

**UNIVERZITET SINGIDUNUM**

**Departman za poslediplomske studije**

**Integracija informacionih sistema i sigurnost razmene  
podataka sa osvrtom na VPN mreže**

**MASTER RAD**

**Mentor:**

**Prof. dr Mladen Veinović**

**Kandidat:**

**Ivan Milić**

**Beograd, 2012.**

## **REZIME:**

Bezbednost informacionih sistema predstavlja izuzetno široku oblast koju karakteriše dinamičan razvoj. Poznato je pravilo da sve ono što je tek napisano ili objavljeno je već i zastarelo, što rečito govori o silovitom razvoju ove oblasti.

Podaci koji se čuvaju i obrađuju na finansijskom tržištu, a samim tim i štite, mogu se u osnovi podeliti na dve grupe : podaci o vlasnicima hartija od vrednosti i podaci o transakcijama hartija od vrednosti. Neophodan uslov za trgovinu vrednosnim hartijama je posedovanje nedvosmislenog dokaza o posedovanju hartija. Kupac u svakom trenutku mora biti siguran da kupuje hartije od pravog vlasnika. U anglosaksonskom konceptu, ne postoji jedna centralizovana institucija koja garantuje vlasništvo nad hartijama, već je ta institucija, uslovno rečeno, distribuirana. Svaka transakcija, koja se odigra na finansijskoj berzi ili van nje, mora biti pravovremeno obrađena i poslata Centralnom registru hartija od vrednosti na obradu u smislu promene vlasništva nad hartijama.

Pri implementaciji bežičnih mreža postavlja se pitanje definicije politike bezbednosti, pre svega koju opremu i metode zaštite podataka odabrati. U ovom radu su, kao teoretska osnova, iznete neke od osnovnih postavki teorije informacija. Navedeni su najčešće korišćeni standardi za bežične računarske mreže, a standardi IEEE 802.11x. i IEEE 802.16 su detaljnije obrađeni. Razmotreni su mehanizmi zaštite podataka i u okviru njih detaljnije analizirane slabosti i pretnje po bezbednost. Korišćeni su dostupni softverski alati sa interneta za prikupljanje i analizu bežičnog mrežnog saobraćaja. Sa tim alatima je praktično isprobano nekoliko mogućnosti ugrožavanja bezbednosti bežične mreže. Pored napretka i dalje postoji nebezbednost u 802.11x. Mogući su napadi uskraćivanjem resursa i lažiranjem zaglavlja paketa. Možda je potrebno redizajniranje celog skupa protokola? Za sada bežične mreže nije preporučljivo koristiti u okruženjima koja ne tolerišu nepouzdanost ili nedostupnost.

**Ključne reči:** VPN, Sigurnost podataka

## **ABSTRAKT:**

Security of information systems present extremely wide area which is characterized by very fast development. The very well known rule is that what of material is written or published is already outdated, what is telling us about tremendous development in this area.

The data is keeping and treated on to the financial market, and also ensured, could be separated in two groups : data about the owners of securities as well as data about their transactions. Necessary condition for trading with securities is owning the definite proof about ownership for shares and bonds. Purchaser have to be ensured, in every moment, that he is buying the securities from approved owner. In Anglo-Saxon concept, there is no one centralized institution which guarantee ownership for securities, yet, mentioned institution is, we can say, distributed. Every transaction, on stock exchange or out of stock exchange, have to be beforehand managed and send to Central registry and depository due to changing the ownership.

In this paper as theoretical base are exposed some basic thesis in information theory. There are named often used standards for wireless networks, and standards IEEE 802.11x. and IEEE 802.16 are detailed presented. There are discussed mechanism for data protection, and in this frame work detailed analysed weakness and threats for data security. It is used from web available software tools for gathering and analyse wireless network traffic. With this tools are practice proved some possibilities for threat wireless network security. No consideration for the well being there are much unsecurity in 802.11x. There are many possibilities for attack type denial of service and masquerade header. Maybe it is necessary to redesign set of protocols? In this moment it is not recommended to use wireless network in conditions where no tolerance for unreliability or unavailability.

**Keywords:** VPN, Data security

## **SADRŽAJ:**

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>Uvod .....</b>                                             | <b>6</b>  |
| <b>1. Pojam informacionog sistema .....</b>                   | <b>8</b>  |
| 1.1. Sistem .....                                             | 8         |
| 1.2. Podatak i informacija .....                              | 9         |
| 1.3. Bezbedna informacija .....                               | 9         |
| 1.4. Proučavanje informacionog sistema .....                  | 11        |
| 1.5. Tipovi informacionog sistema .....                       | 12        |
| 1.6. Informacionog sistema – realni sistem .....              | 12        |
| 1.7. Razvoj informacionog sistema .....                       | 13        |
| 1.8. Faze u razvoju informacionog sistema .....               | 13        |
| 1.9. Planiranje razvoja informacionog sistema .....           | 14        |
| 1.10. Analiza i dizajn informacionog sistema .....            | 16        |
| <b>2. Integracija Heterogenih Informacionih Sistema .....</b> | <b>18</b> |
| 2.1. Integracija podataka .....                               | 18        |
| 2.2. Ciljevi .....                                            | 19        |
| 2.3. Istorija problema .....                                  | 20        |
| 2.4. Real Time Integracija .....                              | 23        |
| 2.4.1. XML web servisi .....                                  | 24        |
| 2.4.2. Service Oriented Architecture (SOA) .....              | 25        |
| <b>3. VPN – Virtuelna privatna mreža .....</b>                | <b>27</b> |
| 3.1. Pojam, prednosti i nedostaci VPN .....                   | 27        |
| 3.2. Klasifikacija virtuelnih privatnih mreža .....           | 29        |
| 3.3. Komponente virtuelnih privatnih mreža .....              | 30        |
| 3.3.1. Protokoli .....                                        | 30        |

