HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Wardriving: jednostavno otkrivanje bežičnih mreža

CCERT-PUBDOC-2004-11-97

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.
Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

***LS&S*, www.lss.hr**- laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Kako se u posljednje dvije godine iznimno povećao broj bežičnih računalnih mreža, proporcionalno su porasle i potrebe za njihovom zaštitom. S obzirom da je poznato da bežične računalne mreže još uvijek posjeduju određene slabosti i nedostatke, zabrinutost onih koji su se odlučili na njihovu implementaciju potpuno je opravdana (pogotovo u poslovno informacijskim sustavima gdje se računalnom mrežom prenose osjetljivi podaci). Ostvarivanje besplatnog i brzog pristupa Internetu, ugrožavanje tajnosti, integriteta, i dostupnosti poslovnih podataka i razne druge maliciozne aktivnosti dovoljan su motiv za provođenjem postupaka otkrivanja nezaštićenih bežičnih mreža.
Jedna od aktivnosti koja u relativno kratkom vremenskom roku i uz vrlo malo financijskih sredstava omogućuje otkrivanje bežičnih mreža jest *wardriving*. *Wardriving* aktivnost opisana u ovom dokumentu ne zadire u pitanje neovlaštenog pristupa bežičnim mrežama, već samo u postupak njihova otkrivanja. Cilj dokumenta je ukazati na jednostavnost provođenja ovog postupka, informacije koje se sakupljaju, odgovornost izvođača *wardriving*-a te odgovornost vlasnika bežične mreže.

2. Wardriving općenito

Postoji nekoliko definicija *wardriving* aktivnosti. Jedna od definicija jest da je *wardriving* aktivnost otkrivanja bežičnih mreža pri kojoj se koristi automobil kao prijevozno sredstvo te oprema i programski alati potrebni za skeniranje radio frekvencije. Aktivnost je ušla u široku primjenu nakon što je Peter Shipley proveo istraživanje o bežičnim mrežama na sveučilištu Berkeley, California. Druga definicija *wardriving*-a kaže da je to aktivnost prikupljanja statističkih podataka o bežičnim mrežama na određenom geografskom području osluškivanjem njihovih javno dostupnih oznaka (eng. *beacon*).
Wardriving je naziv dobio po poznatoj *wardialing* tehnici koja se koristi za otkrivanje neovlašteno instaliranih modema putem kojih se pokušava ostvariti nelegitiman pristup zaštićenoj računalnoj mreži. *Wardriving* aktivnošću otkrivaju se pristupne točke (eng. *access point*) koje omogućuju pristup bežičnoj mreži. *Wardriving* se može promatrati kao aktivnost koji ima korisnu namjenu istraživanja napretka bežičnih mreža, kao i rasta tržišta bežičnih mreža. Statistički podaci o broju bežičnih mreža (zaštićenih ili nezaštićenih) u velikoj mjeri doprinose povećanju svijesti o sigurnosnim problemima takve vrste mreža. Njegovo izvođenje je svakako i zabava, ali takvim se može smatrati samo ako se koristi ispravna i odgovarajuća oprema te ne postoji namjera pristupa mreži otkrivenoj na ovaj način.

2.1. Oprema za wardriving

Za izvođenje aktivnosti potrebno je imati osnovnu opremu (eng. *wardriving rig*), koju čine prijenosno računalo (ili PDA) i bežična kartica te dodatnu opremu koju mogu činiti eksterna antena, GPS uređaj (*Global Postitioning System*), itd.
Konfiguracija prijenosnog računala nema općenitih zahtjeva niti postoji neka preporuka. Zahtjev koji treba biti zadovoljen je da prijenosno računalo ima ugrađenu bežičnu karticu ili da ima *PCMCIA* ili *USB* utor za eksternu bežičnu karticu.
Bežična kartica predstavlja uređaj koji omogućuje detektiranje pristupnih točaka bežičnih mreža tako da "osluškuje" frekvencije. Najvažnija specifikacija kartice je *chipset*. Trenutno najjači *chipset*-i koji se koristi za kartice su:

- *Hermes* kojeg koristi *Lucent*, *Dell*, *IBM* i *Sony*,
- *Prism* kojeg koristi *Intel*, *Linksys*, *NetGear*, *USRobotics*, *Zoom* i *SMC*, te
- *Aironet* kojeg koristi *Cisco*.

