CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

WPA2 zaštita

CCERT-PUBDOC-2009-06-267

+CERT.hr u suradnji s LSS

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

Rezultat toga rada je i ovaj 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

Sigurnost u računalnim mrežama problem je kojim se korisnici najčešće ne zamaraju. Vjerojatno se radi o posljedici neinformiranosti i nedostatku svijesti opasnosti koje vrebaju. Posebnost komunikacijskih tehnologija je ta da su one običnom korisniku danas neophodne, a istovremeno izuzetno složene u smislu razumijevanja načina na koje funkcioniraju. To dovodi do situacije da ljudi koriste sustave koje ne razumiju, što opet dovodi do opasnosti od pogrešne uporabe. Primjerice, većina korisnika vjerojatno ne smatra uključenu *Bluetooth* komunikaciju na prijenosnom računalu ili mobitelu rizičnim ponašanjem, ali ukoliko njihov uređaj nema prikladnu zaštitu, napadač koji je dovoljno blizu (npr. susjedni stol u kafiću) može korištenjem zloćudnih programa upasti u sustav, pokrenuti prijenos podataka ili učiniti nešto slično. Čak štoviše, napadnuto računalo može bez znanja vlasnika štetne programe i širiti dalje.

Navedeni primjer samo je jedan mogući slučaj i način nanošenja štete računalima i korisnicima. Što su sustavi veći i što više osjetljivih podataka sadrže to se više pažnje treba posvetiti njihovoj zaštiti. Uz Internet koji predstavlja izvor opasnosti za lokalne mreže i računala koja su na njega povezana, sigurnosne probleme u računalnim sustavima stvara i bežična komunikacija. Ona je posebno izložena napadima jer se podaci neusmjereno i nekontrolirano odašilju u svim smjerovima u dometu odašiljača, te ih zbog takve karakteristike prijenosnog medija može bilo tko presresti. U ovom dokumentu razmatra se sigurnost bežičnih lokalnih računalnih mreža (WLAN – eng. Wireless Local Area Network) i dostupnih metoda zaštite. Budući da je danas WPA2 najnaprednije sigurnosno rješenje za zaštitu WLAN-a i računala u njemu, posebna će se pažnja posvetiti toj tehnologiji.

2. Bežična komunikacija

Otkad se pojavila mogućnost bežične komunikacije u telekomunikacijskim sustavima, njezina popularnost ne prestaje rasti. Korisnici je odabiru zbog jednostavnosti upotrebe koja ne zahtijeva uspostavljanje nikakvih žičnih veza. Osim toga, bežično se može komunicirati s proizvoljnih područja, uz uvjet postojanja odgovarajućeg signala. Najrašireniji sustavi za bežičnu komunikaciju danas su GSM i WLAN. GSM (eng. Global System for Mobile Communications) je standard kojim se definira komunikacija u okviru mobilne telefonije, a koji koristi preko tri milijarde korisnika u više od 212 država i teritorija diljem svijeta. Procjenjuje se da GSM zauzima preko 80% tržišta mobilne telefonije. WLAN su lokalne računalne mreže u kojima se komunikacija između računala odvija bez žice, a preko pristupnih točaka korisnici se mogu spajati na „obične" lokalne mreže – LAN (povezane žicom) te po potrebi preko njih na Internet. Kao uvod u WAP2 sigurnost dan je uvod u strukturu i obilježja WLAN mreža te u sigurnosne protokole koji su prethodili WAP2 zaštiti.

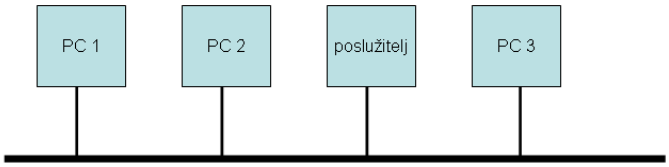
2.1. Bežične lokalne mreže (WLAN)

WLAN (eng. Wireless LAN) je bežična izvedba LAN (eng. Local Area Network) mreže. WLAN može biti cijela lokalna mreža ili samo jedan njezin dio. Poput lokalne mreže, i WLAN mreža prostorno je ograničena, a u dometu omogućuje komunikaciju između računala koja nisu žičano povezana na mrežu. Osim računala za koja je mreža namijenjena, ukoliko nema ugrađen sustav za zaštitu, na takvu se mrežu može spojiti bilo koje drugo računalo u njezinom dometu koje posjeduje mrežnu karticu. WLAN arhitektura zasniva se na LAN arhitekturi s tim da se uvode posebni uređaji i načini rada potrebni za bežičnu komunikaciju.

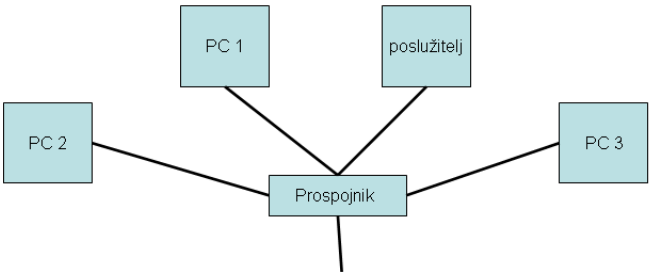
2.1.1. LAN

Lokalne mreže povezuju ograničeni broj računala na ograničenom prostoru. Karakteriziraju ih kvalitetni uvjeti komunikacije i relativno velika brzina prijenosa u odnosu na WAN (eng. Wide Area Network) mreže (do 1Gbps u odnosu na nekoliko Mbps) te mala kašnjenja i male vjerojatnosti pogreške u prijenosu. Komunikacija računala u lokalnoj mreži definirana je Ethernet (IEEE 802.3) standardom. LAN je pomoću usmjerivača (eng. router) i tzv. "*gateway*" uređaja moguće povezati na druge mreže s različitim ili istim komunikacijskim protokolima. LAN je obično u vlasništvu jedne organizacije i u njemu korisnici mogu komunicirati međusobno u boljim uvjetima jer manji prostor i manji broj računala koja se povezuju omogućuju kvalitetniju izvedbu mrežne arhitekture.

U LAN mrežu računala mogu biti povezana putem sabirnice u jednostavnijim arhitekturama, ili putem prospojnika (eng. switch) - uređaja koji komunikaciju čini bržom i učinkovitijom. Naime u mrežama bez preklopnika svako računalo komunicira sa svakim i prati je li poruka koja se šalje kroz mrežu namijenjena njemu. Preklopnik provjerava tok poruka pa zato svako računalo komunicira samo s jednim (ciljnim) računalom što onda omogućava paralelno komuniciranje više (nezavisnih) čvorova u mreži.



Jednostavna sabirnička arhitektura



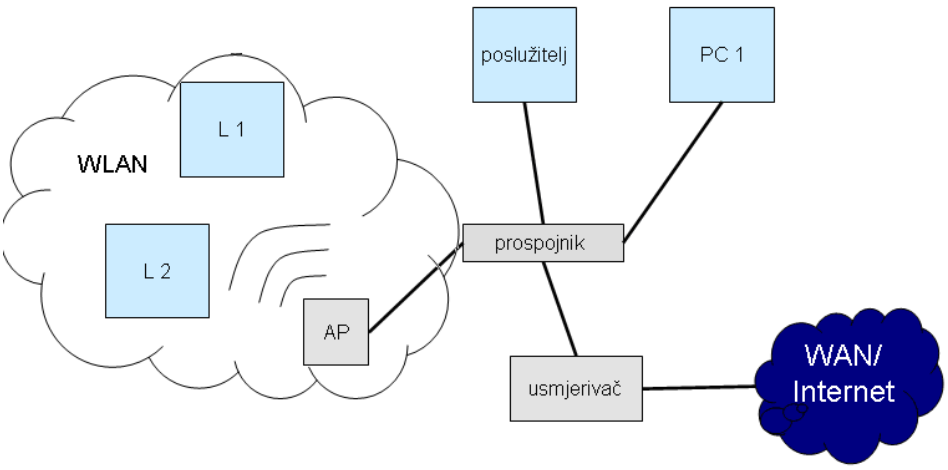
LAN arhitektura s prospojnim uređajem

Slika 1. Shematski prikaz arhitekture LAN-a

Na preklopni uređaj moguće je povezati usmjerivač koji prosljeđuje IP pakete na temelju IP adresa između dvije ili više mreža koje koriste iste komunikacijske protokole ili pristupnik (eng. „gateway“) koji omogućuje razmjenu paketa između mreža s različitim protokolima.

