Aleksandar Skendžić[1]

Stručni rad
UDK 004.7.056

SIGURNOST INFRASTRUKTURNOG NAČINA RADA BEŽIČNE MREŽE STANDARDA IEEE 802.11[2]

SAŽETAK

Bežične mreže sve se češće koriste i danas su postale standard u povezivanju računala nudeći pritom jednostavnu implementaciju uz smanjene troškove, zadovoljavajuće brzine mrežne propusnosti (eng. Bandwith) te veću mobilnost korisnika. Bežična komunikacija korisniku daje veću mobilnost, a samim time brži i lakši pristup izvoru informacija. Kada se govori o bežičnim lokalnim mrežama, kao posebno se važno nameće pitanje sigurnosti. Također, bežične mreže predstavljaju najnesigurniji dio u lokalnoj žičanoj mreži (LAN) zato što im je medij - nosioc zrak, čime mreža postaje dostupna i izvan organizacije u kojoj se koristi. Sigurnosni algoritmi (enkripcije) sprečavaju mogućnost neovlaštenog korištenja mreže, ali ne nude potpunu sigurnost. Ovaj rad dat će pregled sigurnosnih tehnologija infrastrukturnog načina rada bežične mreže (eng. wlan) i dati preporuke sigurnijeg načina rada. Rad nudi pregled metoda infrastrukturne sigurnosti wlan standarda IEEE 802.11.

Ključne riječi: *bežične mreže, IEEE 802.11, sigurnost, infrastrukturni način rada*

1. UVOD

Pojavom IEEE 802.11 mrežnog standarda, problem sigurnosti ostaje prioritetni zadatak administratora bežične mreže. Istraživanje iz 2008. provela je tvrtka RSA Security (http://www.emc.com) otkrivši kako veliki broj mreža koristi enkripcijski sustav integriran u bežične mrežne uređaje i bilježi porast u odnosu na ranija istraživanja. Istraživanjem je također utvrđeno kako razne organizacije, unatoč čestom i negativnom pisanju o sigurnosti bežičnih mreža, ipak koriste bežične mreže. Korištenje bežičnih mreža u Velikoj Britaniji se u 12 mjeseci povećalo za 235 %. Istraživanja sigurnosti bežičnih mreža u Hrvatskoj provele su nezavisne udruge korisnika bežičnih mreža, kao i Centar za prevenciju i otklanjanje problema vezanih uz sigurnost računalnih mreža u suradnji s laboratorijem za sustave i signale Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu. Rezultat istraživanja jest objava javnog dokumenta pod nazivom CCERT-PUBDOC-2003-05-22 čija je svrha poboljšanje sigurnosti bežičnih mrežnih sustava ustanova članica Hrvatske akademske i istraživačke mreže. Enkripcijski algoritmi ne nude potpunu sigurnost od neovlaštenog korištenja te ih se može zlorabiti. Upravo je stoga nužno iskoristiti dodatne mogućnosti infrastrukturnog načina rada u procesima autentikacije korisnika bežične mreže, kako bi se povećala razina sigurnosti.

[1] Mag. edu. inf. est. hist., viši predavač, Veleučilište Nikola Tesla u Gospiću, Bana Ivana Karlovića 16, Gospić, Hrvatska. *E-mail:* wireless82@gmail.com

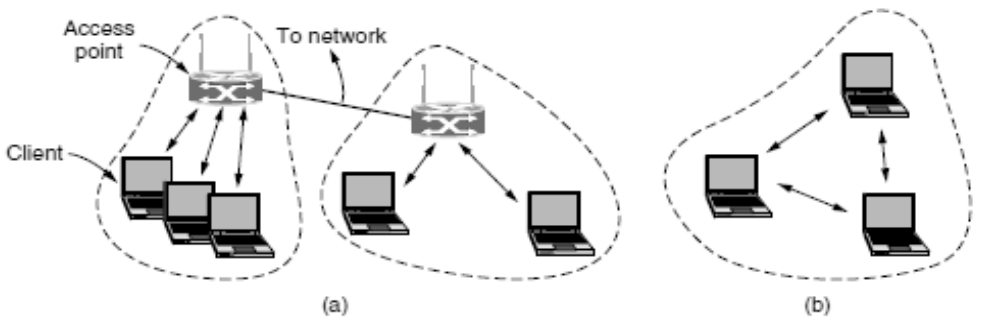
[2] Datum primitka rada: 19. 2. 2014.; datum prihvaćanja rada: 5. 5. 2014.