Od postojećih standarda za bežične mreže, preporučljivo je da je kartica IEEE 802.11b ili IEEE 802.11g standarda. Od kartica koje postoje na tržištu, izuzetno su popularne *Orinoco*, *Cisco*, *D-link*, *Trendnet*, itd. Svakako je pri izboru kartica potrebno obratiti pažnju na to ima li kartica priključak za eksternu antenu. Na slici 1 prikazana je bežična kartica *Orinoco Silver*.

Slika 1: Bežična kartica s *pigtail* kabelom

Eksterna antena je uređaj za primanje radio valova i koristi se opcionalno. Njeno korištenje povećava distancu pristupne točke i prijenosnog računala te domet koji se želi obuhvatiti. Postoji širok spektar antena po veličini, obliku i jačini signala. Obzirom da bežične mreže koriste 2.4 GHz radio-frekvencijski spektar, tada i antena mora podržavati istu frekvenciju. Postoji više kategorija antena: omni-direkciona, sektorska i usmjerena antena. Za potrebe *wardriving*-a obično se koristi omni-direkciona antena, a razlog je što ova vrsta "vidi" u svim smjerovima istovremeno pa omogućuje široko područje skeniranja pristupnih točaka.
Opći pojmovi koji su povezani uz eksterne antene su:

- decibel (dB) – veličina koja predstavlja logaritam odnosa dvaju snaga, u ovom slučaju predstavlja omjer jakog i slabog signala između dva komunikacijska uređaja,
- izotropna antena – antena koja ima radijalno zračenje od 360 stupnjeva,
- dBi vrijednost – omjer jačine antene u odnosu na izotropnu antenu; što je veća dBi vrijednost, veći je doseg antene.

Slika 2 prikazuje eksternu omni-direkcionu antenu.

Slika 2: Eksterna omni-direkciona antena

No, osim kupovine antene, moguće je izraditi "kućnu" antenu.
Spajanje eksterne antene s bežičnom karticom izvodi se pomoću kabela koji se zove *pigtail*. Taj kabel je izuzetno kratak jer su sastavne žice vrlo tanke, a dužina kabela obrnuto proporcionalno utječe na jačinu signala. Funkcija kabela jest adaptiranje konektora na strani kartice s konektorom na strani antene. Standardno, *pigtail* ima N ženski konektor.
Slika 3 prikazuje *pigtail* kabel s konektorima.

Slika 3:*Pigtail* kabel

Spajanjem opreme kreira se sustav koji omogućuje jednostavno otkrivanje bežičnih mreža, a prikazan je na slici 4.

Slika 4: Wardriving oprema

Programski alati za *wardriving* dijele se na komercijalne i *open sorce* alate. Neki od komercijalnih alata su *Sniffer Wireless*, *Airopeek*, itd. Od *open sorce* alata najpoznatiji su *Kismet*, *NetStumbler*, *Airsnort*, *Wellenreiter.* Slika 5 prikazuje uvodni dijaloški okvir alata *Network Stumbler*.

Slika 5: Uvodni dijaloški okvir alata *Network Stumbler*

Bitno je napomenuti da svakako, pri izboru alata za korištenje, treba uzeti u obzir i operacijski sustav. Puno je veći broj alata dostupan za Linux platforme, nego li za Windows operacijske sustave.
Mogućnost izvođenja aktivnosti temelji se na činjenici da su pristupne točke predefinirane tako da objavljuju svoju prisutnost u određenom intervalu (obično 100 ms) tako da odašilju paket koji sadrži njihov SSID (*Service Set IDentifier*) i ostale pripadajuće podatke (osim ako administrator mreže samostalno ne izmjeni konfiguraciju pristupne točke).
Korištenje prethodno navedene opreme omogućuje u relativno kratkom vremenskom roku (vremenski rok ovisi o opsegu područja kojim se vozi te volji sudionika *wardriving*-a), otkrivene mreže pojavljuju se u popisu sa svojim pripadajućim podacima: SSID-om, MAC adresom, jačinom signala, oznakom zaštite, itd.

