CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Wireless forenzika

CCERT-PUBDOC-2008-03-225

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj 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

Forenzika u bežičnim mrežama (eng. *wireless forenzics*) grana je računalne forenzike, koja predstavlja postupak utvrđivanja činjenica primjenom odgovarajućih metoda nad digitalnim medijima, a u svrhu korištenja u sudskom postupku. Spomenute metode obuhvaćaju analitičke postupke otkrivanja, prikupljanja, ispitivanja i skladištenja podataka te često podrazumijevaju ispitivanje računalnih sustava kako bi se utvrdilo njihovo korištenje u ilegalnim ili neautoriziranim aktivnostima, npr. krađa poslovnih tajni, krađa ili uništavanje intelektualnog vlasništva te prijevare.

Termin „bežična forenzika" prvi je upotrijebio stručnjak za računalnu sigurnost Marcus J. Ranum 1997. godine kako bi opisao metode i alate za prikupljanje i analizu prometa u bežičnim računalnim mrežama na način koji omogućuje njihovu primjenu u sudskom postupku. Tako prikupljeni dokazi obuhvaćaju podatkovni promet te, zbog sve češćeg korištenja VoIP (eng. *Voice-over-IP*) tehnologija unutar bežičnih mreža, snimke razgovora.

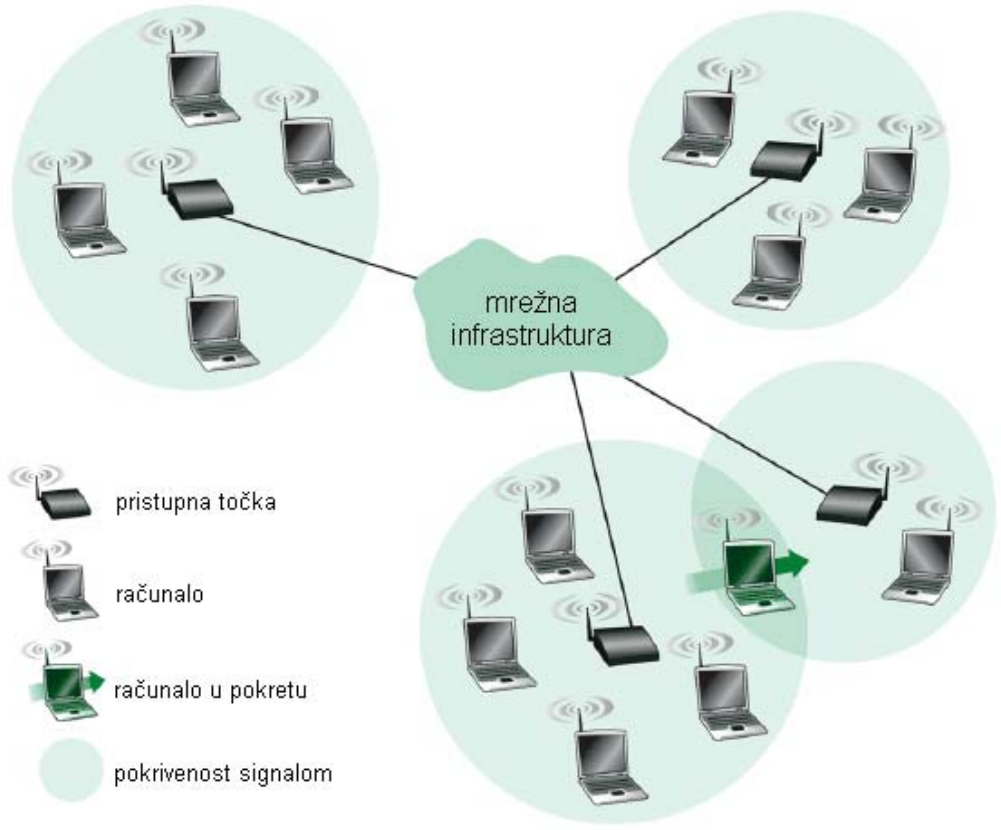
Bežična forenzika odnosi se na prikupljanje svog podatkovnog prometa unutar mreže te njegovu analizu s ciljem otkrivanja neuobičajenih događaja i izvora napada te istraživanja posljedica i uzroka neovlaštenih upada na mrežu i pojedina računala. U postupcima bežične forenzike vrijede općenita pravila računalne forenzike prema kojima je dokaze potrebno izdvojiti od ostalih prikupljenih podataka, očuvati ih i analizirati.

U nastavku dokumenta dan je pregled osnovnih pojmova vezanih uz bežične mreže u kontekstu postupaka forenzičke analize nakon čega slijedi opis alata i metoda korištenih u takvim analizama. Pregled problematike forenzičke analize u bežičnim mrežama zaokružen je osvrtom na tehnike maskiranja i prikrivanja tragova.