2. INFRASTRUKTURNI NAČIN RADA IEEE 802.11

Infrastrukturni način rada sastoji se od najmanje jedne pristupne točke ili usmjerivača povezanih sa žičanom mrežnom infrastrukturom ili nizom bežičnih krajnjih stanica. Ovakva konfiguracija mrežnih elemenata naziva se osnovna skupina (engl. *Basic Service Set - BSS*[3]). Dvije ili više BSS grupa čine podmrežu ili proširenu uslužnu grupu (engl. *Extended Service Set -* ESS[4], Hamidović, 2009). Krajnje stanice u infrastrukturnom načinu rada komuniciraju preko više pristupnih točaka. Infrastrukturni način rada bežičnih mreža podrazumijeva i specifična okruženja koja tvore pristupne točke ili usmjerivače. Postoji nekoliko načina rada bežičnih krajnjih stanica ovisnih o proizvođaču mrežne opreme:

- „*Master*" način rada jest standardni način rada gdje klijent komunicira s pristupnom točkom ili usmjerivačem.
- „*Bridge*" način rada djeluje kao „most" između dvije pristupne točke ili usmjerivača, ali ne dozvoljava spajanje klijenata na uređaje.
- Repetitorski način rada dozvoljava premošćivanje poput „*bridge*" načina rada, ali uz mogućnost istovremenog spajanja klijenata na svaku pojedinu pristupnu točku ili usmjerivač.
- *Wireless Distribution System -* WDS način rada, a označava tehniku povezivanja više pristupnih točaka (AP-ova). WDS je prisutan u obliku raznih *Point-to-Point*/*Multipoint Bridge* implementacija, kao i u obliku nadogradnji standardnih pristupnih točaka.

Slika 1. 802.11 arhitektura a) Infrastrukturni WLAN, b) neovisni WLAN



Izvor: Tanenbaum, A. S., Wetherall, D. J. (2011)

[3] *Basic Service Set (BSS)* je skup svih pristupnih stanica koje međusobno komuniciraju. Svaka stanica posjeduje jedinstveni ID zvan BSSD koja označava MAC adresu pristupne točke u infrastrukturnoj komunikaciji.

[4] *Extended Service Set (ESS)* je proširen skup pristupnih stanica koje međusobno komuniciraju.

Sigurnosna razina infrastrukturnog načina rada je visoka zbog korištenja odgovarajućih enkripcijskih algoritama i protokola. Sigurnosni mehanizmi zaštite bežične mreže u infrastrukturnom načinu rada su:

1. MAC filtriranje
2. IP filtriranje
3. Uporaba enkripcijskog ključa
4. RADIUS
5. LDAP imenički servis i protokol
6. Uporaba sigurnosne zaštitne stijene
7. TKIP
8. AES
9. CCMP
10. IEEE 802.1X

2.1 MAC filtriranje

MAC adresa (engl. *Media Access Control*) je adresa kodirana u ROM (*Read Only Memory*) svakog mrežnog uređaja. Sastoji se od 48 bita i jedinstvena je za svaki uređaj. Koristi se za adresiranje na razini podatkovne veze ISO/OSI referentnog modela. MAC filtriranje je najjednostavniji oblik zaštitnog mehanizama bežične mreže. Temeljem liste dopuštenih/zabranjenih MAC adresa, tj. hardverskih adresa pristupne točke, usmjerivači i klijenti međusobno komuniciraju. Ukoliko MAC adresa nije zapisana u uređaju na kojemu se vrši postupak autentikacije, klijent nema odobrenje za korištenje mrežnih resursa niti se može spojiti na pristupnu točku ili usmjerivač. Nedostatak navedenog sigurnosnog mehanizma jest mogućnosti lakog zaobilaženja jer većina mrežnih adaptera ima mogućnost (privremenog) mijenjanja MAC adrese putem specijaliziranog softvera.

2.2 IP filtriranje

IP filtriranje, kao sigurnosni mehanizam, temelji se na deklariranju pravila IP filtriranja i dodjeljivanja ili uskraćivanja pristupa na određenu IP adresu ili skup adresa. IP filtriranje je dodatni sigurnosni mehanizam zaštite bežičnih mreža. Napadaču je teško odrediti koji se deklarirani raspon IP adresa koristi u pristupnoj točki/usmjerivaču kako bi se na njega prijavio. S obzirom na navedeno, sigurnosna preporuka jest koristiti IP filtriranje.

2.3 Uporaba enkripcijskog ključa

U okviru bežičnog mrežnog standarda 802.11 koriste se tri tipa algoritama za sigurnu komunikaciju. Algoritmi su definirani sljedećim standardima:

a) *Wired Equivalent Privacy* - WEP

b) *Wi-Fi Protected Access* - WPA

c) *Wi-Fi Protected Access II* – WPA2

Svi navedeni algoritmi nastoje ispuniti unutar 802.11 standarda sljedeće pretpostavke:

- Povjerljivost: temeljna svrha algoritama za sigurnu komunikaciju je spriječiti prisluškivanje mrežnog prometa;
- Kontrola pristupa: također ima ulogu kontrole pristupa jer pristupne točke imaju mogućnost zabrane prometa klijentima koji ne prođu uspješno proces autentikacije.

