FBIM Transactions
DOI 10.12709/fbim.06.06.02.13

PRIMENA BEŽIČNIH RAČUNARSKIH MREŽA I BEZBEDNOSNI PROBLEMI

APPLICATION OF WIRELESS COMPUTER NETWORKS AND SECURITY PROBLEMS

Dušan Regodić
Poslovni i pravni fakultet Univerziteta „Union - Nikola Tesla“, Beograd, Srbija

Gojko Grubor
Univerzitet Sinergija, Bijeljina, Bosna i Hercegovina

Radomir Regodić
Zavod za izdavanje udžbenika, Beograd, Srbija

JEL Category: **G32, L86**

Apstrakt
Savremeni uslovi poslovanja i način života doveli su do komercijalne ekspanizije i povećanje broja korisnika bežičnih mreža i pojave upotrebe pametnih telefona. Paralelno sa povećanjem broja korisnika sve je veći broj onih koji nisu upoznati sa sigurnosnim problemima. Bežične računarske mreže nose sa sobom brojne sigurnosne probleme. Laptopovi, pametni telefoni, tableti, i drugi uređaji se danas ne mogu zamisliti bez podrške za povezivanje na bežičnu mrežu. Međutim, nisu svi korisnici bežičnih mreža dobronamerni. Postoje zlonamerni ljudi koji će iskoristiti svoja znanja o bežičnim mrežama, i ne samo kompromitovati podatke koji se šalju kroz mrežu, nego i ukrasti poverljive informacije koje korisnici šalju, kao što su brojevi kreditnih kartica, šifre, itd. nesvesni ko ih sve vidi. Zbog toga je neophodno znati koje opasnosti sa sobom nosi upotreba bežičnih mreža. Kako su napadači uvek korak ispred, neophodan je stalan rad na zaštiti i sigurnosti korisnika bežičnih mreža. Cilj istraživanja ovog rada je da se prikažu bezbednosni problemi u bežičnim računarskim mrežama, slabosti same infrastrukture, i nedovoljna razvijenost bezbednosnih protokola. Društveni cilj ovog rada je da se ukaže svim korisnicima na realne probleme, odnosno pretnje sa kojima se susreću korisnici bežičnih mreža. Sam problem istraživanja, brojne slabosti i bezbednosni problemi u bežičnim računarskim mrežama imaju za cilj podizanje nivoa svesti korisnika i unapređenje nedovoljne razvijenosti upotrebe bezbednosnih protokola.

Ključne reči: *Bežične računarske mreže, slabosti, pretnje, napadi, šifra.*

Adresa autora zaduženog za korespodenciju:
Dušan Regodić
dusanregodic5@gmal.com

Abstract
Modern business conditions and lifestyles have led to commercial expansion and the increase in the number of wireless network users and the

emergence of smartphones. In parallel with the increase in the number of users, there is an increasing number of those who are not familiar with security issues. Wireless computer networks carry many security problems with them. Laptop computers, smartphones, tablets, and other devices today can not be imagined without an access to a wireless network. However, not all users of wireless networks are well-intentioned. There are malevolent people who will use their knowledge of wireless networks, to compromise data sent across the network. They also steal confidential information sent by users, such as credit card numbers, passwords, etc. Therefore, it is necessary to understand the dangers of using wireless networks. As attackers are always a step ahead, it is necessary to work continuously on the protection and security of wireless users. The aim of this paper is to present security issues in wireless computing networks, weaknesses of the infrastructure itself, and insufficient development of security protocols. The social goal of this work is to elaborate about the real problems or threats that wireless network users encounter. The main two problems of the research, numerous weaknesses and security issues in wireless computing networks, are aimed at raising the level of user awareness and improving the insufficient development of the use of security protocols.

Keywords: *Wireless network, vulnerabilities, threats, attacks, password.*

1 UVOD

Bežične računarske mreže su u svoju komercijalnu ekspanziju krenule u drugoj polovini 80-tih godina prošlog veka. Iako klasične žičane mreže imaju dosta prednosti u odnosu na bežične, pre svega u vidu pouzdanosti, bezbednosti i brzini, bežične mreže su svoju primenu pronašle pre svega zbog cene i jednostavnosti instalacije, odnosno svoje mobilnosti. Korisnik više nije vezan za radni sto, nego je u stanju koristiti mrežu sa svojim laptopom ili drugim mobilnim uređajem, svuda u zoni pokrivenosti signala bežične mreže.Jednu od najvećih primena bežične mreže su ostvarile u pružanju usluga Interneta na javnim mestima, kao što su kafići, aerodromi, biblioteke, sportski stadioni, veliki tržni centri itd. A takođe sa padom cena uređaja, postale su veoma popularne i u domaćinstvima.

Međutim jedna od glavnih prednosti u odnosu na žičane mreže, mogućnost prenosa informacija kroz vazduh korišćenjem radio signala, što i omogućava mobilnost uređaja unutar zone pokrivenosti, predstavlja i najveću slabost bežičnih mreža. Pošto se informacije kreću slobodno kroz vazduh, čak i oni kojima nisu namenjene mogu da ih uz određene alate snimaju, čitaju ili menjaju. Uvođenjem E – poslovanja i Internet plaćanja, infromacije koje idu kroz mrežu su osetljivije nego ikad. Nedovoljna upućenost u bezbednosne probleme sa kojima se suočavaju bežične mreže, može dovesti da korisnici svoje podatke nenamerno podele sa zlonamernim korisnicima mreže. Ovo je razlog zašto je bezbednost u bežičnim mrežama veoma aktuelna tema. Da bih se bavili sa bezbednošću, moramo biti upoznati sa slabostima i ranjivostima bežičnih računarskih mreža. Sa povećanjem upotrebe bežičnih mreža u procesu komunikacije, napadači su posvetili više vremena proučavanju njihovih slabosti i mana, kao i pronalaženju novih načina za njihovo iskorištavanje. Nedostatak kablova i fizičkih barijera, i prenos informacija kroz vazduh, učinili su razmenu informacija putem bežične tehnologije podložniji prisluškivanju i presretanju. Imajući ovo u vidu, ovaj rad se bavi sigurnosnim problemima u bežičnim mrežama. Opšta hipoteza istraživanja je da bežične računarske mreže ne nude adekvatnu sigurnost korisnicima. Posebne hipoteze su:

1. Sigurnosni protokoli još nisu razvijeni do tog nivoa, da bi sigurnost bila približna kao onoj koju nude klasične žičane mreže.
2. Alati potrebni za napade na bežične mrežesu napadačima lako dostupni na Internetu i neki od njih ne zahtevaju visok nivo informatičkog znanja da bi se koristili.

Postoji veliki broj literature koja se bavi sigurnošću u bežičnim računarskim mrežama. Autori su pri istraživanju pošli od radova (Kumkar, Tiwari, Gupta, Shrawne, 2012), (Raza, Iqbal, Sharif, Haider, 2012), (Grubor, Milosavljević, 2010), (Rufi,2006), (Nichols, Lekkas, 2002) iz ove oblasti.

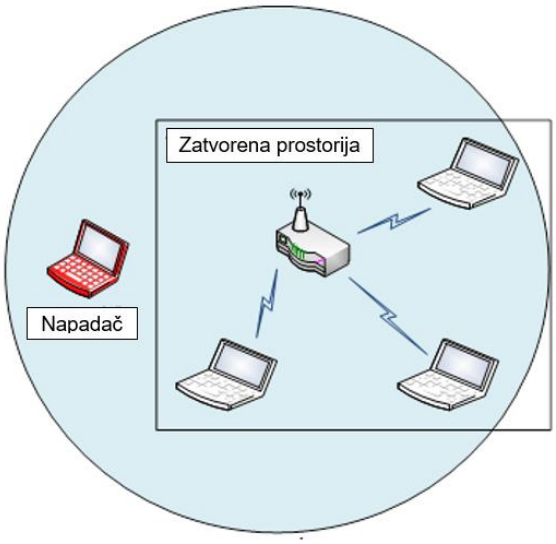
2 BEZBEDNOSNI PROBLEMI BEŽIČNIH RAČUNARSKIH MREŽA

Veća dostupnost informacionih resursa daje bežičnom umrežavanju veću produktivnost i brojne prednosti u odnosu na žičane mreže.

Podešavanje i nameštanje bežične mreže je lakše, brže i jeftinije. Istovremeno, bežična tehnologija stvara nove pretnje i menja sigurnosnu politiku kada su rizici u pitanju. Komunikacija u bežičnim računarskim mrežama odvija kroz vazduh, koristeći radio signale, rizik od presretanja tih informacija je veći nego kod žičanih mreža. U koliko poslata poruka nije šifrovana, ili je šifrovana slabim algoritmom, napadač može da je pročita i samim tim je smanjena poverljivost podataka. Iako bežično umrežavanje dodaje nove rizike ka bezbednosti mreže sa novim pretnjama, bezbednosni ciljevi ostaju isti kao i kod žičanih mreža, a to su: očuvanje poverljivosti, obezbeđenje integriteta i održavanje dostupnost informacija i informacionog sistema.

Prednosti bežičnih računarskih mreža su: pogodnost, mobilnost, produktivnost, raspoređivanje, mogućnost proširivanja i cena. Međutim za neka mrežna rešenja, bežično povezivanje može biti veoma nepoželjno iz više razloga, a to su: sigurnost, domet, pouzdanost i brzina.

Bežične računarske mreže su posebno ranjive iz razloga što je teško sprečiti pristup samoj mreži, slika 1. Jedina prednost toga je što napadač mora fizički biti blizu mreže, što može da ograniči broj potencijalni napadača.



Slika 1: Arhitektura bežične računarske mreže

Međutim, sa antenom, koje su danas lako dostupne, nadapač može da hvata i šalje signal se velike udaljenosti. Iz tog razloga da bi se obezbedila bežična računarska mreža, administrator mora biti upoznat sa slabostima, pretnjama i rizicima bežičnih računarskih mreža. Sve veća upotreba bežičnih LAN (eng *local arena network*) mreža i veliki rast pristupa Internetu sa mobilnih telefona zahtevaju potpuno nove pristupe bezbednosti. Ponekad mali ekrani i nepostojanje fizičke tastature na mobilnim telefonima i tablet uređajima iziskuju promene standardnih pogleda na pristup, identifikaciju i ovlašćenja.