2. Bežične mreže

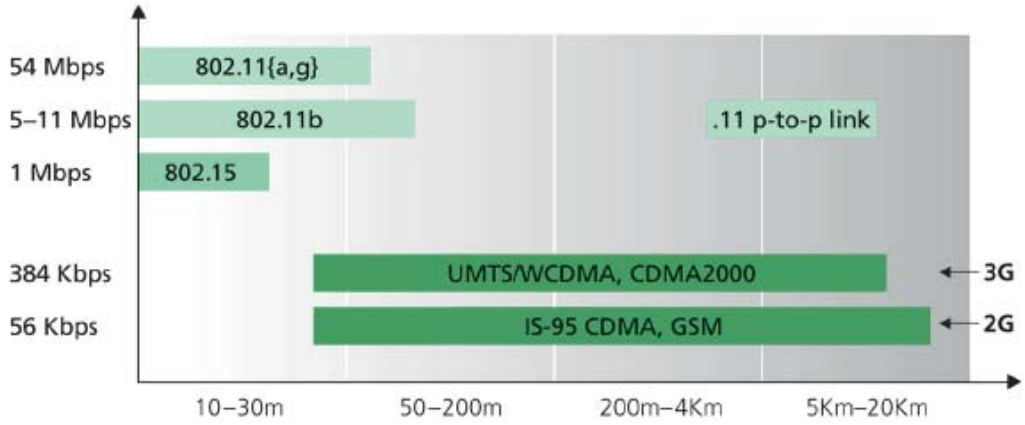
Osnovni elementi bežične mreže prikazani su na slici *Slika 1*. Njihove funkcije i uloge u okviru mreže su sljedeći:

- čvor bežične mreže (eng. *host*) – kao i kod ožičenih mreža, ovo su krajnji uređaji na kojima se izvršavaju aplikacije, a mogu biti stolna, prijenosna i džepna računala.
- bežične veze – računala se s baznom stanicom ili drugim računalima unutar mreže povezuju preko bežične komunikacijske veze. Različite tehnologije bežičnih veza karakteriziraju različite brzine prijenosa kao i različiti dometi. Na slici *Slika 2* prikazane su karakteristike veza najpopularnijih bežičnih standarda.
- bazna stanica - ključni je gradivni element bežične mrežne infrastrukture zadužen za predaju i prijem podatkovnih paketa ka ili od pojedinih računala unutar mreže, kao i za koordiniranu predaju podataka većem broju računala pridruženih toj baznoj stanici. Pristupne točke (eng. *Access Points - AP*) kod 802.11 bežičnih mreža tipični su primjeri baznih stanica. Pristupne točke ne kontroliraju samo pristup mediju nego djeluju i kao mostovi ka drugim bežičnim i ožičenim mrežama.



Slika 1: Elementi bežične mreže

Bazna stanica se najčešće povezuje s nekom većom mrežom, kao što su: Internet, javne telefonske mreže i dr., te djeluje na razini veze. 2. sloja OSI (eng. *Open System Interconnection*) mrežnog modela kao spona između računala u bežičnoj mreži i ostatka svijeta. Za računala koja su pridružena nekoj baznoj stanici kaže se da rade u infrastrukturnom režimu rada (eng. *infrastructure mode*) jer se svi tradicionalni mrežni servisi, npr. dodjela adresa i usmjeravanje, ostvaruju preko mreže na koju je to računalo povezano preko bazne stanice, odnosno pristupne točke za slučaj na slici *Slika 1*.



Slika 2: Karakteristike veza kod tipičnih bežičnih mrežnih standarda

Kod tzv. *ad-hoc* mreža, pojedina računala ne koriste infrastrukturu da bi se povezali. Svaki čvor može izravno komunicirati sa svim drugim čvorovima, tako da bazne stanice nisu potrebne, ali samo ako se nalaze u istom radio dometu. U nedostatku infrastrukture, čvorovi u *ad-hoc* mreži sami osiguravaju usluge kao što su usmjeravanje, dodjeljivanje i prijevod adresa i dr. Zbog toga su oni značajno složeniji od čvorova infrastrukturno bazirane bežične mreže.

Kada pokretno računalo prijeđe iz dometa jedne bazne stanice u područje koje pokriva druga bazna stanica, tada ono promijeni svoju točku pristupa u odnosu na veću mrežu (eng. *handoff*). Pri tome je potrebno riješiti probleme određivanja položaja takvog računala u mreži te usmjeravanja podataka kako ne bi došlo do prekida veze.

U toku devedesetih godina prošlog stoljeća razvijen je veliki broj novih tehnologija i donesen veći broj standarda koji se odnose na bežične LAN (eng. *Local Area Network*) mreže. Ipak čini se da je najšire prihvaćen IEEE 802.11 skup standarda, poznat i pod nazivom Wi-Fi (eng. *Wireless Fidelity*). Spomenuti skup standarda obuhvaća 802.11a, 802.11b i 802.11g standarde. Njihove osnovne karakteristike navedene su u tablici *Tablica 1*.

