



UNIVERZITET SINGIDUNUM

**- MASTER STUDIJSKI PROGRAM -
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Miloš Aksić

**Bezbednosni problemi i zaštita bežičnih i
mobilnih mreža**

- Master rad -

**Mentor:
Prof. dr Mladen Veinović**

**Student:
Miloš Aksić, 410133/2011**

Beograd, 2013.

Sažetak

U radu su opisani su mobilni korisnici, bežični linkovi i mreže, kao i njihov odnos prema većim ožičenim mrežama sa kojima se povezuju. U prvom delu se prikazuje konfiguracija koja razmatra bežične komunikacije i mobilnost – mrežu u kojoj se bežični korisnici povezuju sa većom mrežnom infrastrukturom putem bežičnog linka. Zatim se razmatra karakteristika tog bežičnog linka. U odeljku 3 detaljnije se razmotraju aspekti sloja veze u standardu za bežični LAN, IEEE 802.11 (Wi-Fi), zatim se pominje i Bluetooth. U odeljku 4 daje se pregled mobilnog pristupa Internetu, uključujući 3G i 4G mobilnu telefoniju i celularne mreže. Na kraju u odeljku 5 prikazuju se kako se usluge za mobilnost implementiraju u GSM-u. U radu je opisana organizacija zaštite bežičnih i mobilnih mreža. Zbog činjenice da je organizacija zaštite opterećena preuzimanjem odgovornosti za specijalizovane programe određeni aspekti ove vrste menadžmenta imaju svoje osobenosti.

Abstract

In this paper we will describe cellphone users, wireless links and networks, and also their relationship with bigger wired networks with which they are connected. We will begin with showing a configuration where we will view wireless communication and mobility – network where wireless users connect with larger infrastructure by wireless connection. Then, we will investigate characteristics of that wireless connection. In chapter 3, a bit more detail about aspects of connection layer in standard with wireless LAN, IEEE 802.11 (Wi-Fi), and shortly about Bluetooth. In chapter 4 we will view mobile internet access, including 3G and 4G mobile telephony and cellular networks. And, in chapter 5 we will display how are mobility services implemented in GSM network. This paper describes the organisation of wireless and mobile networks security. Because information security management is charged with taking responsibility for a specialized program, certain characteristics of its management are unique to this community of interest.

Sadržaj

UVOD	7
1. Uvod u bežične mreže	7
1.1 Standard bežičnih mreža	8
1.2 Bežične mreže i sigurnost	10
1.3 Fizičko ograničavanje propagacije signala	11
2. Wi-Fi: Bežični LAN-ovi tipa 802.11	11
2.1 Arhitektura 802.11	13
2.1.2 Kanali i pridruživanje	14
2.2 MAC protokol 802.11	16
2.2.1 Tretiranje sakrivenih terminala: RTS i CTS	18
2.2.2 Korišćenje protokola 802.11 u linku od tačke do tačke	21
2.2.3 Okvir IEEE 802.11	21
2.2.4 Polja adresa	21
2.3 Mobilnost unutar iste IP podmeže	23
2.4 802.15 i Bluetooth	24
3. WEP	25
3.1 Napadi na WEP	27
3.1.1 Pasivni napadi	27
3.1.2 Napad ponavljanjem inicijalizovanog vektora	28
3.1.3 Napad čovek u sredini	29
3.1.4 Krađa sesije	29
3.1.5 Napad ponavljanjem paketa	30
3.2 Upravljanje ključevima	31
3.3 WPA i WPA2	31
4. Celularni pristup Internetu	33
4.1 Opšti pregled celularne arhitekture	33
4.1.1 Osnovna mrežna infrastruktura	33
4.1.2 Pristupne tehnike vazdušnog interfejsa	34
4.2 Celularni standardi i tehnologije	35

4.2.1 Druga generacija (2G).....	35
4.2.2 Prelaz sa druge generacije na treću (2,5G)	36
4.2.3 Treća generacija (3G)	37
4.2.4 Četvrta generacija (4G).....	37
5. Sigurnost GSM mreža.....	38
5.1 GSM mreža.....	38
5.2 Provera identiteta korisnika	40
5.2.1 IMEI.....	41
5.2.2 Algoritmi za šifrovanje komunikacije	41
5.2.3 Anonimnost korisnika.....	41
6. Osnovni ciljevi sistema zaštite podataka	43
6.1 Funkcionisanje zaštitnih procesa	43
6.1.1 Antivirusni program.....	43
6.1.2 Implementacija kontrole pristupa	43
6.1.3 Funkcionisanje identifikacije.....	44
6.1.4 Funkcionisanje mrežnih servisa i protokola	47
7. Topologija zaštite.....	48
7.1 Definisane zahteve u pogledu dizajna	49
7.1.1 Kreiranje zaštitnih zona	49
7.1.2 Rad sa novim tehnologijama.....	52
7.2 Poslovna politika u svetu sistema zaštite	53
ZAKLJUČAK.....	55
REFERENCE.....	56

Metodologija istraživačkog projekta

Uvodne napomene i obrazloženje rada

Master rad ima za cilj da definiše pojmove koji se koriste kada se govori o bežičnim i mobilnim mrežama, bezbednostima, pretnjama i napadima vezane za ovu vrstu mreža. Prikazana su tehnološka rešenja koja su trenutno aktuelna ali i ona koja će u bliskoj budućnosti biti preovlađujuća. Takođe, treba reći da je težište rada uglavnom okrenuto na opšti prikaz mreža, a manje na potencijalne pretnje.

Rad može da koristi manje stručnim korisnicima računara, ali i naprednijim korisnicima kao prikaz bežičnih i mobilnih mreža.

Predmeti istraživanja

Predmet istraživanja je analiza i potpuno sagledavanje bežičnih i mobilnih mreža, odnosno zaštite u njima. Pored poglavlja koje se odnosi na bežične linkove i mrežne karakteristike, veći deo istraživanja posvećen je Wi-Fi i bežičnim mrežama tipa 802.11 i mobilnim mrežama. Za obe vrste mreža prikazani su prednosti i nedostaci kao i mogućnost kombinovanja kako bi se od svake izvukle najbolje performanse, a smanjio uticaj slabosti koju svaka od njih poseduje.

Ciljevi i zadaci istraživanja

Ovaj rad namenjen je pre svega profesionalcima u oblasti računarskih mreža, kao i IT stručnjacima koji treba da urade studiju izvodljivosti uvođenja bežičnih mreža u neku kompaniju. Potrebno je da ovi profili IT stručnjaka imaju dobru osnovu u poznavanju mrežnih tehnologija ali nije nužno da detaljno ulaze u to funkcionisanje protokola kao i način rada pojedinih tehnika i protokola koji se koriste u bežičnim mrežama. Navedeni su neki od konkretnih problema do kojih dolazi a sa kojima se susreću IT stručnjaci koji uvode ili planiraju da uvedu ovu tehnologiju u svoju organizaciju.

Istraživačke hipoteze

Opšta hipoteza

Tokom istraživanja pokazano je da korisnici sve više imaju potrebu za povezivanjem svojih računara i mobilnih telefona na bežičnu mrežu kada se u određenom trenutku nalaze na putu ili pristupaju resursima od svojih kuća.

Metodi istraživanja i tok istraživačkog procesa

Metodologija istraživanja svela se na korišćenje pre svega Interneta ali i na korišćenje ozbiljnih knjiga koje se bave oblašću bežičnih i mobilnih mreža.

Na Internetu, ali i u literaturi uopšte mnogo je manje informacija koje se tiču organizacije bežičnih i mobilnih mreža nego informacija o tehnologijama koje se za to koriste. Zbog toga je istraživanje bilo teže i kompleksnije ali i mnogo interesantnije. Svaka od informacija koja se nalazi u ovom radu proverena je obavezno na više mesta u literaturi da bi se dokazalo da je relevantna. Takođe informacije o bezbednosti računarskih mreža uopšte teško su dostupne i trebalo je puno truda da se pronađu ljudi koji u toj oblasti imaju znanje i iskustvo. Ideja je da ovaj rad pomogne IT stručnjacima da dobiju jasniju o ovoj oblasti kao i da im se ukaže gde mogu da pronađu dodatne informacije koje su im potrebne.

UVOD

Eksplodivan rast bežičnih i mobilnih mreža u poslednje vreme, podseća na ekspanziju Interneta u devedesetim godinama prošlog veka. Tome pogoduje i jednostavnost implementacije, fleksibilnost u radu, kao i veliki izbor uređaja koji se koriste pri implementaciji mreže – mrežnih kartica i pristupnih tačaka. Kad se implementira bežična mreža, troškovi bivaju znatno manji nego u klasičnim lokalnim mrežama zasnovanim na žičanim vezama. Zbog ovih prednosti koje donose bežične mreže, one se danas masovno upotrebljavaju u raznim preduzećima, institucijama, javnim i privatnim organizacijama; u poslednje vreme uočava se i trend postavljanja tzv. „vrućih“ tačaka (*eng. hot spots*), na mestima gde se kreće veliki broj ljudi i koje omogućavaju pristup Internetu preko bilo kog uređaja koji podržava komunikaciju po nekom od standarda za bežične mreže. Mogućnost takozvanog *roaminga* je posebno korisna i često upotrebljavana. Ovaj pristup može biti besplatan ili se zasnivati na pretplati ili naknadnom plaćanju usluge, recimo preko računa za mobilni telefon.

U radu je prikazano kako može doći do napada na bežične i mobilne mreže. Odeljak 2 je objašnjava uopšteno o bežičnim mrežama i zaštiti iste. Odeljak 3 govori o WEP, WPA i WPA2 standardima i primerima nekih od napada na WEP protokol. U odeljcima 4 i 5 razmatra se sigurnost GSM mreže, celularni standardi i tehnologije. Zatim se posvećuje pažnja na osnovne ciljeve sistema zaštite podataka koji se pominju u odeljku 6. O topologiji mreže, kreiranju zaštitnih zona i radom sa novim tehnologijama govori poslednji odeljak ovog rada, 7. odeljak.

Međutim, primena bežičnih mreža donela je i brojne probleme zbog narušavanja sigurnosti i privatnosti. Propagacija signala bežične mreže stvara probleme zbog nemogućnosti jasnog određivanja perimetra (granice) mreže, a pojavljuju se i različite nove pretnje i napadi na sigurnost računarskih sistema i mreža. Ovaj rad se bavi tim problemima i nekim od metoda zaštite bežičnih i mobilnih mreža. S obzirom na to da se radi o relativnoj tehnologiji, ovaj rad daje i neke osnovne (opšte) podatke o tehnologiji i načinu rada bežičnih i mobilnih mreža.

1. Uvod u bežične mreže

U standardima kojima se definišu bežične računarske mreže navode se i definišu razni elementi sigurnosti. Međutim, pokazuje se da ti elementi u većini slučajeva ostaju neiskorišćeni ili nepravilno podešeni što je naravno veliki sigurnosni problem. Čak i kada se aktiviraju svi sigurnosni elementi, to ne mora da znači da je postignut odgovarajući nivo sigurnosti. Razlog leži u mnogim nedostacima samog standarda, koju su naknadno uočeni i koji omogućavaju zlonamernim licima da bez većih teškoća pristupe mrežnim resursima i da ih koriste bez dozvole i znanja vlasnika i administratora mreže ili da ih zloupotrebe. Među propuste u standardu spadaju propusti pri proveru identiteta korisnika mreže i propusti u šifrovanju podataka između pristupne tačke i korisnika. Ovaj rad treba da prikaže trenutno stanje u području sigurnosti bežičnih računarskih mreža, kao i smernice za budući razvoj ove aktuelne oblasti.

1.1 Standard bežičnih mreža

Bežične mreže su definisane u standardu **IEEE 802.11** koji je doneo IEEE (*Institute of Electrical and Electronics Engineers*). U standardu se definišu najniža dva sloja OSI modela: fizički i sloj veze. On je samo deo veće porodice standarda koji definišu lokalne (LAN) i gradske mreže (MAN).

Početna verzija standarda IEEE 802.11 formirana je sredinom 1997, tako što je za rad bežičnih Ethernet sistema određena radna frekvencija od 2,4 GHz i dve brzine prenosa podataka – od 1 i 2 Mb/s (miliona bita u sekundi). Ponuđene su i dve tehnologije prenosa radio signala: FHSS (*Frequency Hopping Spread Spectrum*) i DSSS (*Direct Sequence Spread Spectrum*). Ubrzo po objavljivanju standarda oformljene su sledeće radne grupe:

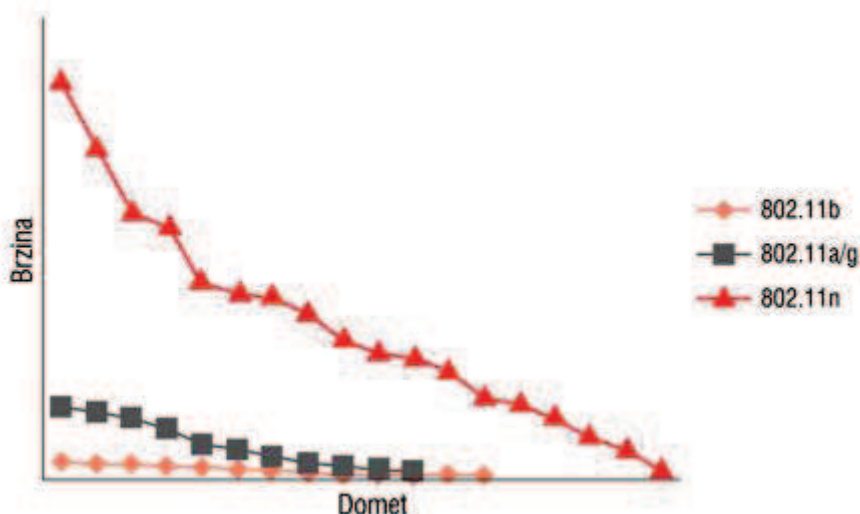
- Grupa „A“, zadužena za unapređenje inicijalnog standarda,
- Grupa „B“, zadužena za izradu bržeg DSSS prenosa na 2,4 GHz,
- Grupa „D“, zadužena za usklađivanje međunarodnih pravilnika o slobodnim radio-frekvencijama,
- Grupa „E“, koja obrađuje kvalitet servisa (QoS),
- Grupa „F“, koja razrađuje podršku za roving, i
- Grupa „G“, zadužena za rad na 54 Mb/s za zahtevne korisnike standarda 802.11b.

Standardi 802.11a, 802.11b i 802.11g, 802.11n razlikuju se prema fizičkom sloju (frekvencijama rada). Sloj veze je jednak u sva tri standarda i sastoje se od podsloja pristupa medijumu (MAC) i posloja logičke kontrole toka (LLC). MAC podsloj se malo razlikuje od takvog sloja u standardu 802.3 koji definiše žičane lokalne mreže. Umesto CSMA/CD, za standard 802.11 karakterističan je protokol CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*).

- **Standard 802.11a.** Fizički sloj ovog standarda definiše rad na frekvenciji 5 GHz (frekvencija koju je po međunarodnim standardima dopušteno koristi bez posebnih dozvola i naknada) sa OFDM (*Orthogonal Frequency Division Multiplexing*) multipleksiranjem kanala. Standard omogućava brzine od 6,9,12,18,24,36,48 i 54 Mb/s. Iako mreže rađene po ovom standardu omogućavaju najveće brzine, one imaju jednu ogromnu manu – domet je ograničen na 15m što je neprikladno za većinu korisnika.
- **Standard 802.11b.** 802.11a je propisao prenos podataka brzinama od 6 do 54 Mb/s, a 802.11b je inicijalni standard pomerio sa 1 na 5,5 i 11 Mb/s. Fizički sloj radi na frekvenciji od 2,4 GHz (takođe frekvencija koja se slobodno može upotrebljavati), koristi DSSS tehnologiju za odašiljanje signala i omogućava maksimalnu propusnost jer se koristi širi frekvencijski opseg. Ovaj standard danas dominira na tržištu ponajviše zbog relativno niske cene implementacije i zadovoljavajućih performansi. Širenje podrške standardu 802.11b ubrzo je dovelo do postavljanja pitanja kompatibilnosti opreme brojnih proizvođača. Zbog toga je formirano udruženje WECA (*Wireless Ethernet Compatibility Alliance*) koje je propisalo test program za sertifikaciju usklađenosti mrežne opreme sa standardom 802.11b. Udruženje WECA potpisuje garanciju usklađenosti sa 802.11b oznakom Wi-Fi.
- **Standard 802.11g** Ovaj standard omogućava maksimalnu propusnost od 54 Mb/s (kao 802.11a) na frekvenciji od 2,4 GHz (kao 802.11b). Bitno je naglasiti da je ovaj standard kompatibilan i sa 802.11a i sa 802.11b. Fizičko sloj se u standardu 802.11g naziva

Extended Rate PHY (ERP). ERP podržava četiri različite modulacije: DSSS-a, OFDM, PBCC, PBCC (*Packet Binary Convolutional Code*), DSSS-OFDM (hibridna modulacija u koje se preambula i zaglavlje modulišu pomoću DSSS-a, a punjenje pomoću OFDM-a). ERP može da detektuje korišćene modulacije pri komunikaciji sa određenim klijentom. Sloj veze isti je kao i u standardima 802.11a i 802.11b.

- **Standard 802.11n** IEEE 802.11n predstavlja narednu generaciju bežične tehnologije, odnosno dopunu standarda IEEE 802.11 a unapređuje prethodne specifikacije 802.11a i 802.11g. Najznačajnije unapređenje se odnosi na povećanje brzine sa 54 Mbit/s do mogućih 600 Mbit/s. Maksimalna brzina 802.11n sistema zavisi od konfiguracije. Ostala unapređenja se odnose na domet i pouzdanost (slika 1.).



Slika 1. Poređenje brzina i dometa 802.11b, 802.11a/g i 802.11n sistema

Wi-Fi trgovačka je marka (brend) koju je licencirala organizacija Wi-Fi Alliance® da bi opisala osnovnu tehnologiju koja se koristi za bežične lokalne mreže (eng. *Wireless Local Area Network*, WLAN) zasnovanu na specifikaciji IEEE 802.11. Ona je bila namenjena za mobilne računarske uređaje kao što su prenosni računari, u LAN mrežama, ali se počela koristiti i za druge usluge, uključujući i Internet pristup, VoIP, igranje, i osnovne usluge povezivanja korisničke elektronike (Televizijska tehnika i DVD plejeri, digitalne kamere, sistemi za nadzor i slično). U toku je razvoj još jednog broja novih standarda koji će između ostalog, omogućiti da se Wi-Fi mreže koriste u automobilima na autoputevima, kao podrška *Intelligent Transportation System*, a da bi se povećala sigurnost, prikupljali statistički podaci, omogućila mobilna trgovina (standard IEEE 802.11p). Logotip Wi-Fi® i Wi-Fi CERTIFIED™ registrovane su trgovačke marke organizacije Wi-Fi Alliance® koja ispituje i sertifikuje uređaje i opremu po standard 802.11x¹. Za ovaj tip mreža koristi se naziv Wi-Fi mreže (simbol prikazan na slici 2).

¹ Wikipedia, <http://en.wikipedia.org/wiki/Wi-Fi>



Slika 2. Logotip Wi-Fi

1.2 Bežične mreže i sigurnost

Iako se u standardima definiše nekoliko sigurnosnih elemenata, činjenica je da su bežične mreže najslabija sigurnosna karika unutar neke organizacije. Standardi ne uspevaju da zadovolje tri osnovna sigurnosna zahteva: pouzdanu proveru identiteta korisnika, zaštitu privatnosti i autorizaciju korisnika. Nekada osnovni sigurnosni mehanizam, *Wired Equivalent Privacy* (WEP), vrlo brzo je pokazao da u njemu samom ima značajnih sigurnosnih propusta. Osim toga, IEEE je ostavio otvorena pitanja o bitnim sigurnosnim elementima kao što su raspodela ključeva i robustan način provere identiteta korisnika. Takođe, većina organizacija koje imaju bežične mreže oslanja se na sigurnost definisanu u standardima ili čak i ne koriste nikakve sigurnosne mere.

