UDC: 004.492 INFO M: str. 4-14

ZAŠTITA BEŽIČNIH MREŽA
SECURITY OF WIRELESS NETWORKS

Siniša Kuprešak, Dejan Simić

REZIME: Brz porast bežičnih LAN (WLAN) sistema dovodi do potrebe za rešenjima zaštite koja ispunjavaju zahteve širokog kruga korisnika. U WLAN-ovima postoje ranjivosti na svim nivoima i zato je zaštita tako važna kod bežičnih mreža. U ovom radu je dat pregled bežičnih komunikacionih tehnologija. Prikazane su osnovne vrste zaštite, kao i napredne metode zaštite.
KLJUČNE REČI: bežične mreže, zaštita
ABSTRACT: The rapid growth of Wireless LAN (WLAN) systems drives the need to support security solutions that meet the requirements of a wide variety of customers. There are vulnerabilities on all levels in WLANs and therefore security is so important for wireless networks. In this paper an overview of wireless communication technologies is given. The basic security types, as well as advanced security methods are described.
KEY WORDS: wireless networks, security

1. UVOD

Razvoj mobilnih računara je uslovio da oni postaju korišćeniji na radnim mestima, čak sve češće preuzimaju ulogu klasičnih desktop računara. Njihova prednost je laka prenosivost, mogućnost korišćenja na poslovnim sastancima, video konferencijama i poslovnim putovanjima. Njihovim povezivanjem na bazi standarda 802.11 formiraju se WLAN-ovi ("Wireless Local Area Networks") koji kompanijama nude sasvim drugu dimenziju poslovanja i veću produktivnost. Ovakve mreže nisu ograničene na samo jednu kompaniju te se mogu koristiti i van klasičnog kancelarijskog okruženja. Mnogi javni Internet servis provajderi (ISP) omogućavaju pristup Internetu na aerodromima, konferencijskim salama i kafeima.

Ideja bežičnog umrežavanja nije tako nova. I ranije su u okviru klasičnih mreža postojali segmenti koji su bili mobilni. Takvi segmenti nisu bili bazirani na standardima i koristili su tehnološke implementacije samog proizvođača. Danas postoji nekoliko standarda za bežične aplikacije, kao na primer: 802.11, "HiperLAN", "HomeRF SWAP" i "Bluetooth".

Prema razlikama u načinu funkcionisanja WLAN-ove možemo podeliti na "peer-to-peer" (P2P) WLAN, "multiple-cell" WLAN, i "building-to-building" WLAN ("point to point" i "point to multipoint"). Kod P2P WLAN-ova mobilni klijenti poseduju bežičnu mrežnu kartu (NIC) i komuniciraju direktno bez pristupne tačke ("access point"-a - AP). Domet je ograničen samo na učesnike te P2P mreže i ne postoji mogućnost pristupa žičanoj mreži. "Multiple-cell" WLAN tj. mreža zasnovana na više ćelija ima domet koji zavisi od samih karakteristika AP-a a veća područja se pokrivaju preklapanjem (tj. preplitanjem) dometa ćelija. Pristup klasičnoj mreži je omogućen preko bežičnog mosta ("wireless bridge"). "Building-to-building" WLAN-ovi povezuju mreže u različitim zgradama u tzv. kampus mrežu. Postoje dve vrste ovakvih mreža i to "point to point" i "point to multipoint". "Point to point" komunikacija može da se realizuje radio talasima (pomoću posebnih fokusirajućih radio antena formira se uski talas koji može da pređe i velike razdaljine) ili laserskim zracima [1].

2. PREGLED BEŽIČNIH KOMUNIKACIONIH TEHNOLOGIJA

"**HiperLAN**" je standard ratifikovan 1996 godine od "European Telecommunications Standards Institute" (ETSI). HiperLAN-1 standard definiše komunikaciju na frekvenciji od 5 GHz brzinom do 24 Mbps. ETSI je u skorije vreme propisao i novi HiperLAN/2 standard koji radi na 5 GHz sa protokom do 54 Mbps.

"**HomeRF SWAP**" **-** 1988 godine HomeRF SWAP Group objavila je "Shared Wireless Access Protocol" (SWAP) standard za bežičnu digitalnu komunikaciju između PC-ja i korisničkih elektronskih uređaja. SWAP podržava prenos glasa i podataka preko klasičnog intrerfejsa brzinom od 1 do 2 Mbps koristeći "frequency-hopping" i "spread-spectrum" tehnike na 2.4 GHz.

"**Bluetooth**" povezuje računare u "Personal-Area Network" (PAN) definisan od strane "Bluetooth Special Interest Group". Ovakva komunikacija je kratkog dometa i koristi "frequency-hopping spread spectrum" tehniku na 2.4 GHz.

