Prijedlog izrade modela vrednovanja sigurnosti bežičnih računalnih mreža u obrazovnim institucijama

Aleksandar Skendžić

Veleučilište Nikola Tesla u Gospiću

53000 Gospić, Hrvatska

Telefon: ++385(91)8823-413; E-mail: askendzic@velegs-nikolatesla.hr

Sažetak:

Kako se uvođenje informacijsko-komunikacijske tehnologije u obrazovne ustanove dotiče svih elemenata obrazovanja, uvođenje novih tehnologija pretpostavlja svojevrsnu reformu cjelokupnog obrazovnog sustava. Važan segment u procesu uvođenja informacijsko-komunikacijske tehnologije u obrazovne institucije čine bežične mreže. Pri tome je važno definirati strateške ciljeve implementacije bežičnih mreža u obrazovnim institucijama: komunikacija i mobilnost, izgradnja mrežnih, digitalnih nastavnih sadržaja, podrška e-obrazovanju, mobilnom učenju (m-učenju) i virtualnim školama. Naglasak metoda vrednovanja očituje se u primjeni ekspertnog sustava u bržem rješavanju problema, osmišljavanja implementacije bežične mreže te standardnih mrežnih servisa kako bi se u svakom trenutku osigurala bolja mobilnost i dostupnost te osigurala maksimalna razina sigurnosti. Glavni uzrok današnjeg intenzivnog korištenja bežične mrežne infrastrukture ogleda se u uznapredovanom razvoju informacijsko-komunikacijske tehnologije koje svoj pristup mreži temelje na bežičnoj komunikaciji, a ista može biti primjenjiva i u obrazovnom procesu.

1. UVOD I DOSADAŠNJA ISTRAŽIVANJA

Razvoj informacijsko-komunikacijske tehnologije uvelike doprinosi poboljšanju kvalitete provođenja nastavnog procesa među učenicima i studentima. Razvojem računalnih mreža i interneta otvorile su se nove mogućnosti komunikacije na razini nastavnik-student te nastavnik-učenik. Svjetski trendovi i dosadašnja istraživanja ukazuju na povećanu zastupljenost korištenja bežičnog pristupa lokalnim mrežama i internetu kao standard već u osnovnom školstvu. U Hrvatskoj se kasni za svjetskim trendovima u osnovnom i srednjem školstvu, dok je u institucijama visokog obrazovanja na razini europskog prosjeka. Kao razlog maloj zastupljenosti bežičnih mreža u osnovnom i srednjem školstvu navode se financijski problemi, nezainteresiranost vodstva institucija te problemi održavanja mrežne infrastrukture. Za kvalitetno rješenje potrebna je strategija razvoja koja će analizirati mogućnosti i potrebe te u skladu s njima implementirati tehnologiju uvođenjem bežičnih mreža. U skladu s navedenim, nužno je omogućiti učenicima i studentima podržani pristup bežičnoj mreži s

osobnih računala. Situacija u Hrvatskoj bilježi i uspjehe u procesu uvođenja bežične mrežne tehnologije u obrazovne institucije projektom educational roaming (Eduroam [9]). Projekt je pokrenut zbog sve učestalije pojave mobilnosti korisnika (i svjetskih trendova) koji traže primjereniji pristup internetu i ostalim mrežnim servisima i izvan granica matičnih ustanova, akademskih mreža, zemalja. Eduroam je zamišljen kao paneuropski romaing sustav koji na jednostavna način omogućuje bežično, „sigurno“ spajanje na mrežu rabeći AAI@EduHr elektronički identitet. Bolonjski proces u Europi pogoduje takvom trendu osobito među studentskom populacijom. Uvođenje bežičnog pristupa lokalnim mrežama u obrazovnim institucijama za posljedicu ima problem sigurnosti. Dosadašnja istraživanja iz 2011. godine, prema neprofitnoj udruzi proizvođača Wi-Fi Alliance i tvrtke koja je provela istraživanje Wakefield Research, upozoravaju kako je pitanje sigurnosti od značajne važnosti među korisnicima bežičnih mreža te se bilježi trend porasta upada u nesigurne bežične mreže. Drugo istraživanje iz 2011. provela je kompanija RSA Security otkrivši kako veliki broj mreža koristi enkripcijski sustav integriran u bežične mrežne uređaje te bilježi porast u odnosu na ranija istraživanja. Istraživanjem je također utvrđeno kako institucije unatoč čestom i negativnom pisanju o sigurnosti bežičnih mreža iste uvelike koriste. Korištenje se bežičnih mreža u Velikoj Britaniji u 12 mjeseci povećalo za 235 posto.