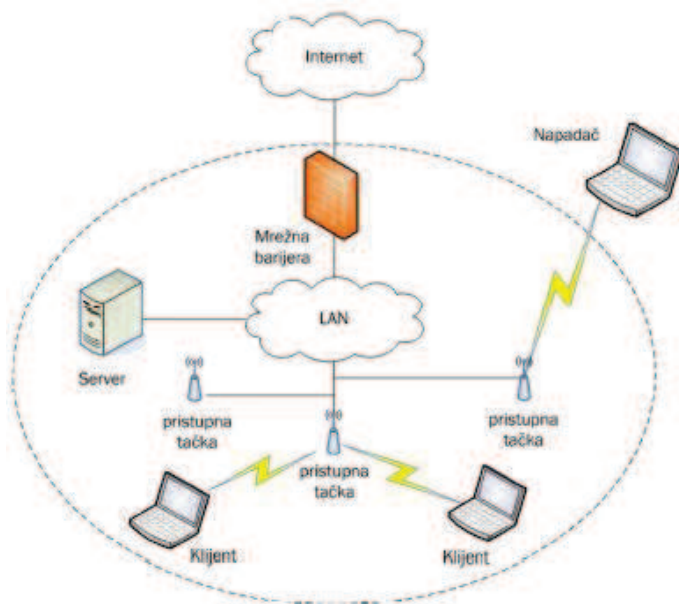
Pre nego što se upustimo u raspravu o sigurnosnim propustima u postojećim standardima, bitno je razmotriti koliko je napad na bežičnu računarsku mrežu izvodljiv u praksi. Početni problem svakog napadača je doći do signala same mreže i tako izvesti aktivan ili pasivan napad. Da bi napadač mogao da izvede pasivan napad, mora imati opremu koja može da osluškuje i presreće saobraćaj između pristupne tačke i klijenta, što znači da napadač mora temeljno da poznaje fizički sloj definisan u standard 802.11. Za aktivan napad potrebno je imati i opremu koja može da šalje podatke na mrežu. Oprema koja bi pouzdano obavljala navedene zadatke nije jeftina. Treba uzeti u obzir i činjenicu da proizvođači bežične mrežne opreme često zanemaruju napade na sloju veze, smatrajući ih nepraktičnim i neizvodljivim, što je pogrešno iz dva razloga.

- Prvi je da može postojati napadač s neograničenim materijalnim resursima i vremenom. Kao primer, može se uzeti industrijska špijunaža, koja je prilično profitabilan posao.
- Drugo, hardver potreban za praćenje i aktivan napad dostupan je svima, u obliku bežičnih kartica za stone i prenosne računare. Postoje pasivni napadi koji su izvedeni s takvim karticama tako što su izmenjeni drajveri (engl. *device drivers*). Izmenjeni drajveri omogućavaju ubacivanje proizvoljnog saobraćaja u mrežu i izvođenje aktivnog napada. Vreme uloženo u takav posao nije malo, ali je izmena drajvera posao koji se obavlja samo jednom. Uz to, ukoliko se gotovi izmenjeni drajveri objave na Internetu, postaće dostupni svima.

1.3 Fizičko ograničavanje propagacije signala

Danas se u mrežama koriste tri vrste antena: **omnidirekciona**, **ravna** i **usmerena** (Yagi) antena. Prilikom projektovanja bežične mreže u nekom području, potrebno je detaljno pregledati to područje i utvrditi optimalnu vrstu antene koja će se koristiti i dovoljnu snagu; uz to treba voditi računa o svim ograničenjima. Takođe, mora se uzeti u obzir da je frekvencija koju koriste mreže 802.11b i 802.11g, od 2.4 GHz nelicencirana, što znači da se može javiti interferencija s bežičnim telefonima (i drugim uređajima koji rade na istoj frekvenciji), a samim tim može nastati i uskraćivanje usluge (DoS do kog dolazi nepažnjom projektanata). Osim toga, dobro je pretpostaviti da potencijalni napadač može imati bolju i osteljiviju opremu od one koja je propisana standardima, što praktično proširuje domet mreže (van fizičkih granica organizacije kojoj mreža pripada). Zbog toga se može javiti potencijalna opasnost jer se omogućava “**napad s parkirališta**” (engl. *parking lot attack*), prikazan na slici 3.

U novije vreme se dosta često koriste različite tehnike za ograničavanje propagacije signala, zasnovane na antenama sa usmeravanjem, ali i ometanje signala nekom od tehnika interferencije, kako bi se signal u pojedinim područjima učinio nerazumljivim tj. “nečitkim”.



Slika 3. „Napad s parkirališta“

2. Wi-Fi: Bežični LAN-ovi tipa 802.11

S obzirom na to da se koriste na poslu, kod kuće, u obrazovnim ustanovama, kafeima, aerodromima i u uličnim govornicama, bežični LAN-ovi danas predstavljaju jednu od najvažnijih tehnologija za pristup mrežama na Internetu. Mada je tokom '90-tih godina razvijeno više tehnologija i standarda, neosporno pobeđuje jedna određena klasa standarda: **bežični LAN IEEE**

802.11, poznat takođe kao **Wi-Fi**. U ovom odeljku detaljno se razmatra bežični LAN 802.11 tako što se proučava struktura okvira 802.11, protokol za pristup medijima 802.11 i međusobno povezivanje mreža LAN 802.11 sa ožičenim Ethernet LAN-ovima.

Za tehnologiju bežičnog LAN-a postoji nekoliko standarda 802.11. Tu između ostalog spadaju 802.11b, 802.11a i 802.11g, 802.11n. U **tabeli 1**, ukratko su prikazane glavne karakteristike ovih standarda. Najzastupljeniji je standard 802.11b, međutim postoji široka ponuda proizvoda 802.11a i 802.11g, 802.11n, pa se u narednim godina može očekivati značajno uvođenje ovih bežičnih LAN-ova sa većim brzinama.

Četiri standarda 802.11 imaju mnoge zajedničke karakteristike. Sva tri koriste isti protokol za pristup medijumima CSMA/CA koji su u radu opisani. Svi za okvire slova veze koriste istu strukturu okvira. Sva tri standarda su u stanju da smanje brzinu prenosa da bi se povećala dostupna udaljenost. Svi omogućavaju „režim infrastrukture“ i „ad hoc režim“, što će se takođe ubrzo opisati. Međutim, kao što se vidi iz **tabele 1** ova četiri standarda sadrže neke bitne razlike u fizičkom sloju.

Bežični LAN 802.11 ima brzinu prenosa od 11 Mb/s, što je više nego dovoljno za većinu kućnih mreža sa pristupom Internetu preko širokopojasnog kabla ili DSL-a. LAN-ovi 802.11b funkcionišu u opsegu frekvencije bez licenci (2.4 do 2.485 GHz), u kojem mora da se bori sa telefonima od 2.4 GHz i mikrotalasnim pećnicama. Bežični LAN-ovi 802.11a imaju kraći domet prenosa za dati nivo snage i podložniji su smetnjama od propagiranja po višestrukim putanjama. Pošto LAN-ovi 802.11g funkcionišu na istom nižom frekventnom opsegu kao 802.11b,a ili pri većim brzinama prenosa kao 802.11a, trebalo bi korisnicima da omoguće „i jare i pare“.

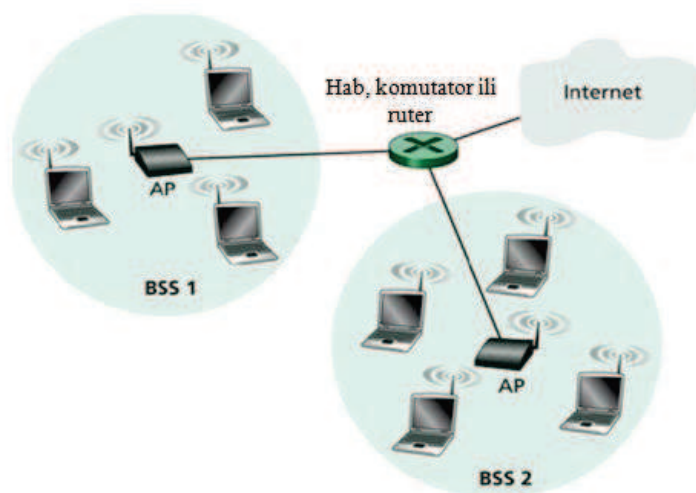
Standard	Raspon frekvencija	Brzina prenosa podataka
802.11b	2.4-2.485 GHz	do 11 Mbps
802.11a	5.1-5.8 GHz	do 54 Mbps
802.11g	2.4-2.485 GHz	do 54 Mbps
802.11n	2.4-5 GHz	do 600 Mbps

Tabela 1. Pregled standarda IEEE 802.11

2.1 Arhitektura 802.11

Na **slici 4** prikazane su glavne komponente arhitekture bežičnog LAN-a 802.11. Osnovni element arhitekture 802.11 je **BSS** (*Basic Service Set*, skup osnovne usluge). BSS sadrži jednu ili više bežičnih stanica i centralnu **baznu stanicu** koja se žargonu 802.11 naziva **AP** (*Access Point*, pristupna tačka). Na **slici 4** prikazano je kako se pristupne tačke (AP) u svakom od dva BSS-a povezuju sa uređajem za povezivanje (hub, komutator ili ruter) koji zatim vodi do Interneta. U prosečnoj kućnoj mreži postoji jedan AP i jedan ruter (često se u istoj kutiji nalazi i kablovski ili ADSL modem) koji povezuje BSS sa Internetom.

Kao i kod Ethernet uređaja, svaka bežična stanica 802.11 ima 6-bajtnu MAC adresu koja se čuva u firmveru kartice (tj. kartice mrežnog interfejsa 802.11). Svaki AP takođe ima MAC adresu za svoj bežični interfejs. Kao i kod Interneta, ovim MAC adresama administrira IEEE i one su (teoretski) globalno jedinstvene.



Slika 4. Arhitektura LAN-a IEEE 802.11

Kao što je napomenuto u **odeljku 1 (uvodu)** bežični LAN-ovi sa pristupnim tačkama često se nazivaju **infrastrukturni bežični LAN-ovi**, gde se infrastruktura koja povezuje pristupne tačke i ruter. Na **slici 5** prikazano je da stanice IEEE 802.11 mogu takođe da se grupišu u ad hoc mrežu – mrežu bez centralne kontrole i bez povezivanja sa „spoljnim svetom“. Ovde se mreža formira „usput“ od mobilnih uređaja koju su trenutno u blizini, a imaju potrebu za međusobnom komunikacijom, iako u blizini nema postojeće mrežne infrastrukture. Ad hoc mreža može da se napravi kada se sastanu ljudi sa laptopovima (na primer, u sali za konferencije, u vozu ili automobilu) koji žele da razmene podatke, a u blizini ne postoji centralizovana pristupna tačka. Kako se širi upotreba prenosivih uređaja za komunikaciju, javlja se izuzetno zanimanje za ad hoc umrežavanje. U ovom odeljku akcenat je na infrastrukturama bežičnih LAN-ova.

2.1.2 Kanali i pridruživanje

Pod protokolom 802.11, da bi bežična stanica mogla da šalje ili prima okvire 802.11 koji sadrže podatke mrežnog sloja, ona se mora pridružiti nekoj pristupnoj tački. Mada svi standardi 802.11 koriste pridruživanje, ova tema se konkretno opisuje u kontekstu protokola IEEE 802.11b.



Slika 5. Ad hoc mreža IEEE 802.11

Kada mrežni administrator instalira pristupnu tačku, on joj dodeljuje identifikacioni broj **SSID** (*Service Set Identifier*) od jedne ili dve reči. (Kada, na primer u Microsoft Windows XP „prikažete dostupne mreže“ prikazuje se lista SSID-ova svih dostupnih pristupnih tačaka.) Administrator mora pristupnoj tački takođe da dodeli i broj kanala. Da bi se shvatili brojevi kanala, imamo na umu da protokol 802.11b funkcioniše u frekventnom opsegu od 2.4 GHz do 2.485 GHz. U ovom rasponu od 85 MHz, protokol 802.11b definiše 11 kanala koji se delimično preklapaju. Dva kanala se ne preklapaju ako i samo ako ih razdvaja 4 ili više kanala. Konkretno, skup kanala 1,6 i 11 je jedini skup od

tri kanala koji se ne preklapaju. Ovo znači da bi administrator mogao da napravi bežični LAN sa ukupnom maksimalnom brzinom prenosa od 33Mb/s tako što bi na istoj fizičkoj lokaciji instalirao 3 pristupne tačke 802.11b, dodelio im kanale 1,6 i 11 i povezo svaku pristupnu tačku sa jednim komutatorom.

Uz ovo osnovno poznavanje kanala 802.11, opisaćemo jednu zanimljivu (ne baš tako retku) situaciju – Wi-Fi džunglu. **Wi-Fi džungla** je svaka fizička lokacija u kojoj bežična stanica prima dovoljno jak signal od dve ili više pristupnih tačaka. Na primer, u mnogim kafeima u New Yorku bežična stanica može da uhvati signal od mnogih obližnjih pristupnih tačaka. Jedna od pristupnih tačaka bi mogla da pripada kafeu dok ostale mogu da budu u stanovima u blizini kafea. Svako od ovih pristupnih tačaka se verovatno nalazi u drugoj podmreži sa nezavisno dodeljenim kanalom.

Pretpostavlja se da u takvu Wi-Fi džunglu ulazite sa svojim prenosivim računarom i naručujete bežični pristup Internetu i piće. Uzmimo da u džungli ima 5 pristupnih tačaka. Da bi dobila pristup Internetu, vaša bežična stanica mora da pristupi tačnoj jednoj podmreži i mora da se **pridruži** tačno jednoj pristupnoj tački. Pridruživanje znači da bežična stanica pravi virtuelnu žicu između sebe i pristupne tačke. Konkretno, samo pridružena pristupna tačka će da šalje okvire podataka (tj. okvire koji sadrže podatke, kao što su datagrami) prema vašoj bežičnoj stanici, a vaša bežična stanica će slati okvire podataka na Internet samo preko pridružene pristupne tačke. Ali, kako će se vaša bežična stanica pridružiti konkretnoj pristupnoj tački? Još važnije, kako će vaša bežična stanica saznati da li u džungli ima pristupnih tačaka i koje su one?

Standard 802.11 zahteva da pristupna tačka povremeno šalje **okvire za navođenje** koji sadrže SSID i MAC adresu pristupne tačke. Pošto zna da pristupne tačke šalju okvire za navođenje vaša bežična stanica osmatra svih 11 kanala i čeka okvir za navođenje bilo koje pristupne tačke u blizini (od kojih neke emituju na istim kanalima – prava džungla!). Kada iz okvira za navođenje utvrdi koje pristupne tačke su dostupne, vaš bežični računar bira jednu od pristupnih tačaka za pridruživanje. Kada se izabere pristupna tačka, vaš bežični računar i izabrana pristupna tačka pregovoraju koristeći protokol za pridruživanje 802.11. Ako se u tom pregovaranju sve dobro završi, vaša bežična stanica postaje pridružena izabranoj pristupnoj tački. Implicitno, tokom faze pridruživanja, vaša bežična stanica pristupa podmreži kojoj pripada izabrana pristupna tačka. Odmah nakon faze pridruživanja, bežična stanica će preko pridružene pristupne tačke obično postati u podmrežu poruku DHCP otkrivanja kako bi dobila IP adresu u podmreži pristupne tačke. Od tog trenutka, vaš računar vidi ostatak Interneta jednostavno kao računar u podmreži svake tačke.

Da bi uspostavila pridruživanje sa konkretnom pristupnom tačkom, bežična stanica ponekad mora pristupnoj tački da dokaže svoju autentičnost. Bežični LAN-ovi 802.11 predviđaju niz alternativa za dokazivanje autentičnosti i za pristupanje. Jedan pristup, koji koriste mnoge

kompanije, jeste da dozvoli pristup bežičnoj mreži na osnovu MAC adrese određene stanice. Drugi pristup, koji se koristi u mnogim Internet kafeima upotrebljava korisnička imena i lozinke. U oba slučaja, pristupna tačka obično komunicira sa serverom za proveru autentičnosti tako što prenosi podatke između kranje bežične stanice i servera za proveru autentičnosti koristeći protokole kao što su RADIUS [RFC 2138] ili DIAMETER [RFC 3588]. Razdvajanjem servera za proveru autentičnosti od pristupne tačke omogućava se da jedan server opsluži mnoge pristupne tačke i centralizuju se (često osetljive) odluke o autentičnosti i pristupu, pa tako troškovi i složenost pristupnih tačaka ostaju niski.

2.2 MAC protokol 802.11

Pošto se bežična stanica pridruži pristupnoj tački, ona može da počne da šalje okvire podataka pristupnoj tački i da ih prima od nje. Ali pošto se dešava da više stanica u isto vreme pokušava da šalje okvire podataka preko istog kanala, potreban je protokol za višestruki pristup koji će koordinisati te prenose. Ovde, **stanica** može biti bežična stanica ili pristupna tačka. U opštem smislu postoje četiri klase protokola višestrukog pristupa: podela kanala, slučajni pristup, redna upotreba i CDMA. Pod uticajem velikog uspeha Ethernet-a i njegovog protokola direktnog pristupa, projektanti protokola 802.11 su za bežični LAN 802.11 izabrali protokol sa direktnim pristupom. Ovaj protokol se naziva **CSMA sa izbegavanjem kolizija** ili ukratko **CSMA/CA**. Kao i kod Ethernetovog CSMA/CD, "CSMA" znači Carrier Sense Multiple Access, što znači da svaka stanica pronalazi kanal pre nego što počne da emituje i da se uzdržava od emitovanja kada oseti da je kanal zauzet. Mada i Ethernet i 802.11 koriste direktan pristup sa ispitivanjem nosioca, između ova dva MAC protokola postoje značajne razlike.

Prvo, umesto otkrivanja kolizija 802.11 koristi tehnike za izbegavanje kolizije. Drugo, zbog relativno visoke učestalosti grešaka u bitovima u bežičnim kanalima, 802.11 (za razliku od Ethernet-a) koristi ARQ šemu u sloju veze za potvrđivanje i ponovno slanje. Sada ćemo opisati izbegavanje kolizija i šeme za potvrđivanje u sloju veze u protokolu 802.11.

Ako se tokom prenosa otkrije da neka druga stanica takođe emituje, ova prekida prenos i pokušava da šalje kasnije po isteku malog, slučajno izabranog vremenskog interval. Za razliku od Ethernet protokola 802.3, MAC protokol 802.11 *ne primenjuje* otkrivanje kolizija. Za to postoje dva važna razloga:

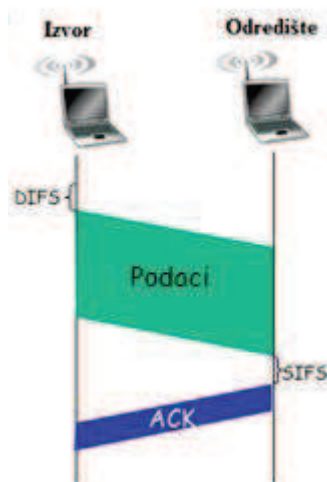
- Sposobnost da se otkriju kolizije zahteva sposobnost istovremenog slanja (vlastitog signala stanice) i primanja (da bi se utvrdilo da li još neka stanica takođe šalje). Pošto je jačina primljenog signala obično veoma mala u poređenju sa jačinom signala koji se šalje sa kartice 802.11, skupo je praviti hardver koji je u stanju da otkrije koliziju.
- Još važnije, čak i kada bi kartica mogla istovremeno da emituje i da sluša (i eventualno prekine slanje kada otkrije opterećenost kanala), adapter ipak ne bi mogao da otkrije sve kolizije zbog problema sakrivenog terminala i opadanja.