802.11 bežična tehnologija - Organizacija IEEE je razvila grupaciju standarda pod nazivom 802.x (802.3 je na primer za "Ethernet"). Neprofitna organizacija, koja se ne bavi prozvodnjom kompjuterske opreme, poznata pod imenom Wi-Fi Alliance vrši brending svih 802.11 tehnologija. Da bi neka komponenta dobila Wi-Fi oznaku mora da prođe testiranje u njihovim laboratorijama čime je garantovana kompatibilnost

sa svim drugim Wi-Fi brend komponentama. 802.11 definiše korišćenje frekventnog opsega u kome se odvija komunikacija. Radi se o području poznatom kao industrijsko-naučno-zdravstveno. Preciznije ovaj standard određuje dva opsega: 2.4 GHz do 2.4835 GHz UHF (802.11 i 802.11b) i 5.15 GHz do 5.825 GHz SHF (802.11a). Spektar je klasifikovan kao nelicenciran, što znači da niko nije njegov vlasnik i da može biti korišćen sve dok uređaji korisnika zadovoljavaju pravila "Federal Communications Commission" (FCC). Ova zakonska regulativa se odnosi na USA. Neki od parametara koje definiše FCC je maksimalna snaga emitovanja, vrsta enkodiranja i frekventna modulacija.

RF metode Emitovanje u području 2.4 GHz se izvodi uz "spread-spectrum" tehnologiju tj. slanje podataka po različitim frekvencijama. Ovo je neophodno izvesti jer ova oblast spektra ima svoje primarne vlasnike – proizvodjače mikrotalasnih pećnica, koje emituju talase u istom opsegu ali neuporedivo veće snage (mrežne kartice računara imaju snagu od 100mW a pećnice 600W). 802.11 definiše dve vrste fizičkog sloja za uređaje koji emituju radio talase: jedan koristi "frequency-hopping" arhitekturu, a drugi komunicira na samo jednoj frekvenciji – direktno sekvencioniranje.

"**Frequency Hopping" (deljenje ili skakanje frekvencija) -** Ovaj metod se koristi u području 2.4 GHz do 2.4835 GHz. Kao što se može videti ukupan interval je 83.5 MHz. Umesto da stalnog emitovanja na istoj učestanosti, vrši se menjanje po unapred predviđenoj matrici na ukupno 79 različitih 1 MHz kanala. Između dva deljenja protekne izuzetno kratak interval (ne duži od 0.4 sekunde). Velika prednost ovog modela je što se umesto očekivanog protoka od 2 Mbps kada imamo monohromatsku emisiju, postižu brzine do 10 Mbps.

Direktno sekvencioniranje i 802.11b - U ovom slučaju opseg 2.4 GHz do 2.4835 GHz se deli na tri područja od 22 MHz. Kada se vrši transmisija nekim kanalom ona se odvija nezavisno od naredna dva, što omogućava da se priključe ukupno tri nezavisna AP-a. Ovo ima za posledicu porast protoka koji dostiže i 11 Mbps po kanalu odnosno ukupno 33 Mbps.

802.11a mreže - 1999. IEEE je ratifikovao novi fizički sloj poznat kao 802.11a. Ovaj standard koristi 5 GHz SHF i ostvaruje protok 54 Mbps. Za razliku od 802.11 i 802.11b standarda, 802.11a standard koristi tip frekvenciono - divizioni multipleks (FDM) nazvan ortogonalni FDM (OFDM). U FDM sistemu, dozvoljen frekventni opseg je podeljen na više nosača podataka. Transmitovani podaci su tada podeljeni između ovih nosača. Ova tehnika smanjuje efikasni frekventni opseg. U OFDM-u, brojni nosači se koriste da bi podelili podatke preko dostupnog spektra, sličnog FDM-u. Međutim, u OFDM sistemu svaki ton mora da bude ortogonalan (nezavisan ili nepovezan) drugim tonovima, i zbog toga ne zahteva granice. OFDM obezbeđuje visokofrekventnu efikasnost u poređenju sa FDM-om.

3. OSNOVNE VRSTE ZAŠTITE

Bežične mreže su postale danas jedna od najinteresantnijih meta za hakere. Današnje kompanije primenjuju bežične tehnologije ubrzanim tempom, često bez razmatranja svih bezednosnih aspekata. Primena je ubrzana zahvaljujući niskoj ceni uređaja, jednostavnoj upotrebi i velikim dobicima u proizvodnji. Zbog toga što se WLAN uređaji dopremaju sa isključenim sigurnosnim opcijama, povećano korišćenje WLAN-a privuklo je pažnju hakerske zajednice. Nekoliko Internet stranica prikazuju potpuno dostupne bežične veze širom USA [2].