U Hrvatskoj istraživanja o korištenju i sigurnosti provedena su od strane nezavisnih udruga korisnika bežičnih mreža, ali i od strane Centra 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 [8] sa svrhom poboljšanja sigurnosti bežičnih mrežnih sustava ustanova članica Hrvatske akademske i istraživačke mreže. Pojavom IEEE 802.11 mrežnog standarda problem sigurnosti ostaje prioritetni zadatak administratora bežične mreže. Enkripcijski algoritmi ne nude sto postotnu sigurnost od neovlaštenog korištenja te ga se može zlorabiti. Model vrednovanja sustavno će se prikazati na primjeru obrazovnih institucija iz razloga što je to jedan od problema u praksi. Administratori mreže u obrazovnim institucijama često nemaju iskustva u optimalnom osmišljavanju bežične mreže kao i razine sigurnosti. Jer, na navedenim radnim mjestima administratora, uglavnom, rade osobe s nedovoljnim iskustvom, neodgovarajuće profesije ili ih nedostaje u dovoljnom broju. U takvim slučajevima institucije angažiraju vanjske suradnike ili tvrtke što za posljedicu ima znatne troškove kako u osmišljavanju i implementaciji, tako i u održavanju sustava.

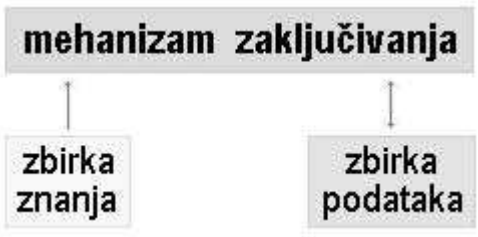
2. EKSPERTNI SUSTAVI

Prema Christopheru Evansu (1979) [1] inteligencija je sposobnost sistema da se prilagodi promjenama u svijetu i što je ta sposobnost veća, odnosno profinjenija snaga prilagođavanja, sistem je inteligentniji. U domeni umjetne inteligencije ekspertni sustavi mogu se koristiti za optimalno rješavanje problema koristeći se pritom bazom znanja.

Ekspertni sustavi [3] su računalni programi temeljeni na znanju iz nekog specijalističkog područja. U tom području oni postižu kvalitetu i efikasnost zaključivanja eksperata te pomažu u rješavanju problema. U rješavanju problema ekspertni sustavi ponajviše se oslanjaju na znanje, što odgovara spoznaji da su eksperti efikasni u rješavanju problema prvenstveno zbog svog akumuliranog znanja. Znanje eksperta može se svrstati u ti osnovne kategorije:

- Činjenice - neosporne tvrdnje i sigurni podaci
- Hipoteze - vjerojatne tvrdnje i ne sasvim sigurni podaci
- Heurističko znanje - sposobnost dobre procjene kada nema činjenica ni podataka

Ekspertni sustav moguće je primijeniti i u slučaju prijedloga konfiguriranja i sigurnosti bežičnih lokalnih mreža. Predložena aplikacija je zamišljena da putem web sučelja korisnik odabire čimbenike svojih karakteristika i potreba poput odabira mrežnih usluga/servisa (www, FTP, VOIP, VPN), broja korisnika, prostorne pokrivenosti bežičnom mrežom, raspoloživost mreže, način rada, autentifikacija, propusnost mreže (engl. bandwith), uporaba vatrozida, te na temelju tih podataka sustav zaključivanja nudi optimalnu mrežnu konfiguraciju s preporučenim sigurnosnim mehanizmima.



Slika 1 Načelna shema ekspertnog sustava.

3. METODE VREDNOVANJA SIGURNOSTI BEŽIČNIH MREŽA

Predložene metode vrednovanja sigurnosti bežičnih mreža su:

1. Jednostavnost i cijena izvedbe
2. Prostorna pokrivenost bežične mreže
3. Broj korisnika
4. Enkripcija
5. Autentifikacija
6. Sprečavanje napada
7. Napredne mogućnosti

Metode vrednovanja koje se odnose na jednostavnost i cijenu izvedbe lokalne bežične mreže prikazani su u tabeli 1.