|                                                              |           |
|--------------------------------------------------------------|-----------|
| 3.3.2. Firewall .....                                        | 31        |
| <b>4. Bezbednost Virtuelnih privatnih mreža .....</b>        | <b>32</b> |
| 4.1. VPN zasnovane na internim mrežama .....                 | 32        |
| 4.2. VPN zasnovane na eksternim mrežama .....                | 33        |
| 4.3. VPN zasnovane na sistemima sa udaljenim pristupom ..... | 34        |
| 4.4. VPN na mrežnom nivou OSI referentnog modela .....       | 34        |
| 4.5. VPN na nivou veze podataka OSI referentnog modela ..... | 35        |
| <b>5. Kontrola pristupa u VPN .....</b>                      | <b>37</b> |
| 5.1. Autentifikacija u VPN .....                             | 37        |
| 5.2. Autorizacija u VPN .....                                | 39        |
| 5.3. Accounting u VPN .....                                  | 39        |
| <b>6. Zaštita VPN .....</b>                                  | <b>43</b> |
| <b>7. Mere za poboljšanje bezbednosti WLAN .....</b>         | <b>45</b> |
| 7.1. Upravljačke mere za zaštitu bezbednosti WLAN .....      | 45        |
| 7.2. Operativne mere .....                                   | 47        |
| 7.3. Tehničke mere .....                                     | 48        |
| 7.4. Honeypot tehnologija za zaštitu bežične mreže .....     | 50        |
| <b>Zaključak .....</b>                                       | <b>53</b> |
| <b>Literatura .....</b>                                      | <b>56</b> |

## UVOD

U današnje vreme, Informacione tehnologije imaju izuzetno veliki značaj u poslovnim strategijama savremenih kompanija. Zapravo, sve moderne kompanije moraju da koriste informacione sisteme da bi olaksale poslovne procese u organizaciji. Svaki informacioni sistem se pravi da bi odgovorio zahtevu korisnika. Programeri rade na projektu koji vodi do pravljenja informacionog sistema koji treba da udovolji potrebama korisnika. Za svaku kompaniju, veoma često ili gotovo uvek u različito vreme u istoriji poslovanja kompanije dolazi do pravljenja ili kupovanja različitih sistema koji su veoma često razvijani različitim tehnologijama s obzirom na stalni napredak i razvoj informacionih tehnologija. Stoga, glavni razlog postojanja različitih informacionih sistema koji su realizovani različitim tehnologijama je:

1. Razlicite veštine: Programeri različitih tehničkih sposobnosti i profila su razvili različite sisteme. Neki od ovih sistema su mogli biti nadograđeni na postojeće sisteme, ali posto su novi programeri imali različite tehničke sposobnosti, odlučili su se pre za pravljenje novog sistema u njima poznatom okruženju i tehnologiji.

2. Promena tehnoloških trendova: Tehnologija se menja i usavršava vremenom. Logično je i razumno koristiti nove, naprednije tehnologije, usavršavati postojeće Informacione sisteme novim tehnologijama. S druge strane, ovo može prouzrokovati nekonzistentost tehnologija u okviru jedne organizacije.

3. Neophodnost softvera za neke aplikacije: Ovo se odnosi na softver koji nije razvijen u okviru same kompanije. Na primer, moguće je da svaki od ovih softvera koristi različite baze podataka.

Virtuelna privatna mreža (*Virtual Private Network* – VPN) je privatna komunikaciona mreža koja se koristi za komunikaciju u okviru javne mreže. Transport VPN paketa podataka odvija se preko javne mreže (npr. Internet) korišćenjem standardnih komunikacionih protokola. VPN omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju.

Virtuelna privatna mreža omogućava korisnicima da razmenjuju podatke vezom koja je emulirana kao direktna veza (point-to-point link - PPP) između klijenta i servera. PPP emulacija dobija se enkapsulacijom podataka zaglavljem koje omogućava rutiranje kroz javnu mrežu do

odredišta koje je deo privatne mreže. Podaci su šifrovani i paketi koji su presretnuti u okviru javne ili deljene mreže ne mogu se pročitati bez ključa za dešifrovanje. Infrastruktura javne mreže je nebitna jer korisnik logički vidi samo svoj privatni link, odnosno nalazi se logički u lokalnoj mreži, iako je od drugih korisnika razdvojen javnom mrežom.

VPN po formi i funkcionalnosti predstavlja WAN mrežu. Glavna razlika je što se VPN uspostavlja kroz javnu telekomunikacionu infrastrukturu (Internet), umesto korištenja iznajmljenih veza (leased lines). Zaštita i privatnost podataka se ostvaruje korištenjem tuneliranja i šifrovanja saobraćaja, kao i sigurnosnim procedurama koje garantuju sigurnost vaših podataka za vreme njihovog prenosa putem Interneta.

XXI vek je doneo nove poglede u mrežnim komunikacijama. Kompanije koje su nekada razvijale svoje komunikacione zahteve se udružuju sa servis provajderima koji im mogu omogućiti da naprave, razviju i održavaju njihovu mrežu na globalnom nivou. Ovo otvara mogućnost za neprekidni rast, povećan profit i najveća dostignuća za obe strane, provajdere i korisnike. Danas, servis provajderi sve više i više upućuju poslovne korisnike na upotrebu VPN mreža za razliku od prošlosti kada su išli na opciju iznajmljenih linija i frame-relay-a.

## **1. Pojam informacionog sistema**

### **1.1. Sistem**

Sistem je funkcionalni skup objekata i njihovih veza. Svaki od objekata u sistemu poseduje niz svojstava (atributa). Takođe i veze između pojedinih objekata (elemenata) sistema se mogu opisati nizom atributa. Sistem inter reaguje sa okolinom. Uticaj okoline na sistem naziva se ulazom dok se uticaj sistema na okolinu naziva izlazom. Takođe, sistem može da intereaguje sa drugim sistemima. Veze sistema sa okolinom se može ostvariti razmenom materije, energije i informacija. Način na koji su elementi sistema povezani određuje strukturu sistema. Struktura sistema direktno određuje funkcionisanje sistema.<sup>1</sup>

---

<sup>1</sup>Stojaković S. Č.; Building Secure Information Systems,dissertation.Prague. 2000.

Sistemi se dele na osnovu razlicitih kriterijuma na:

- |                              |                                    |
|------------------------------|------------------------------------|
| Po načinu kreiranja:         | - prirodne<br>- veštačke           |
| Po stepenu apstrakcije:      | - apstraktni<br>- realni           |
| Po promenljivosti u vremenu: | - statički<br>- dinamički          |
| Po određenosti ponašanja:    | - deterministički<br>- stohastički |
| Po složenosti:               | - prosti<br>- složeni              |
| Po povezanosti sa okolinom:  | - otvoreni<br>- zatvoreni          |

## **1.2. Podatak i informacija**

Podatak je kodirana predstava neke osobine, nekog koncepta, objekta, činjenice ili događaja u realnom sistemu.

