HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sustavi za detekciju neovlaštenih aktivnosti na bežičnim računalnim mrežama

CCERT-PUBDOC-2004-07-83

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

Bežične računalne mreže zauzimaju sve veći udio u području računalne komunikacije, kako u velikim tvrtkama, tako i u manjim (kućnim) uredima. Tome prvenstveno doprinosi njihova niža cijena u odnosu na klasična rješenja koja koriste električne kabele kao medije za komunikaciju, ali i jednostavnost njihove instalacije i upotrebe.

Osim brojnih prednosti, korištenje bežičnih računalnih mreža u sustav unosi i nove sigurnosne rizike i prijetnje koje treba uzeti u obzir. Rizik po bežične mreže predstavljaju inherentne slabosti protokola za zaštitu bežične komunikacije, kao i činjenica da je praktički nemoguće onemogućiti fizički pristup neovlaštenim korisnicima. Mnoge tradicionalne metode zaštite koje se primjenjuju na klasičnim računalnim mrežama, u slučaju korištenja loše podešenih bežičnih mreža, nemaju nikakvog efekta protiv malicioznih korisnika koji na mrežu dolaze putem bežičnih komunikacijskih kanala.

Dokument opisuje osnovne napade vezane uz bežične računalne sustave, tehnike praćenja prometa na istima te mogućnosti detekcije malicioznih aktivnosti. Uz same tehnike, dan je i kratak pregled nekih poznatijih alata koji se koriste u ovu svrhu zajedno s njihovim osnovnim karakteristikama i područjem primjene.

2. Najčešći napadi na bežične mreže

Napadi koji se najčešće primjenjuju kod bežičnih računalnih mreža mogu se svrstati u sljedeće grupe:

- Faza izviđanja – podrazumijeva postupke pregledavanja portova te identifikaciju operacijskih sustava na ciljnim računalima. Eksponiranost računala na ovaj tip napada identična je kao i na klasičnim "žičanim" mrežama,
- Presretanje ili prisluškivanje mrežnog prometa – postupak identičan prisluškivanju prometa na žičanim mrežama. Zbog činjenice da se kod bežičnog prometa komunikacija odvija putem etera, postupak prisluškivanja mrežnog prometa mnogo je lakše izvesti nego što je to slučaj na žičanim računalnim mrežama gdje je potreban fizički pristup sustavu.
- Umetanje poruka i krivotvorenje sjednica,
- Maskiranje poslužitelja,
- Napadi uskraćivanjem usluga.

Ovisno o metodama i načinima provođenja, neke od navedenih napada jednako je teško ostvariti kao i na klasičnim žičanim mrežama, dok je neke od njih mnogo lakše provesti s obzirom na osnovne karakteristike bežičnih mreža i sigurnosne probleme koji se javljaju u ovom području.

2.1. Faza izviđanja

Za razliku od Interneta kao javne mreže, lokalne računalne mreže (LAN) podrazumijevaju određenu razinu privatnosti korisnika koji se njima služe i kao takve najčešće su odvojene i zaštićene od pristupa s javnog Interneta. Uobičajeno je da, zbog navedene privatnosti, operacijski sustavi i servisi na računalima povezanim u lokalnu računalnu mrežu nisu dodatno "ojačani" posebnim mjerama, kao što je to najčešće slučaj sa javno dostupnim računalima. Slične pretpostavke podrazumijevaju se i kod bežičnih lokalnih računalnih mreža (WLAN). Također, zbog radio signala koji doseže mnogo dalje od granica same zgrade u kojoj je bežična mreža implementirana, kod bežičnih računalnih mreža gotovo je nemoguće očuvati zadovoljavajuću razinu privatnosti.

