UDC: 004.732 INFO M: str. 23-28

SIGURNOST IEEE 802.11 BEŽIČNIH MREŽA U BEOGRADU
SECURITY OF IEEE 802.11 WIRELESS NETWORKS IN BELGRADE

Dušan Švenda, Marko Derota, Aleksandar Glišić i Miroslav Djordjević

REZIME: U radu je opisano trenutno stanje bežičnih računarskih mreža standarda IEEE 802.11 u delovima grada Beograda. Izvršeno je merenje i klasifikacija detektovanih bežičnih računarskih mreža u skladu sa upotrebljenim načinom zaštite (enkripcije) na MAC mrežnom nivou standarda IEEE 802.11, kao i zastupljenost pojedinih proizvođača mrežne opreme. Takođe je ispitana povezanost rezultata sa tipom (proizvođačem) bežične mrežne opreme i procenjenim nivoom dodatnih podešavanja implementiranih od strane krajnjih korisnika. Uočeno je da je stepen zaštite bežičnih mreža relativno dobar i poboljšan u odnosu na starije bežične mreže u Beogradu, premda i dalje oko 40% ispitanih bežičnih mreža koristi nesigurne vidove zaštite (WEP) ili uopšte ne koristi enkripciju.

KLJUČNE REČI: Bežične mreže, sigurnost, wardriving, WEP, WiFi, WPA.

ABSTRACT:The paper presents current state of IEEE 802.11 wireless networks in several Belgrade neighbourhoods. Measurements were performed and detected wireless networks were classified according to the type of wireless security (encryption) used on MAC layer of IEEE 802.11 standard. Market share of specific manufacturers of wireless equipment is estimated. Correlation of gathered results and type (manufacturer) of wireless equipment detected, as well as the estimated level of user configuration implemented is investigated. It was noted that the security level of wireless networks is relatively good and presents an improvement over security of older networks in Belgrade, although still about 40% of analyzed wireless networks use compromised security (WEP) or do not use encryption at all.

KEY WORDS: Wireless networks, security, wardriving, WEP, WiFi, WPA.

UVOD

Eksplozivan porast bežičnih mreža u poslednje vreme podseća na ekspanziju Internet servisa krajem prošlog i početkom ovog veka. Bežični prenos podataka nudi visok komfor korisnicima laptop računara, mobilnih telefona i pda uređaja. Povezivanje stacionarnih računara u LAN kao i računara sa perifernim uređajima postaje jednostavno, brzo i jevtino u mnogim praktičnim rešenjima koje nudi WLAN (Wireless Local Area Network) tehnologija.

Prvi pokušaji za standardizaciju bežičnih računarskih mreža započeli su 1991. godine planiranjem IEEE 802.11 i HiperLAN standarda. Tokom godina, IEEE 802.11 postao je dominantan standard dok su ostali ili potisnuti i skoro napusteni (kao HiperLAN), ili dobili potpuno drugačiju praktičnu upotrebu (kao DECT, koji je prvu aplikaciju imao upravu u domenu bežičnih računarskih mreža, ali se sada upotrebljava samo u bežičnoj fiksnoj telefoniji).

Broj korisnika Wi-Fi standarda u svetu je u rapidnom porastu ako uzmemo u obzir sve načine implementacije ove tehnologije. Kamere za video nadzor, štampači, kancelarijski multifunkcionalni uređaji, mobilni telefoni, aktivna mrežna oprema, laptop računari, i razni drugi proizvodi izlaze na tržište sa ugrađenim bežičnim karticama baziranim na jednom ili više IEEE 802.11 standarda.

IEEE 802.11 standard trenutno nudi nekoliko nivoa zaštite podataka koji se prenose između AP i klijenta. Prvi implementirani protokol, nazvan Wired Equivalence Privacy (WEP) bio je uključen u prvu verziju standarda (IEEE 802.11-1997 [1]) i koristi RC4 enkripciju (generalno sigurnu metodu), koja u kombinaciji sa procesom autentifikacije i linearnošću enkripcione funkcije u odnosu na CRC otvara mogućnost otkrivanja tajnog ključa. WEP zaštita je razbijena 2001. godine [2], a kasnije su razvijene metode koje uz pomoć laptop računara mogu da otkriju WEP ključ za svega jedan minut [1]. Pošto se bežična mreža zaštićena WEP-om ne može smatrati sigurnom, 2003. godine je razvijen novi standard, nazvan WiFi Protected Access (WPA).