2.1 Slabosti i ranjivosti bežičnih mreža

Ranjivost se može definisati kao slabost u okviru informacionog sistema koju pretnja može eksploatisati. Slabosti su prisutne u mreži, kao i u pojedinačnim uređajima koji čine mrežu. Neki primeri su bežični mreža koja ne koristi šifrovanje, slabe šifre na pristupnim tačkama (eng *Access point* ili AP), ili pristupna tačka koja šalje bežične signale van zgrade. Mreže obično imaju jednu ili sve sledeće slabosti (Grubor, Milosavljević, 2010):

- Tehnologija kao slabost;
- Konfiguracija kao slabost; i
- Bezbednosna politika kao slabost.

Računarske mreže i tehnologije imaju suštinske bezbednosne slabosti (Wekhande, 2006):

- Slabosti TCP/IP protokola -HTTP, FTP i ICMP su nesigurni. *Simple Network Management Protocol* (SNMP), *Simple Mail Transfer Protocol* (SMTP) i SYN „poplave“ se odnosena nesigurnu strukturu na kojima je TCP dizajniran.
- Slabosti operativnih sistema - UNIX, Linux, Macintosh, Windows NT, 9x, 2K, XP, i OS/2 operativni sistemi imaju sigurnosne probleme koji se moraju rešiti.
- Slabosti mrežne opreme - Razne vrste mrežne opreme, kao što su ruteri, *firewall*-ovi i svičevi, imaju bezbednosne slabosti koje moraju biti pronađene i od kojih se mora zaštititi. Ove slabosti mogu biti: zaštita šifrom, nedostatak autentikacije, protokoli rutiranja, *firewall* propusti, itd.

Mrežni administratori moraju da upoznaju slabosti konfiguracije, pravilno podese računare i mrežne uređaje da bi ih otklonili (Barnes, Bautts, Lloyd, Ouellet, Posluns, Zendzian, O'Farrell, 2002):

- Neosigurani korisnički nalozi–Podaci korisničkih naloga mogu biti preneti nesigurno preko mreže, izlažući korisnička imena i šifre za prisluškivačima.

- Sistemski nalozi sa šiframa koje se lako mogu pogoditi - Ovaj uobičajeni problem je rezultat loše odabranih šifri.
- Loše podešene Internet usluge - Uobičajeni problem je da uključite *JavaScript* u pretraživačima, što omogućava napade preko neprijateljskih *JavaScript* kada pristupate neproverenim sajtovima.
- Neosigurana fabrička podešavanja u okviru proizvoda - Mnogi proizvodi imaju podrazumevane postavke koje omogućavaju bezbednosne rupe.
- Loše podešeni mrežni uređaji–Loše podešavanje same opreme može izazvati značajne probleme bezbednosti. Na primer, loše podešene pristupne liste, ruting protokoli mogu otvoriti velike bezbednosne probleme.

Slabosti bezbednosne politike mogu stvoriti nepredviđene pretnje bezbednosti. Mreža može predstavljati sigurnost rizik, ako korisnici ne slede uputstva politike bezbednosti (Raza, Iqbal, Sharif, Haider, 2012):

- Nedostatak pisane bezbednosne politike – Ne postojanje pisane bezbednosne politike onemogućava njenu primenu ili sprovođenje.
- Nedostatak kontinuiteta - Loše izabrane, lako otkrivene ili fabričke šifre mogu dozvoliti neovlašćen pristup mreži.
- Ne postojanje kontrola - Neadekvatno praćenje i revizija omogućuju napade i neprekidnost neovlašćenog korišćenja, što troši resurse kompanije.
- Promene instaliranog softvera i hardvera ne prate politiku - Neovlašćene promene mrežne topologije ili instalacija neodobrenih aplikacija mogu da stvore bezbednosne nedostatke.

Ranjivost se takođe može definisati kao slabost u komunikacionom mediju ili protokolu zbog kog je ugrožena bezbednost mreže. Većina postojećih slabosti u bežični mrežama su uzrokovane od strane medija za prenos. Pošto se saobraćaj na mreži emituje kroz radio signale, on je lako dostupan svakome ko ima odgovarajuću opremu. Slede tipične slabosti koje postoje u glavnoj komponenti bežičnih računarskih mreža, a to je pristupna tačka (AP) (Zhang, Zheng, Ma, 2008):

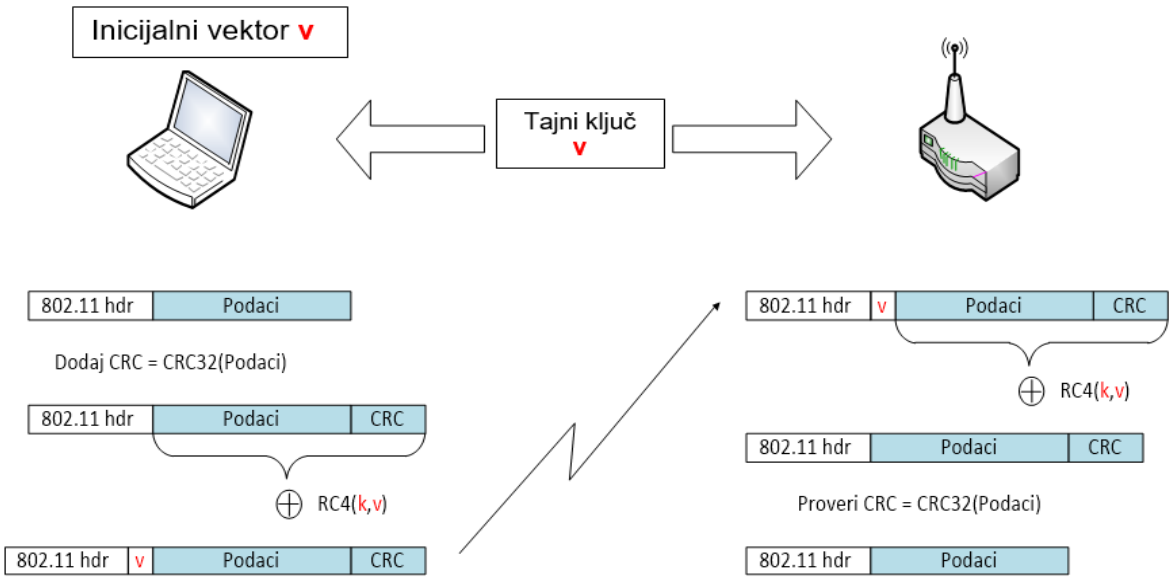
- Domet signala ovlašćenog AP - Ova ranjivost je o mogućnosti proširenja jačine AP signala izvan zadatih perimetara. Shodno tome, pozicioniranje AP-a i jačina signala moraju biti prilagođeni kako bih obezbedili dovoljnu pokrivenost za određenu oblast.
- Fizičko obezbeđenje ovlašćenog AP - AP treba da bude pravilno postavljen kako bi se pre svega izbeglo slučajno oštećenje, ali i onemogućio ne primetan pristup ne ovlaštenim licima samom AP-u.
- Piratski (*Rogue*) AP - Ova ranjivost je vrsta čovek-u-sredini napada, gde napadač može postavite neovlašten (ili piratski) AP na mrežu i konfigurisati ga da izgleda legitimno, što mu omogućuje da dobije pristup osetljivim podacima korisnika bežične mreže. Ovo se događa kada su korisnički uređaji podešeni da se povežu na najjači dostupni signal.
- Jednostavnost instalacije i upotrebe AP-a-U cilju da koriste prednosti internih mreža, zaposleni mogu uvesti neovlaštene bežične mreže. Jednostavna instalacija i konfiguracija AP-a čine ovaj izvodljivim za legitimne ili nelegitimne korisnike.
- AP konfiguracija - Ako AP je slabo konfigurisan ili neovlašćen, onda može da pruži otvorena vrata napadačima. Ovo je izazvano pomoću osnvnih fabričkih podešavanja koja samim tim poništavaju bezbednosne parametre i mehanizme šifrovanja.
- Slabosti protokola i ograničenja kapaciteta na ovlaštenim AP-ovima - Ova ograničenja omogućavaju napade uskraćivanja usluga, od napadača koji koriste neovlaštene AP-ove.

2.2 Slabosti bezbednosnih protokola

Tradicionalni bezbednosni mehanizam za bežične računarske mreže je WEP.WEP je algoritam za šifrovanje dizajniran 1999. godine zajedno sa 802.11b standardnom da pruži bežičnu sigurnost. Međutim, nekoliko ozbiljnih slabosti je identifikovano i WEP je zamenjen *Wi-Fi Protected Access* (WPA) 2003. godine. A zatim potpuno sa IEEE 802.11 i standardom (koji je poznat poznat kao WPA2) 2004. godine. Uprkos ozbiljnim bezbednosnim propustima, WEP i dalje obezbeđuje minimalan nivo bezbednosti.

Prva mera bezbednosti uvedene za bežične računarske mreže je bio WEP (*Wired Equivalent Privacy*). WEP odnosno bezbednost ekvivalentna onoj koju nudi žičana mreža je šema sa ciljem da obezbedi bežične računarske mreže i deo je IEEE 802.11 standarda. Zato što bežične mreže

prenose poruke preko radio signala, posebno su osetljive na prisluškivanje. WEP je trebalo da obezbedi uporedivu poverljivost kao kod tradicionalne žičane mreže. WEP za šifrovanje koristi RC4 algoritam za poverljivost i CRC-32 *checksum* za integritet. Standardni 64-bitni WEP koristi 40-bitni ključ , kome se doda 24-bitni inicijalizacijski vektor (IV) da bi dobili RC4 ključ, slika 2. Međutim WEP je osjetljiv na napade, zbog ranjivosti RC4 algoritma, koji se može probiti i omogućiti pristup mreži (Hulin, Locke, Mealey, Pham, 2010).