2.1.2. WLAN arhitektura i uređaji

WLAN mreža se na LAN povezuje pomoću pristupne točke (eng. AP – Access Point). Riječ je o uređaju koji omogućuje međusobno povezivanje žično povezanih mreža, bežičnih uređaja i uređaja s bežičnim karticama. Bežična komunikacija ostvaruje se primjenom Wi-Fi, Bluetooth ili drugih standarda za bežičnu komunikaciju. Prema IEEE 802.11 standardu kojim se specificira komunikacija u bežičnim mrežama, domet pristupne točke iznosi oko sto metara, a omogućuje komunikaciju s oko trideset računala.



Slika 2. Shema WLAN mreže

Usmjerivač i pristupna točka mogu biti objedinjeni u jednom uređaju koji istovremeno ima ugrađen preklopnik za žično spajanje računala u lokalnoj mreži. Na taj način smanjena je potreba za povezivanjem različitih uređaja (slika 3).

Slika 3. Bežični usmjerivač

2.1.3. IEEE 802.11 standard

IEEE (eng. Institute of Electrical and Electronics Engineers, Inc.) je neprofitna stručna udruga i vodeći autoritet na širokom tehničkom području od računalnih znanosti, biomedicinske tehnike i telekomunikacija, preko električne energije, potrošačke elektronike do mnogih drugih područja. IEEE je nastao 1884. godine, a utemeljen je na idejama nekolicine znanstvenika s ciljem praćenja razvoja elektrotehnike. Danas objavljuje više od četvrtine svih publikacija vezanih za elektrotehniku i računarstvo putem svojih znanstvenih i stručnih publikacija, skupova i IEEE normi. Već je spomenuta IEEE 802.3 ili *Ethernet* norma koja specificira komunikaciju između računala u LAN mreži. IEEE 802.11 je standard kojim se definira bežična komunikacija u WLAN mreži.

Prva inačica IEEE 802.11 standarda izdana je 1997. godine, a uvela je brzinu od 1 do 2 Mbit/s i tri različite tehnologije modulacije signala prilikom fizičkog prijenosa podataka:

1. IrDA (eng. Infrared Data Association) – standard za bežičnu komunikaciju kratkog dosega pomoću infracrvenog spektra elektromagnetskog zračenja,,
2. FHSS (eng. Frequency-Hopping Spread Spectrum) – omogućuje istovremenu komunikaciju većeg broja korisnika preko istog kanala i to zbog brzih izmjena frekvencija na kojima se prenosi informacija
3. DSSS (eng. Direct-Sequence Spread Spectrum) - informacija se prenosi preko cijelog frekvencijskog pojasa izravno, što ovu metodu čini otpornijom na smetnje od FHSS-a. Obje navedene metode koriste se za prijenos radio signala.

Nakon nje objavljen je niz prepravki standarda, a izvorna inačica je zastarjela i nije više u uporabi.

802.11a inačica standarda uvodi u uporabu relativno neiskorišten frekvencijski pojas od 5 GHz i povećava brzine prijenosa teoretski do 54 Mbit/s (realna efektivna propusnost je do 20 Mbit/s). 802.11b inačica standarda uvodi teoretske brzine od 11 Mbit/s u frekvencijskom pojasu od 2GHz, a najrasprostranjenija inačica danas je 802.11g koja u istom frekvencijskom pojasu postiže efektivne brzine prijenosa korisnih podataka od oko 20 Mbit/s.

Najnovija inačica standarda - 802.11n još je u razvojnoj fazi, a trebala bi uvesti značajno ubrzanje (brzine do 540 Mbit/s) na frekvencijama od 5 GHz. Iako još nije ušla u opću uporabu, već se mogu kupiti uređaji koji podržavaju *draft* inačicu 802.11n standarda, a može ih se prepoznati po 3 ugrađene antene.

2.1.4. Obilježja WLAN mreže

Pristup LAN mreži putem WLAN tehnologije korisnicima je omogućena bolja pokretljivost jer se ne moraju držati fizičke veze (UTP priključak) prilikom komunikacije s drugim računalima u mreži već se mogu nalaziti (i kretati) bilo gdje u prostoru do koda dopire radio signal kojeg emitira pristupna točka . Osim toga, bežična komunikacija lakše se uvodi od žične jer zahtijeva samo jednu pristupnu točku za proizvoljan broj računala (u praksi 20 – 30 računala mogu nesmetano paralelno komunicirati). Također, prilikom uvođenja novog računala u mrežu nisu potrebni nikakvi dodatni priključci.

Osim prednosti koje su vezane uz praktičnost uporabe, WLAN ima i određene tehničke nedostatke:

- **brzina prijenosa** – u većim i bržim mrežama gdje se brzine prijenosa mogu kretati i do 1 Gbps, WLAN sa brzinama manjim od 100 Mbps predstavlja usko grlo sustava, odnosno točku koja koči sustav u optimalnom radu,
- **domet** – WLAN je ograničen na domet od nekoliko desetaka metara (može se povećati uvođenjem dodatnih pristupnih točaka, ali ne bitno),
- **pouzdanost** – za razliku od žičnog prijenosa koji je zaštićen, bežični je izložen različitim interferencijama i smetnjama signala što dovodi do toga da se važni mrežni resursi koji moraju biti stalno dostupni u pravilu ne spajaju na mrežu putem WLAN-a,
- **sigurnost** – izloženost WLAN komunikacije čini ga izuzetno ranjivim na napade, upade u mrežu i krađu podataka koji se njome razmjenjuju.

Sigurnost WLAN-a osobito je kritičan problem, koji se može rješavati djelomičnim metodama poput statičkog IP filtriranja ili uvođenjem posebnih sustava zaštite (WEP, WPA, WPA2) koji će biti razmatrani u nastavku dokumenta.

2.2. Sigurnost bežične komunikacije

Bežične mreže sigurnosno su ugroženije od onih u kojima se podaci prenose putem žice zato što se podaci nekontrolirano prenose u cijelom radijusu dometa pristupne točke te svatko tko se nalazi u njemu može ih pokušati presresti. Napadi na bežično povezane dijelove sustava mogu se iskoristiti i za posredni napad na računala u unutrašnjem, žičano povezanom dijelu mreže.

Ključnu ulogu u zaštiti podataka koji se bežično prenose ima kriptografija zato jer se njome onemogućuju otkrivanje i mijenjanje podataka, lažiranje identiteta, poricanje slanja poruka i slični napadi. Iako su dostupne metode za zaštitu bežičnih mreža, najveći problem zapravo predstavlja nebriga korisnika i vlasnika mreže koji te metode ne primjenjuju.