802.11 specifikacija	Širina kanala	Frekvencijski opseg	Modulacija	Maksimalna brzina prijenosa
802.11a	20 MHz	5160-5330 MHz	OFDM (eng. *Orthogonal Frequency Division Multiplexing*)	54 Mbps
802.11b	22 MHz	2401-2495 MHz	DSSS (eng. *Direct Sequence Spread Spectrum*)	11 Mbps
802.11g	22/20 MHz	2401-2495 MHz	DSSS/OFDM	54 Mbps

Tablica 1: Detalji različitih 802.11 specifikacija

Frekvencije dodijeljene 802.11a specifikaciji preporučene su za korištenje u zatvorenim prostorima dok su 802.11b i 802.11g specifikacije dostupne i na otvorenom.

3. Forenzika u bežičnim mrežama

Velika popularnost bežičnih tehnologija učinila je bežične podatkovne mreže, temeljene na 802.11 standardu, čestim ciljem napada. Složenost bežičnih tehnologija pri tome otežava napore stručnjaka za računalnu sigurnost u osiguravanju ovakvih mreža, kao i policijskim službenicima prilikom provođenja istrage u slučaju sumnje na kriminalne aktivnosti.

Glavni tehnološki izazovi odnose se na karakteristike radiofrekvencijske komunikacije, kompleksnost samog fizičkog medija i 802.11 specifikacija.

3.1. Komunikacijski medij

Prilikom odabira forenzičkog alata potrebno je osigurati da on podržava isti komunikacijski standard kao i onaj koji *korist mreža* koju je potrebno nadzirati. Zbog toga se preporuča korištenje 802.11 a/b/g

višepojasnih mrežnih kartica koje podržavaju tri najpopularnija standarda, npr. kartica sa sklopovljem (eng. *chipset*) tvrtke Atheros. Glavni nedostatak takvih kartica je to što, zbog zakonskih ograničenja u Sjedinjenim Državama, ne podržavaju zamjenjive antene. Spomenuti zakon naime zabranjuje korištenje zamjenjive antene na 802.11a opremi koja radi na najčešće korištenom UNII-1 (eng. *Unlicensed National Information Infrastructure*) frekvencijskom pojasu.

Uobičajena bežična oprema sadrži samo jednu radijsku komponentu pa zbog toga u danom trenutku omogućuje komunikaciju na samo jednom kanalu. Kako bi se zaobišao ovaj nedostatak forenzički programski paketi koriste posebnu tehniku pretraživanja cijelog frekvencijskog spektra od interesa i uzorkovanja svih raspoloživih kanala (eng. *channel hopping*). Zbog toga se podaci sa svakog kanala primaju samo nekoliko milisekundi, što je osnovni nedostatak ove metode.

Ako se nadzire samo jedna pristupna točka opisanih poteškoća nema, jer svaka pristupna točka radi na samo jednom kanalu pa mrežnu karticu računala kojim se provodi forenzička analiza jednostavno treba podesiti na korištenje tog kanala. Na primjer, Linux naredba za podešavanje Atheros mrežne kartice za nadzor kanala 13 je:

```
# iwconfig ath0 mode monitor channel 13
```

Međutim, veće bežične mreže s više pristupnih točaka predstavljaju izazov za pouzdan nadzor prometa. Alati za bežičnu forenziku trebaju moći prikupiti sav promet sa svih bežičnih mreža dostupnih na danom području pa je potreban istovremen nadzor svih kanala. To je jedino moguće postići ukoliko je broj raspoloživih radio uređaja jednak ili veći od broja korištenih kanala.

Iako je propisima svake zemlje ograničen broj dozvoljenih 802.11 kanala, kao što je prikazano tablicom *Tablica 2*, napadači često zanemaruju ova ograničenja. Zbog toga se savjetuje nadzor svih raspoloživih kanala. Također, mnoge zemlje imaju specifične propise prema kojima se koriste frekvencijski pojasi izvan FCC (eng. *Federal Communications Commission*), UNII ili ITU (eng. *International Telecommunication Union*) standarda pa je i to prilikom planiranja nadzora i analize potrebno uzeti u obzir.

802.11 specifikacija	SAD	EU	Japan		maksimalni broj kanala
802.11a	8	različito za članice	4		12
802.11b	11	13	14		14
802.11g	11	13	14		14

Tablica 2: Broj dozvoljenih 802.11 kanala

Propisima je također određena maksimalna snaga odašiljanja, u mW ili W, ali je za očekivati da napadači krše ova ograničenja. Prilikom planiranja analize treba u obzir uzeti takva kršenja zakona te mogućnost pojave novih tehnologija, kao što su MIMO (eng. *Multiple-Input Multiple-Output*) 802.11n i WiMAX (eng. *Worldwide Interoperability for Microwave Access*) 802.16.

3.2. Pokretljivost klijenata

Jedna od glavnih prednosti bežičnih mreža je mogućnost kretanja klijentskih računala unutar nje, tj. bez prekida veze na mrežu. Kod većih bežičnih mreža ovo se većinom postiže posebnim postupkom, tzv. *roaming*, koji omogućuje prijelaz s jedne pristupne točke na sljedeću najbližu tijekom slanja i/ili primanja podataka. Navedene mogućnosti značajno otežavaju zadatak provođenja forenzičke analize mrežnog prometa.