Algoritami se međusobno razlikuju po metodama enkripcije komunikacije i autentikacije korisnika. Slijedi pregled enkripcijskih algoritama koji se koriste kao sigurnosni mehanizmi bežičnih mreža:

1. WEP - 802.11 standard navodi WEP kao algoritam koji omogućava siguran prijenos podataka preko bežičnih lokalnih mreža čija sigurnost je ekvivalentna fizičkim sigurnosnim elementima u ožičenim medijima. Unutar WEP-u su se tijekom vremena otkrili nedostaci u njegovoj izradi. WEP se koristi na podatkovnom sloju OSI modela kako bi zaštitio podatke tijekom prijenosa. WEP algoritam se oslanja na tajnosti ključa koji se koristi između pristupne točke i klijenta i pomoću njega enkriptira tijela okvira poruke (Tanenbaum, Wetherall, 2011). Enkripcija se vrši u sljedećim koracima:

   a. Zaštitno kodiranje *(checksumming)*

   Kako bi zaštitili integritet poruke, nad njom se vrši operacija zaštitnog kodiranja s CRC32 polinomom, a zaštita se zapisuje na kraj podatka koji se želi zaštititi. Dakle, čisti tekst (P) dobivamo sljedećim izrazom:

   $$P=\{M,c(M)\}$$

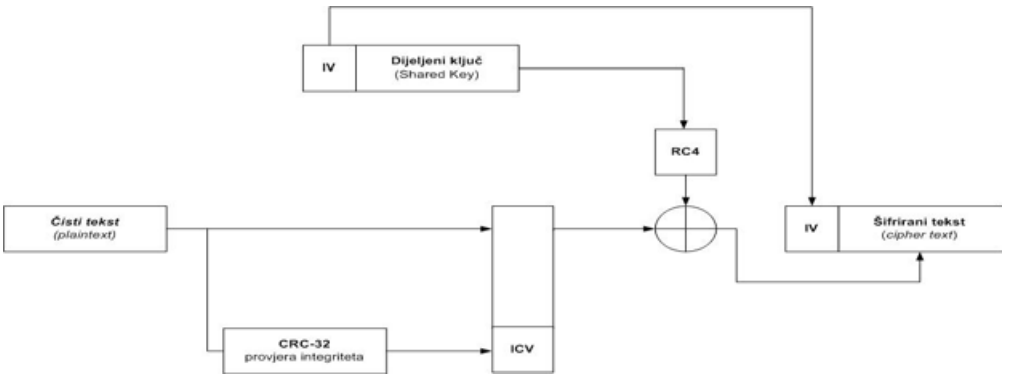
   M predstavlja originalni podatak. c(M) i P ne ovisi o dijeljenom ključu k. Čisti tekst P je ulaz za drugi korak.

   b. Enkripcija

   U drugom koraku enkriptira se čisti tekst iz prethodnog koraka pomoću algoritma RC4. Slučajnim odabirom bira se inicijalizacijski vektor IV koji uz ključ k služi kao ulaz u RC4 algoritam. Algoritam generira veliki broj pseudo-slučajnih bitova kao funkciju ključa k i inicijalizacijskog vektora IV. Ovaj niz bitova označava se s RC(IV,k). Nakon toga se vrši operacija ekskluzivno ili nad bitovima čistog teksta i dobivenim nizom pseudo-slučajnih bitova da bi se dobio šifrirani tekst (*ciphertext*).

   Aktivno probijanje zaštitnog mehanizma WEP algoritma može se prikazati dostupnim programskim alatima poput *Aircracka* francuskog autora Chistophe Devina (http://os2.zemris.fer.hr).

Slika 2. Proces WEP enkripcije



Izvor**:** FER, http://os2.zemris.fer.hr/ns/wireless/2004_maric/wep.htm (7. 7. 2013.)

2. WPA – WPA predstavlja certifikaciju, a ne protokol, odnosno sigurnosni standard. WPA uključuje samo jedan sigurnosni protokol TKIP. WPA je nastao prvenstveno zbog sigurnosnih nedostataka WEP enkripcije, odnosno nedostataka korištenjem inicijalizacijskog vektora. U kolovozu 2001. godine objavljena je kriptoanaliza WEP protokola i načina na koji se koriste RC4 tok za šifriranje i inicijalizacijski vektor (ACM digital library, http://dl.acm.org/citation.cfm?id=694759). Navedena analiza je pokazala da je WPA enkripcijski protokol ranjiv na pasivne napade. Pasivni napadi imaju cilj otkrivanja RC4 ključa iz prikupljenih paketa podataka (ACM digital library, http://dl.acm.org/citation.cfm?id=694759). Ovisno o količini prometa na mreži, odnosno broja uhvaćenih paketa dostupnih za analizu, za uspješno otkrivanje RC4 ključa može biti potrebno i samo nekoliko minuta. WPA i dalje koriste RC4 i CRC32 algoritmi. Uvedeni su TKIP (*Temporal key integrity protocol*), MIC (*Message integrity code*, izračunava se algoritmom Michael[5]) te 802.1x autentikacija. Kombinacijom dugačkog inicijalizacijskog vektora (IV) i TKIP protokola, sustav se može obraniti od napada kakvi se koriste za otkrivanje ključa kod primjene WEP protokola (Tanenbaum, Wetherall, 2011). 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.

