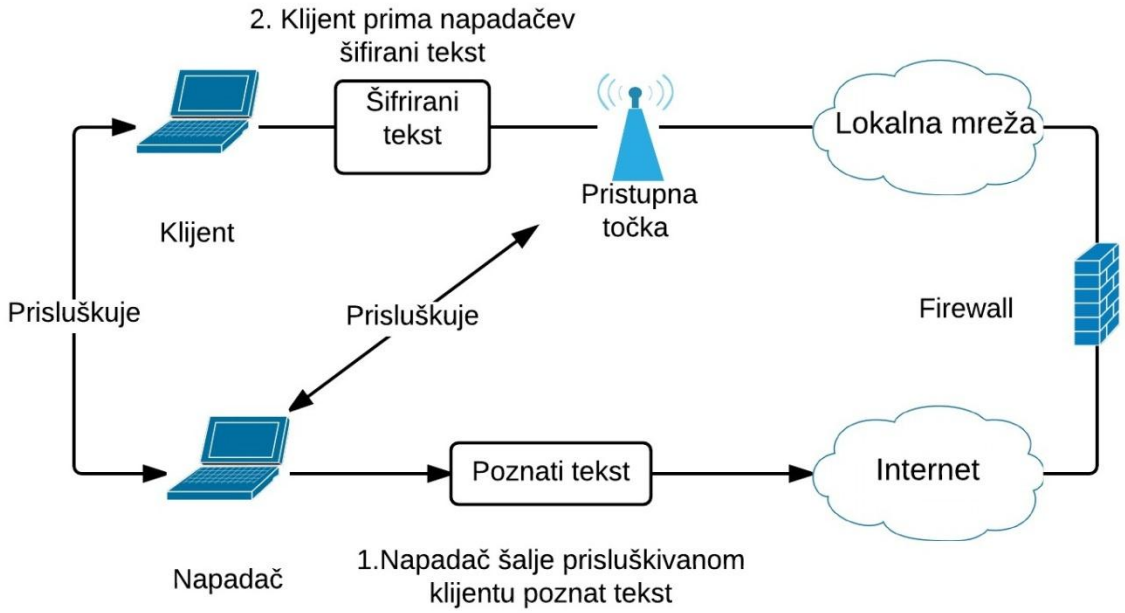
Pasivno prisluškivanje je također jednostavan napad jer napadač samo osluškuje mrežu. Jedini uvjet za uspješan napad ovoga tipa je pristup signalu mreže. Ovdje dolazi do izražaja koliko je mreža fizički zaštićena tj. koliko se vodilo računa o rasprostiranju signala pristupnih točki u prostoru. No čak ako je i mreža, fizički, dobro dizajnirana moguće je da napadač ima bolju opremu nego što standard nalaže i tako uspije dobiti pristup mreži. Standardni scenarij ide tako da napadač osluškuje mrežu i čeka da se ponovi isti inicijalizacijski vektor te tako, na ranije opisan način, dolazi do $P_1 \oplus P_2$. Nakon toga napadač, ukoliko mu je poznata jedna riječ iz para P_1, P_2 može odmah doći do druge poruke. Ukoliko napadač ne zna niti jednu poruku tada može, koristeći ranije dobivene informacije o protokolu, pretpostaviti neke konstantne dijelove poruka i tako doći do podataka.

Napad ponavaljanjem inicijalizacionog vektora

Jedan od mogućih napada na bežičnu mrežu je napad koji se zove „Napad ponavljanjem inicijalizacionog vektora (engl. IV replay attack). Njegov opis može biti ovakav:

- Napadač preko Interneta šalje poruku klijentu koga želi da napadne,
- Napadač pritom pažljivo prisluškuje mrežu i čeka da pristupna točka pošalje klijentu poruku s poznatim tekstom,
- Napadač „skida“ kriptografsku zaštitu s poruke jer mu je poznat inicijalizacioni vektor šifrirane poruke

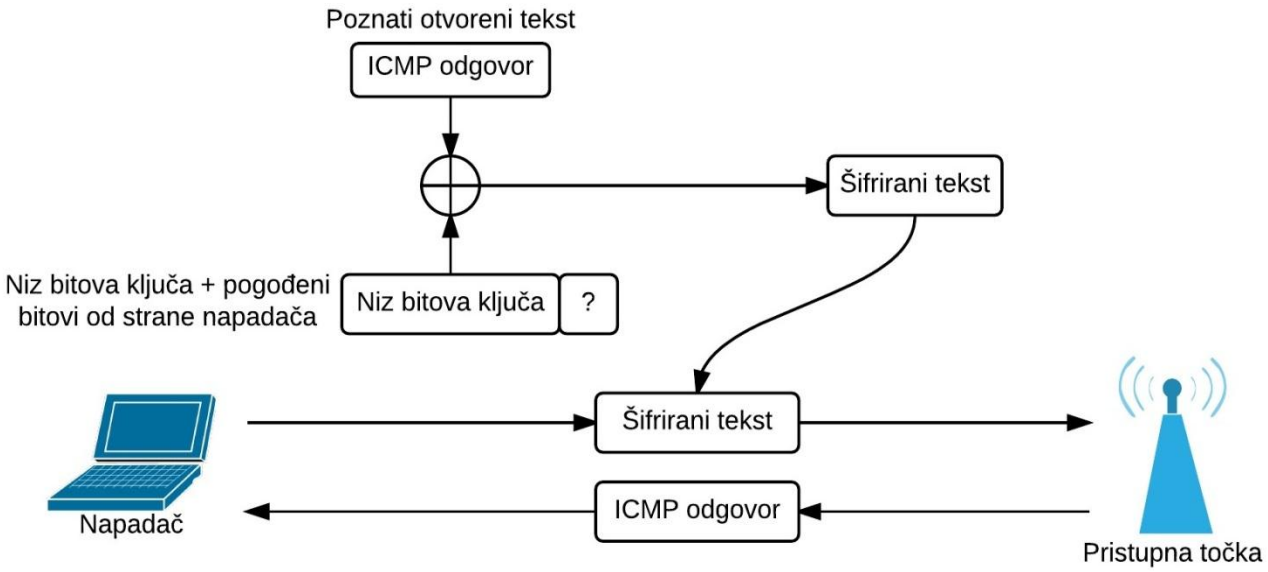
Nakon toga, napadač može dodavati svoje podatke u šifrirane pakete. Pri ovakvom napadu, osnovna pretpostavka je da se taj inicijalizacioni vektor i WEP ključ mogu ponavaljati sve dok mreža ne prihvati da je to ispravan paket. Kada napadač dobije niz bitova kojim je paket šifriran, on može taj niz primjeniti na ostale podatke koje će kasnije sam ubaciti u mrežu.