Klijenti u bežičnim mrežama prespajaju se na sljedeću pristupnu točku kad mrežna kartica zaključi kako je signal trenutne pristupne točke preslab za nastavak pouzdane komunikacije. Prilikom prijelaza često se događa promjena radio kanala na kojem se komunikacija provodi. Ukoliko korišteni forenzički alat u trenutku promjene pristupne točke ne nadgleda sve raspoložive kanale, a naročito dva kanala između kojih se događa prijelaz, određeni broj podatkovnih paketa neće biti zabilježen. Time je ugrožen integritet prikupljenih dokaza.

Pored toga, i konfiguracija bežične mreže, a i položaj pojedinih klijenata unutar nje utječu na mogućnost prikupljanja dokaza s određene lokacije. Na primjer, moguće je da klijent promjenom položaja izađe

izvan područja unutar kojega forenzičar može prikupljati podatkovni promet. U takvim situacijama ponekad je promet moguće prikupljati samo s jedne strane komunikacijske veze.

Jedino mjesto s kojeg je moguće pouzdano prikupljati podatke iz bežične mreže, odnosno jedino mjesto s kojeg su vidljiva oba sudionika razmjene paketa, je okolina pristupne točke. Forenzički alat često nije moguće postaviti na takvu poziciju, npr. kod mreža koje sadrže veći broj pristupnih točaka, jer forenzičar ne može biti u blizini svake, ili kod ad-hoc mreža. Ovaj problem je s forenzičkog stajališta jedino moguće riješiti postavljanjem višestrukih uređaja za snimanje prometa na različitim položajima unutar nadziranog područja. Ako se kroisti tri ili više takvih uređaja također se može odrediti približni položaj pojedinih klijenata postupkom triangulacije.

3.3. Karakteristike prometa

Prilikom prikupljanja podatkovnih paketa iz bežične mreže potrebno je u obzir uzeti karakteristike takvog prometa kao što su veličina podatkovnih paketa i zahtjevi na propusnost veze.

MTU (eng. *Maximum Transmission Unit*) veličina podatkovnog polja paketa prema 802.11 specifikacijama je 2304 okteta. To je veličina podataka prije enkripcije, a konačna duljina paketa ovisi o korištenom enkripcijskom protokolu, npr.:

- WEP (eng. *Wireless Encryption Protocol*) protokol paketu dodaje zaglavlje veličine 8 okteta,
- WPA (eng. *Wi-Fi Protected Access*) protokol paketu dodaje zaglavlje veličine 20 okteta, a
- zaglavlje WPA2 protokola dugo je 16 okteta.

Na primjer, uz korištenje WEP enkripcije maksimalna ukupna veličina paketa je: duljina podatkovnog polja + 802.11 zaglavlje + završni slog (eng. *trailer*) = 2312 + 30 + 4 = 2346 okteta.

802.11 specifikacija definira tri tipa mrežnih paketa: kontrolne, upravljačke i podatkovne pakete. Na primjer, pristupne točke odašilju upravljačke pakete namijenjene sinkronizaciji (eng. *beacon*) i to najčešće svakih šest sekundi. To znači da će forenzičar u bežičnoj mreži koja se sastoji od samo jedne pristupne točke tijekom sat vremena prikupiti 600 ovakvih paketa. Opisanu i slične posebnosti bežičnih mreža potrebno je uzeti u obzir prilikom planiranja forenzičkog postupka kako bi se osigurale zadovoljavajuće performanse i mogućnosti pohrane podataka.

3.4. Performanse uređaja za prikupljanje prometa

Sklopovlje korišteno za prikupljanje prometa u nadziranoj bežičnoj mreži treba moći prihvatiti maksimalnu količinu prometa koja je teoretski moguća. Kako je prema 802.11 specifikacijama na jednom kanalu moguća brzina prijenosa 54 Mbps, maksimalna količina prometa u jedinici vremena za četrnaest kanala je 756 Mbps.

Prilikom odabira uređaja za prikupljanje prometa u obzir treba uzeti propusnost sabirnica koje međusobno povezuju bežične mrežne kartice, te propusnost memorijskih sabirnica i sučelja tvrdih diskova kako ne bi došlo do zagušenja i gubitka potencijalnih dokaznih materijala. Također potrebno je osigurati dostatne kapacitete za pohranu velikih količina podataka karakterističnih za bežičnu forenziku.

Iako je bežičnu forenziku moguće provoditi korištenjem standardnog PC sklopovlja i programskih paketa otvorenog programskog koda, za izgradnju sustava koji bi zadovoljio sve navedene zahtjeve potreban je pažljiv dizajn i relativno skupa implementacija. Na tržištu je prisutno nekoliko komercijalnih uređaja posebno oblikovanih u skladu sa strogim zahtjevima forenzičke analize bežičnih mreža, kao što su *Janus Project* i *WLAN-14*.

4. Forenzički alati i postupci

Nakon prikupljanja podataka iz bežične mreže potrebno ih je analizirati kako bi se potencijalni dokazi odvojili od uobičajenog prometa. Pored ovih podataka u forenzičkoj analizi mogu se koristiti dnevnički zapisi (eng. *log*) pristupnih točaka i drugih mrežnih uređaja, ARP (eng. *Address Resolution Protocol*) i CAM (eng. *Content Addressable Memory*) tablice te podaci koje skuplja bežični IDS (eng. *Intrusion Detection System*) sustav za otkrivanje neovlaštenih pristupa.