U fazi izviđanja neovlašteni korisnici, koristeći se prijenosnim računalom i bežičnom mrežnom karticom, nastoje locirati odgovarajuću bežičnu računalnu mrežu i prikupiti što više korisnih podataka o načinu njenog funkcioniranja. Ovakav oblik neovlaštene aktivnosti naziva se War Drivig. Za provođenje War Driving napada najčešće se koriste alati kao što je Netstumbler (www.netstumbler.org). Dodatni problem predstavlja i činjenica da za provođenje navedenih radnji nije potrebno posebno iskustvo ili vještina, već je i prilično neiskusan haker u mogućnosti vrlo lako doći do korisnih informacija o ciljnoj mreži.

Od ovakve vrste napada vrlo se teško (gotovo nemoguće) zaštititi. Kao moguća mjera smanjenja sigurnosnog rizika može se primijeniti razmještanje bežičnih pristupnih točaka (engl. *Access point*) tako da njihovo zračenje izvan fizičkih granica zgrade bude minimalno, kao i korištenje usmjerenih antena u svrhu smanjenja rasipanja radio valova.

2.2. Presretanje ili prisluškivanje mrežnog prometa

Jednom kada je bežična mreža locirana, koriste se pasivne tehnike identifikacije aktivnih računala i otvorenih mrežnih portova prisluškivanjem mrežnog prometa. Na ovaj način moguće je prikupiti korisne podatke kao što su IP i MAC adrese računala na bežičnoj mreži, ali i vrlo osjetljive korisničke podatke kao što su korisnička imena, zaporke i sl. Analizom prikupljenog mrežnog prometa moguće je utvrditi i postavke mrežnih uređaja i eventualne restrikcije pristupa prema IP ili MAC adresama.

Budući da postupak pasivnog skeniranja nije moguće detektirati, poželjna je enkripcija mrežnog prometa kako bi se neovlaštenim korisnicima onemogućilo provođenje ovakvih aktivnosti. Standardne metode poput WEP (engl. *Wired Equivalent Privacy*) enkripcije pokazale su se ranjivima i vrlo jednostavnim za dekodiranje na mrežama sa pojačanim prometom. Zbog toga je poželjno primijeniti neku od dodatnih metoda enkripcije na višim mrežnim slojevima, kao što je npr. tuneliranje prometa korištenjem virtualnih privatnih mreža (engl. *Virtual Private Network*).

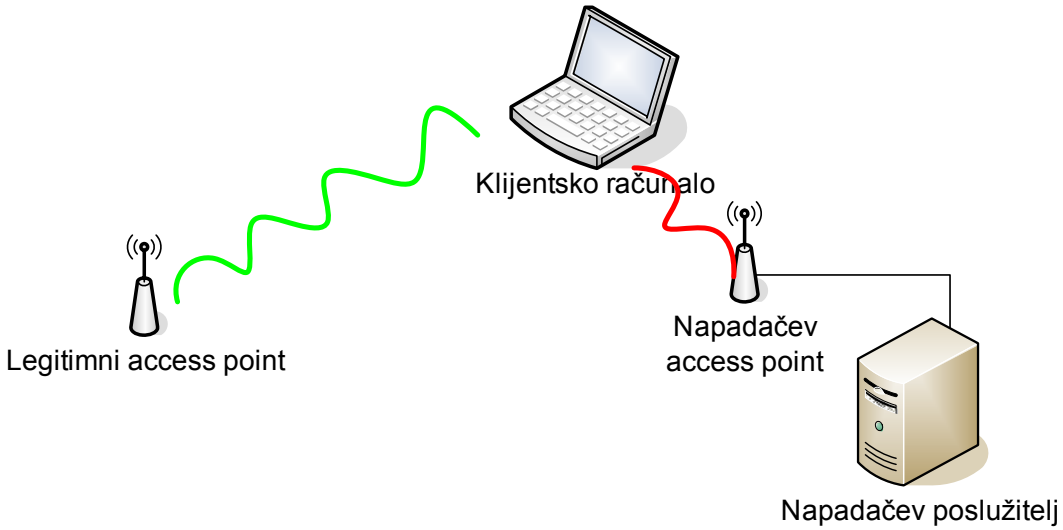
2.3. Umetanje poruka i krivotvorenje sjednica