Informacija je protumačeni podatak odnosno znanje koje se može "izvući" iz podatka. Podatak i informacija se koriste kao sinonimi. Podatak je međutim objektivna kategorija dok je informacija subjektivna kategorija odnosno zavisi od načina na koji neki pojedinac tumači ili koristi predstavljeni podatak.

Podaci se mogu reprezentovati na kompjuterski prihvatljiv način, odnosno mogu se kvantifikovati brojevima, karakteristikama, datumima itd. Međutim, interesantan je proces obrade podataka koji mogu da dovedu do kreiranja drugih podataka ili do određene akcije.

## **1.3. Bezbedna informacija**

Osnovni servisi bezbednosti su poverljivost, integritet i dostupnost informacije. Poverljivost (engl. confidentiality) je jedan od glavnih motiva za uvođenje kriptografskih sistema. Ona znači kontrolu objavljivanja informacija i zaštitu od neovlašćenog pristupa informacijama. Da bi opravdali svoju upotrebu kriptografski sistemi moraju biti efikasni u obezbeđenju poverljivosti podataka.

Ta efikasnost se naziva snaga: jak kriptografski sistem je teško „razbiti“. Umesto snage, često se koristi pojam radnog faktora (work factor) algoritma: on približno određuje vreme koje je neophodno za „razbijanje“ nekog kriptografskog sistema. Smatra se da je kriptografski sistem slab ako dozvoljava upotrebu slabih ključeva, ako poseduje propuste u dizajnu ili ako se može lako dešifrovati. Veliki broj današnjih sistema je dovoljno snažan za poslovnu i ličnu upotrebu, ali je nedovoljno jak za osetljive vojne i vladine aplikacije.

Utvrdjivanje postojanja eventualnih izmena poruke tokom prenosa predstavlja drugi osnovni zadatak kriptografskih sistema. Integritet podataka se obezbeđuje dodavanjem zasebnih podataka u vidu kontrolne sume ili drugih redundantnih podataka koji će biti iskorišćeni u procesu dešifrovanja. Dodavanjem koda za autentičnost poruke (engl. Message Authentication Code - MAC) predstavlja uobičajeni način za proveru njenog integriteta. MAC se dobija na osnovu sadržaja same poruke i ključa. MAC se obično šifrjuje sa samom porukom, i tako šalje, čime se dodaje još jedan sloj provere integriteta. Prijemna strana takođe na identičan način proračunava MAC vrednost i poredi svoj rezultat sa vrednošću koja je poslata uz poruku. Integritet je obezbeđen ukoliko su te dve vrednosti iste.

MAC vrednost je neka vrsta ključa koja se dobija pomoću heš algoritma, SHA, MD5 ili slično. Ključ je obično simetričan, pa se isti proces odvija na oba kraja veze primenom identične funkcije.

Kontrola pristupa (engl. access control) označava metode, procese i mehanizme za sprečavanje neovlašćenih pristupa kriptografskim sistemima. Kriptografski ključevi su osetljivi na krađu, gubitke i ljudske propuste. Kontrola pristupa mora regulisati i fizičke i operativne mere zaštite resursa. Kada je pretnja po bezbednost informacija ostvarena, kažemo da se desio incident. Incident se definiše kao akcija koja verovatno dovodi do ozbiljnih posledica. Jezikom IT to je bilo šta što se dogodi sa informacijama, a da nije poželjno. Prema ranije usvojenom značenju incident bi mogao biti napad u opsegu od relativno bezazlenih pokušaja, kao što je probijanje passworda, neautorizovanih pokušaja prijavljivanja na sistem sa udaljenog mesta, do mnogo ozbiljnijih napada kakvi su kreiranje, ubacivanje virusa ili napada tipa ometanja servisa, itd.

Svaki incident je u stvari kršenje Aksioma 2, koji pretpostavlja zaštitu informacija. Kada se incident dogodi, tada je prekinuta veza između izvora informacije S i observera O i umetnuta je neautorizovana izmena informacije.

Tada se dešavaju dvamoguća slučaja:

- DoS (engl. Denial of Service), gde je veza sa izvorom informacije potpuno prekinuta ili je informacija uništena i observer ne prima nikakve informacije od izvora.
- Neautorizovana modifikacija, je kada observer prima informacije koje su, bez saglasnosti, modifikovane u prenosu od izvora informacije do observera
- Aksiom 2, koji govori o tome da informacija ne može biti uništena u procesu observacije niti je procesu observacije dozvoljeno da kreira nove informacije, je najvažniji aksiom što se tiče bezbednosti informacija. Poverljivost, integritet i dostupnost informacija, koje karakterišu bezbednu informaciju, mogu biti sačuvane samo ako se Aksiom 2 striktno poštuje tokom čitavog procesa observacije.
- Aksiom 3, kojim se opisuje redukovani proces observacije, nije toliko važan za bezbednost informacija.
- Aksiom 4, koji objašnjava kako se neodređenost informacije može izmeriti Šenonovom entropijom, je takođe važan za bezbednost informacija, zato što daje formalni alat za merenje neodređenosti informacije preko jednakosti koje opisuju proces observacije.

Postoji još jedan aksiom koji se može dodati već navedenim.

- Aksiom 5, koji kaže da ako neovlašćena modifikacija informacije nastane, tada observer mora biti sposoban da uoči (i eventualno koriguje) neželjenu modifikaciju.

Posledice Aksioma 5 su sledeće:<sup>2</sup>

- observer mora biti u mogućnosti da uoči razliku između  $H(\beta^*)$ ,  $H(b^*)$  i  $H(\alpha^*)$ ,  $H(a^*)$ , respektivno
- observer mora uočiti razliku između parametra observacije  $\omega$  i  $\theta$ , i (ako je moguće) korigovati pogrešan parametar tako da se postigne minimalna razlika, da bude  $\omega = \theta$
- observer treba da ima neka prethodna znanja o očekivanim rezultatima observacije da bi bio sposoban da uoči razliku između korektne i nekorektne informacije.

