Vanja M. Korać
Matematički institut SANU
vanja@mi.sanu.ac.rs

UDK 004.7.056.5 ; 004.056 ; 621.39:004.7
Izvorni naučni članak

UPUTSTVO ZA POVEĆANJE SIGURNOSTI BEŽIČNIH MREŽA - IMPLEMENTACIJA

APSTRAKT

U ovom tekstu će biti prikazano uputstvo za konfigurisanje bežičnih mrežnih uređaja koji ima za cilj da poveća nivo bezbednosti bežične komunikacije u okviru bežične mreže. Takođe, biće objašnjeni i potrebni bezbednosni parametri, da bi se ostvario što viši nivo sigurnosti u okviru bežične mreže. Takođe, u radu je istaknuta lista odgovarajućih mera opreza koju je potrebno uključiti u implementaciju. Svrha ovog dokumenta je da se realizuje što veća bezbednost u bežičnoj mreži kako u kućnom tako i u poslovnom okruženju u okviru manjih organizacija.

Key words: Bežične mreže, Zaštita, Bežični protokoli, WEP, WPA, WPA-PSK, WPA-Enterprise, WPA2, WPA2-PSK, WPA2-Enterprise, Implementacija bezbednosti, SSID, Filtriranje MAC adresa

UVOD

Zahvaljujući svojoj mobilnosti, fleksibilnosti u odnosu na fiksne „LAN" mreže i jednostavnosti implementacije, bežične mreže postaju sve popularnije i sve prisutnije. Međutim, upravo zbog svoje popularnosti i rasta broja njihovih korisnika postavljaj se veliki broj pitanja u pogledu sigurnosti bežičnih mreža i njihovog upravljanja, i traže se što adekvatniji odgovori. S obzirom da bežične mreže predstavljaju komunikaciju koja se odvija kroz zajednički, deljeni medijum prenosa, postoji opasnost od presretanja poslatih i primljenih podataka. Upravo zbog tih svojih osobina, bežične mreže su podložnije spoljnim upadima zbog toga što je nemoguće signal ograničiti samo na lokaciju gde je fizički smeštena organizacija ili kuća vlasnika.

Iako bežične mreže poseduju razne sigurnosne elemente, iznenađujući je podatak da se u velikom broju organizacija kao i u kućnom okruženju, ne koristi nijedna vrsta mehanizama zaštite kojim bi se osigurao dovoljan nivo bezbednosti.

Pre nego što se donese odluka o uvođenju bežične mreže potrebno je identifikovati potencijalne ranjivosti i sigurnosne pretnje koje će bežična mreža da unese u postojeće okruženje. Pravac razmišljanja je uglavnom o implikacijama koje se odnose na sigurnost i upravljanje. Nakon toga se pravi procena rizika i analiza zaštitnih mera. To ima za cilj da se utvrdi da li troškovi i opasnosti, za definisani nivo zaštite, prevazilaze prednosti koje bežični „LAN" donosi. Nakon toga sledi implementacija definisanog nivoa bezbednosti. Poslednji korak je uspostavljanje bežične mreže. Poseban osvrt biće upravo na implementaciji bez-

bednosnih elemenata, kako u kućnom, tako i u poslovnom okruženju u okviru manjih organizacija.

OSVRT NA OSNOVNE ELEMENTE IMPLEMENTACIJE

Ovaj odeljak daje pregled osnovnih elemenata za početak implementacije sigurnosti. Obrazac koji se koristi u implementaciji za primenu osnovne sigurnosti biće predstavljen koracima koji slede dalje u tekstu.

Povezivanje Access Point ili Wireless router-a sa računarom

Postupak je jednostavan, koristi se mrežni kabl (RJ-45) koji se priključi u bilo koji otvoreni port na Access Point-u ili Wireless router-u, osim onog koji je označen za „WAN" mreže. Drugi kraj kabla se povezuje sa mrežnom karticom računara.

Povezivanje sa Access Point-om ili Wireless router-om putem Web interfejsa

Da bi se pristupilo Web interfejsu koji služi za komunikaciju sa Access Point-om ili Wireless router-om, koristi se jedan od internet pretraživača (Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera itd.), tako što se u Web address bar-u unese default-na adresa Access Point-a ili Wireless router-a. Default-na IP adresa je na većini Wireless uređaja 192.168.1.1, ali se razlikuje kod nekih proizvođača i ona je navedena u korisničkom uputstvu. Nakon unosa odgovarajuće IP adrese u Web address bar pritisne se „Enter" (slika 1)

Slika 1. Adresno polje Web pretraživača

Logovanje na Access Point ili Wireless router i promena lozinke

Kada se veza sa uređajem uspostavi, na ekranu će se pojaviti strana za prijavljivanje na uređaj („Login screen"). Za logovanje na Access Point ili Wireless router, uglavnom se koristi

Slika 2. Interfejs za logovanje na bežični uređaj

korisničko ime „Admin" a lozinka je ili prazna ili „admin" [slika 2.]. Naravno, može se razlikovati od proizvođača do prozvođača, ali je dokumentovana u korisničkom uputstvu.