Pošto bežični LAN-ovi 802.11 ne koriste otkrivanje kolizije, stanica koja počne sa slanjem okvira *šalje okvir u potpunosti*; tj. kad se stanica pokrene, nema više povratka. Logično je da slanje celih okvira (pogotovo dugačkih okvira) u situaciji sa mnogo kolizija može značajno da utiče na performanse protokola višestrukog pristupa. Da bi se smanjila verovatnoća kolizija, 802.11 koristi nekoliko tehnika za izbegavanje kolizija koje ćemo uskoro opisati.

Pre nego što pređemo na razmatranje izbegavanje kolizija, moramo prvo da razmotrimo šemu **potvrda u sloju veze** protokola 802.11. Ranije je već rečeno da kada stanica na bežičnom LAN-u pošalje okvir, on može iz različitih razloga da ne stigne do odredišne stanice. Zbog ove nezanemarljive verovatnoće neuspeha MAC 802.11 koristi potvrde u sloju veze. Kao što je prikazano na **slici 6** kada odredišna stanica primi okvir koji uspešno prođe CRC proveru, ona čeka jedan kratak vremenski interval poznat kao **SIFS** (*Short Inter-frame Spacing*), a zatim vraća okvir potvrde. Ako otpremna stanica u zadatom intervalu ne primi potvrdu, ona pretpostavlja da je došlo do greške i ponovo šalje isti okvir tako što za pristup kanalu ponovo koristi CSMA/CA. Ako potvrda ne stigne nakon određenog broja ponovnih slanja, otpremna stanica odustaje i odbacuje okvir.

Pošto smo opisali kako 802.11 koristi potvrde sloja veze, sada možemo da opišemo CSMA/CA protokol 802.11. Pretpostavimo da stanica (bežična stanica ili pristupna tačka) ima okvir za slanje.

1. Ako stanica na početku vidi da je kanal slobodan, ona šalje svoj okvir nakon kratkog vremenskog intervala poznatog kao **DIFS** (*Distributed Interframe Space*); **slika 6**.
2. Inače stanica bira slučajnu vrednost za odstupanje i odbrojava od te vrednosti sve dok je kanal slobodan. Kada se otkrije zauzeće kanala, vrednost brojača se zamrzava.
3. Kada brojač dođe do 0 (obratite pažnju na to da do toga jedino može doći kada je kanal slobodan), stanica šalje ceo okvir i zatim čeka na potvrdu.
4. Ako se primi potvrda, otpremna stanica zna da je njen okvir pravilno primljen u odredišnoj stanici. Ako stanica ima još neki okvir za slanje, ona pokreće protokol CSMA/CA od tačke 2. Ako se potvrda ne primi, otpremna stanica ponovo prelazi na fazu oporavka i koraka 2 tako što slučajnu vrednost bira iz većeg intervala.



Slika 6. 802.11 koristi potvrde sloja

Možemo da primetimo da u koraku 2 stanica bira slučajnu vrednost za odstupanje i počinje odbrojavanje, pa tako odlaže prenos čak i kada vidi da je kanal slobodan. U Ethernetovom CSMA/CD protokolu za višestruku pristup stanica počinje sa slanjem čim otkrije da je kanal slobodan. Zbog čega se u ovom pogledu CSMA/CD i CSMA/CA tako različito ponašaju?

Da bismo odgovorili na ovo pitanje, razmotrimo scenario u kojem dve stanice imaju okvire podataka za slanje, ali nijedna od njih ne šalje odmah zbog toga što otkriva da neka treća stanica već emituje. U Ethernetovom CSMA/CD-u obe stanice bi počele da šalju čim bi otkrile da je treća stanica prestala sa slanjem. To bi dovelo do kolizije što u protokolu CSMA/CD nije ozbiljan problem pošto bi obe stanice prekinule sa slanjem i tako izbegle nepotrebno emitovanje ostatka okvira koji je pretrpeo koliziju. Međutim, u protokolu 802.11 situacija je sasvim različita. Pošto 802.11 ne prekida prenos kada otkrije koliziju, okvir koji je pretrpeo koloziju da bi se preneo u celosti. U protokolu 802.11 cilj je da se kolizije izbegnu kad god je to moguće. U ovom protokolu, ako dve stanice vide da je kanal zauzet, one obe odmah pokreću odstupanje sa slučajnim vrednostima za koje se pretpostavlja da će biti različite.

Ako su te vrednosti zaista različite, kada se kanal oslobodi jedna od stanica će početi da šalje pre druge stanice, pa će „gubitnička stanica“ (pod pretpostavkom da stanice nisu sakrivene jedna od druge) uočiti signal „pobedničke stanice“, zamrznuti svoj brojač i sačekati sa slanjem sve dok pobednička stanica ne završi svoje slanje. Na ovaj način izbegnuta je skupa kolizija. Naravno, i sa protokolom 802.11 su kolizije moguće: ako su stanice sakrivene jedna od druge ili ako su izabrale identične slučajne vrednosti za odstupanje.

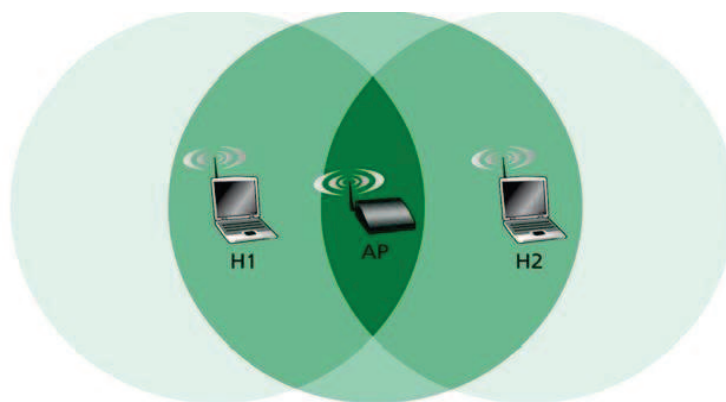
2.2.1 Tretiranje sakrivenih terminala: RTS i CTS

MAC protokol 802.11 takođe sadrži izvanrednu (opcionu) šemu rezervacija koja pomaže da se izbegnu kolizije čak i u slučaju sakrivenih terminala. Ispitajmo ovu šemu u kontekstu **slike 7** gde su prikazane dve bežične mreže stanice i jedna pristupna tačka. Obe bežične stanice su u domenu pristupne tačke (čiji domet je prikazan kako osenčeni krug) i obe su se pridružile

pristupnoj tački. Međutim, zbog opadanja, domet signala bežičnih stanica ograničen je na unutrašnji deo osenčenih krugova prikazanih na **slici 7**. Zbog toga, svaka bežična stanica je sakrivena od druge iako nijedna nije sakrivena od pristupne tačke.

Razmotrimo sada zašto sakriveni terminali mogu da predstavljaju problem. Pretpostavimo da stanica H1 šalje okvir i da na pola tog slanja mrežni sloj u stanici H2 preda MAC protokolu 802.11 jedan okvir (koji ćemo ovde nazvati DATA). Pošto ne primećuje slanje iz stanice H1, H2 će prvo sačekati jedno kratko slučajno izabrano vreme, a zatim će početi da šalje okvir DATA i tako dovesti do kolizije. Kanal će prema tome biti protraćen tokom celog intervala emitovanja iz H1 kao i iz H2.

Da bi se ovaj problem izbegao, protokol IEEE 802.11 omogućava stanici da jednim kratkim kontrolnim okvirom **RTS (Request To Send)** i jednim kratkim kontrolnim okvirom **CTS (Clear To Send)** rezerviše pristup kanalu. Kada pošiljalac hoće da pošalje okvir DATA, on može pristupnoj stanici prvo da pošalje okvir RTS, i naznači ukupno vreme potrebno za prenos okvira DATA i okvira potvrde (ACK). Kada pristupna stanica dobije okvir RTS, ona odgovara difuznim emitovanjem okvira CTS. Okvir CTS ima dve svrhe: on daje pošiljaocu eksplicitnu dozvolu da šalje i takođe obaveštava ostale stanice da ne šalju tokom rezervisanog perioda.



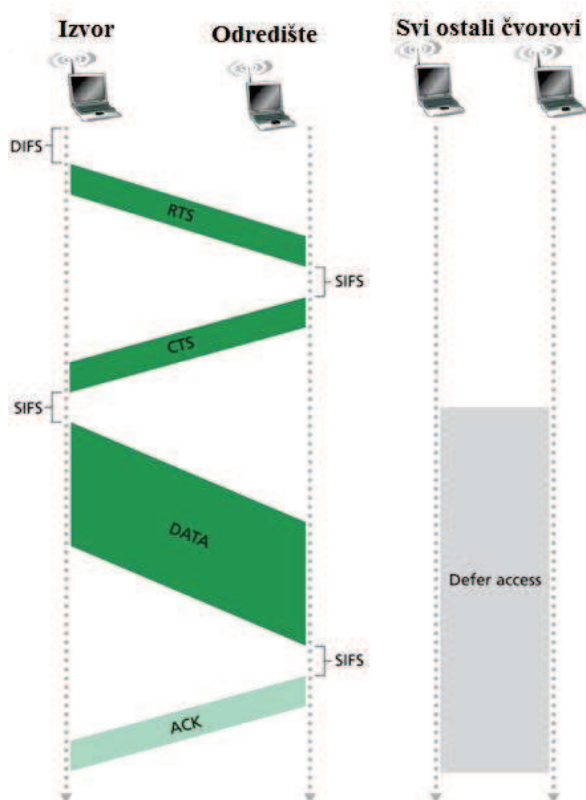
Slika 7. Primer sakrivenog terminala

Na taj način, kako vidimo na **slici 8** pre nego pošalje okvir DATA, H1 prvo difuzno emituje okvir RTS koji čuju sve stanice u njegovom krugu uključujući pristupnu tačku AP. Pristupna tačka zatim odgovara svojim okvirom CTS koji čuju sve stanice unutar dometa, uključujući H1 i H2. Stanica H2, pošto je čula CTS, uzdržava se od slanja u intervalu navedenom u okviru CTS. Na **slici 8** prikazani su okviri RTS, CTS, DATA i ACK.

Korišćenje okvira RTS i CTS poboljšava performanse na dva značajna načina:

- Problem sakrivenih stanica se ublažava pošto se dugački okvir DATA šalje tek pošto je kanal rezervisan.
- Pošto su okviri RTS i CTS kratki, kolizija u kojoj učestvuje RTS i CTS okvir trajaće samo koliko traje takav kratak okvir. Pošto se okviri RTS i CTS ispravno prenesu, naredni okviri DATA i ACK trebalo bi da prođu bez kolizije.

Razmena RTS/CTS može da pomogne u smanjenju broja kolizija, ona takođe dovodi do kašnjenja i troši resurse kanala. Iz tog razloga se razmena RTS/CTS koristi jedino da bi se rezervisao kanal za prenos dugačkog okvira DATA. U praksi, svaka bežična stanica može da uspostavi RTS prag, pa da se paketi RTS/CTS koriste samo ako je okvir veći od zadatog praga. Kod mnogih bežičnih stanica podrazumevana vrednost RTS praga veća je od maksimalne veličine (dužine) okvira, čime se izbegava razmena RTS/CTS za sva slanja DATA okvira.



Slika 8. Izbegavanje kolizije pomoću okvira RTS i CTS

2.2.2 Korišćenje protokola 802.11 u linku od tačke do tačke

Do sada smo opisivali 802.11 u situaciji višestrukog pristupa. Trebalo bi da pomenemo ako dva čvora imaju usmerive antene, oni mogu da usmere te antene jednu prema drugoj i da izvršavaju protokol 802.11 preko linka koji je u suštini od tačke do tačke. Zbog jeftinog hardvera za 802.11, korišćenja usmerivih antena i sve veće jačine prenosa, 802.11 može da se koristi kao jeftin način za bežične konekcije od tačke do tačke na razdaljinama od nekoliko desetina kilometara. U knjizi [Bhagwat 2003] opisana je takva bežična mreža sa više skokova koja funkcioniše u seoskim područjima oko reke Gang u Indiji sa linkovima 802.11 od tačke do tačke.

2.2.3 Okvir IEEE 802.11

Mada okvir 802.11 ima mnogo sličnosti sa Ethernetovim okvirom, on takođe sadrži niz polja specifičnih za njegove bežične linkove.. Brojevi iznad polja u okviru predstavljaju dužinu tih polja u *bajtovima*; brojevi iznad podpolja u kontrolnom polju okvira predstavljaju dužine tih podpolja u *bitovima*. Ispitajmo sada polja u okviru, kao i neke od značajnih podpolja u kontrolnom polju okvira.

2.2.4 Polja adresa

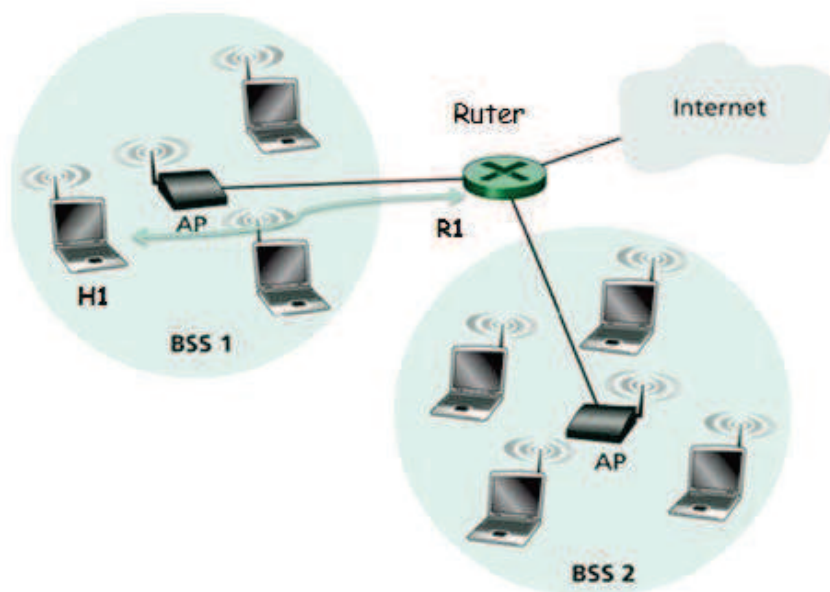
Možda je najupadljivija novost u okviru 802.11 to što postoje *četiri* adresna polja od kojih svako može da primi 6-bajtnu MAC adresu. Ali zašto četiri adresna polja? Zar nije dovoljno MAC polje izvora i MAC polje odredišta kao kod Etherneta? Ispada da su međusobno povezivanje mreža potrebna tri adresna polja – konkretno, za prenos datagrama mrežnog sloja iz bežične stanice kroz pristupnu tačku u interfejs rutera. Četvrto adresno polje koristi se u ad hoc mrežama, ali ne i u infrastrukturnim mrežama. Pošto ovde razmatramo samo infrastrukturne mreže, obratićemo pažnju na prva tri adresna polja. Standard 802.11 definiše ova polja na sledeći način:

- Adresa 2 je MAC adresa stanice koja šalje okvir. Prema tome, ako bežična stanica šalje okvir, u adresno polje 2 stavlja se MAC adresa te stanice. Slično tome, ako pristupna tačka šalje okvir, u adresno polje 2 stavlja se MAC adresa pristupne tačke.
- Adresa 1 je MAC adresa bežične stanice koja treba da primi okvir. Prema tome, ako okvir šalje mobilna bežična stanica, polje adrese 1 sadrži MAC adresu odredišne pristupne tačke. Slično tome, ako okvir šalje pristupna tačka, polje adrese 1 sadrži MAC adresu odredišne bežične stanice.

- Da biste shvatili adresu 3, setite se BSS (koji se sastoji od pristupne tačke i bežičnih stanica) čini deo podmreže i da se ova podmreža povezuje sa drugim podmrežama preko nekog ruterskog interfejsa. Adresa 3 sadrži MAC adresu ovog interfejsa na ruteru.

Da bismo bolje shvatili svrhu adrese 3, razmotrimo primer međumrežnog povezivanja u kontekstu **slike 9**. Na ovoj slici postoje dve pristupne tačke od kojih je svaka zadužena za niz bežičnih stanica. Svaka od pristupnih tačaka ima direktnu vezu sa ruterom koji se zatim povezuje sa globalnim Internetom. Trebalo bi imati na umu da je pristupna tačka uređaj sloj veze, pa ni jedna od njih „ne govori“ IP niti razume IP adrese. Razmotrite sada prenos datagrama od ruterskog interfejsa R1 do bežične stanice H1. Ruter nije svestan da između njega i stanice H1 postoji pristupna tačka AP; iz perspektive rutera, H1 je prosto računar u jednoj od podmreža sa kojima je on (ruter) spojen.

- Ruter, koji zna IP adresu H1 (na osnovu adrese odredišta u datagramu), koristi ARP da bi utvrdio MAC adresu H1, kao u običnom Ethernet LAN-u. Kada pribavi MAC adresu stanice H1, ruterski interfejs R1 enkapsulira datagram u Ethernet okvir. Polje izvorne adrese u ovom okviru sadrži MAC adresu interfejsa R1, a polje adrese odredišta sadrži MAC adresu stanice H1.
- Kada Ethernet okvir stigne u pristupnu tačku AP, AP konvertuje Ethernet okvir 802.3 u okvir 802.11 pre nego što ga pošalje u bežični kanal. AP popunjava prvu adresu MAC adresnog računara H1, a adresu 2 vlastitom MAC adresom, kao što je gore opisano. U polje za treću adresu AP ubacuje MAC adresu rutera R1. Na taj način, H1 će (iz adrese 3) saznati MAC adresu ruterskog interfejsa koji je poslao datagram u podmrežu.



Slika 9. Korišćenje adresnih polja u okvirima 802.11

Razmotrimo sada šta se događa kada bežična stanica H1 odgovori slanjem datagrama iz H1 u R1.

- H1 pravi okvir 802.11 i popunjava adresu 1 MAC adresom pristupne tačke, a polje adrese 2 MAC adresom stanice H1, kao što je gore opisano. U polje adrese 3 H1 unosi MAC adresu rutera R1.
- Kada AP primi okvir, 802.11 konvertuje ga u Ethernet okvir. Polje adrese izvora u tom okviru biće MAC adresa stanice H1, a polje adrese odredišta biće MAC adresa rutera R1. Prema tome, polje adrese 3 omogućava pristupnoj tački da odredi odgovarajuću MAC adresu odredišta da bi napravila Ethernet okvir.

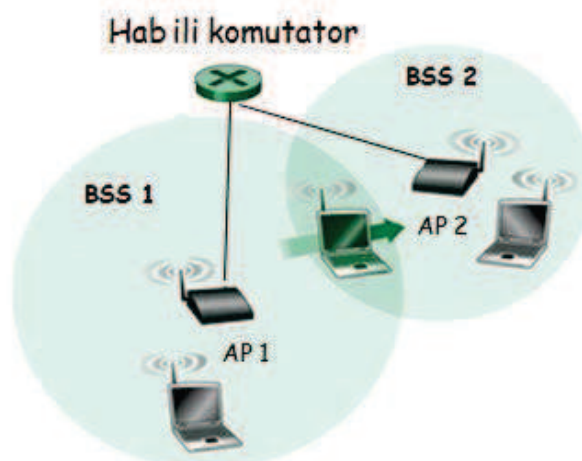
Da rezimiramo adresa 3 igra ključnu ulogu u međusobno umrežavanje bazne stanice sa ožičenim LAN-om.

2.3 Mobilnost unutar iste IP podmeže

Da bi se povećao fizički domet bežičnog LAN-a, kompanije i univerziteti postavljaju više baznih stanica unutar iste IP podmeže. Ovo, naravno, otvara pitanje mobilnosti između baznih stanica – kako da se bežične stanice neprimetno prebacuju sa jedne na drugu baznu stanicu ne prekidajući postojeće TCP konekcije? Kao što ćemo videti u ovom odeljku, kada bazne stanice pripadaju istoj podmreži mobilnost se relativno jednostavno omogućava. Kada se stanice kreću po različitim podmrežama, biće potrebni složeniji protokoli za upravljanje koje ćemo proučiti u narednim odeljcima.