2.2. Sudionici wardriving-a

Otkrivanje bežičnih mreža je, dakle, aktivnost kojom se sakupljaju podaci o količini pristupnih točaka. Potencijalno, ova aktivnost omogućuje neovlašteni pristup bežičnim mrežama. Ovisno o tome tko provodi *wardriving*, on ima pozitivnu ili negativnu konotaciju. Pozitivna konotacija *wardriving*-a je ta

što ovu aktivnost trebaju provoditi IT profesionalci kao temelj za daljnju izgradnju sigurnosti bežične mreže. Bezopasno ga koriste i ljudi koji iz zabave otkrivaju i bilježe rast broja pristupnih točaka. Negativna konotacija na snazi je kada *wardriving* provode ljudi s intencijom zlonamjernosti koji su u potrazi za nezaštićenom bežičnom mrežom čije će resurse neovlašteno koristiti. U skladu s navedenim namjerama otkrivanja bežičnih mreža, sudionike ovog postupka možemo podijeliti na tri glavne grupe:

- IT profesionalce,
- hobiste,
- zlonamjerne napadače.

3. Wardriving u praksi

Wardriving kojim će se prikazati praktičan način izvođenja aktivnosti proveden je u Gradu Rijeci. Cilj je bio prikazati kako se u kratkom vremenskom roku može na jednostavan način saznati broj pristupnih točaka te utvrditi da li one koriste bilo kakav oblik zaštite. Sam *wardriving* trajao je oko pola sata i obuhvaćao je prolaz manjim dijelom Grada Rijeke.

Pri provođenju aktivnosti koristila se, u nastavku, opisana oprema. Naglasak navedene opreme upravo je na tome da su korištene komponente koje bi imao prosječan poznavatelj bežičnih mreža i *wardriving*-a.

Osnovu predstavlja prijenosno računalo Asus A1000 s procesorom Pentium III, 600 MHz te s 128 MB RAM-a. *Orinoco Silver* je bežična kartica koja je također bila sastavni dio opreme. Ova kartica je idealna za *wardriving* jer ima mogućnost dodavanja eksterne antene putem *pigtail* kabela što je standardna opcija kartice. Kartica je dobavljiva u Hrvatskoj, a korištena je upravo stoga što izuzetno dobro obavlja svoj zadatak pod svim operacijskim sustavima.

Eksterna antena koja je korištena jest Pacific Wireless PAWOD24-12 antena. Svojstva korištene antene su da je to vertikalno polarizirana omni-direkciona antena za frekvencije od 2.4 do 2.485 GHz, jačine 12 dB, ima integrirani konektor tipa N, lagana je, vodootporna, radi na temperaturi od -40 do +70° C, dužine je 122 cm, a teška je 0.6 kg.

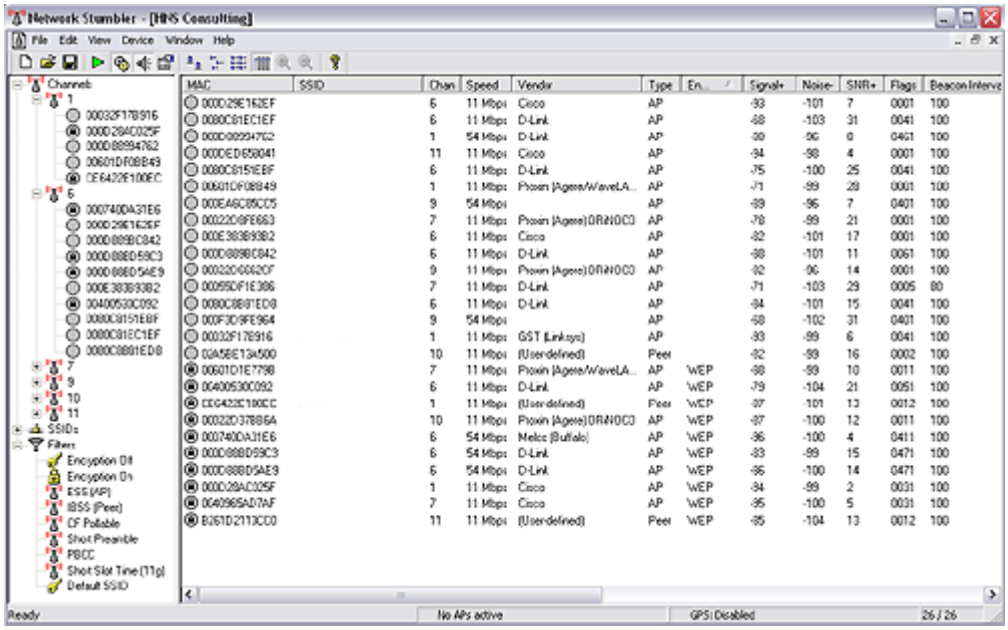
Obzirom da je Windows operacijski sustav još uvijek zastupljeniji od ostalih operacijskih sustava, i u ovom postupku korišten je upravo taj inačice XP s instaliranom sigurnosnom zakrpom *Service Pack* 1.