Iako mnogi hakeri koriste ove konekcije kao način besplatnog pristupa Internetu, ili da sakriju svoj identitet, manje grupe vide ovu situaciju kao mogućnost upada u mreže u koje bi inače teško upali preko Interneta. Za razliku od kablovskih mreža, WLAN šalje podatke kroz etar i može joj se pristupiti i izvan fizičkih granica kompanije. Ako WLAN podaci nisu kodirani, pakete mogu videti svi u oblasti radio-frekventnog dometa. Na primer, osoba sa instaliranim Linux-om na laptopu, WLAN adapterom i programom kao što je TCPDUMP može da preuzme, pogleda i snimi sve pakete koji kruže datim WLAN-om [3].

Interferencija

U bežičnim mrežama može lako doći do interferencije. Uređaji koji koriste "Bluetooth" tehnologiju, tj. isto frekventno područje mogu da ometaju vezu ili da suze frekventni opseg emitovanja. Jednostavan emiter radio talasa može komunikaciju učiniti nemogućom. Na primer, ukoliko se neprestano prijavljujemo na AP sa zahtevom za logovanje, bez obzira da li uspešno ili ne, možemo da oborimo mrežu. Drugi bežični servisi koji rade u istom ili sličnom frekventnom području mogu da smanje korisni spektar bežičnih komunikacija. "Bluetooth" tehnologija na primer koristi isto 2.4 GHz radio frekventno područje kao i WLAN uređaji pa može da dođe do interferencije među njima.

MAC Autentikacija

WLAN AP može da identifikuje svaku mrežnu karticu računara koji se pojavljuje u mreži po njenom jedinstvenom MAC broju. To je adresa računara (tj. mrežne kartice) koja je trajno upisana u hardveru tako da se ne može menjati. Da bi koristili pojedine mreže prilikom logovanja proverava se MAC adresa i ukoliko se ona nalazi na spisku dopuštenih tj. regularnih korisnika onda se može uraditi prijava (logovanje). Iako na prvi pogled ovakva autentikacija deluje izuzetno sigurno postoje i loše strane njene upotrebe. Ukoliko hakeri izvrše "spoofing" ili ukradu mobilni računar moći će neometano da se pojave na mreži.

Ad hoc versus infrastrukturni model

Većina WLAN mreža koje se koriste u kompanijama su izgrađene na tzv. strukturnom modelu. Ovakva

arhitektura je karakteristična po tome što svi korisnici koji koriste mrežu moraju da se prijave preko AP-a. Nasuprot tom modelu WLAN mrežu je moguće organizovati kao nezavisnu P2P mrežu, koja se naziva i *ad hoc* mreža. Desktop ili notebook računari koji su opremljeni odgovarajućom mrežnom opremom, 802.11b ili 802.11a, mogu da komuniciraju i na udaljenostima od 150 metara. Veza se uspostavlja direktno bez posrednika. Ovakav tip mreža ima ozbiljne sigurnosne nedostatke. Bilo koji haker opremljen računarom i odgovarajućom mrežnom opremom koja je setovana identično kao i kod ostalih korisnika *ad hoc* mreže može nesmetano da upadne u ovakav sistem. U poslednje vreme su razvijene metode za identifikaciju i autentikaciju u ovakvim mrežama [4].

”**Denial of Service**”

802.11 menadžment poruke kao što su “request“ ili “response“, “association request“ ili “association response“, “re-association request“ ili “re-association response“, “disassociation“ i “de-authentication“ nisu autentikovane. Bez autentikacije ovih poruka ”denial-of-service” (DoS) napad je moguć. Primer “open source” alata kojim je moguće izvršiti ovakav napad je “wlan-jack” [5].

Lažni AP

U opasne sigurnosne propuste spada i lažni AP. Ove pristupne tačke su uglavnom postavljene od strane zaposlenih koji nemaju pravo pristupa bežičnim resursima. Takvi uređaji obično su jeftini i bez ikakve zaštite, i kao takvi laka meta za napad. Najbolja zaštita od ovakvih propusta je fizička provera računara u mreži i edukacija zaposlenih [6].

Prevencija

Preventivna zaštita se postiže na sledeće načine:

- “Corporate policy“
- Fizička zaštita
- 802.1X

Detekcija

Detekcija potencijalnog napadača na bežičnu mrežu može da se realizuje na sledeće načine:

- Upotrebom bežičnih analizatora ili snifera,
- Upotrebom alata za kriptovanje u žičanom delu mreže,
- Fizičkim nadgledanjem WLAN AP-a i njihove upotrebe.