Slika 8. Napad ponavaljanjem inicijalizacionog vektora (Pleskonjič i sur. 2007. str.383)

Napad proširivanjem ključa

Napadač koji je dobio niz bitova kojim je šifrirani paket (engl. keystream) može primjeniti taj niz na druge podatke koje će sam ubaciti u mrežu. Sam proces proširivanja ključa obavalja se u nekoliko koraka. Napadač može izgraditi paket tako što će ga povećati za jedan oktet. Napadač povečava niz bitova ključa za jedan bit. Vrijednost bita dodatno se pogađa, ali to ne predstavlja problem jer postoji samo 256 mogućih vrijednosti. Kada se pogodi ispravna vrijednost okteta, napadač dobija odgovor na ICMP paket koji je poslao i tako nastavlja ovakav proces dok god ne dobije niz bitova ključa željene veličine. Ovakav proces se naziva „Napad proširivanjem ključa“.



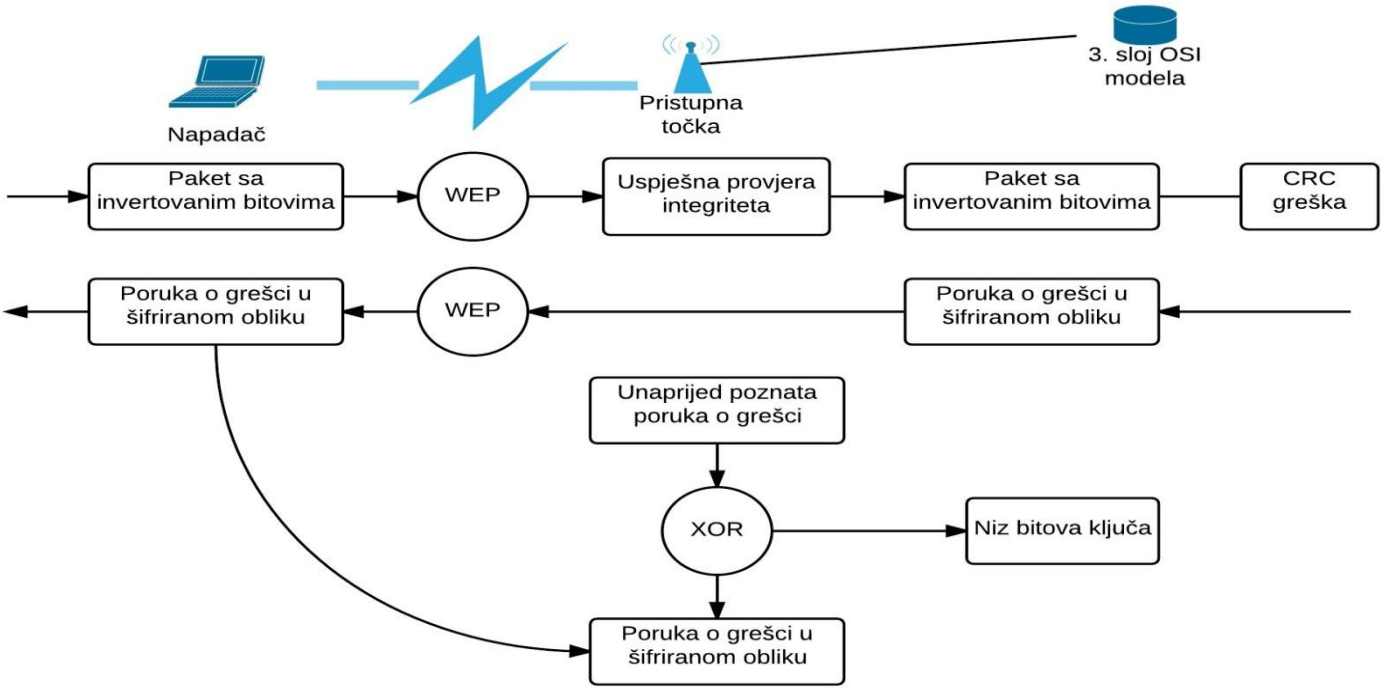
Slika 9. Napad proširivanjem ključa (Pleskonjić i sur., 2007. str. 384)

Napad obrtanjem bitova

Napad obrtanjem bitova (engl. bit-flipping attack) iskorišćuje slabost vektora integriteta poruke (ICV). Iako šifirirani paket nije fiksne dužine, mnogo elemenata se nalazi na fiksnim mjestima u paketu.

Napad se odvija:

- Prvo napadač prisluškuje okvire na mreži, uzima jedan okvir i mijenja vrijednosti nekoliko slučano odabarnih bitova unutar IP paketa koji sadrži poruku. Zatim mijenja sam sadržaj polja u kojem se nalazi ICV i šalje takav paket natrag na mrežu.
- Klijent ili pristupna točka prima paket i i račun ICV-a, zatim uspoređuje izračunatu i dobijenu vrijednost samog ICV-a, ukoliko su ta dva vektora ista, klijent ili pristupna točka prihvača izmjenjeni paket, pakira podatak i predaje ga višem, trećem sloju OSI modela. Pošto je napadač zamjenio bitove IP paketa, provjera integriteta na mrežnom sloju nije uspješna i zbog toga se generira greška.
- Napadač prisluškuje događaj na mreži očekujući širirani odgovor. Kada primi odgovor, napadač dolazi do niza bitova ključa i može ga iskoristiti za napad.



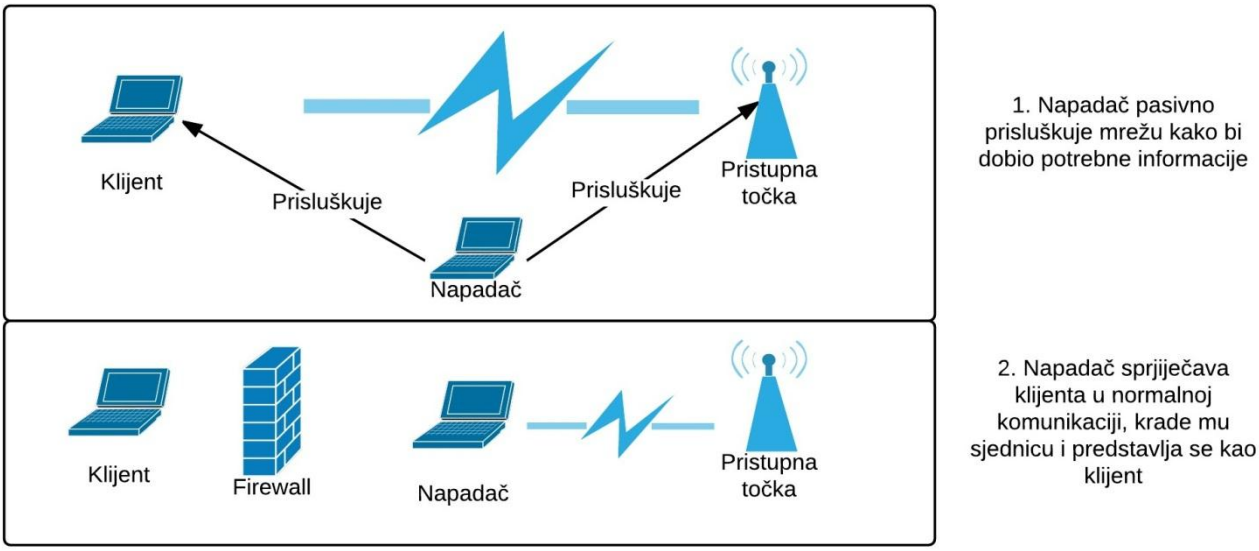
Slika 10. Napad obrtanjem bitova (Pleskonjić i sur. 2007. str. 386)

