Analiza sigurnosti lokalnih bežičnih mreža na području općine Bol

Tonči Buljan, univ.bacc.ing.comp.

Bol, lipanj 2009.

Sadržaj

Zahvala

Ovim putem želio bih se zahvaliti načelniku općine Bol, gospodinu Tihomiru Marinkoviću, na razumjevanju opsega problema i financiranju istraživanja.

Također zahvalio bih se gospodinu Stipi Karmeliću na ustupljenim materijalima bez kojih ovo istraživanje nebi bilo potpuno.

Konačno, zahvalio bih se kolegi i dobrom prijatelju Goranu Zahariji na svestranoj podršci i pomoći prilikom izrade ovog rada.

Autor

Uvod

U današnje vrijeme, zahvaljujući razvoju tehnologija, prijenos podataka se sve više i više odvija bežičnim putem bez debelih i nezgrapnih kablova. Bežične tehnologije se, kao i ostatak informatičke industrije, ubrzano razvijaju, dolaze novi standardi, usvajaju se novi, moderniji načini proizvodnje koji omogućuju sve veće brzine i domet uz povoljniju cijenu. Sukladno ovom rastu, u ne tako dalekoj budućnosti možemo očekivati puno više bežičnih sustava, od malih kućnih, preko uredskih, pa sve do bežično povezanih velikih tvornica i tehnoloških parkova. Sigurnost je jedna od najvažnijih karakteristika bežičnih mreža. S obzirom na način na koji se podaci prenose kod bežičnih mreža, postoji opasnost da signal registriraju i druga računala, tj. neautorizirani korisnici koji žele neovlašteno ući u vaš sustav. Da stvar bude još ozbiljnija, postoje korisnici poznati pod imenom "wardrivers" koji traže bežične mreže s ciljem da se domognu tuđih podataka. Kod žičanih sustava bi za ovakav upad u sustav provalnik trebao imati fizički pristup mreži, a kako kod WLAN sustava se ne koriste žice već se koriste radiovalovi, svatko može doći do signala koji se odašilje ako ima potrebnu opremu.

Eksponencijalni rast bežičnih mreža u posljednje vrijeme jako je sličan rastu Interneta u 90-im godinama prošlog stoljeća. Jednostavnost implementacije, fleksibilnost u radu i različit broj uređaja koji se koriste pri implementaciji bežične mreže su svakako tome pogodovali te ih korisnici pri najmu ADSL opreme rado biraju, iako im ponekad i nisu potrebni.

Iako su u standardima koji definiraju bežične računalne mreže navedeni razni elementi sigurnosti pokazuje se da ti elementi u većini slučajevi ostaju neiskorišteni što je, dakako, velik sigurnosni problem. No i kada se aktiviraju svi sigurnosni elementi to ne znači nužno da je postignuta odgovarajuća razina sigurnosti. Razlog tomu su mnogi nedostaci samog standarda koji su naknadno uočeni i koji omogućavaju zlonamjernoj osobi da bez većih poteškoća pristupi i koristi mrežne resurse bez dozvole i znanja vlasnika ili administratora mreže. Sami propusti u standardu obuhvaćaju propuste pri autentifikaciji korisnika mreže kao i propuste u enkripciji podataka između pristupne točke i korisnika.

Cilj ovog seminarskog rada je testiranje i donošenje kratkog pregleda sigurnosti bežičnih mreža u Bolu na Braču.

Bežične mreže

Lokalna bežična mreža (Wireless Local Area Network – WLAN) je mreža koja spaja dva ili više računala te omogućuje njihovu komunikaciju na ograničenom području. Ovim putem korisnik je dobio određenu mobilnost, sposobnost kretanja unutar ograničenog dosega mreže.

Za kućne korisnike, bežična tehnologija postaje popularna zbog jednostavne instalacije i mobilnosti koju pružaju laptopi koji pak predstavljaju sve češći izbor korisnika. Poslovni subjekti kao što su caffe barovi ili trgovački centri također pružaju uslugu bežičnog pristupa internetu svojim korisnicima. New York City je započeo pilot program u kojem bi u svih pet općina bio dostupan bežični internet. U daljnjem nastavku teksta opisati će se prednosti i nedostaci bežičnih mreža.

Prednosti bežičnih mreža su:

Mobilnost

Mobilnost je izrazito izražena kod bežičnih mreža. Sa porastom broja javnih mreža, korisnik može pregledavati internet sadržaj bez obzira na svoju lokaciju, dokle god je u dosegu mreže.