Poslednjih godina su uočene neke slabosti u WPA algoritmu zaštite koje omogućavaju dešifrovanje pojedinih kratkih paketa ukoliko se koristi IEEE 802.11e QoS [1], kao i generalniji man-in-the-middle napad [3] koji zahteva fizičko postavljanje napadača između AP i klijenta. Navedeni napadi ne omogućavaju otkrivanje WPA šifre, mada je nju moguće otkriti ukoliko se koristi slaba lozinka, bilo kroz napad korišćenjem rečnika (dictionary attack) ili grubom silom (brute force), odnosno ispitivanjem svih mogućih lozinki. Ukoliko se koristi jaka lozinka, WPA se, iako je protokol baziran na WEP zaštiti, trenutno smatra sigurnom tehnologijom.

U okviru IEEE 802.11i amandmana standardu, definisana je nova vrsta zaštite nazvana WPA2 ili RSN (Robust Security Network) koja, za razliku od WEP i WPA protokola, ne koristi RC4 tehniku, već je zamenjuje naprednijim AES (Advanced Encription Standard). WPA2 je, kao i WPA, podložan napadima prilikom autentifikacije (korišćenjem rečnika ili grube sile), međutim napadi predstavljeni u [1] i [3] ne mogu se implementirati, jer ne postoje slabosti RC4 algoritma.

U ovom radu su predstavljeni rezultati snimanja bežičnih mreža u Beogradu, kako bi se stekao uvid o stanju zaštite bežičnih računarskih mreža kod nas. Razmatrana je samo zaštita pristupa pojedinačnim baznim stanicama (AP – eng. acces point), odnosno mrežama, koja je u okviru IEEE 802.11 standarda implementirana na MAC sloju, tako da postoji mogućnost da su neke mreže koje deluju nezaštićeno zapravo dobro osigurane na višim nivoima.

OPIS MERENJA

Merenja su vršena uz pomoć DELL Vostro A840, HP Compaq 6710b i DELL Inspiron 1501 laptop računara, koji su korišćeni na raznim rutama kroz beogradske ulice. Računari su bili pozicionirani na suvozačkom sedištu automobila. Trenutna pozicija određivana je uz pomoć nekoliko GPS prijemnika (Cellular Line Bluetooth GPS440, HTC HD2 SmartPhone, HIACOM HI-408 BT), postavljenih ispod vetrobranskog stakla automobila.

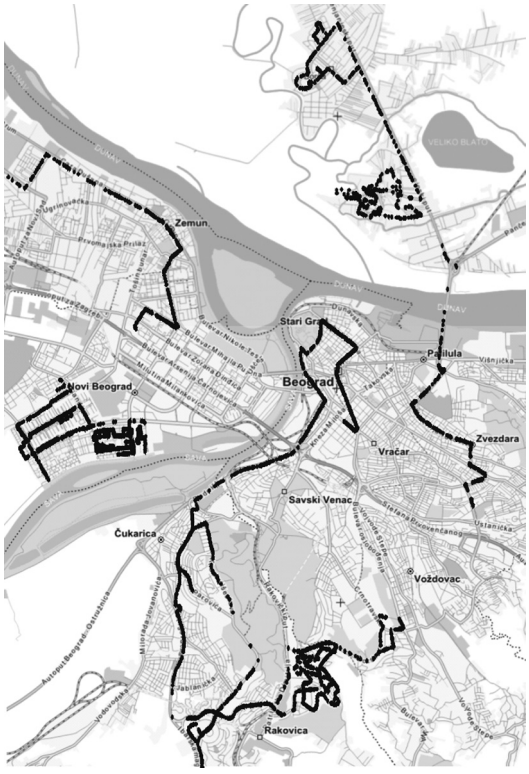
Signali IEEE 802.11b/g mreža su primani pomoću TP-Link TL-WN321G bežične mrežne kartice sa USB konekcijom. Iako korišćeni računari imaju ugrađene bežične kartice, one nisu korišćene, pošto je ekperimentalno utvrđeno da dijagram zračenja antene u računaru ima duboke nule ukoliko se računar nalazi unutar vozila (samim tim, postoje pravci iz kojih je nemoguće ili veoma teško primati signale bežičnih mreža). Osim TP-Link TL-WN321G i bežičnih kartica ugrađenih u računare, ispitana je i upotreba TP-Link TL-WN310G bežične kartice sa PCMCIA konekcijom, koja nije dala zadovoljavajuće rezultate upravo zbog načina pozicioniranja interne antene unutar automobila. Korišćenje bežične kartice sa USB konekcijom ima još jednu prednost, a to je da se ne samo antena, već i sam prijemnik bežičnih signala nalaze van automobila, čime je izbegnuto korišćenje dugačkih produžnih kablova za vezu između antene i prijemnika, a samim tim i unošenje nepotrebnih gubitaka (koji bi, efektivno, smanjili osetljivost prijemnika). Bežična kartica je na laptop računar povezana pomoću produžnog USB kabla, koji, pošto je već izvršen prijem bežičnog signala (u kartici), ne utiče negativno na osetljivost prijemnika, pa može imati veće dužine i omogućiti lakše postavljanje antene van automobila.

