HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost bežičnih LAN-ova

CCERT-PUBDOC-2003-05-22

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Bežične tehnologije zadnjih godina zauzimaju bitno mjesto u svakodnevnom životu i poslu. Korištenje prednosti bežičnih uređaja, poput njihove mobilnosti i pripadnosti pojedinom korisniku, zajedno s integriranjem naprednih tehnologija poput globalnog pozicioniranja (GPS), učinili su razvoj bežičnih uređaja područjem s velikim rastom. Usluge poput korištenja ručnih računala (engl. *Personal digital assistant PDA*), koja omogućavaju pojedincima pristup njihovim adresarima, kalendaru, praćenju poruka elektroničke pošte ili pristup Web sadržajima, utječu na rast popularnosti.
Povećanjem broja ustanova, poduzeća i pojedinaca koji koriste bežične uređaje rastu interes i za opasnosti za sigurnosne rizike koja ta tehnologija nosi. U ovom dokumentu je opisana IEEE 802.11 bežična tehnologija, dan kratak pregled pridruženih rizika i upute za njihovo smanjenje.

1.1. Namjena i opseg dokumenta

Namjena ovog dokumenta je izrada uputa za povećanje sigurnosti bežičnih mreža. U dokumentu su obuhvaćene lokalne računalne mreže i bežične (WLAN) mreže. Tehnologije poput bežičnog radija, mobilnih mreža (GSM, GPRS, EDGE, UMTS), *Bluetooth* tehnologije i ostalih WLAN tehnologija, koje nisu definirane IEEE 802.11 standardom, nisu obuhvaćene u ovom dokumentu.
Bežične tehnologije se brzo mijenjaju. Novi proizvodi i svojstva se uvode kontinuirano. Mnogi od tih proizvoda sadrže i sigurnosna svojstva dizajnirana za uklanjanje postojećih slabosti. No s novim mogućnostima, pojavljuju se nove prijetnje i ranjivosti. Zbog brzog razvoja bežičnih tehnologija bitno je pratiti trendove u tehnologiji i sigurnosti odnosno nesigurnosti tih tehnologija.

1.2. Struktura dokumenta

Dokument se sastoji od slijedećih poglavlja:

- Poglavlje 1 se sastoji od namjene, opsega i strukture dokumenta,
- Poglavlje 2 omogućava pregled bežičnih tehnologija,
- Poglavlje 3 daje pregled 802.11 WLAN tehnologija, njihovih sigurnosnih rizika i uputa njihovo smanjene,
- Poglavlje 4 sadrži zaključak,
- Poglavlje 5 se sastoji od popisa kratica.

2. Pregled bežičnih tehnologija

Bežične tehnologije omogućavaju komunikaciju više uređaja bez fizičke povezanosti. Ove tehnologije koriste prijenos radio valovima. Bežične tehnologije uključuju bežične lokalne mreže (WLAN), mobilne telefone i jednostavne uređaje poput bežičnih slušalica, mikrofona i drugih, koji obrađuju ili spremaju informacije. Uključeni su i infracrveni uređaji poput daljinskih upravljača, bežičnih tipkovnica i miševa, bežičnih naglavnih slušalica kao i svega ostalog što zahtjeva direktnu vidljivost između prijemnika i predajnika. U ovom poglavlju je dan kratak pregled bežičnih mreža, uređaja, standarda i njihovih sigurnosnih karakteristika.

2.1. Bežične mreže

Bežične mreže služe kao prijenosni mehanizam između pojedinih uređaja te uređaja i fiksnih mreža. Na osnovu područja pokrivenosti bežične mreže mogu se podijeliti u tri grupe:

- Bežične mreže širokog područja (engl. *wireless wide area network* WWAN). Obuhvaća tehnologije sa širokim područjem pokrivenosti poput mobilnih mreža, radio i satelitskih mreža.
- Bežične lokalne mreže. Obuhvaća 802.11, HiperLAN i druge tehnologije,
- Bežične osobne mreže (engl. *wireless personal area network* PAN). Obuhvaća tehnologija poput *Bluetootha* i infracrvenih mreža.

Za prijenos u bežičnim mrežama se koriste elektromagnetski valovi područja od radio frekvencija (RF) do pojasa iznad infracrvenog (IC) spektra. U ovom dokumentu bavimo se samo s lokalnim mrežama.
Po načinu povezivanja uređaja bežične mreže možemo podijeliti u dvije skupine:

- Mreže u kojima se uređaji međusobno povezuju preko pristupnih točaka ili baznih stanica,
- Mreže u kojima se dva uređaja direktno povezuju. Takve mreže se u literaturi nazivaju *ad hoc* ili *peer to peer* mreže.

Pojedine mrežne tehnologije, poput 802.11, omogućavaju oba načina povezivanja.

2.1.1. Bežični LAN-ovi

Bežične LAN mreže imaju veću fleksibilnost nego fiksne LAN mreže. Tradicionalni LAN-ovi zahtijevaju kabelsko povezivanje računala s mrežom. Kod bežičnih mreža dovoljna je pristupna točka (engl. *access point*). Pristupna točka je kabelom spojena na fiksnu mrežu, dok je s druge strane preko antena povezana s uređajima s bežičnim mrežnim karticama. Unutar otvorenog prostora pristupne točke pokrivaju udaljenosti do sto metara, dok u zatvorenom ta vrijednost pada na 30 metara. Područje pokrivenosti se obično naziva ćelija. Korisnici se slobodno kreću unutar ćelija s njihovim prijenosnikom ili drugim mrežnim uređajem. Ćelije pristupnih točaka mogu biti povezane na način da omoguće korisnicima "*roaming*" unutar ili između građevina.

2.2. Bežični standardi

Bežične tehnologije su prilagođene različitim standardima i nude različite razine sigurnosnih svojstava. Ovaj dokument se ograničava na IEEE 802.11 standarde.

2.2.1. IEEE 802.11

Originalni 802.11 standard je dizajniran za brzine prijenosa od 1 Mbit/s do 2 Mbit/s. No danas su, ovisno o tehnologiji i brzini prijenosa, definirana tri standarda:

- 802.11a standard koji radi u frekvencijskom pojasu od 5 GHz i podržava brzine prijenosa do 54 Mbit/s,
- 802.11b standard koji radi u frekvencijskom pojasu od 2,4-2,48 GHz i podržava brzine prijenosa do 11 Mbit/s,
- 802.11g (još uvijek u probnoj verziji) standard koji radi u frekvencijskom pojasu od 2,4 –2,48 GHz i podržava brzine prijenosa do 54 Mbit/s.

Trenutno dominantan standard na tržištu je 802.11b, no u zadnje vrijeme velik broj proizvođača nudi uređaje s podržanim 802.11g probnim standardom. Prednost "b" i "g" standarda pred "a" je u tome što rade u pojasu za koji diljem svijeta nije potrebno tražiti licencu. Iako je i pojas od 5 GHz u velikom broju zemalja slobodan, u Europi njegovo korištenje nije dozvoljeno.

Dva druga važna standarda za bežične LAN-ove su 802.1x i 802.11i. IEEE 802.1x, protokol za kontrolu pristupa, omogućava sigurnosni okvir za IEEE mreže, uključujući Ethernet i bežične mreže. 802.11i standard, koji je također u probnoj verziji, je kreiran za specifične bežične sigurnosne funkcije koje rade s IEEE 802.1x. 802.11i je opširnije objašnjen u poglavlju 3.5.

2.3. Bežične sigurnosne prijetnje i umanjivanje rizika

Sve sigurnosne prijetnje definirane za fiksne mreže su potencijalne prijetnje i u bežičnim mrežama. Dapače, bežične mreže su zbog svojih svojstava više izložene. Krađe bežičnih uređaja su mnogo češće zbog njihove prenosivosti. Nadalje, za razliku od fiksnih mreža, bežične mreže su podložne vanjskim upadima zbog toga što je nemoguće signal ograničiti na područje gdje je fizički smještena organizacija, poduzeće ili kuća vlasnika. Maliciozni korisnici mogu dobiti pristup mreži prisluškivanjem komunikacije i jednostavnim programima za probijanje enkripcije.

Ukupan rizik u bežičnim mrežama je jednak sumi rizika u fiksnim mreža plus novi rizici, specifični za bežične mreže. Za smanjene tih rizika potrebno je usvojiti sigurnosna mjerenja i procedure koje donose rizike na upravljački nivo. Na primjer, prije postavljanja bežične mreže potrebno je odrediti prijetnje i ranjivosti koje će bežična mreža unijeti u postojeće okružje. Prilikom procjene potrebno je uzeti u obzir postojeće sigurnosne politike, poznate prijetnje i ranjivosti, zakone i pravilnike, pouzdanost, performanse sustava, procjenu troškova sigurnosnog praćenja i mjerenja i tehničke zahtjeve. Prema rezultatima procjene potrebno je zatim napraviti plan implementacije. Nakon uspostave sustava, potrebna je periodička procjena politika i praćenje zbog kontinuiranog razvoja

tehnologije i malicioznih prijetnji. Donja lista daje popis izraženijih prijetnji i ranjivosti bežičnih sustava:

- Sve ranjivosti koje postoje u konvencionalnim fiksnim mrežama primjenjive su i na bežične tehnologije,
- Maliciozni korisnici mogu dobiti neautorizirani pristup mreži kroz bežičnu vezu, premošćujući vatrozidnu zaštitu,
- Osjetljive informacije koje nisu kriptirane, i prenose se između dva bežična uređaja, mogu biti presretane i otkrivene,
- *Denial of Service* (DoS) napadi mogu biti usmjereni direktno na bežičnu vezu ili uređaj,
- Maliciozni korisnici mogu ukrasti identitet legitimnog korisnika i koristiti se njegovim pravima na internoj ili eksternoj korporativnoj mreži,
- Ručna računala i slični uređaji mogu biti ukradeni i osjetljivi podaci na njima mogu biti otkriveni,
- Podaci mogu biti izdvojeni bez opažanja iz loše konfiguriranih uređaja,
- Virusi ili drugi maliciozni kod mogu oštetiti podatke na bežičnim uređajima, te se kasnije umetnuti u fiksnu mrežnu vezu,
- Maliciozni korisnici se mogu, kroz bežičnu mrežu, spojiti na druge institucije, u svrhu pokretanja napada i skrivanja svoje aktivnosti,
- Uljezi, izvana ili iznutra, mogu dobiti mogućnosti upravljanja mrežom, te onemogućiti ili ometati njeno funkcioniranje,
- Interni napadi mogući su preko *ad hoc* prijenosa podataka.

Kao i kod fiksnih računalnih mreža, potrebno je biti svjestan odgovornosti za gubljenje osjetljivih informacija ili za napade pokrenute iz kompromitirane mreže.

3. Bežični LAN-ovi

U ovom poglavlju je dan detaljan pregled 802.11 WLAN tehnologije. Poglavlje uključuje slijedeće podatke o 802.11 tehnologiji: frekvencijski opseg, brzinu prijenosa i mrežnu topologiju. Nadalje, razmatraju se sigurnosne prijetnje i ranjivost bežičnih LAN-ova te su prikazani različiti načini smanjenja rizika i povećanja razine sigurnosti bežičnog LAN okružja.