2.3.1 Ranjivost WPA certifikacije

2008. godine otkriven je sigurnosni propust TKIP komponente. TKIP komponenta je korištena kako bi se osigurala kompatibilnost sa starijim mrežnim adapterima, odnosno mrežnom opremom koja je podržavala isključivo stariji WEP enkripcijski algoritam. Da

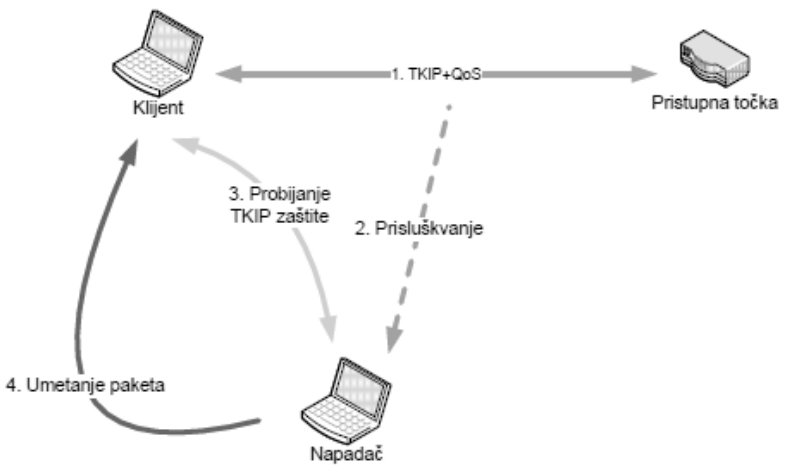
[5] Algoritam koji u WPA uključuje brojač okvira čime se isključuje mogućnost promjene sastava poruka u komunikacijskom kanalu. Michael algoritam dovoljno je siguran i moguće ga je koristiti na starijim mrežnim adapterima.

bi napadač mogao izvesti aktivni napad na bežičnu mrežu zaštićenu WPA TKIP načinom rada, mrežna oprema mora ispunjavati sljedeće uvijete:

- Pristupna točka mora podržavati tzv. višestruke struje (eng. *multiple streams*) podataka o kvaliteti usluge (*Quality of Service* - QoS) uključene u IEEE 802.11e standardu i podržane u većini današnjih uređaja;
- Napadač mora poznati raspon IP adresa mreže na koju izvodi napad ;
- Interval obnove privremenog ključa (eng. *Temporary Key*) mora biti veći od 2000 sekundi.

Na slici 3 dan je prikaz napada na bežičnu mrežu zaštićenom WPA TKIP certifikacijom s uključenim QOS uslugom na pristupnoj točki.

Slika 3. Prikaz napada na bežičnu mrežu zaštićenom WPA TKIP certifikacijom [7].



Izvor: CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-12-001_0.pdf (26. 8. 2013)

WPA2 - WPA2 (802.11i standard (http://os2.zemris.fer.hr/) također predstavlja certifikaciju, a ne sigurnosni standard kako se često navodi. Osnovna razlika između 802.11i i WPA je upotreba AES-CCMP algoritma enkripcije (http://os2.zemris.fer.hr/). Izveden je iz WPA certifikata s mogućnošću korištenja dva sigurnosna standarda TKIP te, noviji, CCMP[6] (Cole, 2007). Iako predstavlja sigurniju alternativu u odnosu na WEP standard, WPA2 certifikacija također je ranjiva u određenim načinima rada.

2.3.2 Ranjivost WPA2 certifikacije

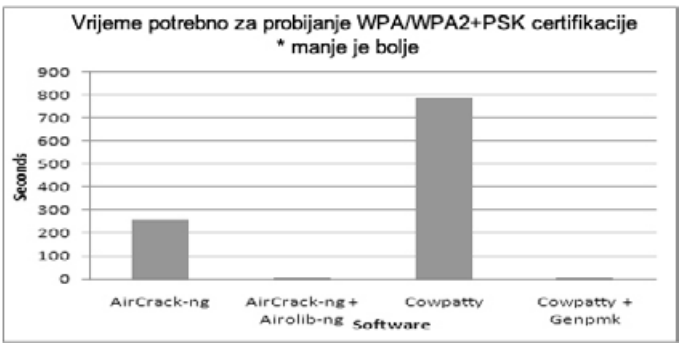
Ranjivost WPA2 certifikacije ogleda se u korištenju WPA2+PSK[7] načinu rada. PSK pruža mogućnosti jednostavnijeg postavljanja sustava bez autentifikacijskog poslužitelja. PSK je niz znakova od 256 bita ili riječ od 8 do 63 slova preko kojega se izračunava ključ (http://www.cert.

[6] *Counter Cipher Message Protocol* - CCMP je poboljšani kriptografski mehanizam zaštite bežičnih mreža po standardu IEEE 802.11.