---

<sup>2</sup> Simić N, Marić N, DoS Napadi na IEEE 802.11 Radio sisteme. Telfor, Beograd. 2004.

#### **1.4. Proučavanje informacionog sistema**

Informacioni sistemi se proučavaju na različitom nivou na velikom broju škola i fakulteta. Na tehničkim fakultetima informacioni sistemi se obično proučavaju iz ugla projektanta, programera, održavanja, računarske povezanosti, projektantna baza podataka. Na fakultetima društvenih nauka obično se proučavanje informacionih sistema sagledava sa stanovišta podrške poslovnim procesima. Na zapadu postoje posebni fakulteti na kojima se izučavaju informacioni sistemi.

#### **1.5. Tipovi informacionih sistema**

- Upravljački informacioni sistem - UIS (Management Information Systems - MIS) je sistem koji prenosi čuva i obrađuje podatke potrebne za upravljanje.
- Sistem za podršku odlučivanju (Decision Support Systems) je informacioni sistem koji potpomaže donošenje odluka.

Po načinu primjene informacione sisteme možemo grubo podeliti na one koji vrše samo skladištenje i pronalaženje informacija i one koji vrše obradu. Mi ćemo razmatrati sistem koji sa svojim podsistemima može da realizuje obe ove operacije.

#### **1.6. Informacioni sistem - realni sistem**

Mi u principu nećemo sagledavati originalni sistem već ćemo polaziti od modela informacionog sistema. U praksi se međutim originalni sistem prvo mora modelovati. Sredstava za modeliranje sistema ima više. Samu suštinu informacionog sistema predstavlja baza podataka (ili sistem baza podataka) koja sadrži međusobno povezane podatke kojima se modeluju objekti, veze između objekata (entiteta) kao i odgovarajući atributi (obilježja - osobine) objekata i veza.

Pored podataka informacioni sistem mora da sadrži podatke o procesima (ili model procesa). Pod procesima se podrazumjevaju radnje koje generišu promene stanja u informacionom sistemu i koje generišu izlaze iz sistema. Pored toga često se vrši i modelovanje resursa sistema.

### **1.7. Razvoj informacionog sistema**

Projekat informacioni sistem po pravilu realizuje tim stručnjaka koji nisu sastavni deo organizacije u kojoj se implementira. Naravno, očekuje se visok stepen saradnje organizacije i projektanata. Da bi se obavio uspešan razvoj informacioni sistem neophodno je:

- obezbediti podršku rukovodstva firme;
- uključiti korisnike u sve faze razvoja;
- koristiti dokazane metodologije razvoja informacionog sistema;
- jasno definisanje ciljeva i zadataka sistema;
- usredsrediti se na najvažnije probleme i eventualne povoljnosti;
- jednostavan i adekvatan dizajn;
- dobar program obuke uključenih osoba;
- adekvatan plan uvođenja nakon završetka projekta;
- dobro definisan i organizovan program održavanja.

### **1.8. Faze u razvoju informacionog sistema**

- Planiranje razvoja;
- Analiza i dizajn;
- Implementacija;
- Funkcionisanje i održavanje;
- Vrednovanje i kontrola.

Svaka od pomenutih faza se mora odraditi. Faze se mogu deliti na podfaze ili aktivnosti.

### **1.9. Planiranje razvoja informacionog sistema**

Ova faza je dio strateškog planiranja jedne organizacije. Aktivnosti u okviru ove faze su:

**1. Identifikacija i definisanje problema.** Potreba za kreiranjem novog informacionog sistema potiču iz sledećih razloga:

- Problemi sa postojećim informacionim sistemom;
- Želja za iskorišćavanjem novih šansi i pogodnosti;
- Rastuća konkurencija;

- Potreba za efikasnijim korišćenjem informacija;
- Reorganizacija u organizaciji (spajanje, razdvajanje, i slično);
- Razvoj same organizacije;
- Promene na tržištu i okruženju.

**2. Analiza postojećeg informacionog sistema.** Treba sagledati stanje hardvera, sistemskog i aplikativnog softvera, informatičkih kadrova, troškova funkcionisanja; iskorišćenosti postojećih resursa, te na kraju treba proceniti kvalitet, pravovremenost, primerenost količine, načina prezentacije samih informacija koje postojeći sistem pruža.

**3. Treba se odlučiti na uvođenje potpuno novog ili modifikovanog informacionog sistema.** Da bi se ovo postiglo treba uporediti koje će se funkcije iz postojećeg sistema zadržati, koje će biti modifikovane a koje će biti uvedene. Treba zatim razmotriti organizaciju podataka i klasa podataka, baza podataka itd. Na osnovu razlika između projektovanog i trenutnog informacionog sistema donosi se odluka o tipu promena u informacionom sistemu.

**4. Projektovanje logičke strukture baze podataka.** Ovaj deo se realizuje na nivou entiteta (objekata) i veza među njima (ERWIN).

**5. Definisanje koncepcije tehničke podrške.** Na osnovu ciljeva koji se žele postići informacionim sistemom, veličine organizacije itd., donosi se odluka o obimu i strukturi računarskih resursa, komunikacione i periferijske opreme, sistemskog softvera, itd. Kod hardvera treba obezbediti:

- visoku integraciju;
- modularnu izgradnju (hardverski sistem bi trebao da zaživi na relativno malom procentu nominalne opreme i da se naknadnim ugradnjama samo postižu poboljšavanja i proširivanja primene);
- visoka pouzdanost, sigurnost i raspoloživost (na kritičnim mestima treba predvideti dupliranje kapaciteta);
- lako održavanje.

Sistemske softver treba da obezbedi:

- Modularnost;
- User friendly okruženje;
- podrška drugim programskim alatima;
- efikasno korišćenje postojeće opreme;
- jednostavno održavanje.

**6. Definisanje modela kadrovske podrške.** Ovo se odnosi na način kako su organizovani delovi i pojedinci u organizaciji kojima je povereno vođenje poslova u domenu informacionog sistema.

**7. Specifikacija potrebnih ulaganja.** Ova stavka obuhvata procenu ulaganja u sledeće elemente informacionog sistema:

- hardver;
- sistemski softver, softver za rad sa bazama podataka;
- softver za automatizaciju kancelarijskog poslovanja;
- razvoj i obuku informatičkih kadrova.