Prvo, što je potrebno uraditi kada se pristupi uređaju, je da se promeni default-na lozinka za pristup Access Point-u ili Wireless router-u. Mesto gde se nalazi stranica za promenu default-ne lozinke, razlikuje se od proizvođača do proizvođača, na primer:

- Proizvođač D-link postavlja promenu lozinke na „Tools" stranu
- Proizvođač Linksys postavlja promenu lozinke na „Administration" stranu
- Proizvođač Netgear spotavlja promenu lozinke na „Maintenance" stranu
- Proizvođač TP-Link postavlja promenu lozinke na „System tools" stranu

Kada pronađemo traženu stranu za izmenu lozinke, potrebno je da se unese nova lozinka. Preporuka je da se ne koriste kratke lozinke, već je potrebno da ona sadži najmanje 8 karaktera (koja podrazumeva kombinaciju velikih i malih slova, brojeva i znakova). Izbor lozinke sa višim stepenom složenosti takođe će pomoći jačanju bezbednosti, kako samog mrežnog uređaja tako i bežične mreže koju taj uređaj realizuje. Na primer, lozinka „1234" se vrlo lako može probiti, u odnosu na složenije lozinke kao na primer „Nesalom1vo$t" Posle promene lozinke, sačuvati podešavanja pritiskom na „Save Settings" ili „Update" dugme. Time je sačuvana nova lozinka. Posle toga će biti zatraženo ponovno prijavljivanje, koristeći novu lozinku. Ova lozinka će se koristiti svaki put za prijavljivanje na bežični uređaj da bi se na njemu promenila određena podešavanja. Dodatni savet bi bio da se lozinka Acess Point-a ili Wireless router-a češće menja.

Promena naziva Identifikatora mreže tj. SSID-a

Veoma je važno da se promeni naziv SSID-a. Identifikator mreže SSID (Service Set Identifier) predstavlja kod koji postaje vezan za svaki podatak (ili „paket") i služi da identifikuje informacije koje se šalju i primaju.

Svi bežični uređaji koji pokušavaju međusobno da komuniciraju moraju deliti isti SSID.

Svaki Access Point ili Wireless router uređaj nekoliko puta u sekundi emituje tzv. Beacon frame (koji sadrži SSID, vreme, mogućnosti, podržane brzine prenosa...) koji služi za sinhronizovanje bežične mreže. Kada se na računaru prikazuju bežične mreže koje su dostupne za vezu, ime svake bežične mreže je prikazano vrednošću koju sadrži parametar SSID. Ako se ostavi vrednost u SSID, kao default-na postavka, u tom slučaju drugi korisnici mogu da znaju koji tip Access Point-a ili Wireless router-a koristite, čime se uređaj postavlja u nepovoljan položaj sa aspekta bezbednosti. Promena SSID-a se radi na sledeći način:

Nakon logovanja na Web interfejs-u koji služi za komunikaciju sa Access Point-om ili Wireless router-om, odabere se stranica „Wireless" koja se nalazi na vrhu ekrana i upiše se odgovarajuće ime za SSID, u ponuđeno polje (slika 3). Mora se napomenuti da je SSID „case-sensitive" tj. razlikuje velika i mala slova i može sadržati do 32 slovna znaka. Nakon unosa potvrditi sa „Primeni" i time je dodela imena SSID završena. Ovo podešavanje je tipično za većinu modela Access Point-a ili Wireless router-a.

Postoji još jedna metoda koja ima za cilj da poveća osnovnu sigurnost, a to podrazumeva isključivanje emitovanja SSID-a na Access Point-u ili Wireless router-u. Ovo se može uraditi tako što se ukloni potvrda pored „Wireless SSID Broadcast" (emitovanje SSID). Time se omogućava „nevidljivost" bežične mreže od strane drugih bežičnih korisnika, ali to ne znači da je nju nemoguće pronaći. Isključivanjem emitovanja SSID-a, Access Point ili Wireless router neće emitovati SSID, ali klijent koji se spaja hoće, jer svaki „association request" (zahtev za pridruživanjem) nosi u sebi SSID. Ako se zaustavi emitovanje SSID bežične mreže, onda se mora za svaki računar ručno podešavati konekcija ka našem bežičnom uređaju uz odgovarajući SSID, jer se naša mreža neće pojaviti u standardnom „wireless network discovery" čarobnjaku koji dolazi sa Microsoft Windows operativnim sitemom.[1]

Slika 3. Strana za podešavanje imena SSID

Upotreba statičkog IP adresiranja

Većina današnjih sistema koriste DHCP (eng. The Dynamic Host Configuration Protocol) servere za dinamičko dodeljivanje IP adresa računarima čim se spoje na mrežu. Iako ovakav način adresiranja umnogome olakšava posao IT administratorima, kao i korisnicima, sa druge strane olakšava upad i neautoriziranim korisnicima, čime se sigurnost sistema može dodatno ugroziti. Isključivanjem funkcije DHCP servera na Wireless router-u, i ručnim podešavanjem IP adresa, opasnost od upada se može smanjiti.[2] Prednost upotrebe statičkog IP adresiranja je ta, što može da spreči neke ARP napade, ali mana je što će se stvoriti mnogo dodatnog posla administratorima i nije baš primenjivo u okruženjima gde korisnici većinom koriste prenosne (lap-top) računare.

1 Samo isključivanje slanja imena SSID na sve uređaje je svakako slaba zaštita bežičnih mreža i ne osigurava ni približno dovoljnu sigurnost. Ukoliko se ostavi emitovanje imena SSID u mreži (što može biti značajno u poslovnoj mreži), obavezno promeniti default-no ime, jer ukoliko se to ne uradi, šalje se signal napadačima da se nisu preduzele ni ostale zaštitne mere. U tom slučaju primeniti, ukoliko AP ili Wireless router podržava, SSID Client Isolation opciju. Ovom opcijom se zabranjuje bežičnim klijentima njihova međusobna komunikacija, iako su u istom subnet-u čime se sprečava njihovo zaobilaženje firewall-a. U kućnim uslovima preporučuje se da se isključi emitovanje SSID-a na AP ili Wireless router-u, jer nema potrebe da se svima emituje postojanje bežične mreže. Time smo na neki način smanjili vidljivost prema potencijalnim napadačima.