Umetanje poruka podrazumijeva kreiranje specijalno osmišljenih mrežnih paketa i njihovo ubacivanje u komunikacijski kanal između dvije točke komunikacije (npr. između klijenta i poslužitelja). Maliciozne pakete korisnikovo će računalo, tj. korisnik prepoznati kao legitiman mrežni promet i kao takav, tretirati ga vjerodostojnim. Na taj način, moguće je provesti otimanje korisničke sjednice, što je kod servisa koji koriste UDP protokol relativno lako izvedivo.

2.4. Maskiranje poslužitelja

Uz otimanje sjednica i krivotvorenje poruka, veliku opasnost predstavljaju i tehnike maskiranja poslužitelja kao što je npr. *DNS spoofing* napad. Napadi ovakvog tipa najčešće se koriste za preusmjeravanje legitimnog prometa na napadačevo računalo s ciljem prikupljanja osjetljivih korisničkih podataka ili kompromitiranje korisničkog računala.

Kao i kod ostalih napada, činjenica da se radi o bežičnoj mreži dodatno olakšava provođenje napada. Jedan od napada specifičnih za bežične mreže je krivotvorenje ili lažiranje *access point* uređaja (**Slika 1**). Radne stanice na bežičnoj mreži tipično su podešene za *auto-associate* način rada, u kojem se priključuju na najbliži legitimni pristupni uređaj, tj. onaj sa najjačim signalom. Ukoliko korisnik postavi malicioznu pristupnu točku, podešenu da se ponaša identično kao i ona legitimna i da pritom nadjača njen signal radna stanica će se umjesto sa legitimnom povezati sa malicioznom pristupnom točkom. Na taj način vrlo efektno se može provesti tzv MitM (engl. *Man-in-the-middle*) tip napada, koji neovlašteni korisnik može iskoristiti za dolazak do povjerljivih korisničkih podataka. Rizik dodatno povećava i postojanje gotovih programa (npr. Monkey_jack) koji i manje iskusnim korisnicima olakšavaju provođenje ovakvog tipa napada.



Slika 1: *Krivotvorenje access point uređaja i maskiranje malicioznog poslužitelja*

2.5. Napadi uskraćivanjem usluga

Osim standardnih napada uskraćivanjem računalnih resursa, postoji i posebna skupina napada na koje su bežične računalne mreže dodatno ranjive. Takvi napadi tipično obuhvaćaju preplavljivanje pristupnih točaka različitim oblicima mrežnih paketa (de-autentikacijskim zahtjevima, neispravnim autentikacijskim zahtjevima, slanjem posebno oblikovanih *beacon* paketa koji stvaraju privid velikog broja nepostojećih pristupnih točaka i sl.). Već i samo emitiranje šuma, tj. radio smetnji na frekvenciji rada bežičnih računalnih mreža, u mogućnosti je zagušiti promet i u potpunosti onemogućiti rad mreže.