[7] *Pre Shared Key* – ključ s dijeljenom tajnom jedan je od načina rada WPA2 certifikata u sigurnosti bežičnih mreža. Nije se pokazao pouzdanim jer ga je moguće zaobići putem dostupnih programskih alata poput Aircracka.

hr). Ovaj način osiguravanja sigurnosti bežične mreže je korisnicima „najpraktičniji" jer se u praksi uglavnom koriste razne fraze ili izrazi. Napad na ključ podrazumijeva isprobavanje svih potencijalnih kombinacija od strane napadača. Eventualni problem takvih vrsta napada jest problem vremenskog trajanja i vrlo je često neizvediv u zadovoljavajućim vremenskim okvirima (http://www.cert.hr). Usporedni prikaz alata i vremensko trajanja probijanja WPA/WPA2 PSK certifikacije prikazan je u grafikonu 1. Nezavisni rezultati mjerenja od strane korisnika ukazuju da najduže trajanje probijanja WPA/WPA2+PSK certifikacije alatom Cowpatty traje približno 14 min, dok AirCrack isto čini za približno 4 min (http://blog.g0tmi1k.com).

Grafikon 1. Usporedni prikaz alata i vremena potrebnog za probijanje WPA/WPA2+PSK certifikacije



Izvor: http://blog.g0tmi1k.com

2.3.3 Usporedba WEP/WPA/WPA2 protokola

Osim razlike u primjeni CCMP kao sigurnijeg algoritma enkripcije u WPA2 protokolu, WPA i WPA2 protokoli su vrlo slični. WPA2 podržava TKIP protokol, tj. kompatibilan je s WPA protokolom. Nesigurnosti WPA zaštite proizašle su iz ograničenja nametnutih prilikom oblikovanja WPA protokola. Ograničenje WPA protokola je prisutno zbog zadržavanja kompatibilnosti s ranjivim WEP protokolom na starijim mrežnim adapterima. 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 (http://www.cert.hr). Usporedba WEP certifikacije te WPA/WPA2 protokla prikazana je u tablici 1.

Tablica 1. Usporedbe WEP i WPA/WPA2 protokola

Protocol	Encryption	Authentication	Key Management
WEP	• RC4 with 40 bit key/28 bit hash • Static keys	• Pre Shared keys • Open System (SSID)	• Manual key rotation, i.e., no key management
WPA	• TKIP with 128 bit key (over RC4) • Constant key rotation	• 802.1x with EAP and RADIUS • Pre-shared key	• Per packet key rotation
802.11i	• TKIP with 128 bit key (over RC4) • AES-CCMP • Constant key rotation	• 802.1x with EAP and RADIUS • Pre-shared key	• Per packet key rotation (TKIP) • Per session key rotation (AES-CCMP)

Izvor: http://www.fidis.net

2.4 RADIUS i funkcija „AAA"

RADIUS (eng. *Remote Authentication Dial In User Service*) je definiran kao mrežni protokol koji, prilikom spajanja računala na mrežu i korištenja mrežnih usluga, omogućava centralizirano upravljanje autentikacijom, autorizacijom i administracijom korisnika (eng. AAA – *Authentication, Authorization, Accounting*, http://www.cert.hr).

RADIUS je protokol koji radi na principu komunikacije klijent-poslužitelj. Komponenta RADIUS klijenta komunicira s RADIUS poslužiteljem te se izvršava kao pozadinski proces na računalu s UNIX/Linux ili Windows operacijskim sustavom.

RADIUS poslužitelj podrazumijeva tri funkcije (http://www.cert.hr):

1. autentikacija korisnika ili uređaja prije odobravanja pristupa mreži
2. autorizacija korisnika ili uređaja
3. praćenje aktivnosti korisnika usluga

1. Autentikacija je proces putem kojega korisnik mreže potvrđuje vlastiti digitalni identitet. Potvrda digitalnog identiteta obično se ostvaruje putem neke vrste identifikatora odnosno pripadnih podataka poput zaporke, tokena i digitalnih certifikata.

2. Autorizacija je proces putem kojega se utvrđuje je li određeni subjekt/korisnik ovlašten izvoditi određenu aktivnost. Autorizacija se može provoditi nizom ograničenja poput vremenskog, ograničenja fizičke lokacije ili ograničenja protiv višestrukih prijava istog entiteta ili korisnika. Primjeri tipova usluga su filtriranje IP adrese, dodjeljivanje adrese, dodjeljivanje puta usmjeravanja, kvaliteta usluge (*QoS*), diferencijalne usluge, kontrola pojasne širine, upravljanje prometom, obavezno tuneliranje do određene krajnje točke i enkripcija (http://www.cert.hr).

3. Administracija korisnika je proces praćenja korištenja mrežnih usluga, odnosno resursa. Administracija u realnom vremenu odnosi se na podatke koji se dostavljaju za vrijeme korištenja resursa. Skupna administracija (eng. *batch accounting*) odnosi se na podatke koji se čuvaju i kasnije dostavljaju pružatelju mrežne usluge za razna statistička izvješća te kontrolu resursa.