802.11 je nesiguran

802.11b i 802.11a su danas najzastupljeniji standardi u WLAN tehnologijama. Tradicionalna 802.11 WLAN zaštita uključuje korišćenje otvorenih i deljenih ključeva ali i “wired equivalent privacy“ (WEP) ključeve za autentikaciju. Samo kombinacija pomenutih ključeva nudi rudimentalnu zaštitu pristupa i privatnosti, dok se korišćenje samo jedne vrste ključa ne preporučuje. U narednim odeljcima je opisano sa kakvim se izazovima susrećemo u implementaciji pomenutih načina zaštite.

Autentikacija

Korišćenje otvorenih ključeva predstavlja nešto više od samo provere identiteta. Korišćenje WEP-a štiti klijenta od slanja podataka ka AP-u ili primanja podataka od AP-a sve dok se klijent ne identifikuje odgovarajućim WEP ključem. U sistemu otvorenih ključeva AP šalje klijentu probni tekst koji on treba da dešifruje korišćenjem WEP ključa i vrati poruku AP-u. Ukoliko klijent nema pravi WEP ključ autentikacija se neće dogoditi i on ne može pristupiti AP-u. Ovakva autentikacija se ne smatra sigurnom jer ukoliko haker presretne probni i dekriptovani tekst može da zaključi i kako izgleda WEP ključ.

Upravljanje ključevima

Drugi tip ključeva, koji je mnogo češće korišćen ali što ne znači i da je potpuno siguran, je sistem statičkih WEP ključeva. Ovi ključevi, koji mogu biti 40 ili 128 bitni, su definisani od strane sistem administratora mreže i koriste se kako na AP-u tako i na svim klijentskim računarima koji komuniciraju sa datim AP-om. Očigledno je da definisanje ovog ključa od strane administratora mora biti izvršeno u istom trenutku za sve učesnike u komunikaciji.

Iako sistem deluje izuzetno sigurno može se probiti na vrlo jednostavan način. Ukoliko neko ukrade računar sa odgovarajućim ključem moći će da se infiltrira u mrežu neopaženo i koristi njene resurse sve dok neko ne obavesti sistem administratora o krađi uređaja. U takvoj situaciji osoba zadužena za sigurnost sistema mora da promeni ključeve na svim uređajima koji su u mreži. Ukoliko WLAN uključuje nekoliko stotina ili čak hiljada računara takav posao zaista može biti obiman. Još lošiju situaciju srećemo kada haker ukrade WEP ključ skenirajući saobraćaj korišćenjem alatki kao što je AirSnort. U tom slučaju administrator čak i ne zna da je bezbednost narušena.

WEP

WEP je jednostavan sistem zaštite definisan standardom 802.11 i štiti komunikaciju između AP-a i mrežne kartice na nivou protoka podataka. Iako preporučen od IEEE 802.11b kao 40 bitni danas WEP koristi 128 bitni ključ. Uprkos povećanju dužine izuzetno ga je lako razbiti. Na primer za probijanje 128 bitnog ključa potrebno je samo 15 minuta. Za ovakvo dešifrovanje potreban je samo “off the shelf“ alat koji se može naći na Internetu.

WEP koristi RC4 algoritam kodiranja razvijen od strane Ron Rivesta (RSA Data Security Inc). RC4 algoritam za enkripciju je simetričan i podržava promenljivu dužinu ključa. IEEE 802.11 standard opisuje upotrebu RC4 algoritma i WEP ključa, ali ne definiše specifičnu metodu distribucije ključeva. Bez automatske metode

za distribuciju ključeva svaki protokol za enkripciju može imati problema sa implementacijom zbog potencijalnih ljudskih grešaka u unošenju ključa, načina skladištenja i upravljanja. Kao potencijalno rešenje ovog problema od strane IEEE je ratifikovan standard 802.1X, što danas većina prizvođača mrežne opreme i koristi.

Inicijalizacioni vektor je centralni problem većine rasprava o sigurnosti WEP-a. Pošto se inicijalizacioni vektor transportuje kao čist tekst smešten u 802.11 zaglavlju svako ko snifuje WLAN može da ga vidi. Dužina inicijalizacionog vektora je 24 bita i nudi ukupno 16777216 mogućih vrednosti. Istražujući ovu problematiku grupa stručnjaka sa Univerziteta Berkli je došla do zaključka da ukoliko se koristi inicijalizacioni vektor isti kao i ključ za enkripciju paketa, (fenomen poznat pod imenom kolizija inicijalizacionog vektora), haker može da uhvati okvir podataka i iz njega izvuče kako podatke tako i informacije o mreži [7].

Ozbiljnost problematike potvrđuju i imena institucija koja su sarađivala na utvrđivanju propusta i njihovom rešavanju. Univerzitet Berkli, Univerzitet Merilend i Cisco Sistems sarađujući na ovom problemu objavili su rešenje pod imenom sofisticirano upravljanje ključevima [8].