Slika 2: Funkcionalni model WEP protokola

Inicijalni vektor (IV) se šalje kao čisti tekst (*plaintext*) sa šifrovanim paketom. Dakle, svako može lako da oslušne ovu informaciju iz radio signala i tako sazna prva tri karaktera ili tajni ključ. IKSA (*Key Scheduling Algorithm*) i PRGA (*Pseudo Random Generation Algorithm*) odaju informacije tokom prvih nekoliko iteracija njihovog algoritma. XOR (ekskluzivno ili) je jednostavan proces koji se lako može koristiti da se dobije nepoznata vrednost, ako su druge dve vrednosti poznate. Format je (B + 3, 255, x), gde je B bajt tajnog ključa koji se razbija.

U cilju otkrivanja WEP ključa bežične pristupne tačke, mora se sakupiti veliki broj IV. Normalan mrežni saobraćaj obično ne generiše IV veoma brzo. Teoretski, ako se strpljivo, može se skupiti dovoljno IV za razbijanje WEP ključa, jednostavno osluškujući mrežni saobraćaju i snimajući ih (Kumkar, Tiwari, Tiwari, Gupta, Shrawne, 2012). U cilju ubrzavanja procesa može se koristiti tehnika ubrizgavanja (eng *injection*). Ubrizgavanje podrazumeva slanje izabranih paketa sa pristupne tačke iznova i iznova veoma brzo. Ovo omogućava da se snimi veliki broj IV u kratkom vremenskom periodu. Kada se uhvati veliki broj IV, koriste se da se otkrije WEP ključ. U praksi WEP se lako razbija pomoću alata kao što su *Aircrack*, itd. Slabosti WEP-a su (Kumkar, Tiwari, Tiwari, Gupta, Shrawne, 2012):

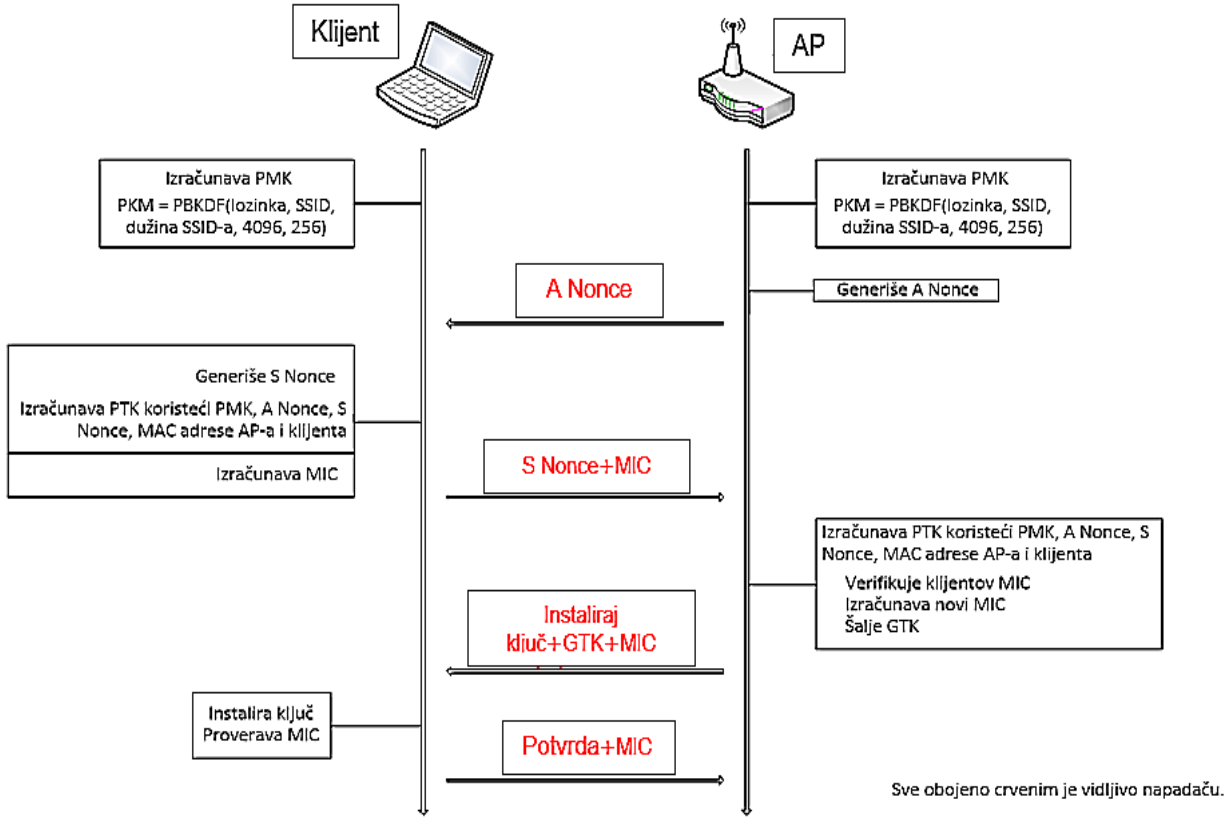
- WEP ne sprečava falsifikovanje paketa .
- WEP ne sprečava ponovne napade (eng *replay attacks*). Napadač može jednostavno snimite i ponovo slati pakete po želji, i da će biti prihvaćeni kao legitimni.
- WEP koristi RC4 algoritam. Ključevi koji se koriste su veoma slabi, a mogu se otkriti na standardnim računarima u roku od nekoliko sati do nekoliko minuta, i to koristeći slobodno dostupan softver.
- WEP vise puta koristi iste inicijalne vektore. Raznolikost dostupnih kriptoanalitičkih metoda može da dešifruje podatke bez znanja ključ za šifrovanje.
- WEP omogućava napadaču, bez da bude otkriven, da izmenite poruku bez poznavanja ključ za šifrovanje.
- Nedostaje upravljanje ključevima.

Wi-Fi Protected Access (WPA), je poboljšani bezbednosni standard za bežične mreže, dizajniran da zameni manje bezbedan WEP protokol. WPA koristi 128-bitnu enkripciju ključa i dinamičke ključeve za sesiju da obezbedi

privatnost bežične mreže. WPA je dizajniran za upotrebu sa 802.1X serverima za autentikaciju, koji raspodeljuje različite ključeve za svakog korisnika. Međutim, može da se koristi u manje bezbednom *pre-shared key* (PSK) modu, gde je svaki korisnik dobije istu frazu za prolaz (eng *pass-phrase*). Podaci se šifruju pomoću RC4 algoritma za šifrovanje sa 128-bitnim ključem i 48-bitnim inicijalnim vektorom (IV). Jedan od glavnih poboljšanja u odnosu na WEP je *Temporal Kei Integriti Protocol* (TKIP), koji dinamički menja ključeve u toku rada sistema. Kada je u kombinaciji sa mnogo većim IV, postaje otporniji na napade kojima je WEP bio ranjiv. Pored autentifikacije i šifrovanja, WPA takođe pruža znatno poboljšan integritet podataka. WPA u odnosu na WEP koristi sigurniji algoritam za autentikaciju pod nazivom MichaelMIC (*Message Integrity Code*), koji uključuje i brojač okvira što ga čini još sigurnijim u odnosu na WEP (Zhang , Zheng, Ma , 2008).

WPA je uradio odličan posao rešavanja problema u WEP-u. Sa samo softverskom nadogradnjom, WPA je ispravio skoro svaki bezbednosni problem koji je WEP stvorio ili ignorisao. Međutim, WPA je stvorio nove problem (Hulin, Locke, Mealey, Pham, 2010):

- Jedna greška dozvoljava napadaču da izazove napade uskraćivanja usluga, ako napadač uspe da zaobiđe i nekoliko drugih slojeva zaštite.
- Drugi propust postoji u metodu kojom WPA inicijalizuje svoje šifrovanje.



Slika 3: WPA rukovanje iz četiri koraka

Tokom rukovanja pristupna tačka i svaka stanica trebaju individualni PTK ključ (*Pairwise Transient Key*), da štiti jednosmernu komunikaciju između njih. PTK je izveden iz PMK ključa (*Pairwise Master Key*), i fiksnog stringa, MAC adrese pristupne tačke, MAC adrese klijenta i dva slučajna broja. WPA-PSK slabost je zasnovana na PMK ključu, koji je izveden iz sklopa zajedničke šifre, SSID-a, dužine SSID-ai *nonce*-a (broj ili bit koji se koristi samo jednom u svakoj sesiji). Algoritam je PMK = PBKDF2 (šifra, SSID, SSID dužina, 4096, 256). Dobijeni string sepretresa 4.096 puta da generiše 256-bitnu vrednost, a zatim u kombinaciji sa vrednosti *nonce*-a. Kao što je već pomenuto, PTK je izvedena iz PMK pomoću rukovanja iz četiri koraka (*4-Way Handshake*) i svi podaci koji se koristi za izračunavanje njegove vrednosti prenose se u obliku čistog teksta(eng

plain text), slika 3. Po zauzimanju rukovanja, imaju se podaci potrebni da se šifra podvrgne napadu korišćenjem rečnika (Raza, Iqbal, Sharif, Haider, 2012).

WPA2 je nadogradnja na WPA. Konkretno MIC (*Michael*) algoritam je zamenjen sa CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) kodom za autentikaciju poruka, koja se smatra u potpunosti bezbedna (Kumkar, Tiwari, Gupta, Shrawne, 2012), i RC4 je zamenjen sa AES (*Advanced Encription Standard*). WPA2 daje bežičnim mrežama kako poverljivost podataka tako i integritet. Tabela 1. prikazuje poređenje bezbednosni protokola za bežične računarske mreže.

Tabela 1. Bežični bezbednosni protokoli

Opis	WEP	WPA	WPA2
Autentikacija	Nema	IEEE 802.1x/EAP/PSK	IEEE 802.1x/EAP/PSK
Kriptografski algoritam	RC4	RC4	AES
Veličina ključa	40 ili 104 bita	128 bita	128 bita
Metod enkricpije	WEP	TKIP	CCMP
Dužina inicijalizacijskog vektora	24 bita	48 bita	48 bita
Brojač okvira	Ne	Da	Da

2.3 Pretnje bežičnih računarskih mreža

Pretnja je indikacija o nameri da se izazovu smetnje u informacionom sistemu (Grubor, Milosavljević, 2010). Neki primeri pretnji su hakeri, nezadovoljni zaposleni, kao i zlonamerni softver (virusi, trojanci, itd.). Postoje četiri osnovna klase pretnji bezbednosti mreže. Lista koja sledi opisuje svaku klasu pretnji u par reči.