Instalacija

Inicijalna instalacija bežične mreže uglavnom se sastoji od konfiguracije pristupne točke (Access Point). Žičane mreže imaju dodatne troškove u vidu kablova, konektora te krimpanja kablova.

Proširivost

Dodavanje novih korisnika u bežičnu mrežu je iznimno jednostavno, dok kod žičanih infrastruktura to zahtjeva dodatno kabliranje i eventualno dodatne priključke (ports) na mrežnih uređajima.

Nedostaci bežičnih mreža:

Sigurnost

Bežični radio predajnici služe pružanju usluge bez obzira na fizičke preprekena putu do predajnika. Bežične mreže podložnije su napadima zbog svojstva da korisnik ne mora biti fizički spojen na mrežu.

Doseg

Doseg bežične mreže nije beskonačan. Ukoliko postoji vidna linija između predajnika i prijemnika ta udaljenost može iznositi i do par stotina metara, dok ukoliko postoje prepreke (zidovi, kuće) ta ista udaljenost pada na samo nekoliko desetina metara.

Brzina

Brzina bežične mreže poprilično je sporija od brzine žičanog LAN-a. Kod prijenosa žicom danas je praktički standard 100 Mb/s dok je ta brzina kod radio prijenosa uvelike manja. Ipak, koliko god bila manja, ta brzina je ipak dovoljna jer se usko grlo ne stvara kod korisnikove bežične mreže već kod "izlaza" prema van, prema internet operateru, čak i pri najvećim ADSL brzinama.

Radio emisije

Bežični LAN koristi radio signale koji su podložni interferenciji sa ostalim uređajima koji mogu imati neželjene učinke na ljudsko zdravlje.

ZAŠTITA BEŽIČNE MREŽE

Kod bežičnih mreža razlikujemo tri osnovne razine zaštite, to su:

- WEP
- WPA
- WPA2

WEP

WEP je skraćenica od "Wired Equivalent Privacy" ili "Wireless Encryption Protocol", a predstavlja sigurnosni protokol za bežične mreže utvrđene standardom 802.11b. Od WEP protokola se očekuje stupanj sigurnosti jednak onom kod tradicionalnih ožičenih lokalnih mreža. WEP djeluje na dva donja sloja OSI modela – na fizičkom i na sloju veze i temelji se na enkripciji podataka između krajnjih točaka.

WEP za funkcioniranje koristi različite veličine ključeva, standardnih duljina 64-, 128- i 256 bita. Što je ključ duži to ga je teže probiti, no i samim je računalima potrebno više vremena kako bi dekodirali podatke koji se prenose. Tajni ključ je poznat samo mobilnim stanicama i pristupnoj točki na koju se spajaju. Uz pomoć tajnog ključa paketi se kriptiraju prije slanja, a dodatno se vrši provjera integriteta kako bi paket na odredište stigao nepromijenjen. Za enkripciju se koristi RC4 sustav zaštite koju je osmislio američki stručnjak Ronald Rivest, 1987. godine. RC4 proširuje kratak niz znakova u beskonačno dugačak pseudo nasumičan niz koji pošiljatelj pomoću funkcije XOR i originalne poruke pretvara u kriptiranu poruku koju šalje primatelju. Kako primatelj posjeduje isti ključ, prilikom preuzimanja on ga iskorištava te time dobiva identičan niz znakova koji uz pomoć XOR funkcije dekriptira i dobiva originalnu poruku.

Praksa je, nažalost, pokazala da **WEP ipak ne nudi očekivanu razinu sigurnosti** bežičnih lokalnih mreža, a velika količina danas dostupnog softvera omogućuje da i manje iskusni korisnici otkriju ključ po kojem se podaci kriptiraju i u vrlo kratkom vremenu dođu do tuđih podataka. 2005. godine je tim iz FBI-ja demonstrirao kako se korištenjem softvera dostupnog na Internetu može probiti WEP enkripcija u manje od tri

minute. Probijanje dužih ključeva zahtjeva više presretnutih paketa, no aktivnim napadima moguće je stimulirati dovoljnu količinu paketa da bi se otkrio ključ.

WPA

Skraćeno od "**W**iFi **P**rotected **A**ccess", ovaj sustav zaštite sastavni je dio 802.11i standarda. Radi se o sustavu za uspostavljanje sigurnih bežičnih mreža čija je svrha da zamijeni manje siguran WEP protokol. WPA uključuje mogućnost enkripcije podataka i autentifikacije korisnika.
Podaci su kriptirani RC4 sustavom sa 128-bitnim ključem i 48-bitnim inicijalizacijskim vektorom. Prednost nad WEP standardnom je u korištenju TKIP protokola, koji dinamički mijenja ključeve za vrijeme korištenja sustava. Kombinacijom dugačkog inicijalizacijskog vektora i TKIP protokola sustav se može lagano obraniti od napada kakvi se koriste za otkrivanje ključa primjenom WEP protokola.