3.1. Osnovne informacije

Tehnologija bežičnog LAN-a započinje s razvojem sredinom 1980-ih, kada se omogućava korištenje RF spektra u industriji. Danas, zahvaljujući niskoj cijeni, velikom broju proizvođača i nelicenciranosti frekvencije, tržište 802.11 tehnologije bilježi izuzetan rast. Dodatni poticaj će svakako biti daljnji razvoj 802.11g standarda koji omogućava brzine prijenosa do 54 Mbit/ s. Kao uvod u ovu tehnologiju služi Tablica 1.

Karakteristike	Opis
Fizički sloj	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread (FHS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frekvencijski pojas	2,4 GHz (nelicencirani ISM pojas) i 5 GHz.
Brzina prijenosa	11 Mbit/s (b), 54 Mbit/s (a i g).
Podatkovna i mrežna sigurnost	Algoritam zasnovan na RC4 za povjerljivost, autentikaciju i integritet. Ograničeno upravljanje ključevima (AES se razmatra unutar 802.11i).
Područje rada	Do 50 metara u zatvorenom prostoru i 400 metara na otvorenom (ovi brojevi variraju u ovisnosti o području rada te korištenoj opremi; a antenama velikog dometa moguće je ostvariti komunikaciju i na udaljenostima od oko 30 km).
Pozitivni aspekti	Brzine Ehterneta bez kabela; velik broj proizvoda velikog broja različitih proizvođača. Cijene pristupnih točaka i klijentskih kartica su u padu.
Negativni aspekti	Niska razina sigurnosti u osnovnom modu; propusnost se smanjuje s udaljenošću i opterećenjem.

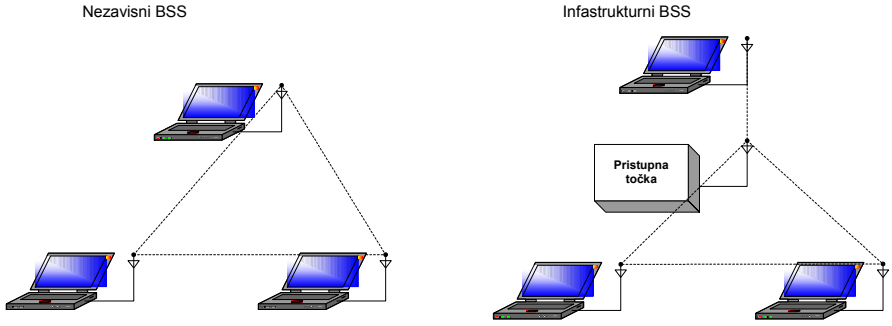
Tablica 1: Ključne karakteristike 802.11 mreža

3.1.1. Frekvencija i brzina prijenosa

IEEE je razvio 802.11 standarde u cilju omogućavanja bežične mrežne tehnologije poput žičnog Etherneta. 802.11a standard radi na frekvenciji od 5 GHz te, koristeći OFDM tehnologiju, omogućava brzine prijenosa do 54 Mbit/s. Trenutno najpopularniji 802.11b standard radi na nelicenciranom ISM (engl. *Industrial, Scientific and Medical*) pojasu od 2,4 GHz – 2,5 GHz. ISM pojas je postao popularan za bežične komunikacije pošto je omogućen širom svijeta. 802.11b tehnologija omogućava teoretske brzine prijenosa do 11 Mbit/s.

3.1.2. 802.11 arhitektura

Osnovni gradivi element 802.11 mreža je BSS (engl. *basic service set*), koji predstavlja grupu stanica koje međusobno komuniciraju. Komunikacija se odvija unutar područja zvanog osnovno područje usluge (engl. *Basic Service Area*), definiranog propagacijskim karakteristikama bežičnog medija. Kada se jedna mobilna stanica nalazi unutar osnovnog područja usluge, ona može komunicirati s drugim članovima BSS-a. BSS dolazi u dva oblika, prikazana na slici 1.



Slika 1: Nezavisni i infrastrukturni BSS-ovi

Nezavisne mreže

Na lijevoj strani se nalazi nezavisni BSS (engl. *independent BSS*; iBSS). Mobilne stanice u jednom iBSS-u međusobno izravno komuniciraju i moraju biti unutar direktno dostupnog komunikacijskog područja. Najmanju moguću 802.11 mrežu čini iBSS s dvije mobilne stanice. Tipično, iBSS-ovi su sastavljeni od manjeg broja mobilnih stanica postavljenih za specifične svrhe i na kratke vremenske periode. Radi svog kratkog vremena u kojem se takva komunikacija koristi, male veličine i usko fokusirane svrhe, iBSS se ponekad nazivaju i *ad hoc* BSS-ovi ili *ad hoc* mreže.

Infrastrukturne mreže

Na desnoj strani slike 1 nalazi se infrastrukturni BSS (obično se označava samo kao BSS). Infrastrukturne mreže koriste pristupne točke. Pristupne točke (engl. *access point*) se koriste za svu komunikaciju u infrastrukturnoj mreži, uključujući komunikaciju između mobilnih čvorova na istom području usluge. Ako jedna mobilna stanica u infrastrukturnom BSS-u treba komunicirati sa drugom mobilnom stanicom, komunikacija se odvija kroz dva skoka. Prvo, odašiljačka stanica šalje okvire pristupnoj točki. Nakon toga, pristupna točka prijenosi okvire odredišnoj stanici. Osnovno područje usluge koje odgovara jednom infrastrukturnom BSS-u je definirano točkama u kojima se može primiti signal pristupne točke. Iako prijenos s više skokova koristi veći prijenosni kapacitet nego direktno slanje, ovaj način ima dvije glavne prednosti:

- Infrastrukturni BSS je definiran udaljenošću od pristupne točke. Zahtjev je za sve stanice da se nalaze unutar područja pokrivenosti pristupne točke, ali ne postoji ograničenje na međusobnu udaljenost stanica. Omogućavanje direktne komunikacije među stanicama štedi prijenosni kapacitet, ali na trošak povećanja kompleksnosti na fizičkom sloju, zbog toga što će mobilna stanica morati održavati komunikaciju sa svim drugim mobilnim stanicama unutar područja usluge.
- Pristupne točke u infrastrukturnim mrežama su u poziciji da pomažu mobilnim stanicama u čuvanju energije. Pristupna točka može zabilježiti kada stanica ulazi u mod štednje energije i čuva okvire za nju. Stanice koje koriste baterije mogu isključiti slanje i uključiti se samo za slanje i primanje sačuvanih okvira u pristupnoj točki.

U infrastrukturnoj mreži, stanice moraju biti pridružene pristupnoj točki za dobivanje mrežne usluge. Pridruživanje je proces u kojem se mobilna stanica priključuje na 802.11 mrežu i logički je ekvivalentno ukopčavanju mrežnog kabela u Ethernet mrežu. Ovo nije simetričan proces. Mobilne stanice uvijek iniciraju proces pridruživanja, a pristupna točka može odabrati prihvaćanje ili odbijanje pristupa, ovisno o sadržaju zahtjeva za pridruživanje. Bitno je napomenuti da mobilna stanica može istovremeno biti pridružena samo jednoj pristupnoj točki.

3.1.3. Komponente bežičnih LAN-ova

Bežična mreža obuhvaća dva tipa opreme: bežične stanice i pristupne točke. Stanica, odnosno klijent, je obično prijenosno računalo s bežičnom mrežnom karticom. Kao bežični LAN klijenti u zadnje vrijeme se koriste i ručna računala, "*barcode*" skeneri, POS uređaji za naplatu. Bežične mrežne kartice se obično izrađuju s USB ili PCMCIA sučeljem. Bežična mrežna kartica je opremljena antenom, preko koje radio valovima komunicira s bežičnim LAN-om. Pristupna točka funkcionira kao most (engl. *bridge*) između bežične i fiksne mreže, a sastoji se od bežičnog mrežnog sučelja, fiksnog mrežnog sučelja (obično Ethernet) i odgovarajuće programske podrške za premošćivanje.

3.2. Ugrađena sigurnost 802.11 bežičnih LAN-ova

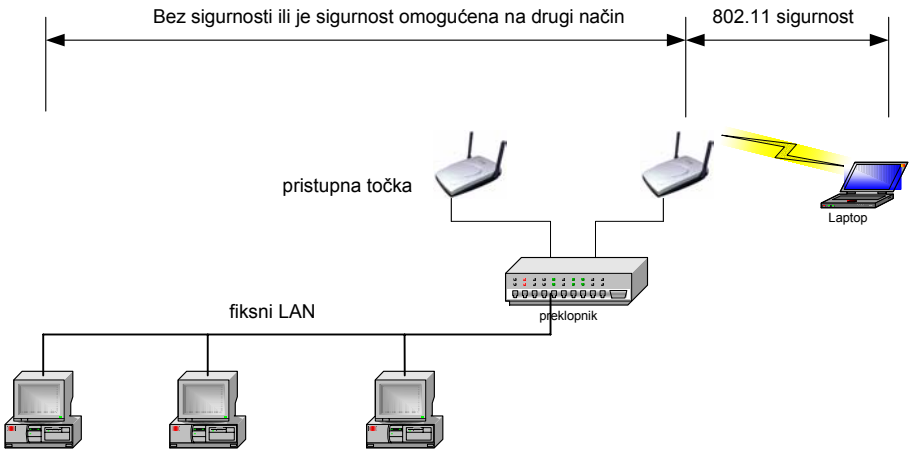
Ovo poglavlje se bavi ugrađenim sigurnosnim svojstvima 802.11 standarda. Bilo koji protokol koji pokušava osigurati podatke tijekom puta kroz mrežu mora zadovoljiti slijedeća tri glavna cilja:

- **Povjerljivost -** Zaštita podataka od presretanja i prisluškivanja neovlaštenih korisnika.
- **Integritet -** Čuvanje cjelovitosti informacije.
- **Autentikacija -** Identifikacija korisnika i izvora. Korisnik mora biti siguran da podaci dolaze od očekivanog izvora.

IEEE 802.11 specifikacija identificira nekoliko usluga za omogućavanje sigurnosti u području djelovanja bežičnih LAN-ova. Sigurnost bežičnih LAN-ova uključuje korištenje SSID-a (engl. *Service Set Identifier*), otvorene ili dijeljene autentikacije ključeva i statičkih WEP ključeva.
SSID je zajedničko mrežno ime uređaja u bežičnom podsustavu. Korištenjem SSID-a onemogućava se pristup bilo kojeg klijentskog uređaja koji nema SSID. Inicijalno pristupna točka šalje svoj SSID. Ako se i isključi slanje SSID-a, uljez ga može odrediti prisluškivanjem.
802.11 standard specificira dva načina klijentske autentikacije: otvorena i autentikacija dijeljenim ključem. Otvorena autentikacija uključuje malo više nego postavljeni ispravni SSID. S autentikacijom dijeljenim ključem, pristupna točka šalje klijentskom uređaju "*challenge*" tekstualni paket, koji korisnik onda mora enkriptirati s ispravnim WEP ključem i vratiti ga pristupnoj točci. Ukoliko korisnik ima krivi ključ ili ga nema, autentikacija će biti neuspješna i klijentu neće biti dopušteno pridruživanje pristupnoj točki. Autentikacija dijeljenim ključem se ne smatra sigurnom zbog toga što uljez koji odredi "*challenge*" sa čistim tekstom i onaj enkriptiran WEP ključem, može dešifrirati WEP ključ.
Drugi tip ključa koji se često koristi je statički WEP ključ. Statički WEP ključ definira administrator.