Krađa sjednice

Krađa sjednice (engl. session hijacking) je napad koji se usmjeren protiv integriteta sjednice između korisnika i pristupne točke. Napadač može ukrasti sjednicu autentificiranom i autoriziranom korisniku mreže. Meta zna da je izgubila sjednicu ali ne zna da je njezinu sjednicu preuzeo napadač i meti se to čini kao normalni ispad bežične mreže. Jednom kada je napadač uspio ukrasti klijentovu sjednicu on može nastaviti raditi u mreži proizvoljno dugo.

Za uspješan napad ovoga tipa potrebna su dva uvjeta:

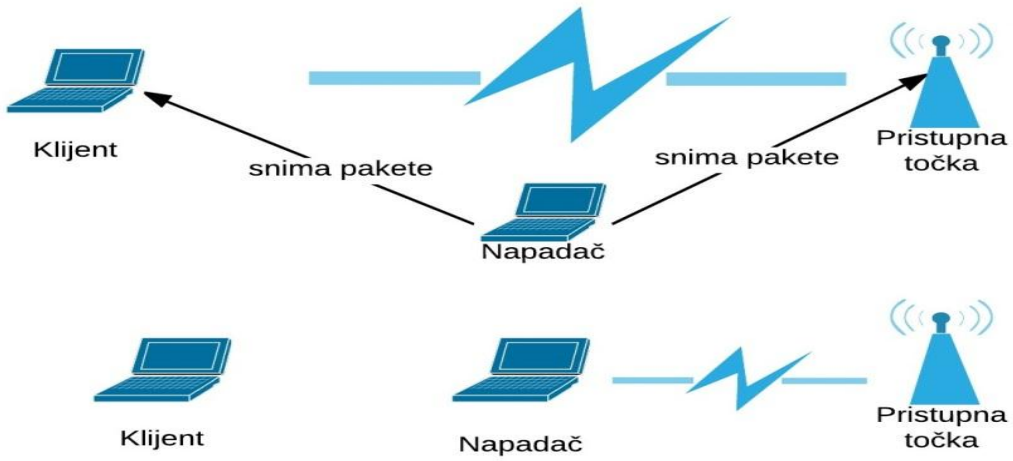
- Prvo se mora prikazati mreži kao meta da bi ga mreža uopće prihvatila. To uključuje krivotvorenje paketa višeg sloja, korištenje metode autentifikacije koju mreža koristi te primjenu zaštitne enkripcije ako mreže to zahtijeva. Ovim radnjama najčešće prethodni pasivni napad prisluškivanjem kako bi napadač doznao potrebne informacije.
- Druga potrebna radnja je sprječavanje mete u komunikaciji sa pristupnom točkom. Napadač ovu zadaću obavlja slanjem lažiranih kontrolnih okvira koji meti signaliziraju prekid trenutne sjednice.



Slika 11. Krađa sjednice (http://os2.zemris.fer.hr/)

Napad ponavljanjem paketa

Napad ponavljanjem paketa je, također, usmjeren na povredu integriteta informacija na mreži. Ovaj napad se koristi kako bi napadač dobio pristup mreži, ali za razliku od prethodnog, ničim se ne utječe na sjednice koje su u tijeku. Napad se ne odvija u realnom vremenu nego se događa nakon što je klijent završio svoju sjednicu. Napadač snima sjednicu između klijenta i pristupne točke ili više takvih sjednica kako bi ih kasnije iskoristio. Kada klijent završi svoju sjednicu napadač ponavlja njegove pakete i tako dobiva pristup mreži. Bez daljnjih sigurnosnih prepreka napadač može koristiti sve ovlasti klijenta čiju je sjednicu snimio. Čak iako napadač ne može zaobići enkripciju koja se koristi na mreži on je u mogućnosti modificirati pakete kako bi oštetio integritet podataka.



Slika 12. Napad ponavljanjem paketa (Pleskonjić i sur., 2007. str. 387)

4. Načini zaštite od napada na bežičnu mrežu

Iako se u predhodnim poglavljima govorilo o standardima zaštite, i kako pomoću njih se može dobro zaštiti mreža, to su samo standardi zaštite koji uvijek mogu biti probijeni preko različitih softverskih programa, i bilo koji malo bolji poznavaoc mreža može probiti našu mrežu u par koraka pogotovo ako se radi o WEP standardu. Zato će se u ovom poglavlju pokazati jos neki od načina koje korisnik može napraviti da bi se zaštitio, a ti načini veoma mogu biti korisni i biti od pomoći u što težem probijanju korisničkovoj bežičnoj mreži.

Korištenje Firewalla

„Vatreni zid ili vatrozid je sustav preko kojeg se odvija prijenos podataka u neku mrežu i iz te mreže. Vatrozid može poboljšati zaštitu računala od hakera koji računalu pokušavaju pristupiti putem mreže ili Interneta. To je zaštita ukoliko se dogodi da nam već netko nepozvan uspije nakaćiti na mrežu. On ima ulogu „vratiju“ koja povezuju računalnu mrežu neke tvrtke ili institucije sa Internetom. Vatrozid ima tada ulogu „vratara“ (na tim mjestima) koji dopušta neke prijenose podataka (u mrežu ili iz nje) a druge prijenose sprječava.“ Radovan (2011, str.235). Za vatrene zidove kažemo da filtriraju tokove podataka koji hoće ući u štičenu mrežu, kao i tokove podataka koji hoće izaći iz te mreže. Mreža tvrtke, institucije ili naše doma sadrži jedan usmjerivač kojeg se naziva vratima (engl. gateway) ili vratnim usmjerivačem (engl. gateway router) te mreže. Sav promet koji ulazi u štičenu mrežu ili izlazi iz nje prolazi preko vratiju mreže. Na tim vratima se nalazi vatrozid kao softverski sustav koji izvodi filtriranje prometa koji pokušava ući u mrežu i prometa koji pokušava izaći iz mreže. Filtrirati ovdje znači da vatrozid pušta neke pakete da uđu za štićenu mrežu, a druge ne pušta u mrežu.