Tabela 1. Jednostavnost i cijena izvedbe

Predmet razmatranja	Loše	Prosječno	Dobro
Troškovi informatizacije	Visoki	Srednji	Niski
Zahtjeva dodatni hardware (server)	Da	-	Ne
Zahtjeva dodatni mrežni hardware	Da	-	Ne
Broj korisnika	Veliki broj korisnika	-	Mali broj korisnika

Metode vrednovanja koje se odnose prostornu pokrivenost lokalne bežične mreže prikazani su u tabeli 2.

Tabela 2. Optimalna prostorna pokrivenost bežične mreže

Predmet razmatranja	Loše	Prosječno	Dobro
Zahtjeva dodatni mrežni hardware	Ne	-	Da
Veliki broj korisnika mreže	Ne	-	Da
„Warchalking“[1]	Ne	-	Da

Metode vrednovanja koje se odnose na broj korisnika lokalne bežične mreže prikazani su u tabeli 3.

Tabela 3. Broj korisnika bežične mreže

Predmet razmatranja	Loše	Prosječno	Dobro
Zahtjeva dodatni mrežni hardware	Ne	-	Da
Zahtjeva dodatni	Ne	-	Da

[1] „Warchalking“ - informira korisnike bežičnog interneta o tome da su se našli u dometu WLAN mreže označene sa informacijama vezane uz istu (SSID, enkripcija, tip mreže).

mrežni hardware			
Sigurnosna razina	Niska	-	Visoka

Metode vrednovanja koje se odnose na enkripcijsku zaštitu lokalne bežične mreže prikazani su u tabeli 4.

Tabela 4. Enkripcija

Predmet razmatranja	Loše	Prosječno	Dobro
Tip enkripcijskog ključa	Statički	-	Dinamički
Tip ključa za šifriranje (algoritam)	RC4 (WEP)	-	AES (WPA/WPA2)
Duljina ključa za šifriranje	40 ili 104 bitna enkripcija	128 bitna enkripcija	128 bitna enkripcija + 64 bitna autentifikacija
Vrijeme potrebno za „probijanje“ zaštite	Nekoliko sati	Nekoliko dana	Stoljećima
Količina mrežnih paketa potrebnih za enkripciju	Nekoliko miliona	-	Nekoliko trilijuna
Korištenje sustava za upravljanje enkripcijskim ključevima	Nema	Statički	EAP

Metode vrednovanja koje se odnose autentifikaciju lokalne bežične mreže prikazani su u tabeli 5.

Tabela 5. Autentifikacija

Predmet razmatranja	Loše	Prosječno	Dobro
Tip autentifikacije	Enkripcijski ključ (WEP/WPA)	Enkripcijski ključ + MAC adresa klijenta	RADIUS server
Zahtjeva dodatni hardware (server)	Ne	-	Da
Korištenje mehanizama autentifikacije	Ne	-	EAP (802.11x)

Metode vrednovanja koje se odnose mogućnost sprečavanja napada unutar lokalne bežične mreže prikazani su u tabeli 6.

Tabela 6. Sprečavanje napada

Predmet razmatranja	Loše	Prosječno	Dobro
Pervencija ponovljenog napada	Ne	-	Da
Sprečavanje poznatih napada	Ne	Djelomično	Potpuno
Korištenje	Ne	-	EAP (802.11x)

mehanizama autentifikacije			
Minimizacija štete uzrokovane napadom	Ne	-	Da

Metode vrednovanja koje se odnose na neke napredne mogućnosti lokalne bežične mreže prikazani su u tabeli 7.

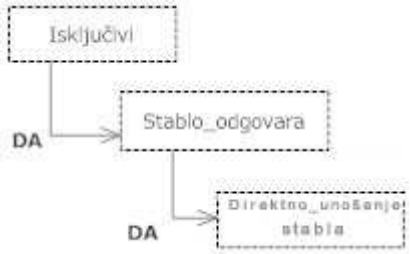
Tabela 7. Napredne mogućnosti mreže

Predmet razmatranja	Loše	Prosječno	Dobro
Mogućnost otkrivanja fizičke lokacije korisnika mreže	Ne	-	Da

4. METODOLOGIJA EKSPERTNOG SUSTAVA

Prijedlog optimalne konfiguracije bežične mreže sa uključenim sigurnosnim aspektom bio bi cilj ekspertnog sustava. Aplikacija bi predstavljala „pomoćnika“[5] koji na temelju određenih parametara korisnika predlaže optimalno rješenje konfiguracije bežične mreže sukladno potrebama i karakteristikama korisnika. S druge strane, ekspertni sustav mogu koristiti mrežni administratori za brzo pronalaženje optimalnog rješenja postavljanja bežične mreže s uključenim mehanizmima sigurnosti kao i korisnici koji se po prvi puta susreću s navedenom problemom.