2.2.1. Osnovni sigurnosni zahtjevi

Značajke sigurne komunikacije su:

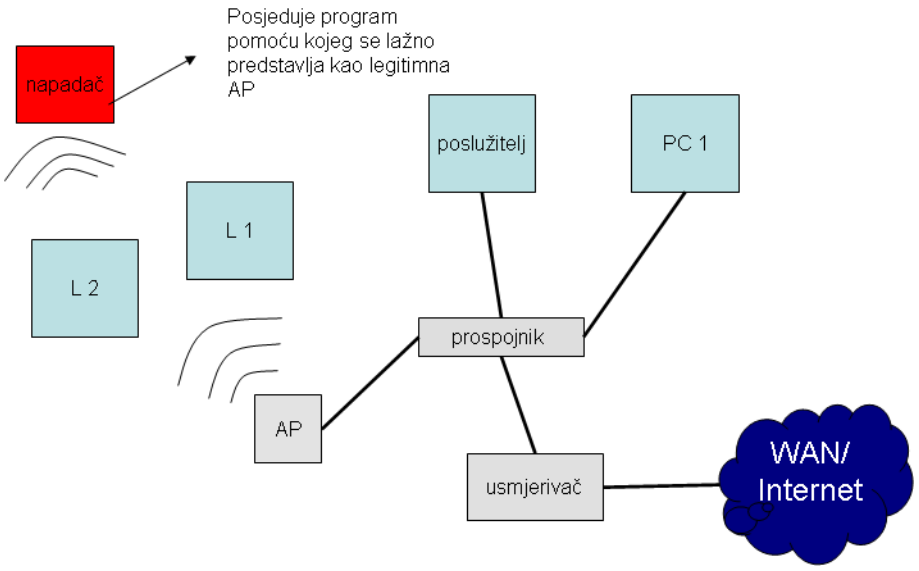
- **tajnost podataka** koji se prenose,
- **besprijekornost podataka** - sigurnost da nisu mijenjani u prometu,
- **autentičnost pošiljatelja** - onaj koji je naveden kao pošiljatelj to doista i jest i
- **neporecivost** - ako je netko poslao poruku ne može to kasnije poreći.

Najveći problem za bežične sustave predstavlja tajnost podataka koji se prenose i neovlašteno spajanje na bežičnu mrežu. Ukoliko se napadač uspješno spoji na nezaštićeni WLAN, može izvoditi različite štetne radnje na računalima u njoj ili čak u LAN mreži na koju je ranjivi WLAN spojen preko pristupne točke.

2.2.2. Napadi na WLAN

Neovlašteno pristupanje WLAN mrežama može se izvesti na nekoliko načina:

- slučajno povezivanje (eng. accidental association) - ako se u istom prostoru koristi više nezaštićenih bežičnih mreža, korisnik se slučajno može spojiti na krivu mreži i time možda dovesti u opasnost sebe i tuđi sustav.
- zlonamjerno povezivanje (eng. malicious association) - izvodi se posebnim programima koji mrežnu karticu napadača predstavljaju kao legitimnu pristupnu točku (napadačeve) mreže. Posljedica uspješnog napada je ta da se sav mrežni promet te bežične mreže preusmjerava kroz napadačevo računalo (slika 4).



Slika 4. Shema napada zlonamjernim povezivanjem

- ad-hoc mreže – budući da se u ovakvim mrežama komunikacija odvija bez pristupne točke, tj. izravno između dva računala (eng. peer-to-peer) i da se često ne koriste zaštitne metode kakve se mogu uvesti kroz pristupnu točku, sustav je osjetljiviji na lažno predstavljanje, otkrivanje podataka i druge vrste napada.
- netradicionalne mreže – podrazumijevaju *Bluetooth* i slične tehnologije čijoj se sigurnosti zbog kratkog dometa komunikacije često ne pridaje dovoljno pažnje. To pak otvara prostor napadačima za različite zlouporabe.
- krađa identiteta – ako je omogućeno prisluškivanje mrežnog prometa (podaci nisu kriptirani), napadač može saznati MAC (eng. Medium Access Control) adrese računala koje se koriste u lokalnoj mreži i pomoću nekog alata lažno se predstaviti kao ovlašteni korisnik mreže.
- napadi posredovanjem u komunikaciji (eng. man-in-the-middle) – ukoliko se, primjerice, uspješno izvede napad zlonamjernog povezivanja, napadač može saznati osjetljive podatke koje zatim može koristiti za posredovanje u komunikaciji tako da su krajnji korisnici nesvjesni da podatke šalju posredniku i primaju putem posrednika (koji se predstavio kao pristupna točka).
- mrežno ubacivanje (eng. network injection) – ova vrsta napada cilja na izmjenu radnih postavki mrežnih uređaja kao što su usmjerivači i preklopni uređaji, a kojima se iz WLAN mreže pristupa pomoću pristupne točke.

3. WPA2 zaštita bežičnih mreža

U zaštiti bežičnih mreža mogu se koristiti djelomične metode za zaštitu od upada u mrežu kao što su statičko IP filtriranje ili filtriranje na razini MAC adresa. Statičko IP filtriranje zahtjeva korištenje statičkih IP adresa za računala i zabranjuje pristup mreži svim računalima koja imaju nedozvoljenu IP adresu. To nije potpuna zaštita zato što se IP adrese mogu lažirati, a i u takvom sustavu onemogućeno je dinamičko dodjeljivanje IP adresa računalima. MAC filtriranje zasniva se na identifikacijskim brojevima mrežnih uređaja koji su ugrađeni prilikom proizvodnje u ROM. MAC sadrži dvije informacije: identifikacijski broj proizvođača i oznaku uređaja u seriji. Ipak niti ovakva vrsta zaštite nije dovoljna jer su dostupni programi kojima je moguće lažirati MAC adresu. Potpuna i prava zaštita bežične mreže postiže se korištenjem posebno oblikovanih protokola kao što su WEP, WPA i WPA2. U nastavku poglavlja dan je uvod u navedene protokole s naglaskom na WPA2 zaštiti.

3.1. WEP

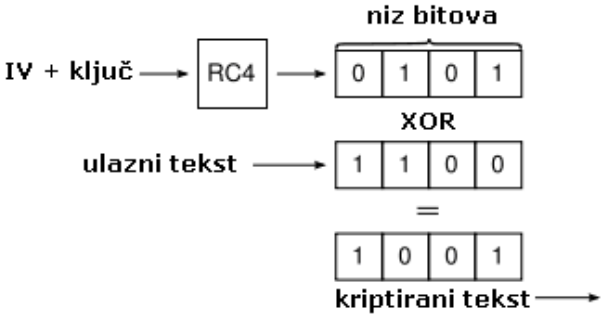
WEP (eng. Wireless Encryption Protocol) je protokol za zaštitu bežičnih mreža, opisan IEEE standardom 802.11b. WEP zaštita odnosi se na fizički i sloj podatkovne poveznice (OSI model računalne mreže) u računalnoj mreži, a temelji se na enkripciji podataka između krajnjih točaka. WEP koristi kriptografske ključeve standardnih duljina od 64, 128 i 256 bita. Optimalna duljina ključa je ona koja onemogućuje njegovo otkrivanje (što veća), a da se enkripcija istovremeno može obaviti što brže (što manja). Kriptiranje i dekriptiranje podatka obavlja se tajnim ključem u krajnjim točkama, a protokol uključuje provjeru integriteta poruke i provjeru identiteta korisnika, odnosno metode kojima se može utvrditi je li poruka bila mijenjana između izvorišta i odredišta.

WEP enkripcija koristi RC4 sustav za kriptiranje podatkovnih tokova, koji na temelju ključa stvara pseudo nasumičan niz kojim se pomoću XOR funkcije kriptira ulazna poruka. Poznavanjem ključa moguće je upotrebom iste funkcije niz dekriptirati na odredištu.