RADIUS protokol je doživio nekoliko izmjena i nadopuna od vremena kada je definiran kao standard 1997. godine. Prikaz kronologija razvoja RADIUS protokola dan je u tablici 2.

RADIUS protokol povećava sigurnost prilikom prijave i korištenja bežične mreže kakve nalazimo u IT infrastrukturi obrazovnih institucija u Hrvatskoj. Premda isti način podešavanja i izvedbe bežične mreže već uvelike koriste sistem-inženjeri obrazovnih institucija, treba ukazati na prednosti u sigurnosti bežične mreže. Prednost RADIUS protokola ogleda se u samom procesu prijave u mrežu. Važno je napomenuti kako RADIUS protokol, osim 802.11, podržava i žičani 802.3 ethernet standard.

Prilikom prijave u mrežu, korisnik šalje svoje podatke RADIUS klijentu koji potom izmjenjuje RADIUS poruke s RADIUS poslužiteljem. Svrha navedenih poruka upravo je ostvarivanje autentikacije, autorizacije i administracije korisnika, odnosno funkcije „AAA". Proces razmjene RADIUS poruke prikazan je na slici 5.

Tablica 2. Kronologija razvoja RADIUS protokola

Broj dokumenta	Naslov dokumenta	Datum izdavanja	Zamijenjen dokumentom
RFC 2058	*Remote Authentication Dial In User Service (RADIUS)*	siječanj 1997.	RFC 2138
RFC 2059	*RADIUS Accounting*	siječanj 1997.	RFC 2139
RFC 2138	*Remote Authentication Dial In User Service (RADIUS)*	travanj 1997.	RFC 2865
RFC 2139	*RADIUS Accounting*	travanj 1997.	RFC 2866
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*	ožujak 1999.	
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	lipanj 2000.	Nadopunjavaju ga RFC 2868, 3575 i 5080
RFC 2866	*RADIUS Accounting*	lipanj 2000.	Nadopunjava ga RFC 2867
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*	lipanj 2000.	Nadopunjava RFC 2866

Izvor**:** CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-07-306.pdf (10. 2. 2013.)

Slika 5. Proces razmjene RADIUS poruke

Izvor: CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-07-306.pdf (10. 2. 2013.)

2.5 LDAP imenički servis i protokol

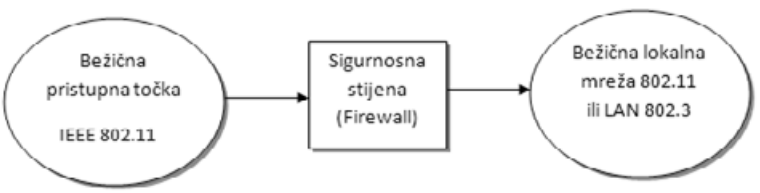
Lightweight Directory Access Protocol - LDAP je naziv za aplikacijski protokol, odnosno imenički servis koji omogućava pristup imeničkim servisima putem računalne mreže. Imenik LDAP-a predstavlja datoteka ili skupina organiziranih podataka koji sadrže podatke o korisnicima, datotekama i aplikacijama te sigurnosne postavke istih. U kontekstu sigurnosti bežičnih mreža LDAP u sprezi s RADIUS protokolom (RADIUS+LDAP) predstavlja jednu od najsigurnijih metoda, kako žičane, tako i zaštite bežične mreže.

2.6 Uporaba sigurnosne zaštitne stijene

Sigurnosna zaštitna stijena (eng. *Firewall*) je računalo ili neka nakupina komunikacijskih uređaja koje fizički odvajaju dvije mreže (Budin, 1998:364). Isto tako, sigurnosna zaštitna stijena ograničava pristup nekoj privatnoj lokalnoj mreži iz javne mreže. U kontekstu bežične mreže po standardu IEEE 802.11, sigurnosna zaštitna stijena može se koristiti kao dodatni sigurnosni mehanizam. Sigurnosna zaštitna stijena postavlja se između žičane mreže i mrežnih uređaja koji omogućavaju bežično spajanje na lokalnu mrežu (najčešće pristupne točke ili usmjerivači). Zaštitne stijene, podešene tako da zahtijevaju strogu autentikaciju i autorizaciju pristupa, vrlo su djelotvoran mehanizam u sigurnosti mreže. Sigurnosne stijene možemo podijeliti u tri skupine, s obzirom na djelovanje (Budin, 1998:365):

- stijene koje filtriraju komunikacijske pakete (engl. *packet filter*),
- stijene koje djeluju kao prividni poslužitelji (engl. *proxy server*),
- stijene koje djeluju kao stvarni poslužitelji (engl. *full server*).

Slika 6. Prikaz moguće pozicije sigurnosne stijene lokalne mreže



Izvor: autor

Stijene koje filtriraju komunikacijske pakete djeluju na nižim razinama komunikacijskih protokola. Na temelju adrese primatelja, pošiljatelja te smjera kretanja mrežnog paketa, stijena može neke pakete propustiti, a neke blokirati. Blokiranje se može realizirati i na aplikacijskoj razini.