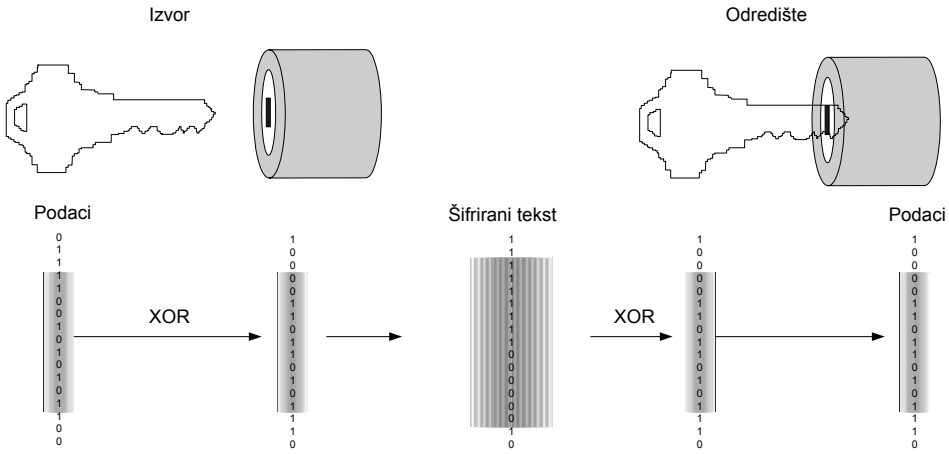
3.2.1. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) je protokol koji štiti podatke na sloju podatkovne veze, za vrijeme prijenosa između pristupne točke i klijenata. Ovaj protokol omogućuje postupke koji pokušavaju zadovoljiti gore navedene ciljeve.
WEP algoritam se implementira u MAC podsloj bežičnih mrežnih kartica. Korisnik može koristiti WEP protokol ili ne. Ukoliko korisnik aktivira WEP, mrežna kartica enkriptira svaki 802.11 okvir prije prijenosa koristeći RC4 šifru. Prijemna stanica, pristupne točke ili druge stanice dekriptiraju poruku nakon dolaska okvira. Stoga, kao što se vidi iz slike 2, WEP omogućava sigurnost samo na bežičnom dijelu veze. U trenutku kada okvir dođe do fiksnog dijela mreže, WEP se više ne primjenjuje.



Slika 2: Bežična sigurnost 802.11

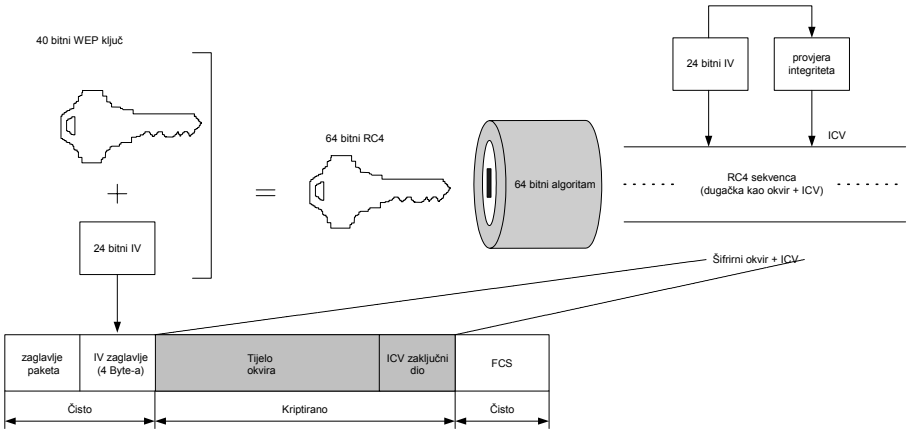
WEP algoritam se, prije svega, koristi za zaštitu bežičnih komunikacija od prisluškivanja. Druga funkcija WEP-a je prevencija neautoriziranih pristupa bežičnoj mreži. Ova funkcija nije eksplicitno cilj u 802.11 standardu, ali ju se obično smatra svojstvom WEP-a.
WEP se bazira na tajnom ključu koji se dijeli između mobilne stanice (npr. prijenosno računalo s bežičnom karticom) i pristupne točke (npr. bazna stanica). Tajni ključ se koristi za enkripciju paketa, prije slanja za provjeru integriteta, u svrhu osiguranja da paket nije promijenjen u prijenosu. Standard ne objašnjava kako nastaje dijeljeni ključ. U praksi, većina izvedbi koristi jedan ključ koji se dijeli između svih mobilnih stanica i pristupnih točaka.
WEP koristi RC4 kriptografski algoritam s varijabilnom duljinom ključa za zaštitu prometa. Iako 802.11 standard podržava WEP kriptografske ključeve od 40 bita, neki proizvođači opreme su implementirali produkte s 104-bitnim i 128-bitnim ključevima. U dobro dizajniranim kriptografskim sustavima, dodatna sigurnost se postiže koristeći dulje ključeve. Svaki dodatni bit udvostručuje broj potencijalnih ključeva i teoretski udvostručuje količinu vremena zahtijevanog za uspješan napad. RC4 enkripcijski algoritam je poznat kao tekuće šifriranje. Tekuće šifriranje funkcionira proširivanjem kratkog ključa u beskonačnu pseudo-slučajnu sekvencu. Pošiljatelj radi XOR funkciju nad sekvencom, s običnom porukom, i proizvodi šifriranu poruku. Prijemnik ima kopiju istog ključa i koristi ju za generiranje identične sekvence. Upotrebom XOR funkcije, sekvenca i šifrirani tekst daju originalnu poruku. Slika 3 prikazuje osnovni princip šifriranja pseudo-slučajnim ključem.



Slika 3: Šifriranje podataka pseudo-slučajnim ključem

Povjerljivošću i integritetom se rukuje istovremeno, kao što je prikazano na slici 4. Prije enkripcije, okvir prolazi kroz algoritam provjere integriteta, generirajući vrijednost provjere integriteta, ICV (engl. *Integrity Check Value*). ICV štiti sadržaj od neovlaštene promjene. Okvir i ICV su enkriptirani, tako da ICV nije dostupan napadaču.

Originalni WEP ključ specificira korištenje 40-bitnim sigurnim ključem. Sigurnosni WEP se kombinira s 24-bitnim inicijalizacijskim vektorom (IV) za kreiranje 64-bitnog RC4 ključa. RC4 uzima 64 ulazna bita i generira sekvencu jednaku duljini okvira plus IV. Nakon toga se obavlja XOR funkcija sekvence s okvirom i IV-om radi šifriranja. IV se smješta u zaglavlje okvira radi omogućavanja dešifriranja poruke na prijemniku.
Za zaštitu prometa od napada dešifriranja koristeći silu, WEP koristi skup od do četiri inicijalna ključa te također može upotrijebiti ključeve parova, zvane i mapirani ključevi, kada je to omogućeno. Inicijalni ključevi se dijele između svih stanica u podmreži. Jednom kada stanica dobije inicijalni ključ za svoju podmrežu, može komunicirati koristeći WEP.
Iako u većini proizvoda maksimalna duljina WEP ključa iznosi između 40 i 104 bita, neki proizvođači upotrebljavaju i WEP ključeve duljine 128 bita. Kako se duljina RC4 ključa dobije zbrajanjem WEP ključa i 24 bita IV-a tako neki proizvođači specificiraju ključeve duljine 128 RC4 bita kao "128-bitni WEP ključ", iako je WEP, tajni dio ključa zapravo samo 104 bita. WEP ključevi duljine 128 bita tvore RC4 ključ duljine 153 bita (128 + 24).
Ponovno korištenje ključa je često slabost kriptografskih protokola. Zbog toga WEP ima drugi razred ključeva za komunikaciju između para stanica.



Slika 4: WEP postupak

3.2.2. Nedostaci standardne IEEE 802.11 sigurnosti

U ovom poglavlju razmataju se poznate ranjivosti standardne sigurnosti 802.11 bežičnog LAN protokola.
Ponovno korištenje sekvence je glavna slabost bilo kojeg sustava šifriranja. Kada su paketi enkriptirani istom RC4 sekvencom, XOR dva enkriptirana paketa je jednak XOR-u dva paketa sa čistim tekstom. Analizirajući razlike između dva toka, zajedno sa strukturom tijela okvira, napadač može doći do zaključaka o sadržaju samih okvira sa čistim tekstom. Za izbjegavanje toga WEP koristi IV za enkripciju različitih paketa s različitim RC4 ključevima. Ipak, IV je dio zaglavlja paketa i nije enkriptiran, tako da prisluškivači mogu uočiti pakete enkriptirane istim RC4 ključem.
Kriptografi su identificirali mnoge slabe točke WEP algoritma. RC4 je snažna enkripcija, no napadači nisu ograničeni na frontalni napad na kriptografski algoritam, već mogu napasti njegovu bilo koju slabu točku.
U kolovozu 2001. Scott Fluhrer, Itskin Mantin i Adi Shamir su objavili dokument "*Weaknesses in the Key Scheduling Algorithm of RC4*", u kojem su objasnili slabosti RC4 algoritma na kojem se bazira WEP. Na kraju dokumenta su opisali i teoretske mogućnosti napada na WEP. Bit napada je iskorištavanje slabosti u načinu na koji RC4 generira sekvencu. Pretpostavili su mogućnost obnove prvog okteta enkriptirane poruke. Na nesreću, 802.11 koristi LLC enkapsulaciju, a vrijednost originalne poruke prvog okteta se zna da je 0xAA (prvi oktet SNAP zaglavlja). Zbog toga što je poznata vrijednost prvog okteta originalne poruke, prvi oktet šifrirane poruke može jednostavno biti odgonetnut koristeći običnu XOR operaciju s prvim enkriptiranim oktetom.

Koristeći se gore navedenim radom, Stubblefield, Ionannidis i Rubin su primijenili eksperimentalni napad. Trebalo im je manje od tjedan dana za pripremu izvođenja napada. Vrlo lako su izveli uspješan napad.
Završni udarac WEP-u je zadalo pojavljivanje AirSnorta, javno dostupnog alata, s kojim se može probiti WEP ključ.

3.3. Sigurnosni zahtjevi i prijetnje

U ovom poglavlju je dan kratak pregled sigurnosnih rizika u bežičnim LAN mrežama kao što su: napadi na povjerljivost integriteta informacije i mrežna dostupnost.
Napadi na mrežnu sigurnost se obično dijele na pasivne i aktivne:

- **Pasivni napadi** – Napadi u kojima neautorizirani korisnik dobiva pristup informaciji, pri čemu ne mijenja sadržaj. Pasivni napadi se dijele na prisluškivanje i analizu prometa.
    - **Prisluškivanje** – Napadač prati prijenos sadržaja poruke. Primjer ovakvog napada je kada osoba sluša prijenos između radnih stanica ili upada u prijenos između bežičnog uređaja i bazne stanice.
    - **Analiza prometa** – Napadač dobiva povjerljive podatke prateći prijenos uzoraka komunikacije. Značajna količina informacija sadržana je u toku poruka između sudionika u komunikaciji.
- **Aktivni napadi** – Napadi u kojima neautorizirani korisnik modificira poruku, tok podataka ili datoteku. Ovaj tip napada je moguće detektirati, ali nekad ga je nemoguće izbjeći. Aktivni napad može biti jedan od slijedeća četiri tipa (ili kombinacija nekih od njih): maskiranje, odgovor, modifikacija poruke ili napad uskraćivanjem računalnih resursa (engl. *Denial-of-Service DoS*). Ovi napadi se definiraju kako slijedi:
    - **Maskiranje** – Napadač se pretvara da je autorizirani korisnik i tako dobiva određene neautorizirane privilegije.
    - **Odgovor** – Napadač prati prijenos (pasivni napad) i šalje poruke kao legitimni korisnik.
    - **Modifikacija poruke** – Napadač mijenja legitimne poruke brisanjem, dodavanjem, mijenjanjem ili promjenom redoslijeda.
    - **Uskraćivanje računalnih resursa** – Napadač sprječava ili zabranjuje normalnom korisniku upravljanje svojstvima komunikacije.