Za Windows operacijske sustave preporučljiv programski alat za izvođenje *wardriving*-a svakako je *Netstumbler* (*Network Stumbler*, čiji je autor Marius Milner). *Netstumbler* je službeno definiran kao alat za otkrivanje bežičnih mreža i njihovu analizu. Najpopularnija kombinacija za njegovo korištenje je Windows operacijski sustav i *Hermes* ili *Aironet chipset* kartica. Besplatan je i lak za instalaciju. Njegova funkcionalnost temelji se na IEEE 802.11b i IEEE 802.11g standardu na način da emitira ispitnu poruku (eng. *probe request*) te zahtjeva od pristupnih točaka da pošalju odgovor. Pristupne točke konfigurirane su predefinirano tako da šalju odgovor ispitnim porukama. Ovaj alat podržava aktivno skeniranje bežičnih pristupnih točaka, GPS, ima izuzetno dobro grafičko sučelje, grafički mjerač jačine signala, itd. Osim za *wardriving*, koristi se i za detekciju lažno postavljenih pristupnih točaka (eng. *rogue access point*). U ovom slučaju *wardriving*-a korišten je upravo ovaj alat.

Kao što je spomenuto, *wardriving* je proveden na području Grada Rijeke, a obuhvaćeni su dijelovi grada s početkom na Turniću, širi centar grada te Vežica.

4. Statistički podaci izvedenog otkrivanja bežičnih mreža

U vremenskom intervalu od pola sata otkriveno je ukupno 26 pristupnih točaka. Od tog broja, 10 ih je zaštićeno, a 16 je nezaštićeno. Na slici 6 prikazano je sučelje alata *Netstumbler* s rezultatima postupka bez vrijednosti polja SSID.



Slika 6: Sučelje programa NetStumbler s rezultatima otkrivanja

Podaci koje su prikazani u sučelju alata su:

- MAC adresa pristupne točke (*Machine Address Code*) – jedinstvena adresa sklopovlja,
- SSID pristupne točke (*SSID*) – naziv bežične mreže,
- kanal (*Chan*) – broj kanala na kojem mreža radi koji za IEEE 802.11b standard iznosi od 1 do 13,
- brzina prijenosa podataka (*Speed*) – maksimalna brzina prijenosa u Mbps,
- proizvođač opreme (*Vendor*),
- tip opreme (*Type*),
- enkripcija (*Encryption*) – oznaka koja označava zaštićenu mrežu (*Wired Equivalency Privacy*, *WEP* ili *Wi-Fi Protected Access*, *WPA*),
- signal (*Signal+*) – maksimalan RF signal,
- buka (*Noise-*) – minimum RF buke,
- SNR – maksimalan RF *signal-to-noise* odnos,
- oznaka (*Flags*) – 802.11 oznaka u heksadecimalnom kodu,
- interval slanja odgovora na ispitnu poruku (*Beacon Interval*).

Sučelje alata prikazuje slijedeće statističke podatke (u odnosu na ukupan broj od 26 pristupnih točaka):

- korišteni kanali su 1 (5 AP), 6 (10 AP), 7 (4 AP), 9 (3 AP), 10 (2 AP) i 11 (2 AP),
- 20 pristupnih točaka ima brzinu od 11 Mbps, a 6 brzinu od 54 Mbps,
- zastupljeni proizvođači opreme su Cisco, D-link, Proxim, GST i Melco,
- prema tipu opreme 25 je pristupnih točaka, a 1 je *peer-to-peer*,
- WEP-om ili WPA-om je zaštićeno 10 pristupnih točaka (iako je zaštita WEP-om vrlo upitna),
- 1 pristupna točka ima interval slanja odgovora od 80 ms, dok ostale imaju standardnu vrijednost od 100 ms.

Slika 7 prikazuje sažete rezultate aktivnosti.