Bežična kartica TP-WN321G bila je pozicionirana 60cm iznad krova (pričvršćena na ugrađenu FM-antenu) u prvom slučaju, odnosno iznad vetrobranskog stakla automobila u drugom slučaju, čime je osigurana uniformnost zračenja u svim pravcima, odnosno umanjen uticaj karoserije automobila na dijagram zračenja. Pojačanje antene bežične kartice iznosi oko 0dBi, što je u našem slučaju predstavljalo prednost, pošto su samo relativno bliske bežične mreže bile u dometu uređaja.

Bežična kartica u jednom trenutku prima podatke samo sa jednog (od mogućih 13) kanala u okviru spektra namenjenog za bežične lokalne računarske mreže. Da bi se osluškivao čitav spektar, korišćeni programski paketi periodično menjaju kanal na kome bežična kartica radi. Imajući ovo u vidu, brzina vožnje značajno utiče na količinu prikupljenih podataka. Ukoliko se automobil kreće prebrzo u delu grada koji je gusto prekriven bežičnim mrežama, može se dogoditi scenario gde određena mreža biva „preskočena“, pošto, dok je mreža u dometu, bežična kartica prima podatke sa drugih kanala. Stoga se u našem istraživanju automobil kretao maksimalnom brzinom od 20 km/h, ukoliko je to bilo moguće, odnosno sigurno. Primer mesta gde nije poštovana preporuka o maksimalnoj brzini je, na primer, Bulevar Vojvode Mišića, gde je bilo nesigurno voziti značajno sporije od ostalih vozila. Drugi način prikupljanja detaljnijih podataka o mrežama sa pojedinih lokacija je prolaženje istim trasama nekoliko puta. Zbog materijalnih troškova, delove grada gde su vršena višestruka merenja ograničili smo na područje blokova 70 i 70a na Novom Beogradu, kao i Rakovicu i Kotež.

Tokom merenja vršenih u blokovima 70 i 70a na Novom Beogradu, korišćena je bežična kartica ugrađena u laptop računar, koja podržava i IEEE 802.11n standard u opegu od 2.4 GHz.

Rezultati prikazani u ovom radu predstavljaju plod istrazivanja koje su tri autora rada obavila u sklopu izrade specijalističkih radova na Visokoj školi strukovnih studija za informacione i komunikacione tehnologije (Visoka ICT). Ovaj rad nije bio finansiran od strane sponzora (Visoka ICT je delimično pomogla davanjem delova neophodne opreme na korišćenje), a pošto je iziskivao određene materijalne troškove (vezane za nabavku pojedine opreme i gorivo), rute kojima su se vozila kretala tokom našeg istraživanja birana su na taj način da se sa jedne strane minimizuju troškovi putovanja (autori su vršili merenja većim delom u relativnoj blizini svog prebivališta, odnosno duž trase koju uobičajeno prelaze prilikom odlaska na posao), a sa druge strane da bi se teritorija grada Beograda dovoljno gusto „prekrila“. Prilikom izbora rute, imali smo u vidu da specifikacije korišćene TP-Link TP-WN321G bežične kartice navode 300m kao maksimalni domet kada se kartica koristi na otvorenom, tako da se prilikom kretanja kroz pojedine ulice beleže i bežične mreže čije su bazne stanice (access point) relativno udaljene. Prilikom snimanja nema dupliranja rezultata (potencijalno moguće, pošto se prilikom osluškivanja IEEE 802.11 učestanosti pojedine mreže više puta registruju), pošto se pozicija pojedine mreže (unikatno određena MAC adresom korišćene bazne stanice) utvrđuje na osnovu maksimalnog nivoa primljenog signala.



Slika 1. Otkrivene bežične mreže u Beogradu

U ovom radu je izvršeno pasivno snimanje i prikupljanje javno dostupnih parametara bežičnih mreža (ime mreže, MAC adresa AP, tip enkripcije, korišćeni standard, kanal na kome AP emituje,...). U skladu sa članom 302 Krivičnog zakonika [4], nije vršeno „razbijanje“ WEP zaštite, a ni napadi pomoću rečnika protiv WPA (da bi se utvrdilo da li je korišćena WPA lozinka dobro izabrana), pošto nije bilo moguće dobiti potrebnu saglasnost vlasnika mreža. Bežične kartice su radile u prijemnom modu i nije vršeno slanje paketa baznim stanicama sa namerom da se od pojedine bazne stanice „izmame“ odgovori. Sadržaj IEEE 802.11 paketa koji se odnosio na korisničke podatke (van zaglavlja paketa koje sadrži gore navedene parametre bežičnih mreža), s obzirom da potiče sa viših nivoa ISO modela, nije analiziran.