Posle svega navedenog, jasno je da je potrebno osim implementacije osnovne bezbednosti primeniti i odgovarajuće naprednije tehnike zaštite koje će biti razmatrane u narednim poglavljima.

2 Hlušička 2007

Onemogućiti automatsko povezivanje sa Wlan-om

Na velikom broju računara dopušteno je automatsko spajanje na bilo koju otvorenu Wifi mrežu bez ikakvog obaveštenja. Ova postavka nije po default-u, međutim mnogi pojedinci to koriste jer im je lakše i brže spajanje na bežične mreže. Nažalost ovakva postavka predstavlja veliki sigurnosni propust.[3] Da bi se to sprečilo potrebno je sprovesti sledeće korake :

1. Na Windows računaru otići na „Start-Settings-Control Panel-Network Connections".
2. Selektovati „Wireless Network Connections", primeniti na njega desni klik i odabrati „Properties".
3. Odabrati "Wireless Networks" tab.
4. Ako opcija „Use Windows to configure my wireless network settings" nije čekirana, onda se za bežičnu konekciju koristi neki „third-party connection software". U tom slučaju konsultovati dokumentaciju proizvođača kako i na koji način se onemogućuje „Automatic Wireless connections". Ako je „Use Windows to configure my wireless network settings" čekirana, preći na sledeći korak.
5. Pod opcijama „Preferred networks" i „Advanced" otčekirati "Automatically connect to non-preferred networks".

Na ovaj način se utiče na zaštitu bežičnog klijenta sprečavajući mogućnost kompromitacije njegovog računara, a to sa druge strane doprinosi da taj računar neće kompromitovati bežičnu mrežu organizacije u kojoj implementiramo zaštitne mehanizme.

Kontrola RF signala

Sve dok je Wireless mreža u funkciji ona odašilje RF (Radio frequency) signale. Oni prenose podatke između AP ili Wireless router –a i ostalih bežičnih klijenata. Ovde postoje dva problema. Prvi problem su poteškoće pri održavanju signala zbog prepreka i smetnji tzv. problem interferencije, a drugi problem, kod bežičnog signala, je taj što se on odašilja i van predviđenog mesta.

Na stvaranje prvog problema utiču određeni materijali (noseći armaturni zidovi, metalne površine, električne instalacije) sprečavajući prolaz signala. Kao rezultat toga javljaju se poteškoće u održavanju WLAN signala. Sve 802.11 komunikacije (802.11a pre svega) su osetljive na ove prepreke. Savet je, da se bežični uređaj nikad ne pozicionira pored mikrotalasnih uređaja na minimum 3 metra. Drugi česti izvori smetnji su upravo bežični uređaji koji rade na frekvenciji 2,4 GHz npr. bežični telefoni, monitori, otvarači za garažna vrata itd…

Ukoliko dođe do inerferencije signala preporuka je da se na AP ili Wireless rotuter-u promeni kanal. Može se izabrati bilo koji kanal od 1-11 videti u tabeli [tabela 1.]. Koristeći različite kanale neće se uvek rešiti problem, ali se mogu eliminisati unakrsne Wlan smetnje. U nastavku je data tabela sa frekvencijama kanala:

Drugi problem se još naziva i „curenje" mreže, koji omogućava potencijalnim napadačima da pronađu bežičnu mrežu i koriste je bez znanja vlasnika. Preporuka je, da se ruter postavi u sredinu objekta, a ne u blizini prozora i vrata.

Savremeni Wireless router-i imaju mogućnost kontrole jačine signala koji on emituje. Uglavnom se kod većine proizvođača nalazi pod opcijom Transmit power (Lowest, Low, Medium, High, Highest). Na nekim AP ili Wireless routerima postoji opcija i uključivanja i isključivanja neke od antena (leve ili desne ili središnje) koje postoje na samom uređaju (opcija „Antenna selection"). Navedene opcije su vrlo korisne jer možemo da eliminišemo „višak" signala tj. da ga maksimalno iskontrolišemo, a „curenje" signala da svedemo na minimum, odnosno da ga pojačamo tamo gde se signal gubi.

Isključivanje AP ili Wireless router-a prilikom duže odsutnosti

Razlog isključivanja uređaja je taj što time ni mreža ne može biti zloupotrebljena. Ukoliko se planira duža odsutnost ili nekorišćenje mreže jedno vreme, preporuka je da se Wireless uređaj isključi. Ovakav način zaštite nije idealan, ali je izuzetno efikasan kada nema prisutnih osoba u blizini wireless uređaja koji mogu da zaštite mrežu od potencijalnog napada.[4]

3 Kremer 2009

4 Mitrović 2009

Operativni kanali	• IEEE 802.11b compliant • 11 kanala (US, Canada) • 13 kanala (ETSI) 14 kanala (Japan)				
Tabela Kanala sa frekvencijama					
Kanal	**Frekvencija (MHz)**	**USA**	**Canada**	**ETSI**	**Japan**
1	2412	+	+	+	+
2	2417	+	+	+	+
3	2422	+	+	+	+
4	2427	+	+	+	+
5	2432	+	+	+	+
6	2437	+	+	+	+
7	2442	+	+	+	+
8	2447	+	+	+	+
9	2452	+	+	+	+
10	2457	+	+	+	+
11	2465	+	+	+	+
12	2467			+	+
13	2472			+	+
14	2484				+

Tabela 1. Operativni kanali i njihove radne frekvencije

Primena bezbednosnih opcija

Jedan od nabitnijih koraka bezbednosne implementacije u bežičnoj mreži, podrazumeva primenu bezbednosnih opcija.