Uz spomenuta unaprjeđenja, WPA protokol također donosi i sigurniji sustav provjere identiteta u odnosu na CRC koji se koristi kod WEP protokola. Naime, kod CRC-a napadač može promijeniti sastav poruke koja se šalje i vratiti vrijednost CRC-a na originalnu, čak i bez da je ključ, kojim je kriptirana poruka, poznat.

Uz pomoć navedenih tehnologija, probijanje u bežični mrežni sustav zaštićen WPA protokolom je relativno teško. „Michael“ algoritam je najsloženiji algoritam koji su WPA dizajneri mogli napraviti, a da je kompatibilan sa starijim mrežnim karticama. Zbog neizbježne slabosti tog algoritma, WPA u sebi ima ugrađene protumjere u vidu specijalnog mehanizma koji blokira pristup napadaču ako sustav primijeti pokušaj probijanja TKIP protokola.

Kako je RC4 sustav kriptiranja podataka relativno star, a njegovo probijanje ne predstavlja veliki napor hakerima, razvijen je WPA 2 protokol koji koristi napredni sustav kriptiranja zvan AES-CCMP.

WPA2

Glavna razlika između WPA i WPA 2 protokola je u korištenju naprednog AES-CCMP algoritma. CCMP je skraćenica od engleskog "**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol", a temelji se na "naprednom enkripcijskom standardu", tj. AES protokolu.
Od 13. ožujka 2006. godine sva mrežna oprema koja želi dobiti certifikat "WiFi Certified" mora podržavati ovaj algoritam.

Valja spomenuti da WPA i WPA 2 mogu raditi u dva načina rada: Enterprise i PSK. Osnovna razlika je u činjenici da Enterprise način rada zahtijeva prisutnost servera za autentifikaciju, koji standardno koristi RADIUS protokol za autentifikaciju i distribuciju ključeva. Zbog toga postoji mogućnost centralizacije ključeva, no ovakve mogućnosti nisu namijenjene kućnim korisnicima (zbog investicije u RADIUS server). Pre-Shared Key ne zahtjeva server za autentifikaciju jer koristi tajni ključ koji korisnik odredi. Svaki korisnik mora odrediti lozinku za pristup mreži koja mora biti duža od 8, a kraća od 63 ASCII znaka ili može odrediti 64 heksadecimalne znamenke (256 bita).

Posljedice upada u bežičnu mrežu

U slučaju da pristup mreži nije zaštićen ili da je sigurnost mreže kompromitirana, moguće su različite posljedice. Ako napadač nema maliciozne namjere, može iskoristiti dio našeg bandwidth-a, što u najboljem slučaju znači usporavanje veze ali u slučaju da nam se Internet naplaćuje prema količini prenesenih podataka, napadač nam može nanijeti veću materijalnu štetu. Napredniji napadači, jednom kad su spojeni na mrežu, mogu pokušati pristupiti routeru i na taj način mijenjati naše postavke i u potpunosti blokirati naš pristup Internetu. Iako je za pristup routeru potrebno unijeti korisničko ime i lozinku, korisnici često nisu svjesni toga pa ne mijenjaju šifre koje su unaprijed zadane.

Ukoliko dijelimo resurse na mreži (koristimo mrežne diskove), napadač može vrlo lako doći do tih podataka praktički bez ikakvog korisnikovog saznanja o napadu. To možda i nije problem ukoliko se radi o par lektira skinutih sa interneta, ali ukoliko se radi o nekakvoj državnoj službi tipa suda ili općine, krađa takvih podataka može nanijeti velike gubitke vlasnicima istih.

Ukoliko napadač stvarno hoće poslati u zatvor vlasnika bežične mreže, sve što treba je skidati pornografiju sa interneta. Pedofili su jedan od najvećih problema današnje mreže svih mreža i policija ulaže velika sredstva u njihov pronalazak i registraciju. Ukoliko napadač napravi takav “napad”, on ostavlja za sobom IP adresu (jedinstvenu adresu svakog uređaja spojenog na internet), no ta adresa će biti adresa vlasnika mreže kojeg telekom operater može vrlo jednostavno i brzo locirati prema vremenu spajanja. U navedenom slučaju vlasnik će imati velike probleme da objasni da on nije surfao i skidao zabranjeni sadržaj.