REZULTATI

Prikazani rezultati uključuju mreže detektovane u nekoliko delova Beograda. Iako istraživanjem nisu obuhvaćene sve beogradske bežične mreže, broj detektovanih mreža (6230) i ruta kojom su se automobili kretali (Banjica, Rakovica, Cerak, Žarkovo, centar, Novi Beograd, Krnjača, Kotež, Borča, Zemun, Zvezdara - Slika 1) omogućavaju visok nivo pouzdanosti rezultata primenjenih na celokupno područje Beograda. Zbog ograničenja upotrebljene opreme, merenjem nisu obuhvaćene mreže koje koriste IEEE 802.11a i 802.11n standarde, pri čemu treba imati u vidu da IEEE 802.11a mreže nisu veoma popularne u svetu, pa ni u Srbiji, dok je IEEE 802.11n standard relativno nov (objavljen oktobra 2009.), tako da je oprema koja ga podržava relativno skupa a samim tim i trenutno malo zastupljena u Beogradu. Na delu trase gde je korišćena oprema koja podržava IEEE 802.11n standard na nižem opsegu učestanosti (2.4 GHz) novi standard bio je zastupljen u oko 7% slučajeva, tako da isključivanjem ovih mreža iz analize u ostalim delovima grada ne pravimo veliku grešku u ovom trenutku.

KORIŠĆENI STANDARDI

Standard koji bežična mreža koristi određen je na osnovu upotrebljene modulacije. Stariji standard (IEEE 802.11b) koristi tehniku proširenog spektra sa direktnom sekvencom (DSSS), dok noviji standard (IEEE 802.11g) upotrebljava ortogonalni frekvencijski multipleks (OFDM) [5]. Tabela 1 prikazuje udeo 802.11b i 802.11g standarda u beogradskim bežičnim mrežama u zavisnosti od posmatranog dela grada.

Iako postoje fluktuacije u procentu korišćenja starijeg standarda među različitim delovima grada, može se uočiti da je u većini naselja 802.11b standard upotrebljavan u manje od 10% slučajeva. Kotež i Zvezdara koriste 11.5% i 10.7% starijeg standarda, respektivno, dok korisnici na Banjici upotrebljavaju čak 17.1% mreža starijeg standarda. Treba imati u vidu da je našim merenjem „pokriven“ mali deo teritorije Banjice, kao i da je broj posmatranih bežičnih mreža relativno mali (123), tako da nije ispravno donositi zaključke o povećanoj zastarelosti opreme korišćene na Banjici u odnosu na ostale delove grada.

Relativno mali broj IEEE 802.11b mreža može se objasniti činjenicom da je taj standard ratifikovan 1999. godine, u trenutku kada u Srbiji nisu postojali preveliki zahtevi za bežičnim mrežama, kao i da su uređaji bazirani na IEEE 802.11g standardu (ratifikovan nepune četiri godine nakon 802.b) bili potpuno kompatibilni sa starim standardom i veoma brzo se izjednačili po ceni sa starim uređajima.

Tabela 1: Raspodela po tipu standarda.

Naselje	IEEE 802.11b	IEEE 802.11g	Ukupno
Zemun	36 (9.5%)	342 (90.5%)	378
Novi Beograd	96 (5.0%)	1831 (90.0%)	1927
Kotež	40 (11.5%)	309 (88.5%)	349
Borča	23 (7.8%)	271 (92.2%)	294
Zvezdara	49 (10.7%)	411 (89.3%)	460
Centar	42 (4.8%)	827 (95.2%)	869
Senjak	9 (9.4%)	87 (90.6%)	96
Čukarica-Banovo brdo	20 (4.2%)	455 (95.8%)	475
Banjica	21 (17.1%)	102 (82.9%)	123
Rakovica	35 (4.6%)	728 (95.4%)	763
Cerak	12 (9.3%)	117 (90.7%)	129
Vidikovac	21 (5.7%)	346 (94.3%)	367
Beograd (ukupno)	404 (6.5%)	5826 (93.5%)	6230

PROIZVOĐAČI

Tabela 2 prikazuje broj AP (i udeo u ukupnom broju) u zavisnosti od proizvođača opreme. Proizvođač opreme je određen na osnovu MAC adrese pošiljaoca (AP) koja se prenosi nezaštićeno u zaglavlju rama na MAC sloju u 802.11 standardu i javno dostupne liste MAC prefiksa [6]. Nakon što je programima WiFi Hopper i ViStumbler izvršeno snimanje bežičnih mreža, rezultati su zapisani u tekstualnu datoteku (u csv formatu). Jednostavni program u C programskom jeziku je zatim korišćen da uporedi MAC adrese detektovanih bežičnih mreža iz csv datoteke sa listom MAC prefiksa koju publikuje IEEE, kako bi se u csv datoteku dodala kolona sa imenom proizvođača bežične opreme. Podaci su zatim učitani u program Microsoft Excel, gde je izvršena finalna obrada podataka.