Za rad vatrozida karakteritične su tri osnovne stvari:

- Sav promet iz vanjske mreže u štičenu mrežu, i iz štičene mreže u vanjsku mrežu, treba prolaziti preko vatrozida. Štičene mreže mogu biti različitih veličina; velike mreže mogu biti vezane na vanjsku mrežu preko više mjesta i koristiti razne vrste vatrozida. Ali da bi zaštita mreže mogla biti uspješna, potrebno je da sav promet u tu mrežu i iz nje prolazi preko barem jednog vatrozida koji je štiti.
- Administrator mreže treba postaviti na vatrozidu pravila koja određuju adrese, vrste prijenosa i vrste sadržaja onih tokova podataka koji smiju ući u štićenu mrežu, i svih

onih koje mogu izači iz nje. Vatrozid treba sprječavati sve druge tokove podataka u štičenu mrežu i iz nje.

- Vatrozid treba biti dobro zaštičen od svih vrsta napada. On je element mreže, tako da je ispostavljen svim vrstama mrežnih napada. Da bi mogao uspješno štiti onu mrežu na čijem se ulazu nalazi, vatrozid treba najprije zaštiti sebe od vanjskih napada koji mogu poremetiti njegov rad i tako ga učiniti beškonačinim, čak i štetnim.

Većina vatrozida omogućuje u postavkama da se podese postavke sigurnosti. Na prijemer možemo postaviti sigurnost na razine Low, Medium i High (niska, srednja i visoka). Ove postavke podešavaju razinu zaštite koju vatrozid pruža. Općenito govoreći, što je postavka viša, veća je zaštita. Međutim, više postavke načelno mogu smetati pri korištenju Interneta. Preoprezni vatrozidovi mogu prekidati surfanje webom, preuzimanje datoteka i druge procese koje smatramo normalnim, ali im vatrozid ne vjeruje. Niža sigurnost općenito poboljšava jednostavnost korištenja ali i povećava izloženost napadima i infiltriranju, tako da treba pronaći odgovarajuću ravnotežu.

Promjena i važnost lozinki

Korištenje neprobojne lozinke jedan je od najvažnijih koraka u zaštiti računala od hakera i drugih neželjenih korisnika. Previše je riskantno koristiti istu lozinku ili napraviti lozinke koje je lako pogoditi. Najbolje je koristiti neke nepovezane brojke i slova. U prošlosti su ljudi pamtili tako što bi si negdje napisali na papir te lozinke i to nije bio baš najbolji izbor.

Idealno je osmisliti lozinku koja ima tim veću entropiju (veći nivo nepredvidivosti ili nasumičnosti podataka), odnosno ima takva svojstva da je tipičnim metodama (brute force) za pogađanje lozinki izuzetno teško otkriti lozinku ili je to vremenski neisplativo. Iako se čini da su tipične nasumično generirane lozinke koje se sastoje od alfanumeričkih znakova i posebnih znakova izuzetno teške za probijanje, to zapravo nije potpuna istina. „Ključni parametar kvalitetne lozinke jeste njena duljina (dugačka lozinka uvijek će imati veću entropiju od kraće naizgled složenije lozinke) i to uvijek treba imati na umu pogotovo kod dodjeljivanja lozinke na servisima koji ne ograničavaju duljinu lozinki. Vodeći se time, pri izboru lozinke bolje je osloniti se na, primjerice, uzrečice, stihove ili rečenice koje se mogu lako upamtiti te tome slično. Doda li se tako osmišljenim lozinkama i zamjenski znakovi kao što brojevi i znakovi interpunkcije (na primjer, umjesto slova "i" mogao bi se staviti uskličnik), dobit će se kvalitetna lozinka koju je lako upamtiti, kasnije jednostavno mijenjati (moguće je zamijeniti redoslijed riječi u rečenici ili slično) i koju je iznimno teško probiti.“ (Gračanin, 2014).

MAC filtriranje

Jedan od mehanizama koji se koristi za zaštitu od neovlaštenog pristupa jeste dozvoljavanje pristupa samo onim klijentima koji imaju MAC (engl. Media Access Control) adresu zabilježenu u evidenciji bazne stanice, tj. pristupne točke. MAC sadrži dvije informacije: identifikacijski broj proizvođača i oznaku uređaja u seriji. „MAC adresa je jedinstveni broj koji se dodjeljuje svakoj kartici mrežnog sučelja (Network Interface Card – NIC) – ne postoje dva NIC-a s istim brojem. NIC, koji se ponekad naziva i Ethernet kartica, koristi se za spajanje računala na računalne mreže.“ (Murray i Weafer, 2005., str. 180).

Svaki uređaj spojen na mrežu posjeduje fizičku adresu zapisanu u njegovom ROM-u, a koja se sastoji od 12 heksadecimalnih znakova od kojih prva četiri označavaju ime proizvođača, dok ostatak predstavlja model i serijski broj uređaja. Većina danas dostupnih pristupnih točaka sadrži algoritam zaštite putem filtriranja MAC adresa koji administrator tako podesi da samo računala sa određenom MAC adresom mu mogu pristupiti. Iako ovakav način zaštite može na prvi pogled djelovati siguran s obzirom da su podaci o MAC adresama zapisani u ROM-u uređaja, danas postoje softverski alati (primjerice Soft MAC) koji omogućava dodjeljivanje MAC adrese po želji mrežnom adapteru. S tim u vidu, samostalno korištenje MAC filtriranja ne predstavlja preveliku prepreku za hakere. Budući da je svaka MAC adresa jedisntvena, MAC filtriranje je efikasan način blokiranja pristupa nepoznatih računala bežičnoj mreži. Međutim takva adresa može se izmjeniti ili lažirati pomoću odgovarajućih alata.

Statičko IP adresiranje

Mnogi današnji sustavi koriste DHCP (Dynamic Host Configuration Protocol) servere za dinamičko dodjeljivanje IP adresa računalima čim se spoje na mrežu. Iako ovakav način adresiranja uvelike olakšava posao IT osoblju, kao i korisnicima, olakšava upad i neautoriziranim korisnicima čime se sigurnost sustava može dodatno ugroziti. Isključivanjem funkcije DHCP servera na router-u, te ručnim podešenjem IP adresa opasnost od pada se može dodatno smanjiti. Smanjenjem vrijednosti subnet-a na najmanju moguću vrijednost možemo dodatno povećati sigurnost jer je broj mogućih IPadresa manji, a sve ostale su zabranjene putem vatrozida.