Načini kako otežati napadaču

U ovom poglavlju u par kratkih natuknica objasniti ću kako dodatno osigurati bežičnu mrežu i računala spojena u nju da bi spriječili/otežali eventualne napade. Natuknice su preuzete sa adrese http://windowshelp.microsoft.com:

Korištenje vatrozida

Vatrozid može poboljšati zaštitu računala od hakera ili zlonamjernih programa (kao što su crvi) koji računalu pokušavaju pristupiti putem mreže ili Interneta. Vatrozid također može spriječiti računalo da drugim računalima pošalje zlonamjerne programe.

Korištenje antivirusa

Vatrozid sprječava pristup crvima i hakerima, ali nije dobra zaštita od virusa pa biste trebali instalirati i koristiti protuvirusni program. Viruse možete primiti putem privitaka u porukama e-pošte, datoteka na CD-ovima ili DVD-ovima ili datoteka preuzetih s Interneta. Provjerite je li protuvirusni program ažuriran te ga postavite da redovito pregledava računalo.

Koristite mrežni sigurnosni ključ

Ako imate bežičnu mrežu, trebali biste postaviti mrežni sigurnosni ključ jer tako uključujete šifriranje. Kada je uključeno šifriranje, korisnici bez sigurnosnog ključa se ne mogu povezati s vašim računalom. Štoviše, sve informacije poslane putem mreže šifrirane su tako da samo računala s ključem za dešifriranje mogu pročitati informacije. Tako dodatno onemogućujete pokušaje neovlaštenog pristupa vašoj mreži i datotekama. Uobičajene su metode šifriranja bežičnih mreža zaštićeni bežični pristup (Wi-Fi Protected Access, WPA) i WPA2.

Promjena zadanih lozinki

Ako koristite usmjerivač ili pristupnu točku, vjerojatno ste koristili zadano ime i lozinku za postavljanje opreme. Većina proizvođača za svu svoju opremu koristi isti zadani naziv i lozinku, što bi netko mogao iskoristiti za pristup usmjerivaču ili pristupnoj točki bez vašeg znanja. Da biste to izbjegli, promijenite zadano administratorsko korisničko ime i lozinku za usmjerivač. Upute za promjenu imena i lozinke potražite u informacijama dobivenima s uređajem.

Promijenite zadani naziv mreže (Service set identifier, SSID)

Umjerivači i pristupne točke koriste naziv bežične mreže, tzv. naziv mreže (Service set identifier, SSID). Većina proizvođača koristi isti SSID za sve svoje usmjerivače i pristupne točke. Preporučujemo da promijenite zadani SSID da biste onemogućili preklapanje vaše bežične mreže s drugim bežičnim mrežama koje koriste zadani SSID. Tako ćete i lakše prepoznati svoju bežičnu mrežu ako ih u blizini ima više jer se SSID najčešće prikazuje na popisu dostupnih mreža.

Pažljivo postavite usmjerivač ili pristupnu točku

Bežični se signal može prenositi nekoliko stotina metara pa se signal s vaše mreže može emitirati i izvan vašeg doma. Postavljanjem usmjerivača ili pristupne točke bliže središtu kuće nego vanjskom zidu ili prozoru možete ograničiti područje koje pokriva bežični signal.

Obavezno uključite filter MAC adresa

Svaka mrežna kartica ima jedinstvenu fizičku adresu (MAC adresa) koja joj je dodjeljena od strane proizvođača mrežne opreme. Poželjno je pri konfiguraciji usmjerivačnog uređaja (router) uključiti filter koji omogućava samo određenim MAC adresama da se spoje na mrežu.