Pogledajmo sada konkretan primer mobilnosti između baznih stanica u istoj podmreži. Na **slici 10** prikazane su dve međusobno povezane bazne stanice i jedan računar, H1 koji se kreće između baznih stanica BSS1 i BSS2. Pošto u ovom primeru uređaj koji međusobno povezuje bazne stanice *nije* ruter, sve stanice i ovih baznih stanica, uključujući i pristupne tačke AP pripadaju istoj IP podmreži. Prema tome, kada H1 pređe sa BSS1 na BSS2 on može da zadrži svoju IP adresu i sve TCP konekcije koje su u toku. Da je uređaj za međusobno povezivanje bio ruter, tada bi H1 morao ili da promeni IP adresu, pa da prekine TCP konekcije koje su u toku ili da upotrebi protokol za mobilnost iz mrežnog sloja kakav je mobilni IP.

Ali, šta se konkretno dešava kada H1 pređe sa BSS1 na BSS2? Kako se H1 udaljava od pristupne tačke AP1, on otkriva da signal pristupne tačke slabi pa počinje da traži jači signal. H1 prima okvire za navođenje od pristupne tačke AP2 (koje će u mnogim korporacijskim univerzitetima okruženjima imati isti SSID kao AP1). H1 zatim raskida pridruživanje sa pristupnom tačkom AP1 i pridružuje se tački AP2 zadržavajući istu IP adresu i ne prekidajući TCP konekcije koje su bile u toku.



Slika 10. Mobilnost u istoj podmreži

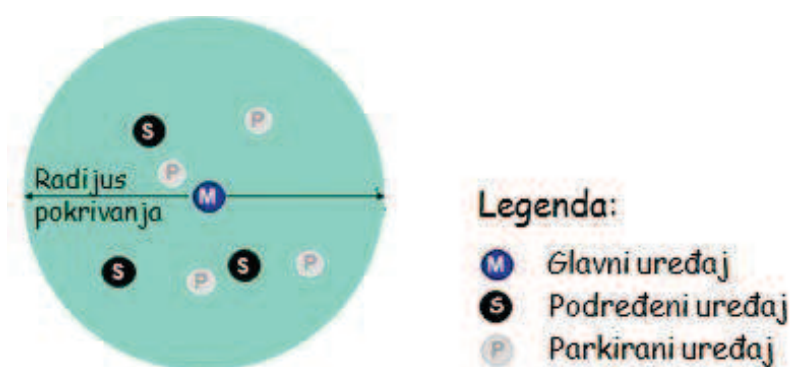
Ovo sve funkcioniše kako treba ako je uređaj za međusobno povezivanje svih hub (hab). Ali, ako taj uređaj komutator – što je često slučaj – potrebno je obratiti posebnu pažnju. Pomenimo da komutatori “sami uče” i automatski grade svoje tabele za prosleđivanje. Ta njihova sposobnost je korisna prilikom povremenih premeštanja (na primer, kada nekog zaposlenog premeste iz jednog odljenja u drugo); međutim, komutatori nisu projektovani za podršku veoma pokretnih korisnika koji žele da održe TCP konekcije dok se premeštaju između baznih stanica.

Da bismo shvatili problem koji se ovde javlja, imajmo na umu da pre premeštanja komutator u tabeli prosleđivanja ima stavku u kojoj se MAC adresa stanice H1 uparuje sa izlaznim interfejsom komutatora preko kojeg se može pronaći H1. Ako se H1 na početku nalazi na baznoj stanici BSS1, tada će datagram čije je odredište H1 uputiti preko pristupne tačke AP1. Međutim, kada se H1 pridruži BSS2, njegove okvire treba uputiti prema pristupnoj tački AP2. Jedno rešenje (u suštini doskočica) je da AP2 odmah nakon novog pridruživanja pošalje komutatoru difuzno emitovani Ethernet okvir sa adresom izvora H1. Kada komutator primi taj okvir, on ažurira svoju tabelu prosleđivanja i tako dozvoljava da se do H1 stigne preko AP2. U grupi standard 802.11f razvija se protocol za komunikaciju među pristupnim tačkama koj se bavi ovim i sličnim pitanjima.

2.4 802.15 i Bluetooth

Kao što znamo iz prethodnog, Wi-Fi standard IEEE 802.11 namenjen je komunikaciji među uređajima udaljenim do 100 metara dok pristup mreži preko mobilne telefonije ima domet na desetine kilometara. Pre nego što se upustimo u detalje ovih bežičnih mreža sa većim udaljenostima, pomenimo ukratko standard 802.15 **WPAN** (*Wireless Personal Area Network*) koji je u familiji IEEE 802 srodan sa 802.11, a namenjen je povezivanju među ličnim uređajima na rastojanju od približno 10 metara. 802.15 je u suštini tehnologija male snage, kratkog dometa i malih brzina, „zamenjena za kabal“ za međusobno povezivanje notbuka, perifernih uređaja, mobilnih telefona i PDA-a dok je 802.11 „pristupna“ tehnologija veće snage, srednjeg dometa i veće brzine².

² R. Morrow, *Bluetooth: Operation and Use*,



Slika 11. Piko mreža 802.15

Mreža IEEE 802.15 funkcioniše na kratkom rastojanju, majom snagom i manje košta. Slojevi veze i fizički sloj 802.15 zasnivaju se na prethodnoj specifikaciji **Bluetooth** a lične mreže. Mreže 802.15 funkcionišu u radio opsegu 2,4 GHz za koji nisu potrebne licence, u vremenskom multipleksu i sa vremenskim odseccima od 624 mikro sekunde. U svakom vremenskom odsečku pošiljalac emituje na jednom od 79 kanala tako što se kanal menja na poznat, ali pseudo slučajan način od odsečka do odsečka. Taj oblik preskakanja kanala, poznat kao **FHSS** (*Frequency Hopping Spread Spectrum*) emituje sa podelom vremena po frekventnom spektru. 802.15 omogućuje brzine do 721 Kb/s.

Mreže 802.15 su ad hoc mreže: za povezivanje uređaja 802.15 nije potrebna nikakva mrežna infrastruktura (npr. pristupna tačka). Prema tome, uređaji 802.15 moraju sami da se organizuju. Uređaji 802.15 prvo se organizuju u **piko mreže** od najviše osam aktivnih uređaja kao što je prikazana na **slici 11**. Jedan od ovih uređaja postaje glavni, a ostali uređaji su mu podređeni. Glavni čvor zaista upravlja piko mrežom – njegov sat određuje vreme u piko mreži, on može da emituje u svakom neparnom odsečku dok podređeni može da emituje samo pošto je glavni čvor sa njim komunicirao u prethodnom odsečku, pa čak i tada on može da emituje samo prema glavnom čvoru. Pored podređenih uređaja u mreži može biti i maksimalno 255 parkiranih uređaja. Ovi uređaji ne mogu da komuniciraju dok im glavni čvor ne promeni status iz parkiranog u aktivni.

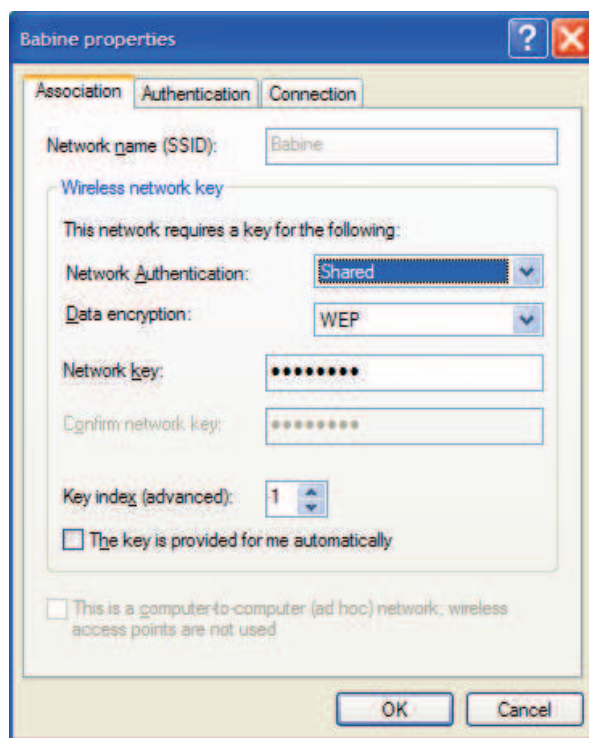
3. WEP

WEP (*Wired Equivalent Privacy*) definisan je u standard 802.11 i cilj mu je da obezbedi sledeće:

- poverljivost poruka – osnovna namena je sprečavanje prisluškivanja mrežnog saobraćaja (engl. *eavesdropping*),
- kontrolu pristupa – pristupne tačke mogu zabraniti klijentima pristup mreži ukoliko ne zadovolje proveru identiteta,
- integritet poruka – dodatno polje u okviru služi za proveru integriteta samog okvira

WEP se koristi radi zaštite podataka na sloju veze OSI modela. Na **slici 12** prikazan je Windows XP dijalog za izbor načina provere identiteta (pomoću deljenog ključa) i šifrovanja podataka (WEP).

WEP protokol je dizajniran kao kombinacija kontrole pristupa, privatnosti linka i Message Integrity sistema za WLAN. Bežični ruteri i tačke pristupa koriste WEP sigurnost za šifrovanje podataka koji se šalju i primaju preko bežičnih uređaja. WEP protokol je usvojio 802.11 komitet i služi za zaštitu bežičnog saobraćaja. Postoji 3 tipa WEP ključeva za šifrovanje koje koriste Off-the-shelf bežični ruteri: 40-bit, 128-bit i 256-bit (RC4). Kao dodatak WEP ključu, Service Set Identifier (SSID) treba da bude podešen na bežičnoj tački pristupa (Access Pointu). SSID identifikuje ime bežične mreže; ovaj iznos se emituje preko tačke pristupa u formi čistog teksta i može se dobiti korišćenjem prostog *protocol analyzer* u sekundama. Neke bežične tačke pristupa imaju mogućnost da zabrane emitovanje SSID i samim tim čine da maliciozni korisnici ne mogu lako da se konektuju.



Slika 12. Dijalog *Wireless network properties*, kartica *Association*

U upotrebi su dva WEP standard i to su: Statički WEP i dinamički WEP

- **Statički WEP** Wired Equivalent Privacy (WEP) je prvi put predstavljen da asistira u kreiranju mogućnosti vazduha koja je jednaka sigurnosti u kablovima. Statički WEP ima nekoliko ograničenja i ona uključuju: Teško je upravljati klijentskim WEP ključevima zato što svi klijenti dele isti statički WEP ključ. Kompromitovanje ovog ključa može da ugrozi kompletnu komunikaciju. Statički WEP ključevi obično se ne menjaju što rezultuje time da napadač ima više vremena da osmisli napad. WEP ključ može lako da se oporavi koristeći dostupne alatke.

- **Dinamički WEP** je nestandardna tehnologija. Ona definiše samo postavke za šifrovanje podataka i integritet bežičnih mreža. Ovaj metod mora da bude spojen sa naprednom sigurnosnom solucijom koja uključuje jaku autentifikaciju i dinamičko ponovno dodeljivanje ključeva za šifrovanje (Re-keying). Iako je ovaj metod siguran u praksi, administrator bi trebali da budu upoznati sa sledećim problemima: Dinamički WEP koristi odvojen statički ključ za globalnu transmisiju kao što je emitovanje (Broadcast) paketa. Za razliku od individualnih korisničkih ključeva, globalni ključ se ne obnavlja. Korišćenje statičkih ključeva za globalni prenos podataka daje napadaču mogućnost otkrivanja informacija o mreži kao što su IP adresa i imena kompjutera; WEP Protected Network Frames daje slabu zaštitu integritetu.

Sigurnost WEP-a je zasnovana na tajnosti ključa pomoću kog se telo okvira poruke šifrjuje na relaciji pristupna tačka - klijent. Konkretno, snaga WEP-a se temelji na težini otkrivanja tajnog ključa pomoću napada grubom silom; međutim, zahvaljujući nekim sigurnosnim propustima, napadi na WEP su znatno brži i uspešniji.

3.1 Napadi na WEP

Postoji nekoliko vrsta napada na WEP, a oni se grubo mogu klasifikovati u dve kategorije:

- **Pasivni napadi** – napadač samo prisluškuje komunikaciju korisnika s mrežom. U ove napade spadaju analiza mrežnog saobraćaja i pasivno prisluškivanje;
- **Aktivni napadi** – napadač aktivno utiče na mrežni saobraćaj tako što ubacuje svoje podatke, lažira komunikaciju između klijenata i pristupne tačke, zagušuje saobraćaj na mreži ili neovlašćeno koristi mrežne resurse. U ove napade spadaju ponavljanje inicijalizacionog vektora, obrtanje bitova, čovek u sredini, krađa sesije i napad ponavljanjem paketa.

3.1.1 Pasivni napadi

Analiza mrežnog saobraćaja je najjednostavniji pasivni napad – napadač prisluškuje mrežu i prati broj i veličinu paketa u mreži. Za ovu vrstu napada napadaču je potrebna zadovoljavajuća antenna, mrežna kartica koja radi u režimu slušanja (ne šalje nikakve pakete) i softver koji će analizirati veličinu i broj paketa. Pomoću toga napadač može saznati tri osnovne informacije:

- količinu mrežnog saobraćaja – pojava naglog povećanja saobraćaja na mreži obično ukazuje na neki bitan događaj,
- fizičku lokaciju pristupnih tačaka – pomoću usmerene, tj. Yagi antene, u kombinaciji s GPS-om (engl. *Global Positioning System*) napadač metodom triangulacije može doći do fizičke lokacije pristupne tačke ili centra bežične mreže,
- vrste protokola koji se koriste na mreži.

Pasivno prisluškivanje je takođe relativno jednostavan napad jer napadač samo osluškuje mrežu. Jedini uslov za uspešan napad ovog tipa jeste pristup signal mreže, a tu do izražaja dolazi fizička sigurnost mreže, tj. koliko je projektant vodio računa o prostiranju signala pristupnih tačaka u prostoru. Prema nekom standardnom scenariju napada, napadač osluškuje mrežu čekajući da se ponovi isti inicijalizacijski vektor i tako, na prethodno opisani način, dolazi do vrednosti $P_1 \oplus P_2$. Posle toga, napadač na osnovu poznatih reči jedne poruke može odmah doći do druge poruke. Ukoliko napadač ne zna nijednu poruku, koristeći informacije o protokolima dobijene napadom analiza saobraćaja, može prepoznati neke konstantne delove poruka i tako doći do podataka. Na primer, izvorišna i odredišna IP adresa koje su fiksne dužine nalaze se na fiksnoj udaljenosti od početka paketa. TCP protokol ima na tačno određenom mestu zapisan izvorišni i odredišni port. Isti se princip može primeniti na zaglavlja raznih aplikacija koje imaju potpuno definisan oblik (na primer, HTTP protokol).

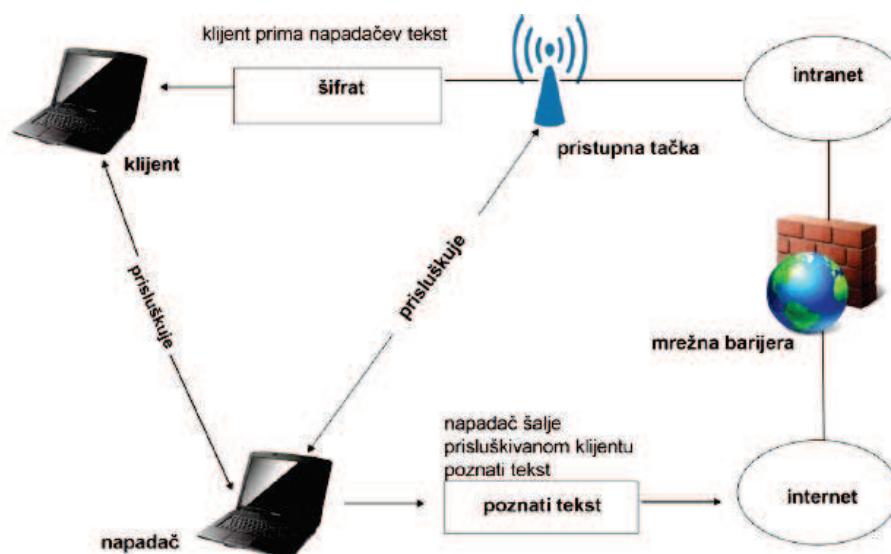
3.1.2 Napad ponavljanjem inicijalizovanog vektora

Jedan od mogućih scenarija napada **ponavljanjem inicijalizovanog vektora** (engl. *IV replay attack*) jeste sledeći:

- napadač preko Interneta šalje poruku klijentu koga želi da napadne,
- napadač zatim pažljivo priskuškuje mrežu i čeka da pristupna tačka pošalje klijentu poruku s nepoznatim tekstom,
- napadač “skida” kriptografsku zaštitu s poruke jer mu je poznat inicijalizacioni vektor šifrovane poruke.

Nakon toga napadač može dodavati svoje podatke u šifrovane pakete. Pri ovakvom napadu, osnovna pretpostavka je da se inicijalizacioni vektor i WEP ključ mogu ponavljati sve dok mreža ne prihvati da je to ispravan paket. Kada napadač dobije niz bitovi kojim je paket šifrovan, on može taj niz primeniti na druge podatke koje će sam ubaciti u mrežu. Napad je prikazan na **slici 13**.

Napadač koji je dobio niz bitova kojim je šifrovan paket (engl. *keystream*) može primeniti taj niz na druge podatke koje će sam ubaciti u mrežu. Sam process proširivanja ključa obavlja se u nekoliko koraka. Napadač može izgraditi paket tako što će ga povezati za jedan octet. Idealni kandidat za to je ICMP odgovor. Napadač povećava niz bitova ključa za jedan bit. Vrednost bitova dodatnog okteta se pogađa, ali to ne predstavlja problem jer postoji samo 256 mogućih vrednosti. Kada pogodi ispravnu vrednost okteta, napadač dobija odgovor na ICMP paket koji je poslao.



Slika 13. Napad ponavljanjem inicijalizacionog vektora

3.1.3 Napad čovek u sredini

Napad **čovek u sredini** može se iskoristiti za čitanje ili modifikaciju podataka. Zasnovan je na propustu u standard koji ne omogućava obostranu proveru identiteta klijenata i pristupne tačke. Napadač se postavlja u komunikacioni kanal između klijenata i pristupne tačke i presreće komunikaciju, a zatim izvodi napad.

- Napadač prekida komunikaciju klijenata i pristupne tačke i ne dopušta klijentu da ponovno uspostavi vezu s pristupnom tačkom.
- Klijent nastoji da uspostavi vezu s pristupnom tačkom, ali pošto ne može, uspostavlja vezu s napadačevim računarom koji glumi pristupnu tačku. Napadač se predstavlja pristupnoj tački kao klijent i upostavlja vezu s njom. Na ovaj način napadač uspostavlja dva tunela: napadač – klijent i napadač – pristupna tačka.

Kao podvrsta ovog napada izdvajaju se ARP napadi, koji mogu da se iskoriste i protiv računara koji nisu na bežičnoj mreži. Napadač lažno predstavlja pristupnoj tački i time dobije pristup mreži. Napadač šalje lažni odgovor na ARP upit i tako menja način na koji se do tada povezivala određena MAC adresa sa IP adresom. Nakon toga, napadač se nalazi između dva klijenata i može uticati na komunikaciju.