Ovaj korak podrazumeva upotrebu najbezbednijeg protokola zaštite koju podržava uređaj potreban za realizaciju bežične mreže. Najčešći protokoli koji su danas prisutni u bežičnim mrežnim uređajima su sledeći: WEP (eng. Wired Equivalent Privacy) (koji je prevaziđen ali je još uvek prisutan), WPA (eng. Wi-Fi Protected Access), WPA2. Svakako povećanju bezbednosti mogu doprineti i sigurnosne funkcije samog bežičnog uređaja, kao npr. filtriranje MAC adresa.

Više o njima i njihovoj implementacji biće u narednom poglavlju koji se bavi elementima implementacije veće bezbednosti.

ELEMENTI ZA OKVIR IMPLEMENTACIJE VEĆE BEZBEDNOSTI

Postoje različite bezbednosne opcije u bežičnim mrežama koje su podržane u većini bežičnih AP i Wireless router-a koje dodatno podižu nivo zaštite: WEP, WPA-PSK, WPA-Enterprise, WPA2-PSK, WPA2-Enterprise kao i filtriranje MAC adresa.

WEP zaštita

Ovaj postupak podrazumeva upotrebu WEP zaštitnog mehanizma. WEP je skraćenica od „Wired Equivalent Privacy", predstavlja sigurnosni protokol bežičnih mreža, a utvrđen je standardom 802.11b. Od WEP protokola se očekivao nivo sigurnosti jednak onom kod tradicionalnih žičnih lokalnih mreža. WEP deluje na dva donja sloja OSI modela – na fizičkom (eng. physical) i na sloju veze (eng. data link layer) i bazira se na enkripciji podataka između krajnjih tačaka.[5] WEP koristi ključeve standardnih dužina 64, 128- i 256 bita (uključujući inicijalni vektor od 24 bita). Što je ključ duži teže ga je probiti, ali to utiče dodatno na brzinu prenosa podataka, jer je računarima potrebno više vremena kako bi dešifrovali podatke koji se prenose. Za šifrovanje se koristi RC4 sistem zaštite i CRC-32 za proveru integriteta podataka.

Nakon logovanja na Web interfejs koji služi za komunikaciju sa Access Point-om ili Wireless router-om, odabere se stranica „Wireless", zatim se odabere „Wireless Security" (važi za većinu Wireless Access Point / Wireless router modela)[6]. Zatim se postavi „Security mode" na

5 Hlušička 2007

6 Linksys by Cisco 2009

„WEP encryption". Dalje sledi da se izabere dužina ključa iz padajuće liste pod „WEP Key". Ključevi se mogu postaviti na dva načina. Prvi je, da se u polju „Passphrase" unese neka vrednost koja će služiti da se automatski izgenerišu ključevi. Kada se pritisne na dugme „Generate" dobićemo izgenerisane ključeve u HEX formatu (koriste se samo slova od A-F i brojevi od 0-9). Ti izgenerisani ključevi se ručno unose za svaki računar koji se povezuje na bežičnu mrežu koju realizujemo. Drugi način je, da sami unosimo vrednosti ključeva u HEX formatu. Kod nekih proizvođača postoji unošenje vrednosti ključeva i u ASCII formatu pod opcijom „Wep Key format". Videti sliku 4.

Slika 4. Strana za podešavanje protokola WEP

Metodi autentifikacije koje se mogu primeniti kod WEP-a su sledeći:

„Open system authentication" i „Shared key authentication".

Kada je reč o „Open system authentication" WLAN klijent ne daje svoje podatke AP ili Wireless router-u prilikom autentifikacije. Svaki klijent bez obzira na njegov WEP ključ može autentikovati sam sebe sa AP ili Wireless router-om, i onda pokušati pridružiti se. Nakon autentifikacije i konektovanja WEP se može koristiti za šifrovanje okvira podataka. U ovom trenutku klijent mora imati pravi ključ.

Kada je reč o „Shared key" autentifikaciji, WEP se koristi za autentifikaciju koja podrazumeva četvorosmerni "challenge response handshake":

1. Klijent šalje zahtev za autentifikaciju prema AP ili Wireless router-u
2. AP ili Wireless router vraća „clear-text challenge" poruku
3. Klijent šifruje „clear-text challenge poruku" koristeći konfigurisani WEP ključ i šalje natrag u drugom autentifikacijskom zahtevu.
4. AP ili Wireless router dešifruje materijal i upoređuje ga sa clear-tekstom koji je poslao. U zavisnosti od ove provere AP ili Wireless router šalje pozitivan ili negativan odgovor. Posle autentifikacije i pridruživanje WEP se koristi za šifrovanje okvira podataka.

Iako je na prvi pogled „Shared key" autentifikacija više sigurna, praksa je pokazala da nije tako. Moguće je stvoriti statički WEP ključ, hvatanjem sva 4 „handshake" okvira u „Shared key" autentifikaciji.[7] Preporuka je da se koristi „Open system" autentifikacija za WEP autentifikaciju.

Nakon logovanja na Web interfejs koji služi za komunikaciju sa Access Point-om ili Wireless router-om, odabere se stranica „Wireless", zatim se odabere „Advanced wireless Security" (važi za većinu Wireless Access Point / Wireless router modela)[8].