- *Nestrukturisane pretnje* - Nestrukturisane pretnje su uglavnom od strane neiskusnih pojedinaca koji koriste lako dostupne hakerske alate kao što su skripte i razbijači šifri.
- *Strukturisane pretnje* - Strukturisane pretnje dolaze od napadača, koji su više motivisani i tehnički kompetentani. Ovi ljudi znaju sistemske slabosti i mogu da razumeju i razviju zlonameran kod i skripte..
- *Spoljne pretnje* - Spoljni pretnje mogu nastati od strane pojedinca ili organizacije koji rade izvan kompanije, inemaju ovlašćen pristup računarskom sistemu ili mreži.
- *Unutrašnje pretnje* - Unutrašnje pretnje se dešavaju kada neko ko ima ovlašten pristup mreži,da li sa nalogom na serveru ili fizički pristup na mrežu, vrši zloupotrebu.

Kako su vrste pretnji, napada i eksploatacija napredovali, dodeljivani su nazivi da bi se opisale različite vrste napadača (Grubor, Milosavljević, 2010). Neki od najčešćih termina su:

- *Haker (eng Hacker)* je opšti pojam koji je istorijski korišćen da opiše stručnjaka za programiranje. Međutim ovaj termin se najčešće koristi u negativnom smislu da opiše osobu koja pokušava da dobije neovlašten pristup mrežnim resursima sa zlom namerom.
- *Kraker (eng Cracker)* je termin za koji se generalno smatra da preciznije opisuje osobu koja pokušava da dobije neovlašćen pristup mrežnim resursima sa zlomnamerom.
- *Spamer (eng Spammer)* je pojedinac koji šalje veliki broj neželjenih e-mail poruka. Spameri često koriste viruse da preuzmu kontrolu nad kućnim računarima da bi ih iskoristili za slanje svojih masovnih poruka.
- *Fišer (eng Phisher)* koristi e-mail ili druga sredstva u pokušaju da prevare druge da im odaju osetljive informacije, kao što su brojevi kreditnih kartica ili šifre. Fišer se maskira kao pouzdana stranka koja bi imala legitimnu potrebu za tim informacije.
- *Beli šešir (eng White hat)* je termin koji se koristi da se opiše osoba koja koriste svoje sposobnosti da pronađe ranjivosti u sistemima ili mrežama, a zatim izvesti vlasnike sistema o ovim ranjivostima, da bi one mogle biti ispravljene.
- *Crni šešir (eng Black Hat)* je još jedan termin za pojedince koji koriste svoje znanje o računarskim sistemima da se probiju u sisteme ili mreže, a za koje nisu ovlašćeni da ih koriste.

WLAN odnosno bežični LAN, radi na isti način kao i žičani LAN, osim što se podaci transportuje preko bežičnog medija, odnosno najčešće radio talasa, u odnosu na kablove. Shodno tome WLAN ima mnoge iste ranjivosti kao žičani LAN, plus neke koje su specifične za njega. Razmotrićemo neke od uobičajenih pretnji sa kojima se suočavaju bežične računarske mreže.

2.3.1 Prisluškivanje

Glavna pretnja jepotencijal da neovlaštena lica prisluškuje radio signale koji se razmenjujuizmeđu bežične stanice i jednog AP-a, kompromitujući poverljivostinformacija. Prisluškivanje jepasivan napad. Kada AP šalje poruku preko radio talasa, svi ostali korisnici opremljeni kompatibilnim prijemnikom, koji se nalaze u rasponu prenosa signala mogu da osluškuju poruke. Osim toga, prisluškivač može da osluškuje poruke bez promene podataka, tako da pošaljilac i primalac poruke nisu ni svesni toga (Kumkar, Tiwari, Gupta, Shrawne, 2012).

Da bi neko prisluškivao bežičnu mrežu može da se nalazi i na određenoj udaljenosti od mreže,a može čak biti i van fizičkih granica sredine u kojoj mreža funkcioniše. To je zato što radio signali koje emitujebežična mreža mogu da propagiraju van oblasti u kojima nastaju, a mogu da prodiru zidove zgrade i druge fizičke prepreke, u zavisnosti od tehnologije prenosa koju koriste i snage signala. Oprema sposobna da presrećebežični saobraćaj je na raspolaganju potrošačima uobliku bežičnih adaptera i drugih proizvoda kompatibilnih sa standardom 802.11.

2.3.2 Neovlašćeno korišćenje

Druga pretnja bezbednosti bežičnih mreža je potencijal za napadače da uđu u sistem bežične mreže maskirani kao ovlašteni korisnici. Jednom unutra, napadač može kršiti poverljivost i integritet mrežnog saobraćaja slanjem, primanjem, menjanjem ili falsifikovanjem poruka. Ovo se smatra aktivnim napadom, i može se sprovesti pomoću bežičnog adapter koji je kompatibilan sa ciljanom mrežom ili pomoću ugroženog (ili ukradenog), uređaja koji je povezan na mrežu.

Jedan od načina neovlaštenog pristupa je napadač koji obmanjuje bežične stanice postavljanjem piratskog AP-a. Kada se bežična stanica prvi put uključi ili kada se implementira u novi sistem, ona bira AP sa kojim će se povezati na osnovu jačine signala. Ako bude prihvaćena od strane AP-a, stanica počinje da koristiradio kanal koji i AP koristi. Postavljanjem lažnog AP-a sa jakim signalom, napadač može da privuče stanicu na njegovumrežu u cilju krađe tajnih ključeva i šifri. Nasuprot tome, napadač može odbaciti pokušaje prijavljivanje, ali snimiti poruke prenete tokom procesa prijavljivanja u istom cilju. Prvi tip napada je veoma teško sprovesti, jer napadač mora imati detaljne informacije da bi mogao da prevari stanicu uveravajući je da je pristupila svojojmatičnoj mreži. Druga vrsta napada je lakše za sprovesti, jer napadač zahteva samo prijemnik i antenu koji su kompatibilan sa ciljanim stanicama. Ovaj napad je takođe teži za otkriti, jer su neuspeli pristupi relativno uobičajeni u bežičnoj komunikaciji (Raza, Iqbal, Sharif, Haider, 2012).

2.3.3 Smetnje i ometanje

Treća pretnja bezbednosti bežičnih mreža su radio smetnje koje mogu ozbiljno smanjiti propusni opseg (protok podataka). U dosta slučajeva smetnje su slučajne, jer bežične mreže koriste ne licencirane radio talase, gde recimo i drugi elektromagnetni uređaji rade 2.4GHz radio frekventnom opsegu i mogu se preklapati sa saobraćajem bežičnih računarskih mreža. Potencijalni izvori mešanja uključuju predajnike visoke energije, koji mogu biti u amaterske, vojne, industrijske, naučne svrhe. Druga briga je rad dve ili više bežičnih mreža u istoj zoni pokrivenosti.

Naravno, smetnje mogu biti i namerne. Ako napadač ima moćan predajnik, on može da generiše radio signal dovoljno jak da nadvlada slabije signale, i samim tim ometa komunikaciju. Ovo stanje poznato kao ometanje (eng *jamming*), odnosno uskraćivanje usluga (eng *Denial-of-service*-DoS) (Raza, Iqbal, Sharif, Haider, 2012). Dve vrste ometača mogu da se koriste u cilju ometanja bežičnog saobraćaja, i to ometači velike snage koje pokrivaju ceo frekvencijski spektar kog koristi ciljani signali, i ometači manje snage koji pokrivaju samo deo frekvencije koju koriste ciljani signali. Oprema za ometanje je dostupna potrošačima, ili može biti napravljena od stane napadača koji poseduju to znanje. Pored toga, ometanje se može vršiti sa lokacije udaljene od ciljane mreže (najčešće iz vozila parkiranog u blizini).

2.3.4 Fizičke Pretnje

Bežične računarske mreže se mogu oboriti oštećenjem ili uništenjem osnovne fizičke infrastrukture. Kao kod žičane mreže, i infrastruktura bežične mreže oslanja se na različitim fizičke komponenti, uključujući pristupne tačke, kablove, antene i bežične adaptere i softver. Oštećenja na bilo koji od ovih komponenti može dovesti do smanjenja signala, smanjiti granicu pokrivanja signalom, ili smanjiti protok,

samim tim ometati sposobnost korisnika za pristup podacima i informacijama. Ako su dovoljno velika, oštećenja fizičke infrastrukture mogu čak dovesti i do gašenja bežične mreže. Infrastrukturne komponente su osetljivi na uslove životne sredine u kojima rade, pogotovo ako su napolju. AP-ove mogu da se ometaju sneg, led, i drugi radio signali. Antene montirane na vrhu stubova ili objekata mogu biti savijene od strane vetra ili leda, menjajući ugao prostiranja signala. Ovo može biti posebno problematično za antene sa uskom širinom snopa signala. Zatim AP-ovi mogu biti oštećeni obližnjim udarom groma Konačno, nesreće, kao i nepravilno rukovanje može oštetiti bežične adaptere i bežične stanice (Hulin, Locke, Mealey, Pham, 2010).

Fizičke komponente takođe mogu biti predmet napada. Na primer, napadač može da iseče kablove koji povezuje AP sa žičanom mrežom. Napadač takođe može biti u mogućnosti da ošteti ili uništi izložene AP-ove ili antene povezane sa njim.

Rizici u vezi sa ugroženim bežičnim mrežama su: pun pristup podacima koji se prenose ili su čak smešteni na serveru; ukradene šifre; presretnuta e – pošta; tačka koja omogućava ulaz kroz takozvana zadnja vrata (eng *back-door*) u vašu žičanu mrežu; napadi uskraćivanja usluga koji izazivaju zastoje i smanjenje produktivnosti; povrede državnih ili međunarodnih zakona i propisa koji se odnose na privatnost, finansijsko izveštavanje, itd.; "*zombiji*" -napadači koji koriste vaš sistem da napadnu druge mreže, i to tako da vi izgledate kao negativci; s*pamovanje* – napadač koristi vaše*-mail* server ili radne stanice za slanje spam-a, trojanaca, virusa ili drugih besmislenih *e-mail*-ova.