**8. Analiza izvodljivosti projekta.** Kada se ovo analizira treba voditi računa o sledećem:

- Tehnička izvodljivost (obezbeđivanje hardvera i softvera);
- Ekonomski (da li se mogu obezbediti sredstva i da li će dalje poslovanje informacionog sistema biti isplativo);
- Zakonski (da li postoje zakonske smetnje za rad zamišljenog informacionog sistema. Operacionalni (da li će sistem biti prilagođen podršku ljudima koji će ga koristiti);
- Planski (da li se sistem može realizovati na vreme).

**9. Utvrđivanje prioriteta i izbor projektanta.** Informacioni sistem se uvodi na najkritičnijim mestima prvo (mestima koja su vezana za najveći broj radnika, ili za najviše rukovodstvo, ili za najvažnije poslove firme).

**10. Planiranje realizacije projekta.** Ovo je složena faza koja se poverava nekom stručnjaku iz oblasti organizacije rada.

**11. Prihvatanje ili odbijanje plana razvoja.** Ako su prikupljene informacije dovoljne za donošenje odluke treba doneti odluku o razvoju informacionog sistema (pozitivnu ili negativnu, odluka nije pozitivna jer su ulaganja obično značajna), a ako nema dovoljno informacija treba zahtevati prikupljanje dodatnih informacija i činjenica o informacionom sistemu. Trenutna procena da ne treba ići na novi ili modifikovani informacioni sistem ne znači da predloženi plan razvoja nije dobar već samo da ne treba ići u dalji razvoj u ovom trenutku. Takvi projekti se "skladište" i mogu se koristiti možda u narednom periodu.

### **1.10. Analiza i dizajn informacionog sistema**

U ovu se fazu ide kada je plan razvoja informacionog sistema usvojen. Analiza se provodi detaljno na sve automatizovane i neautomatizovane poslove. Osnovno sredstvo koje se danas koristi za analizu informacionog sistema je sistemska strukturirana analiza kojoj će biti posvećeni naredni časovi.

Dizajn sistema je specifikacija novog sistema koji će postavljene zahtjeve obaviti na efikasan način.

Kod dizajna sistema postoje dve važne faze:

- logičko projektovanje;
- fizičko projektovanje.

Logičko projektovanje obuhvata modeliranje podataka i modeliranje procesa. Rezultat logičkog projektovanja mora biti razumljiv za korisnika i projektanta i treba da bude nezavisan od implementacije.

Fizičko projektovanje je prevođenje logičkog projekta na konkretnu opremu, konkretne softvere koji uključuju konkretne baze podataka.

Faze analize i dizajna su karakteristične po bogatoj dokumentaciji koja ih prati. Težnja je da se danas razviju sistemi koji će na osnovu projekta odrađenog u nekom programskom paketu vršiti automatsko vođenje dokumentacije.

## **2. Integracija Heterogenih Informacionih Sistema**

### **2.1. Integracija podataka**

U uslovima ubrzanog razvoja informacionih sistema, sve više se javlja potreba za sistemima koji funkcionišu u uslovima heterogenog okruženja. Zbog ovakve situacije dolazi do potrebe za naučnim istraživanjima usmerenim ka načinima integracije raznorodnih komponenata heterogenih informacionih sistema. Kompanije savremenog poslovanja imaju veliki broj poslovnih procesa, odgovarajućih službi koji ih realizuju, ali i odgovarajućih informacionih sistema koji pokrivaju pojedine procese. Ove kompanije rade dugi niz godina, i u svojim službama koriste informacione sisteme koje su razvijali sami, ili ih nabavili na tržištu. Ovi informacioni sistemi sadrže veliku količinu informacija, a svaki od sistema je razvijan ili nabavljan nezavisno. Zbog toga su takvi sistemi često heterogeni u pogledu metodologije projektovanja, operativnog sistema, platforme koja je korišćena za razvoj, sistemu za upravljanje bazama podataka pa čak u formatu zapisa podataka.

Problemi nastaju kada se pojavi potreba za integracijom poslovnih procesa (business process integration - BPI), koji su sami već podržani zaokruženim informacionim sistemima. BPI zahteva kompleksnu informatičku podršku, s obzirom da se radi o automatizovanoj razmeni podataka između autonomnih informacionih sistema. Zato je potrebno odabrati pravi pristup za integraciju informacionih sistema.

Sposobnost kompanija (tj. njihovih aplikacija) da se adaptiraju u heterogenom okruženju, u kome su promene česte, je od ključne važnosti da se opstane na tržištu.

Jedno od rešenja za podršku Integracije Heterogenih Informacionih sistema je potpuna integracija, koja zahteva reinžinjerung svih sistema i implementaciju potpuno novog, unapred integrisanog sistema. Očigledno je da je ovakvo rešenje najskuplje, ali ne mora biti i najbolje. Postojeći informacioni sistemi se obično koriste dugi niz godina, implementiraju poslovne procese u kompaniji i sadrže veliku količinu podataka.

Zamena ovakvih sistema podrazumeva vremenski dug proces koji zahteva postupno preuzimanja podataka, paralelni rad starog i novog sistema, obuku i školovanje kadrova, obično zahteva nabavku nove opreme i sl.

Ipak, najskuplje je to što sveobuhvatni informacioni sistem, posle nekog vremena, počinje da guši poslovne procese koje automatizuje, jer počiva na definisanim zahtevima koji su bili aktuelni u momentu projektovanja.

Sa druge strane, jaka (ali nepotpuna) integracija može kasnije rezultirati previše rigidnim sistemom, koji je teško promeniti. Na primer, ako hronološki posmatramo, posle uspešne automatizacije nekih procesa pomoću jednog softvera, kreće se u automatizaciju drugih procesa pomoću drugog softvera. Zatim se javlja potreba za integracijom informacija koje se nalaze u ova dva softvera. Posle uspešne integracije, može se dobiti spregnuti sistem, u kojem se promena bilo kog procesa se odražava na oba softvera. Kako su dobavljači softvera često različite kompanije, problem promena i usklađivanja softvera postaje ozbiljan.

Slaba integracija može rezultirati nekvalitetnim sistemom, koji nije u stanju da pruži tražene informacije. Na primer, ukoliko se za prethodni slučaj odabere data warehousing pristup, kasnije je teško realizovati povratnu spregu, jer se radi sa zastarelim informacijama.