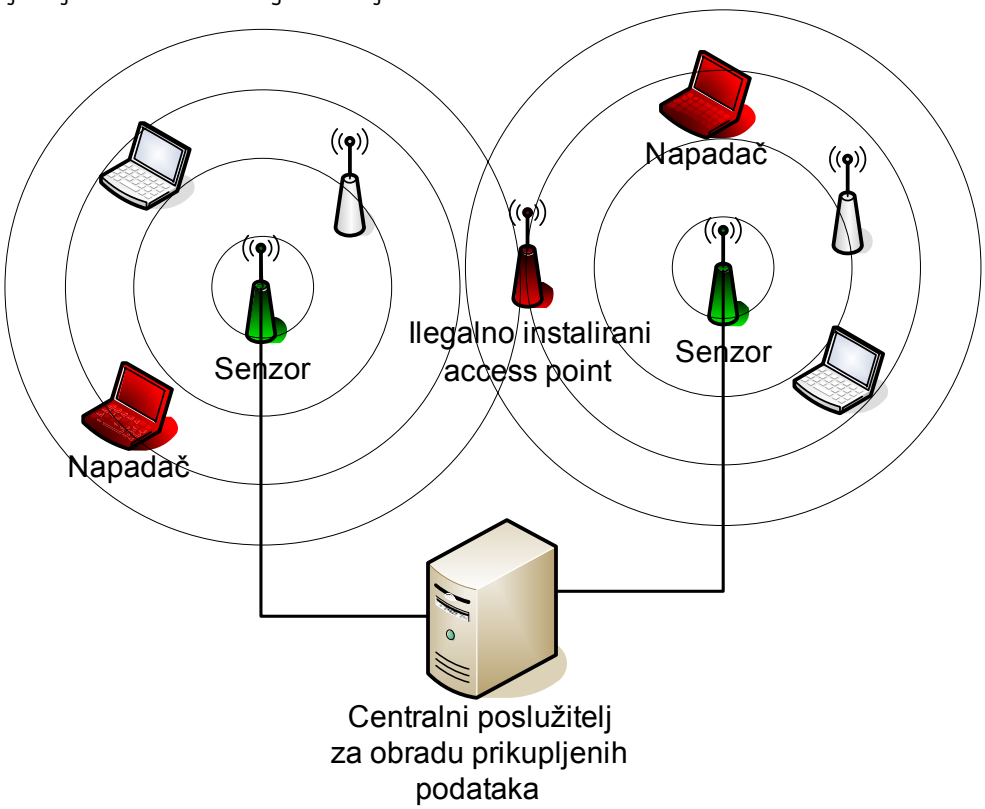
Protiv ovakvog oblika napada vrlo se teško zaštititi, budući da je neovlaštenim korisnicima gotovo nemoguće zabraniti pristup bežičnim mrežnim uređajima.

3. Koncept bežičnih IDS sustava

U daljnjem tekstu opisan je koncept idealnog bežičnog IDS (engl. *Intrusion Detection System*) sustava. Budući da trenutno ovakav sustav u praksi još nije izveden, sljedeće poglavlje donosi opis nekoliko konkretnih rješenja temeljenih na ovom konceptu.

3.1. Fizička arhitektura

Prvi korak kod uspješnog praćenja bežičnog mrežnog prometa je pažljivo razmještanje senzora. Senzorski uređaji moraju biti sposobni prisluškivati bežični mrežni promet i prosljeđivati ga centralnom poslužitelju na obradu (**Slika 2**). Obrada prikupljenih informacija moguća je i na samom senzorskom uređaju, ali ovakav pristup podiže njegovu cijenu i u slučaju velikih mreža čini takvo IDS rješenje neadekvatnim zbog visoke cijene.



Slika 2: *Fizička arhitektura bežičnog IDS sustava*

Budući da se napadač može nalaziti na bilo kojoj lokaciji unutar, ili u blizini objekta u kojem je bežična mreža implementirana, potrebno je osigurati pravilan raspored senzora. U većini slučajeva broj senzora jednak je broju instaliranih pristupnih točaka i u takvoj konfiguraciji senzori se smještaju u neposrednu blizinu svakog od njih. Na taj način pokriva se cjelokupno područje dometa bežične mreže. U slučaju da bežična mreža ne pokriva cijeli objekt, senzore je dodatno potrebno razmjestiti i u dijelove objekta u kojima nema pristupnih uređaja. Ovakav pristup neizbježan je ukoliko se žele uočiti bežični mrežni uređaji koje neovlašteni korisnici mogu instalirati praktički svugdje gdje je dostupna klasična žičana mreža.