4.1. Zahtjevi i preporuke

Prilikom provođenja forenzičke analize prometa bežične mreže preporučeno je držati se određenih procedura te koristit alate s odgovarajućim mogućnostima:

- Savjetuje se korištenje uređaja s 15 radio komponenti kako bi se moglo nadzirati svih 14 802.11b/g kanala te istovremeno pretraživati radio spektar u potrazi za novim mrežama.
- Korištenje GPS (eng. *Global Positioning System*) navigacijskog sustava omogućuje stvaranje preciznih vremenskih oznaka (eng. *timestamp*) te utvrđivanje položaja na otvorenom, ukoliko je na forenzički postupak postavljen zahtjev potvrđivanja mjesta i vremena prikupljanja dokaza. Pri tome je potrebno u dnevničke zapise bilježiti intervale sinkronizacije uređaja s GPS satelitima kako bi bilo moguće dokazati da su njegova očitanja točna.
- Forenzički alat treba prikupljati sav promet, bez filtriranja, kako analizi ne bi promakli pojedini bežični uređaju prisutni na mreži. Filtre je moguće koristiti kasnije tijekom analize prikupljenih podataka zbog ubrzavanja postupka.
- Preporučeno je da forenzički alat bude potpuno pasivan, tj. da ne odašilju pakete. Ovo je moguće postići na sklopovskoj razini korištenjem prigušnika ili jednosmjernih pojačala te na programskoj razini postavljanjem mrežne kartice u nadzorni način rada (eng. *monitor mode*).
- Savjetuje se korištenje uređaja na koje je moguće priključiti vanjsku antenu s ciljem povećanja osjetljivosti prijemnika.
- Zbog specifičnosti pojedinih forenzičkih zadataka uređaj za prikupljanje prometa može biti na takvom mjestu da mu je pristup vrlo težak ili čak nemoguć.. Tada je potrebna mogućnost udaljenog pristupa uređaju, npr. pomoću zasebnog 802.11b/g sučelja. Pri tome spomenuto sučelje treba dobro zaštititi odgovarajućim autentikacijskim i enkripcijskim mehanizmima.
- Kako bi se omogućila procjena udaljenosti osumnjičenog od forenzičkog uređaja, savjetuje se bilježenje podataka o snazi signala. Ove informacije nisu jednoznačne zbog svojstava radio signala, kao što su: refleksija, lom, ogib i rasipanje signala.
- Savjetuje se zapisivanje prikupljenog prometa u standardnom Pcap formatu kojeg podržava većina alata kako komercijalnih tako i onih otvorenog programskog koda.
- Preporučeno je korištenje sklopovlja (mrežnih kartica i radio komponenti) s velikom osjetljivošću prijemnika kako prikupljanje paketa ne bi bilo prekinuto u slučaju pogoršanja uvjeta rada.
- Kako bi se omogućila rekonstrukcija postupaka forenzičkog alata, što može biti potrebno tijekom sudskog procesa, savjetuje se korištenje naprednih mogućnosti stvaranja dnevničkih zapisa. Valjanost takvih zapisa potrebno je zaštititi pomoću jednosmjernih (eng. *hash*) algoritama kao što su MD5 (eng. *Message Digest 5*) i SHA-1 (eng. *Secure Hashing Algorithm 1*).

4.2. Komercijalni i alati otvorenog programskog koda

Forenzičar za uspješnu analizu prometa unutar bežične mreže treba, jednako kao i kod forenzike žičanih mreža, detaljno poznavati korištene komunikacijske protokole. Kod bežičnih računalnih mreža to su najčešće TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) temeljeni protokoli prilagođeni 802.11 specifikacijama.

Skup alata korištenih za forenzičku analizu mrežnog prometa naziva se NFAT (eng. *Network Forenzic Analysis Tool*). Najpoznatiji komercijalni alati namijenjeni forenzičkoj analizi žičanih mreža su *„Sandstorm NetIntercept“*, *„Niksun NetVCR“* i *„eTrust Network Forensics“* alati. Kako bi ih bilo moguće primijeniti kod bežičnih mreža potrebne su napredne analitičke funkcije specifičnih 802.11 zaglavlja i sekvenci poruka karakterističnih za bežične protokole.

Navedenim komercijalnim alatima ne postoji kompaktna alternativa među programskim paketima otvorenog programskog koda. Međutim, na raspolaganju su brojni alati namijenjeni analizi mrežnog prometa koji forenzičaru mogu pomoći u pretraživanju prikupljenih podataka. Neki od takvih alata su:

- **Wireshark** je alat s grafičkim korisničkim sučeljem koji omogućuje detaljnu analizu polja prikupljenih podatkovnih paketa,
- **ngrep** (eng. *Network Global Regular Expression Parser*) omogućuje traženje znakovnih nizova u kontekstu podatkovnih paketa,

- **tcdump** i **tshark** su alati za stvaranje skripti s tekstualnim grafičkim sučeljem, a namijenjeni su automatizaciji pojedinih analitičkih zadataka kao što je filtriranje prikupljenog prometa prema postavljenim kriterijima.