Gašenje ADSL uređaja

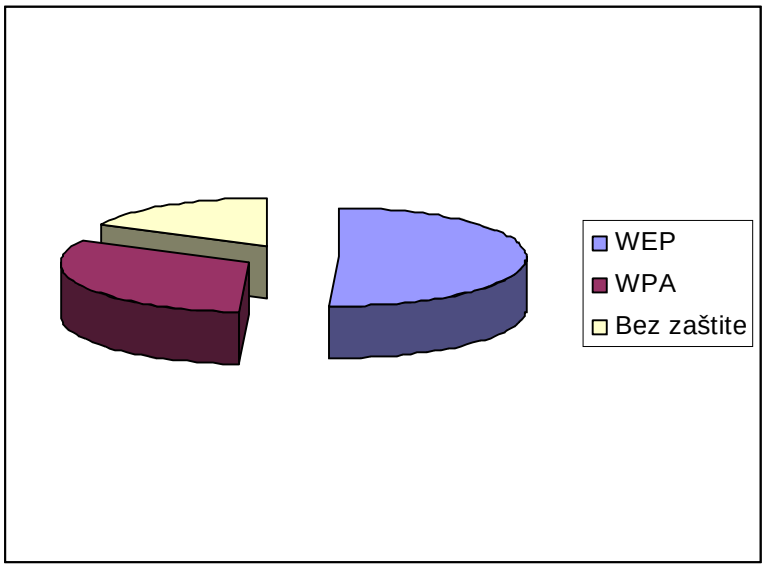
Možda i nije najpopularnija metoda ali svakako je najsigurnija. Ukoliko smatrate da ste ugroženi od strane napadača, slobodno ugasite ADSL modem nakon korištenja interneta. Vaša telefonska linija i dalje će ostati **potpuno funkcionalna**.

Testiranje sigurnosti na području općine Bol

Testiranje sigurnosti bežičnih mreža na području općine Bol provedeno je u trajanju od 28.3.2009. do 7.6.2009. U tom periodu pronađeno je 110 bežičnih mreža od kojih je 56 mreža koristilo osnovnu i najslabiju WEP zaštitu, napredniju zaštitu u obliku WPA enkripcije koristilo je 35 mreža dok je 19 mreža bilo nezaštićeno. U tablici 1 i na slikama 1 i 2 dan je pregled mreža:

	Bez zaštite	**WEP**	**WPA**	**Ukupno**
Broj	19	56	35	110
Postotak	17.3 %	50.1 %	31.81 %	100 %

Tablica 1 Raspodjela mreža prema zaštiti



Slika 1 Grafički prikaz raspodjele

Naravno, ovim istraživanjem nisu pokrivene sve mreže na području Bola, takvo istraživanje bi trajalo daleko duže a ni tada nebi mogli sa sigurnošću tvrditi da smo pokrili cijeli prostor Općine Bol, ali usudio bih reći da dobar dio jest pa i ove rezultate možemo smatrati kao reprezentativne.

Slika 2 Fizička raspodjela mreža u Bolu

Napomena:
U priloženoj pdf datoteci nalazi se ista slika ali u većoj rezoluciji.

Zaključak

Bežične mrežne tehnologije predstavljaju novi oblik mrežne komunikacije koji ubrzano napreduje i u budućnosti će vrlo vjerojatno zamijeniti ožičene mrežne sustave kako po pitanju brzine, tako i po pitanju sigurnosti. Na novim se standardima stalno radi, oprema postaje sve sofisticiranija, softver sve brži, a sustavi zaštite također napreduju. Unatoč tome činjenica je da korisnici nisu svjesni, a niti educirani o opasnostima koje donosi bežična mreža. Zabrinjava i činjenica da su i mnoge male tvrtke potpuno nezaštićene što bi zlonamjerni korisnici mogli itekako dobro iskoristiti u svoju korist, a da vlasnici tih sustava niti nisu svjesni da na taj način mogu izgubiti važne podatke i povjerljive dokumente. Međutim, čak i korištenjem nekog od sustava zaštite računala nisu 100% sigurna, a uz taj nedostatak problem se javlja i u značajnom usporenju mreže ako se koriste jači sustavi kriptiranja.

Gledajući rezultate dobivene ovim testiranjem, može se doći do zaključka da se razina educirasnosti prosječnog korisnika o sigurnosti bežičnih mreža postepeno povećava. Ipak da moram, a moram, izvući neki generalni zaključak o sigurnosti bežičnih mreža u Bolu, rekao bih da je postotak od 17 % nezaštićenih mreža poprilično velik ukoliko gledamo isto istraživanje u gradu Splitu gdje se ta brojka uglavnom kreće oko 10 % (isti autor). Prije svega prijateljska okolina i vrlo dobro poznavanje susjeda dovode do činjenice da je u Bolu veći postotak nezaštićenih mreža u odnosu na Split pa bih donekle isključio neinformiranost Boljana o zadanoj tematici. Slično kao i u Splitu, najveći broj zaštićenih mreža koristi najslabiju WEP enkcipciju i ta brojka se uglavnom kreće oko 50 %.

Ukoliko više želite saznati o ovom istraživanju svakako pogledajte sljedeću **emisiju Potrošački kod na HRT**-u kada će tamo detaljnije biti prezentirani rezultati ovog i sličnih istraživanja.

Tonči Buljan, univ.bacc.ing.comp.