Definicija XOR funkcije je sljedeća:

XOR(1,1) = 0
XOR(0,0) = 0
XOR(1,0) = 1
XOR(0,1) = 1

Na sljedećoj slici dana je shema RC4 kriptiranja:

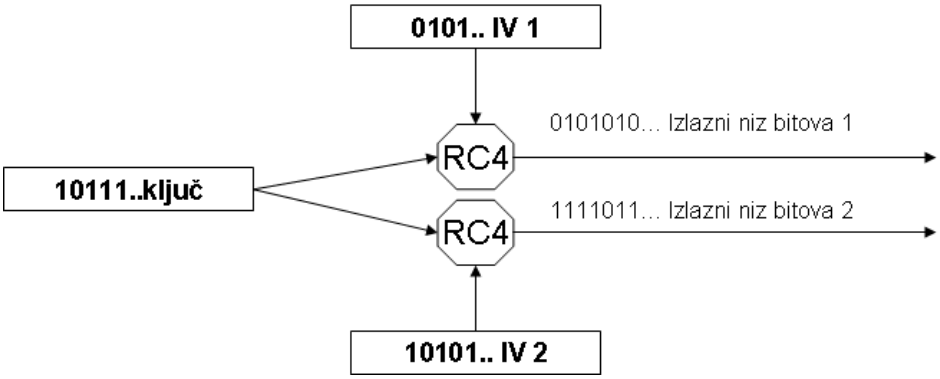


Slika 5. Shema RC4 kriptiranja

3.1.1. Razbijanje WEP enkripcije

Slaba točka WEP protokola upravo je enkripcija podataka. Zbog toga što WEP kriptira bit po bit ulaznog niza, ne smije se dopustiti da se niz bitova kojima se kriptira tekst. Razlog tome leži u činjenici da ukoliko napadač ima mogućnost prisluškivanja mreže te zna kako se stvara niz u RC4 algoritmu kriptoanalizom može otkriti tajni ključ. Kako bi se izbjeglo ponavljanje nizova kojima se kriptiraju podaci uz ključ se u RC4 poruci šalje i proizvoljni inicijalizacijski vektor (IV). Ipak za mreže kroz koje prolazi velika količina prometa 24-bitnih inicijalizacijskih vektora postoji i velika vjerojatnost ponavljanja istog niza (npr. isti niz ponovit će se s vjerojatnošću od čak 50% nakon

5000 kriptiranih paketa). Dodatan problem je taj što korisnici za vrijednosti ključa često uzimaju predvidljive nizove, što kriptoanalitičarima dodatno olakšava posao.



Slika 6. Shema stvaranja različitih kriptografskih nizova pomoću različitih IV

Prvi napad na WEP izveden je 2001. godine i tada je pokazano da se privatni ključ može, prisluškivanjem mreže, otkriti za manje od jedne minute. Napad je ubrzo nakon toga i programski izveden, a 2005. je pokazano da se za tri minute može ostvariti neovlašten pristup bilo kojoj mreži zaštićenoj WEP metodom i to uz pomoć javno dostupnih programskih alata.

3.1.2. Poboljšani WEP

Nakon što je dokazana nesigurnost WEP protokola, izašle su njegove poboljšane inačice:

- WEP2 – uključuje povećanu vrijednost inicijalizacijskog vektora IV i ključa na 128 bita
- WEPplus - povećana učinkovitost onemogućivanjem korištenja loše oblikovanih IV vektora koji se lako otkrivaju, a posebno je učinkovit ako se koristi na oba kraja veze i
- Dynamic WEP – mijenja ključeve dinamički.

Problem kod poboljšanih inačica WEP-a je taj što ih ne podržavaju svi proizvođači, nisu pogodne za izvedbu zbog velog zahtjeva za procesorskom snagom, a i ne omogućavaju zadovoljavajuću zaštitu (i dalje postoje metode koje više ili manje uspješno zaobilaze ovaj tip zaštite). Zato se za poboljšanje sigurnosti bežičnih mreža koristi WPA/WPA2 protokol.

3.2. WPA/WPA2

WPA2 je najrašireniji sustav zaštite bežičnih lokalnih mreža, a razvijen je u okviru Wi-Fi Alliance udruženja 2004. godine. Riječ je o poboljšanoj inačici WPA protokola nastalog u okviru iste organizacije. U ovom poglavlju razmatra se WPA protokol kao prethodnik WPA2 protokola, zatim načini postizanja sigurnosti u WPA2 protokolu te poboljšanja koja on uvodi u odnosu na WEP i WPA protokole. No najprije slijedi kratak uvod u rad Wi-Fi organizacije koja potiče razvoj WLAN tehnologija i certificira proizvode koji ih kvalitetno ostvaruju.

3.2.1. Wi-Fi Alliance

Wi-Fi Alliance je globalno neprofitno udruženje tvrtki kojima je cilj unaprjeđenje i promicanje Wi-Fi tehnologije na tržištu. Udruženje je osnovano 1991. godine, a danas broji preko tristo članova u više od 20 zemalja. Wi-Fi Alliance razvija i provodi provjere kvalitete proizvoda koji primjenjuju IEEE 802.11 standard. Svrha takvih provjera je osigurati kvalitetu proizvoda koji korisnicima omogućuju korištenje bežičnih lokalnih mreža.

U okviru Wi-Fi Alliance udruženja provodi se nekoliko obaveznih i proizvoljnih certifikacijskih programa. Obavezni uključuju:

- provjeru zadovoljavanja IEEE specifikacija 802.11a, 802.11b, 802.11g u jednostrukom ili dvostrukom načinu rada (802.11b i 802.11g) te u višepojasnom načinu rada (2.4GHz and 5GHz),

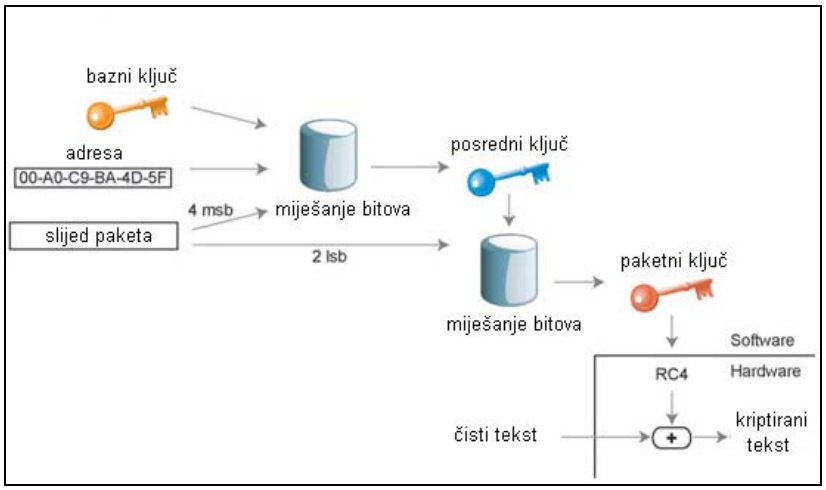
- provjeru zadovoljavanja sigurnosnih protokola WPA (eng. Wi-Fi Protected Access) i WPA2 (eng. Wi-Fi Protected Access 2) za osobne i poslovne korisnike te
- provjeru EAP (eng. Extensible Authentication Protocol) protokola za provjeru identiteta mrežnih uređaja.

Wi-Fi logo na certificiranim proizvodima znači da su oni prošli rigorozne provjere kojima je utvrđena sukladnost sa svim drugim Wi-Fi certificiranim proizvodima neovisno o njihovim proizvođačima.

Slika 7. Wi-Fi logo

3.2.2. WPA

WPA (eng. Wi-Fi Protected Access) je sustav zaštite bežičnih mreža, opisan u okviru IEEE 802.11i standarda, koji omogućuje enkripciju podataka i provjeru identiteta korisnika. Kao i WEP, i WPA koristi RC4 sustav za kriptiranje podataka i to uz 128-bitni ključ i 48-bitni inicijalizacijski vektor (IV). Prednost nad WEP standardom je u korištenju TKIP protokola (eng. Temporal Key Integrity Protocol), koji 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 ključa kod primjene WEP protokola. Naime, slabosti prethodnih sustava ležale su u premalom broju mogućih inicijalizacijskih vektora koji su uz isti tajni ključ davali nesigurne nizove podataka. To znači da je analizom tih nizova bilo moguće otkriti vrijednosti ključa. Na ovaj način opisani algoritam napada gotovo je nemoguće iskoristiti.