5. Probijanje WEP zaštite (praktični dio)

U predhodnim poglavljima objasnili smo zašto WEP zaštita nije toliko dobra, i da je bolje imati zaštite tipa WPA ili WPA2 jer su bolje podtkovane, a samim time teže ih je za probiti, iako nije nemoguće, samo za razliku od probijanja WEP enkripcije treba dosta više vremena. Svi znamo da hakiranje, napadanje tuđih lozinka nije legalna aktivnost i da su kazne veoma drastične, zato se u ovom praktičnom radu prikazaj napad na kućnu mrežu od samog autora.

Općenito o alatima za napadanje

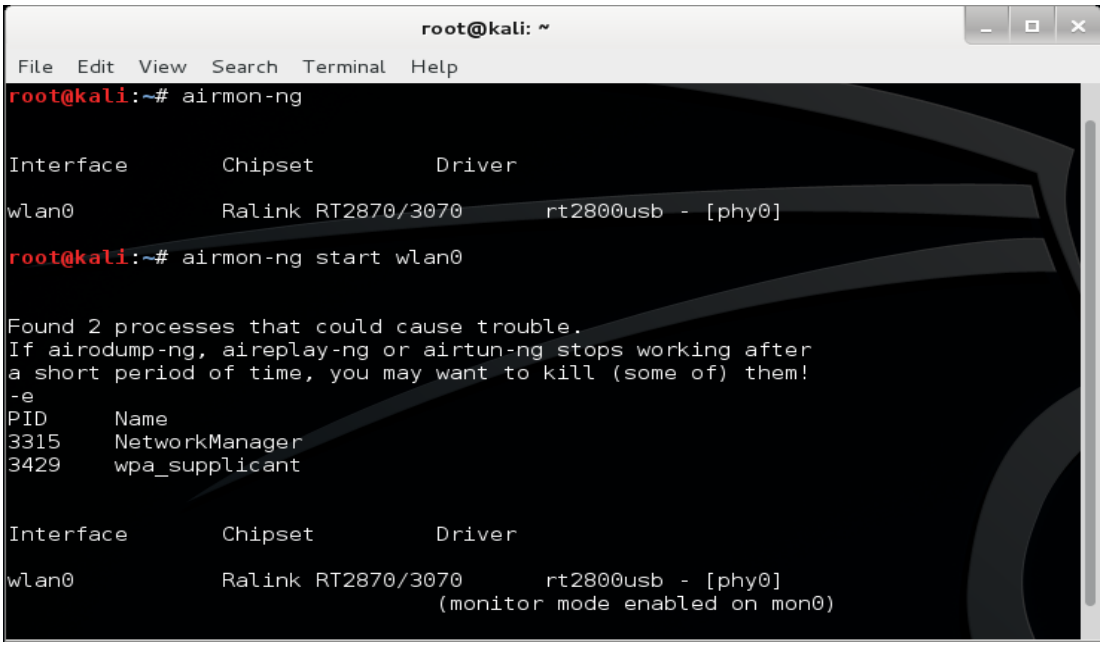
Za probijane bežične mreže i njezine sigurnosti, danas se koristi mnoštvo alata. „Alati koji mogu razbiti WEP zaštitu, koji koriste slabosti inicijalizacionog vektora (IV) zovu se FMS alati. Jedan od privih takvih alata je Airsnort. Airsnosrt osluškuje mrežu i kada sakupi dovoljno šifrovanih paketa (oko 5-10 miliona paketa) generira WEP ključ za vrlo kratko vrijeme (manje od 1 sekunde na prosječnom PC računalu)“ (Pleskonjić i sur. 2007). Također slični programi kao Airsnort su WEPCrack i AirCrack kao i alat Weplab koji kombinira više različitih vrsta napada (napad grubom silom, riječnikom, FMS metodom) sa cijeljem otrkivanja WEP ključa. Ali jedan od najboljih alata za probijanje jest Linuxova distribucija Kali.

Kali Linux je distribucija koja služi za napredno ispitivanje penetracije, tj. proboja i sigurnosti i sadrži veliki broj alata koje možemo upotrijebiti za provjeru sigurnosti naše bežične mreže. Ova distribucija je zasnovana prema prijašnjoj distribuciji BackTrack uz pridržavanje Debianovih razvojnih standarda. Kali Linux sadrži više od 300 alata za provjeru sigurnosti. Kali Linux snažno podržava otvoreni kod, besplatan je, njihovo razvojno stablo je dostupno svima na uvid i svatko može pristupiti izvornom kodu, te mijenjati i prilogođavati pakete svojim potrebama. Kali je razvijan uz pridržavanje standarda hijerarhije datotečnog sustava (engl. Filesystem Hierarchy Standard, FHS). To znači da svi korisnici Linuxa mogu jednostavno pronaći dijelove datotečnog sustava. Primjer tom problemu je kad pokušavamo podesiti instalirani ili instalirati novi paket. U distribuciji je podržan veliki broj bežičnih uređaja. Kompatibilan je s različitim USB i sličnim bežičnim uređajima. To je napravljeno iz razloga da ga je moguće koristiti kao alat za testiranje na što većem broju hardverskih platformi. Iako je većina alata i dokumentacije napisano na engleskom, Kali Linux podržava višejezičnost, ukoliko nepoznavanje engleskog nekome predstavlja problem.

Za probijanje mreže u ovom radu koristila se upravo Kali Linux distribucija i ovo je prikaz probijanja autorove WEP zaštite kroz par koraka:

1. Otvaranje root terminala i provjera bežične kartice

Ovaj postupak nije toliko bitan, ali dobro ga je znati. Prvo se otvori root terminal (u distribuciji ih ima dva, običan terminal kao primjerice u UbuntuLinux i root terminal). Zatim se upiše prva naredba **airmon-ng** kako bih se provjerila bežična kartica i koji je trenutni driver na njoj u slučaju potrebe novog ažuriranja. A druga naredba je **airmon-ng start wlan0** koja opisuje kako staviti svoje sučelje u mod monitora, te na slici vidimo da je taj monitor mod omogućen na mon0 što je ključna riječ koju ćemo koristiti u svim ostalim naredbama jer bez nje ne, nebi imali prikaz ostavernog procesa.