Korisna, no ne i obavezna opcija je mogućnost senzora da istovremeno prati sve mrežne kanale. Nažalost zbog specifične i relativno skupe opreme ovakav pristup se često odbacuje. Osim visoke cijene, u prilog praćenju prometa na samo jednom kanalu ide i činjenica da se većina "zanimljivog" prometa odvija isključivo na kanalu koji se koristi od strane legitimne bežične mreže. Budući da većina programa za otkrivanje bežičnih mreža korištenih od strane neovlaštenih korisnika odašilje

promet na svim kanalima, praćenjem prometa na samo jednom kanalu moguće je detektirati i ovakvu vrstu aktivnosti.

3.2. Detekcija neovlaštenih aktivnosti

Jednom kada je uspostavljena prikladna fizička pokrivenost mreže IDS senzorima, može se pristupiti fazi prikupljanja podataka i njihovoj obradi.

Detekcija neovlaštenih aktivnosti na bežičnoj mreži odvija se na više mrežnih slojeva. Osnovna razina detekcije obuhvaća praćenje MAC adresa mrežnih kartica koje se pokušavaju povezati na računalnu mrežu. Pregledavanjem lista dozvoljenih i zabranjenih adresa moguće je prepoznati potencijalnog uljeza. Ovakva metoda nije praktična za velike sustave sa mnogo korisnika bežične mreže. Velik broj mrežnih kartica zahtijevao bi čestu brigu oko održavanja liste dozvoljenih kartica, što može smanjiti cjelokupnu efikasnost sustava. Ipak, MAC adrese nisu u potpunosti nasumično odabrane. Prva tri bajta adrese dodijeljena su pojedinom proizvođaču mrežne opreme, a oni za svoje potrebe uglavnom upotrebljavaju određen, unaprijed poznat, broj adresa. Poznavanjem ovih parametara provodi se provjera MAC adrese pomoću koje je moguće odrediti da li je adresa legitimna, ili nasumce generirana od strane uljeza.

Prepoznavanje pasivnih uljeza koji prisluškuju mrežni promet gotovo je nemoguće, ali zbog određenih manjkavosti u upravljačkim programima većine mrežnih kartica, postoji metoda kojom je i ovakve korisnike moguće detektirati i pratiti. IEEE 802.11b standard definira *Request to Send* (RTS) i *Clear to Send* (CTS) okvira pomoću kojih se provjerava potrebna propusnost medija i rezervira vremenski okvir za slanje podataka. Na svaki primljeni RTS okvir, bežični mrežni uređaj odgovara CTS okvirom. Odgovor je u većini slučajeva generiran od strane upravljačkog programa kartice i korisnikov softver nema kontrolu nad njime. Drugim riječima, ukoliko se primijeti postojanje određene MAC adrese na mreži, uzastopnim slanjem RTS paketa na tu adresu, moguće je locirati uljeza čak i kada je mrežna kartica postavljena u tzv. *monitoring* način rada za prisluškivanje mrežnog prometa.

Treća razina praćenja je provjeravanje sadržaja prometa koje, ukoliko je pažljivo izvedeno, može otkriti mnogo korisnih podataka o potencijalnom napadu na sustav. Praćenjem prometa moguće je detektirati sumnjiv mrežni promet, poput nasumičnih upita koji ukazuju na uljeza koji skenira mrežu ili bio kakve druge anomalije u njenom radu. Ovakav tip praćenja prometa već je razvijen za više mrežne slojeve kod klasičnih IDS sustava. Za potrebe bežičnih IDS sustava, ovu metodu potrebno je primijeniti za autentikaciju kod IEEE 802.11b protokola i primjerice praćenje RTS/CTS okvira.

Kada se sustav za praćenje i pregledavanje prometa uspostavi, potrebno je kreirati odgovarajuće potpise pomoću kojih se napadi prepoznaju. Proces kreiranja potpisa uobičajena je stvar kod klasičnih IDS sustava i ne razlikuje se niti kod bežičnih inačica.