Slika 8. Shema TKIP protokola
Izvor: SmartBridges

Uz spomenuta unaprjeđenja, WPA protokol također donosi i sigurniji sustav provjere besprijekornosti poruke u odnosu na CRC (eng. Cyclic Redundancy Check) sustav koji se koristi kod WEP protokola. Naime, kod CRC provjere napadač može promijeniti sastav poruke koja se šalje i vratiti vrijednost CRC-a na izvornu, čak i bez poznavanja ključa kojim je poruka kriptirana. Sigurniji način provjere je korištenje tzv. „Michael" (MIC - eng. Message Integrity Code) koji u WPA uključuje brojač okvira čime se isključuje mogućnost promjene sastava poruka u komunikacijskom kanalu (detaljnije opisano u poglavlju o CCMP enkripciji). Michael algoritam izveden je tako da bude dovoljno siguran, a da ga je ipak moguće koristiti na starijim mrežnim karticama.

3.2.3. Poboljšanje u odnosu na WEP i nedostaci WPA protokola

Već je spomenuto kako je jedno od glavnih poboljšanja WPA i WPA2 tehnologija u odnosu na WEP uvođenje TKIP (eng. Temporal Key Integrity Protocol) protokola. Osim sigurnije provjere besprijekornosti poruke koja je opisana u prethodnom poglavlju, TKIP koristi složenije funkcije za stvaranje niza bitova kojima se kriptira tekst. Na taj način napadaču se otežava otkrivanje tajnog ključa prisluškivanjem mrežnog prometa. Osim toga, TKIP jamči da je svaki paket u mreži kriptiran drukčijim ključem.

U studenom 2008. godine otkrivena je ranjivost TKIP protokola koju napadač može iskoristiti za otkrivanje niza bitova kojima je kriptiran određeni paket. Napad je pritom moguće izvesti samo na kratkim porukama većinom poznatog sadržaja kao što su ARP (eng. Address Resolution Protocol) poruke za otkrivanje sklopovske adrese na temelju mrežne adrese uređaja. Posljedice uspješne zlouporabe mogu biti podmetanje lažnih ARP paketa ranjivom klijentu. Ova se ranjivost odnosi samo na WPA (ne i na WPA2) protokol.

3.3. Osobitosti WPA2 protokola

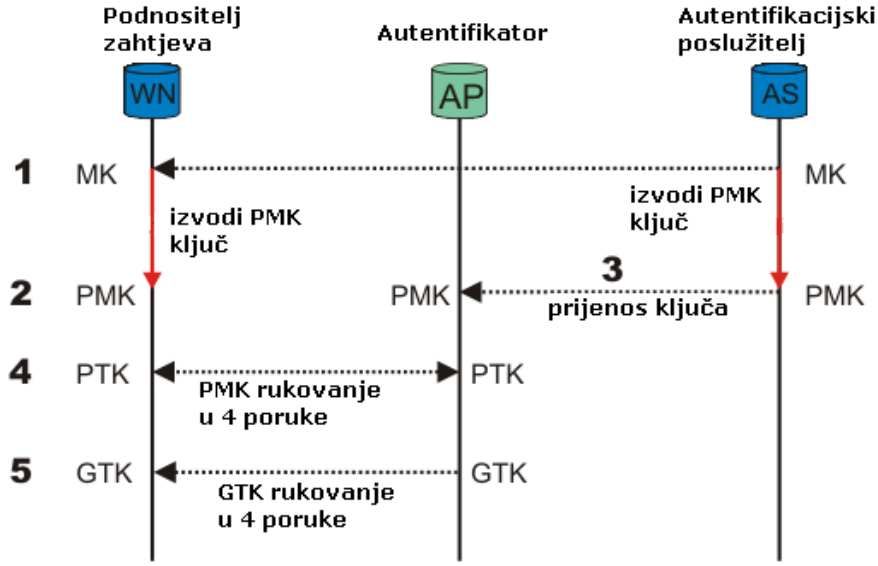
U prethodnom poglavlju dan je uvod u poboljšanja koja WPA i WPA2 uvode u odnosu na WEP sustav zaštite bežičnih mreža. U ovom poglavlju prikazane su glavne metode WPA2 zaštite te njezina unaprjeđenja u odnosu na WPA zaštitu. WPA2 se kao i WPA temelji na IEEE 802.11i standardu i uključuje sve mehanizme koje koristi WPA s tim da uvodi i dodatna poboljšanja od kojih je možda najvažnija CCMP enkripcija. Sigurnosni dio IEEE specifikacije koji opisuje enkripciju i sigurnu komunikaciju među čvorovima u bežičnoj mreži naziva se i Robust Security Network (RSN) model.

3.3.1. WPA2 autentikacija

U okviru WPA protokola spomenuta je EAP (eng. Extensible Authentication Protocol) autentikacija. Ona je zadržana i kao dio WPA2 protokola. EAP definira format poruka koje se izmjenjuju prilikom bežične autentikacije. Protokoli koji koriste EAP metodu moraju definirati način na koji će se te poruke enkapsulirati u podatkovne pakete. Ova metoda autentikacije izvodi se na sloju podatkovne poveznice kao PPP (eng. Point-to-Point Protocol) protokol. Riječ je o metodi izravnog povezivanja dvaju čvorova u mreži pri čemu se omogućuje i zaštita komunikacije (autentikacija i enkripcija). Prilikom autentikacije u WPA2 protokolu izvodi se i razmjena ključeva pomoću kojih će se kriptirati podaci koji se šalju. WAP2 autentikacija izvodi se dinamičkim protokolom koji uključuje razmjenu u četiri koraka – svi potrebni podaci kojima se jamči sigurnost kasnije komunikacije razmjenjuju se u četiri poruke. Nakon što se EAP autentifikacijom razmjeni PMK (eng. Pairwise Master Key) ključ, on se koristi za razmjenu PTK (eng. Pairwise Transient Key) ključeva koji se zatim mogu koristiti za enkripciju, dokazivanje posjedovanja PTK ključa te za distribuciju GTK (eng. Group Temporal Key) ključa. On se pak koristi za dekripciju tzv. „broadcast" i „multicast" prometa koji se šalje većem broju uređaja ili svim uređajima u mreži.

Naziv ključa	Uporaba ključa
Master Key (MK)	Za izvođenje tajnog PMK ključa
Pairwise Master Key (PMK)	Za razmjenu PTK tajnog ključa
Pairwise Transient Key (PTK)	Za enkripciju, razmjenu GTK ključa, dokazivanje identiteta
Group Temporal Key (GTK)	Za dekripciju *multicast* i *broadcast* prometa

Tablica 1. WPA2 autentifikacijski ključevi



Slika 9. Shema WPA2 autentifikacije i razmjene ključeva

Izvor: 802.1X Port-Based Authentication HOWTO

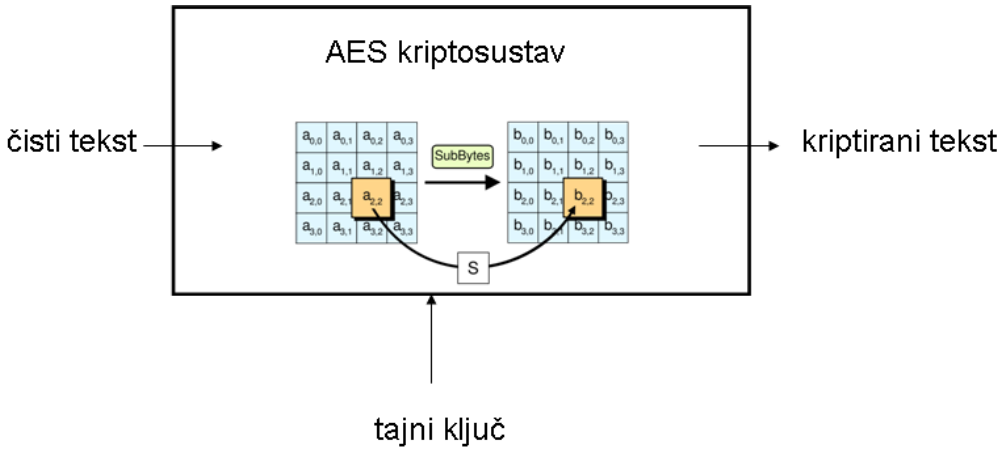
Inačice EAP autentifikacije podržane u WPA/WPA2 sustavima su:

- EAP-TLS,
- EAP-TTLS/MSCHAPv2,
- PEAPv0/EAP-MSCHAPv2,
- PEAPv1/EAP-GTC i
- EAP-SIM.