Ukupan broj AC-a	26
Zaštićeno	10
Nezaštićeno	16
Predefinirani SSID	5
Predefinirani SSID i nezaštićeno	5

Slika 7: Rezultati *wardriving*-a dijela Grada Rijeke 2004. godine

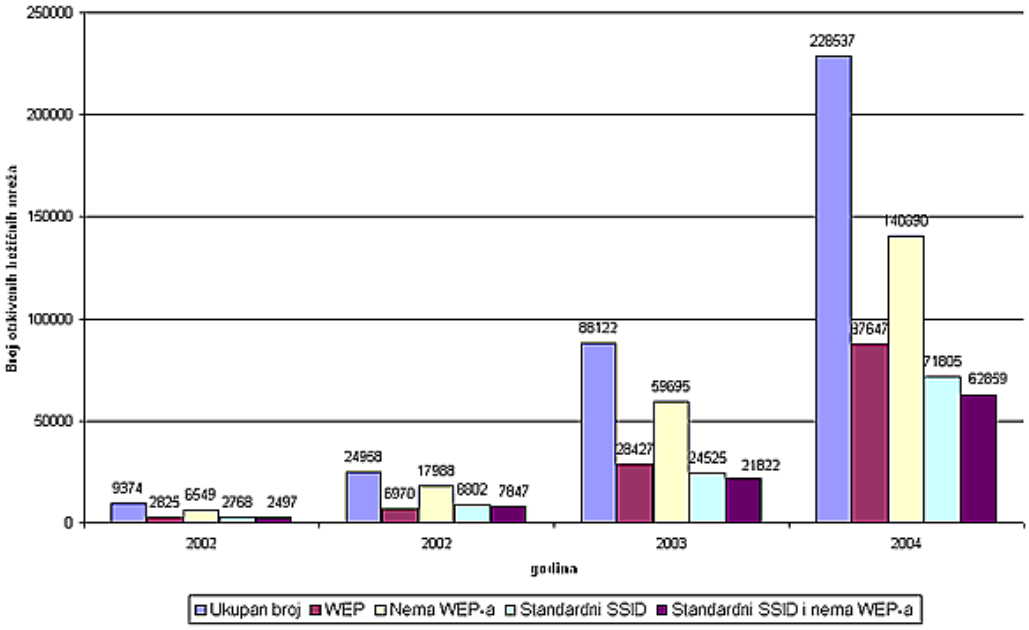
Što se sve krije iza tih mreža, u ovom slučaju nije testirano niti se uopće preporučuje bilo kakav pristup otkrivenoj mreži, iz pravnih i etičkih razloga. Obzirom da pristupna točka predstavlja *gateway* LAN-u, uobičajeno je se iza toga krije pristup računalima koja sadrže korisnička imena, zaporke, povjerljive dokumente, financijske podatke, jednom riječju, organizaciji bitni podaci i informacije za koje vrijedi uspostaviti sustav sigurnosne zaštite koje će barem otežati pristup zlonamjernim napadačima, ako ga sasvim ne uklone.

5. Svjetski trendovi

Osim *wardriving*-a, u svijetu se koriste alternativne metode za otkrivanje bežičnih mreža kao što su *warwalking*, *warflying* ili korištenje sredstava javnog prijevoza (tramvaj, autobus).
Veliku zanimljivost predstavljaju organizirana natjecanja u *wardriving*-u u kojima natjecatelji sakupljaju bodove za otkrivene pristupne točke, a broj bodova ovisi i o konfiguraciji otkrivenih pristupnih točaka. Jedno takvo natjecanje organizirano je u sklopu *DefCon*-a kojeg je sponzorirala ekipa *Netstumbler*-a s antenama, bežičnim karticama s *pigtail* kabelima i majicama kao nagradama.
U kolovozu 2002. godine po prvi puta provedeno je natjecanje *WorldWide WarDrive 1 (WWWD1)* koje je obuhvatilo 6 zemlja na dva kontinenta (Sjeverna Amerika i Europa).
Rezultati natjecanja su impresivni. Otkriveno je 9.374 pristupnih točaka, od kojih je 2.825 imalo WEP enkripciju (30,13%), a 2.768 (29,53%) je imalo predefiniran SSID. *WorldWide WarDrive 2 (WWWD2)* natjecanje održano u listopadu 2002. godine u kojem su sudjelovali sudionici s četiri kontinenta otkrilo je 24.958 pristupnih točaka, od kojih je samo 27,92% bilo enkriptirano. *WWWD3* natjecanje održano u srpnju 2003. godine pokazalo je da se broj pristupnih točaka povećava, otkriveno je njih 88.122, a sigurnost ostaje na vrlo niskom nivou, samo 27.92% imalo je WEP. Ove godine natjecanje je održano u lipnju, pod imenom *WWWD4*, a ukupan broj otkrivenih pristupnih točaka je 228.537, od čega je 38,3% zaštićeno WEP-om. Rezultati za svih *WWWD* natjecanja prikazani su u tablici na slici 8 te grafikonom na slici 9.