Važan zahtjev koji se postavlja pred bežične IDS sustave je poznavanje fizičke lokacije napadača. Poznavanje ovog parametra značajno je zbog provođenja aktivne zaštite, kao i lakšeg razlučivanja napadača koji se nalazi izvan objekta u kojem je sustav instaliran, od zaposlenika koji se koristi neregistriranom mrežnom karticom. Pravilnim razmještajem IDS senzora, centralni sustav vrlo lako može izračunati približnu lokaciju napadača i na taj način pridonijeti preciznosti detekcije.

Pri praktičnoj realizaciji bežičnog IDS sustava potrebno je obratiti pozornost na sve gore navedene metode detekcije kako bi se postigla maksimalna efikasnost sustava.

3.3. Aktivna zaštita

Standardni IDS sustavi uglavnom koriste pasivne oblike zaštite poput bilježenja napada u log datoteke i uzbunjivanja administratora sustava u stvarnom vremenu. Iako bežični IDS sustavi također posjeduju ove funkcionalnosti, zbog smanjene fizičke sigurnosti bežičnih mreža i u određenim slučajevima nemogućnosti lociranja neovlaštenog korisnika, ponekad je neophodna primjena aktivnog odgovora na uočenu prijetnju (engl. *Intrusion response*).

Najefikasnija aktivna zaštita je fizički odgovor na detektirane neovlaštene aktivnosti. Većina napada na bežične mreže odvija se u neposrednoj blizini objekta u kojem se mreža nalazi i u vrlo kratkom vremenskom periodu. Analizom signala sa nekoliko senzora i poznavanjem njihove fizičke lokacije, moguće je vrlo brzo odrediti približan položaj neovlaštenog korisnika te ga identificirati.

U slučaju nemogućnosti fizičkog odgovora, najjednostavnije je nesigurnost bežičnih mreža iskoristiti protiv samog neovlaštenog korisnika. Iako najjednostavniji, klasični *flooding* napadi, kao odgovor na

prijetnju se ne preporučuju zbog mogućnosti zagušenja čitave mreže. Kao alternativa *flooding* napadima, može se koristiti slanje pažljivo oblikovanih malicioznih paketa izravno prema neovlaštenom korisniku što će u slučaju uspješnog iskorištavanja ranjivosti unutar 802.11b protokola izazvati nasilan prekid rada softvera na uljezovom računalu (engl. *crash*). Ukoliko se uljez uspješno prijavio na mrežu, praćenjem prometa moguće je približno odrediti vrstu i inačicu njegovog operacijskog sustava, što također otvara mogućnosti za napad i onemogućavanje rada istog.
Važan aspekt aktivne zaštite predstavlja i ometanje neovlaštenih korisnika koji prisluškuju mrežni promet. Budući da su u tom slučaju mrežne kartice postavljene u *monitor* načinu rada, prisutnost ovih korisnika nije moguće otkriti. Bez obzira na to, odašiljanjem pažljivo oblikovanog mrežnog prometa, takve korisnike moguće je zbuniti i onemogućiti ih u provođenju malicioznih namjera. Najčešće metode su oponašanje pristupnih uređaja te odašiljanje lažnog mrežnog prometa čiji su parametri modificirani tako da onemoguće pravilan rad softvera na uljezovom računalu. Kao i kod *flooding* napada i ovdje je riječ o emitiranju prometa na dijeljeni medij, što zahtijeva izniman oprez kako se aktivnim metodama zaštite ne bi ometali i legalni korisnici sustava.