Zatim se postavi "Authentication Type" na „Open system". WEP se više ne preporučuje kao zaštita u bežičnim mrežama. Pokazalo se da WEP ne nudi dovoljnu sigurnost. 2001. godine uočene su ranjivosti WEP algoritma. 2004. godine dolazi do zamene WEP-a novim WPA algoritmom. 2005. godine FBI tim je imao demonstraciju kako se korišćenjem programa dostupnog na Internetu može probiti WEP enkripcija za manje od 3 minute. Za probijanje dužih ključeva zahteva se više presretnutih paketa da bi se otkrio ključ. Postoje i naprednije varijante WEP protokola:[9]

WEP2 (povećana je vrednost inicijalnog vektora, primenjena je 128-bitna enkripcija),

WEPplus (ili WEP+, u vlasništvu je Agere Systems, učinak je povećan samo ako se koristi na oba kraja veze, što u većini slučajeva nije lako ostvarivo),

Dynamic WEP (menja WEP ključeve dinamički, koristi se samo kod nekih proizvođača mrežne opreme, na primer kod 3Com-a),

WEP cloaking (vlasništvo Air Defense-a, uklanja nedostatke WEP enkripcije slanjem simuliranog prometa koji onemogućuje korišćenje alata za dekripciju bilo pri pasivnim ili aktivnim napadima).

Iako je preporuka izbegavati korišćenje WEP zaštite, bolje je koristiti bar neku nego uop-

7 Kremer 2009

8 Linksys by Cisco 2009

9 Hlušička 2007

šte ne koristiti zaštitu. Ovo se najviše odnosi na starije bežične rutere koji podržavaju samo WEP enkripciju. Na takvom bežičnom uređaju je svakako potrebno podesiti najveću moguću dužinu ključa. Postoji nekoliko načina da se iz WEP-a izvuče maksimum:

1. Redovno menjanje WEP ključa
2. Korišćenje najbolje metode šifrovanja koju uređaj podržava
3. Korišćenje metode za autentifikaciju koju uređaj podržava

Postoje drugi protokoli za bežičnu sigurnost koji su mnogo bezbedniji od WEP-a. Tu spadaju WPA (WiFi Protected Access) i WPA2. Njih je daleko bolje koristiti nego WEP, (u daljem tekstu biće razmatrana njihova implementacija). WEP koristiti samo ukoliko nisu podržani napredniji protokoli zaštite u okviru samog uređaja. Preporuka je da se, uradi upgrade firmware-a ukoliko to AP ili Wireless uređaj podržava, čime može da se omogući primena bar WPA zaštite na njemu.

WPA ZAŠTITA

WPA ili „WiFi Protected Access", predstavlja noviji standard za WiFi sigurnost. Ovaj sistem zaštite predstavlja sastavni deo 802.11i standarda. Nastao je kao odgovor na nedostatke WEP standarda i ima za cilj uspostavljanje sigurnih bežičnih mreža usled poboljšanih mehanizama autentifikacije korisnika i šifrovanja podataka.

Podaci se šifruju RC4 sistemom sa 128-bitnim ključem i 48-bitnim inicijalnim vektorom. Ključna prednost nad WEP standardom je korišćenje protokola TKIP (eng. Temporal Key Integrity Protocol). Njegova glavna odlika je ta što dinamički menja ključeve za vreme prenošenja paketa podataka, tako da svaki paket koji se pošalje ima svoj jedinstveni šifarski ključ u kombinaciji sa proverom integriteta poruke. Zbog TKIP protokola i velikog inicijalnog vektora, sistem se može uspešno odbraniti od napada kakvi se koriste za otkrivanje ključa pri WEP zaštiti.

U odnosu na WEP, WPA protokol dominira i na polju provere integriteta podataka. Naime, WEP protokol koristi CRC (eng. Cyclic Redudandy Check) za proveru integriteta podataka, kod koga potencijalni napadač može izmeniti sastav poruke koja se šalje i vratiti vrednost CRC na originalnu, čak bez poznavanja ključa. WPA koristi sigurniji način za proveru integriteta korišćenjem „koda za autentifikaciju poruke" (eng. Message Authentication Code, skraćeno MAC), tj. „koda za integritet poruke" (Message Integrity Code – MIC) poznatijeg kao „Michael" koji u WPA uključuje brojač frame-ova čime se isključuje mogućnost promene sastava poruka u komunikacionom kanalu.[10] Još jedna pozitivna osobina je ta što WPA ima u sebi ugrađenu zaštitu u vidu specijalnog mehanizma koji sprečava pristup potencijalnom napadaču ako sistem primeti pokušaj probijanja TKIP protokola. Mana mu je ta što koristi relativno star sistem šifrovanja RC4 pa je to jedan od glavnih propusta. Ova mana se otklanja korišćenjem WPA2 protokola koji ima napredniji način šifrovanja. WPA je potrebno implementirati u uređajima koji ga podržavaju kao maksimalni nivo sigurnosti tj. ukoliko ne postoji WPA2 mehanizam zaštite na njima.

WPA protokol može raditi u 2 režima : Enterprise i PSK (Pre-Shared Key).

Ono što razlikuje ova dva režima rada WPA je način na koji oni vrše autentifikaciju i distribuciju ključeva. Naime, kada je reč o Enterprise režimu rada podrazumeva se prisutnost posebnog servera za autentifikaciju koji koristi RADIUS (eng. Remote Authentication Dial-In User Service) protokol. Ovo je jako dobro sa stanovišta bezbednosti, jer postoji mogućnost centralizacije ključeva, ali zahteva dodatnu investiciju - RADIUS server. Pre-shared key ne zahteva poseban server za autentifikaciju jer koristi tajni ključ kojeg odredi administrator bežične mreže. Lozinka za pristup mreži mora biti duža od 8, a kraća od 64 ASCII znaka.