3.1.4 Krađa sesije

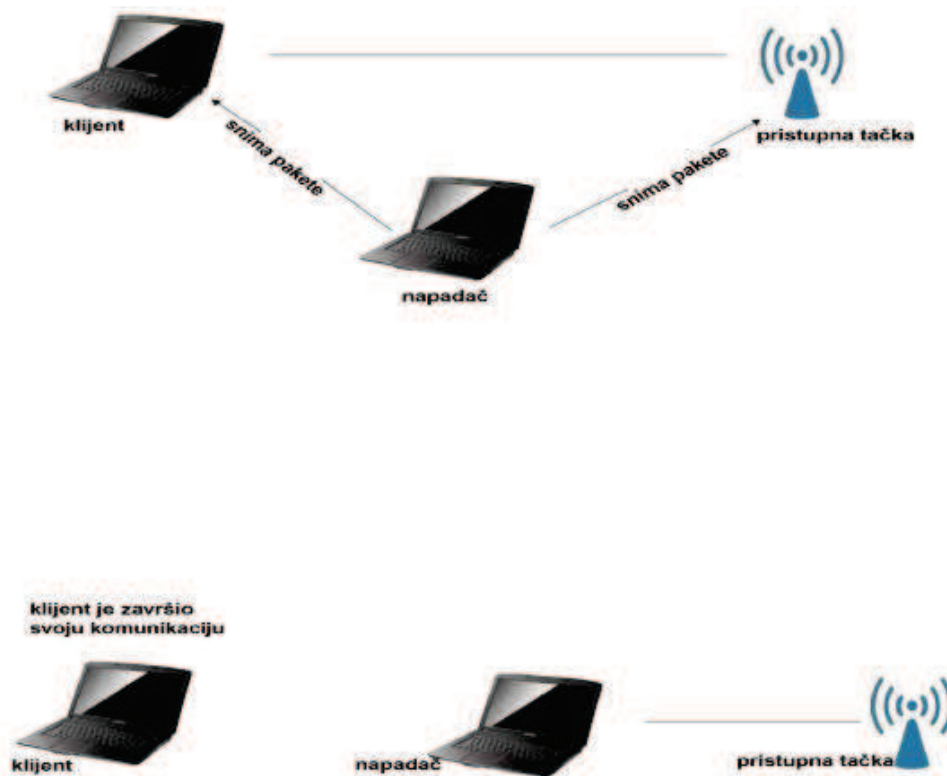
Krađa sesije (eng. *Session hijacking*) predstavlja napad usmeren protiv integriteta sesije između korisnika i pristupne tačke – napadač krađe sesiju identifikovanom i autorizovanom korisniku mreže. Žrtva zna da je izgubila sesiju, ali ne zna da je tu sesiju preuzeo napadač; žrtvi se čini da je u pitanju normalan prestanak rada bežične mreže. Napadač koji je ukrao sesiju može nastaviti

da radi u mreži proizvoljno dugo. Preduslovi za uspešan napad ovog tipa su mogućnost lažiranja paketa viših slojeva, korišćenje onih metoda provere identiteta i šifrovanja koje mreža zahteva, i mogućnost da se spreči dalja komunikacija žrtve s pristupnom tačkom.

3.1.5 Napad ponavljanjem paketa

Napad ponavljanjem paketa (engl. *packet re-play attack*) takođe je usmeren na narušivanje integriteta informacija na mreži. Za razliku od prethodnog napada, ovde se ničim ne utiče na tekuće sesije – napad se odvija kada klijent završi svoju sesiju. Napadač snima jednu ili više sesija između klijenata i pristupne tačke kako bi ih kasnije iskoristio. Kada klijent završi svoju sesiju, napadač ponavlja njegove pakete i tako dobija pristup mreži (**slika 14**). Bez daljih sigurnosnih prepreka, napadač može koristiti sve privilegije klijenata čije je sesiju snimio. Ukoliko napadač ne može da zaobiđe šifrovanje koje se koristi na mreži, on je i dalje u mogućnosti da modifikuje pakete kako bi narušio integritet podataka.

Kao što se iz izloženog vidi, postoji veliki broj mogućih napada na WEP, a neki od njih sui uspešno izvedeni. To sve govori u prilog činjenici da je WEP, a samim tim i standard koji ga definiše, potpuno nesiguran i da bi što pre trebalo da se zameni nekim sigurnijim i boljim standardom koji bi potpuno uklonio navedene propuste.



Slika 14. Napad ponavljanjem paketa

3.2 Upravljanje ključevima

Ovaj vrlo bitan detalj nije definisan u standard, nego je njegovo rešavanje prepušteno na volju proizvođačima mrežne opreme. Zbog toga je samo nekoliko najvećih proizvođača mrežne opreme ugradilo u svoje uređaje bilo kakav način upravljanja ključevima. Nažalost, i ti proizvođači ne iznose dovoljno informacija o nivou sigurnosti koju su ugradili u svoje proizvode. Da stvari budu gore, neki proizvođači u opisu svojih rešenja iznose da koriste protokole i metode s dobro poznatim sigurnosnim propustima, na primer Diffie-Hellmanov protokol koji je ranjiv na napad “čovjek u sredini”.

Standard definiše dve metode za korišćenje WEP ključeva.

- U prvoj metodi koristi se prozor sa četiri ključa. Klijent ili pristupna tačka mogu dešifrovati podatke koji su šifrovani s bilo kojim od ta četiri ključa. Ali sam prenos podataka je ograničen na samo jedan od ta četiri ključa – standardni (engl. *default*) ključ.
- Druga metoda je **mapiranje ključa** (engl. *key mapping method*). U ovoj metodi, svaka jedinstvena MAC adresa može imati svoj ključ. Ključevi su zapamćeni u pristupnoj tački i broj različitih ključeva zavisi od kapaciteta pristupne tačke. Odvojeni ključ za svaku MAC adresu nameće pitanje koliko često će se menjati ključevi jer se oni menjaju tako što se ručno unose (pošto je to jedini siguran način) kod svakog korisnika mreže, što donosi nove problem kako korisnicima tako i administrator bežične mreže. Ovde je opisan standardni WEP sa 40-bitnim ključem. Izvoz dužih ključeva je prema američkim zakonima dugo bio zabranjen. Sada proizvođači uvode svoje nadogradnje i proširuju ključ na 128 bitova, što smanjuje verovatnoću uspešnog napada grubom silom, ali ne doprinosi ukupnoj sigurnosti mreže, jer se za inicijalizacioni vector i dalje koriste 24 bita pa veličina ključa nije važna ukoliko se dvaput upotrebi isti inicijalizacioni vektor.

3.3 WPA i WPA2

Korišćenje bežične mreže podrazumeva prenos putem medijuma koji je dostupan svima na mnogo većem prostoru od onog koji neophodna samom korisniku. Prema tome, svako može da presretne pakete podataka koji su u etru. Dovoljan je bežični adapter, odgovarajući softver i malo znanja. Ukoliko se možete konektovati na svoju bežičnu mrežu bez ukucavanja lozinke to je znak da ne postoji nikakav sistem zaštite. U tom kontekstu, termin sigurnost označava enkriptovane podatke dok se prenose kroz vazduh. Cela ideja zaštite se svodi na sprečavanje drugih da dođu u posed tih informacija i samim tim i zloupotrebu istih.

Oko 25% bežičnih veza uopšte nisu obezbeđene, što znači da svako može da koristi njihove internet veze i da vrlo lako provali u računare u tim mrežama. A onda su bankovni računi, lični podaci i ostale adrese i lozinke slobodne za zloupotrebu.

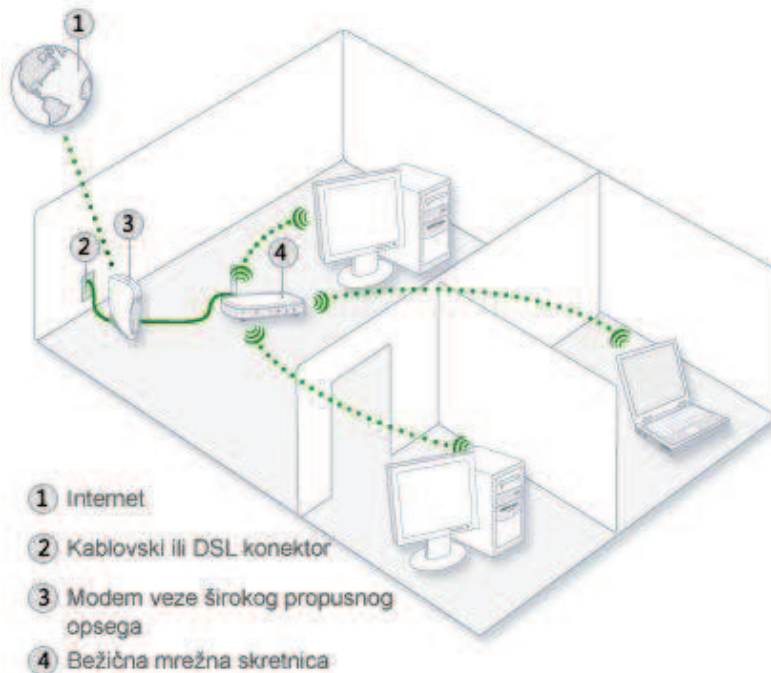
Wi-Fi mreže nude tri opcije zaštite:

- WEP
- WPA
- WPA2

WEP (Wired Equivalent Privacy) je najstariji vid zaštite definisan još davne 1999 godine. Zasnivao se na unapred poznatom ključu i obično se koristi u 64-bitnoj i 128-bitnoj varijanti. Pokazao se kao veoma slab i samo vam daje lažni osećaj sigurnosti jer se uz odgovarajući softver praćenjem saobraćaja između stanica moguće razbiti ključ u roku od nekoliko minuta. Nemojte ga koristiti.

Oko 25% bežičnih mreža je „obebeđeno“ WEP enkripcijom, čije se ključevi vrlo lako mogu provaliti uz pomoć besplatnih alata na internetu.

WPA/WPA2 (Wi-Fi Protected Access) su protokoli izvedeni iz 802.11i standarda i mnogo su bezbedniji od WEP-a. WPA tehnički predstavlja sertifikaciju. Ne predstavlja sigurnosni standard obzirom da uključuje samo jedan sigurnosni protokol TKIP. Kombinacija WPA i TKIP protokola nije najbolje rešenje, ali pruža zadovoljavajuću sigurnost. WPA dozvoljava dve vrste autentifikacije: WPA-802.1x (WPA-Enterprise) i WPA-PSK. WPA-802.1x (RADIUS) podrazumeva da postoji RADIUS (Remote Authentication Dial-in User Service) server u mreži. RADIUS server vrši autentifikaciju na osnovu sertifikata koji su ranije dodeljeni klijentskim stanicama i ne dozvoljava pristup nikome ko ne poseduje validan sertifikat. Ova vrsta WPA protokola se koristi uglavnom u većim organizacijama, dok je za SOHO i kućno okruženje zadužen WPA-PSK. WPA-PSK za autorizaciju koristi lozinku dužine od 8 do 63 karaktera koja mora biti uneta i na klijentu i na pristupnoj tački (access point). Ako je lozinka dovoljne dužine (preporučuje se barem 13 karaktera) i složenosti, da bi se izbegao napad sa pogađanjem lozinke iz rečnika ili brute force-om, WPA2-PSK je potpuno bezbedan protokol.



Slika 15. Smernice za zaštitu bežičnih mreža

4. Celularni pristup Internetu

U prethodnom odeljku ispitali smo kako računar može da pristupi Internetu kada se nađe unutar Wi-Fi lokacije za aktiviranje tj. kada se nalazi u blizini pristupne tačke 802.11. Ali, većina Wi-Fi lokacija a aktiviranje ima mali domet, između 10 i 100 metara u prečniku. Šta da radimo kada imamo očajničku potrebu za bežičnim pristupom Internetu, a nije nam dostupna Wi-Fi lokacija za aktiviranje? S obzirom na to da je mobilna telefonija sada sveprisutna na mnogim područjima u celom svetu, prirodna strategija bi bila da se celularne mreže prošire tako da podrže ne samo govornu telefoniju već i bežični pristup Internetu. Idealno bi bilo da taj pristup Internetu bude brz i da obezbedi nesmetanu mobilnost tada da korisnici ne prekidaju TCP konekcije za vreme putovanja, na primer, autobusom ili vozom. Pod uslovom da uzvodne i nizvodne brzine budu dovoljne, korisnik bi čak mogao da održi video konferencijsku sesiju dok kreće. Taj scenario nije posebno nerealan.

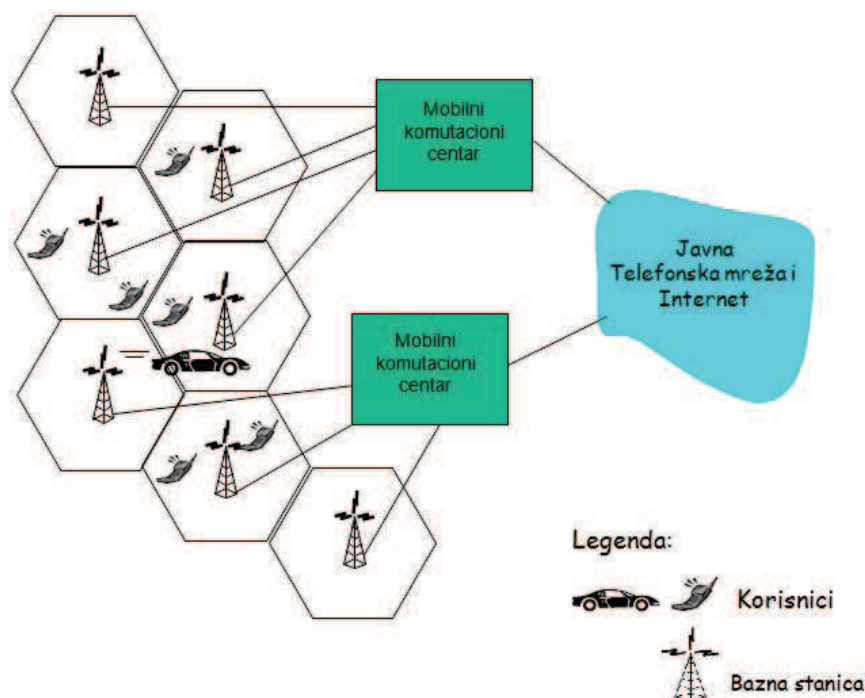
U ovom odeljku daćemo kratak pregled tehnologija za pristup Internetu koje trenutno postoje ili se upravo pojavljuju. Fokus će nam biti na bežičnom prvom skoku između mobilnog telefona i ožičene infrastrukture telefonske mreže.

4.1 Opšti pregled celularne arhitekture

Izraz *celularni* odnosi se na činjenicu da se geografsko područje deli na određen broj geografskih područja pokrivanja, koje nazivamo **ćelijama**, kao što na levoj strani **slike 16**. Svaka ćelija sadrži jednu baznu stanicu koja emituje signale i prima signale od mobilnih stanica u svojoj ćeliji. Područje pokrivanja jedne ćelije zavisi od mnogih faktora uključujući emisiju snagu bazne stanice, emisiju snagu mobilne stanice, od građevina koje zaklanjaju prostor u ćeliji i visinu antene bazne stanice. Mada na **slici 16** svaka ćelija sadrži jednu baznu stanicu koja se nalazi na sredini ćelije, mnogi današnji sistemi postavljaju bazne stanice na uglove gde se seku tri ćelije tako da jedna bazna stanica sa usmerenim antenama može da opsluži tri ćelije.

4.1.1 Osnovna mrežna infrastruktura

Kao što se vidi na **slici 16** svaka bazna stanica povezana je sa regionalnom mrežom – kao što je javna telefonska mreža – ili direktno sa Internetom preko ožičene infrastrukture. Konkretno, na **slici 16** vidi se da je svaka bazna stanica povezana sa mobilnim komutacionim centrom MSC (*Mobile Switching Center*) koji upravlja uspostavljanjem i raskidanjem poziva mobilnih korisnika. MSC sadrži dobar deo funkcionalnosti koji postoji u običnom telefonskom komutacionom centru (kakav je PBX ili centrala), ali ima dodatnu funkcionalnost potrebnu za rad sa mobilnim korisnicima.



Slika 16. Komponente arhitekture celularne mreže

4.1.2 Pristupne tehnike vazdušnog interfejsa

Uobičajena je situacija da se u datoj ćeliji istovremeno obavlja više poziva. Ovi pozivi moraju da dele raspon radio spektra koji je dodeljen posredniku za celularne usluge. Većina celularnih sistema danas koristi jedan od dva opšta pristupa za deljenje radio spektra:

- *Kombinacija frekventnog (FDM) i vremenskog (TDM) multipleksiranja.* Kod frekventnog multipleksiranja kanal deli na određen broj frekventnih opsega tako da se svaki opseg namenjuje jednom pozivu. Takođe kod čistog vremenskog multipleksiranja vreme se deli na okvire i svaki okvir se dalje deli na odsečke, pa svaki poziv dobija na korišćenje određeni odsečak u pokrentom okviru. U sistemima sa kombinacijom FDM/TDM kanal se deli na niz frekventnih podopsega; u svakom podopsegu se vreme deli na okvire i odsečke. Prema tome, u sistemu sa kombinacijom FDM/TDM, ako je kanal podeljen na F podokvira, a vreme na T odsečaka, tada će kanal biti u stanju da podrži $F * T$ istovremenih poziva.
- *Višestruki poziv sa kodnom podelom (CDMA).* Sećamo se da CDMA ne deli ni frekvencije niti vreme. Umesto toga, svi korisnici dele istu radio frekvenciju u isto vreme. Svaki korisnik u ćeliji dobija zaseban niz bitova koji nazivamo niz za seckanje. Kao što smo prethodno videli, kada pošiljalac i primalac koriste isti niz za seckanje, primalac može iz istovremenih slanja svih pošiljalaca da rekonstruiše ono što je poslao

njegov pošiljalac. Glavna prednost sistema CDMA je u tome što eliminiše potrebu da se dodeljuju frekvencije. Kada se koristi FDM/TDM, na primaoce utiče interferencija od drugih signala u istom frekventnom opsegu. Prema tome, u sistemu FDM/TDM se data frekvencija može ponovo koristiti samo u ćelijama koje su prostorno dovoljno udaljene tako da ne bude interferencije. Prilikom projektovanja CDMA sistema takvo **ponovno korišćenje frekvencija** ne predstavlja značajno pitanje.

4.2 Celularni standardi i tehnologije

Kada ljudi govore o celularnim tehnologijama, obično ih klasifikuju na nekoliko „generacija”. Starije generacije su bili projektovane pre svega za govorni saobraćaj; novji celularni sistemi osim govora podržavaju i pristup Internetu. Pošto mi u radu pominjemo umrežavanje, nas, naravno, više zanimaju novije generacije celularnih sistema. Ali, pošto su novije generacije direktno nastale od starijih, ipak ćemo početi pregled kratkim opisom bežičnih sistema prve i druge generacije.

Pri opisivanju ovih generacija naići ćemo na niz izraza koji se koriste u različitim tehnologijama. Kao čitalac, nemamo obavezu da potpuno prihvatimo i zapamtimo sve ove izraze i skraćenice. Svrha ovog pregleda jeste da nam pruži uvidu u postojanje različitih generacija bežičnih sistema i da posluži kao brzi podsetnik za različite izraze i skraćenice.

Sistemi prve generacije (1G) su bili analogni FDMA sistemi projektovani samo za govorne komunikacije. Ovi sistemi su sada skoro nestali, a zamenili su ih digitalni sistemi 2G.

4.2.1 Druga generacija (2G)

Sistemi druge generacije, iako su digitalni takođe su projektovani za govornu komunikaciju. Ali, pošto su današnji sistemi 2,5G, 3G i 4G, projektovani da podrže i prenos podataka, nastali od sistema 2G, važno je reći nekoliko reči o sistemima 2G. Mobilni telefon 2G konvertuje analogni govorni signal u digitalni format pre nego što ga modulira i zatim pošalje u etar. Digitalna tehnologija 2G ima mnoge prednosti nad analognom tehnologijom 1G a to su povećani kapacitet usluga unutar ćelije, napredna bezbednost od zloupotreba i naprednije usluge kao što su identifikacija pozivaoca i poruke. Većina današnjih mobilni operatera koristi tehnologiju 2G. U širokoj upotrebi su različiti 2G standardi i tehnologije. Neke od njih su:

- **IS-136** (*Interim Standard 136*) TDMA. Ovo je kombinovani FDM/TDM sistem koji potiče iz FDMA tehnologije 1G. On je u širokoj upotrebi u Severnoj Americi.
- **GSM** (*Global System for Mobile Communications*). Tokom '80-tih godina Evropljani su uvideli potrebu za digitalnim sistemom koji će važiti svuda u Evropi i zameniti njihove nekompatibilne sisteme 1G i omogućiti neprimetnu mobilnost među zemljama kao i mogućnosti i usluge koje nisu moguće u analognim sistemima. Ova potreba dovela je do

standarda GSM za celularne komunikacije. Evropljani su veoma uspešno uveli GSM tehnologiju početkom '90-tih. GSM se zatim proširio na Aziju i Severnu Ameriku, i sada predstavlja standard za celularnu komunikaciju sa najširoom primenom. GSM standard za celularne sisteme 2G za vazdušni interfejs koristi kombinovani FDM/TDM. GSM sistemi se sastoje od opsega frekvencija od po 200 kHz gde svaki opseg podržava 8 TDM poziva. GSM kodira govor na 13 kb/s i 12,2 kb/s.