Poslednji vid integracije koja će se razmazrati je Real Time Integracija sa predhodnom Migracijom podataka. Naime, moguće je zadržati sve pogodnosti pojedinih sistema ali s obzirom da su pojedini sistemi zaduženi za pojedine segmente poslovnog procesa želi se i dalje nastaviti sa tom praksom sa dodatkom da su pojedini sistemi svesni podataka u drugim zavisnim sistemima. Drugim rečima, neophodno je deljenje podataka medju sistemima u Real Time maniru. Ovo se postiže različitim tehnologijama a sve se zasnivaju na transakcijama koje su inicijalizovane pri nekom događaju na jednom od integrisanih sistema (Event Based Transactions).

### **2.2.Ciljevi**

Proces odabira pristupa za integraciju informacionih sistema zahteva nekoliko koraka. Treba uraditi analizu postojećih tehnologija za integraciju informacija, i upoznati njihove mogućnosti i ograničenja. Potom je potrebna analiza postojećih tehnologija za integraciju informacionih sistema. Ove tehnologije omogućavaju različite nivoe integracije, i imaju direktan uticaj na informacione sisteme koje integrišu, a samim tim i poslovne procese. Na kraju je potrebna analiza implementiranih informacionih sistema, naročito stepena njihove heterogenosti.

U svetlu ovih analiza je potrebno sagledati ciljeve željene integracije informacionih sistema, i odrediti način rešenja problema.

Rešenje problema (pristup integraciji) treba biti kvalitetno dokumentovan, u smislu ograničenja koja ovakav integrisani sistem nameće. Ograničenja proističu iz primenjenog rešenja, odnosno nivoa interoperabilnosti.

Istraživanja pokazuju da standardizacija kod realizacije interoperabilnosti ne predstavlja prihvatljivo rešenje. Rešenje mora biti skalabilno i otvoreno, fer za sve potencijalne učesnike u komunikacijama, tako da bilo koja služba kompanije bez obzira na veličinu i vrstu poslovanja može participirati. To znači da mora da se definiše jedan zajednički okvir jednostavan za implementaciju sastavljen od otvorenih komponenti koji će obezbediti ad-hoc interoperabilnost aplikacija na svim nivoima (mreža, podaci, poslovni procesi) bez potrebe za ljudskom intervencijom.

Ovaj diplomski rad se odnosi na:

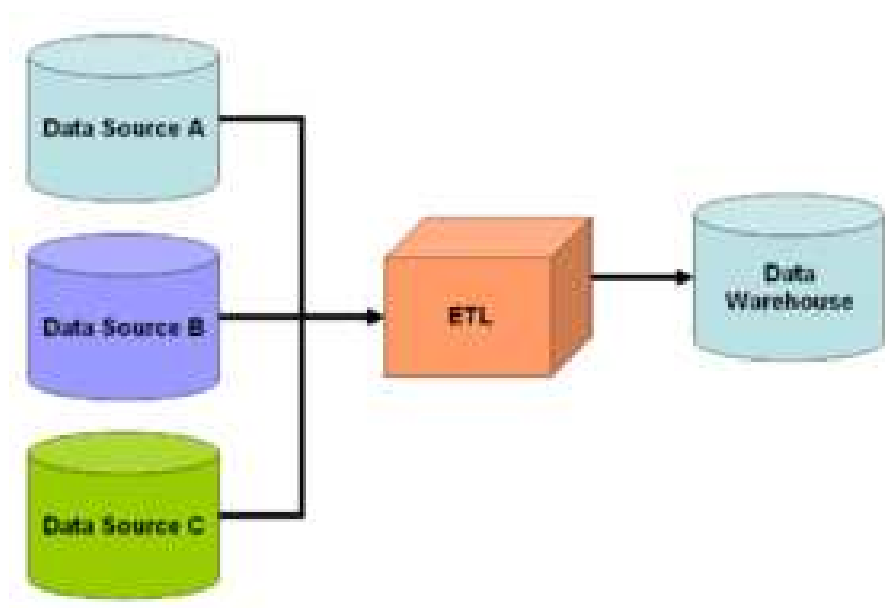
- Metodologiju i alate za realizaciju integracije Heterogenih informacionih sistema unutar kompanije.
- Rad treba da da pregled standardnih savremenih tehnologija za integraciju Heterogenih informacionih sistema kao i detaljan pregled Real Time tehnologija, SOA tehnologije na prvom mestu.
- Takođe biće izložene prednosti i mane pojedinih tehnologija kao i uporedni prikaze analiziranih rešenja.
- Na kraju će biti izvedeni zaključci o gore pomenutim tehnologijama i razmatranjima.

### **2.3. Istorija problema**

Problem Integracije Heterogenih Informacionih sistema postoji već dugo vremena. Ubrzano prihvatanje baza podataka posle 1960. godine, prirodno je vodio do potrebe da se dele ili sinhronizuju postojeće riznice podataka. Sinhronizovanje može biti urađeno na nekoliko različitih nivoa arhitekture baze podataka.

Ovde su podaci iz nekoliko različitih izvora su pročitani, transformisani i učitani novu bazu kojoj može biti pristupano kroz jedinstvenu konekciju. Sa arhitekturne tačke gledišta, ovo može biti posmatrano kao potpuna integracija jer se podaci nalaze u jedinstvenoj bazi u vreme

korišćenja. Problem koji se javlja sa ovim načinom je svežina podataka, na primer kada se jedna od originalnih baza promeni, nova jedinstvena baza ima stare podatke i tada je potrebno pokrenuti proces stapanja podataka ponovo. Takođe, nije lako napraviti Jedinstvenu riznicu u slučajevima kada imate samo pristup podacima ali ne i potpunu kontrolu nad njima u svim sistemima koji treba da budu objedinjeni, sto je u praksi zapravo veoma čest slučaj zbog problema bezbednosti podataka i politike pojedinih organizacija.