Treba voditi računa i tome da je računare potrebno ažurirati (engl. Update) da bi mogli da podržavaju WPA/WPA2. To se rešava instaliranjem Service pack-a 2 za Windows XP. Takođe, preporuka je da se bežični klijenti, AP i Wireless router-i redovno ažuriraju najnovijim drajverima tj. firmware-rima.

10 Hlušička 2007

Slika 5. Strana za podešavanje WPA-PSK parametara

Primena WPA Personal (WPA-PSK)

Da bi se koristio WPA-PSK postavlja se statični ključ ili „passphrase", kao i za WEP, ali se koristi TKIP protokol. WPA-PSK automatski menja ključeve za šifrovanje prema definisanom vremenskom intervalu.

Izabere se WPA-Personal sa TKIP šifrovanjem (videti sliku 5.), unese se lozinka u polje Passphrase od 8-63 karaktera, i unese se vremenski interval za obnovu ključeva.[11] Vrednost se kreće između 0 i 99.999 sekundi, što daje instrukcije AP ili Wireless router-u koliko često treba promeniti ključeve za šifrovanje. Duži i složeniji „Passphrase" tj. lozinka obezbeđuje veću sigurnost bežične mreže.

Primena WPA Enterprise

Primena ovog rešenja je preporučljiva kod srednjih i većih poslovnih okruženja.

WPA se koristi u kordinaciji sa RADIUS serverom. (Ovaj sistem se koristi samo kada je RADIUS server povezan sa ruterom). U tom slučaju mehanizam autentifikacije je prepušten RADUIS serveru. Ovim se omogućava korisnicima da svoj identitet potvrde preko RADIUS servera sa njihovim korisničkim imenom i lozinkom ili sertifikatom.

Izabere se „Security mode" WPA-Enterprise (videti sliku 6). Zatim se unese IP adresa RADIUS servera i broj porta „1812", i upisuje se ključ koji se deli između AP ili Wireless uređaja i RADIUS servera. Poslednji parametar se odnosi na obnovu ključeva. Samo podešavanje RADIUS servera prevazilazi okvire ovog rada.

WPA2 zaštita

WPA 2 predstavlja noviju poboljšanu verziju WPA (Wi-Fi Protected Access). Poboljšanje se ogleda u primeni naprednijeg algoritma za šifrovanje u odnosu na WPA. WPA 2 koristi AES-CCMP algoritam. CCMP predstavlja skraćenicu od engleskog „Counter Mode with Cipher Block Chaining Message Authentication Code Protocol", a zasniva se na „naprednom standardu za

11 Linksys by Cisco 2009

Slika 6. Strana za podešavanje WPA-Enterprise parametara

šifrovanje", tj. AES protokolu (eng. Advanced Encryption Standard).[12]

WPA 2 protokol kao i WPA može raditi u 2 režima: Enterprise i PSK (Pre-Shared Key). Razlika se ogleda u načinu na koji oni vrše autentifikaciju i distribuciju ključeva o čemu je već bilo reči u poglavlju koji se bavio WPA.

Potrebno je naglasiti da je računare potrebno ažurirati (Update) da bi mogli da podržavaju WPA2. To se rešava instaliranjem Service pack-a 2 za Windows XP. Takođe, preporuka je i da se bežične klijenti, AP i Wireless router-i redovno ažuriraju najnovijim drajverima tj. firmverima. Patch se nalazi na Microsoft starnici : http://www.microsoft.com/downloads/details.aspx?familyid=662BB74D-E7C1-48D6-95EE-1459234F4483&displaylang=en

Primena WPA2 Personal (WPA-PSK)

WPA2 Personal (WPA-PSK) nam pruža dve metode šifrovanja, TKIP i AES, uz dinamičko šifrovanje ključevima.

Najbolju zaštitu pruža ako se odabere AES (kao na slici 7). U opcijama postoji i mogućnost korišćenja TKIP + AES, što ustvari znači da će se koristiti AES za šifrovanje, ali ukoliko bežični klijent ne podržava AES, biće korišćen TKIP.

Potrebno je još definisati lozinku „WPA shared key" od 8-63 karaktera.[13] Zatim se definiše period obnove ključeva čija je default-na vrednost 60 minuta (videti sliku 7)

Primena WPA2 Enterprise

Primena WPA2 Enterprise rešenja se preporučuje kod srednjih i većih poslovnih okruženja.

WPA2 se koristi u kordinaciji sa RADIUS serverom. (Ovaj sistem se koristi samo kada je RADIUS server povezan sa ruterom). U tom slučaju mehanizam autentifikacije je prepušten RADUIS serveru. Ovim se omogućava korisnicima da svoj identitet potvrde preko RADIUS servera sa njihovim korisničkim imenom i lozinkom ili sertifikatom.

Izabere se „Security mode" (videti sliku

12 Hlušička 2007

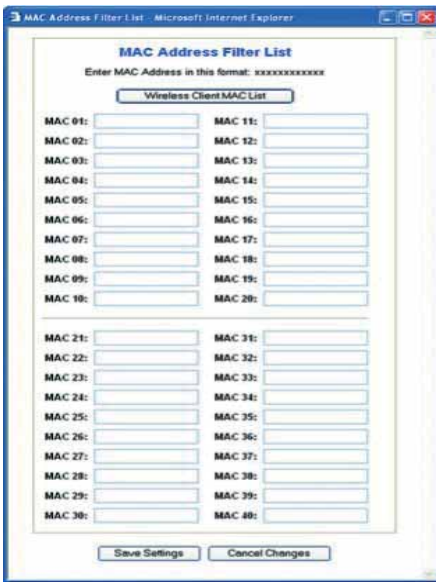
13 Linksys by Cisco 2009

Slika 7. Strana za podešavanje WPA2-PSK parametara

Slika 8. Strana za podešavanje WPA2-Enterprise parametara

8) WPA2-Enterprise. Drugi korak je odabir algoritma koji će se koristiti za šifrovanje. Opcije su AES ili TKIP+AES. Najbolju zaštitu pruža ako se odabere AES (kao na slici). U opcijama postoji i mogućnost korišćenja TKIP + AES, što ustvari znači da će se koristiti AES za šifrovanje, ali ukoliko bežični klijent ne podržava AES, biće korišćen TKIP.