- **IS-95 CDMA.** Za razliku od sistema IS-136 i GSM, koji koriste FDM/TDM, sistem IS-95 CDMA koristi višestruki pristup sa kodnom podelom. Kompanija Qualcomm demonstrirala je izvodljivost sistema CDMA za mobilnu telefoniju krajem '80-tih godina; od tad je uvedemo više sistema IS-95, pogotovo u Severnoj Americi i Koreji.

4.2.2 Prelaz sa druge generacije na treću (2,5G)

2G sistemi kao što su IS-95, GSM i IS-136 optimizirani su za govorne usluge i nisu pogodni za prenos podataka. Tokom '90-tih organizacije za standarde utvrdile su da postoji potreba za celularnu tehnologiju 3G koja bi bila pogodna i za govor i za prenos podataka (uključujući pristup Internetu). Međutim, pošto je uvođenje tehnologije 3G trajala godinama, kompanije su razvile privremene protokole i standarde koje su omogućavali prenos podataka preko postojeće infrastrukture 2G. Takvi sistemi nose zajedničko ime „celularni sistemi 2,5G”. Navodimo neke od njih:

- **GPRS (General Packet Radio Service)** je razvijen iz GSM-a. Za rad sa podacima, GSM igra uslugu modema između korisničkog uređaja i određene mreže podataka tj. GSM koristi komutiranje vodova kako za podatke tako i za govorni saobraćaj. Standard GSM podržava brzine prenosa do 9,6 kb/s što je nedopustivo sporo za bilo šta osim za čisti tekst. GPRS predstavlja privremeno rešenje koje omogućavaju efikasnije usluge za podatke sa paketima pri većim brzinama (obično u rasponu od 40 do 60 kb/s). GPRS usluga pruža se na osnovu postojeće GSM mreže. Međutim, za razliku od čistog GSM'a, mobilna GPRS stanica može na zahtev da koristi više vremenskih odsečaka u datom kanalu. Kada se koristi GPRS, određen broj odsečaka se rezerviše za prenos podataka i dinamički se dodeljuje mobilnim stanicama zavisno od njihove trenutne potražnje.
- **EDGE (Enhanced Data Rates for Global Evolution).** Glavni cilj sistema EDGE jeste da se povećaju moguće brzine u mreži GSM/GPRS, tj. da se bolji iskoristi GSM kanal od 200 KHz sa okvirima od po 8 TDMA odsečaka. To se postiže pre svega zamenom modulacione šeme GSM'a jednom snažnijom šemom. Teoretski, EDGE može korisnicima da obezbedi 384 kb/s za prenos podataka.
- **CDMA2000, faza 1.** Ova tehnologija 2,5G nastala je od IS-95. Ona može da obezbedi usluge za pakete podataka do 144,4 kb/s i priprema teren za uvođenje 3G sistema CDMA2000, faza 2.

4.2.3 Treća generacija (3G)

Celularni sistemi treće generacije potrebni su za pružanje telefonske usluge, kao i za prenos podataka pri osetno većim brzinama od odgovarajućih sistema druge generacije³. Od sistema treće generacije se pre svega očekuje da omoguće:

- 144 kb/s za korisnike u vožnji;
- 384 kb/s za upotrebu van zgrade u mirovanju ili pri brzini hoda;
- 2 Mb/s za upotrebu u zgradi

U područje treće generacije postoje dva glavna standarda koja se trenutno bore za prevlast:

- **UMTS (Univesal Mobile Telecommunications Service)** je prošireni GSM sa podrškom za mogućnosti treće generacije. Arhitektura UMTS mreže većim delom nasleđuje već uspostavljenu arhitekturu GSM mreže. Međutim, radio pristup UMTS-a značajno se razlikuje od šeme FDM/TDM-a koja se koristi za GSM. Konkretno, UMTS koristi CDMA tehniku poznatu pod imenom DSWCDMA (Direct Sequence Wideband CDMA). UMTS se upravo uvodi u velikom delu Evrope što ne iznenađuje s obzirom na to da UMTS potiče od GSM-a.
- **CDMA-2000** je razvijen od 2G sistema IS-95 i kompatibilan je unazad sa sistemom IS-95. Kako bi se očekivalo na osnovu imena, on u svom vazdušnom interfejsu takođe koristi CDMA. CDMA-2000 se uvodi u Severnoj Americi i u delovima Azije.

4.2.4 Četvrta generacija (4G)

Pošto smo razmotrili i tehnologiju bežičnog LAN-a i niz tehnologija za celularni pristup, vratimo se malo i razmotrimo šta bismo mi kao korisnici u idealnoj situaciji očekivali od bežičnog pristupa Internetu. Verovatno ste do sada nebrojeno puta videli oznaku 4G, ali niste sigurni šta to zaista znači i predstavlja.

Oznaka 4G se odnosi na četvrtu generaciju bežične mobilne telefonije. Sve je počelo davne 1980. godine sa 1G analognim uređajima koji su bili teški i imali velike dimenzije. Kasnije, digitalne mreže su dozvolile proizvodnju 2G mobilnih telefona, koji su se koristili za slanje poruka i pozive. 3G mreže su sa sobom donele razvoj smartphone uređaja i brzog prenosa informacija. Sa 4G tehnologijom se briše razlika između glasa i drugih vrsta podataka. 4G tehnologija pretvara mobilni uređaj u Voice-over-IP (VoIP) sistem. VoIP je protokol za prenos glasa preko Interneta i drugih paketnih mreža. Glas se na ovaj način prenosi u obliku digitalizovanog zvuka, najčešće komprimovanog i ućaurenog u tok paketa podataka u IP mreži.

³ J. Korhonen, Introduction to 3G Mobile Commucations, 2nd ed., Artech House,

VoIP podrazumeva bržu i jasniju komunikaciju. Međunarodna telekomunikaciona unija definiše 4G kao mogućnost skidanja podataka pri brzinama od 100 megabita (Mb) do 1 gigabita (Gb) u sekundi. Pošto trenutno ne postoje mreže koje mogu da podrže te brzine, razvijen je koncept "dugoročne evolucije" ili "Long Term Evolution" (LTE), čija je maksimalna brzina teoretski postavljena na 100 Mbps. Brzine prenosa u realnom vremenu su 20 Mbps ili manje.

5. Sigurnost GSM mreža

Korišćenje mobilnih uređaja doživljava veliku ekspanziju u poslednjih nekoliko godina. Pretpostavlja se da će se upotrebljavati možda i nekoliko stotina miliona uređaja. Trend rasta već nekoliko godina i može se očekivati da će u dogledno vreme broj mobilnih uređaja premašiti broj fiksnih linija.

U računarskim mrežama u kojima se za prenos podataka koriste žičani i optički medijumi, postoji viši nivo inherentne fizičke sigurnosti nego u Wi-Fi mrežama (potreban je fizički pristup telefonskoj žici). Analogno tome, fiksna telefonija je sigurnija od mobilne. Pojednostavljeno rečeno, svako s radio-prijemnikom teoretski može oslušivati eter, dok je u fiksnoj telefoniji potrebno fizički pristupiti prenosnom medijumu ili centrali. Zbog toga je bilo potrebno u GSM sistemu ostvariti zavidan nivo sigurnosti mobilnih uređaja, odnosno prenosa govora i podataka, pogotovo nakon propusta koji su bili uočeni u starijim mobilnim tehnologijama.

GSM specifikacija identifikuje tri sigurnosne usluge značajne za GSM komunikaciju:

- **Provera identiteta korisnika** – sposobnost mobilnog uređaja da dokaže kako ima dozvolu za korišćenje određenog pretplatničkog računa kod GSM operatera,
- **Poverljivost podataka i signalizacionih paketa** – svi podaci (govor i tekstualne poruke) i signalizacioni paketi moraju biti šifrovani,
- **Anonimnost korisnika** – u trenutku provere identiteta pretplatnika, jedinstveni IMSI mora biti šifrovan.

Iako GSM tehnologija obezbeđuje zadovoljavajući nivo sigurnosti, ona ipak ima i određene sigurnosne nedostatke koji su se mogli iskoristiti za kompromitovanje korisnika. Ti nedostaci su najčešće bili posledica štednje na sigurnosnim implementacijama i neznanja odgovornih ljudi. Novije tehnologije, kao što su GPRS, UMTS tj. 3G, ispravljaju i te nedostatke.

U ovom poglavlju ukratko ćemo opisati sigurnost GSM tehnologije, uključujući i njene nedostatke, kao i metode otklanjanja tih nedostataka⁴.

5.1 GSM mreža

Za ostvarivanje pokretljivosti u javnoj mreži, najvažniji današnji opšti sistem za mobilne komunikacije (engl. *Global System for Mobile Communications*, GSM), njegovo proširenje opštim paketskim radio-uslugama (*General Packet Radio Services*, GPRS), i opštim sistemom za mobilne komunikacije (*Universal Mobile Telecommunication System*, UMTS), koji je ujedno i predstavnik treće generacije (3G) mobilnih mreža.

⁴ Wikipedia, <http://en.wikipedia.org/wiki/GSM>

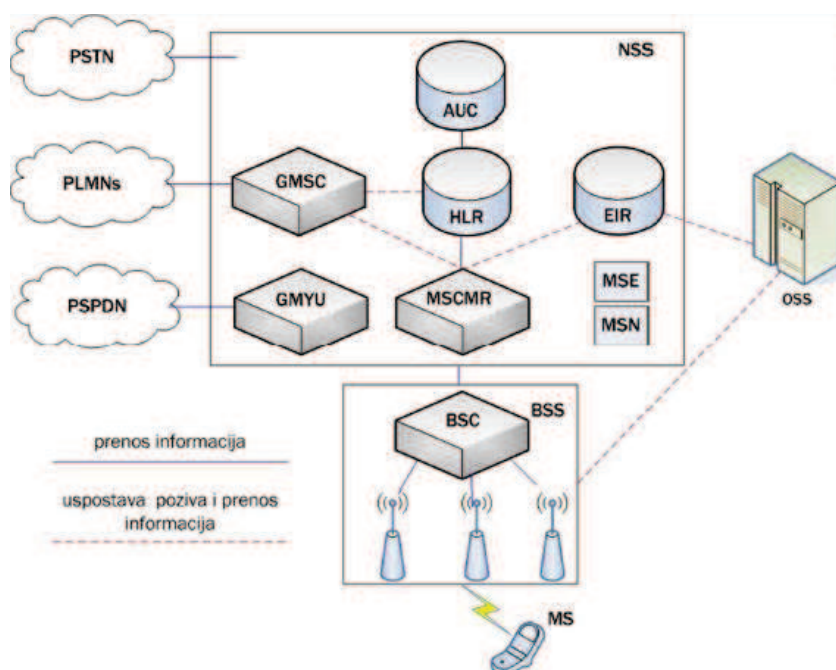
GSM mreža pokriva područje radio-signalom na principu ćelija (engl. *cellular*). **Ćelija** je područje koje pokriva jedna **bazna stanica**. Ovakva struktura je pogodna jer omogućava dobru iskorišćenost raspoloživih frekvencija – u sesednim ćelijama se koriste različite frekvencije, a u udaljenim ćelijama je moguće koristiti iste frekvencije. GSM je digitalni sistem u kome se višestruki pristup ostvaruje u vremenskoj podeli tako da je na svakoj od 124 frekvencije raspoloživo 8 kanala, što daje ukupno 992 kanala.

GSM mrežu čine četiri osnovna dela (prikazani na **slici 17**).

- [1] Korisnični terminal, tj. **mobilni uređaj** (*Mobile Station, MS*) sastoji se od komunikacione pokretne opreme i pametne kartice (engl. *smartcard*) – SIM (*Subscriber Identity Module*). Svaki mobilni uređaj ima jedinstveni identifikacioni broj – IMEI (*International Mobile Equipment Identity*), koji identifikuje pretplatnika u mobilnoj mreži.
- [2] **Sistem baznih stanica** (*Base Station System, BSS*). Sve funkcije za radio-prenos obavljaju se unutar BSS-a koji se sastoji od kontrolnih baznih stanica (*Base Station Controllers, BSC*) i primopredajnih baznih stanica (*Base Transceiver Station, BTS*). BSC je preklopnik visokog kapaciteta koji pruža sve kontrolne funkcije i fizički povezuje komutacioni centar (MSC) i BTS. Jedan MSC opslužuje više BSC-ova. BTS upravlja radio- saobraćajem s mobilnim uređajima. Sadrži radio-opremu (primopredajnici i antene) potrebnu za opsluživanje svih ćelija u mobilnoj mreži. BSC kontroliše grupu BTS-ova.
- [3] **Mrežni i komutacioni sistem** (*Network and Switching, NSS*). Komutacioni sistem služi za obradu poziva i pretplatničkih usluga, a čine ga:
 - **Domaći lokacijski registar** (*Home Location Register, HLR*). Baza podataka koja sadrži informacije o pretplatnicima, pretplatničkim uslugama, informaciji o lokaciji pretplatnika i aktivacioni status mobilnog uređaja. U jednom GSM mreži postoji samo jedan HLR.
 - **Komutacioni centar mobilnih usluga** (*Mobile Services Switching Center, MSC*). Komutacioni sistem koji upravlja pozivima s drugih telefona ili komunikacionih uređaja (ili ka njima), naplaćivanjem, povezivanjem različitih mobilnih mreža i signalizacijom.
 - **Gostujućí lokacijski registar** (*Visitor Location Register, VLR*). Baza podataka koja sadrži privremene informacije o gostujućim pretplatnicima potrebne MSC-u. Kada se pretplatnik nađe u lokacijskom području određenog MSC-a, VLR povezan s dotičnim MSC-om zatražiće informacije o pretplatniku od njegovog HLR-a i na taj način omogućiti pozive, bez potrebe da se svaki put upostavlja kontakt sa HLR-om.
 - **Centar za proveru identiteta** (*Authentication center, AC*). Sadrži parameter za proveru identiteta i šifrovanje kojima se proverava identitet pretplatnika i obezbeđuje sigurna komunikacija.
 - **Registar identifikacione opreme** (*Equipment Identity Register, EIR*). Baza podataka koja sadrži informacije o identitetu mobilnih uređaja na osnovu njihovog identifikacionog broja (IMEI).
- [4] **Operacione sistem i sistem podrške** (*Operation and Support System, OSS*). Povezan je sa svom opremom i komutacionom sistemom i sa BSC-om, što omogućava GSM operateru da upravlja GSM sistemom i nadzire mrežu.

Ostali funkcionalni elementi GSM mreže su:

- Centar za poruke (*Message Center, MXE*). Upravlja SMS porukama, govornom poštom, faks porukama i porukama elektronske pošte.
- Čvor za mobilne usluge (*Mobile Service Node, MSN*) upravlja inteligentnim mobilnim uslugama.
- Usmerivač usluga komutacionog centra (*Gateway Mobile Services Switching Center, GSMC*). Povezuje dve različite mobilne mreže.



Slika 17. Struktura GSM mreže

5.2 Provera identiteta korisnika

Proverom identiteta se sprečava prijavljivanje neovlašćenih korisnika i neovlašćena upotreba korisničkih naloga ovlašćenih korisnika, tj. pretplatnika. U suprotnom, neovlašćeni korisnik bi mogao da „otme“ tuđi pretplatnički nalog i da ga koristi, ali bi račun i dalje stizao oštećenom pretplatniku. Da bi se rešio taj problem, potrebno je uvesti proveru samog mobilnog uređaja.

5.2.1 IMEI

IMEI je jedinstven petnaestocifreni broj koji se koristi za identifikaciju mobilnog uređaja u mobilnoj mreži. Utisnut je na unutrašnjoj strani mobilnog uređaja (kod baterije), a moguće ga je i očitati pozivom na broj **#06#*. Sastoji se od tri polja:

- *Type Allocation Code*, TAC – osmocifreni broj koji određuje zemlju porekla mobilnog uređaja i proizvođača
- *Serial Number*, SNR – šestocifreni serijski broj uređaja
- *Check Digit*, CD – kontrolni broj koji se koristi za proveru verodostojnosti IMEI broja na različitim tipovima mobilnih uređaja.

U slučaju krađe mobilnog mobilnog, vlasnik uređaja koji zna IMEI broj uređaja može da prijavi krađu svom operateru, koji će onemogućiti korišćenje tog mobilnog uređaja u svojoj mreži. Operater bi trebalo da prosledi tu informaciju i ostalim operaterima koji takođe treba da učine isto tj. da onemoguće korišćenje ukradenog mobilnog uređaja. Teoretski, svi operateri bi trebalo da budu spojeni sa centralnom bazom podataka CEIR (*Central EIR*) u kojoj se nalaze svi IMEI brojevi svih mobilnih uređaja na svetu. Međutim u praksi to nije slučaj.

5.2.2 Algoritmi za šifrovanje komunikacije

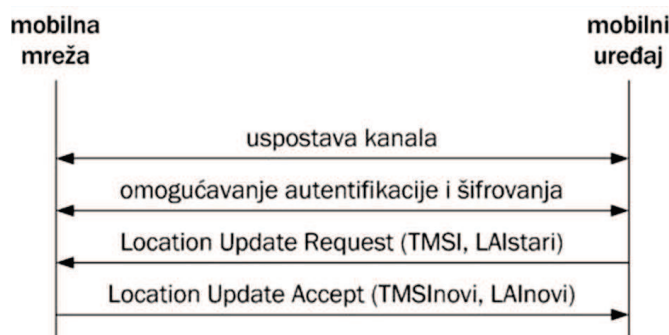
Mobilna mreža može da koristi do 7 različitih algoritama za šifrovanje (može i da ih ne koristi, tj. da ne koristi nijedan), ali sme da koristi samo one algoritme koje pojedini mobilni uređaji podržavaju. Trenutno su defitisana tri algoritma: A5/1, A5/2 i A5/3. A5/1 i A5/2 su izvorni algoritmi definisani u GSM standardu i zasnivaju se na jednostavnom linearnom pomeračkom registru s povratnom spregom (enlg. *Linear feedback shift register*, LFSR). Algoritam A5/1 sabira po modulu 2 bitove koje generišu tri LFSR-a koji se sinhronizuju pomoću bitova u samim registrima. A5/2 namerno oslabljena verzija algoritama koja se koristi u manje razvijenim regijama, dok se A5/1 koristi u Sjedinjenim Američkim Državama, Velikoj Britaniji i Australiji. A5/3 je dodat 2002. godine i zasniva se na otvorenom algoritmu Kasumi (koji se može jednostavno implementirati u hardveru) koji je definisano 3GPP.

Mobilna mreža može započeti šifrovanje podataka u bilo kom trenutku posle provere identiteta; za to se koristi generisani Kc. Mreža može izabrati bilo kkoji algoritam koji mobilni uređaj podržava. Šifarski algoritmi koje podržava mobilni uređaj šalju se mobilnoj mreži porukom *classmark* koja specificira mogućnosti mobilnog uređaja. Algoritam radi tako što generiše pseudoslučajnu sekvencu koja se po modulu 2 (operacili ekskluzivno ILI) dodaje korisničkim podacima koje se prenose etrom. Podase se dešifriju ponavljanjem XOR operacije nad šifratom tj. sabiranjem šifrata i pseudoslučajne sekvence po modulu 2.