Sigurnosne stijene koje djeluju kao prividni poslužitelji prihvaćaju zahtjeve za obavljanje određenih usluga, iste zahtjeve analiziraju i prosljeđuju stvarnom zaštićenom poslužitelju, ukoliko su prošli sigurnosnu provjeru.

Sigurnosne stijene koje djeluju kao stvarni poslužitelji obavljaju kontrolirane usluge prema vanjskim klijentima i ne dopuštaju neposredni kontakt vanjskih klijenata i unutarnjih korisnika.

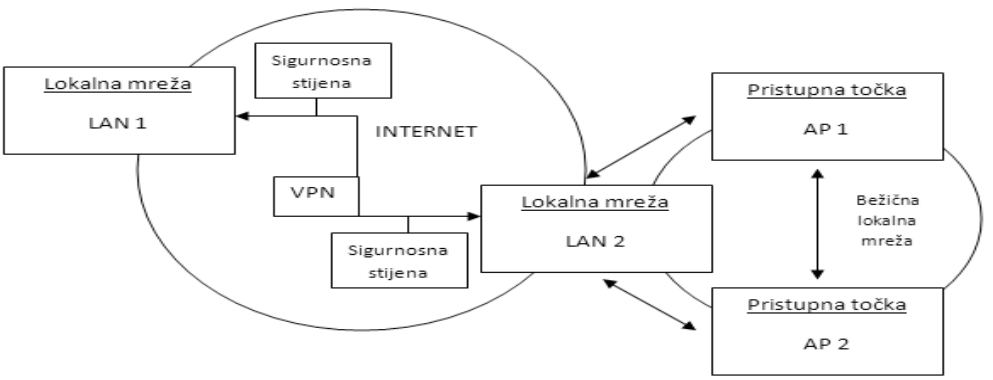
Važno je napomenuti kako su sigurnosne stijene samo jedan dodatni mehanizam u sigurnosti bežičnih mreža, kako žičanih, tako i bežičnih, te ostvaruju zaštitu samo na granici mreže, dok na unutarnju sigurnost nemaju nikakav utjecaj.

2.7 Virtualne privatne mreže

Uporabom virtualnih privatnih mreža temeljnih na bežičnoj mrežnoj infrastrukturi (engl. *Virtual Private Network* – VPN) znatno se podiže sigurnosna razina rada u mrežnom okruženju. Iako VIN tehnologija nema izravan utjecaj na procese autentikacije

korisnika prilikom spajanja na bežičnu pristupnu točku, ona doprinosi unutarnjoj sigurnosti bežične mreže. Iz navedenog razloga tehnologija virtualnih privatnih mreža neće se podrobnije razmatrati s obzirom da se radi o unutarnjoj sigurnosnoj razini, a ne o zaštitnom mehanizmu od neovlaštenog pristupa korištenjem bežične mrežne tehnologije. VPN je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko distribuirane ili javne mrežne infrastrukture. VPN podrazumijeva korištenje određenih sigurnosnih i upravljačkih pravila unutar lokalnih mreža. VPN veze mogu se uspostaviti preko različitih komunikacijskih kanala poput interneta, komunikacijske infrastrukture davatelja internetskih usluga i drugih. Važno je napomenuti kako virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točaka.

Slika 7. Mogućnost integracije bežične lokalne mreže i VPN-a.



Izvor: autor

Prema konceptu VPN-a, osnovna zadaća tehnologije je kreiranje sigurnog komunikacijskog kanala između privatnih mreža putem javne mreže. Uobičajena je kombinacija sklopovskog i programskog pristupa u kreiranju medija za siguran prijenos podataka. Prilikom komunikacije, podaci iz lokalne mreže prolaze kroz *gateway* uređaj koji ima ulogu zaštite komunikacijkog medija. Isti postupak se primjenjuje kada podaci dolaze u lokalnu mrežu, također prolaze kroz gateway[8] uređaj. VPN štiti tako odaslane podatke automatskim šifriranjem prilikom slanja podataka između dviju udaljenih privatnih mreža i enkapsuliranjem u IP pakete, te automatskim dešifriranjem paketa na drugom kraju komunikacijskog kanala (http://www.cis.hr). Kada se govori o korištenju, implementaciji i sigurnosti VPN-a u mrežnom povezivanju, bežične mreže se u osnovi ne razlikuju od žičanih lokalnih mreža. Razlika je isključivo u pristupnom dijelu mreže (pristupni medij), dok se sa sigurnosnog aspekta u potpunosti podudaraju, odnosno ovise o upravljačkoj mrežnoj infrastrukturi. Korištenje VPN-a u bežičnoj mrežnoj infrastrukturi, bežičnoj lokalnoj mreži daje proširene pristupne mogućnosti (bežični pristup) uz optimalnu sigurnosnu razinu.