Rizici pridruženi 802.11 su rezultat jednog ili više napada. Posljedice tih napada obično uključuju gubitak vlasničkih informacija, pravne troškove i troškove obnove, narušen imidž i gubitak mrežnih usluga.

3.3.1. Gubitak povjerljivosti

Povjerljivost je osnovni sigurnosni zahtjev za većinu organizacija. Zbog prirode širenja radio valova, povjerljivost je zahtjev kojem je puno teže udovoljiti u bežičnim mrežama. Osim što nije potrebno direktno se ukopčati kabelom u mrežu, problem kod bežičnih mreža je i nemogućnost kontroliranja područja pokrivenosti signalom.
Pasivno prisluškivanje 802.11 bežičnih komunikacija može uzrokovati značajan rizik za korisnika. Prisluškivanjem je moguće saznati osjetljive informacije poput mrežnog ID-a, zaporke i konfiguracijskih podataka. Zbog širenja signala izvan područja zgrade u kojoj se mreža nalazi, prisluškivanje i analiza prometa može biti urađena s obližnjeg parkirališta.
Analizatori bežičnog prometa, kao što su AirSnort i WEPcrack su alati lako dostupni na Internetu. Iako je AirSnort prvotno kreiran za automatizaciju procesa analize mreže, često se koristi za upad u bežičnu mrežu, upotrebom slabosti RC4. Ovaj alat, pokrenut na Linux operativnom sustavu prijenosnog računala s bežičnom karticom, može izračunati enkripcijski ključ nakon najmanje 100 MB praćenog prometa. Vrijeme potrebno za skupljanje ove količine prometa ovisi o količini prometa na mreži. Kada maliciozni korisnik sazna WEP ključ, on može čitati pakete koji putuju preko bežične mreže.
Slijedeći rizik gubitka povjerljivosti nastaje jednostavnim praćenjem *broadcast* prometa. Ukoliko je pristupna točka spojena na koncentrator, korisnik sa prijenosnim računalom može pratiti cjelokupni promet na koncentratoru. Zbog toga se preporuča korištenje preklopnika.

Osim gore navedenih pasivnih napada, postoji mogućnost i aktivnih napada. Lažno predstavljanje, odnosno maskiranje u legitimnog korisnika je jedan od njih. Koristeći lažno korisničko ime, zaporku i IP adresu neovlašteni korisnik može doprijeti do mrežnih resursa i osjetljivih informacija.
Vrlo neugodan oblik napada je postavljanje pristupne točke u mrežu od strane napadača ili nesavjesnog korisnika (engl. *rogue access point*). Takve pristupne točke se obično postavljaju na skrivena mjesta. Ukoliko se takva pristupna točka postavi u područje legalnog bežičnog LAN-a, te se ponaša kao legitimna pristupna točka, a njezina snaga je konfigurirana tako da bude veća od one legalne pristupne točke, tada ona uspijeva postići to da klijenti šalju poruke kroz nju. Bitno je napomenuti da se ovakve pristupne točke često postavljaju od strane nesavjesnih korisnika, bez znanja administratora sigurnosti i odgovarajuće sigurnosne konfiguracije. Kroz takve, loše konfigurirane pristupne točke, maliciozni korisnik lagano upada u mrežu.

3.3.2. Gubitak integriteta

Problematika zaštite integriteta bežičnih mreža je slična onoj fiksnih. Integritet podataka je jako teško postići u okolinama bez adekvatne kriptografske zaštite. Primjer takvog napada je brisanje ili modifikacija poruke elektroničke pošte s korisničkog računa na bežičnoj mreži. Ovakvi napadi se dešavaju ukoliko poruka nije odgovarajući kriptirana.

3.3.3. Gubitak mrežne dostupnosti

Uskraćivanje mrežne dostupnosti uključuje neke oblike DoS napada poput radio ometanja. Ometanje se postiže na način da maliciozni korisnik emitira signal koji nadjača legitimni bežični signal što uzrokuje prekid komunikacije. Drugi način uskraćivanja dostupnosti je *download* ili *upload* velike količine podataka te na taj način zauzimanje cijelog prijenosnog pojasa. Ovo je čest slučaj korištenjem tzv. p2p protokola za razmjenu podataka poput Kazaa ili Gnutela. Za sprječavanje se obično koriste sigurnosne politike koje ograničavaju tipove i količinu podataka koje korisnik može prenijeti preko mreže.

3.3.4. Ostali sigurnosni rizici

Prilikom udaljenog spajanja u mrežu svoje organizacije udaljeni korisnici se sve više koriste bežičnim mrežama u hotelima, aerodromima, na konferencijama i sličnim mjestima. Ovakve javne mreže unose tri primarna rizika:

- Zbog toga što su javne, ovakve mreže su dostupne i malicioznim korisnicima,
- Kako služe kao premosnik prema korisnikovoj vlastitoj mreži, potencijalno dopuštaju svakome na javnoj mreži napad ili dobivanje pristupa u premoštenu mrežu,
- Kako se obično koriste antene s velikim dobitkom za poboljšanje prijema i povećanje područja pokrivenosti, one omogućavaju malicioznim korisnicima prisluškivanje.

Povezivanjem na svoju vlastitu mrežu, a preko neprovjerene mreže, korisnik može prouzročiti ranjivosti u mrežama svojih organizacija.
Socijalni inženjering i "kopanje po smeću" (engl. *dumpster diving*) također moraju biti uračunati prilikom proučavanja potencijalnih sigurnosnih rizika.

3.4. Metode za umanjivanje rizika

U ovom poglavlju su objašnjeni postupci za umanjivanje rizika. Potpuno uklanjanje rizika je nemoguće. Objašnjeni načini i postupci su opći i nisu primjenjivi na sve organizacije jednako, budući da potrebna razina zaštite, a samim time i visina troškova, varira.

3.4.1. Sigurnosna politika

Prilikom definiranja potreba za osiguranjem bežičnih mreža, prvi korak predstavlja izrada sigurnosne politike i pripadajućih pravilnika i procedura. Sigurnosna politika bežičnih LAN mreža morala bi uključivati slijedeće:

- Identificirati korisnike bežične tehnologije,
- Utvrditi potrebu za pristupom Internetu,
- Definirati tko može instalirati pristupne točke i drugu bežičnu opremu,

- Definirati procedure definicije, davanja i oduzimanja korisničkih prava,
- Odrediti i osigurati ograničavanje fizičkog pristupa pristupnoj točki,
- Definirati tipove informacija koje se mogu slati preko bežične veze,
- Definirati standardne sigurnosne postavke za pristupnu točku,
- Definirati sklopovlje i programsku podršku za sve bežične uređaje,
- Definirati procedure za prijavu gubitka bežičnog uređaja,
- Definirati procedure za prijavu sigurnosnog incidenta,
- Definirati proceduru za korištenje enkripcije i upravljanje ključevima,
- Definirati frekvenciju i opseg sigurnosnih procjena rizika.

Vrlo je bitno dobro obučiti mrežne administratore za korištenje bežičnih tehnologija, kao i upozoriti ih na sve rizike. Nadalje, vrlo je bitno imati pripremljene i svjesne krajnje korisnike, bez čega je nemoguće uspostaviti sigurnost.

3.4.2. Implementacija

Prilikom implementacije bitno je voditi računa o području koje pristupna točka pokriva signalom. Ukoliko signal izlazi iz područja uredskih zidova, to može uzrokovati sigurnosne ranjivosti. Raznim alatima za mjerenje polja može se utvrditi da li signal prelazi okvire zgrade. Dobar način za smanjenje područja dostupnosti signala je i korištenje usmjerenih antena čime se postiže kontrola zračenja. Ipak, direktne antene ne štite u potpunosti mrežne veze, zbog zračenja tzv. sekundarnih latica.
Iako vođenje računa o području pokrivenosti signalom može donijeti prednosti za sigurnost, to ne može biti prihvaćeno kao apsolutno sigurno rješenje. Uvijek postoji mogućnost da maliciozni korisnik, s antenom koja ima veliki dobitak, prisluškuje promet.
U nastavku poglavlja dan je prikaz tehničkih protumjera za onemogućavanje napada. Tehničke protumjere uključuju korištenje hardverskih i softverskih rješenja za uspostavu sigurnih mrežnih sučelja.

3.4.2.1. Softverska rješenja

Softverska rješenja uključuju ispravno konfiguriranje pristupnih točki, redovno osvježavanje softvera, implementaciju IDS rješenja, pregledavanje sigurnosnih zapisa i uspostava efikasne enkripcije.

3.4.2.1.1. Konfiguracija pristupne točke

Mrežni administratori trebaju konfigurirati pristupne točke u skladu s sigurnosnim politikama i zahtjevima. Ispravno konfiguriranje Ethernet MAC *Access Control List* (ACL), administratorske zaporke, postavki enkripcije, funkcije resetiranja, automatske funkcije povezivanja na mrežu, dijeljenih ključeva i SNMP agenata pomaže u eliminiranju mnogih ranjivosti naslijeđenih od inicijalne konfiguracije proizvođača softvera.
Korištenje MAC ACL funkcionalnosti. Većina pristupnih točaka dolazi s jednostavnim filtriranjem MAC adrese, koje sadrži listu MAC adresa dozvoljenih stanica. Ovaj način je obično dovoljan za osnovnu sigurnost, no njegov velik nedostatak je da se prisluškivanjem lako utvrde MAC adrese autoriziranih stanica te se iste mogu zloupotrijebiti.
Ažuriranje inicijalne zaporke. Svaki WLAN uređaj dolazi s postavljenim inicijalnim postavkama. Na nekim pristupnim točkama administratorska zaporka je postavljena na prazan znak tako da maliciozni korisnik može jednostavno doći do pristupa uređaju. Administratori trebaju promijeniti inicijalne postavke koristeći "snažne administratorske zaporke" (npr. duljine najmanje osam znakova, korištenje velikih i malih slova, brojki, specijalnih znakova).
Uspostava odgovarajućih enkripcijskih postavki. Enkripcija treba biti postavljena na najjaču dostupnu u produktu. Tipična pristupna točka ima nekoliko dostupnih enkripcijskih postavki: bez postavke, 40-bitni dijeljeni ključ i 104-bitni dijeljeni ključ. Napadi na WEP donose različite rezultate ovisno o duljini ključa.
Kontrola funkcije resetiranja. Funkcija resetiranja sadrži specifičan problem zbog toga što dopušta pojedincu da poništi bilo koju sigurnosnu postavku, nakon što je administrator konfigurirao u pristupnu točku. Ovime se vraćaju inicijalne tvorničke postavke. Inicijalne postavke općenito ne zahtijevaju administrativnu zaporku i mogu npr. onemogućiti enkripciju. Resetiranje se vrši

jednostavnim pritiskom točkastog predmeta poput olovke u šupljinu za resetiranje. Iako se redovnim praćenjem sustava neovlašteno resetiranje može uočiti, jedini pravi način zaštite je kontrola fizičkog pristupa mjestu gdje se pristupna točka nalazi.