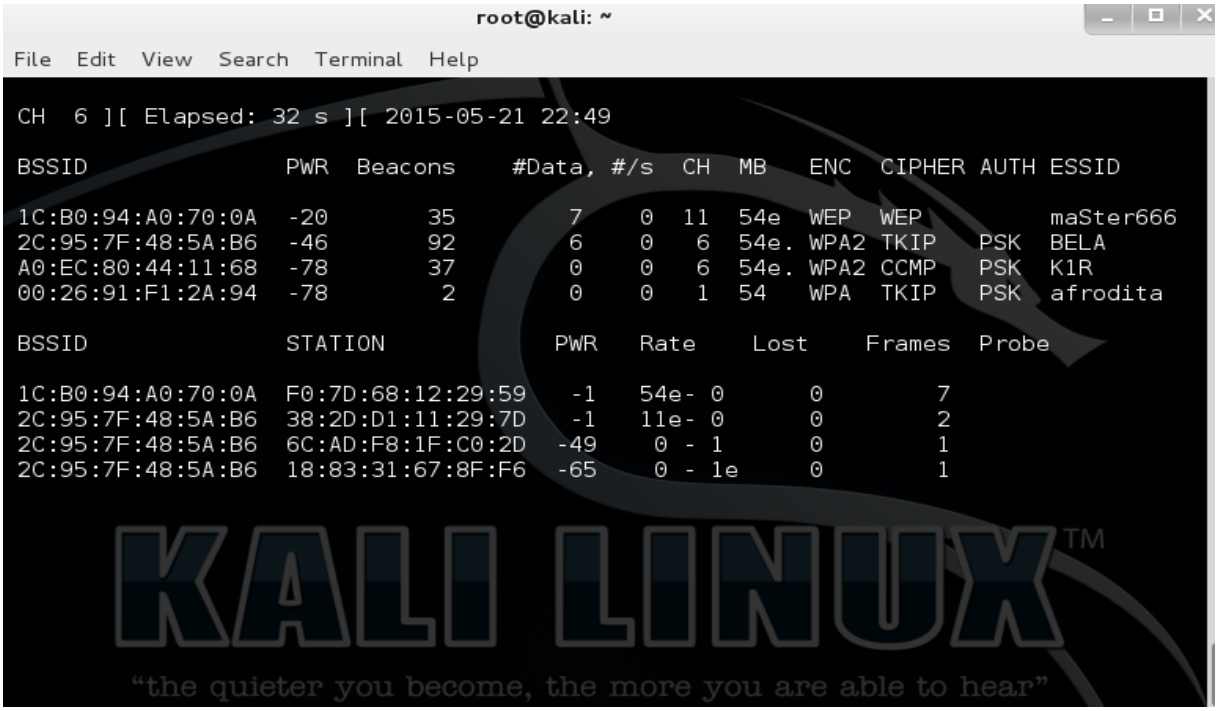


Slika 13. Prikaz bežične kartice i monitor mod-a (Izvor: Autor)

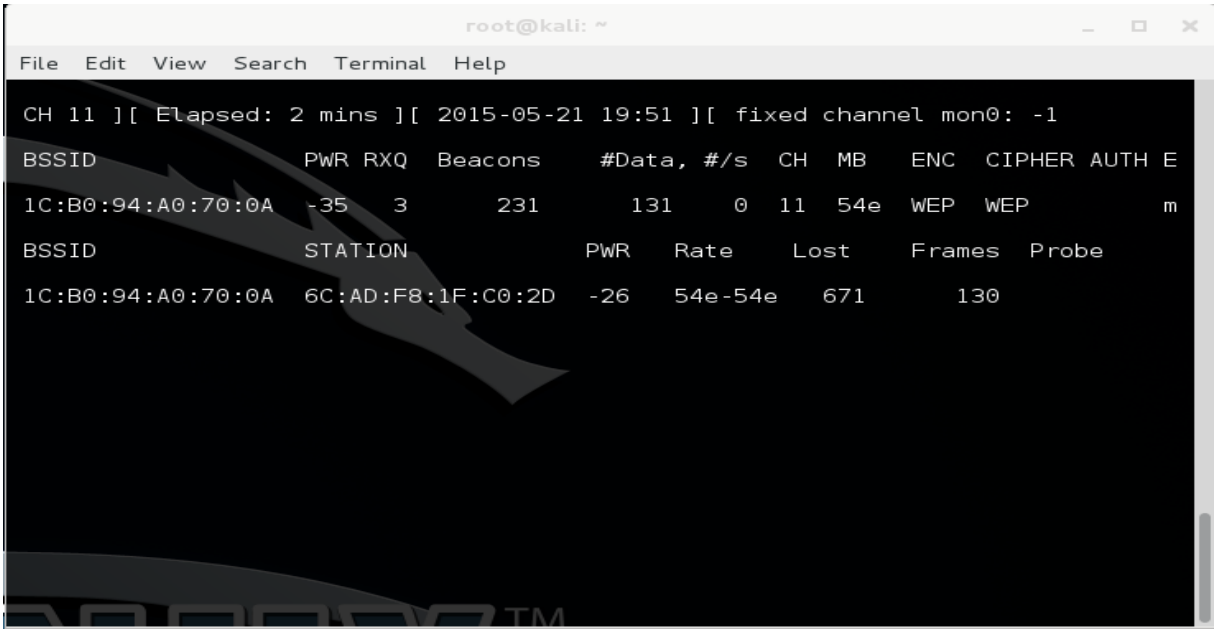
2. Prikaz svih dostupnih pristupnih točaka

U drugom koraku s naredbom **airodump-ng mon0** prikazuju se sve dostupne pristupne točke koju je naša mrežna kartica uspijela pronaći, naravno što je signal jači i veći to se više i pristupnih točki može pronaći. U ovom primjeru ih ima četri, u nekoj zgradi će ih biti mnogo više, naravno. Vidimo sav opis i dole je navedeno tko sve trenutno koristi čiju pristupnu

točku, nas zanima pristupna točka „maSter666“ koja ima WEP enkripciju. Zatim slijedi naredba s kojom ćemo tu našu pristupnu točku „izvući“ iz ovih četri navedenih mreža, tako da imamo pregled samo na nju i procese koje se vrte oko nje. A to „izvlačenje“ radimo naredbom airodump-ng –w (ime pristupne točke, tj. SSID) – c (broj kanala u kojem se nalazi, u našem slučaju to je 11) - - bssid (MAC adresa pristupne točke, 1C: B0 : 94 : A0 : 70 :0A) mon0. Prikaz možemo vidjeti na sljedečim slikama.