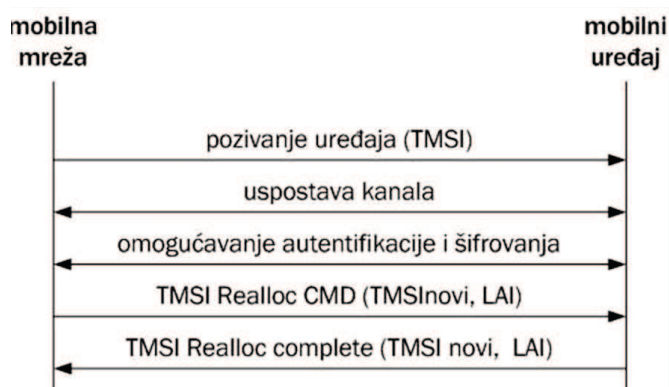
5.2.3 Anonimnost korisnika

Kada se govori o sigurnosti GSM mreža, važno je izbegavanje slanja IMSI identifikacionog broja u obliku otvorenog teksta kroz etar i onemogućavanje zlonamernika u prisluškivanja legitimnih korisnika (u kom se području korisnik nalazi i koje usluge koristi). Slanje IMSI broja u obliku otvorenog teksta izbegnuto je korišćenjem 32-bitnog TMSI broja koji je upotrebljiv na

samo jednom lokalitetu (*Location Area, LA*). Pomoću 32-bitnog TMSI broja pretplatnik se predstavlja ili se poziva. TMSI se obnavlja prilikom svake promene lokaliteta (slika 18) ili u unapred određenim vremenskim intervalima (slika 19). Kraće vreme znači obaveznu promenu TMSI, a mobilna mreža može promeniti TMSI kad god poželi. Promenjeni TMSI se uvek šalje u šifrovanom obliku ako da napadač ne može da zna kada je nastupila promena.



Slika 18. Dodela novog TMSI broja (u slučaju promene lokaliteta)



Slika 19. Dodela novog TMSI broja (u slučaju da nema promene lokaliteta)

Mobilni uređaj mora sačuvati TMSI i posle isključivanja mobilnog uređaja; TMSI se najčešće čuva na SIM kartici. Inicijalno, tj. odmah nakon proizvodnje, mobilnom uređaju nije dodeljen TMSI, već samo IMSI. Prilikom prvog šifrovanja (pri prvom uključivanju) dodeljuje se TMSI. VLR koji kontroliše lokaciju u kojoj je TMSI upotrebljiv, održava vezu između TMSI i IMSI brojeva tako što, u slučaju da mobilni uređaj uđe u područje drugog VLR-a, javlja kome pripada TMSI (koji nije odgovarajući u području drugog VLR-a).

6. Osnovni ciljevi sistema zaštite podataka

Ciljevi sistema za zaštitu podataka su jasni i precizni. Oni predstavljaju okvir za planiranje kompletnog sistema zaštite i za njegovo održavanje.

Prevenција podrazumeva sprečavanje nastanka prekršaja u vezi sa računarima ili podacima. Pojave narušavanja sistema zaštite se nazivaju i incidenti. Incidenti se mogu javiti zbog narušavanja propisanih procedura zaštite. Jednostavni incidenti se javljaju u obliku gubitka lozinke ili ostavljanja uključenog terminala preko noći sa uključenim korisnikom.

Detekcija podrazumijeva identifikaciju događaja nakon njihovog nastanka. Ona je često otežana, napad na neki sistem može biti preduzet znatno pre nego što se pokaže uspešnim. Detekcija incidenta podrazumeva utvrđivanje dela opreme koja je izložena napadu. Proces detekcije zahteva primenu složenih alata dok je ponekad dovoljno pregled sistemskih datoteka-dnevnika (log datoteka).

Odgovor podrazumeva razvoj strategija i tehnika radi neutralisanja napada i gubitaka. Ukoliko incident predstavlja samo ispitivanje terena, napadač verovatno želi da prikupi podatke o mreži i računarskim sistemima.

6.1 Funkcionisanje zaštitnih procesa

Sistem zaštite se može posmatrati kao kombinacija procesa, procedura i politike. Pored ljudskog, zaštita podataka obuhvata i tehnički faktor. Pitanja sa ljudskim faktorom razrađena su u politici zaštite koja su usvojena u organizaciji. Tehnička komponenta obuhvata alatke koje su instalirane na računarskim sistemima na kojima rade korisnici.

6.1.1 Antivirusni program

Računarski virusi, odnosno aplikacije kojima se realiziraju zlonamerne aktivnosti, predstavljaju jedan od najzamornijih trendova današnjice. Virus i ispoljavaju svoje delovanje na korisničke podatke ili na operativne sisteme, ali su, u principu, kreirani radi nanošenja štete, i to bez znanja korisnika.

Proizvodnja i prodaja softvera za zaštitu od virusa je danas prerasla u čitavu industriju. Antivirusni programi pretražuju računarsku memoriju, datoteke na disku i dolaznu i odlaznu elektronsku poštu. Redovnim ažuriranjem datoteka-definicija virusa osigurava se relativno visok stepen zaštite računarskih sistema.

6.1.2 Implementacija kontrole pristupa

Uspostavljanje kontrole pristupa predstavlja ključni deo čitavog sistema zaštite. Kontrola pristupa definiše međusobnu komunikaciju korisnika i računarskih sistema. Ona ograničava i kontroliše pristup sistemskim resursima, uključujući i podatke, čime se sprečava neovlašćen pristup podacima. Mandatory Access Control (MAC), obavezna kontrola pristupa predstavlja statički model koji koristi unapred definisani skup prava pristupa ka datotekama u nekom računarskom sistemu. Parametre definiše sistem administrator, nakon čega ih dodeljuje nalogima, datotekama ili resursima. MAC model može biti veoma restriktivan, prava definiše

administrator i to je jedina osoba koja ih izmenjuje. MAC model koristi labela za definisanje osetljivosti, koje se dodeljuju raznim objektima.

Discretionary Access Control (DAC), proizvoljna kontrola pristupa predstavlja model prava pristupa koji definiše vlasnik podataka-resursa. Za razliku od MAC modela, u ovom modelu labela nisu obavezne. DAC model omogućava deljenje datoteka između korisnika, odnosno rad sa datotekama koje je neka druga osoba proglasila deljivim. Model uspostavlja listu kontrole pristupa (ACL-Access Control List), u kojoj su navedeni svi korisnici kojima je dozvoljen pristup do podataka.

Role-Based Access Control (RBAC), kontrola pristupa na osnovu uloga, predstavlja model koji definiše ulogu koju korisnik ima u organizaciji. Korisnicima se dodeljuju određene uloge na nivou čitavog sistema, na osnovu kojih oni obavljaju određene funkcije ili dužnosti. RBAC model uobičajen je za razne uloge administratora na mreži. Npr. Backup operator ima samo ona prava koja su predviđena upravo za tu ulogu.

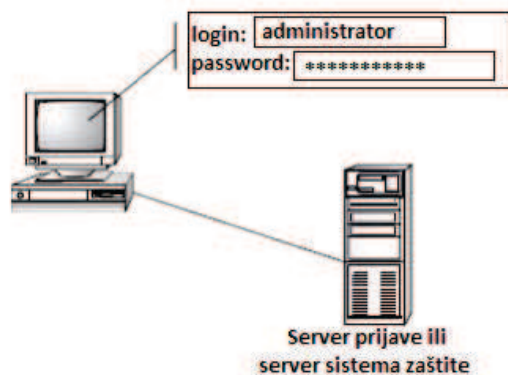
6.1.3 Funkcionisanje identifikacije

Procesom identifikacije utvrđuje se da li je neka osoba, zaista ona osoba za koju se predstavlja. Ona je ključni deo sistema zaštite. U suštini, to je deo procesa koji se naziva Identification and Authentication (I&A).

Sistemi ili metodi identifikacije zasnovani su na sledećim faktorima:

- na nečemu što korisnik zna, kao što su lozinka ili PIN
- na nečemu što korisnik poseduje ,poput smart kartice ili nekog identifikacionog uređaja
- na nečemu što fizički određuje korisnika, kao što su otisak prsta ili izgled mrežnjače oka

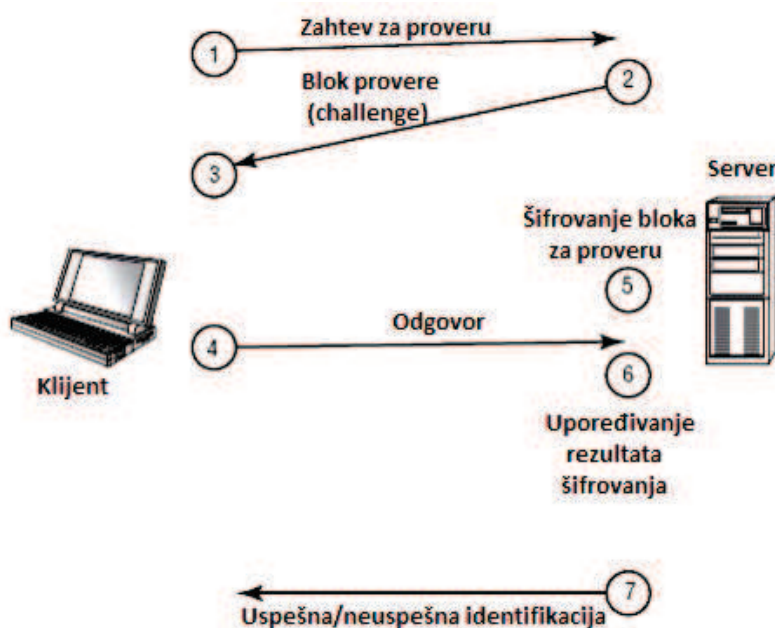
Korisničko ime i lozinka jednoznačno identifikuju korisnika tokom prijave na sistem (logon). Većina operativnih sistema koristi korisnički ID i lozinku za proces identifikacije. ID lozinka se preko mreže mogu slati u otvorenom ili šifrovanom obliku. Na **slici 20.** prikazan je proces prijave na sistem uz slanje lozinke.



Slika 20. Proces prijave na sistem preko radne stanice

Password Authentication Protokol (PAP) ne nudi punu sigurnost ali je jedan od najjednostavnijih metoda identifikacije. Korisničko ime i lozinka se u obliku otvorenog teksta šalju na server gde se vrši njihova provera. U slučaju da ime i lozinka odgovaraju podacima na serveru korisniku se odobrava pristup, u suprotnom, pristup je zabranjen.

Challenge Handshake Authentication Protocol (CHAP) koristi proveru sistema da bi ustanovio identitet korisnika. On ne koristi mehanizam korisnički ID/lozinka. Korisnik šalje zahtev za prijavu sa klijentskog računara prema serveru, server šalje blok za proveru (challenge) ka klijentu. Klijentski računar šifruje dobijeni blok i vraća ga do servera. Server proverava dobijenu vrednost i u slučaju da je ispravna potvrđuje identifikaciju. Na **slici 21.** ilustrovana je CHAP procedura.



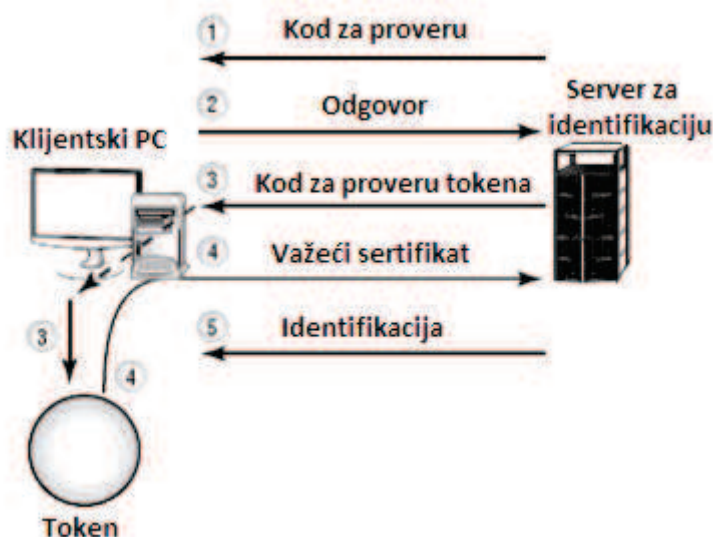
Slika 21. CHAP identifikacija

Sertifikati se izdaju u obliku fizičkih uređaja, poput smart kartica, ili u elektronskom obliku, u kom se upotrebljavaju kao deo procesa identifikacije. Izdavanje i upravljanje sertifikatima je definisano dokumentom čiji je naziv Certificate Practice Statement (CPS). Na **slici 22.** prikazano je kako server izdaje sertifikat klijentu nakon identifikacije.



Slika 22. Izdavanje sertifikata nakon ispravne identifikacije korisnika

Sigurnosni tokeni su po funkciji slični sertifikatima. Sistem za identifikaciju kreira token prilikom svakog prijavljivanja korisnika ili na početku sesije. Nakon završetka sesije token se uništava. Na **slici 23.** prikazan je proces upotrebe sigurnosnog tokena.



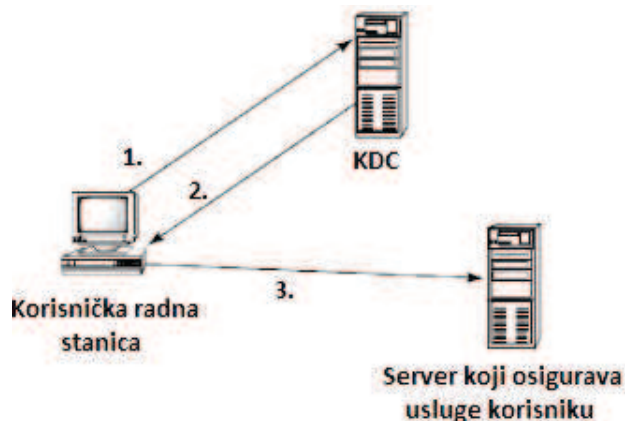
Slika 23. Identifikacija pomoću sigurnosnog tokena

Kerberos je protokol namenjen identifikaciji korisnika. Kerberos identifikacija koristi usluge KDC-a (Key Distribution Center) koji reguliše čitav proces. KDC vrši identifikaciju inicijatora procesa i dodeljuje mu kartu. Izdata karta se može iskoristiti za identifikaciju prilikom pristupa drugim objektima. Taj proces se odvija automatski kada drugi objekt uputi zahtev za identifikaciju. Na **slici 24.** prikazan je proces identifikacije pomoću Kerberos protokola, zajedno sa kartom koja se izdaje sistemu koji je prošao uspešnu identifikaciju na KDC-u.

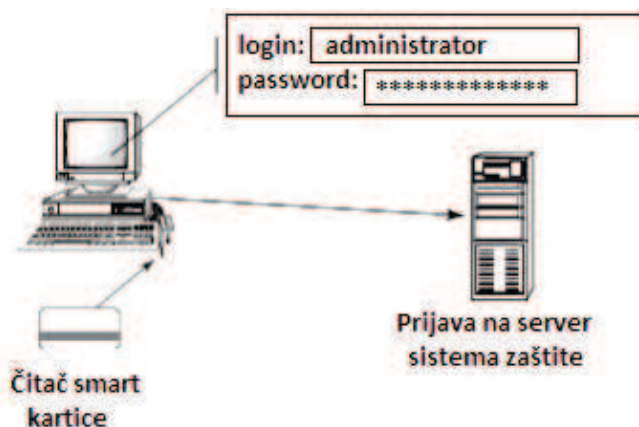
Višestruka identifikacija je proces identifikacije koji se vrši pomoću dva ili više različitih metoda. Ukoliko sistem koristi smart kartice i lozinke za pristup resursima, govorimo o dvostrukoj identifikaciji. Primer dvostruke identifikacije prikazan je na **slici 25.** U njemu su za pristup neophodne i smart kartica i lozinka.

Smart kartce sadrže podatke o identitetu korisnika i njegovim pravima pristupa. Čitač kartice je povezan sa radnom stanicom, preko koje sigurnosni sistem proverava karticu.

Biometrija je metoda identifikacije korisnika i to njegovih fizičkih karakteristika kao što su dlan i mrežnjača ali se očekuje da će se uskoro pojaviti i DNK skeneri.



Slika 24. Kerberos proces identifikacije



Slika 25. Dvostruka identifikacija

6.1.4 Funkcionisanje mrežnih servisa i protokola

Korisnicima računara na usluzi stoji veliki broj različitih servisa i protokola. Web, elektronska pošta i drugi protokoli omogućavaju komunikaciju između različitih sistema. Svaki protokol ili servis koji je instaliran na mreži povećava njenu „ranjivost“ i donosi potencijalne probleme u pogledu zaštite.

Elektronska pošta je servis koji je potreban najvećem broju korisnika i svakoj organizaciji. To znači da plan mera zaštite mora uključiti kontrolu i dolazne i odlazne elektronske pošte. Sistem elektronske pošte koristi nekoliko portova u zavisnosti od programa koji se koristi Web.

Većina poslovnih okruženja koristi razne web strategije kao osnovu za komunikaciju. Te strategije uključuju serverske i klijentske proizvode (Web preglednike). Web preglednici koriste nekoliko portova radi komunikacije sa odgovarajućim servisima. Ti portovi omogućavaju slanje i prijem podataka i klijentima i serveru.

Telnet je servis koji udaljenim korisnicima omogućava pristup na sistem emulacijom terminala. Telnet danas nije uobičajeni servis, mada se i dalje često sreće. Povezivanje korišćenjem Telneta u principu ne osigurava zaštitu podataka, tako da ga treba zameniti sličnim rutinama koje nude veću sigurnost.

File Transfer Protocol (FTP) FTP se intenzivno koristi na Internetu. FTP sesije nisu šifrovane, dok većina FTP implementacija čak ne šifrue ni korisnička imena ni lozinke na početku sesije. Većina Unix sistema nudi anonimnu verziju FTP servisa, pod nazivom Trival File Transfer Protocol (TFTP), čiju upotrebu treba izbegavati po svaku cenu.

Network News Transfer Protocol (NNTP) NNTP omogućava pristup news serverima širom Interneta. Promet se odvija slanjem i prijemom poruka sa Usenet servera, koji skladište i prosleđuju poruke. Danas postoji više od 20.000 Usenet foruma ili news grupa.

Domain Name Service (DNS) DNS se koristi za prevođenje naziva računara u internet adrese. To je uobičajeni servis koji se koristi na najvećem broju mreža. Ukoliko vaša organizacija ima svoj web sajt preko koga nudi svoje usluge, DNS će predočiti spoljnim korisnicima gde se server tačno nalazi. DNS prevodi web adrese, kao što je www.sybex.com , u TCP/IP adrese, poput 192.168.0.110.

Instant Messaging (IM) IM predstavlja vrstu trenutne elektronske pošte koja se razmenjuje između dva ili više korisnika. IM klijenti su obično izloženi zlonamernom kodu (obično kroz transfer datoteka), ali su podložni i socijalnim formama napada, pri čemu hakeri „igraju“ na osećaj krivice korisnika da bi postigli ono što žele.

Internet Control Message Protocol (ICMP) ICMP predstavlja alat za slanje poruka (kao što je Ping) u okviru mreže. Ping je rutina koja omogućava proveru dostupnosti nekog sistema slanjem paketa do njega. ICMP znatno olakšava mnoge aspekte komunikacije preko Interneta.

7. Topologija zaštite

Topologija zaštite na mreži definiše dizajn mreže i implementaciju sa stanovišta sistema zaštite. Za razliku od mrežne topologije, topologija zaštite se bavi tehnikama pristupa, zaštitom i upotrebljenom tehnologijom. Topologija zaštite obuhvata četiri osnovna pitanja:

- dizajnerske zahteve
- zaštitne zone
- tehnologiju
- zahteve poslovnog procesa

7.1 Definisanje zahteva u pogledu dizajna

Dizajnerski zahtevi topologije zaštite određuju probleme poverljivosti, integriteta, dostupnosti i nadležnosti. Obično se kaže da su poverljivost, integritet i dostupnost CIA sistema mrežne sigurnosti, mada je i nadležnost isto tako važna.