U tabeli 2 prikazano je 14 najpopularnijih proizvođača, dok je merenjem detektovano 79. Proizvođači koji nisu izlistani u tabeli 2 imaju manje od 1% učešća u beogradskim bežičnim mrežama, pri čemu 48 (od 65) ima manje od 10 detektovanih AP.

Za većinu proizvođača je izvršena agregacija rezultata. Naprimer, detektovani Cisco-Linksys AP se na IEEE OUI

listi [6] pojavljuju pod sledecim imenima: „Cisco“, „Cisco Systems“, „Cisco-Linksys“, „Cisco-Linksys LLC“, „Cisco-Linksys, LLC” i „The Linksys Group, Inc.”

Ukoliko se izuzmu bežični uređaji koje je, u okviru svih ADSL promocija, krajnim korisnicima na korišćenje isporučivao Telekom Srbija (Askey Computer, Pirelli, Intracom S.A.), sa ukupnim učešćem od 28.4%, daleko ispred svih proizvođača nalazi se TP-Link sa 28.2%. Zatim sledi Cisco-Linksys sa svega 10.5%, dok ostali poznati proizvođači bežične opreme za kućne potrebe (D-Link, Belkin, Netgear, Planet) imaju značajno manji procenat zastupljenosti.

Takođe, treba obratiti pažnju na relativno veliki broj (87, odnosno 3.1%) AP čije se MAC adrese ne nalaze na IEEE OUI listi (navedene u tabeli pod “Nepoznat”). Čak i kada MAC adresa nije promenjena od strane korisnika („falsifikovana“), ime proizvođača dobijeno preko MAC adrese ne mora se poklapati sa imenom koje zaista stoji na samom kućištu aparata. Naprimer, uređaji čija MAC adresa odgovara proizvođaču „Askey Computer“ zapravo su bežični ADSL modem-ruter uređaji koje proizvodi Huawei (HG520x), a isporučuje ih Telekom Srbija uz svoje ADSL pakete. Kompanija „Askey Computer“ proizvodi bežični modul u uređaju, pa se čitav ADSL modem-bežični ruter bežičnim korisnicim identifikuje kao „Askey Computer“.

Tabela 2: Raspodela po proizvođaču opreme.

Proizvođač	Broj AP
TP-Link	1756 (28.2%)
Askey Computer	1323 (21.2%)
Cisco-Linksys	653 (10.5%)
D-Link	320 (5.1%)
Pirelli	239 (3.8%)
Intracom S.A.	205 (3.3%)
Belkin	202 (3.2%)
Netgear	176 (2.8%)
Nepoznat	172 (2.8%)
Planet	171 (2.7%)
ASUStek	169 (2.7%)
Vertex	125 (2.0%)
Siemens	120 (1.9%)
Wistron	73 (1.2%)
Ostali	526 (8.4%)

ZAŠTITA WLAN MREŽA

U ovom poglavlju rada, ispitujemo korišćenje zaštitnih tehnika definisanih u standardu IEEE 802.11 u bežičnim računarskim mrežama na teritoriji Beograda. Broj zaštićenih mreža i njihov tip zaštite ispitivan je za različite delove grada. Pošto je IEEE 802.11b stariji standard čiji harware omogućava manje protoke i inicijalno je podržavao samo WEP tip enkripcije (napredniji vidovi zaštite omogućeni su na nekim uređajima uz pomoć dodatnih programa – firmware update), rezultati istraživanja su prikazani i analizirani pojedinačno za mreže koje koriste IEEE 802.11b i IEEE 802.11g standard.

Vrste upotrebljene zaštite u starijim IEEE 802.11b uređajima prikazane su u Tabeli 3. Broj bežičnih mreža u Beogradu koje koriste IEEE 802.11b standard je relativno mali, tako da statistička analiza rezultata po delovima grada nema jako uporište. Uzorak od svega devet bežičnih mreža na Senjaku, odnosno 12 na Ceraku, kao i svega dvadesetak na Banovom brdu, Borči, Čukarici, Banjici i Vidikovcu (videti Tabelu 1.) je previše mali da bi se izveli validni zaključci. Tvrdnja da su, recimo, sve ispitane mreže IEEE 802.11b standarda na Ceraku bez ikakve zaštite može zvučati kao bitan podatak, imajući u vidu da relativno blizu, u Rakovici, „svega“ 63% mreža nema zaštitu, ali kada se uzme u obzir broj otkivenih mreža, validnost tvdnje je značajno redukovana.