Prema korištenoj metodologiji razvoja ekspertnog sustava, model ekspertnog sustava koji rješava problem postavljanja i sugurnosti bežičnih mreža može se klasificirati u skupinu preporuke, odabira i savjeta. Funkcionalnost se temelji na odabiru mrežnih servisa/usluga koje se primarno koriste u obrazovnim institucijama, iz liste ponuđenih servisa/usluga, koja odgovara potrebama i željama korisnika. U završnoj fazi se iz baze podataka ispisuju konkretni podaci. Pretvorba modela rješenja u strukturiranu hijerarhiju (strukturiranje znanja) podrazumijeva da su znanje i proces zaključivanja podijeljeni u nekoliko zadaća. Zadaće će se nalaziti u određenoj hijerarhiji te će se, shodno tome, primijeniti veze tehnikom ulančavanja. Akvizicija znanja pojedinačnih zadaća prikupiti će se od eksperata ili dokumentacije (stručni priručnici, knjige). Znanje ES-a bazirati će se na znanju eksperta te iz stručne literature koja pokriva područje bežičnih mreža i sigurnosti. Odabir odgovarajuće metodologije akvizicije znanja može se predstaviti stablom odlučivanja (Slika 2.).



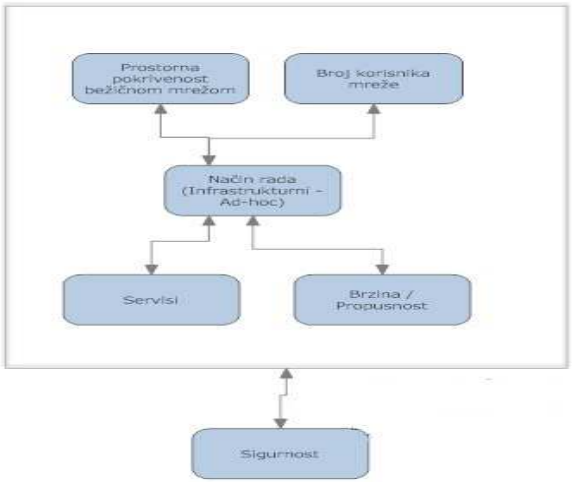
Slika 2. Stablo odlučivanja

Prilikom izrade ekspertnog sustava bila bi korištena metodologija direktnog unošenja stabla odlučivanja. Zadaće ekspertnog sustava imaju isključive izlaze pri čemu će biti primijenjena dijagnostika.

5. RJEŠENJE EKSPERTNOG SUSTAVA

Rješenje ekspertnog sustava ovisiti će o sljedećim parametrima:

a) Prostorna pokrivenost
b) Broj korisnika
c) Mrežni način rada (infrastrukturni ili ad-hoc)
d) Željeni mrežni servisi/usluge
e) Potrebna brzina/propusnost (engl. bandwith)
f) Sigurnosna razina



Slika 3. Shematski prikaz određivanja prioriteta korisnika bežične mreže [2]

Ako je A prostorna pokrivenost bežične mreže, B broj korisnika, C način rada, D mrežni servisi, E brzina/propusnost i F sigurnost onda općeniti izraz za elemente koji utječu na

postavljanje/konfiguriranje bežične mrežne infrastrukture s uključenim sigurnosni faktorom glasi:

$$A * B * C * D * E * F = A^n B^n C^n D^n E^n F^n$$

Pretpostavka je da vrijeme raspoloživosti (engl. *uptime*) bežične mreže bude 99% odnosno 30 dana u mjesecu x 24 h = 720 sati mjesečno. Metodologija pristupa rješavanja sigurnosnog problema ekspertnog sustava ovisiti će prvenstveno o željama i potrebama korisnika, ali i o tehničkim pretpostavkama. Sigurnost bežične mreže 802.11 standarda ovisi o namjeni odnosno jednostavnosti konfiguriranja pristupa s korisničke strane te se može prikazati u nekoliko razina [2]:

- Otvoreni tip (engl. Open type) – bez sigurnosnog mehanizma zaštite
- Dijeljena tajna (engl. Shared key) – sa enkripcijskim algoritmima i certifikatima poput: WEP, WPA, WPA2 (Personal i Enterprise).