4.3. Analiza bežičnog prometa

Analiza mrežnog prometa sastoji se od većeg broja postupaka koji uključuju:

- normalizaciju podataka,
- tzv. podatkovno rudarenje (eng. *data mining*), koje omogućuje jednostavno rukovanje i pretraživanje prikupljenog prometa,
- prepoznavanje uzoraka, kako bi se otkrile anomalije i sumnjivi uzorci,
- analizu protokola (eng. *protocol dissection*), koja je važna za razumijevanje različitih zaglavlja pojedinih protokola te
- rekonstrukciju aplikacijskih sjednica.

Navedeni postupci u osnovi su jednaki kod žičanih i bežičnih mreža, a specifičnosti bežične forenzike odnose se na:

- spajanje prometa više kanala,
- rukovanje prometom preklapajućih kanala,
- filtriranje i
- ubrzavanje analize.

Značajnu razliku u odnosu na analizu prometa unutar žičanih mreža predstavljaju enkripcijske mogućnosti ugrađene u 2. sloj 802.11 specifikacije.

4.3.1. Spajanje prometa više kanala

Ako se za prikupljanje podataka u bežičnoj mreži koristi uređaj s većim brojem mrežnih kartica, svaka od njih nadzire jedan kanal i prikupljene podatke pohranjuje u zasebnu datoteku. To su često datoteke Pcap (eng. *Packet capture*) formata uobičajenog kod analize i nadzora računalnih mreža.

Ponekad, na primjer u slučaju pokretnih klijenata, podatke prikupljene na različitim kanalima potrebno je ujediniti kako bi se rekonstruirale sjednice. Alat *mergecap*, sastavni dio *Wireshark* programskog paketa, omogućuje spajanje više Pcap datoteka u jednu naredbom:

```
# mergecap -w all_channels.pcap channel_1.pcap … channel_n.pcap
```

U grafičkom sučelju *Wireshark* alata, odabirom *File* → *Merge* moguće je datoteke spajati kronološkim redom.

Obnavljanje sjednica potrebno je, na primjer, ukoliko se želi rekonstruirati VoIP razgovor klijenta koji je tijekom sjednice promijenio kanal na kojemu vrši bežičnu komunikaciju. Pored mogućnosti spajanja Pcap datoteka, *Wireshark* alat omogućuje i izdvajanje audio zapisa razgovora rekonstrukcijom VoIP RTP (eng. *Real-time Transport Protocol*) sjednica u sljedećim koracima:

- dekodiranje RTP paketa: označivanjem prvog RTP paketa unutar Pcap datoteke te odabirom *Statistics → RTP → Stream Analysis* …
- analiza RTP podatkovnog niza: odabirom *Save payload* pohranjuje se podatkovni niz (eng. *stream*),
- spašavanje audio datoteke u .au (eng. *Audio*) formatu.

4.3.2. Rukovanje prometom preklapajućih kanala

Tijekom prikupljanja mrežnog prometa na jednom kanala moguće je istovremeno bilježenje paketa s drugih kanala, odnosno prometa iz susjednih bežičnih mreža. Mogućnost istovremenog prikupljanja paketa s više kanala ovisi o karakteristikama pristupnih točaka i uređaja za bežičnu forenziku, kao što su:

- Tx (eng. *Transmission*) snaga odašiljanja,
- Rx (end. *Receive*) osjetljivost forenzičkog uređaja te
- karakteristike antene.

Promete koji pripadaju različitim kanalima moguće je razlikovati na temelju tzv. *beacon* paketa pristupnih točaka. Točnije, podaci o mreži nalaze se u *DS Parameter set: Current Channel* polju, koje je dio *Tagged parameters* odjeljka *IEEE 802.11 wireless LAN management frame* zaglavlja. Tijekom analize prikupljenog prometa podvostručene pakete s više kanala potrebno je odbaciti te na odgovarajući način rukovati ostalim posljedicama preklapanja paketa.

4.3.3. Filtriranje i ubrzavanje analize

Nakon spajanja višestrukih datoteka s prikupljenim prometom potrebno je u tako dobivenoj velikoj količini podataka prepoznati i izdvojiti sumnjive sjednice, odnosno podatkovne pakete. Filtriranjem prometa prema MAC (eng. *Media Access Control*) adresama moguće je dobiti pregledan prikaz svog prometa jednog klijenta preko više različitih kanala. S druge strane, moguće je filtriranjem prometa prema BSSID (eng. *Basic Service Set Identifier*) oznakama dobiti prikaz prometa samo jedne pristupne točke. Nadalje, promet pristupne točke moguće je filtrirati prema vrsti paketa, odnosno prikazivati samo podatkovne, upravljačke ili kontrolne podatkovne pakete.

