SVEUČILIŠTE U SPLITU
POMORSKI FAKULTET U SPLITU

Zaštita integriteta bežične komunikacije

Autori:

Hrvoje Lozančić

Doc. dr. sc. Danko Kezić, dipl. ing.

Mr. sc. Anita Gudelj, prof.

Split, lipanj 2007.

Kratki sadržaj

Povećanjem broja organizacija koje svoj mrežni rad dijelom ili u potpunosti zasnivaju na primjeni bežičnog mrežnog prijenosa, rastu i problemi odnosno sigurnosni rizici. Različiti mehanizmi sigurnosti su definirani IEEE 802.11 standardom, no njihova primjena ne znači nužno da je postignuta zadovoljavajuća razina sigurnosti. Bežične komunikacije sa sobom donose izraženije sigurnosne probleme u odnosu na žične sustave. Budući da bežična mreža koristi radio signal koji se širi kroz zidove i razne druge prepreke, to omogućava bilo kome u dometu tog signala primanje podataka sudionika bežične komunikacije. Stoga je potrebno obratiti iznimnu pozornost u definiranju sigurnosnih mehanizama koji će se sudionicima bežičnih mreža osigurati povjerljivost, integritet, neporecivost i raspoloživost podataka. Sigurnosni mehanizmi su raznovrsni, od WEP-a (Wired Equivalent Privacy) do VPN-a (Virtual Private Netvork). Pokazalo se da oni imaju slabosti i da ostavljaju mreže ranjivima na napade. Razvojem novih zaštitnih mjera i mogućnosti, pojavljuju se na vidjelo novi sigurnosni propusti i ranjivosti.

Namjera ovog rada je predstaviti novi koncept i praktični model sigurnosne zaštite koji problem zaštite inegriteta razmjene podataka vraća na fizičku razinu.

Nove smjernice razvoja zaštite u bežičnim sustavima dijelom odbacuju dosadašnji pristup isključivo enkripcijske zaštite. Zbog stalnog razvoja i unaprjeđenja mogućnosti računala, vrijeme za brutal force napad se smanjuje. Do sada se taj problem rješavao na način da se podiže složenost enkripcije, složenost inicijalizacijskog vektora, vektora integriteta ili hash funkcije. To nije rješenje jer ne nudi konačni model. Osim toga, dolazimo do paradoksa pri kojem će svaki okvir razmjene podataka u budućnosti imati veći teret na strani enkripcije i verifikacija, nego li na strani samog korisnog sadržaja. Stoga su nužna nova rješenja.

Riješenja su poređena kroz 3 nova koncepta:

1. Optimal Message Transfer Autenticator

2. Integrity regions (I regions)

3. Integrity codes (I codes)

Kod Optimal Message Transfer Autenticator modela, koncept je zasnovan na tome da se za svaku poruku generira njezin hash, odnosno izračun vrijednosti određenog paketa podataka. Hash je algoritam koji je određeni paket podataka u stanju prikazati određenim

heksadecimalnim brojem, na osnovu izračuna. Svaki podataka ima jedinstveni hash i on se smatra „otiskom prsta“ koji kao jedinstven posjeduje svaki podatak.

Integrity regions (I regions) omogućuju na provjeri pozicije s koje je odaslan signal. Do sada su slični modeli kontrolirali radijus u kojem pristupna točka odašilje signal, ovjeravali korisnika GPS pozicionerom. No ti su koncepti kompromitirani. I regions pristupa verifikaciji korisnika, njegove pozicije unutar zadane regije, koristeći ultrazvučni mjerač, koji mjeri s odstupanjem od najviše 1 cm.

Integrity codes (I codes) koristi složenost postupka pri kojem se može ukloniti trag emitiranog signala, emitiranjem signala protufaze i protuvrijednosti. Ovakav pristup objedinjuje tri osnovna mehanizma: On-off keying, signal anti-blocking i I codein

1. On-off keying je modulacija u kojoj se informacija prijenosi na način da se postojanjem ili nepostojanjem signala u određenom vremenskom intervalu.

2. Signal anti-blockning podrazumjeva rad sa signalima takve energetske razine koji se nemogu blokirati, a da se na valnom obliku to i ne primjeti.

3. Da bi oveli dodatnu kontrolu integriteta sadržaja koristi se kodiranje pri kojem je svaka „0“ i svaka „1“ obilježene sa po jednakim brojem „0“ i „1“. Takva vrsta kodiranja se zove Manchester code. Svaki slog podataka odvaja se delimiterom a to je najkraća sekvenca koja nije ponovljiva u Manchester kodu (111000). Zbog trajanja signala (5-10ms) realno je nemoguće generatorom vala, poništiti tragove, na način da se signal maskira i umjesto njega generira lažni.

Sigurnost I-coda zasnovana je na spobnosti napadača da obrne „0“ i „ 1“, čime je povrijedio integriter poruke. Napadač mora biti sposoban promjenuti poruku na takav način da je primatelj primi o ocjeni kao validnu. Dva su glavna razloga koja otežavaju uspiješnost:

1. Nepredvidivost signala koji se emitira

2. Nepredvidivost stanja etera u kojem se emitira signal (šumovi, interferencije...)

Stoga nije realno očekivati da napadač ima metodu i način da promjeni sadržaj poruke.

Nove metode načelno su postavljene i za sada nisu logični opovrgnute. Praktična rješenja i primjena se tek očekuje.