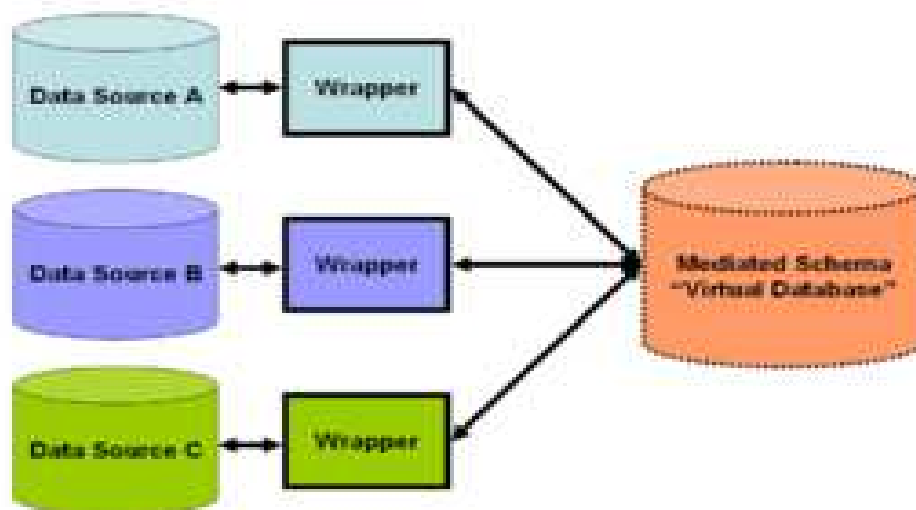


*Slika 1. - Uskladištenje Podatka*

Novi trend u Integraciji Heterogenih Informacionih sistema je da olabavi sjedinjene sistema. Ovde je idea da se omogući jedinstven pristup podacima koji se i dalje nalaze na različitim bazama (slika 2). Ovaj jedinstveni pristup je nakon inicijalizacije transformisan u pristupe različitim originalnim bazama koje zaista fizički drže podatke. Ovaj process može takođe biti pozivan kao na pogledu baziran upit (view based query), zato što je često moguće da svaka od ovih baza bude dostupna preko istog Pogleda.

Formalno, ovakav pristup se naziva Lokalni kao Pogled (Local As View – LAV) gde se Lokalni odnosi na lokalnu bazu. Alternativni model Integracije je i onaj gde je objedinjena šema napravljena da bude pogled preko izvorne (originalne) šeme. Ovaj pristup se naziva Globalni Kao Pogled (Global As View – GAV) gde se Globalni sada odnosi na globalnu, objedinjenu

šemu i često se koristi zbog jednostavnosti odgovora na zahteve za podacima preko globalne šeme. U svakom slučaju, očigledan nedostatak je potreba da ponovo napišu Pogledi za globalnu šemu svaki put kada se neka od originalnih Izvor šema promeni.



*Slika 2. - Integraciji Heterogenih Informacionih sistema*

Neki od postojećih radova na istraživanju Integracije podataka se odnose na Značenjski Integracioni problem (Semantic Integration problem). Ovaj problem nije o tome kako napraviti arhitekturu integracije, nego kako razrešiti značenjski konflikt između heterogenih izvora podataka.

Na primer ako dve kompanije, sinhronizuju svoje baze podataka, određeni koncepti i definicije u njihovim šemama kao 'Zarade' neizbežno imaju različito značenje. U jednoj bazi to može značiti profit u eurima recimo (decimalni broj), dok u drugoj bazi može značiti broj prodaja (koji je celobrojni tip). Uobičajena strategija za razrešenje takvog problema je da se koriste ontologije koje eksplicitno definišu termine šema kako bi se razrešili Semantički konflikti. Ovaj pristup je takodje poznat pod nazivom Ontologijski zasnovana Integracija Podataka (Ontology based data integration).

## **2.4.Real Time Integracija**

Za razliku od Integracije Heterogenih Informacionih sistema ili podataka na heterogenim bazama, Real Time Integracija se oslanja na deljenje podataka u vremenu unosa podataka. Naime, zbog složenosti poslovnih procesa u modernom poslovanju javlja se potreba za postojanjem više informacionih sistema koji vode računa o jednom ili grupi srodnih poslovnih procesa. Real Time integracija omogućava da ti informacioni sistemi budu svesni podataka u drugim integrisanim sistemima i u svakom datom trenutku potpuno sinhronizovani. Ovo podrazumeva da promena podatka u jednom od Integrisanih sistema automatski šalje informaciju drugim informacionim sistemima o toj promeni. Ova transakcija je bazirana na nekom događaju u samom Informacionom sistemu (event based), na primer na sačuvavanju promenjenog rekorda.

Vazno napomenuti za Real Time integraciju je da pre početka korištenja treba dovesti Integrisane Heterogene Informacione sisteme u sinhronizovano stanje. Ovo se postiže prethodnom migracijom podataka. S obzirom da je sama migracija podataka dosta široka tema, ona neće biti razmatrana u ovom radu ali će se podrazumevati da je ovaj uslov ispunjen pre početka implementacije Real Time Integracionih tehnologija.

U prošlosti su se za ovo koristile tehnologije kao što su Database Stored procedures i Functions koje su bivale inicijalizovane događajima osluškivanjem od strane trigeru ili vremenski inicijalizovane Cron Task aktivnošću. Ovo je bilo korisno u to vreme, međutim jedan od velikih problema je bilo Logovanje i tretiranje Error situacija. Drugim rečima, stare tehnologije za Real Time Integraciju su imale problem nedovoljne kontrole same Transakcije od strane Tehničkog Lica. Procedure i Trigeri su u novije vreme zamenile nove tehnologije koje pružaju bolju i lakšu kontrolu ove sinhronizacije podataka. Među najperspektivnijim su Servisno Orijentisane Arhitekture (SOA) koje se zasnivaju na slanju poruka između sistema posredstvom servisa. Postoje različiti formati i protokoli ovih poruka ali XML format je najzastupljeniji iz praktičnih razloga. Dalje izlaganje biće posvećeno Service Oriented Architecture tehnologiji.

### **2.4.1.XML Web Servisi**

Najrasprostranjeniji, najprihvaćeniji i najuspešniji tip servisa je XML Web Servis. (nadalje će se nazivati samo Web Servis ili jednostavno servis).