4.4. Analiza kriptiranog bežičnog prometa

Glavni problem forenzičke analize bežične mreže je stjecanje enkripcijskog ključa korištenog za zaštitu prometa. 802.11 standard propisuje više razina enkripcijske zaštite: od nesigurne komunikacije bez enkripcije do 802.11i specifikacije koja propisuje korištenje naprednih enkripcijskih algoritama, kakav je AES (eng. *Advanced Encryption Algorithm*) algoritam. Metode stjecanja enkripcijskih ključeva sumirane su u tablici *Tablica 3*.

enkripcija	**ključ**	**razina sigurnosti**	**alat**	**stjecanje ključa**
Open	-	-	Sniffer	nije potrebno
WEP	PSK	niska	Aircrack-ng	moguće
WPA ili WPA2 - *Personal*	PSK	srednja	CoWPAtty	moguće
WPA ili WPA2 - *Enterprise*	EAP	visoka	N/A	druge metode

Tablica 3: Metode zaobilaženja enkripcije u bežičnim mrežama

Sakupljanjem dovoljne količine mrežnog prometa uvijek je moguće prepoznati WEP ključ. WEP enkripcija je, kao i njene izvedenice (WEP+, DWEP i dr.), nesigurna i moguće ju je zaobići na više načina. Jedan od njih je korištenje Aircrack-ng alata.

Razina sigurnosti WEP/PSK (eng. *Pre-Shared Key*) temelji se na snazi dijeljenog ključa. Ako ovaj ključ nije dovoljno dug ili ako se temelji na poznatim riječima moguće ga je otkriti tzv. rječničkim napadom (eng. *dictionary attack*). Postupak otkrivanja mrežnog ključa moguće je ubrzati korištenjem prethodno izračunatih ključeva (tzv. *Rainbow* tablice). Jedan od alata koji omogućuje stjecanje enkripcijskog ključa kod mreža s ovom razinom zaštite je „CoWPAtty".

WPA(2)/Enterprise ključeve nasumično stvara RADIUS (eng. *Remote Authentication Dial-In User Server*) poslužitelj pa stoga nisu ranjivi na rječničke napade. Eventualne ranjivosti ovog zaštitnog mehanizma mogu ležati u različitim načinima EAP (eng. *Extensible Authentication Protocol*) autentifikacije.

Dakle, WPA ili WPA2 *Personal* enkripcija, s dijeljenim ključem duljim od 20 znakova i koji nije temeljen na riječima, te *Enterprise* enkripcija, uz korištenje robusnog EAP protokola, kakvi su PEAP (eng. *Protected EAP*) i EAP/TLS (eng. *Transport Layer Security*), mogu se smatrati neranjivima. U takvim slučajevima forenzičar treba iznaći drugačiji način za stjecanje pristupa mrežnom prometu, npr. otkrivanjem enkripcijskog ključa pristupne točke, bežičnih klijenata, RADIUS poslužitelja ili pristupanjem autentifikacijskoj bazi podataka. Međutim, ako zlonamjerni korisnik neovlašteno koristi tuđu bežičnu mrežu, što je vrlo čest slučaj, onda je on uspio probiti korištenu enkripciju te je isto moguće i forenzičkom stručnjaku.

4.5. Napredna analiza

Ukoliko se u bežičnoj mreži koristi enkripcija na višim slojevima OSI modela, kao što su VPN (eng. *Virtual Private Network*) rješenja temeljena na IPSec (eng. *IP Security*), SSL (eng. *Secure Sockets Layer*) ili SSH (eng. *Secure Shell*) protokolima, nužna je primjena naprednih metoda analize prometa.

Bez probijanja enkripcije prisutne na 2. ili višim slojevima nije moguće pristupiti podatkovnom sadržaju prikupljenih mrežnih paketa te se tada uobičajeno provodi statistička analiza protokola. Pored toga, kod bežičnog mrežnog prometa mnogo se informacija šalje bez enkripcije, npr. zaglavlja podatkovnih paketa te cjelokupni upravljački i kontrolni paketi. Na temelju tih podataka moguće je otkriti pokušaje povezivanja osumnjičenog na određene bežične mreže, jesu li ti pokušaji bili uspješni, koje su autentifikacijske metode pri tome korištene, mogućnosti bežične mreže idr.

Alati kao što je „fl0p“ mogu biti vrlo korisni prilikom analize kriptiranog mrežnog prometa. Riječ je o pasivnom alatu za analizu podatkovnog toka koji djeluje na 7. mrežnom sloju. Analizu provodi nadzorom razmjene poruka između klijenta i poslužitelja, njihove veličine i vremena slanja. Prikupljene podatke uspoređuje s unosima u bazi podataka poznatih komunikacijskih uzoraka te se tako identificiraju događaji kao što su neuspjeli pokušaji prijave, razlikuju se ljudski korisnici od automatiziranog prometa, a ponekad je moguće čak otkriti pojedine sigurnosne postavke nadzirane mreže.