3.4. Mogući nedostaci

Unatoč brojnim prednostima bežičnih IDS sustava, potrebno je razmotriti i moguće nedostatke. Budući da se radi o relativno novoj tehnologiji, potreban je izniman oprez prilikom implementacije konkretnih rješenja na potpuno funkcionalnu računalnu mrežu. Nepažljiva i nepromišljena instalacija bežičnih IDS sustava može rezultirati visokim postotkom pogrešno detektiranih napada (engl. *false positives*), a moguće ranjivosti u programskom kodu konkretnih implementacija dodatno mogu oslabiti otpornost mreže na napade.
U određenim slučajevima, visoka cijena implementacije IDS sustava može u potpunosti ukloniti prednost u cijeni koju bežična mreža posjeduje u odnosu na klasična žičana rješenja. Upitnoj isplativosti opisanih rješenja u prilog ide i brzina razvoja bežičnih mreža i protokola, koja može rezultirati vrlo brzim zastarijevanjem instalirane IDS opreme i potrebom za njenom zamjenom ili nadogradnjom.
Visokoj cijeni rješenja pridonosi i broj administrativnog osoblja koja se brine o održavanju ovakvog sustava. Efikasnost IDS sustava usko je povezana s brojem ljudi koji prate prikupljene podatke i analiziraju upozorenja. Kod bežičnih IDS sustava potreba za kvalificiranim osobljem još je izraženija budući da je određen broj ljudi potreban i za fizički aspekt nadzora računalne mreže, tj. pronalaženje i hvatanje neovlaštenih korisnika.

4. Bežični IDS alati

U ovom trenutku na tržištu postoji nekoliko komercijalnih bežičnih IDS alata, kao i nekoliko *open source* projekata kojima je cilj razviti funkcionalne IDS sustave. Većina ovih sustava nudi prepoznavanje napada i aktivnu zaštitu, međutim niti jedna od njih za sada ne predstavlja idealno IDS rješenje, pogotovo za veće bežične mreže prisutne u većim tvrtkama ili ustanovama. U daljnjem tekstu opisano je nekoliko popularnijih rješenja.

4.1. AirDefense

AirDefense (http://www.airdefense.net/) je komercijalno Wireless IDS rješenje koje se sastoji od softverskog i hardverskog dijela. Sustav se temelji na nizu senzora koji se rasprostiru unutar granica bežične mreže i prikupljene podatke šalju centralnom uređaju koji se konfigurira i nadzire putem posebne konzole. AirDefense detektira uljeze i napade na bežičnoj mreži, a u mogućnosti je prepoznati i potencijalne ranjivosti zbog neispravne konfiguracije mreže. Prema tvrdnjama proizvođača, ovaj sustav je u mogućnosti otkriti većinu napada opisanih u ovom dokumentu.
Unutar tvrtke koja je razvila ovaj proizvod istovremeno se razvija i dodatak sustavu pod nazivom ActiveDefense. Ovaj dodatak nudio bi aktivni odgovor na detektirane neovlaštene aktivnosti i tako nadograđeni sustav bio bi najsličniji idealnom sustavu opisanom u prethodnom poglavlju.

4.2. Snort wireless

Snort-Wireless (http://snort-wireless.org/) je Open Source projekt pokrenut s ciljem izrade besplatnog i skalabilnog bežičnog IDS sustava, koji će se lako integrirati u postojeću IDS infrastrukturu. Softver je u potpunosti kompatibilan sa Snort 2.0.x IDS sustavima, a osim toga uključuje i neke dodatne mogućnosti. Trenutno Snort-Wireless podržava dodavanje specifičnih pravila za bežičnu mrežu, a u stanju je identificirati i maliciozne pristupne uređaje, AdHoc mreže, pokušaje skeniranja mreže Netstumbler alatom. Zbog brzine razvoja Open Source softvera, popis novih funkcionalnosti proširuje se gotovo svakodnevno, što čini ovaj alat najvećom konkurencijom AirDefense IDS sustavu.