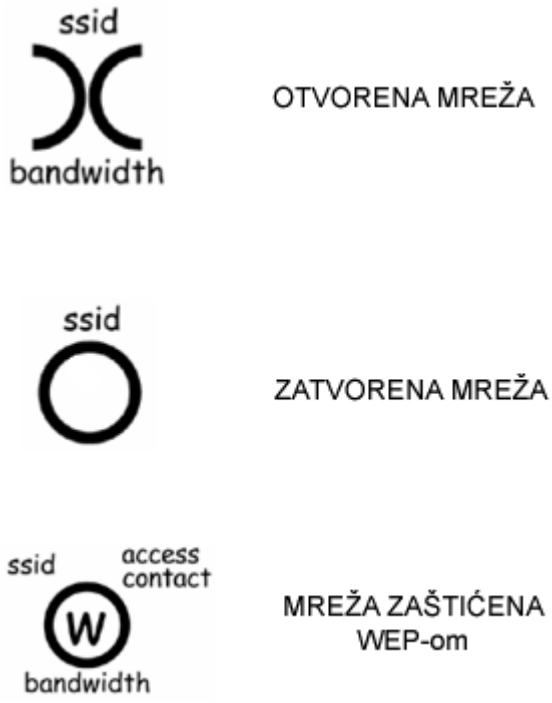
Godina	2002	2002	2003	2004
Ukupan broj AC-a	9.374	24.958	88.122	228.537
Zaštićeno	2.825	6.970	28.427	87.647
Nezaštićeno	6.549	17.988	59.695	140.890
Predefinirani SSID	2.768	8.802	24.525	71.805
Predefinirani SSID i nezaštićeno	2.497	7.847	21.822	62.859

Slika 8: Rezultati natjecanja WWWD od 2002. do 2004. godine



Slika 9: Rezultati natjecanja WWWD od 2002. do 2004. godine

Sudionici *wardriving*-a i njemu sličnih aktivnosti otkrivanja bežičnih mreža u svijetu su razvili i svoj jezik poznat pod imenom *warchalking*. Svrha jezika je međusobno pružanje pomoći u otkrivanju bežičnih mreža, a sastoji se od crtanja jednostavnih simbola na javnim površinama (zgrada, ulica, zid) u blizini pristupne točke. Simboli prikazuju informaciju o mreži te ostalim sudionicima olakšavaju daljnje otkrivanje. Naravno, ovaj jezik simbola podijelio je publiku na dva tabora. Jedni smatraju da *warchalking* zaista postoji, dok drugi imaju mišljenje da je on produkt medija. Simboli *warchalking*-a prikazani su na slici 10.



Slika 10: Warchalking simboli i značenje

6. Zakonska regulativa

Pojavom novih tehnologija izuzetno je bitno definirati kako se trenutno važeća zakonska regulativa bavi pitanjima koje novine postavljaju. Kako raste tržište bežičnih mreža, aplikacija i sklopovlja, tako raste potreba za razumijevanjem pravne prakse za aktivnosti koje zadiru u bežične mreže, a naročito u *wardriving*.

Zakonska regulativa koja je primjenjiva na bežične mreže je Zakon o telekomunikacijama (NN, 122/03) i to člancima u kojima se propisuje otvorena radio frekvencija te izračena snaga antene. U skladu s time, korištenje antene prilikom izvođenja *wardriving*-a nije nelegalna akcija ukoliko antena koristi frekvenciju koja je navedenim zakonom definirana kao otvorena te je u granicama dopuštene izračene snage.