4. NAPREDNE METODE ZAŠTITE

IPsec

IPsec je okvir otvorenog standarda za poboljšanje sigurnosti privatne komunikacije preko IP mreža. VPN-ovi koriste servise definisane preko IPsec-a da bi obezbedili tajnost, integritet i autentičnost podataka u komunikaciji preko javne mreže kao što je Internet. IPsec takođe ima praktičnu primenu u sigurnosti WLAN-a. Implementacija IPsec u okruženju bežičnih mreža izgleda ovako: IPsec se smešta na svaki računar koji je na mreži i od korisnika se zahteva da uspostavi IPsec tunel vezu ka bilo kom segmentu žičane mreže. Filtrira se bežični saobraćaj samo ka VPN gateway-u i DHCP-u ili DNS serveru. IPsec omogućava tajnost IP saobraćaja i autentikaciju. Tajnost je postignuta enkripcijom baziranom na različitim simetričnim algoritmima kao što su: "Data Encryption Standard" (DES), trostruki DES (3DES), ili najnoviji "Advanced Encryption Standard" (AES).

802.1X/EAP

Alternativni pristup WLAN sigurnosti fokusira se na razvoj radnih okvira koji omogućavaju centralizovanu autentikaciju i dinamičku distribuciju ključeva. Ova metoda je bazirana na Task Group i "end-to-end" okviru koji koristi 802.1X i "Extensible Authentication Protocol" (EAP). Cisco je inkorporirao 802.1X i EAP u svoje WLAN sigurnosno rešenje i nazvao ga Cisco "Wireless Security Suite". Tri glavna elementa 802.1X i EAP su:\

- Međusobna autentikacija među klijentima i autentikacioni RADIUS ("Remote Access Dial-In User Service") server,
- Enkripcioni ključ dinamički se raspoređuje posle autentikacije,
- Centralizovana kontrola polisa gde prekid sesije povlači za sobom ponovnu autentikaciju i generisanje novog enkripcionog ključa.

Kada su ovi standardi implementirani, bežični klijent u komunikaciji sa AP-om ne može da ostvari pristup mreži sve dok korisnik ne ispuni uslov ulaska u mrežu. Posle uspostavljanja kontakta klijent i mreža (AP ili RADIUS server) razmenjuju EAP poruke uspostavljajući međusobnu autentikaciju, pri čemu klijent verifikuje RADIUS server i obrnuto. EAP korišćen na klijentskoj strani dobija korisničke podatke (korisnički ID i lozinku, korisnički ID i jednokratnu lozinku - OTP, ili digitalni sertifikat). U toku klijent-server međusobne autentikacije RADIUS server i klijent razmenjuju WEP ključ za klijenta koji će on koristiti u toku datog logovanja. Korisnikova lozinka i ključ za sesiju nikada se ne šalju u čitljivom obliku preko bežične veze.

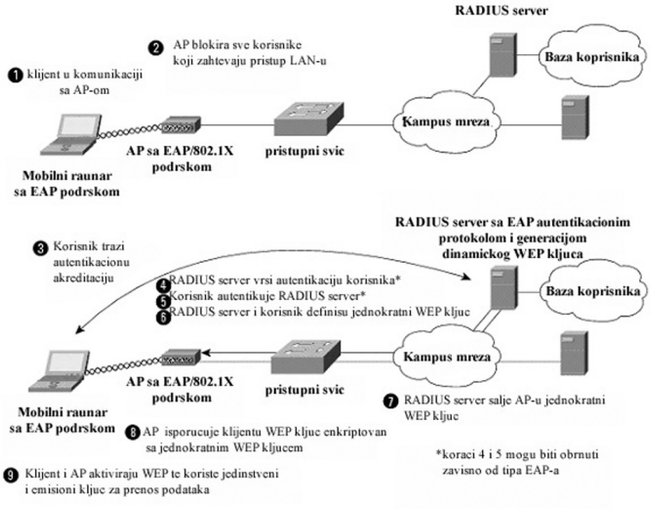
EAP pruža tri značajne prednosti u poređenju sa osnovnim 802.11:

- Prva prednost je međusobna autentikaciona šema. Ovakav princip uspešno eliminiše pretnju poznatu kao "man-in-the-middle" (MITM) napad izazvanu lažnim AP i RADIUS serverom.
- Druga prednost je centralizovano upravljanje i distribucija ključeva.
- Treća prednost je mogućnost definisanja centralizovane kontrole polise, gde okidač vremenskog isteka konekcije izaziva reautentikaciju i definisanje novog ključa.