4.3. Widz

WIDZ (www.loud-fat-bloke.co.uk) je "*proof of concept*" IDS alat, čija je primarna namjena demonstracija rada bežičnih IDS sustava. Po svojim funkcionalnostima, ovaj paket konkurira komercijalnim IDS sustavima, ali potrebna je dodatna nadogradnja što se tiče centralnog poslužitelja za obradu podataka i korisničkog sučelja. Budući da je programski kod ovog alata javan, korisnicima se ostavlja mogućnost njegove izmjene i nadogradnje.
Program je trenutno podijeljen na dva modula, *access point monitor* (*widz_apmon*) i sondu za praćenje prometa i detekciju napada (*widz_probemon*).:

- **Access point monitor** - služi za detekciju malicioznih pristupnih uređaja, podešenih tako da se lažno predstavljaju s ciljem prikupljanja povjerljivih korisničkih podataka. Osim toga, ovaj modul otkriva i pristupne uređaje instalirane od strane neovlaštenih osoba. Takvi uređaji najčešće su pogrešno konfigurirani i predstavljaju veliku opasnost po računalnu mrežu na koju su priključeni.
- **Traffic monitor** – ovaj modul nastoji prepoznati maliciozne aktivnosti na mreži. Trenutno je podržana detekcija zahtijeva bez podešenog ESSid polja, kao i pokušaje napada preplavljivanjem paketa (*flooding attacks*). Unutar *traffic monitor* modula također se detektiraju i bilježe greške u radu mreže. Budući da većina pristupnih uređaja ne posjeduje mogućnost zapisivanja log poruka, ova opcija se može pokazati iznimno korisnom prilikom detekcije problema u radu mreže.

4.4. Garuda

Garuda (http://garuda.sourceforge.net) je vrlo napredan bežični IDS sustav s mogućnošću detekcije War Driving napada, malicioznih pristupnih uređaja i krivotvorenja MAC adresa. Alat sadrži module za

statističku, enumeracijsku i detekciju pomoću pravila što rezultira detekcijom velikog broja napada i visokom preciznošću prilikom prepoznavanja istih. Neke od mogućnosti obuhvaćaju:

- Prepoznavanje War Driving napada koji se izvode pomoću Netstumbler i Pocket Warior alata,
- Detekcija Null probing napada,
- Detekcija DoS napada,
- Detekcija krivotvorenja MAC adresa,
- Mogućnost dodavanja novih pravila u bazu za prepoznavanje napada,
- Detekcija na 2., 3. i 4. mrežnom sloju,...

Programski kod ovog alata također je javan i moguće ga je nadograđivati.

5. Zaključak

Bežični IDS sustavi predstavljaju značajan faktor u zaštiti računalnih mreža od neovlaštenih aktivnosti, a u kombinaciji sa odgovarajućom infrastrukturom za rješavanje incidenata predstavljaju najbolji trenutno dostupan oblik zaštite.

Unatoč nekim nedostacima koje ovakva rješenja posjeduju i ponekad prevelike cijene, prednosti koje bežični IDS sustavi nude nedvojbeno opravdavaju njihovu implementaciju. Naravno, kao i u slučaju klasičnih računalnih mreža, IDS sustavi samo su jedan od dijelova cjelokupnog sigurnosnog rješenja i svakako je potrebno razmotriti ostala sigurnosna rješenja s ciljem postizanja optimalne razine sigurnosti mreže.

6. Reference

[1] Jamil Farshchi, *"Statistical-Based Intrusion Detection"*, http://www.securityfocus.com/infocus/1686

[2] Jamil Farshchi, *"Wireless Intrusion Detection Systems"*, http://www.securityfocus.com/infocus/1742

[3] Dr. Joshua Lackey, Andrew Roths, Jim Goddard, *"Wireless Intrusion Detection"*

[4] Yu-Xi Lim, Tim Schmoyer, John Levine, Henry L. Owen, *"Wireless Intrusion Detection and Response"*

[5] Mark Osborne 802.11b Security Pages, http://www.loud-fat-bloke.co.uk/