Promjena SSID-a. Inicijalna tvornička vrijednost SSID-a se treba promijeniti. Inicijalne vrijednosti SSID-a, korištene kod mnogih proizvođača 802.11 opreme, su objavljene i dobro poznate stoga ih je potrebno promijeniti radi sprječavanja lakog pristupa.

Onemogućavanje razašiljanja SSID svojstava. SSID se koristi kao oznaka bežične mreže. Klijenti koji se žele priključiti mreži pregledavaju područje tražeći dostupne mreže i priključuju se pridruživanjem ispravnog SSID-a. SSID, ASCII skup znakova koji obično završava s "0", ima duljinu od 0 do 32 okteta. Slučaj u kojem je duljina nula okteta naziva se SSID razašiljanja. Bežični klijent može odrediti sve mreže u području aktivnim pretraživanjem pristupnih točaka i korištenjem razašiljanja *Probe Request* poruke sa SSID-om duljine nula. Ova poruka inicira slanje odgovora (*Probe Response*) od svih 802.11 mreža u okolini. Onemogućavanje svojstva SSID razašiljanja u pristupnoj točki uzrokuje da pristupna točka ignorira poruke od klijenata čime ih prisiljava na korištenje aktivnog skeniranja (koristeći specificirani SSID).

Promjena inicijalnih kriptografskih ključeva. Proizvođač omogućava jedan ili više ključeva za autentikaciju između uređaja koji pokušavaju osigurati pristup mreži ili pristupnoj točki. Kako mnogi proizvođači koriste iste inicijalne dijeljene ključeve, koji su obično poznati malicioznim korisnicima, njihovo korištenje može uzrokovati ozbiljne sigurnosne ranjivosti. Promjena inicijalnih dijeljenih ključeva umanjuje rizik.

Korištenje SNMP-a. Korištenje SNMP agenata kod pristupnih točaka pojedinih proizvođača omogućava mrežnim upravljačkim programima praćenje statusa pristupnih točaka i klijenata. Zbog svojih mehanizama jake sigurnosti, upotreba SNMPv3 se preporuča u mrežama u kojima se zahtjeva korištenje SNMP-a.

Promjena inicijalnog kanala. Prilikom postavljanja pristupne točke potrebno je voditi računa o potencijalnim drugim pristupnim točkama u okolini. Ukoliko na istom području više pristupnih točaka radi na bliskim kanalima, lako može doći do ometanja i DoS-a kao rezultata radio interferencije. Optimum se postiže podešavanjem kanala na način da je razlika između kanala koji koriste susjedne pristupne točke 5. Obično se koriste 1, 6 i 11 kanal.

Korištenje DHCP-a. Automatsko povezivanje na mrežu uključuje upotrebu DHCP poslužitelja koji korisnicima dijeli IP adrese iz svog opsega adresa. Sigurnosna prijetnja u slučaju korištenja DHCP-a je da maliciozni korisnik može jednostavno dobiti neautorizirani pristup mreži korištenjem prijenosnog računala s bežičnom mrežnom karticom. Kako DHCP poslužitelj ne zna koji bežični uređaj ima pristup, on će automatski prijenosnom računalu dodijeliti IP adresu. Ovaj rizik se izbjegava korištenjem statičkih IP adresa, ukoliko je to moguće. Druga mogućnost je korištenje DHCP poslužitelja unutar vatrozida fiksne mreže koji dopušta pristup bežičnim mrežama izvan njega.

3.4.2.1.2. Sigurnosne zakrpe i nadogradnja

Proizvođači opreme pokušavaju ispraviti uočene sigurnosne softverske i hardverske ranjivosti. Ispravke dolaze u obliku sigurnosnih zakrpi i nadogradnji, čije izdavanje je mrežni administrator dužan redovno pratiti i implementirati.

3.4.2.1.3. Autentikacija

Kvalitetna autentikacija je pouzdan način dopuštanja pristupa mreži samo autoriziranim korisnicima. Rješenja uključuju klasičnu upotrebu korisničkog imena i zaporke, *smart card* rješenja, biometriku i PKI ili kombinaciju navedenih metoda.

Bez obzira na sigurnosni stupanj, potrebno je koristiti snažne sigurnosne politike zaporke. Za veći stupanj sigurnosti se mogu koristiti druga rješenja poput PKI-a.

3.4.2.1.4. Osobni vatrozidi

Resursi u javnim bežičnim mrežama nose veće sigurnosne rizike napada nego interni resursi. Osobni vatrozidi su softverska rješenja koja se nalaze na korisnikovom uređaju i služe za zaštitu od pojedinih vrsta napada. Iako pružaju određeni stupanj zaštite, osobni vatrozidi ne štite od naprednih vrsta

napada. Stoga, ovisno o sigurnosnim zahtjevima, ponekad su potrebni dodatni sigurnosni slojevi za zaštitu.

3.4.2.1.5. Intrusion Detection System (IDS)

Intrusion detection system (IDS) je efikasan alat za utvrđivanje da li neautorizirani korisnici pokušavaju kompromitirati računalnu mrežu. Postoje tri tipa IDS sustava:

- *Host-based.* Instaliran na individualnom sustavu (npr. mrežni poslužitelj) i prati zapise i logove sustava, tražeći sumnjivo ponašanje.
- *Network-based.* Prati mrežni promet, paket po paket, u stvarnom vremenu, u cilju određivanja da li se trenutne aktivnosti poklapaju s uzorcima pojedinih napada.
- *Hybrid.* Sustavi koji su kombinacije gornje dvije vrste.

U nekim slučajevima, osim samog praćenja, IDS može zaustaviti napad na sustav, iako je njegova primarna funkcija skupljanje logova i analiza događaja i poslanih upozorenja.
IDS sustav postavljan u fiksnom dijelu mreže ima bitno ograničenje u zaštiti bežičnog dijela mreže. Mrežni (engl. *network-based*) IDS senzori, koji se nalaze na fiksnom djelu mreže, iza pristupne točke. neće detektirati napad jednog bežičnog klijenta na drugog. Naime, taj dio prometa se odvija jedino u bežičnom dijelu mreže i oni će reagirati tek kada se iz kompromitiranog bežičnog klijenta napadne klijent unutar fiksnog dijela mreže.
U slučaju potrebe više razine zaštite, potrebna je implementacija bežičnog IDS rješenja koje omogućava slijedeće:

- Identifikaciju fizičke lokacije bežičnih uređaja unutar građevine i okolnog prostora,
- Detekcija neautorizirane P2P (*peer-to-peer)* komunikacije unutar bežične mreže, koja nije vidljiva iz fiksne mreže,
- Analiza bežičnih komunikacija i praćenje 802.11 RF prostora te generiranje upozorenja nakon detektiranja neautoriziranih konfiguracijskih promjena na bežičnim uređajima koji povrjeđuju sigurnosnu politiku,
- Detekcija i alarmiranje u slučaju kada se "r*ogue access point*" pojavi u području sigurnosnog opsega organizacije ili tvrtke,
- Omogućavanje centraliziranog praćenja i upravljačkih svojstava kod integracije u postojeće IDS rješenje te praćenje i izvještavanje sigurnosnog statusa bežične i fiksne mreže.

3.4.2.1.6. Enkripcija

Kako je gore napomenuto, preporuče se primjena najdulje (104-bitne) enkripcije.

3.4.2.1.7. Sigurnosna procjena

Sigurnosna procjena ili pregled je osnovni alat za provjeru sigurnosnih postavki bežičnih LAN-ova i za utvrđivanje akcija koje je potrebno provesti za daljnje održavanje nivoa sigurnosti. Vrlo je važno obavljati periodičke preglede bežičnim mrežnim analizatorima i ostalim alatima. Pregled se može obavljati samostalno, no preporuča se korištenje nezavisnih konzultanata. Nezavisni konzultanti su obično u toku s najnovijim ranjivostima, bolje obučeni i opremljeni. Isto tako, pregledi nezavisnih konzultanta obično sadrže i testiranje probojnosti (engl. *penetration testing*), koje utvrđuje da li je sustav u skladu s donesenom sigurnosnom politikom i procedurama i u toku s najnovijim softverskim zakrpama i nadogradnjama.

3.4.2.2. Hardverska rješenja

Hardverska rješenja za umanjenje rizika bežičnih mreža uključuju implementaciju pametnih kartica (engl. *smart card*), VPN-ova, PKI, biometrike i drugih hardverskih rješenja.

3.4.2.2.1. Pametne kartice

Pametne kartice se obično koristite kada autentikacija s korisničkim imenom i zaporkom nije dovoljna. Korisnik se certificira, a druge informacije se spremaju na samu karticu i obično zahtijevaju od korisnika da zapamti PIN broj.

3.4.2.2.2. *Virtualne privatne mreže*

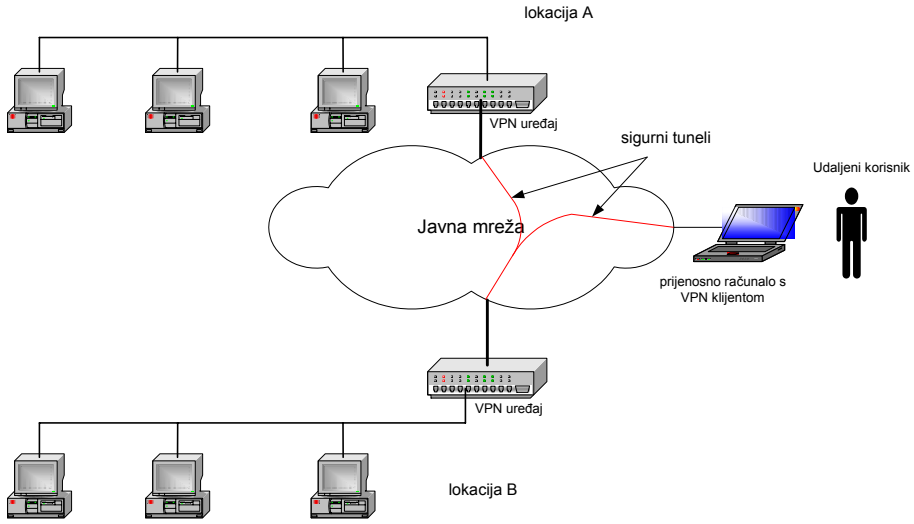
Virtualne privatne mreže (engl. *Virtual Private Network*, VPN) omogućavaju siguran prijenos podataka kroz javnu mrežnu infrastrukturu. VPN se obično koristi na tri različita načina:

- Pristup udaljenog korisnika,
- Povezivanje dva LAN-a,
- Extranet.

Osnovni koncept VPN tehnologije je implementacija sigurnog medija između privatnih mreža, a preko javne mreže. Taj medij može biti programski ili sklopovski orijentiran, a uobičajene su i kombinacije tih pristupa. Slika 5 prikazuje korištenje VPN-a za sigurnu komunikaciju između dvije lokacije i udaljenog korisnika.

Kada računalo šalje podatke prema drugom računalu na udaljenoj mreži, podaci koji u tom slučaju izlaze iz lokalne mreže moraju proći kroz *gateway* uređaj koji štiti tu mrežu, putovati kroz javnu mrežu, te na drugoj strani također proći kroz *gateway* uređaj. VPN štiti tako odaslane podatke automatskim enkriptiranjem prilikom slanja podataka između dviju udaljenih privatnih mreža i enkapsuliranjem u IP pakete, te automatskim dekriptiranjem paketa na drugom kraju komunikacijskog kanala.