Parametri koji utječu na sigurnost bežične mreže ovise o korištenim mrežnim servisima kao i tehničkim pretpostavkama. Primjer sigurnosnih mehanizama koji direktno utječu na sigurnost bežične mreže:

- Broj korisnika,
- SSID Broadcast,
- Autentifikacija i autorizacija,
- Enkripcija (WEP/WPA/WPA2),
- MAC filtriranje,
- Pristup internetu,
- Firewall,
- VPN

Primjenu ekspertnog sustava moguće je prikazati na primjeru *pristupa internetu* putem bežične mreže kao jedna od usluga čije korištenje obrazovne institucije podrazumijevaju. Bežični pristup internetu analizirati će se s obzirom na broj predviđenih korisnika. Na temelju broj korisnika i prostorne površine pokrivenosti bežičnim mrežnim signalom definirati će se broj pristupnih točaka (te pripadajućih antenskih primopredajnika) u infrastrukturnom načinu rada (WDS, Repeater mode). Zatim slijedi uporaba sigurnosnih mehanizama koji će se

primijeniti za pristup internetu. U obzir će se uzeti i jednostavnost konfiguriranja te autorizacija korisnika. S obzirom da se radi o pristupu internetu te korištenju Word Wide Web servisa putem HTTP protokola isti će biti prilagođen na način da se korisniku omogući optimalno korištenje uz zadovoljavajuću brzinu rada. Brzina rada ovisna je o primijenjenim mrežnim standardima poput 802.11 b/g/n. Ukoliko korisnik zahtjeva veću stabilnost u radu, veći doseg, ali niže brzine prijenosa primijeniti će se 802.11 b standard u protivnom standard 802.11 g/n. Važno je voditi računa i o frekvencijskom opsegu rada bežičnih mrežnih standarda (2,4 – 5 Ghz) kako bi se izbjegle interakcije s drugim uređajima te, shodno tome , degradirale performanse. Primjenjivi model sigurnosti mora osigurati jednostavnost autentifikacije, prilagođenu brzinu pristupa, dobru pokrivenost, zaštitu prijenosnog medija odgovarajućim sigurnosnim mehanizmima. **Prva** mogućnost podrazumijevala bi korištenje WPA/WPA2 certifikata TKIP/CCMP protokolom (autentifikacija temeljena na dijeljenoj tajni) te RC4 ili AES enkripcijskih algoritama s isključenim Wireless Protection System (WPS) mogućnostima pristupne točke/usmjerivača. **Druga,** ukoliko računalna (mrežna) infrastruktura posjeduje odgovarajuću opremu, proces autorizacije može biti potpomognut korištenjem RADIUS protokola uz odgovarajući LDAP imenik, koji se primarno koristi u ustanovi. Korištenjem RADIUS protokola proces prijave na bežičnu mrežu podrazumijeva generiranje jedinstvenog ključa putem korisničkog imena i zaporke za svakog pojedinog korisnika. Takav način dodatno zahtjeva složenije konfiguriranje klijentskog računala, ali znatno podiže razinu sigurnosti. Ukoliko pridodamo i mogućnost korištenja vatrozida sigurnosna razina mrežnom pristupu biva na vrlo visokoj razini. **Treća** mogućnost daje odobrenje pristupa bežičnoj mreži putem MAC adrese računala (MAC filtriranje) koja je u kontekstu sigurnosti najizloženija neželjenim napadima s obzirom na mogućnost promjene fizičke MAC adrese klijentskih mrežnih adaptera putem javno dostupnih alata. WEP algoritam je u potpunosti isključen, kao jedna od mogućih opcija zaštite neovlaštenog pristupa bežičnoj mreži, jer se je isti pokazao ranjiv na aktivne i pasivne mrežne napade zbog ranjivog inicijalizacijskog vektora mrežnog sloja koji se koristi u procesu odobrenja pristupa. Valja uzeti u obzir i sigurnosni rizik koji proizlazi „unutarnjom stranom“ mreže. Sve nabrojane mogućnosti ekspertni sustav uzima u obzir te predlaže optimalno rješenje.

Broj korisnika također predodređuje parametre koji su ključni u izgradnji bežične mrežne infrastrukture. Veći broj korisnika mreže bitno zauzima hardverske resurse pa se isti moraju prilagoditi broju korisnika. Činjenica jest da komercijalno dostupne pristupne točke (engl. Access Point) omogućavaju teorijsko opsluživanje do 256 klijenata (ovise o brzini i

arhitekturi ugrađenog mikroprocesora te programskim mogućnostima). U praksi do taj broj iznosi u rasponu od 8-10 klijenata. Ekspertni sustav u ovom slučaju bi trebao predložiti specifične uređaje koji mogu opsluživati i više od 10 klijenata. Veći broj korisnika mreže podrazumijeva visok rizik od mrežnih upada te visoku razinu sigurnosti, ali zahtjeva složenost konfiguriranja te jednostavnost pristupa. Ekspertni sustav vodi računa i o maksimalnoj teorijskoj propusnosti (bandwith) mreže kako ne bi došlo do zagušenja mrežnog prometa.