Wardriving kao postupak otkrivanja mreže nije nelegalna akcija dok god ne postoji intencija povrede integriteta, povjerljivosti i dostupnosti informacijskih resursa organizacije. Točnije, pristupne točke bežičnih mreža su javno pristupne točke bežične mreže. Postupak kojim osoba, korištenjem legalne opreme za slanje aktivnog upita pristupnoj točki, dobije informacije o identifikaciji jest legalan postupak jer se javno pristupne točke na upit moraju identificirati. FBI također smatra da, na teritoriju Sjedinjenih Američkih Država, skeniranje pristupnih točaka nije nelegalna radnja.

Kaznena odgovornost izvođača *wardriving*-a može se utvrditi zakonima koji propisuju kaznena djela (npr. Kazneni zakon, NN 110/97) isključivo u slučaju kada je osoba izvela zlonamjernu akciju u kojoj je ugrožen integritet, povjerljivost i dostupnost resursa tj. za radnje poduzete nakon samog postupka otkrivanja pristupnih točaka. Pri tome je važno obratiti pozornost za zaštitu bežične mreže. Ukoliko vlasnik bežične mreže nije omogućio njenu zaštitu na odgovarajući način, osoba koja je koristila resurse bežične mreže u vlastite svrhe kazneno ne odgovora, ali se time ulazi u sferu građanske odgovornosti prema Zakonu o obaveznim odnosima (NN 3/94) i Zakonu o vlasništvu i drugim stvarnim pravim (NN 91/96).

Kako bi se osoba koja skenira pristupne točke radi sakupljanja statističkih podataka u znanstvene ili edukativne svrhe sigurno zadržala u legalnim granicama, potrebno je držati se četiri osnovna pravila:

- ne provaljuj (ne smije se ostvariti nelegalan pristup mreži)
- ne gledaj (ne smije se ispitivati sadržaj mreže),
- ne diraj (ne smije se dodavati, brisati ili mijenjati bilo što na mreži),
- ne igraj se (ne smije se koristiti Internet pristup u vlastite svrhe).

Sva navedena pravila ponašanja mogu se svesti na jedno glavno pravilo koje glasi – ne spajaj se na otkrivenu mrežu.

7. Zaključak

Broj bežičnih mreža svakodnevno se povećava u svijetu, a porast je i u Hrvatskoj. U prilog tome govori i velik broj *wireless* udruga kojih je trenutno 31 (prema podacima Hrvatske udruge korisnika bežičnih mreža do 30. listopada 2004. godine). Činjenica je da je i *wardriving* kao aktivnost vrlo zabavna i stječe veliki broj poklonika koji žele sudjelovati u otkrivanju bežičnih mreža uz niske troškove i minimalna tehnička znanja. Pitanje je vremena da li će se i kada će se natjecanja koja su veliki hit u svijetu, organizirati i u Hrvatskoj. *Wardriving* ipak treba shvatiti kao jednostavan način otkrivanja bežičnih mreža u svrhu organizacije njihove zaštite te sakupljanje statističkih informacija o povećanju broja njihove implementacije. S pravnog stajališta, obzirom da je kazneno odgovorna samo ona osoba koja zlonamjerno ostvari pristup mreži koja je prethodno zaštićena, vlasnicima bežičnih mreža preporučuje se da ostvare odgovarajući nivo sigurnosti.

8. Reference

[1] Chris Hurley, Michael Puchol, Russ Rogers and Frank Thornton: WarDriving: Drive, Detect, Defend: A Guide to Wireless Security, Syngress Publishing 2004

[2] Etter, Andrew: A Guide to Wardriving and detecting wardrivers, http://www.sans.org/rr/papers/68/174.pdf

[3] Fred: Wardriving Howto, http://www.wardriving.com/doc/Wardriving-HOWTO.txt

[4] Montcalm, Erik: How to avoid ethical and legal isus in wireless network discovery http://www.sans.org/rr/papers/index.php?id=176

[5] Hrvatska udruga korisnika bežičnih mreža, http://www.wifihr.net/index.php
[6] Šupica Žaklina, Kučan Berislav, Žorž Mirko: Wardriving: jednostavno otkrivanje bežičnih mreža, Zbornik radova KOM 2004, Opatija, 2004.
[7] Netstumbler, http://www.netstumbler.org/
[8] Wikipedia, http://en.wikipedia.org/wiki/Wardriving
[9] FAQ's, http://faq.wardrive.net/
[10] Narodne novine, http://www.nn.hr