3.3.2. CCMP enkripcija

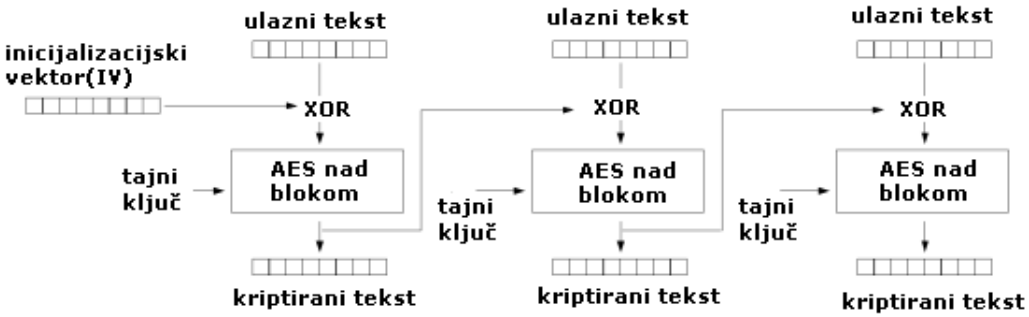
Kao odgovor na slabost TKIP enkripcije kod WPA protokola, WPA2 uvodi CCMP (eng. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol enkripciju koja se temelji na AES algoritmu i ulančanom kriptiranju blokova.

AES (eng. Advanced Encryption Standard) je simetrični kriptografski algoritam koji podatke kriptira po blokovima od 128 bita, a ključ kojim se kriptira može biti veličine 128, 192 ili 256 bita. Algoritam se provodi u više koraka, a ključan trenutak je zamjena bitova na temelju nelinearnih supstitucijskih tablica (Rijndael S-box). Ovakva enkripcija podataka smatra se potpuno sigurnom.



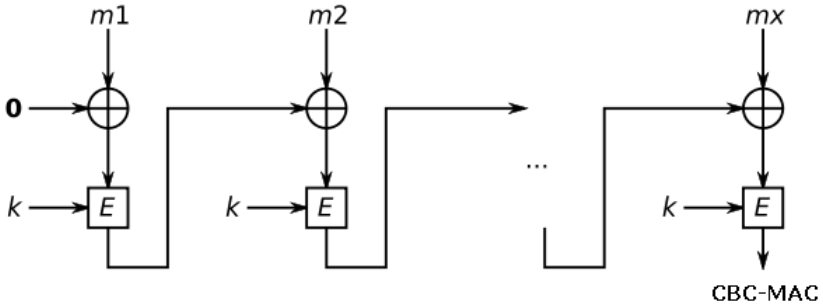
Slika 10. AES kriptosustav

Osim AES-a, CCMP uvodi način rada koji koristi brojač i ulančano kriptiranje blokova za izradu autentifikacijske oznake poruke. Ulančano kriptiranje blokova znači da tekst dijeli na blokove nad kojima se prije kriptiranja izvodi XOR operacija s kriptiranim prethodnim blokom. Za prvi blok definira se nekakav proizvoljni inicijalizacijski vektor.



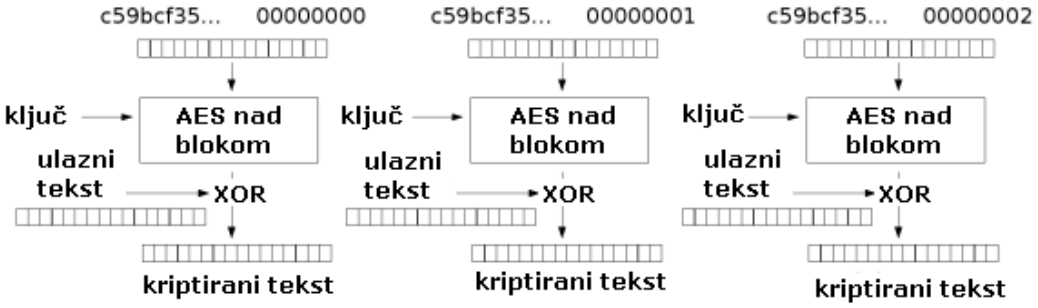
Slika 11. CBC kriptiranje

Kod CBC-MAC (eng. Cipher Block Chaining Message Authentication Code Protocol) izrade autentifikacijske oznake poruke inicijalizacijski vektor postavlja se na tzv. „nul-vektor“, odnosno sve vrijednosti u vektoru postavljaju se na nulu., MAC je zapravo izlaz zadnjeg kriptiranog bloka (broj blokova proporcionalan je s veličinom poruke koja se kriptira). Na taj način osigurava se da promjena bilo kojeg bita u čistom ulaznom tekstu mijenja konačni MAC kod.



Slika 12. CBC izrada MAC oznake

Counter mode kriptiranje znači da se kod kriptiranja blokova zapravo kriptira inicijalizacijski vektor čija se ulazna vrijednost u svakom koraku povećava, a zatim se nad takvim kriptiranim vektorom i ulaznim blokom izvodi XOR funkcija.



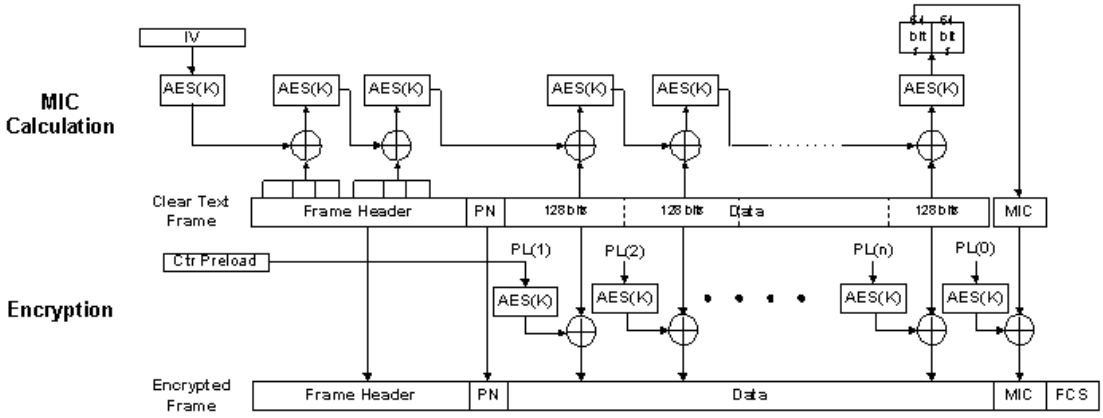
Slika 13. Counter mode kriptiranje blokova

CCMP MPDU (eng. Medium Access Control Protocol Data Unit) podatkovni paketi sastoje se od pet dijelova:

1. MAC zaglavlje,
2. CCMP zaglavlje,
3. podatkovna jedinica,
4. MIC (eng. Message Integrity Code) kod i
5. FCS (eng. Frame Check Sequence) niz za provjeru okvira.

Od navedenih dijelova, jedino se podatkovna jedinica i MIC kod kriptiraju.