Sigurnost VPN-a temelji se na enkripciji. Cilj je ograničiti pristup podacima koji se prenose samo odgovarajućim korisnima, odnosno računalima. VPN koristi kompletnu enkripciju paketa, od jednog kraja virtualnog spoja do drugog (engl. *end-to-end*). Ova tehnika spremanja šifriranih podataka u otvorena zaglavlja naziva se tuneliranje. Prilikom spajanja, VPN otvara sigurni tunel koji omogućava enkapsulaciju i šifriranje podataka, te autentikaciju korisnika.



Slika 5: Korištenje VPN-a za sigurnu komunikaciju između dvije lokacije i udaljenog korisnika

Postoji nekoliko elemenata koje VPN rješenje mora sadržati:

- skalabilnost,
- sigurnost,
- VPN servisi,
- uređaji,
- upravljanje.

Skalabilnost podrazumijeva da svaki element mora biti izveden tako da može podržati VPN platforme od malih uredskih konfiguracija, pa do velikih korporacijskih implementacija. Mogućnost prilagodbe VPN-a prema potrebama propusnosti i načinu veze ključna je u svakom VPN rješenju.

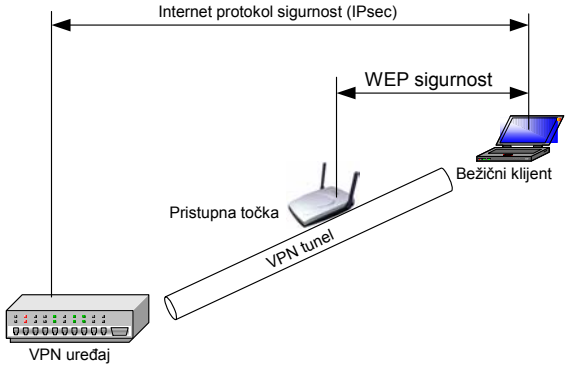
Sigurnosni pojmovi kao što su tuneliranje, šifriranje i autentikacija paketa, nužni su za sigurnost prijenosa podataka preko javnih mreža. Osim toga, autentikacija korisnika i kontrola pristupa nužne su za dodjelu odgovarajućih ovlasti i prava pristupa mrežnim resursima.

Uloga VPN servisa je upravljanje propusnošću komunikacijskog kanala, te implementacija funkcija koje osiguravaju kvalitetu usluge, poput izbjegavanja zagušenja, oblikovanja prometa, klasifikacije paketa itd. Također, važni dijelovi VPN tehnologije jesu protokoli koji osiguravaju usmjerivačke servise, poput

EIGRP (engl. *Enhanced Interior Gateway Router Protocol*), OSPF (engl. *Open Shortest Path First*), te BGP (engl. *Border Gateway Protocol*).
Uređaji poput vatrozida, sustava za detekciju neovlaštenih aktivnosti, te aktivno praćenje sigurnosnih parametara nužni su za uspostavu odgovarajuće razine sigurnosti pri korištenju VPN-a.
Upravljanje propusnosti kanala, definicija i primjena sigurnosnih pravila, te nadgledanje mrežnog prometa također su nužni elementi svakog VPN rješenja.
Unutar infrastrukture međusobno povezanih mreža, tuneliranje predstavlja tehniku prijenosa podataka namijenjenih određenoj mreži preko druge mreže. Protokol kojim se implementira tuneliranje, umjesto da šalje originalni okvir, enkapsulira okvir u dodatno, posebno oblikovano, zaglavlje. Takvo zaglavlje osigurava informacije nužne za usmjerivanje enkapsuliranih podataka kroz mrežu koja služi za prijenos do odredišta. Enkapsulirani podaci šalju se između krajnjih točaka tunela. Tunel je logički put kroz koji enkapsulirani podaci prolaze kroz mrežu, koja je medij za prijenos. Kada takav okvir dođe do svog odredišta, iz njega se ekstrahiraju korisni podaci koji se zatim šalju na ciljno odredište. Tuneliranje uključuje čitav proces enkapsulacije, prijenosa i ponovne ekstrakcije originalnih podataka.
Danas postoje razne tehnologije koje implementiraju tehniku tuneliranja. Najvažnije od njih su sljedeće:

- DLSW (engl. *Data Link Switching*),
- GRE (engl. *Generic Routing Encapsulation*),
- ATMP (engl. *Ascend Tunnel Management Protocol*),
- Mobile IP – za mobilne korisnike,
- IPSec (engl. *Internet Protocol Security Tunnel Mode*),
- PPTP (engl. *Point-to-Point Tunneling Protocol*),
- L2F (engl. *Layer 2 Forwarding*),
- L2TP (engl. *Layer 2 Tunneling Protocol*).

Od gore nabrojanih tehnologija danas se najčešće koristi IPSec. IPSec je standard definiran od strane IETF-a, a cilj njegove izrade bio je siguran transport informacija preko javnih IP mreža. IPSec je protokol treće razine (engl. *Layer 3*), te u sebi sadržava nekoliko sigurnosnih tehnologija da bi osigurao tajnost, integritet i autentikaciju. IPSec implementira šifriranja i autentikaciju u mrežnom sloju, osiguravajući tako sigurnu komunikaciju od početka do kraja unutar mrežne infrastrukture.
IKE (engl. *Internet Key Exchange*) služi za određivanje sigurnosnih parametara i razmjenu ključnih informacija između entiteta koji sudjeluju u komunikaciji. Sigurnosni parametri definiraju vezu između dvaju ili više entiteta, te definiraju kako će ti entiteti koristiti sigurnosne servise, u cilju uspostave međusobne sigurne komunikacije. IPSec, sam po sebi, ne posjeduje mehanizam se određivanje takvih sigurnosnih parametara. IETF je odabrao IKE kao standardnu metodu za definiranje sigurnosnih parametara za potrebe IPSec-a. Pri tome se također koristi IKMP (engl. *Internet Key Management Protocol*). IKE stvara autenticirani, sigurni tunel između dvaju entiteta, te zatim definira sigurnosne parametre potrebne za IPSec. Kroz taj proces dva entiteta se moraju međusobno autenticirati, te dogovoriti zajedničke ključeve.
Slika 6 prikazuje primjer korištenja IPSec-a u bežičnim LAN mrežama. Iz slike se vidi da je IPsec sigurnost neovisna o WEP sigurnosti na drugom sloju.



Slika 6: VPN sigurnost kao dodatak WEP-u

3.4.2.2.3. *Public Key Infrastructure (PKI)*

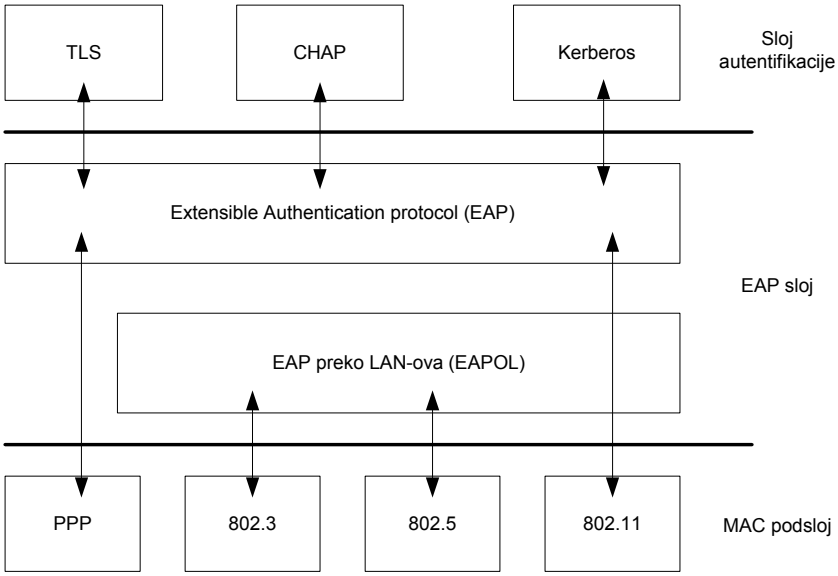
PKI predstavlja okvir i usluge za generiranje, distribuciju, kontrolu i *accounting* certifikata javnih ključeva. On omogućava aplikacije sa sigurnom enkripcijom i autentikaciju mrežnih transakcija, kao i integritet podataka. Bežični LAN-ovi mogu integrirati PKI za autentikaciju i sigurnu mrežnu transakciju. PKI se npr. ugrađuje u prijenosne uređaje i pametne kartice.
Zbog kompleksnosti i cijene implementacije i administriranja PKI-a, ovo rješenje se preporuča jedino tamo gdje je potrebna veća razina sigurnosti.

3.4.2.2.4. *Biometrika*

Biometrijski uređaji u bežičnim LAN mrežama, kao i u drugim slučajevima, uključuju prepoznavanje otiska prsta, šarenice oka, prepoznavanje lica i govora. Biometrija se obično koristi za autentikaciju tamo gdje je potrebna visoka razina sigurnosti.

3.4.2.3. 802.1X

802.1X standard je primarno razvijen za korištenje s IEEE 802 LAN-ovima, no u nedostatku gotovog rješenja primjenjuje se i za bežične LAN-ove. Ovo uključuje zahtjev za korištenjem EAP (engl. *Extensible Authentication Protocol*) metode, podržavajući obostranu autentikaciju, upravljanje ključevima i otpornost na napade.



Slika 7: EAP model

IEEE 802.1X može u biti u potpunosti implementiran na pristupnoj točki (omogućavajući podršku za jednu ili više EAP metoda) ili može iskoristiti pozadinski autentikacijski poslužitelj. IEEE 802.1X standard podržava autentikacijske protokole poput RADIUS-a, Diametera i Kerberosa.
Postoje dva glavna načina autentikacije krajnjeg korisnika ili uređaja: digitalnim certifikatima ili zaporkama. Najčešća autentikacijska metoda zasnovana na digitalnim certifikatima je EAP-TLS. Ostale česte metode koje koriste 802.1x EAP protokol su EAP-MD5, EAP-TTLS, i LEAP. U ovom dokumentu se koriste samo standardi i objavljeni probni standardi EAP-a. Privatne autentikacijske metode, poput CISCO LEAP-a protokola, nisu obrađene u ovom dokumentu.