3 NAPADI NA BEŽIČNE RAČUNARSKE MREŽE

Napadači imaju mnogo razloga za napade na bežične mreže. Oni možda žele da pristupe resursima na mreži, kao što su poverljivi podaci, ili da ostvare pristup ka žičanoj mreži. Drugi napadači možda jednostavno žele da se priključe na Internet, ne želeći da plaćaju za tu uslugu. Zatim to može biti napadač koji želi da pošalje veliku količinu elektronske pošte (eng *spam mail*) koji neće moći da se prati nazad do njega, ili neko ko je napisao crva, i želi da ga distribuiše sa sigurne lokacije. Na kraju to može biti napadač koji želi da poremeti bežičnu mrežu, da li iz lične satisfakcije, ili iz želje da napravi štetu konkurentu. Bežične računarske mreže imaju slabosti kao i sve žičane mreže, tako i slabosti svojstvene 802.11 mrežama.

Bežične mreže su predmet i pasivnih i aktivnih napada. Pasivni napad je onaj u kom napadač hvata signale, dok je aktivni napad onaj u kom napadač i šalje signale. Pasivni napadi su izuzetno lako sprovesti, i praktično se nemogu otkriti. Napadi na bežične računarske mogu biti:

Netehnički napadi

Ove vrste napada koriste različite ljudske slabosti, kao što su nedostatak svesti, nebriga, i suviše poverenja prema strancima. Takođe postoje fizičke ranjivosti koje napadač može da iskoristi da bi pristupio važim bežičnim uređajima, koje su nekada najjednostavnije za iskoristiti. Ovi napadi uključuju:

- Pristup do bežičnih uređaja koji su korisnici sami instalirali i ostavili neobezbeđene.
- Takozvani socijalni inženjering napadi, kada se napadač predstavlja kao neko drugi i ubeđuje korisnike da mu daju previše informacija o vašoj mreži.
- Fizički pristup pristupnim tačkama, antenama i drugim uređajima bežične infrastrukture da bi ih rekonfigurisali ili ukrali podatke sa njih.

Mrežni napadi

Postoji mnogo tehnika koje napadači mogu da koriste da sebi omoguće pristupu vašu bežičnu mrežu (Grubor, Milosavljević, 2010). Ti napadi mogu biti:

- Instaliranje lažnih bežičnih pristupnih tački i varanje bežičnih klijenata u povezivanje sa njima.
- Snimanje podataka sa mreže iz daljine, šetajući ili vozeći se okolo.
- Napad na mrežne transakcije putem obmane MAC adresa (eng*MAC spoofing*) maskiranjem kao legitimnog bežičnog korisnika, postavljanje čovek-u-sredini napada,..itd.
- Iskorištavanje mrežnih protokole kao što SNMP(*Simple Network Management Protocol*).
- Napadi uskraćivanja usluga.
- Ometanje radio signala.

Softverski napadi

Kao da bezbednosni problemi sa 802.11 protokolom nisu bili dovoljni, sada morate da brinete i o operativnim sistemima i aplikacijama na računarima klijenata koji koriste bežičnu mrežu, koji mogu biti ranjivi na napada (Beaver, Davis, 2005). Evo nekih primera softver napada:

- Hakovanje operativnog sistema ili drugih aplikacija na računarima klijenata koji koriste bežičnu mrežu.
- Upadi preko fabričkih podešavanja kao što su SSID i šifre koje se lako utvrđuju.
- Razbijanje WEP ključeva i ulazak mrežni sistem šifrovanja.
- Dobijanje pristupa iskorištavanjem slabog sistema autentikacije.

Napadi na mreže su klasifikovani u sledeće četiri primarne klase (Raza, Iqbal, Sharif, Haider, 2012).

Izviđanje– Izviđanje (eng. *reconnaissance*) je neovlašteno otkrivanje i mapiranje sistema, usluga i slabosti. U suštini to je prikupljanje informacija o bežičnoj mreži, sa ciljem da se iskoriste prilikom neke druge vrste napada.

Pristup–Pod ovim se po podrazumeva sposobnost neovlaštenog korisnika da dobije pristup uređaju ili resursu za koji on nema korsnički nalog I šifru. Da bi to postigao napadač obično koristi softverske alate koji iskorištavaju poznate slabosti sistema ili aplikacija koji se napadaju.

Uskraćivanje usluga–Pod ovim napadima se podrazumeva da napadač onemogućava ili kvari mreže, sisteme ili servise, sa namerom da onemogući usluge korisnicima kojima su namenjene. Napadi uskraćivanja usluga uključuju ili obaranje sistema ili usporavanje istog do tačke kada je ne upotrebljiv.

Crvi, virusi i trojanci–Maliciozni program je kod koji se tajno ubacuje u drugi program sa namerom da se nanese šteta, unište podaci, pokrenu destruktivni programi ili kompromituje bezbednost informacija.

I na kraju podela napada prema cilju koji napadač želi da ostvari (Grubor, Milosavljević, 2010), a zatim ćemo opisati neke od najčešćih napada:

- Napadi neovlaštenog pristupa – cilj ovih napada je da se prodre u bežičnu računarsku mrežu koristeći ili zaobilazeći mere kontrole pristupa na bežičnoj mreži. Neki od napada sa ovim ciljem su: *War Driving, Rogue Access Points, Ad Hoc Associations, MAC Spoofing*.
- Napadi na poverljvost – Ovi napadi za cilj imaju presretanje privatnih informacija poslatih preko bežične mreže, bez obzira da li su poslati sa enkripcijom ili bez. U ove napade se ubrajaju: *Eaves dropping, WEP Key Cracking, Evil Twin AP, AP Phishing, Man in the Middle*.
- Napadi na integritet - Ovi napadi šalju pakete sa lažnim podešavanjima, podacima itd. preko bežične mreže sa ciljem da se obmane primalac poruke, ili da se izvrši priprema za neku drugu vrstu napada, npr. DoS. Ovi napadi su: *802.11 Frame Injection, 802.11 Data Replay, 802.1X EAP Replay, 802.1X RADIUS Replay.*
- Napadi na dostupnost - Ovi napadi za cilj imaju otežavanje ili onemogućavanje pružanja usluga bežične mreže legitimnim korisnicima.U ove napade ubrajamo raznenapade uskraćivanja usluga: *802.11 Associate/Authenticate Flood, 802.11 TKIP MIC Exploit, 802.11 Deauthenticate Flood, 802.1X EAP-Start Flood* itd.

3.1 Wardriving

Wardriving je praksa traženja bežične mreže u pokretu (Grubor, Milosavljević, 2010). Prvobitno se mislilo na ljude u potrazi za bežičnim mrežama koji se vozi u automobilima, ali je to danas termin koji se generalno odnosi na ljude u potrazi za bežičnim mrežama dok se kreću.

Zahvaljujući odsustvu fizički barijera, bežičnom medijumu, a samim tim i bežičnoj mreži se lako dostupno. Danas je provera za prisustvo neke vrste bežične mreže veoma jednostavno, dovoljno je samo uključiti bežični interfejs i čekati. Ova akcija je sami osnov *wardriving*-a, termin koji se prvobitno odnosio na aktivnost „voziti unaokolo i tražiti bežične mreže“. Danas ova aktivnost podrazumeva tri koraka: 1. pronalaženje bežične mreže, 2.Određivanje geografski koordinata pomoću GPS uređaja, i 3. Objavljivanje lokacije na specijalizovanim sajtovima da se obogati *wardriving* zajednica.

Sa povećanjem broja bežičnih mreža, posebno onih na osnovu isplativih IEEE 802.11 tehnologija, potraga za bežičnim signalimaje veoma jeftina aktivnost. Jedan od razloga je i to što se IEEE

802.11 tehnologija prvobitno oslanjala (i još uvek se oslanja) na slabe bezbednosne mehanizme. Pored toga, mnogi korisnici nesvesno koriste svoje bežične mreže, bez aktiviranja bilo kakvih mehanizama za poverljivost, integritet i dostupnost, što otvara vrata napadačima.

Drugi termin koji je nastao uz *wardriving* je ***warchalking***. *Warchalking* je crtanje (*chalk* - kreda) simbola na javnim mestima (zidovi, trotoari, zgrade, znakovi, drveće) da se ukaže na postojanje bežične mrežne konekcije, koja obično nudi Internet vezu, tako da i drugi mogu imati koristi od besplatnog bežičnog pristupa.

3.2 Napadi na šifre

Napadi na šifre mogu biti realizovan pomoću nekoliko metoda, uključujući napad sirove sile (eng. *brute fotce attack*), trojance, lažiranje IP adresa i snimanje paketa. Iako lažiranje IP adresa i snimanje paketa mogu dati korisničke naloge i šifre, pod napadima na šifre se obično smatraju ponavljani pokušaji da se identifikuje korisnički nalog ili šifra, ili oboje. Ovi napadi se vrše pomoću programa koji su danas veoma lako dostupni. Preko njih napadač pokušava doći do nekog resursa na mreži, kao što je server. I ako uspe, ima iste privilegije kao nalog koji je kompromitovan, a ako nalog ima više privilegije, napadač može napraviti zadnja vrata (eng. *back door*) koji će mu omogućiti kasnije ponovni pristup. Dva metoda otkrivanja šifri su napad rečnikom i napad sirovom silom.

Napad rečnikom (eng. *dictionary attack*) je metod probijanja sigurnosnih sistema, pre svega otkrivanja šifre tih sistema, i to na taj način što unosi svaku reč iz rečnika kao moguću korisničku šifru. Napad rečnikom se takođe može koristiti za pronalazak ključa kojim se šifruju poruke ili podaci (Grubor, Milosavljević, 2010). Ovi napadi se vrše pomoću programa, u kojima se može podesiti da se recimo počinje sa rečima koja imaju veću šansu da se koriste kao šifre, npr. vlastita imena, imena lokacija itd. Napad rečnikom radi iz prostog razloga što veliki broj korisnika računara koristi obične reči kao šifre. I ovaj metod je veoma brz u pronalaženju šifru i tom slučaju. Međutim ovi napadi su retko uspešni protiv sistema koji koriste šifre od vise reči, a možemo reći neuspešni protiv sistema koji u šiframa koriste nasumične kombinacije velikih i malih slova, brojeva i specijalnih karaktera.