Na sljedećoj slici dana je cjelokupna shema CCMP kriptiranja:



Slika 14. Izrada CCMP podatkovnog okvira

Izvor: Michigan Tech

CCMP enkripcija može se sažeti u sljedeće korake:

1. podijeliti sadržaj na blokove,
2. prepisati zaglavlje i broj paketa u izlaznu poruku,
3. pomoću AES algoritma i brojača kriptirati blokove i zapisati ih u izlaznu poruku,
4. pomoću AES algoritma i inicijalizacijskog vektora izračunati MIC i zapisati ga iza podataka u izlaznu poruku te
5. izračunati niz za provjeru okvira (FCS) i zapisati ga na kraj poruke.

CCMP dekripcija može se sažeti u sljedeće korake:

1. pročitati zaglavlje, broj paketa i FCS broj,
2. provjeriti FCS paketa,
3. podijeliti sadržaj na blokove,
4. pomoću brojača i AES-a dekriptirati blokove te
5. pomoći AES-a i inicijalizacijskog vektora izračunati MIC i usporediti s onim zapisanim u paketu

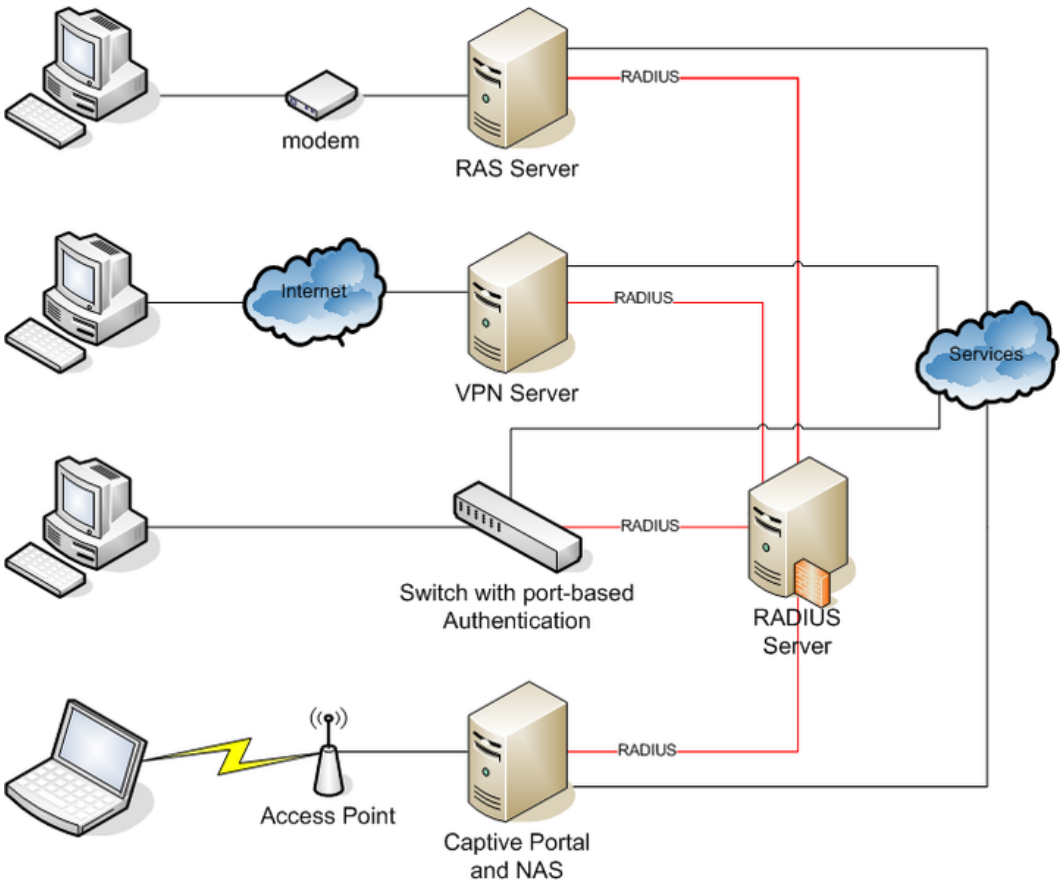
3.3.3. Načini korištenja protokola

WPA i WPA2 protokoli mogu se koristiti na dva načina:

1. PSK (eng. Pre-Shared Key) – podrazumijeva prethodnu razmjenu ključeva između pristupne točke i svih klijenata.
2. Enterprise – podrazumijeva zaseban ključ između pristupne točke i svakog klijenta.

PSK način rada još se naziva i privatni (eng. personal) i namijenjen je privatnim mrežama ili manjim poslovnim mrežama. Bitno je jednostavniji za izvedbu od Enterprise sustava jer ne zahtjeva autentifikacijski poslužitelj, već se jednostavno definira jedinstveni 256 bitni ključ koji se koristi za svu komunikaciju u mreži. Taj se ključ može unijeti kao 64 heksadecimalne znamenke ili niz od 8 do 63 ASCII znakova na temelju kojeg se računa ključ. Budući da za 256 znakova postoji ~10^{78} mogućih kombinacija, ključ je nemoguće izračunati iz *hash* vrijednosti u razumnom vremenu. Ukoliko korisnik unese predvidljive nizove znakova, tada napadačima otkrivanje ključa može olakšati tzv. „brute force" napad koji podrazumijeva pretraživanje prostora svih mogućih kombinacija. Upravo zbog toga dobra je praksa nelogičnih, nasumičnih nizova znakova prilikom stvaranja ključa.

Enterprise način pak nudi bolju zaštitu jer se svaki uređaj u mreži mora autentificirati (identificirati i ovjeriti identitet lozinkom), no uvođenje i održavanje takvog sustava zahtijeva bitno više posla. WPA Enterprise autentifikacija opisana je u poglavlju o WPA2 autentifikaciji koja se temelji na IEEE 802.1x standardu[7]. WPA2 Enterprise autentifikacijski poslužitelji koriste RADIUS (eng. Remote Authentication Dial In User Service) mrežni protokol za centraliziranu autentifikaciju.



Slika 15. Provjera pristupa u poslovnoj mreži koja koristi RADIUS protokol
Izvor: Wikipedia

3.3.4. Usporedba WPA i WPA2 protokola

Osim razlike u primjeni robusnijeg i sigurnijeg algoritma enkripcije u WPA2 protokolu (CCMP), WPA i WPA2 protokoli zapravo su vrlo slični. WPA2 podržava TKIP protokol, tj. kompatibilan je s WPA protokolom. Valja napomenuti i kako su nesigurnosti WPA zaštite proizašle zapravo iz ograničena nametnutih prilikom oblikovanja tog protokola. Smisao ograničenja bila je sukladnost WPA s dokazano ranjivim WEP protokolom, odnosno zamjena ranjivog WEP-a na starijim mrežnim karticama. Bez obzira na manji broj otkrivenih ranjivosti, WPA se još uvijek smatra sigurnim protokolom. WPA2 je njegova napredna inačica koja se koristi na novijim sustavima.

3.4. Konfiguracija WPA2 zaštite na pristupnoj točki

Kod konfiguracije pristupne točke potrebno je uvesti i neku vrstu zaštite. Hoće li to biti WEP, WPA, WPA2 ili neke metode poput MAC filtriranja, IP filtriranja ili isključivanja SSID (eng. Service Set Identifier) mreže, ovisi o potrebama korisnika. Zadnje tri metode ne predstavljaju potpunu zaštitu mreže, ali mogu biti dovoljne za mreže kojima se ne razmjenjuju osobito osjetljive informacije i koje se ne smatraju osobito ugroženima. WEP, WPA i WPA2 predstavljaju potpune sustave zaštite. Uzimajući u obzir ranjivosti WEP-a, prednost se daje WPA i WPA2 sustavima. Oba su sustava vrlo sigurna s tim da WPA2 kao sustav nove generacije ipak uključuje moćniju zaštitu. Ukoliko se korisnik odluči na korištenje WPA2 zaštite može konfigurirati njezinu Enterprise ili Personal inačicu.