3.4.2.3.1. *EAP-TLS autentikacija*

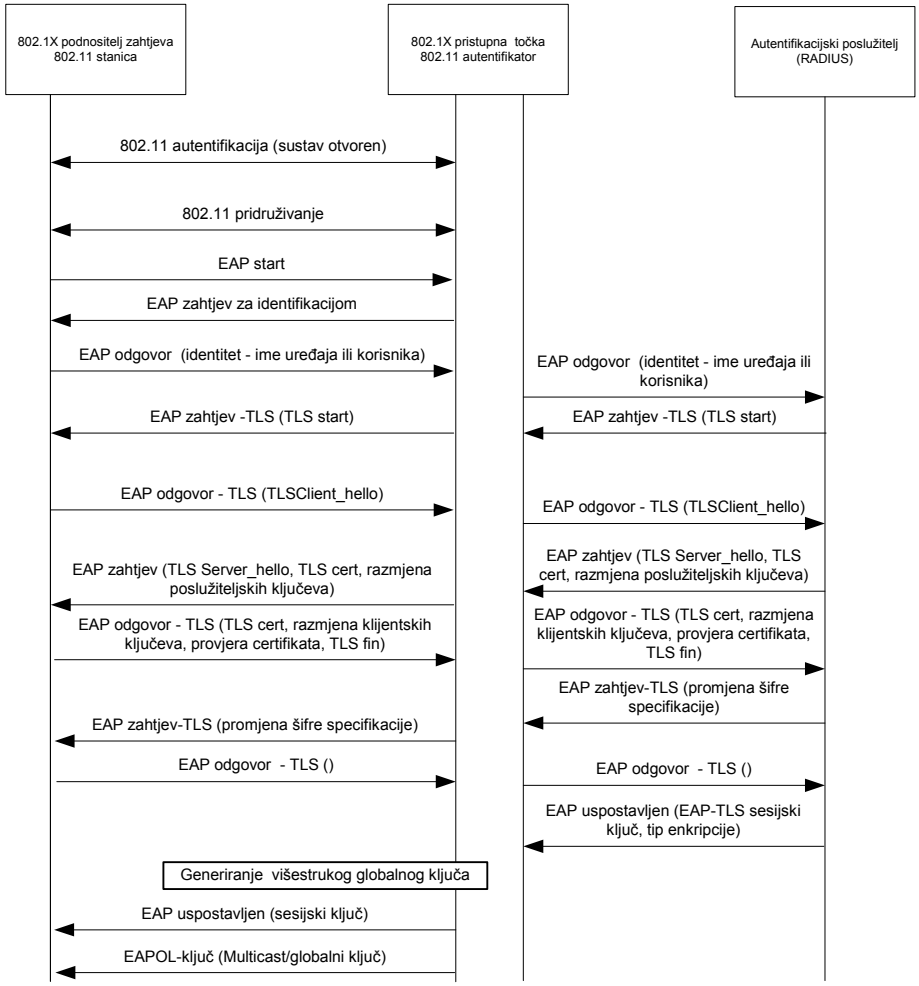
EAP-TLS (engl. *transport level security*) protokol omogućava mehanizme za obostranu autentikaciju na osnovi certifikata, zajedno s uspostavom sigurnog ključa u stanici, RADIUS poslužitelju i pristupnoj točki. Ovo zahtijeva prethodnu distribuciju klijentskih i poslužiteljskih certifikata preko sigurne žične veze do ciljane mreže. RADIUS autentikacijski poslužitelj podržava EAP-TLS, a zahtijevana je i sposobnost upravljanja certifikatima. Slika 8 prikazuje pojednostavljenu razmjenu poruka za EAP-TLS. EAP autentikacijska poruka poslana od/prema stanice do RADIUS poslužitelja prelazi preko pristupne točke.

3.4.2.3.2. EAP-MD5

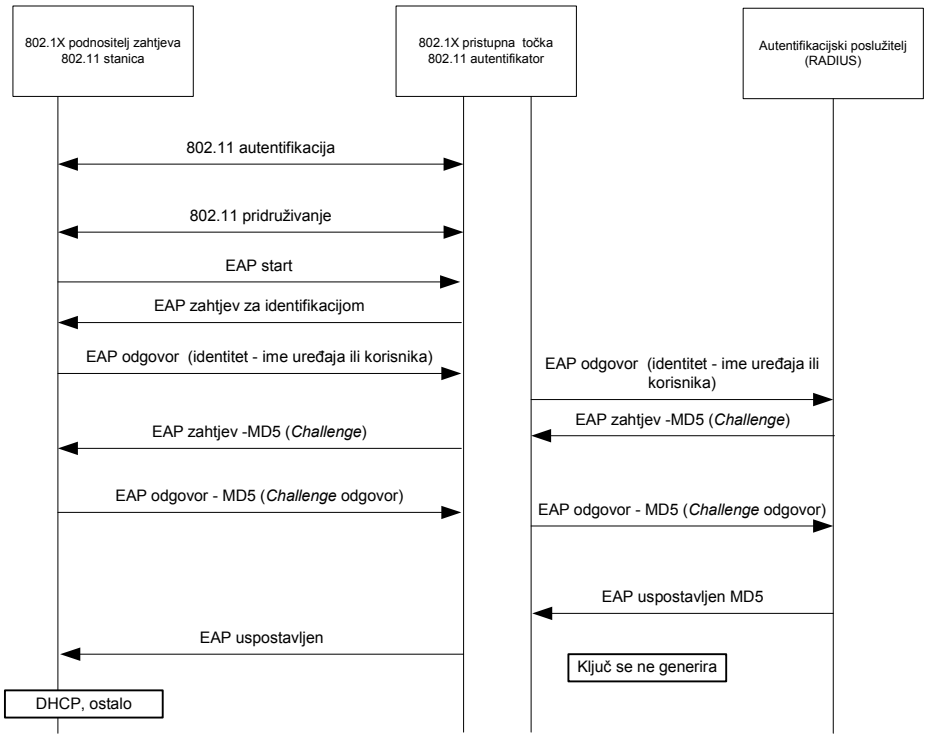
EAP-MD5 autentikacijski algoritam omogućava jednosmjernu mrežnu autentikaciju klijenta zaporkom. Ovaj algoritam može se koristiti za bežične aplikacije s manje striktnim sigurnosnim zahtjevima u bežičnom LAN-u. Npr. korištenje EAP-MD5 autentikacije može biti dovoljno za aplikacije u javnom prostoru u kojima je enkripcija omogućena na aplikacijskom sloju. Nedostatak korištenja EAP-MD5 u bežičnim LAN aplikacijama je da se ne generiraju enkripcijski ključevi. Također, iako se protokol može koristiti od strane klijenta za autentikaciju mreže, on se tipično koristi samo za autenticiranje klijenata. Kako se poruka odjavljivanja ne autenticira, uspostavljena sesija može biti oteta od strane napadača. Slika 9 prikazuje tok poruka.

3.4.2.3.3. EAP-TTLS

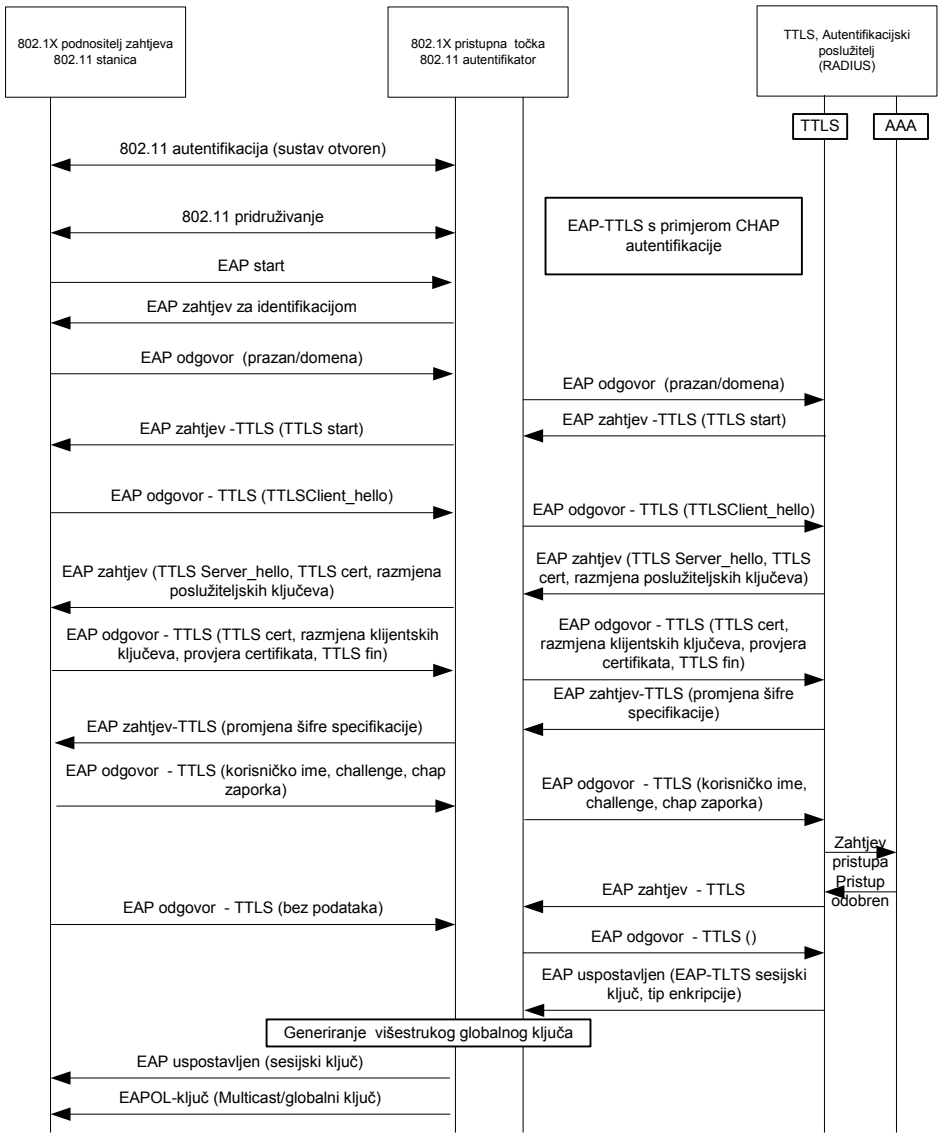
EAP-TTLS (engl. *tunneled transport level security*) se može promatrati kao zanimljiva kombinacija EAP-TLS i tradicionalne metode zasnovane na zaporci poput CHAP-a (engl. *Challenge Handshake Authentication Protocol*). U ovoj metodi, TLS tunel se prvo uspostavlja između stanice i autentikacijskog poslužitelja. Klijent autenticira mrežu na koju je spojen autentikacijom digitalnog certifikata, omogućenog od strane TTLS poslužitelja. Ovaj način je analogan tehnici korištenoj za povezivanje sigurnog Web poslužitelja. Jednom kada je autenticirani tunel postavljen, autenticira se i krajnji korisnik. EAP-TTLS-u ima dodanu zaštitu identiteta krajnjeg korisnika od pogleda preko bežičnog medija. Na ovaj način omogućena je anonimnost krajnjeg korisnika. EAP-TTLS također omogućuje ponovno korištenje postojećim autentikacijskim sustavima krajnjih korisnika.



Slika 8: Pojednostavljeni prikaz EAP-TLS razmjene poruka



Slika 9: EAP-MD5 tok poruka



Slika 10: Pojednostavljena EAP-TTLS razmjena poruka

3.5. Nadolazeći standardi i tehnologije

Kao odgovor na porast prijetnji bežičnim LAN-ovima, IEEE trenutno radi na nekoliko odvojenih inicijativa za poboljšanje sigurnosti bežičnih mreža. Prva uključuje IEEE 802.11 i radnu grupu TGi (engl. *Task group i*), koja preporuča značajne modifikacije postojećeg 802.11 standarda. TGi definira dodatnu enkripciju zasnovanu na novoizdanim AES-om (engl. *Advanced Encryption Standard*). AES zasnovano rješenje će omogućiti visoko otporno rješenje za budućnost, no zahtijevati će novi hardver i promjenu protokola. TGi trenutno dizajnira zahtjeve koji rješavaju poznate probleme WEP-a, uključujući prijevare, detekciju i odgovor na napade.

Slijedeća inicijativa za poboljšanje WLAN sigurnosti je WPA (engl. *WiFi Protected Access*) koji pokušava riješiti WEP probleme. Definiran je TKIP (engl. *Temporal Key Integrity Protocol*) za rješavanje problema bez zahtjeva za promjenom hardvera, zahtijevajući jedino promjene ROM softvera i pokretačkih programa.