Za razliku od napada rečnikom, napad sirovom silom (eng. brute force attack) će u svojim iteracijama proći kroz svaku moguću kombinaciju znakova npr: aaaaaaa, aaaaaab, aaaaaac, aaaaaad, itd. Prilikom podešavanja programa za ove napade može se navesti da li će se koristiti samo slova od A do Z, ili i cifre od 0 do 9, ili i specijalni karakteri. Šifra će se uvek pronaći ako se sastoji od karaktera koji su izabrani da se koriste u proveri. Međutim najveći nedostatak ovih napada je vreme potrebno da se pronađe šifra. Ako na primer korisnik unese šifru od 8 karaktera, i gde su svi karakteri mala slova engleske abecede, to znači 26^8 mogućih kombinacija, što je jednako 208827064576. Ako jedan računar može da proveri 1000 šifri u jednoj sekundi, onda je potrebno vreme da bi se proverile sve šifre 208827064576/1000= 208827064,576 sekundi, što je opet 58007,52 sata (Beaver, Davis, 2005). Ovo pokazuje da je napad sirovom silom efikasniji kada su u pitanju kraće šifre.

3.3 MAC Spoofing

Jedan od prvih pokušaja obezbeđivanja bežičnih računarskih mreža je bio da se sprovede filtriranje MAC adresa. Ova jednostavna tehnologija je uključivala listu MAC adresa kojima je dozvoljeno da se povežu na AP, i listu MAC adresa kojima nije bio dozvoljen pristup na AP.

Ova radnja se zasniva na činjenici da su sve IEEE 802.11 kartice za pristup mreži bežičnim putem imaju fizičku adresu poznatu kao MAC adresa. MAC adresu drajver mrežne kartice obično čita sa samog hardvera, ali korisnik može namestiti da drajver mrežne kartice ignoriše ono što je pročitao sa hardvera i koristi drugu MAC adresu.

Problem predstavlja to što mnogi uređaji imaju MAC adresu koja je navedena kao parametar za konfigurisanje,a MAC adresa može biti lako ukradena ili lažirana (eng. *spoofed*). Jedna od definicija *spoofing*-a je da je napadač u mogućnosti da prevari mrežnu opremu da misli da je veza koju ostvaruje validna i da omogući pristup mrežnim resursima. Ako napadač otkrije važeću MAC adresu, on lako može promeniti MAC adresu svoje kartice da odgovara važećoj. Pored ugrađenog interfejsa većine bežičnih kartica, postoje razne aplikacije koje se mogu korstiti za promenu MAC adrese vaše bežične kartice, kao što je SMAC (Spoof MAC Address) ili TMAC (*Technitium Mac Address Changer*).

Koristeći jednostavne alate za prisluškivanje, napadač može brzo odrediti MAC adresu korisnika koji je povezan na AP. A ako su povezani to znači da je korisnikova MAC adresa u listi trenutno dozvoljenih adresa na tom AP-u. Sve što napadač sada treba da uradi je da konfiguriše svoju MAC adresu, a zatim se poveže sa datim AP-om (Beaver, Davis, 2005).

3.4 Prisluškivanje

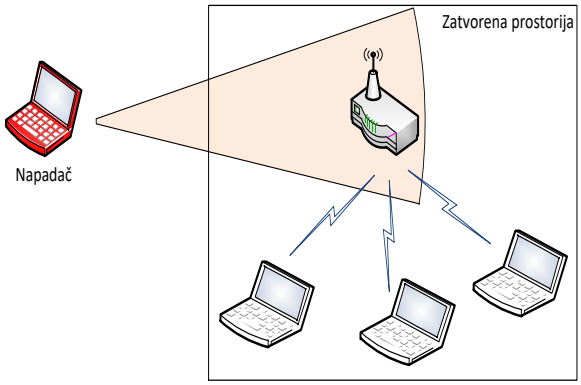
Pod prisluškivanjem (eng. *eavesdropping*) se podrazumeva radnja prikupljanja informacija iz mreže hvatanjem paketa koji se prenose, odnosno neovlašteno presretanje privatne komunikacije. Informacije ostaje netaknuta, ali je njegova privatnost ugrožena. Termin proizilazi iz situacije kada jedna osoba prisluškuje razgovor druge dve osobe bez njihovog znanja. Izraz koji se takođe često koristi kada se misli na prisluškivanje bežičnih mreža je *sniffing* (njušenje). Prisluškivanje ima svrhu kada se hvataju ne šifrovani podaci, ili šifrovani, kada se posjeduje ključ za njihovo dešifrovanje. Od prisluškivanja nema neke koristi ako se hvataju šifrovani podaci koje nismo u stanju da dešifrujemo.

Zahtevi znanja i veština potrebnih za prisluškivanje bežičnog prenosa nisu previsoki, a tehnologija, hardver i softver je lako dostupan.Danas postoje brojne aplikacije koje se mogu korstiti u svrhu prisluškivanja, kako besplatne tako i komercijalne. Neke od njih su: *OmniPeek Personal, AiroPeek, Network Instruments Observer, AirMagnet Laptop Analyzer, Jawin CAPSA, WireShark* itd (IEEE Std 802.11b,1999).

Kada koristite ne zaštićenu mrežu napadač koji prisluškuje mrežu će biti u stanju da hvata podatke kao što su: Internet prezentacije koje posjećujete, podaci koji se šalju preko mreže, korisničke naloge i šifre koje koristite za pristup raznim servisima itd.

3.5 Uskraćivanje usluga

Postoje mnoge metode onemogućavanja dostupnosti (eng *Denial-of-Service - DoS*) bežičnih pristupnih tačaka. Ovi napadi ne dozvoljavaju napadaču da dobije neovlašten pristup mreži, ali oni su u stanju da poremete usluge legitimnim korisnicima. Pošto bežične mreže koriste radio signale za prenos podataka, da se poremeti usluge dovoljno je samo emitovanjem buke na kanalu, slika 4.



Slika 4: Ometanje pristupne tačke

Međutim, ovo zahteva veliku snagu prenosa i lako je ući u trag izvoru prekida. Tako, neki od glavnih ciljeva DoS napada su da izbegnu otkrivanje, i održavanje ometanjau najdužem mogućem roku (Beaver, Davis, 2005).

Napad održavanje ometanja (*The Transmit Duration attack*) koristi algoritam za izbegavanje sudara 802.11 protokola. 802.11 okviri sadrže polje u kome se nalazi vreme trajanje prenosa, koje omogućava čvoru da rezerviše kanal i do tridesetog dela sekunde. Ako napadač ubacuje pakete u mrežu sa maksimalnim trajanjem prenosa, onda će drugi čvorovi morati čekati da počnu sa svojim prenosom. Tako napadač tada može zauzeti kanal mreže slanjem 30 paketa u sekundi. Ovo je jednostavan, i efikasan način da napadač obori mrežu, ali to zahteva mogućnost ubrizgavanja paketa u mrežu.

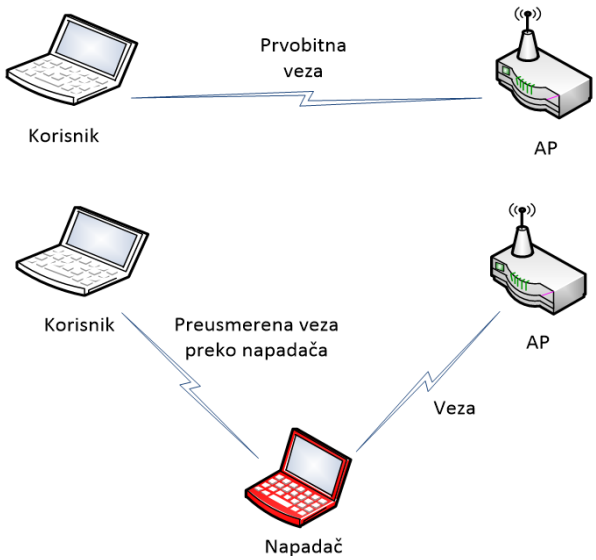
DoS napad nasumičnim uništavanjem paketa (*The Random Packet Destruction DoS attack*) dizajniran je da bude energetski efikasan, težak za detekciju, a lak za izvođenje. Ovaj napad je dizajniran da funkcioniše čak i kada ne postoji način da se upadne u mrežu ili ubrizga pakete u mrežu. Sve što je neophodno da ovaj napad radi je sposobnost da detektuje prenose paketa preko bežične mreže. Napad slučajno uništava pakete sa verovatnoćom *p* na mreži emitujući buku na kanalu u kratkim vremenskim periodima (minimum oko 10 mikrosekundi). Pod pretpostavkom da se TCP koristi za mrežni saobraćaj, istraživači su pokazali da ako je *p* 40%, stopa gubitka TCP paketa će biti oko 20%, što je dovoljna da sruši mrežu. Dok to ne utiče značajno na propusnost, za napad sepokazalo da degradira CBR (*constant bit rate*) saobraćaj, kao što su VoIP (*Voice over*

IP), povećanjem neželjenih odustajanja i odlaganja. DoS napadi mogu ciljati različite slojeve mreže kao što su (IEEE Std 802.11a, 1999):

- Sloj aplikacije : DoS napad se dešava kada se šalje velika količina legitimnih zahteve. Ima za cilj da onemogući drugim korisnicima pristup servisu, primoravajući server da odgovora na velikom broj transakcionih zahteva.
- Transportni sloj: DoS napad je kada su šalje mnogo zahteva za uspostavljanje veze. Meta je operativni sistem računara koji se cilja. Tipičan napad u ovom slučaju je *SYN„*plavljenje".
- Mrežni sloj: DoS napad zahteva da mreža dozvoli pristup korisniku. Tada napadač može preplaviti mrežu sa saobraćajem da odbije pristup drugim uređajima. Ovaj napad se može sastojati od sledećih koraka:
  - zlonamerni čvor učestvuje u saobraćaju, i samo ubacuje po nekoliko paketa podataka. Ovo izaziva pogoršavanje veze.
  - zlonamerni čvor odašilje falsifikovano ažuriranje rute saobraćaja ili stara ažuriranja ruta. Ovo može rezultirati neuspelim rutama, sto pogoršava performanse.
  - zlonamerni čvor smanjuje *time-to-live* (TTL) polje u zaglavlju IP paketa, tako da paket nikada ne stiže do odredišta.
- Sloj veze: DoS koji cilja sloj veze može se izvršiti na sledeći način:
  - Ako smo pretpostaviti da postoji jedan kanal koji se iznova koristi, držeći kanal zauzetim u čvoru, dovodi do DoS napada na tom čvoru.
  - Koristeći poseban čvor koji stalno odašilje lažne podatke, baterija tog čvora može da se isprazni.
- Fizički sloj: Ova vrsta DoS napada se može vršiti emitujući veoma jakeradio frekventne smetnje na kanalu koji se koristi. To će izazvati smetnje u svim bežičnim mrežama koje rade u tom ili blizu tog kanalu.