Zatim se unese IP adresa RADIUS servera i broj porta „1812", i upisuje se ključ koji se deli između AP ili Wireless uređaja i RADIUS servera. Poslednji parametar se odnosi na obnovu ključeva, default-na vrednost je 60 minuta. Samo podešavanje RADIUS servera prevazilazi okvire ovog rada.



Slika 9. Lista za unos MAC adresa

Primena filtriranja MAC adresa

Noviji Wireless AP i Wireless ruter-i imaju dodatnu bezbednosnu funkciju koja se zove filtriranje MAC adresa (Media Access Control). MAC adresa je jedinstvena fizička adresa uređaja zapisana u njegovoj memoriji da bi se razlikovao jedan NIC (Network Interface Card) od drugog. Da bismo implementirali veću bezbednost u našu bežičnu mrežu potrebno je koristiti ovu funkciju. Ova funkcija omogućava registrovanje naših bežičnih uređaja našem AP ili Wireless router-u, a odbija komunikaciju onih uređaja koji nisu na listi pristupa AP ili Wireless router-u. Filtriranje MAC adresa, u kombinaciji sa dobrom enkripcijom pruža veoma dobru zaštitu.

MAC tehnologija omogućava jedinstvenu identifikaciju i kontrolu pristupa za računare povezane na IP (Internet Protocol) mreže. U bežičnom umrežavanju, MAC predstavlja radio kontrolni protokol za bežični mrežni adapter.

Svakom IP mrežnom adapteru se dodeljuje jedinstveni broj od strane proizvođača i on se naziva MAC adresa. MAC adresa je dužine 48 bita. Obično se zapisuje kao niz od 12 cifara heksadecimalno kao što je prikazano primerom:

48-3F-0A-91-00-BC

MAC adrese se još zovu i fizičke adrese.

Prvih šest cifara, u heksadecimalnom zapisu adrese, predstavljaju jedinstveni identifikator proizvođača, a poslednjih šest cifara predstavljaju serijski broj uređaja. Ova funkcija je obično po default-u isključena od strane proizvođača. Da bi se poboljšala bezbednost AP ili Wireless router-a preporuka je da se obezbedi filtriranje MAC adresa. Bez filtriranja MAC adresa, svaki bežični klijent može da se priključi (da se autentifikuje) bežičnoj mreži, ako se poznaju neki parametri mreže kao što je SSID, i neki drugi bezbednosni parametri kao što su ključevi za šifrovanje. Da bi se podesilo filtriranje MAC adresa, prvo se mora konfigurisati lista klijenata kojima će biti dozvoljeno da se priključe na mrežu (videti sliku 9), a zatim omogućiti (Enable) filtriranje MAC adresa (videti sliku 10). Kada je implementirano filtriranje MAC adresa, bežični uređaj vrši proveru parametara tako što ako pronađe MAC adresu uređaja na listi dopustiće konekciju, ako ne konekcija će biti odbijena. Što se više sigurnosnih provera implementira, smanjuje se mogućnost mrežnih upada. Da bi sve ovo funk-

Slika 10. Strana za podešavanje MAC filtriranja

cionisalo potrebni su odgovarajući koraci.

Administrator mreže mora imati listu MAC adresa svih bežičnih uređaja klijenata koji imaju potrebu da budu konektovani na AP ili Wireless router. Ovo se jednostavno realizuje pod Linux i pod Windows OS sa naredbom ifconfig (Linux OS) odnosno Start-run-cmd-ipconfig/all (Windows OS).

Sledeći korak je pristup Web interfejsu koji služi za komunikaciju sa Access Point-om ili Wireless router-om preko adrese uređaja npr. http://192.168.1.1 (default-na pristupna adresa kod većine proizvođača) i odaberemo stranicu "Wireless" i na njoj nađemo stranicu „Wireless MAC filter".

Zatim, dobijene MAC adrese unesemo u naš uređaj preko dugmeta „Wireless Client MAC List"i snimimo promene.

Na kraju unosa se uključi opcija filtriranja opcijom „Enable" Time smo omogućili filtriranje bežičnih korisnika putem MAC adrese.

To znači da kad god AP ili Wireless router primi zahtev za pridruživanje sa WLAN-om, on upoređuje MAC adresu tog klijenta sa listom koja je uneta u AP ili Wireless router. Klijenti sa listi će biti autentfikovani od strane AP ili Wireless router-a, dok oni koji se ne nalaze na listi neće proći autentifikaciju i biće im zabranjen svaki pristup WLAN-u. Nažalost, ni ovaj vid zaštite nije savršen. Problem je što MAC adrese mogu da se menjaju. Nekada su MAC adrese bile dodeljivane hardware-skim rasporedom jumpera, ali danas se uglavnom postavljaju u flash memorije i mogu se menjati sa određenim programima za tu namenu. Filtriranje MAC adresa u kombinaciji sa nekim od navedenih protokola zaštite značajno povećava bezbednost bežične mreže. Preporuka bi bila da se Filtriranje MAC adresa kombinuje sa WPA2 protokolom zaštite ukoliko to bežični uređaj podržava.