Kako je IEEE 802.1X primarno razvijen za korištenje s IEEE 802 LAN-ovima, a ne za korištenje s bežičnim LAN-ovima, 802.11i probni standard definira dodatne mogućnosti zahtijevane za implementaciju IEEE 802.1X na 802.11 mrežama. Ovo uključuje zahtjeve za korištenje EAP metode podržavajući obostranu autentikaciju, upravljanje ključevima i otpor na poznate napade. Dodatno,

802.11i definira hijerarhiju korištenja s TKIP i AES šifriranjem i upravljanje ključeva četverosmjernim rukovanjem (engl. *handshake*), koje se koristi za osiguranje da je stanica autenticirana od strane pristupne točke i autentikacijskog poslužitelja, ukoliko je postavljen.

3.6. Implementacija bežičnih LAN-ova u radnoj okolini

U ovom poglavlju će biti objašnjen proces uspostave bežične sigurnosti u tvrtci ili organizaciji. Prije nego što se donese odluka o uspostavi, potrebno je na identificirati potencijalne ranjivosti i prijetnje. Nakon toga je potrebno napraviti evaluaciju rizika i analizu mogućih protumjera, te utvrditi da li troškovi i opasnosti za definiranu razinu zaštite prelaze prednosti koje bežični LAN-ovi donose.
Prilikom evaluacije rizika potrebno pažnju obratiti na slijedeća četiri područja:

- fizička sigurnost,
- lokacija pristupne točke,
- konfiguracija pristupne točke,
- sigurnosna politika.

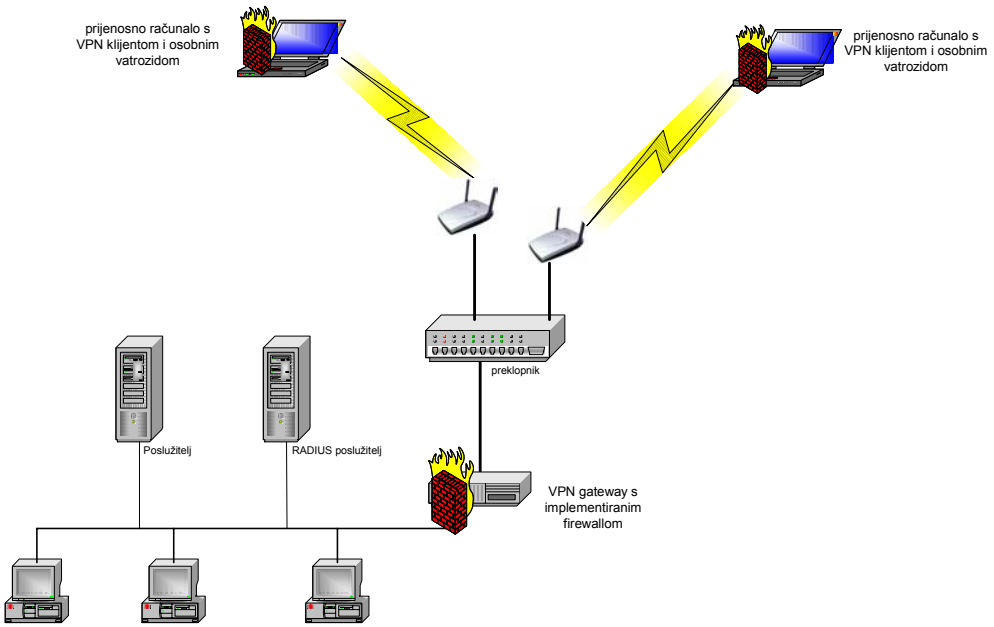
Za zaštitu fizičke sigurnosti vrlo je važno voditi računa da, ukoliko je to moguće, pristup u građevinu u kojoj se nalazi bežična mreža imaju samo osoblje i akreditirani gosti. Nadalje, vrlo je važno smjestiti pristupnu točku na sigurnom mjestu, na koje pristup imaju samo mrežni administratori.
Prilikom smještanja pristupnih točaka potrebno je minimalizirati mogućnost pristupa neautoriziranih korisnika bežičnoj mreži izvan građevine. Stoga je potrebno za svaku pristupnu točku odrediti najbolji položaj. Ovo uključuje sigurnosno mapiranje gdje korisnici imaju bežični pristup mreži. No, kako je nemoguće osigurati potpuni nestanak signala izvan građevine, korisnik s antenom koja ima veliki dobitak može prisluškivati mrežni promet. Zbog toga se bežična mreža postavlja izvan vatrozida i propušta promet preko VPN-a visoke razine enkripcije.
Prilikom uspostave bežičnog LAN-a, posebnu pažnju potrebno je posvetiti ranjivostima vezanim za konfiguraciju pristupne točke. Prije svega, potrebno je promijeniti inicijalne tvorničke postavke odabirući "čvrste" zaporke. Enkripciju je potrebno postaviti na maksimalnu vrijednost (obično 104 ili 128 bita duljine). Tamo gdje je to moguće, potrebno je koristiti MAC ACL. Kako mnogi proizvođači koriste inicijalne autentikacijske ključeve, neautorizirani uređaji mogu dobiti pristup mreži ukoliko poznaju inicijalni ključ. Zbog toga je potrebno propisati upotrebu korisničkog imena i zaporke kao dodatne metode autentikacije pristupnih točaka. Ukoliko se u mreži koristi SNMP, potrebno je zabraniti udaljeni pristup na ovaj servis i omogućiti ga jedino od strane internih uređaja.
Sigurnosna politika i procedure definiraju način postavljanja, održavanja i korištenja mreže. Prije svega, potrebno je zahtijevati od administratora redovno testiranje i primjenu sigurnosnih zakrpi i nadogradnji čim ih proizvođač izda. Nadalje, sigurnosna politika treba biti definirana na način da obeshrabri korisnike od procesiranja povjerljivih i privatnih podataka drugih korisnika unutar bežičnog LAN-a. Također, potrebno je razraditi procedure oko dodjeljivanja korisničkih računa, nabave novih uređaja (popis MAC adresa), postupaka u slučaju gubitka ili krađe prijenosnog uređaja.
Kao dodatna sigurnosna mjera preporuča se korištenje IDS-a. IDS utvrđuje da li neautorizirani korisnik pokušava pristupiti mreži, već joj je pristupio ili kompromitirao.
Zbog brzih promjena u razvoju tehnologije i pronalaženju novih ranjivosti, potrebna je stalna edukacija korisnika i administratora o rizicima i mjerama zaštite.

3.6.1. Preporučene mjere zaštite

U ovom poglavlju je dan popis mjera zaštite bežičnog LAN-a:

- Osiguranje fizičkog pristupa pristupnim točkama i mrežnim uređajima,
- Onemogućavanje dijeljenja direktorija i datoteka na računalima,
- Osiguranje osjetljivih datoteka zaporkom i enkripcijom,
- Rekonfiguriranje inicijalnih postavki Windows XP onemogućavanjem korištenja svih nesigurnih postavki,
- Isključivanje svih servisa na pristupnoj točki koji nisu neophodni,
- Korištenje preklopnika umjesto koncentratora za povezivanje pristupne točke s fiksnom mrežom (drugi sloj OSI modela),
- Ukoliko je moguće, korištenje fiksnih IP adresa umjesto dijeljenja DHCP-om,
- Uključivanje spremanja logova (ukoliko pristupna točka to podržava), te redovno praćenje,

- Educiranje korisnika, definiranje i provođenje bežične sigurnosne politike s posebnim naglaskom na:
  - Zabranu korištenje nezavisnog "*Ad hoc*" moda,
  - Zabranu postavljanja neautoriziranih pristupnih točaka "*rogue access point*",
  - Gašenje pristupne točke kada se ne koristi,
  - Reduciranje ili zabranjivanje korištenja aplikacija koje koriste veliki prijenosni pojas i slanje iznimno povjerljivih podataka,
- Dizanje niva sigurnosti pristupne točke i pritom:
  - Izabrati "snažnu" zaporku,
  - Koristiti (104/128-bitnu enkripciju),
  - Kreirati listu MAC adresa korisnika i omogućiti provjeru pristupnih točaka,
  - Promijeniti inicijalni SSID i onemogućiti njegovo razašiljanje (engl. *broadcast*),
  - Promijeniti inicijalne vrijednosti WEP ključeva,
  - Onemogućiti udaljeni SNMP.
- Provođenje istraživanja pokrivenosti signalom i strateško postavljanje pristupne točke,
- Uspostavljanje VPN tunela (*gateway* i klijent) s integriranim vatrozidom,
- Instaliranje osobnih vatrozida i antivirusnog softvera na strani klijenta,
- Istraživanje i odabiranje isključivo 802.11 produkata s najboljom dugoročnom bežičnom sigurnosnom strategijom i dugovječnosti na tržištu,
- Odabiranje proizvoda sa SNMP v3 (ili drugim načinom enkriptiranog nadzora i upravljanja) na pristupnoj točki i s integriranim vatrozid-VPN uređajem,
- Praćenje broja priključenih klijenata,
- Periodičko (najmanje tromjesečno) praćenje da li je postavljen "*rogue access point*". Dobro rješenje za to je besplatni alat NetStumbler ,
- Traženje pomoći eksperata koji će provjeriti sigurnosne prijetnje nakon postavljanja mreže, te periodički raditi ispitivanje.



Slika 11: Uspostava sigurnosti bežičnih LAN-ova

4. Zaključak

Bežične mreže pružaju veliku mobilnost, otvaraju nova područja primjene osobnih računala, ručnih računala i ostalih prijenosnih uređaja, no otvaraju i nove sigurnosne ranjivosti. Sigurnost bežičnih mreža zbog svojstava bežičnog medija je osjetljivija i treba joj posvetiti dodatnu pažnju. Prilikom odluke o primjeni bežičnih mreža potrebno je dobro analizirati potencijalne sigurnosne probleme, željeni stupanj zaštite i financijske izdatke potrebne za ostvarivanje tog stupnja zaštite. Zbog svojstava bežičnih mreža, one će vjerojatno predstavljati najosjetljiviji i napadu najizloženiji segment mreže. U ovom dokumentu je prikazan pregled potencijalnih ranjivosti i načina smanjivanja rizika. Koji stupanj zaštite će biti primijenjen prije svega ovisi o potrebi i mogućnostima. Bitno je naglasiti da je sigurnosni sustav dinamičan, te da je jedini način smanjivanja rizika na minimum redovito praćenje razvoja tehnologije, redovna primjena zakrpa i nadogradnje, precizno definirana sigurnosna politika i procedure, te stalna edukacija korisnika i administratora.

5. Popis kratica

AAA	Authentication Authorization Accounting
AP	Access Point (hr. pristupna točka)
BGP	Border Gateway Protocol
BSS	Basic Service Set
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EIGRP	Enhanced Interior Gateway Router Protocol
FHS	Frequency Hopping Spread
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	EAP protokol definiran od CISCO-a
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task For
IP	Internet Protocol
IPSec	IP Security
IR	Infrared
MAC	Medium Access Control
OSPF	Open Shortest Path First
OFDM	Orthogonal Frequency Division Multiplexing
PKI	Public Key Information
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Level Security
TTLS	Tunneled TLS
UMTS	Universal Mobile Telecommunications System
VPN	Virtual private network
WEP	Wireless Equivalent Privacy
WLAN	Wireless local area network