3.6 Otimanje sesije

Napadač može izmeniti pakete koje šalje dadeluju kao da su od nekog drugog. Ovo se može koristiti da ubede korisnici da je napadač legitimna pristupna tačka, ili da se napadač predstavi kao legitimni korisnik pristupne tačke, slika 5.



Slika 5: Otimanje sesije

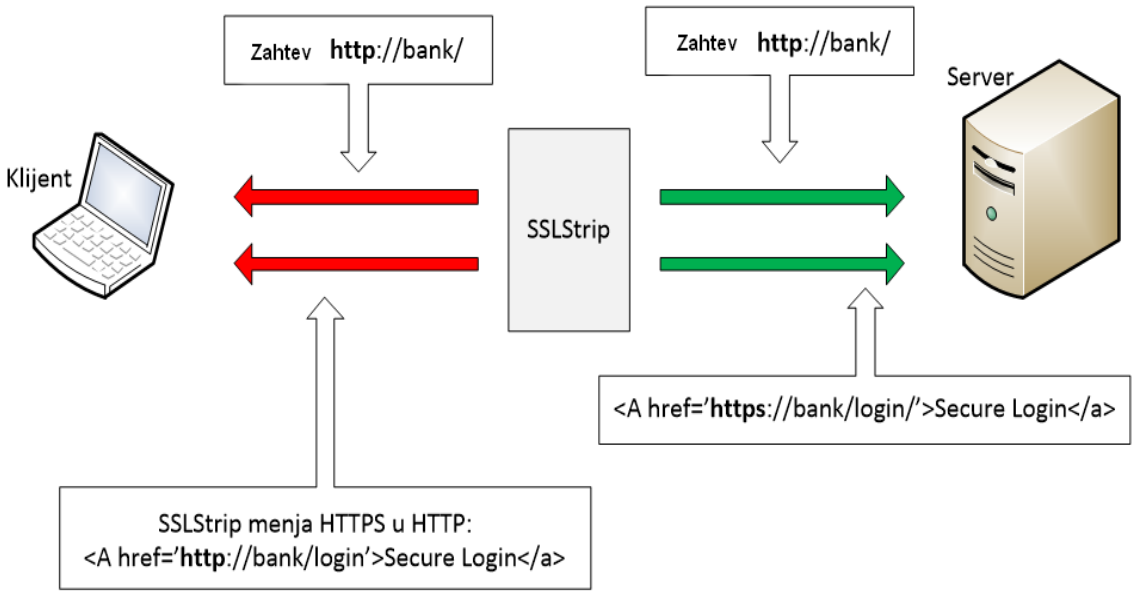
Ako napadač uspešno izvrši napad, i ubedi korisnike da je legitimna pristupna tačka, sav saobraćaj bežične mreže će ići preko napadačevog uređaja, tako da će on biti u mogućnosti da vidi šifre ili druge informacije koje korisnici šalju preko mreže, ubeđeni da koriste legitimnu pristupnu tačku. Otimanje sesije (eng *Hijacking*) se obično koristi kao deo nekog drugog napada.

Jedna česta upotreba ovih napada je napad deautentikacijom koji se koristi u napadima na WPA, u kojima napadač šalje pakete za deautentikaciju klijentu kao da je u pitanju pristupna tačka, i pristupnoj tački kao da je u pitanju klijent. Ovaj napad može da omogući napadaču da povrati SSID mreže koja ga ne uključuje u *beacon* pakete. Kada se klijent ponovo poveže, paketi u postupku rukovanja će sadržati SSID pristupne tačke, omogućavajući napadaču da ga snimi. Napadi deautentikacijom mogu da se koriste kao ciljani DoS napadi, onemogućavajući samo određenog klijenta da koristi mrežu (Hulin, Locke, Mealey, Pham 2010).

3.6.1 Čovek u sredini

Ovaj napad pokušava da ubaci napadača u sredinu (eng *middle – Man In The Middle*) komunikacije, odnosno između legitimne pristupne tačke i korisnika (Zhang, Zheng, Ma, 2008). Za ovaj tip napada nije neophodno da se napadač fizički nalazi u blizini korisnika mreže, niti

čak da se nalazi u prostoriji ili zgradi, potrebno je samo da je u dometu radio signala. Jedan od načina da se izvede je da napadač koristi napad deautentikacijom da izbaci klijenta sa mreže, a zatim se maskira kao pristupna tačka kada se klijent ponovo poveže. Onda napadač može uhvatiti podatke koje šalje klijent i izmeniti ih po želji. Napadač sada možete pročitati sav nešifrovan saobraćaj koji klijent šalje, ali neće imati pristup SSL šifrovanim podacima za povezivanje. Jedan od načina da se zaobiđe ovo ograničenje je da sepreprави sajt za preusmeravanje i linkovi koji se šalju klijentu uklanjanjem „https://“, iz njih, da se smanji verovatnoća da će se SSL koristiti za šifrovanje sesije, slika 6. Jedan alat koji pomaže u takvim napadima je *Marlinspike's sslstrip*. Sslstrip obezbeđuje nekoliko napada na HTTP saobraćaj, onemogućujući korisnicima pristup HTTPS verzijama sajtova i prepravlja da bezbedni sajtovi koriste običan HTTP, što omogućava napadaču da snimi podatke za povezivanje. Ova vrsta napada zahteva da je napadač u stanju da se poveže sa mrežom koju napada.



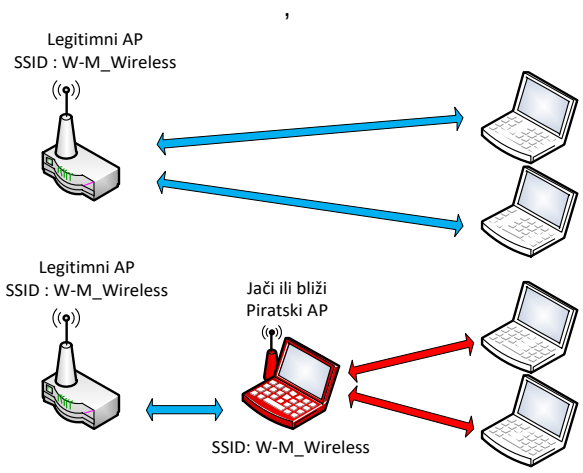
Slika 6: Sslstrip šematski prikaz

3.6.2 Piratska pristupna tačka

Ovo je jedna vrsta „čovek u sredini“ napada, i podrazumeva da napadač postavi neautorizovanu pristupnu tačku na bežičnu mrežu, a zatim je konfiguriše da izgleda legitimna korisnicima mreže.To mu omogućava pristup podacima na mreži, a sve to iz razloga jer se korisnički uređaji, ako nisu drugačije podešeni, povezuju na pristupnu tačku sa najjačim signalom. Po definiciji ako je pristupna tačka postavljena na mrežu bez direktne konsultacije sa informatičkim osobljem, i koja ne podleže kontroli, odgovornosti i nadgledanju infomatičkog osoblja, ta pristupna tačka se naziva piratska pristupna tačka (eng *Rogue Access Point*) (IEEE Std 802.11a, 1999).

Kako se cene pristupnih tačaka smanjuju, tako postaje sve jednostavnije za napadača da ih postavi u bežičnu lan mrežu. Napadač će pokušati da postavi piratsku pristupnu tačku što bliže mestu gde se odvija bežični saobraćaj, ali gledaće da to ne bude preblizu legitimne pristupne tačke, jer bi to dovelo do velikog broja ponavljanog udruživanja, što bi privuklo pažnju o postojanju nove pristupne tačke. Kada je pristupna tačka pozicionirana, napadač podešava MAC i SSID pristupne tačke da odgovara onom koji koristi legitimna pristupna tačka. Kada korisnik upali računar na području koje je pokriveno sa bežičnom mrežom, osnovna mrežna podešavanja će ga udružiti sa pristupnom tačkom koja odašilje jači signal, sto je u ovom slučaju piratska pristupna tačka, slika 7.