Monitoring i analiza logova

Većina AP ili Wireless rotuer-i imaju ugrađenu opciju za logovanje podataka. Za dobijanje što veće sigurnosti potrebno je omogućiti ovu opciju sa „Enable". Time smo omogućili praćenje saobraćaja u našoj bežičnoj mreži. Veoma bitna stvar u zaštiti mreže je i samo proveravanje tih logova mreže (Wireless Access Logs) i to što je moguće češće. Preko monitoringa logova mogu se detektovati nepoznati klijenti konektovani na mrežu i preduzeti koraci u vidu promene ključeva. Ovi logovi nam omogućuju i proveru statusa svih MAC adresa koje su konektovane na mrežu, i time možemo da utvrdimo da li su u pitanju samo poznati uređaju kojima je dozvoljen pristup.

ZAKLJUČAK

Shodno svemu navedenom, sledi spisak sigurnosnih elemenata koje bi trebalo sprovesti u cilju povećanja bezbednosti bežične mreže:

1. Promena pristupne lozinke na AP ili Wireless router uređaju;
2. Promena naziva Identifikator mreže – SSID-a;
3. Isključivanje emitovanja SSID-a (u kućnom okruženju);
4. Periodična promena imena SSID-a;
5. Onemogućavanje automatskog povezivanja bežičnih klijenata sa Wlan-om;
6. Regulisanje RF signala – sprečavanje interferencije i "curenje" bežične mreže;
7. Omogućavanje filtriranja MAC adresa;
8. Korišćenje najboljeg mogućeg algoritma zaštite (WEP, WPA-PSK, WPA2-PSK) koji može da podržava AP ili Wireless router;
9. Korišćenje u srednjim i velikim poslovnim okruženjima WPA2 Enerprise sa Radius Serverom za autentifikaciju;
10. Periodične promene WEP, WPA i WPA2 ključeva;
11. Monitoring i analiza logova;
12. Upotreba statičkog IP adresiranja ukoliko je izvodljivo;
13. Isključivanje AP ili Wireless router-a prilikom duže odsutnosti (u kućnom okruženju).

Veoma je važno podesiti bezbednost svoje bežične mreže ispravno. U prethodnim poglavljima bile su objašnjene različite bezbednosne opcije podržane od strane AP ili Wireless router-a: WEP, WPA-PSK, WPA Enterprise, WPA2-PSK i WPA2 Enterprise.

WPA je daleko veća zaštita od WEP-a. Implementacija WEP-a predstavlja najosnovniji ele-

ment zaštite i treba ga koristiti samo u slučaju da uređaj ne podržava naprednije protokole zaštite. WPA2 predstavlja unapređenu verziju WPA i ima bolju zaštitu. Modovi rada u WPA i WPA2 su PSK ili Enterprise. Ukoliko to sredstva dozvoljavaju, korisno bi bilo da se koristi Enterprise u srednjim poslovnim okruženjima zbog dodatnog mehanizma zaštite, koja se dobija koordinacijom sa RADIUS serverom.

Ono što sledi iz svega do sada navedenog, a postavlja se kao krajnji cilj, odnosi se na postizanje maksimalne zaštite u bežičnoj mreži i to odabirom najboljeg mogućeg algoritma zaštite koji podržava uređaj koji se konfiguriše, u kombinaciji sa svim ostalim implementiranim elementima zaštite.

BIBLIOGRAFIJA:

Hlušička, Darko, Metode zaštite bežičnih mreža, http://www.pczenith.com/darco/metode_zastite_wlana.php , (septembar, 2009).

Kremer, Darijan, Vrste enkripcija i zaštita bežičnog mrežnog sustava, Uvod u bežične mreže, http://www.scribd.com/doc/26786178/Vrste-enkripcija-i-zastita-bezicnog-mreznog-sustava (5. Mart, 2009).

Linksys by Cisco, Wireless-G Broadband Router - User Guide, http://downloads.linksysbycisco.com/downloads/userguide/wrt54gl_v11_ug_c-web.pdf , (2. Decembar, 2009).

Mitrović, Ninoslav, Zaštita wireless mreže u 10 koraka, http://www.inforepublic.org/2009/04/13/zastita-wireless-mreze-u-10-koraka/ (8. Mart, 2009).

Steven Powell, J. P. Shim, Wireless Technology: Applications, Management, and Security, Hardback - 259 pages, Springer (2009).

Mark Ciampa, Cwsp Guide to Wireless Security, Paperback - 462 pages, Course Technology (2006).

Johnny Cache, Vincent Liu, Hacking exposed wireless: wireless security secrets & solutions, Paperback - 387 pages, McGraw-Hill (2007).

Jim Geier, Implementing 802.1X Security Solutions for Wired and Wireless Networks, Hardback - 330 pages, John Wiley & Sons (2008).

John R. Vacca, Guide to wireless network security, Hardback - 848 pages, Springer (2006).

GUIDELINES FOR SECURING WIRELESS NETWORK - IMPLEMENTATION

In this paper, guidelines for configuration of wireless network - implementation will be explained,which aim to rise the security level of wireless communication within the wireless network - WLAN. Further on, the needed security parameters will be explained, in order to secure a high security level within the WLAN. Also in this paper, a list of appropriate security measures is given, which are needed within the implementation. The purpose of this document is to establish security within a wireless network in a home environment as well as in small organization.

KEY WORDS: Wireless networks, Security, Wireless Protocols, WEP, WPA, WPA-PSK, WPA-Enterprise, WPA2, WPA2-PSK, WPA2-Enterprise, Implementation of Security, SSID, MAC address filtering