Slika 14. Prikaz svih dostupnih pristupnih točaka (Izvor: Autor)



Slika 15. Prikaz određene pristupne točke (Izvor: Autor)

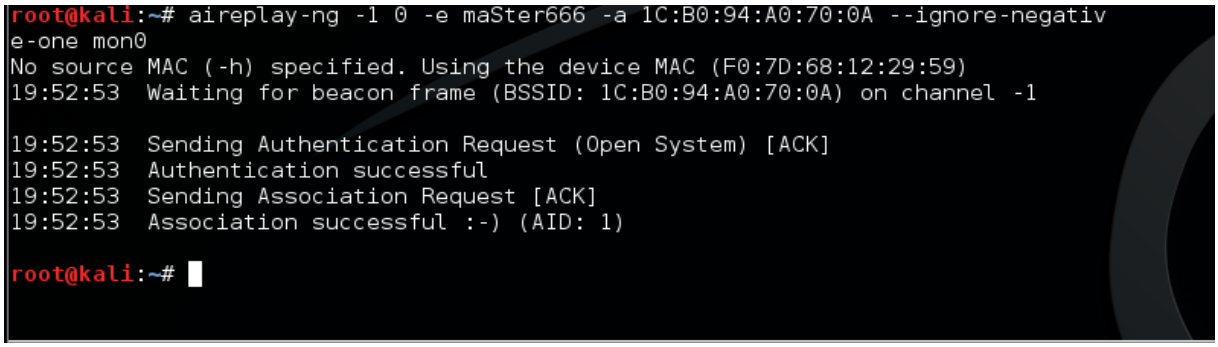
3. Lažna autentifikacija

Postoje mnoge vrste napada na WEP, ovdje se koristio napad lažne autentifikacije. Lažni autentifikacijski napad omogućuje izvođenje dvije vrste WEP autentikacije (otvoreni sustav autentifikacije i dijeljenih ključeva) uz pomoć pristupne točke. Naredba za ovakav napad je:

- aireplay-ng -1 0 – e maSter666 –a 1C: B0 : 94 : A0 : 70 :0A mon0.

Značenje:

- -1 znači autentifikacija,
- 0 vremenska odgoda u sekundama,
- -e ime mreže
- -a MAC adresa pristupne točke

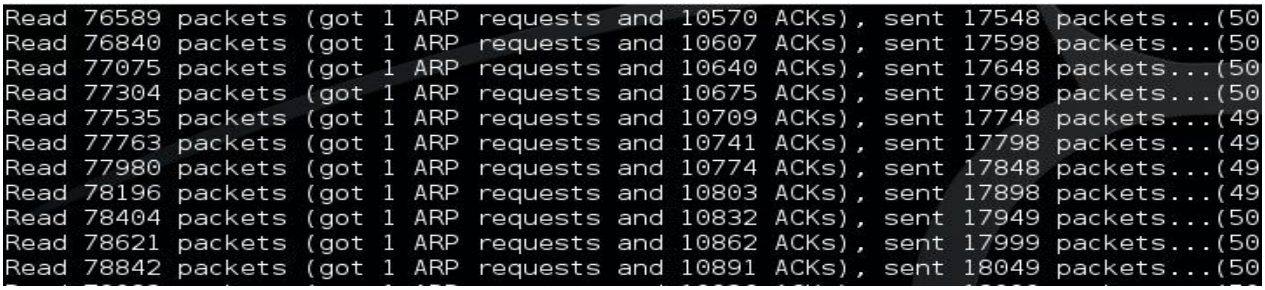


Slika 16. Napad lažnom autentifikacijom (Izvor: Autor)

4. Slanje ARP zahtjeva

ARP (Address Resolution Protocol) omogućuje dinamičko povezivanje IP adresa sa odgovarajućim MAC adresama (i obrnuto) u jednoj lokalnoj mreži. ARP je vrlo jednostavan protokol koji se sastoji od četiri vrste poruka: ARP zahtjev, ARP odgovor, obrnuti ARP zahtjev ili RARP (eng. Reverse ARP Request) te RARP odgovor. Napadač veže svoju MAC adresu s nekom IP adresom koju ostali uređaji u lokalnoj mreži koriste. Na taj način preusmjerava sav promet prema toj IP adresi na svoje računalo. I jednom kad ti podaci dođu do nas moguće je vidjeti korisnikovu lozinku kao u ovom slučaju. Ovako to izgleda kad upišemo naredbu : **aireplay-ng -3 –e maSter666 –b 1C: B0 : 94 : A0 : 70 :0A mon0.** U tom dijelu moramo čekati dok se ne skupi dovoljno podataka da bi sam napad bio uspješan. Potrebno je gledati u sliku 15. jer u njoj bi se nakon ovog postupka treba znatno podići broj u #data, i kad on bude preko 10 000 otprilike tad bi se trebalo znati dali smo uspijeli.

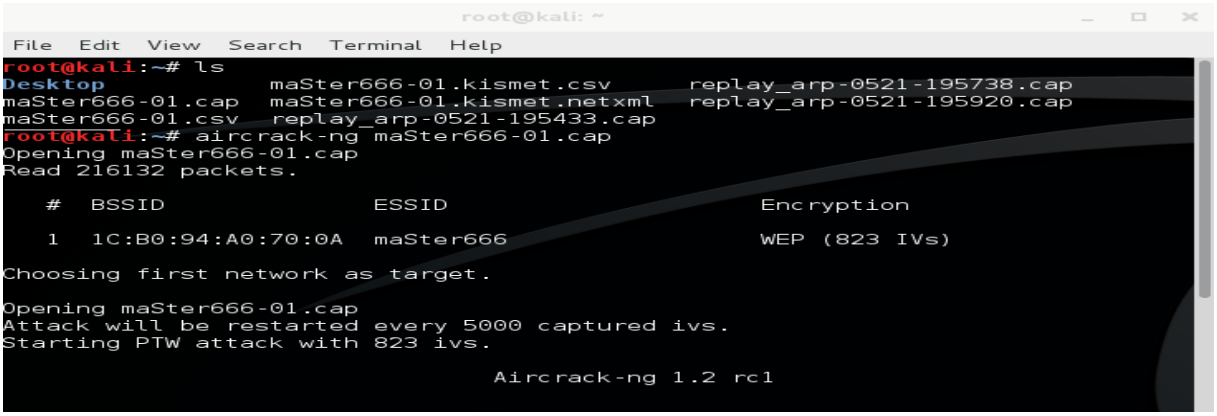
Za ovaj proces potrebno je nekome više, a nekome malo manje vremena ovisno o jačini mreže. Prikaz možemo vidjeti na sljedećoj slici:



Slika 17. Prikaz slanja ARP zahjteva (Izvor: Autor)