Na nivou Beograda, međutim, broj mreža IEEE 802.11b standarda je dovoljno veliki da se izvuku značajni pokazatelji. Skoro tri četvrtine bežičnih mreža ne upotrebljava nikakvu enkripciju, a 11% upotrebljava prevaziđenu i nesigurnu WEP enkripciju (moguće i zbog toga što uređaji ne podržavaju naprednije zaštite). Uzimajući u obzir da samo 15% IEEE 802.11b bežičnih mreža upotrebljava jaku enkripciju, nije teško zaključiti zbog čega je nekad vladalo mišljenje da su bežične mreže u Beogradu mahom nezaštićene.

Tabela 3: Tip zaštite 802.11b mreža.

Naselje	Bez enkripcije	WEP	WPA	WPA2
Zemun	28 (77.8%)	1 (2.8%)	7 (19.4%)	0 (0.0%)
Novi Beograd	61 (63.5%)	14 (14.6%)	15 (15.6%)	6 (6.3%)
Kotež	35 (87.5%)	2 (5.0%)	1 (2.5%)	2 (5.0%)
Borča	19 (82.6%)	1 (4.3%)	2 (8.7%)	1 (4.3%)
Zvezdara	37 (75.5%)	4 (8.2%)	7 (14.3%)	1 (2.0%)
Centar	28 (66.7%)	6 (14.3%)	7 (16.7%)	1 (2.4%)
Senjak	6 (66.7%)	3 (33.3%)	0 (0.0%)	0 (0.0%)
Čukarica-Banovo brdo	15 (75.0%)	1 (5.0%)	2 (10.0%)	2 (10.0%)
Banjica	19 (90.5%)	1 (4.8%)	0 (0.0%)	1 (4.8%)
Rakovica	22 (62.9%)	7 (20.0%)	2 (5.7%)	4 (11.4%)
Cerak	12 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Vidikovac	16 (76.2%)	5 (23.8%)	0 (0.0%)	0 (0.0%)
Beograd	298 (73.8%)	45 (11.1%)	43 (10.6%)	18 (4.5%)

Tabela 4 pokazuje detektovani stepen zaštite IEEE 802.11g mreža. Najmanji procenat u potpunosti nezaštićenih mreža (na MAC sloju) nalazi se na Zvezdari, Čukarici, Banovom brdu i Novom Beogradu, s tim da je većina delova grada jako blizu gradskom proseku od 22% nezaštićenih mreža, pri čemu odskaču Senjak, Kotež i Borča sa oko 30%. Udeo mreža koje koriste WEP enkripciju je povećan u odnosu na starije mreže, što je donekle začuđujuće, pošto bi većina IEEE 802.11g mreža trebalo da podržava WPA i WPA2 zaštitu, pa smo, samim tim, očekivali i primetno smanjenje korišćenja WEP

zaštite, koje bi oslikavalo smanjenje koje vidimo kod nezaštićenih mreža. Očigledno je da korisnici bežičnih računarskih mreža u Beogradu nisu dovoljno obavešteni o ranjivosti zaštite koju pruža WEP i da je potrebno edukovati korisnike o prednostima koje pružaju noviji metodi zaštite kao što su WPA i WPA2. Finalno, broj mreža koje upotrebljavaju sigurnu enkripciju (WPA i WPA2) drastično je povećan (u odnosu na starije mreže) i skoro je uniformno raspoređen po delovima Beograda, jako blizu gradskog udela od 60%.

Tabela 4: Tip zaštite 802.11g mreža.

Naselje	Bez enkripcije	WEP	WPA	WPA2
Zemun	88 (25.7%)	59 (17.3%)	98 (28.7%)	97 (28.4%)
Novi Beograd	358 (19.6%)	311 (17.0%)	541 (29.5%)	621 (33.9%)
Kotež	91 (29.4%)	32 (10.4%)	122 (39.5%)	64 (20.7%)
Borča	76 (28.0%)	32 (11.8%)	78 (28.8%)	85 (31.4%)
Zvezdara	65 (15.8%)	75 (18.2%)	142 (34.5%)	129 (31.4%)
Centar	174 (21.0%)	156 (18.9%)	204 (24.7%)	293 (35.4%)
Senjak	28 (32.2%)	13 (14.9%)	14 (16.1%)	32 (36.8%)
Čukarica-Banovo brdo	87 (19.1%)	91 (20.0%)	124 (27.3%)	153 (33.6%)
Banjica	26 (25.5%)	17 (16.7%)	27 (26.5%)	32 (31.4%)
Rakovica	184 (25.3%)	154 (21.2%)	190 (26.1%)	200 (27.5%)
Cerak	26 (22.2%)	21 (17.9%)	38 (32.5%)	32 (27.4%)
Vidikovac	81 (23.4%)	77 (22.3%)	77 (22.3%)	111 (32.1%)
Beograd	1284 (22.0%)	1038 (17.8%)	1655 (28.4%)	1849 (31.7%)