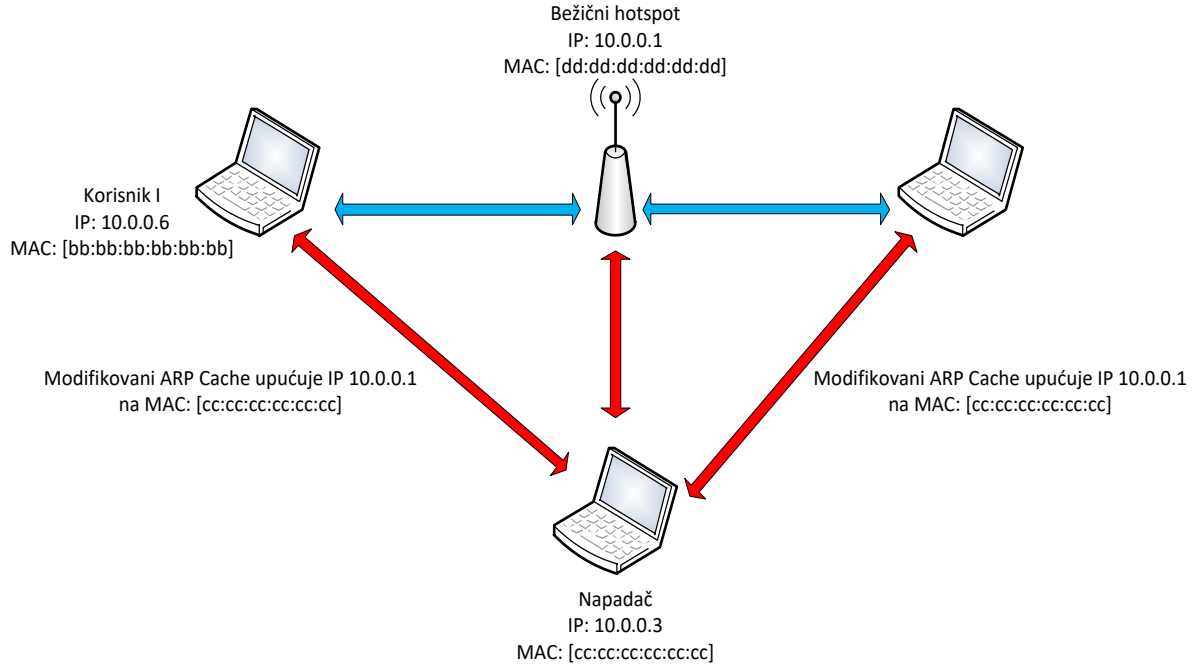
Kada je piratska pristupna tačka postavljena, napadač je u stanju da analizira sav saobraćaj koji prolazi kroz nju. Tako će napadač biti u mogućnosti da snima ključeve za autentikaciju, šifre, poverljivu e-poštu ili da menja i koriguje podatke koji idu preko pristupne tačke itd.



Slika 7. Piratska pristupna tačka

3.6.3 ARP trovanje

ARP trovanje (eng *ARP poisoning*) je uobičajeni napad na mrežu koji se može koristiti da se postavi čovek u sredini napada. Može se realizovati na dva načina: menjajući ARP odgovore ili slanje lažnih IP paketa. ARP (*Address Resolution Protocol*) se koristi da pronađe MAC adresu domaćina sa određenom IP adresom. Ako napadač može dobiti ARP tabele ulazana mrežni prolaz (eng *gateway*) da bi klijentske čvorove uputio na sebe, onda se svi paketi koje klijent pokušava da pošalje van mreže, ići prvo kod napadača slika 8. Ovaj metod zahteva pristup mreži razbijanjem mrežnog ključa (IEEE Std 802.11, 1999).



Slika 8. ARP trovanje

4 ZAKLJUČAK

Da bi se uspešno zaštitili od zlonamernih korisnika na bežičnoj mreži, neophodno je poznavati koje su slabosti bežične mreže, načine nanošenja štete, i koje tehnike će koristiti da bi te slabosti iskoristile. Cilj ovog rada je bio da prikaže navedene probleme. Radom je potvrđena opšta hipoteza da bežične računarske mreže ne nude adekvatnu sigurnost korisnicima.

Bežične mreže još ne nude odgovarajući nivo sigurnosti, u čemu su daleko ispod nivoa sigurnosti žičnih mreža. Kao osnovna komponenta bežičnih mreža pristupna tačka je prva na udaru napadača. Kako su pristupne tačke postale komercijalno dostupne, osmišljena su fabrička podešavanja, sa ciljem da korisnicima koji nisu stručnjaci za mreže olakšaju podizanje njihove bežične mreže. Iako nude opcije za podizanje nivoa bezbednosti, neupućeniji korisnici će najradije sve ostaviti po fabričkim podešavanjima. Zatim *hotspot* uređaji po kafićima, aerodromima, itd. najčešće ne nude ni jedan stepen sigurnosti, jer njima nije cilj zaštita korisnika, nego najčešće da im omoguće pristup Internetu. U tim slučajevima napadaču ništa ne predstavlja prepreku da presreće i snima podatke koje korisnici šalju ili primaju sa Interneta. A i ako

nude neki oblik bezbednosti to je često u vidu WEP ili WPA protokola, a kao što smo i videli, njih je relativno lako zaobići, ako napadač ima odgovarajući alat. WEP protokol je nastao 1999 god, a i danas se nudi kao sigurnosna opcija, WPA je takođe dosta star, ali za razliku od WEP-a ima viši stepen sigurnosti. WPA2 protokol je podigao nivo sigurnosti, ali zahteva noviju opremu, što je trošak za većinu korisnika, tako da su na javnim mestima pretežno, ako ne i uvek ranjivi na napade.

Zbog navedenog, korisnici javnih bežičnih mreža, ne bi trebali da šalju osetljive podatke putem njih. Pregledanje Internet sadržaja, čitanje novina na Internetu, nekom ko prisluškuje saobraćaj, neće biti od velike koristi, ali ako se korisnik loguje na e-mail, ili na neki sajt gde korisnički nalog ima visoka prava, a da ne govorima o podacima kao što su brojevi kreditnih kartica, ili bankovni računi, sve to napadač može da iskoristi da bi vam naneo štetu. Napadi izviđanja ne predstavljaju pravu opasnost, u smislu nanete štete, oni se najčešće koriste kao deo pripreme za izvršenje novog napada čije posledice mogu biti mnogo veće. Najveću štetu korisnicima bežičnih računarskih mreža nanose napadi otimanja sesije i uskraćivanje usluga. Uskraćivanje usluga neće ostaviti datog korisnika bez poverljivih informacija, ali će mu onemogućiti rad sa mrežom, da li pristup ka Internetu, pristup ka žičanoj mreži, ili pristup ka mrežnim resursima kao što su serveri. Dok napadač prilikom otimanja sesije, postavljajući se kao čovek-u-sredini, striktno za cilj ima praćenje i snimanje saobraćaja koji ide kroz mrežu. Ako se ovaj napad izvede u nekoj kompaniji, u tom slučaju korisnici ni ne sumnjaju da je mreža kompromitovana, i šalju osetljive informacije preko mreže, što napadač može neometano da snima. Ovi napadi zahtevaju visoko znanje iz oblasti informatike, a često zahtevaju od napadača da se nalazi u neposrednoj blizini mreže koju napada.

Sve veća upotreba bežičnih LAN (eng *local arena network*) mreža i veliki rast pristupa Internetu sa mobilnih telefona zahtevaju potpuno nove pristupe bezbednosti. Na osnovu navedenog može se zaključiti da bežične računarske mreže još uvek ne bi trebalo da se povezuju u sklopu mreža kroz koje se kreću osetljive informacije. Preporučuje se postavljanje žične mreže u skladu sa potrebama i mogućnostima. Administrator mora biti upoznat sa slabostima, pretnjama i rizicima bežičnih računarskih mreža. Danas i velike korporacije iz mrežne oblasti, kao što je Cisco, ne mogu da garantuju ni približno onaj nivo bezbednosti njihovih uređaja za bežične mreže, kao za klasične žičane mreže.

CITIRANA DELA

Barnes, C., Bautts T., Lloyd D., Ouellet E., Posluns J., Zendzian D. M., O'Farrell N., *(*2002), *Hack Proofing Your Wireless Network*, Syngress Publishing, Rokland.

Beaver, K., & Davis P. T., (2005), *Hacking Wireless Networks For Dummies*, Wiley Publishing, Indianapolis.

Grubor, G., & Milosavljević M., (2010), *Osnove zaštite informacija*, Singidunum, Beograd.

Hulin K., Locke C., Mealey P., & Pham, A. (2010). *Analysis of Wireless Security Vulnerabilities, Attacks, and Methods of Protection,* The University of Texas.

IEEE Std 802.11a-(1999) *„Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band“.*

IEEE Std 802.11b-(1999) *„Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band “.*

Jie Chen *„IEEE 802.11 (part 2)“.*

Kumkar V., Tiwari A., Tiwari P., Gupta A., Shrawne S., (2012), *Vulnerabilities of Wireless Security protocols*, International Journal of Advanced Research in Computer Engineering & Technology.

Nichols R. K., Lekkas P. C., (2002), *Wireless Security Models, Threats, and Solutions*, The McGraw-Hill Companies, New York.

Ohrtman, F., & Roeder, K. (1999). *Wi-Fi Handbook: Building 802.11b Wireless Networks.* IEEE Std 802.11, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".*

Raza M., Iqbal M., Sharif M., Haider W., (2012), *World Applied Sciences Journal*, IDOSI Publications.

Rufi A., (2006), *Network Security 1 and 2 Companion Guide*, Cisco Press, Indianapolis.

Wekhande V., (2006), *Wi-Fi technology: Security issues*,Rivier College, Našua.

Zhang Y., Zheng J., Ma M., (2008), *Handbook of Research on Wireless Security*, Information Science Reference, London.

Datum prve prijave: 16.03.2018.
Datum prijema korigovanog članka: 23.07.2018.
Datum prihvatanja članka: 05.09.2018.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Regodić, D., Grubor, G., & Regodić, R. (2018, 10 15). Primena bežičnih računarskih mreža i bezbednosni problemi. (Z. Čekerevac, Ur.) *FBIM Transactions, 6*(2), 117-133. doi:10.12709/fbim.06.06.02.13

*Style – **Chicago** Sixteenth Edition:*

Regodić, Dušan, Gojko Grubor, i Radomir Regodić. 2018. „Primena bežičnih računarskih mreža i bezbednosni problemi." Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 6 (2): 117-133. doi:10.12709/fbim.06.06.02.13.

*Style – **GOST** Name Sort:*

Regodić Dušan, Grubor Gojko i Regodić Radomir Primena bežičnih računarskih mreža i bezbednosni problemi [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 10 2018. - 2 : T. 6. - str. 117-133.

*Style – **Harvard** Anglia:*

Regodić, D., Grubor, G. & Regodić, R., 2018. Primena bežičnih računarskih mreža i bezbednosni problemi. *FBIM Transactions,* 15 10, 6(2), pp. 117-133.

Style – **ISO 690** Numerical Reference:

Primena bežičnih računarskih mreža i bezbednosni problemi. **Regodić, Dušan, Grubor, Gojko i Regodić, Radomir.** [ur.] Zoran Čekerevac. 2, Beograd : MESTE, 15 10 2018, FBIM Transactions, T. 6, str. 117-133.