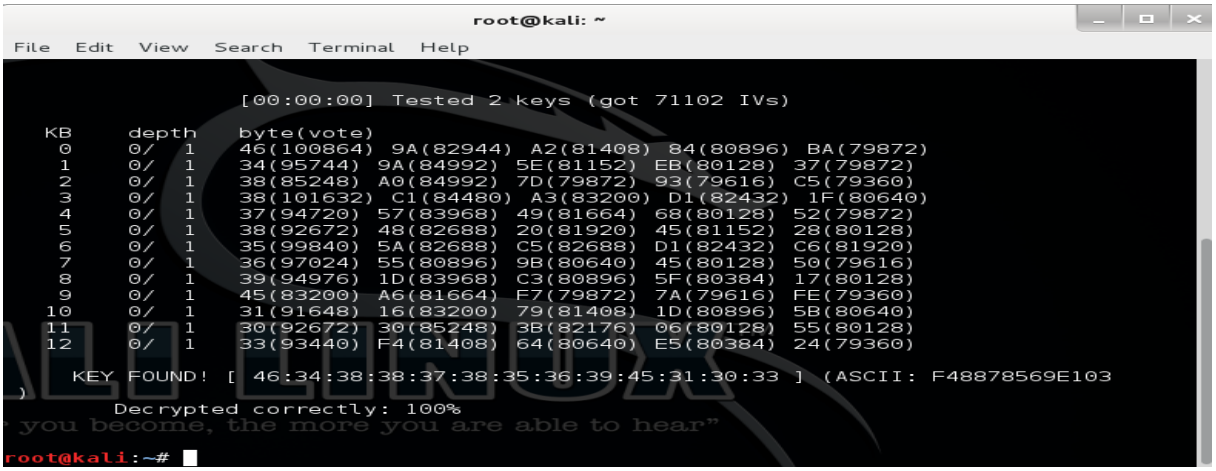
5. Provjera uspješnosti napada

U terminalu upisujemo ls i time dobivamo imena fajlova u kojem bi se trebao nalazit naš ključ. Takav fajl završava sa .cap ekstenzijom kao što vidimo na slici.



Slika 18. (Izvor: Autor)

Za kraj upsuijemo naredbu **aircrack-ng maSter-01.cap** i ako je napad uspješan prikazat će nam se naša dobivena lozinka, a ako ne dobijemo rješenje, to znači da je potrebno čekati jos malo dok se podaci ne povečaju i bude više od 10 000 (#data).



Slika 19. Uspješan napad i pronalazak ključa (Izvor: Autor)

6. Zaključak

Bežične mrežne tehnologije sigurno su odličan oblik sadašnjice ali i buduće mrežne komunikacije i tehnologije koja već je u ogromnom postotku zamjenila žičnu mrežu, odnosno LAN kabel. Ali za razliku od žične mreže kod bežičnih mreža najveći problem je svakako njihova sigurnost i rizik koja ona donosi. Sigurnost je veoma bitna stavka, i zato je određena mnogim standardima zaštite, i u odnosu na statičku WEP zaštitu upoznali smo i mnoge druge koje su tu da bi jos više poboljšale zaštitu ali i eliminirale sigurnosne nedostatke. Na novim standardima stalno se radi, oprema postaje bolja, a i sustavi zaštite napreduju. Ali same bežične mreže dodatno su izložene i interesantnije napadačima baš zbog neadekvatnog stupnja zaštite kao što sam pokazao u praktičnom dijelu ovog rada koji pokazuje da ne treba mnogo informatičkog znanja da bi se probila zaštita bežične mreže, radilo se naravno o WEP standardu zaštite ali i druge standarde je moguće probiti samo treba više vremena i strpljenja. Preporuke kako bi se još moglo osigurati je ta da koristimo MAC filtriranje, poželjno je pri konifuraciji usmjerivača uključiti filter koji omogućava samo određenim MAC adresama da se spoje na mrežu, budući da je svaka MAC adresa jedinstvena, MAC filtriranje je efikasan način blokiranja pristupa nepoznatih računala bežičnoj mreži, također trebalo bi obratiti pažnju na samo postavljanje usmjerivača tj. pristupne točke, jer postavljanjem pristupne točke bliže središtu kuće možemo ograničiti područje koje pokriva bežični signal i tako smanjiti izlaznu snagu uređaju (transmit power). Naravno uz sve navedno potrebno je ponovno naglasiti ulogu vatrozida koji može poboljšati zaštitu računala od neovlaštenih napada.

7. Literatura

Knjige:

1. Ilišević S. (2003). Brzi vodič kroz kućne mreže,(str 29-32) SysPrint, Zagreb

2. Gast M. (2002). 802.11 Wireless Networks: The Definitive Guide, (str. 14-15) O'Reilly

3. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M. (2007). Sigurnost računarnih sistema i mreža (str.376-400), Mikro knjiga, Beograd

4. Murray, A., Weafer, V. (2005). SIGURNI NA INTERNETU: Praktičan vodić kroz siguran rad na Internetu kod kuće, (str-175-181) Symatec Corporation

5. Radovan M. (2011). Računalne mreže 2, (str.253-255) Digital point tiskara d.o.o., Rijeka

Internet:

1. How-to Geek (2014). < http://www.howtogeek.com/180649/htg-explains-whats-the-difference-between-ad-hoc-and-infrastructure-mode/>. Pristupljeno 18.travnja 2015.

2. Cisco (2008). <http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html?mdfid=279537740 >. Pristupljeno 20. travnja 2015.

3. Wi-Fi Alliance (2012). < http://www.wi-fi.org/file/the-state-of-wi-fi-security-wi-fi-certified-wpa2-delivers-advanced-security-to-homes>. Pristupljeno 21. travnja 2015.

4. Nerandžić, D. (2005). Ranjivost standarda 802.1x u žičanom okruženju, < http://sistemac-arhiva.srce.hr/index.php%3F%26id%3D89%26backPID%3D91%26begin_at%3D85%26tt_news%3D386%26cHash%3Dcd16d600ef.html>. Pristupljeno 4. Svibnja 2015.

5. Carnet (2006). Autentikacija u bežičnim mrežama, <http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-170.pdf>. Pristpljeno 8. Svibnja 2015.

6. Stjepanović, D., Prlina G. (2010). Sigurnosni propusti Wep protokola, str. 1014-1015, <http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-170.pdf>. Pristupljeno 13. Svibnja 2015.

7. Gračanin, M. (2014). Sve o lozinkama i kako biti siguran < http://www.svet-bezbednosti.rs/sr/clanak/2014/9/sve-o-lozinkama-i-kako-biti-siguran,448,14646.html>. Pristupljeno 15. Svibnja 2015.