[8] Gateway je uređaj koji se nalazi u čvoru računalne mreže i služi za komuniciranje s nekom drugom mrežom. Gateway je i prevodilac mrežnih protokola te omogućava priključivanje na mrežu s drugom vrstom protokola.

3. ZAKLJUČAK

Bežične mreže izložene su sigurnosnim ugrozima jer se podaci neusmjereno i nekontrolirano odašilju u svim smjerovima u dometu odašiljača pa ih zbog takve karakteristike prijenosnog medija može bilo tko presresti. Budući da je danas WPA2 protokol najnaprednije sigurnosno rješenje za zaštitu WLAN-a i računala u njemu, ipak ne predstavlja maksimalnu zaštitu bežične mreže. Posebice je to WPA2+PSK konfiguracija zaštite koja se može probiti dostupnim alatima, poput *Aircracka* ili CommViewa. Zaključuje se kako sigurnost infrastrukturnog bežičnog LAN-a nije preporučljivo temeljiti isključivo na zaštitnim enkripcijskim protokolima (WEP/WPA/WPA2), već treba koristiti i druge mogućnosti infrastrukturnog bežičnog LAN-a (vatrozid, LDAP, RADIUS, MAC filtriranje i sl.), ovisno o dostupnoj mrežnoj infrastrukturi. Pri tome treba voditi računa o jednostavnosti autentikacije korisnika na sustav. U kontekstu sigurnosti bežičnih mreža, LDAP u sprezi s RADIUS protokolom predstavlja jednu od najsigurnijih metoda, kako žičane tako i zaštite bežične mreže koja se može preporučiti ukoliko postoje tehničke mogućnosti. Infrastrukturni bežični LAN zahtjeva korištenje dodatnog mrežnog hardvera (poslužitelji, usmjerivači, pristupne točke) što sa sigurnosnog aspekta predstavlja i proporcionalno veći financijski trošak. Navedene smjernice mogu biti temelj sigurnosne politike ustanove (organizacije) koja će predstavljati svojevrstan nacrt sigurnosti unutar određenog sustava s točno opisanim ciljevima i procedurama sigurnosti.

LITERATURA

Tanenbaum, A. S., Wetherall, D. J. (2011) *Computer networks, 5 edition* SAD, Prentice Hall

ACM digital library, http://dl.acm.org/citation.cfm?id=694759 (08. 02. 2013.)

CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-07-306.pdf, (10. 2. 2013.)

http://blog.g0tmi1k.com/2010/02/video-cracking-wifi-wpawpa2-aircrack-ng.html (11. 2. 2013.)

CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-12-001_0.pdf (26. 8. 2013)

Cole, T. (2007) IEEE *Std 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, New York, 2007.

Čerić, M., Birolla, H, Varga, M. (1998) *Poslovno računarstvo*, Zagreb: Znak, str 467.

CIS, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf (11. 3. 2013.)

FER, http://os2.zemris.fer.hr/ns/wireless/2004_maric/wep.htm (7. 7. 2013)

Hamidović, H. (2009) *WLAN - Bežične lokalne računalne mreže*. Zagreb: Info press

EMC, http://www.emc.com/about/news/press/2008/20081027-03.htm (10. 2. 2013)

FER, http://os2.zemris.fer.hr/ns/wireless/2007_mercep/Seminar[2007]Mercep_Ljubo.htm (7. 7. 2013)

http://blog.g0tmi1k.com/2010/02/video-cracking-wifi-wpawpa2-aircrack-ng.html (7. 7. 2013)

http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf (7. 7. 2013)

http://www.fidis.net/resources/deliverables/hightechid/int-d37003/doc/12/ (7. 7. 2013)

Aleksandar Skendžić [1]

Professional paper
UDC 004.7.056

SECURITY OF INFRASTRUCTURE MODE OF IEEE 802.11 WIRELESS NETWORK STANDARD[2]

ABSTRACT

Wireless networks are increasingly used today and have become the de facto standard for connecting computers while at the same time offering simple implementation with reduced costs, satisfactory bandwidth speeds and greater mobility of users. Wireless communication provides users with greater mobility, and therefore faster and easier access to sources of information. When talking about wireless local area networks, a particularly important issue is that of security. Wireless networks are the least secure part of the wired local area network (LAN) because they use air as the medium for transmission, and in so doing the network becomes available outside the organization in which it is used. Security algorithms (encryption) prevent the possibility of unauthorized use of the network, but they do not offer one hundred percent security. This paper will present an overview of security technologies regarding infrastructure mode of wireless network and make recommendations for secure mode. The paper provides an overview of the methods of infrastructure security with regard to the IEEE 802.11 WLAN standard.

Keywords: *wireless networks, IEEE 802.11, security, infrastructure mode*

[1] Mag. edu. inf. est. hist., Senior Lecturer, Polytechnic Nikola Tesla in Gospić, Bana Ivana Karlovića 16, Gospić, Croatia. E-mail: wireless82@gmail.com

[2] Received: 19. 2. 2014.; accepted: 5. 5. 2014.