Prilikom konfiguracije pristupe točke za Enterprise sigurnost potrebno je proći sljedeće korake (postupak je specifičan za različite AP uređaje, ovo su samo okvirne upute):

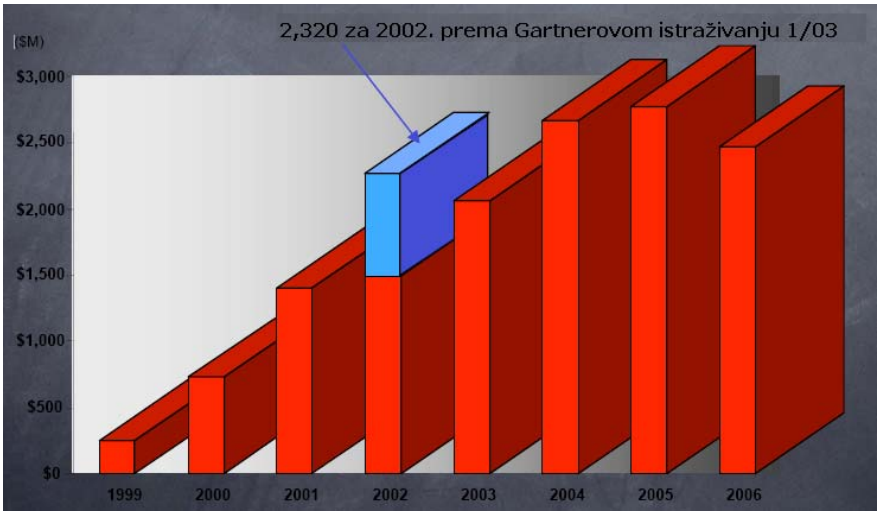
- odabrati SSID mreže,
- konfigurirati AP točku kao RADIUS poslužitelj,
- odabrati LEAP (eng. Lightweight Extensible Authentication Protocol) protokol za komunikaciju između RADIUS poslužitelja i bežičnih klijenata,
- odabrati komunikacijske priključke (eng. port) i tajni kod za RADIUS poslužitelj,
- odabrati AES-CCMP enkripciju,
- odabrati EAP autentifikaciju.

Konfiguracija WPA2 zaštite u Personal, odnosno PSK načinu nešto je jednostavnija i uključuje sljedeće korake:

- odabrati SSID-a mreže,
- odabrati AES-CCMP enkripciju,
- odabrati PSK autentifikaciju,
- unijeti PSK ključ koji se sastoji od barem dvadeset znakova ili dvadeset i četiri heksadecimalne znamenke.

3.5. Budućnost sigurnosti WLAN mreža

WLAN tržište u stalnom je porastu kao i drugi oblici bežičnih komunikacija. Cilj je danas omogućiti što bržu razmjenu informacija i što jednostavniji pristup do njih, a oblikovanje komunikacijskih sustava podređuje se tim zahtjevima.



Slika 16. Rast prodaje WLAN uređaja
Izvor: In-Stat/MDR, 7/02

Pitanje sigurnosti pritom nije zanemarivo, osobito kada se radi o većim poslovnim mrežama u kojima kolaju vrlo važne informacije. Trenutno, WPA2 sustav predstavlja dostatnu zaštitu takvih mreža po pitanju tajnosti podataka i autentičnosti sudionika komunikacije. Do sada nije zabilježeno uspješno narušavanje tajnosti i autentičnosti komunikacije uz WPA2 zaštitu. Otkrivene su neke metode koje ubrzavaju otkrivanje ključa tzv. „brute force" metodama koje ispituju sve moguće vrijednosti ključa. No za otkrivanje ključa na ovaj način potrebna je golema i skupa računalna snaga tako da nema realne opasnosti. Ipak, osjetljivost na DoS (eng. Denial of Service) napade koji se mogu izvoditi slanjem velikog broja (lažnih) paketa i zagušuju mrežni promet i dalje ostaje sigurnosni problem. Osim toga, pokazuje se da najveći izvor nesigurnosti predstavljaju sami korisnici neodgovornim i nepažljivim ponašanjem. To nije samo slučaj s bežičnom komunikacijom, već s telekomunikacijskim sustavima općenito.

Uz WPA2, kao relativno nov i dobar sustav, može se očekivati njegova dominacija u bližoj budućnosti. No bez sumnje, sa širenjem i napretkom tehnologije, napredovat će i napadi na tehnologiju pa se od nje očekuje držanje nekoliko koraka ispred. Osim toga, nevezano uz tehnologiju koja se rabi, ono što u svakom slučaju treba stalno rasti jest svijest korisnika o mogućim izvorima opasnosti kod korištenja telekomunikacijskih sustava.

4. Zaključak

Bežične lokalne mreže sve se češće koriste. Njihova dostupnost što se tiče cijene i izvedbe usporediva je s običnim lokalnim mrežama (LAN), dok su pogodnosti njihovog korištenja bitno veće. Bežična komunikacija korisniku daje slobodu kretanja, a samim time brži i lakši pristup izvoru informacija. Osim toga, na bežične mreže lakše se povezuje veći broj korisnika. Možda najveću prepreku u njihovu korištenju danas predstavlja brzina prijenosa podataka i nestabilnost komunikacije koji zaostaju za klasičnim LAN-ovima.

Kad se govori o bežičnim lokalnim mrežama, kao posebno važno nameće se pitanje sigurnosti. Budući da su takve mreže izložene napadačima kao što su izložena i nezaštićena računala na Internetu, potrebno je uvesti dodatne sigurnosne protokole u komunikaciju u takvim lokalnim mrežama. Za razliku od LAN-a koji je, ako nije povezan na vanjsku nesigurnu mrežu, potpuno siguran, WLAN to nije. Kako bi se zaštitila komunikacija u WLAN mreži osmišljeno je nekoliko protokola. Prvo se radilo o WEP protokolu za koji je kasnije pokazano da je nesiguran. Kao odgovor na slabosti WEP-a razvijeni su protokoli WPA i WPA2. WPA posjeduje neke slabosti, dok je WPA2 danas najbolji sustav zaštite bežičnih mreža. WPA2 uključuje autentifikaciju mrežnih uređaja, kriptiranje podataka koji se šalju mrežom i zaštitu integriteta poruka koje se šalju. Međutim, osjetljivost na napade uskraćivanjem usluge upotrebom ove tehnologije nije moguće otkloniti. WPA2 se može koristiti za privatne mreže ili za poslovne mreže i za to se može prilagoditi u dva načina rada - poslovni (Enterprise) ili privatni (PSK). Prva opcija pruža sigurnost i robusnost, dok druga pruža nešto manju, ali i dalje tehnološki dostatnu sigurnost, a uz to i jednostavnost uporabe.

Konačno razmatranjem postojećih opasnosti od upada u bežičnu mrežu i štete koju joj je moguće nanijeti (od krađe podataka do stvaranja velike količine prometa), dolazi se do zaključka da svaki takav sustav treba zaštiti, a pri odbiru zaštite WPA2 se nameće kao dovoljno kvalitetno rješenje za zaštitu podataka koji se razmjenjuju putem bežičnih mreža.

5. Reference

1. Wireless_security, http://en.wikipedia.org/wiki/Wireless_security , lipanj 2009.
2. Wi-Fi_Protected_Access, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access , lipanj 2009.
3. William A. Arbaugh, The Convergence of Ubiquity: The Future of Wireless Security, http://www.usenix.org/events/usenix03/tech/arbaugh.pdf , lipanj 2009.
4. CCMP, http://en.wikipedia.org/wiki/CCMP , lipanj 2009.
5. WLAN, http://hr.wikipedia.org/wiki/WLAN , lipanj 2009.
6. Wi-Fi Alliance, http://www.wi-fi.org/ , lipanj 2009.
7. 802.1X-2004 - Port Based Network Access Control , http://www.ieee802.org/1/pages/802.1x-2004.html, lipanj 2009.
8. Wi-Fi Protected Access 2 (WPA 2) Configuration Example, http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008054339e.shtml, lipanj 2009.