EAP Autentikacioni Protokoli

Danas postoje različite vrste EAP-a za autentikaciju preko žičane ili bežične mreže. Kao što je prikazano na slici 1. oni uključuju:

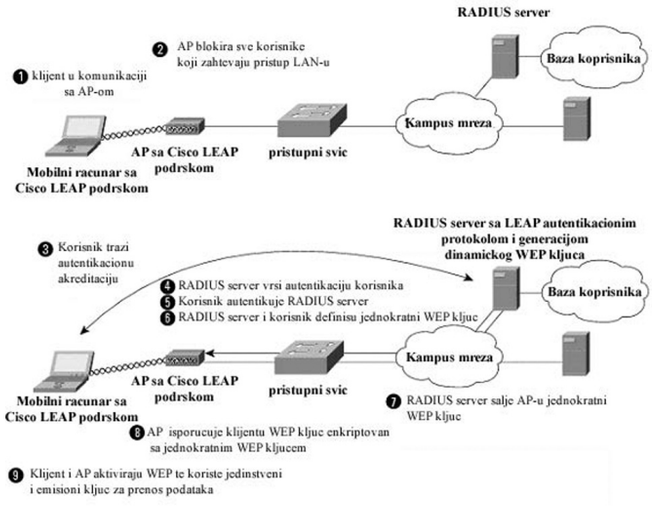
- EAP-Cisco Wireless (LEAP),
- EAP-"Transport Layer Security" (EAP-TLS),
- "Protected" EAP (PEAP),
- EAP-"Tunneled" TLS (EAP-TTLS) i
- EAP-"Subscriber Identity Module" (EAP-SIM).



Slika 1. – *EAP Autentikacioni proces*

Cisco LEAP

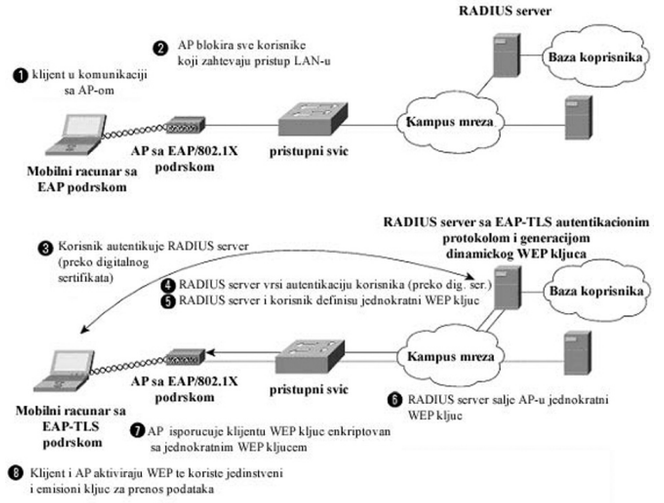
Cisco LEAP je vrsta EAP-a koja je u širokoj upotrebi u današnjim WLAN mrežama. LEAP podržava sva tri 802.1X i EAP elemente koji su prethodno navedeni. Sa njim međusobna autentikacija se bazira na deljenoj tajnosti, korisnička lozinka je poznata klijentu i mreži. RADIUS server šalje autentikacioni izazov klijentu koji koristi jednosmernu *hash* lozinku za kreiranje odgovora RADIUS serveru, kao što je prikazano na slici 2. Koristeći informacije iz svoje baze podataka RADIUS server kreira vlastiti odgovor i vrši poređenje sa odgovorom klijenta. Kada je RADIUS server autentikovao klijenta proces se ponavlja u suprotnom smeru omogućavajući klijentu autentikaciju RADIUS servera. Kada je procedura završena EAP-Success poruka se šalje klijentu i oba učesnika u komunikaciji definišu WEP ključ [9].



Slika 2. – *LEAP Autentikacioni proces*

EAP-TLS

EAP-TLS je "Internet Engineering Task Force" (IETF) standard (RFC 2716) koji je baziran na TLS protokolu (RFC 2246). EAP-TLS koristi digitalni sertifikat kako za korisničku