Kao poslednji primer, tabela 5 prikazuje nivoe enkripcije za AP šest proizvođača koji zajedno zauzimaju skoro tri četvrtine svih detektovanih bežičnih mreža. Među proizvođačima se izdvajaju „Askey Computers“ i „Intracom S.A.“, koji imaju preko 30% nezaštićenih mreža. Ovakvo odstupanje od opšteg trenda može se lako objasniti činjenicom da navedene kompanije predstavljaju proizvođače bežičnih ADSL modema-rutera koje je Telekom Srbija besplatno delio svojim korisnicima, sa inicijalno uključenim bežičnim delom modema. Mnogi korisnici nisu ni znali da emituju, odnosno nisu uopšte menjali konfiguraciju ADSL modema, o čemu svedoči i podatak da od nezaštićenih mreža proizvođača „Askey Computers“ 80% ima nepromenjeno inicijalno ime bežične mreže („HG520c“, „HG520i“ ili „HG520s“, u zavisnosti od verzije modema).

Bežični ADSL modemi proizvođača „Pirelli“, koje u skorije vreme korisnicima isporučuje Telekom Srbija, imaju inicijalno onemogućenu bežičnu mrežu, pa je broj nezaštićenih mreža kod ovog proizvođača smanjen na skoro polovinu prethodnog broja. Takođe, u okviru „Quick Setup“ programa prilikom inicijalnog podešavanja Pirelli modema, WEP zaštita nije ni ponuđena, već se, ukoliko je zaista nezaobilazna zbog postojanja starije opreme, mora podesiti u okviru naprednih podešavanja modema [7]. Zato i ne čudi da od svih proizvođača Pirelli ima najmanji broj korisnika koji koristi WEP zaštitu (svega 1%). Web podešavanja modema-rutera Pirelli predstavljaju primer dobre prakse sa stanovišta sigurnosti bežičnih mreža, gde je korisnicima otežano odabiranje nesigurnih tehnologija.

Tabela 5: Enkripcija i proizvođač opreme.

Proizvođač	Bez	WEP	WPA	WPA2
TP-Link	17%	25%	17%	42%
Askey Computers	31%	19%	37%	13%
Cisco-Linksys	26%	15%	22%	38%
D-Link	16%	22%	19%	43%
Pirelli	17%	1%	69%	13%
Intracom S.A.	34%	10%	7%	49%

ZAKLJUČAK

U radu je ispitano trenutno stanje sigurnosti bežičnih mreža u Beogradu. Merenja su vršena uz pomoć nekoliko laptop računara opremljenih bežičnim karticama i GPS prijemnicima. Trase kojima su se vozila kretala tokom merenja odabrane su tako da se omogući što veći i bolji uzorak bežičnih mreža u Beogradu. Zabeleženo je preko 6000 unikatnih bežičnih mreža u gradu i za svaku mrežu je zabeležena pozicija, ime, proizvođač bežičnog mrežnog uređaja, tip IEEE standarda koji koristi, kao i implementirani nivo enkripcije.

Tendencija porasta broja bežičnih mreža u Beogradu je evidentna imajući u vidu odnos broja mreža novijeg u odnosu na stariji standard. Globalni razvoj modernih telekomunikacionih i IT tehnologija nije zaobišao ni Beograd pa bi se prognozirana dalja ekspanzija ove tehnologije u svetu mogla očekivati i kod nas, pre svega na polju mobilnih uređaja, odnosno uređaja koji predstavljaju integraciju mobilnih telefona, foto-aparata i računara.

Bezbednost WI-FI mreža u Beogradu je iznenađujuće dobra u odnosu na očekivano stanje bezbednosti. Starije beogradske mreže su većinom potpuno nezaštićene (na MAC sloju standarda IEEE 802.11), a zaštićene mreže skoro ravnomerno koriste stari i prevaziđeni, odnosno nesigurni, WEP sistem zaštite, i novije WPA i WPA2 sisteme zaštite.

Novije mreže imaju značajno povećan nivo sigurnosti, pri čemu oko 60% mreža koristi naprednije (i sigurnije) metode zaštite na MAC sloju. Korišćenje WEP zaštite nije redukovano, što pokazuje relativni nedostatak informacija o sigurnosti pojedinih tehnologija kod kranjih korisnika. Finalno, preko petine bežičnih mreža novijeg standarda u Beogradu je i dalje potpuno nezaštićena, što, sa jedne strane može da čudi, ali, sa druge strane, postoje i korisnici kojima ne odgovara postojanje zaštite. Primer ovakvih korisnika su firme koje svojim mušterijama nude privremene usluge korišćenja pristupa internetu (ugostiteljske radnje i slično) i ne žele komplikovaniji pristup za korisnike koji se često menjaju (ukoliko je veoma lako dobiti šifru za pristup mreži, recimo uz plaćenu porudžbinu, onda je i sigurnost podataka koji se prenose takvom mrežom kompromitovana, pa se postavlja pitanje validnosti upotrebe zaštite).