SSID Broadcast vrlo je važan čimbenik u sigurnosti. SSID (engl. Service Set Identifier) je jedinstveno ime koje moraju dijeliti svi uređaji (pristupne točke, usmjerivači, mrežne kartice) unutar jedne bežične mreže. Emitiranje SSID Broadcasta otkriva naziv bežične mreže te tako ista biva izloženija eventualnim vanjskim napadima. Isključivanje emitiranja SSID Broadcasta doprinosi sigurnosti, ali zahtjeva kombiniranu uporabu i ostalih mehanizama sigurnosti te dodatno otežava pristup korisniku zbog manualnog podešavanja postavki mrežnog adaptera odnosno, unosa SSID-a.

Autentifikacija i autorizacija. Pod autentifikacijom podrazumijevamo provjeru da je korisnik upravo onaj koji tvrdi da je, dok je autorizacija vezana uz dodjeljivanje takvom korisniku određenih prava. U procesu autentifikacije sudjeluje sam korisnik/klijent dok autorizacija jest proces koji se izvršava na hardverskoj i softverskoj razini cjelokupnog mrežnog sustava. U poraba mehanizama zaštite u procesu autentifikacije i autorizacije ovisi o faktorima jednostavnosti spajanja korisnika, konfiguriranju mreže, uporabi specifičnih uređaja/softvera te jednostavnosti administriranja mreže. Ovisno o željama i potrebama korisnik te o zahtjevnim mrežnim servisima, proces autentifikacije mora biti krajnje jednostavan.

Enkripcija. Siguran pristup bežični mrežama ovisi o uporabi specifičnih mrežnih certifikata i algoritama putem kojih se korisnicima dopušta/ne dopušta pristup. Kod zaštićenih bežičnih mreža su uglavnom WEP algoritmi, WPA/WPA2 certifikati, TKIP/CCMP protokoli, RADIUS protokol te filtriranje putem MAC adresa mrežnih adaptera. Danas, certifikat s najvećom razinom sigurnosti jest WPA2 (Enterprise) koji uključuje i korištenje LDAP imenika. WEP algoritam se ne preporučuje zbog ranjivosti na aktivne i pasivne mrežne napade. Bežična mreža može se uvijetno podesiti i bez sigurnosnih mehanizama zaštite pristupa tzv. otvorenim tipom mreže(engl. Open type) uz ograničenje brzine, propusnosti te onemogućavanje pojedinih usluga/servisa (npr. torrent, FTP i dr.)

MAC filtriranje. Mana ove metode je činjenica da je administriranje statičkih filter lista kod velikih mreža vrlo nepraktično i zahtjeva puno truda i vremena. Pristupne točke /usmjerivači bežične mreže koji komuniciraju s klijentom zahtijevaju više vremena prilikom prijave kako bi se podaci (MAC adresa pristupnog adaptera) upisali u autentifikacijsku tablicu pristupne točke/usmjerivača. Ova metoda pokazala se je ranjivom iz razloga što u adresnoj tablici pristupne točke/usmjerivača ostaju zapisane sve MAC adrese uređaja koji imaju ovlašteni pristup, a koje bi „napadač“ mogao iskoristiti.

Vatrozid (engl. Firewall) dodatni je mehanizam zaštite lokalnoj mreži, kako žičanoj mreži po ethernet 802.3 standardu tako i bežičnoj mreži po 802.11 standardu. Vatrozid filtrira cjelokupni mrežni promet lokalne mreže te visoko podiže razinu sigurnosti. Ovisno o arhitekturi mreže, vatrozid može filtrirati lokalni i Internet mrežni promet. Ekspertni sustav će, ovisno o namjeni mreže, razmotriti mogućnost uporabe vatrozida. Pri tom je važno napomenuti da implementacija vatrozida zahtjeva složeniji način konfiguriranja, napredno znanje administratora mreže te sa sobom nosi i neka ograničenja s kojima korisnici moraju biti upoznati. (nemogućnost korištenja specifičnih web stranica, usluga i servisa te protokola).