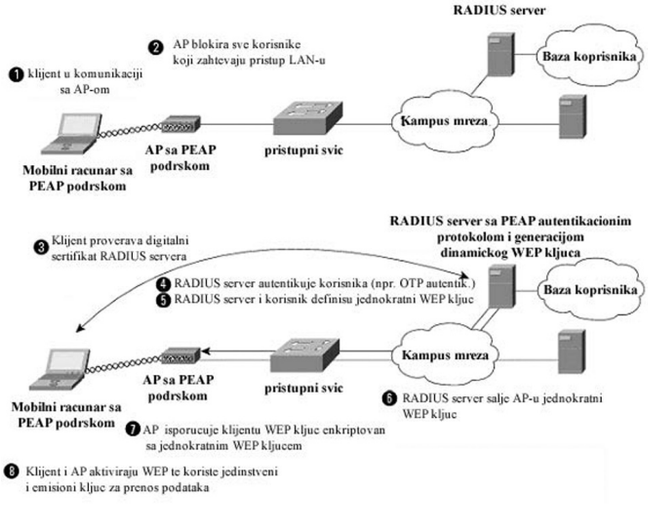


Slika 3. – *EAP-TLS Autentikacioni proces*

tako i serversku autentikaciju i podržava prethodno navedena tri elementa 802.1X/EAP. RADIUS server šalje svoj sertifikat klijentu u prvoj fazi autentikacione sekvence ("server-side" TLS). Klijent vrši validaciju RADIUS server sertifikata proveravajući izdavaoca sertifikata ali i sadržaj digitalnog sertifikata, kao što je prikazano na slici 3. Kada je ova procedura okončana klijent šalje svoj sertifikat RADIUS serveru u fazi 2 autentikacione sekvence ("client-side" TLS). RADIUS server odobrava klijentov sertifikat proveravajući izdavaoca sertifikata ("certificate authority server entity") kao i sam sadržaj digitalnog sertifikata. Kada je i ova procedura završena EAP-Success poruka se šalje klijentu i oba učesnika definišu dinamički WEP ključ.

PEAP

PEAP je IETF autorizovan od strane Cisco Systems, Microsoft i RSA Security. PEAP koristi digitalne sertifikate za autentikaciju servera, dok za autentikaciju korisnika PEAP podržava različite EAP-enkapsulirane metode sa zaštitnim TLS tunelom. PEAP podržava tri glavna elementa 802.1X/EAP. Faza 1 autentikacione sekvence, kao što je prikazano na slici 4, je ista kao kod EAP-TLS ("server-side" TLS). Na kraju faze 1 enkriptovani TLS tunel je kreiran između korisnika i RADIUS servera za transport EAP autentikacionih poruka. U fazi 2 RADIUS server autentikuje klijenta kroz enkriptovani TLS tunel ka drugom tipu EAP-a. Na primer, korisnik može biti autentikovan sa OTP korišćenjem EAP-GTC podtipa (PEAP DRAFT). U ovom slučaju RADIUS server se bazira na OTP podacima (korisnički ID i OTP). Kada je ovo završeno EAP-Success poruka se šalje klijentu pa klijent i RADIUS server definišu WEP ključ [10].



Slika 4. – *PEAP Autentikacioni proces*

WLAN diferencijacija korisnika

U žičanim mrežama je često moguće segmentirati korisnike deleći ih u radne grupe. Implementacija ovakvog rešenja se postiže na trećem, tj. mrežnom

sloju. U bežičnoj segmentaciji razlikujemo menadžment i R&D segmente. Ovakva segmentacija obuhvata izgradnju distribuiranih modula, koji čine prvi segment trećeg mrežnog sloja. Drugi način segmentacije bi bio filtriranje IP adresa. Prema IP-u bi odredili kojoj korisničkoj grupi pripada data osoba i prema tome joj davali ili oduzimali pojedina ovlašćenja. Ovakva segmentacija je administrativno kompleksna jer funkcionalna i fizička separacija su često dve potpuno različite stvari. Na primer finansijski kontrolor kome je neophodno omogućiti pristup detaljima finansijskih tokova kompanije može da sedi odmah pored osobe čiji opis posla definiše pristup samo najosnovnijim podacima i servisima. Slično kao i u klasičnim mrežama, deljenje korisnika u bežičnom svetu može da se postigne kreiranjem bežičnih virtuelnih LAN-ova. Korišćenjem više tehnologija u isto vreme (802.1X/EAP i IPsec VPN) pruža nam kreiranje više virtuelnih mreža, pri čemu svaka od njih koristi specifičnu sigurnosnu šemu. Unikatni bežični VLAN-ovi koriste unikatni SSID koji je kreiran po uzoru na žičani VLAN ID. Ako se vratimo primeru finansijskog kontrolora i običnog korisnika primećujemo da ovakvom tehnologijom njima dodeljujemo različite SSID, pri čemu je svaka identifikacija kreirana po istoj šemi kao i žičani unikatni VLAN ID. Ovaj mehanizam može da se implementira korišćenjem RADIUS servera. Na primer AP može dinamički da mapira finansijskog kontrolora prema VLAN ID prosleđujući RADIUS serveru uspešnu 802.1X/EAP autentikaciju. Takođe predstavljanje VLAN-ova AP-u omogućava kompanijama deljenje AP menadžment saobraćaja od protoka informacija korisnika. Uvođenje ovakvog rešenja ne samo da se preporučuje nego i odsustvo implementacije virtuelnih mreža dovodi do pojave sigurnosnih rupa [11].