U bežičnim mrežama trivijalno je oteti identitet korisnika ukoliko se koristi samo osnovna autentifikacija na temelju MAC adresa. Stjecanjem MAC adrese ovlaštenog klijenta zlonamjerni korisnik može neometano pristupati i razmjenjivati podatke na mreži. U takvim situacijama osnovni zadatak forenzičara je razlikovanje ovlaštenih korisnika od napadača. To je moguće postići pomoću pasivne analize prometa te metodama otkrivanja operacijskih sustava udaljenih računala (eng. *fingerprinting*) ukoliko napadač koristi operacijski sustav i/ili mrežnu karticu koji nisu uobičajeni u nadgledanoj mreži.

Pasivni alati koji omogućuju otkrivanje operacijskog sustava, npr. „p0f“, analizu provode na 3. i 4. mrežnom sloju tako da u slučaju enkripcije na 2. sloju njihova primjena nije moguća. Tada je zlonamjernog korisnika moguće otkriti naprednim metodama identifikacije bežičnog stoga (eng. *stack fingerprinting*), na primjer pomoću „lib802finger“ alata.

5. Tehnike maskiranja i prikrivanja tragova

Istodobno s razvojem novih metoda forenzičke analize pojavljuju se tehnike njihova izbjegavanja i zavaravanja. Neki od jednostavnijih postupaka za zaobilaženje forenzičke analize su: komunikacija na nedopuštenim kanalima, npr. kanala 14. u SAD i EU, ili korištenje snažne enkripcije na 2. mrežnom sloju.

Zlonamjernom korisniku na raspolaganju su i brojne metode prikrivanja mrežnog prometa kao što su korištenje skrivenih kanala te izmjene 802.11 specifikacija. Na primjer, Raw „Covert alat“ koristi neke mogućnosti Linux pogonskih mrežnih aplikacija (eng. *driver*) za umetanje podataka u 802.11 kontrolne pakete. Spomenuti programski paket podatke umeće u polje adrese primatelja (eng. *Receiver Address - RA*) ACK (eng. *Acknowledge*) paketa te time skriva komunikaciju jer većina alata za nadzor bežičnih mreža ne analizira ACK pakete. Opisanu metodu moguće je implementirati i umetanjem podataka u druge kontrolne pakete, u upravljačke pakete te čak i u neispravne 802.11 pakete.

„WiFi Advanced Stealth Patches“ dodatak „madwifi-ng“ Linux pogonskoj aplikaciji namijenjenoj Atheros čipsetima implementira 802.11 protokol s izmijenjenim MAC slojem. Riječ je prilagođenom mrežnom stogu koji može komunicirati samo s drugim stogom koji je izmijenjen na jednak način. Iako se pri tome koriste uobičajene 802.11 frekvencije, IDS sustavi i sustavi za prikupljanje mrežnog prometa ne mogu identificirati takve pakete.

Prilikom provođenja forenzičke analize potrebno je imati u vidu navedene alate i tehnike za skrivanje i maskiranje bežičnog prometa.

6. Zaključak

Bežične tehnologije, prije svega Wi-Fi, u budućnosti će nalaziti primjenu na sve širim područjima te u sve većem obimu. Pri tome je sigurno kako će znatan broj primjena biti zlonamjerne prirode. U tom kontekstu očita je važnost i nužnost odgovarajućih metoda forenzičke analize u postupcima otkrivanja i analize sigurnosnih incidenata.

Osnovni zadatak forenzičke analize bežične mreže prikupljanje je svog ostvarenog prometa. Ukoliko nije moguće pouzdano prikupiti sav ostvareni promet, te isto tijekom sudskog procesa dokazati, valjanost dokaza je, u najboljem slučaju, upitna. Pri tome je potrebno nadzirati sve dostupne radio kanale, bilježiti snage signala te prostorne i vremenske oznake, probiti enkripciju korištenu za zaštitu prometa, ukoliko je prisutna, te uočiti korištenje naprednih alata za prikrivanje bežičnog prometa. Prikupljeni promet potom je potrbno filtrirati i analizirati, pri čemu se koriste metode u osnovi jednake metodama analize žičanog bežičnog prometa.

Usporedno s razvojem tehnologija bežične komunikacije razvijaju se noviji i sofisticiraniji načini njihove zlouporabe. Ovdje, kao i na svim ostalim poljima računalne sigurnosti, traje tzv. „utrka u naoružanju“ između zlonamjernih korisnika i sigurnosnih stručnjaka pa potrebno stalno školovanje osoblja i ažuriranje korištenih alata.

7. Reference

[1] *Wireless forenzics*, http://en.wikipedia.org/wiki/Wireless_forensics, travanj 2008.

[2] Bežične i mobilne mreže, http://es.elfak.ni.ac.yu/rmif/Materijal/bezicne%20i%20mobilne%20mreze-802.11.pdf, travanj 2008.

[3] Raul Siles: *Wireless Forenzics: Tapping the Air - Part One*, http://www.securityfocus.com/infocus/1884, travanj 2008.

[4] Raul Siles: *Wireless Forenzics: Tapping the Air - Part Two*, http://www.securityfocus.com/infocus/1885, travanj 2008.

[5] Specification of E-Detective 802.11 a/b/g Wireless LAN Forensics Appliance, http://www.edecision4u.com/forensics.html, travanj 2008.