Poverljivost sprečava ili umanjuje mogućnost neovlašćenog pristupa i otkrivanja zaštićenih podataka i informacija. Postoji veliki broj podataka čija se tajnost mora štititi u skladu sa zakonskim odredbama i propisima. Takvi su, na primer, podaci o socijalnom osiguranju, o platama i zaposlenima, o bolesnicima i o raznim firmama. Oni mogu izazvati probleme u vezi odgovornosti i druge neprijatnosti ukoliko dospeju u pogrešne ruke.

Integritet podataka treba da osigura korektnost podataka sa kojima se radi. On je ključan sa stanovišta topologije zaštite. Organizacije rade sa podacima koji su im dostupni i u skladu sa njima donose važne odluke. Ukoliko podaci sa kojima se trenutno radi nisu ispravni ili ih je izmenila neovlašćena osoba, posledice mogu biti katastrofalne.

Dostupnost osigurava zaštitu podataka i sprečava njihov gubitak. Ukoliko se podacima ne može prići, njihova vrednost je minimalna. Kada neka nezgoda ili napad obore ključni server ili bazu podataka, podaci sa njega neće biti dostupni korisnicima kojima su neophodni. Takva situacija može izazvati nesagledive posledice u nekoj organizaciji.

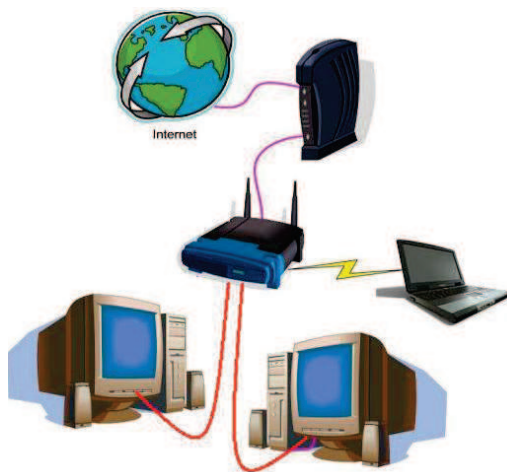
Nadležnost Najveći deo resursa neke organizacije ima deljiv karakter, tako da ih koristi više organizacionih celina i pojedinaca. Poželjno je definisati vlasnika podataka ili subjekta koji je odgovoran za njihovu validnost je dobra praksa

7.1.1 Kreiranje zaštitnih zona

Ono što je u početku izgledalo kao skup računara koji međusobno dele resurse veoma brzo prerasta u elektronsku „noćnu moru“. U njima se često javljaju veze između različitih organizacionih celina, kompanija i država, kao i različiti oblici javnog pristupa preko privatnih komunikacijskih linija i preko Interneta. Uspostavljanjem sigurnosnih zona u mrežama postiže se efekat koji omogućava izolovanje sistema i sprečavanje neovlašćenog pristupa. U praksi se najčešće sreću četiri tipa sigurnosnih zona:

- Internet
- intranet
- ekstranet
- demilitarizovana zona (DMZ)

Internet (slika 26) predstavlja globalnu mrežu koja povezuje računare i pojedinačne mreže. Može ga koristiti svako ko ima pristup preko operatera (ISP – Internet Service Provider). Takvo okruženje nameće potrebu za niskim stepenom poverenja u ostale korisnike Interneta. Zbog visokog stepena ugroženosti na Internetu, korisnici moraju obavezno štititi svoje podatke sa najvećim stepenom predostrožnosti.



Slika 26. Internet mreža

Intranet je vrsta privatne mreže koja je uspostavljena u nekoj kompaniji ili organizaciji. Može se tretirati kao Internet čije granice ne prelaze granice kompanije, to je interna mreža organizacije, gde je pristup dozvoljen samo onim sistemima koji su već spojeni na mrežu. Intranet (slika 27) koristi iste tehnologije kao i Internet. Pristup intranet mreži dozvoljen je samo proverenim korisnicima unutar korporativne mreže ili korisnicima na udaljenim lokacijama.



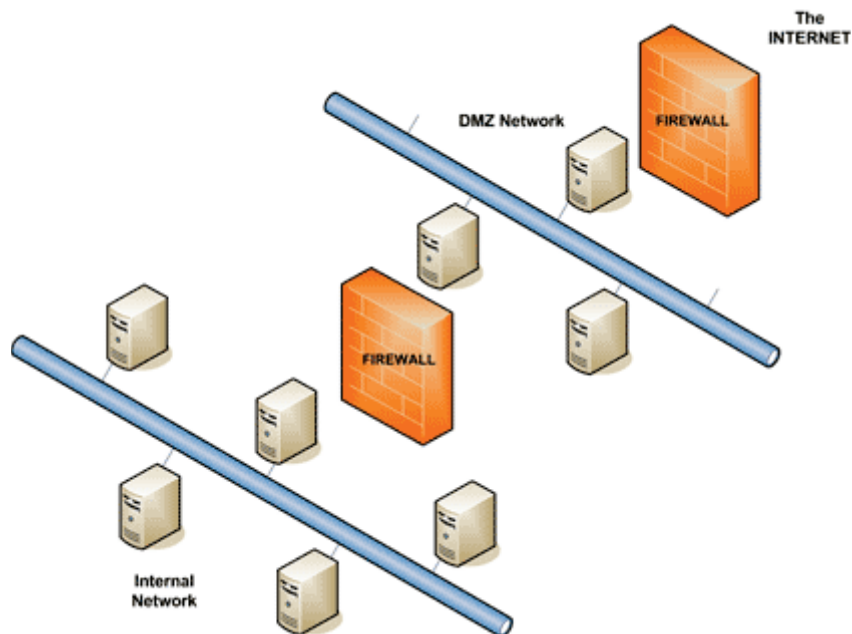
Slika 27. Prikaz intranet mreže

Ekstranet proširuje granice intranet mreže, tako da u nju uključuje i veze ka spoljnim saradnicima. Saradnici mogu biti prodavači, snabdevači ili slične institucije kojima je neophodan pristup do baze podataka u organizaciji koja je vlasnik intraneta. Ekstranet podrazumeva povezivanje onih organizacija koje uživaju međusobno poverenje. Primer ekstranet mreže dat je na **slici 28**.



Slika 28. Prikaz ektranet mreže

Demilitarizovana zona (DMZ) predstavlja oblast u kojoj se smešta javni server radi pristupa onih osoba koje ne uživaju puno poverenje. Izolovanjem servera u okviru DMZ prikriva se ili se sprečava pristup do ostatka mreže. Serveru se i dalje može pristupiti sa lokalne mreže, ali spoljni korisnici neće moći da koriste ostale mrežne resurse. Zona se kreira pomoću zaštitnog zida (engl. firewall), koja potpuno izoluje ostatak mreže.



Slika 29. Tipična DMZ

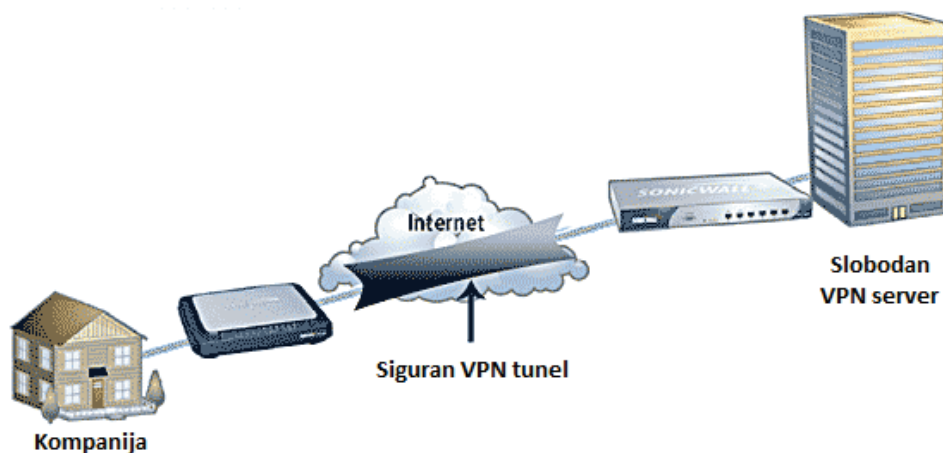
7.1.2 Rad sa novim tehnologijama

Privlačna strana tehnologije sadržana je u činjenici da se ona stalno menja; u istoj činjenici je sadržana i loša strana. Na tržištu se pojavilo nekoliko relativno novih tehnologija koje mogu pomoći u formiranju manje "ranjivih" računarskih sistema. U ovom odeljku ćemo predstaviti tri takve tehnologije: virtualne lokalne mreže (VLAN), Network Address Translation (NAT) i tunelovanje. One omogućavaju poboljšanje stepena zaštite mreže, uz minimalne dodatne troškove.

Virtualna privatna mreža (virtual local area network - VLAN) omogućava formiranje grupe korisnika i računarskih sistema i njihovo grupisanje u okviru segmenta na mreži. Podela mreže na segmente omogućava njihovo međusobno prikrivanje, čime se osigurava i kontrola pristupa. VLAN se može podesiti da kontroliše put podataka od jedne tačke do druge. On predstavlja dobar način za zadržavanje mrežnog saobraćaja u okviru određenog dela mreže.

Network Address Translation (NAT) pruža zasebnu mogućnost za poboljšanje zaštite mreže. Povećanje broja upotrebljivih internet adresa je osnovna namena NAT-a. Pomoću njega organizacija može povezati sve računare na Internet preko jedne jedine IP adrese. NAT server osigurava IP adrese za hostove ili sisteme u mreži, uz istovremeno praćenje dolaznog i odlaznog saobraćaja. Ukoliko neka organizacija koristi NAT servis, ona se na Internetu pojavljuje kao jedna jedina konekcija. Ta konekcija se realizuje preko rutera ili preko NAT servera. Eventualni napadač može dobiti samo podatak o adresi te konekcije. NAT praktično skriva lokalnu mrežu od ostatka sveta, tako da napadači teško mogu da utvrde vrstu računarskih uređaja sa druge strane rutera.

Tunelovanje podrazumeva kreiranje namenske virtualne veze između dva sistema ili mreže. Tunel (slika 30) između dve tačke kreira se (enkapsulacijom) podataka u zaseban protokol prenosa koji je ugovoren između dve strane. U većini implementacija podaci koji dolaze kroz tunel izgledaju kao da potiču sa drugog dela mreže. Protokoli tunelovanja obično osiguravaju i zaštitu podataka i njihovo šifrovanje.



Slika 30. Tipično tunelovanje

7.2 Poslovna politika u svetu sistema zaštite

Funkcionisanje neke organizacije ili poslovnog procesa obavlja se bez problema ukoliko se redovno vrši procena efikasnosti sistema zaštite. Sigurnosna procena obuhvata utvrđivanje resursa, detaljnu procenu eventualnih rizika, definisanje pretnji i proračun "ranjivosti". Pomoću navedenih komponenata upravljački organi mogu shvatiti protiv čega se bore i kako mogu ostvariti ciljeve, uz minimalne troškove.

Utvrđivanje resursa

Svaka organizacija i poslovni proces imaju vredne resurse i aktivu, na koje se mora računati, kako u fizičkom, tako i u funkcionalnom smislu. *Utvrđivanje resursa* (engl. asset identification) predstavlja proces u kome kompanija procenjuje vrednost podataka i sistema kojima raspolaže. Ponekad je to jednostavan proces koji se svodi na obično prebrojavanje sistema i softverskih licenci. Takvo fizičko utvrđivanje resursa je uobičajeni deo standardne računovodstvene procedure (popis), koju organizacije moraju redovno sprovoditi.

Procena vrednosti podataka predstavlja znatno složeniji deo procesa utvrđivanja resursa. U nekim slučajevima može se utvrditi samo šteta koja bi nastala zbog nedostupnosti ili gubitka podataka. Ukoliko bi gubitak podataka blokirao čitav posao, njihova cena je nemerljiva. Takva vrsta podataka pojednostavljuje proces definisanja metoda i pristupa za njihovu zaštitu.

Procena rizika

Postoji nekoliko načina za procenu rizika (engl. risk assessment ili risk analysis), od znanstvenih metoda, zasnovanih na formuli, do običnog razgovora s korisnicima. U principu, u proceni rizika treba identifikovati troškove zamene ukradenih podataka ili sistema, troškove usled nefunkcionalnosti sistema i sve druge faktore kojih se možete setiti. Procenu rizika je moguće izvršiti tek nakon utvrđivanja resursa. Tek kada utvrdite da Vaša baza sadrži podatke iz otvorenih izvora (kao što je US Census), koji se uvek mogu regenerisati bez problema, odnosno da tu bazu ne treba posmatrati u istom svetlu kao i onu koja sadrži specifične podatke karakteristične za poslovni proces, možete početi izračunavanje eventualnih troškova.

Definisanje pretnji

Utvrđivanje politike zaštite obavezno uključuje i procenu rizika od internih i eksternih pretnji (engl. threat) kojima podaci i mreža mogu biti izloženi. Kreiranje zaštićenog okruženja koje sprečava sve napade van neće imati nikakvu vrednost ako pretnje uglavnom potiču iznutra. Ukoliko član Vašeg tima donese u kancelariju disk "zaražen" virusom i učita njegov sadržaj na računar, virus se može proširiti preko čitave mreže, zbog toga što je potpuno imun na mere zaštite koje su usmerene prema spoljašnjem svetu.

Interne pretnje

Najveći broj dokumentovanih internih pretnji spada u grupu finansijskih zloupotreba. Zloupotrebe se javljaju u vidu prevara ili krađa. Takve pretnje, posebno u okruženjima sa intenzivnom primenom računara, teško se otkrivaju i istražuju. One su dugotrajne i obično se javljaju u obliku malih transakcija u dužem vremenskom periodu. U jednoj takvoj prevari kod velikog softverskog proizvođača nosioc je bio profesionalni računovođa, koji je pravio lažne račune za fiktivne poslove koji nikada nisu obavljani.

Eksterne pretnje

Veliki broj internih pretnji s kojima se kompanije bore uključuju i primenu procedura i metoda koje su postale industrijski standard. Eksterne pretnje, s druge strane, imaju porast koji je već na granici dramatičnosti. Pre nekoliko godina većinu incidenata izazivala su deca ili osobe koje su to radile iz hobija i radi zabave. U najvećem broju slučajeva ti incidenti nisu bili zlonamerne prirode; samo mali broj je dovodio do izmene ili uništenja podataka i sloga u bazama. Veliki broj kompanija danas koristi obimne baze podataka, interaktivne narudžbine, plaćanja, isporuke, online popis i administriranje ključnih podataka pomoću složenih sistema. Takvi sistemi su povezani sa drugim sistemima na kojima su smešteni poverljivi korporativni podaci, poslovne tajne, strategijski planovi i drugi oblici vrednih podataka.

Proračun "ranjivosti"

Zaštitne mogućnosti softvera i sistema koji se koriste u poslovanju će verovatno biti osnovna preokupacija specijaliste u oblasti računarske zaštite. Veliki broj proizvođača operativnih sistema je u bliskoj prošlosti pitanjima zaštite poklanjala samo deklarativnu pažnju. Jedan od popularnih operativnih sistema je u svrhu zaštite koristio tehniku prijave korisnika uz odgovarajuću lozinku. Nakon pojave dijaloga za prijavu na ekranu, korisnik je jednostavno mogao pritisne taster Cancel, nakon čega je imao pristup većini mrežnih i kompletnim lokalnim resursima. Ukoliko je zaštita ekrana (Screensaver) bila zaštićena lozinkom, ponovni pristup sistemu je bio moguć unosom lozinke, ali i prostim resetovanjem sustava. Takva rešenja su bila opasnija od onih bez ikakve zaštite. Veliki broj korisnika je smatrao da je njihov sistem zaštićen, mada u suštini zaštite nije bilo - rezultat su bile brojne krađe podataka koje su vršile kolege na poslu.

ZAKLJUČAK

Cilj ovog rada bio je da se prikaže situacija na tržištu usluga koje se pružaju u oblasti zaštite mreža kako bežičnih tako i mobilnih. Ukoliko bi se neka kompanija odlučila na primer da osigura bezbednu komunikaciju između svojih radnih stanica koje se ne nalaze samo u lokalnoj mreži i svojih servisa koji se nalaze kod različitih provajdera imala bi poteškoća da to ostvari. Temeljno višemesečno istraživanje pokazalo je da i ovakav na izgled jednostavan zahtev nije jednostavno sprovesti u delo. U ovom radu data su rešenja i konkretni predlozi koji mogu da pomognu IT menadžerima u kompanijama da prevaziđu neke od problema prilikom implementacija bezbednosnih sistema.

Rad započinjemo jednim uvodom u bežične i mobilne mreže, povlačeći značajnu granicu između zadataka koje nameće *bežična* priroda komunikacionih linkova u tim mrežama i onih koji su posledica *mobilnosti* koje ti bežični linkovi omogućavaju. Na taj način bolje razdvajamo, prepoznajemo i savladavamo ključne koncepte svakog od ovih područja. O Wi-Fi bežičnim mrežama i LAN-ovima tipa 802.11 objašnjeno je u drugom odeljku. Prvo se usredsređuje na napade u WEP-u koji su razmotreni u odeljku 3. U odeljcima 4 i 5 razmotreni su alati za napade sigurnost GSM mreže i celularni pristup Internetu. Zatim se posvećuje pažnja na osnovne ciljeve sistema zaštite podataka koji su opisani u odeljku 6. O topologiji mreže, kreiranje zaštitnih zona i radom sa novim tehnologijama govori se poslednjem odeljku ovog rada, odeljak 8.

REFERENCE

- [1] <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029>
- [2] <http://computerlearnhow.com/the-difference-between-internet-and-intranet/>
- [3] IEEE 802.11 a/b/g, the set of IEEE standards for wireless computer communications, <http://standards.ieee.org/getieee802/802.11.html>
- [4] http://www.sans.org/reading_room/whitepapers/wireless/80211-8021x-wireless-security_171
- [5] <http://en.wikipedia.org/wiki/GSM>
- [6] http://www.mikroknjiga.rs/Knjige/SRSM/01_SRSM.pdf
- [7] Luis Zarzo Fuertes „*OFDM PHY Layer Implementation based on the 802.11a Standard and System Performance Analysis*“;
- [8] <ftp://mirror01.transact.net.au/sourceforge/f/project/fi/fileuploads/scea/sun-certified-enterprise-architect.pdf>
- [9] <http://www.digit.co.rs/srp/mreze/bezicne-mreze.php>
- [10] *802.11 Security* The Unofficial 802.11 Security Web Page, <http://www.drizzle.com>
- [11] *Bisdikian 2011* C. Bisdikian, „An Overview of the Bluetooth Wireless Technology,“ *IEEE Communications Magazine*, No. 12 (decembar 2001): 86-94.
- [12] *Bluetooth 2002* R. Morrow, *Bluetooth: Operation and Use*, New York: McGraw-Hill, 2002.
- [13] *Cerf 1974* V. Cerf i R. Kahn, „A Protocol for Packet Network Interconnection,“ *IEEE Transactions on Communications Technology*, Vol. COM-22, No. 5, str. 627-641.
- [14] *Dornan 2007* A.Dornan, *The Essential Guide to Wireless Communications Applications: From Cellular Systems to WAP and M-Commerce*, Prentice Hall, Upper Saddle River, N.J., 2007
- [15] *Goodman 1997* David J. Goodman, *Wireless Personal Communications Systems*, Prentice-Hall, 1997.
- [16] *IEEE 802.11 2004* „IEEE 802 LAN/MAN Standards Committee“, <http://www.ieee802.org/>
- [17] *Korhonen 2003* J. Korhonen, *Introduction to 3G Mobile Communications*, 2nd ed., Artech House, 2003.