5. ZAKLJUČAK

Praksa je pokazala da dosadašnja rešenja ne mogu da obezbede visok nivo zaštite u bežičnoj mreži. Zbog toga se ne savetuje korišćenje ovih metoda zaštite u sistemima kod kojih je neophodan visok nivo zaštite. Kao potencijalna grupa koja bi se mogla zadovoljiti ovim modelom bi bila mala organizacija ili kompanija koja u svojoj mreži ne koristi poverljive podatke. Sve druge kompanije bi trebale investirati u naprednije sisteme zaštite.

Preporuka za kompanije u kreiranju svojih mreža je da koriste IPsec ili 802.1X/EAP sa TKIP ili Cisco TKIP, ali generalno gledano ne oba sistema istovremeno. Specifični dizajn u kome su iskorišćena oba sistema zaštite je testiran u Cisco-vim laboratorijama. Ukoliko se od mreže zahteva najviši nivo sigurnosti trebalo bi koristiti IPsec ali pri tome je potrebno znati da je implementacija IPsec-a mnogo kompleksnija od 802.1X/EAP sa TKIP. Međutim, za većinu mreža sigurnost koju pruža 802.1X/EAP sa TKIP je sasvim dovoljna.

U određenim stručnim krugovima postoji i znatno drugačije mišljenje. “The National Science Foundation“ je nosilac inicijative koja bi trebala doneti potpuno novu arhitekturu Interneta sa već ugrađenim sigurnosnim sistemima i podrškom za bežične komunikacije - ”The Global Environment for Networking Investigations” (GENI). Ovaj podatak je objavljen u Filadelfiji na konferenciji ”Special Interest Group on Data Communication” krajem avgusta 2005. godine. Dizajneri mreža, među kojima je i Guru Parulkar sa MIT-a, smatraju da će se izgradnjom nove mreže rešiti trenutni problemi sigurnosti.

LITERATURA

[1.] LXE Inc. (EMS Technology); *RF/Wireless Basics, An Intro to Wireless Data Collection Networks, Products, Standards and Solutions*; ZDNet; September 2003

[2.] David W. Johnson, Harold Koch; *Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?;* Proceedings of the 39th Hawaii International Conference on System Sciences; 2006

[3.] CERT; *Analiza Snnifing Alata i Zaštite*; Novembar 2001,

[4.] Frank Kargl, Stefan Schlott, Michael Weber; *Identification in Ad hoc Networks*; Proceedings of the 39th Hawaii International Conference on System Sciences; 2006

[5.] Kathy Keenan; *What Hackers Don’t Want You to Know About Your WLAN*; AirMagnet, Inc. ; Novembar 2004

[6.] LXE Inc. (EMS Technology); What You Need to Know Before Purchasing A Rugged Mobile Computer; TheServerSide.NET, Oktobar 2004

[7.] Nikita Borisov, Ian Goldberg, and David Wagner; *Security of the WEP algorithm*; 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, July 16-21, 2001

[8.] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan; *Your 802.11 Wireless Network has No Clothes*; March 30, 2001

[9.] LXE Inc. (EMS Technology); *Wireless Security - The New ‘Keeping the Bad Guys Out of Your 802.11*; Wireless Network-2004 Edition; Mart 2004

[10.] Sean Convery, Darrin Miller and Sri Sundaralingam; Cisco SAFE: *Wireless LAN Security in Depth - version 2*; SAFE Blueprint - Cisco Systems; 2003

[11.] Sean Convery, Darrin Miller, and Sri Sundaralingam; *Wireless Virtual LAN Deployment Guide*; SAFE Blueprint - Cisco Systems; 2003

Dr Dejan Simić, FON
Oblast interesovanja: primena informacionih tehnologija, zaštita podataka i računarskih sistema

Siniša Kuprešak, Fakultet za fizičku hemiju
Oblast interesovanja: Bežične mreže, Sistemi plaćanja na Internetu

CIP - Katalogizacija u publikaciji Народна библиотека Србије, Београд 659.25
INFO M: časopis za informacionu tehnologiju i multimedijalne sisteme = journal of information technology and multimedia systems / glavni i odgovorni urednik Dragana Bečejski Vujaklija. - štampano izd. -
God. 1,br. 1 (2002) -.- Stara Pazova: Savremena poslovna obrada - SAVPO,2002 - (Stara Pazova: SAVPO).- 30 cm
Postoji i izdanje na CD ROMu: INFO M = ISSN 1451-4435. - Nastavak publikacije: Info Science = ISSN 1450-6254.
- Tromesečno ISSN 1451-4397 = INFO M (Štampano izd.) COBISS.SR-ID 105690636