Analizirana je i raspodela korišćenja enkripcije po raznim proizvođačima, pri čemu su se negativno izdvojili bežični modem-ruteri koje je u prethodnom periodu Telekom Srbija davao na korišćenje korisnicima svojih ADSL usluga. Sa druge strane, modemi-ruteri koje u poslednje vreme isporučuje Telekom Srbija navedeni su kao primer dobre prakse prilikom podešavanja bežičnih mreža.

Rezultati eventualnih budućih istraživanja bi mogli pokazati i tendenciju u zaštiti mreža, kao i stanje sigurnosti i raspodelu upotrebljenih frekvencijskih kanala najnovijeg IEEE 802.11n standarda. Takodje mogle bi, u skladu sa zakonom, biti ispitane i novopronađene ranjivosti WPA i WPA2 zaštita.

LITERATURA

[1] Tews, E. and Beck, M., "Practical attacks against WEP and WPA", in *Proc. of the Second ACM Conference on Wireless Network Security*, Zurich, Switzerland, 2009, pp. 79-86.

[2] J. R. Walker, "Unsafe at any key size; an analysis of the WEP encapsulation", *IEEE Document 802.11-00/362*, Oct. 2000.

[3] T. Ohigashi and M. Morii, "A practical message falsification attack on WPA." [Online]. Available: http://tinyurl.com/nban35

[4] "Krivični zakonik", *Službeni glasnik RS*, 85/05, Available: http://www.parlament.gov.rs/content/cir/akta/akta_detalji.asp?Id=285&t=Z#

[5] IEEE-SA Standards Board, "IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", Available: http://standards.ieee.org/getieee802/download/802.11-2007.pdf

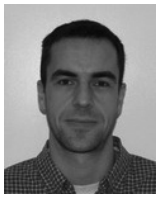
[6] Organizationally Unique Identifier (OUI) Listing, *IEEE Registration Authority*. Available: http://standards.ieee.org/regauth/oui/oui.txt

[7] Telekom Srbija, „Uputstvo za podešavanje modema Pirelli DRG A226G za bežični pristup" Available: http://www.open.telekom.rs/Dokumenta/isp/privatni/images/modemi/pirelli_uputstvo_za_korisnika_srpski.pdf

Dušan Švenda
Telekom Srbija, Beograd
e-mail: dusan.svenda@gmail.com
Oblasti interesovanja: bazne stanice, GSM, 3G telekomunikacije, CDMA, fiksni bežični pristup

Marko Derota
Visoka ICT, Beograd
e-mail: derota.marko@gmail.com
Oblasti interesovanja: Računarske mreže, administriranje sistema, IP telefonija

Aleksandar Glišić
Galeb GTE, Beograd
e-mail: acaglisic@gmail.com
Oblasti interesovanja: Bežične mreže, GSM, GPS



Dr Miroslav Djordjević,
Visoka ICT
e-mail: miroslav@ieee.org
Oblasti interesovanja: Numerička elektromagnetika, antene, propagacija radio talasa

infoM

UPUTSTVO ZA PRIPREMU RADA

1. Tekst pripremiti kao Word dokument, A4, u kodnom rasporedu 1250 latinica ili 1251 ćirilica, na srpskom jeziku, bez slika. Preporučen obim – oko 10 strana, single prored, font 11.
2. Naslov, abstakt (100-250 reči) i ključne reči (3-10) dati na srpskom i engleskom jeziku.
3. Jedino formatiranje teksta je normal, bold, italic i bolditalic, VELIKA i mala slova (tekst se naknadno prelama).
4. Mesta gde treba ubaciti slike, naglasiti u tekstu (Slika1...)
5. Slike pripremiti odvojeno, VAN teksta, imenovati ih kao u tekstu, radi identifikacije, u sledećim formatima: rasterske slike: jpg, tif, psd, u rezoluciji 300 dpi 1:1 (fotografije, ekranski prikazi i sl.), vektorske slike – cdr, ai, fh,eps (šeme i grafikoni).
6. Autor(i) treba da obavezno priloži svoju fotografiju (jpg oko 50 Kb), navede instituciju u kojoj radi, kontakt i 2-4 oblasti kojima se bavi.
7. Maksimalni broj autora po jednom radu je 5.

Redakcija časopisa Info M