VPN je tehnologija koja omogućava sigurno povezivanje privatnih mreža u zajedničku virtualnu privatnu mrežu kroz javnu mrežnu infrastrukturu, što je danas najčešće internet. Ostvaruje se siguran "tunel" između dvije krajnje točke. Kod tuneliranja se provodi kompresija i/ili kriptiranje podataka. Pristup virtualnim privatnim mrežama dodatno je zaštićen procesom autentifikacije i autorizacije. Dakle, korištenje enkripcije pristupa bežičnoj mreži samo je jedan od sigurnosnih mehanizama zaštite. VPN mreže zahtijevaju obavezno korištenje i vatrozida čime postavljanje sigurnosnih mehanizama ovog tipa mreže zahtjeva složeniji pristup te znanje administratora. Osim korištenja enkripcije u pristupu mreži bežičnim putem, sigurnosni zahtjevi VPN mreže su:

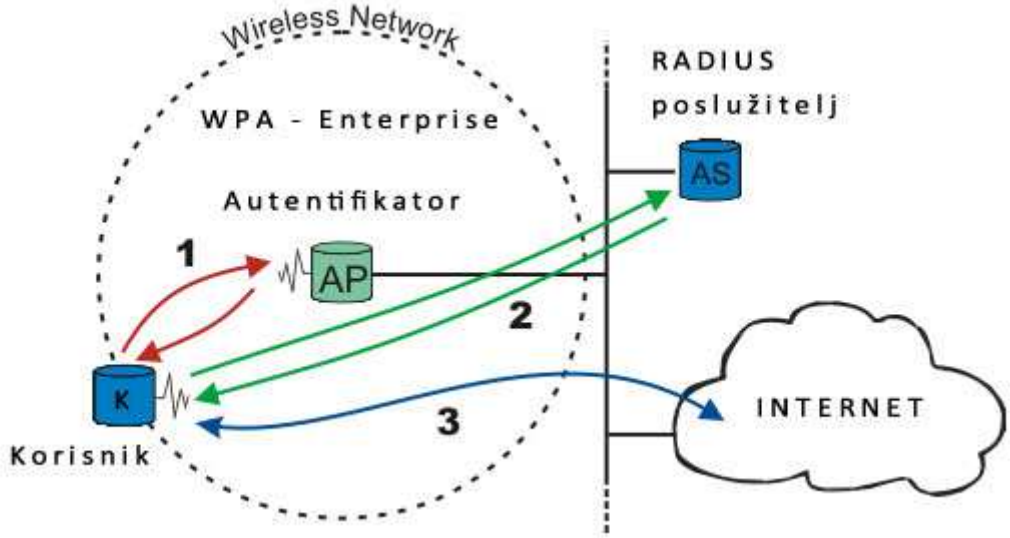
1. Pravo pristupa – VPN osigurava provjeru identiteta korisnika i dopušta VPN pristup samo registriranim korisnicima te osigurati praćenja događaja (engl. logging),
2. Autentikacija i autorizacija – provjera autentičnosti korisnika te dodjeljivanje korisničkih prava,
3. Integritet podataka – VPN mora osigurati provjeru jesu li podaci putem promijenjeni. Za to se najčešće koristi MD5 algoritam,

4. Povjerljivost – VPN mora osigurati kriptiranje podataka tako da ih nitko, osim klijenta odnosno poslužitelja ne može pročitati. To se postiže raznim algoritmima, a neki od njih su DES, RSA te Diffie-Hellman.

6. PRIMJER VERIFIKACIJE MODELA

Predloženi model može se verificirati na slijedećem primjeru. Potrebno je osigurati bežični pristup internetu korisnicima obrazovne institucije „X“. Pristup internetu podrazumijeva korištenje www servisa. Pristup internetu trebaju imati isključivo osobe koje pohađaju nastavu ili su u radnom odnosu u navedenoj instituciji. Ekspertni sustav će od korisnika tražiti unos (Ulaz) te putem mehanizama zaključivanja predložiti optimalno rješenje (Izlaz). Verifikacija modela prikazana je na slici 4. te započinje slijedom:

a) Ulaz: prostorna pokrivenost bežičnim mrežnim signalom. U ovom slučaju ona neka iznosi DxŠ prostora. Izlaz: na temelju veličina prostora ekspertni sustav će odabrati broj bežičnih pristupnih točaka (Access Points-AP) te predložiti infrastrukturni način rada.
b) Ulaz: broj korisnika je također važna faktor zbog odabira pristupnih točaka koji mogu opsluživati veći broj korisnika. Izlaz: odgovarajući modeli pristupnih točaka.
c) Ulaz: Servisi također su vrlo važni prilikom definiranja sigurnosti mreže jer u protivnom neki parametri sigurnosti mogu onemogućiti rad ostalih servisa/usluga mreže. U primjeru to je www servis.
d) Ulaz: odabir bežičnih mrežnih standarda definira u određenoj mjeri i brzinu/propusnost bežične mreže. Trenutačno su aktualni 802.11g, i n standard.
e) Izlaz: s obzirom da se radi o obrazovnoj instituciji prijedlog jest da autentifikacija korisnika bude provedena putem RADIUS protokola i LDAP imenika. Takva konfiguracija iziskuje postojanje centralnog poslužitelja te dodatne mrežne opreme. Navedeni mehanizam zahtjeva bazu podataka registriranih korisnika (učenici/studenti te djelatnici) koji posjeduju elektroničke korisnike identitete putem kojih se prijavljuju na bežičnu mrežu.
f) Izlaz: na temelju prethodnih parametara definira se razina sigurnosti bežične mreže od neovlaštenog pristupa. U primjeru preporučiti će se pristup s dijeljenom tajnom (Shared key) i to WPA Enterprise enkripcija s RADIUS protokolom. Dodatna sigurnost postići se podešavanjem vatrozida (firewall).



Slika 4 Shema predloženog modela konfiguracije bežične mreže sa uključenim sigurnosnim mehanizmima

7. ZAKLJUČAK

Predloženi model vrednovanja uzima u obzir parametre te servise/usluge koji su ključni u sigurnosti lokalnih bežičnih mreža u obrazovnim institucijama, ali daje i mogućnost uključivanja dodatnih sigurnosnih parametara kako bi se zadovoljile specifične potrebe korisnika i u drugim organizacijama.

Kreirani ekspertni sustav može poslužiti kao svojevrsna pomoć u razumijevanju, kreiranju bežične mrežne konfiguracije u odnosu na zahtijevane usluge s naglaskom na sigurnosni aspekt. Praktični doprinos ekspertnog sustava očituje se u izradi projektnog rješenja sigurnosti lokalnih bežičnih mreža u obrazovnim institucijama. Ekspertni sustav može se tehnički izvesti s danas komercijalno dostupnim alatima poput objektno-orijentiranog programskog jezika engl. *Hypertext Preprocessor* (PHP) te jezika za relacijskih model podataka engl. *Structured Query Language* **(**SQL).

REFERENCE

1. Web izvor: Davies, J., *The Cable Guy* August 2005, 11.8.2005., *Wi-Fi Protected Access Dana Encryption and Integrity*, http://www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx, 25.08.2012.

2. Web izvor: Lehembre, G., Hacking WiFi, 26.4.2006., *WiFi security – WEP, WPA and WPA2*, http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf, 25.08.2012.
3. Web izvor: Borisov, N., Goldberg, I., Wagner, D., *WEP Draft*, 2.2.2001., *Intercepting Mobile Communications: The Insecurity of 802.11*, http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf, 25.08.2012.
4. Evans, C. *The Mighty Micro.*London, Gollancz: 1979.
5. Carnet dokument, CCERT-PUBDOC-2003-05-22
6. Hamidović, H. *WLAN Bežične lokalne mreže*. Zagreb, INFOPRESS: 2006.
7. Polišćuk, E.,J.*Ekspertni sistemi*. ETF, Podgorica, 2008.
8. Čerić, V., Varga, M. *Informacijska tehnologija u poslovanju*. Zagreb, Element: 2004.
9. Bača, Miroslav; Ivanda, Stipe. *Razvoj ekspertnog sustava u detekciju neovlaštenog upada u računalni sustav*. // Policija i sigurnost. 11 (2002) , 4-6; 212-231.
10. Klepac, Goran. *Primjena inteligentnih računalnih metoda u managementu*. Zagreb, Sinergija: 2001.
11. Stankov, Slavomir; Lovrić, Gordan. *Inteligentno i interaktivno okruženje učenja i poučavanja - iskustva u primjeni* // *MIPRO'99, Računala u školi* / Rijeka : MIPRO, 1999. 56-59.
12. Web izvor: http://ponude.biz/knjige/tutorijali/Sigurnost_bezicnih_LAN-ova.pdf (05.06.2012.)
13. Web izvor: http://www.eduroam.hr/ (05.06.2012.)