Ovaj tip servisa ima dva fundamentalna zahteva:

- Komunicira preko Internet protokola (najčešće preko HTTP)
- Šalje i prima podatke formatirane u vidu XML Dokumenta

Ovo je i osnovna karakteristika. Moguće je napisati jednostavan ASP ili JSP skript koji radi na Web Serveru šaljući i primajući XML formatirane poruke preko HTTP-a i najveći deo posla je već završen.

Šira prihvaćenost Web Servis dizajna je rezultirala brzom razvoju pratećih tehnologija koje su uistinu postale standard. Stoga je od industrijski standardnog Web Servisa generalno za očekivati:

- Da obezbedi servisni opis koji je, u najmanju ruku, u skladu sa WSDL dokumentom
- Da bude u mogućnosti da transportuje XML dokumente koristeći SOAPpreko HTTP-a

Ove tehnologije ne menjaju suštinsku funkcionalnost Web Servisa dokle god uspevaju da zadrže sposobnost da komuniciraju na standardan način. Mnoge od arhitektonskih konvencija iznetih u ovom poglavlju podrazumevaju da su SOAP i WSDL delovi opisanog radnog okruženja Web Servisa.

Dodatno je uobičajeno za Web servise da:

- Budu u stanju da se ponašaju kao requestor i provider servis
- Budu registrovani kroz pratećeg agenta tako da mogu biti locirani

U tipičnoj konverzaciji sa Web Servisom, klijent koji inicira zahtev je Web Servis takođe. Kao što je pokazano na slici 3., svaki intefejs koji je izložen preko Klijent Servisa se takođe kvalifikuje kao servis preko kog drugi servisi mogu zahtevati informacije. Stoga, Web Servisi se ne uklapaju u standardni Klijent-Server model.

Umesto toga, oni nastoje da uspostave peer-to-peer sistem, gde svaki servis može igrati ulogu klijenta ili servera i te uloge se zamenjuju u toku komunikacije.

### **2.4.2. Service Oriented Architecture (SOA)**

SOA obezbeđuje metode za razvoj i integraciju Heterogenih Informacionih sistema gde sistemi grupišu funkcionalnost vezanu za poslovne procese i pakuju ih kao interoperabilne servise. SOA infrastruktura dozvoljava različitim aplikacijama da razmene podatke između sebe dok učestvuju u poslovnom procesu. Servisna orijentacija cilja na slabo povezivanje servisa sa operativnim sistemom, programskim jezicima i drugim tehnologijama koje nose aplikaciju. SOA odvaja funkcije u različite jedinice, ili servise, koje developeri učine dostupnim preko mreže kako bi ih korisnici mogli kombinovati i ponovo upotrebljavati u procesu korišćenja poslovnih aplikacija. Ovi servisi komuniciraju jedni sa drugima tako što šalju informacije od servisa do servisa, ili koordinirajući aktivnosti između dva ili više servisa. Mnogi komentatori, vide SOA koncept kao izgrađen na i proizašao iz starih koncepta distribuiranog i modularnog programiranja.

Service Oriented Architecture (SOA) bi se mogla definisati kao grupa servisa koji komuniciraju međusobno. Ovo komuniciranje obuhvata jednostavno slanje podataka ili koordinisano obavljanje iste aktivnosti od strane više servisa.

SOA ima za cilj da omogući korisnicima povezivanje velikih delova funkcionalnosti u formu ad hoc aplikacije koja je izgrađena skoro u potpunosti od postojećih servisa. Što su veći ti delovi funkcionalnosti, to je manje Interface Point-a potrebno da bi se implementio dati set funkcionalnosti. Svaki Interface nosi sa sobom određeno količinu procesiranja, tako da postoji potreba i za razmatranjem performansi pri odabiru granularnosti servisa. Veoma značajno obećanje SOA je da marginalni trošak pravljenja n-te aplikacije je nula, budući da softver potreban za izradu aplikacije već postoji. U idealnom slučaju, potrebno je samo izvršiti orkestrizaciju da bi se napravila nova aplikacija.

Od 2008., povećan broj third-party softverskih kompanija nudi softverske servise na tržištu. U budućnosti, SOA sistemi će se možda sastojati od takvih third-party servisa kombinovanim sa drugim unutar kompanije napravljenim. Ovo potencijalno može dovesti do povećanja standardizacije u Informacionoj Tehnologiji.

### **3. VPN – Virtuelna privatna mreža**

#### **3.1. Pojam, prednosti i nedostaci VPN**

Virtualna privatna mreža engleski *Virtual Private Networking* (VPN), obezbeđuje mehanizme za bezbednu komunikaciju i prenos podataka i drugih informacija kroz javnu mrežu kao što je Internet, a takođe predstavlja i jeftinu alternativu za iznajmljene telekomunikacione linije između kompanija i njihovih udaljenih organizacionih jedinica. Pored velikog broja pogodnosti koje pruža, VPN omogućava zaposlenima da mogu sa bilo koje tačke na svetu da bezbedno pristupaju podacima na kompanijskim serverima na isti način kao što to čine iz svoje kancelarije.

Treba napomenuti da VPN ne može da ukloni sve rizike koji postoje na mreži, ali znatno može da ih smanji naročito u komunikaciji koja se odvija preko javne mreže. Jedan od mogućih problema je i komplikovana implementacija što se naročito odnosi na tradicionalno rešenje zasnovano na IPsec protokolu. Znatno jednostavnije rešenje je implementacija preko SSL VPN-a, novog načina na koji se konfigurišu virtualne privatne mreže. U osnovi ove vrste VPN-a je SSL protokol čija je najveća prednost u tome što obezbeđuje korisnicima da koristeći samo Web pretraživač, bez dodatnih komponenti instaliranih na klijentskoj strani kao što to zahteva IPsec protokol, mogu nesmetano da pristupaju mrežnim servisima.<sup>3</sup>

Tradicionalne privatne mreže podrazumevaju da su njihove performanse korisnicima unapred određene i poznate, a pošto se o njihovom održavanju staraju sami korisnici, to automatski znači i jedno predvidljivo ponašanje.

Nagli porast zainteresovanosti za virtuelne privatne mreže povezan je sa razlozima ekonomske prirode. Naime, u današnje vreme velike korporacije i organizacije (glavni vlasnici privatnih mreža) se sastoje od mnoštva geografski udaljenih delova. Uspostavljanje tradicionalne WAN mreže (*Wide Area Network*) u ovom slučaju bi ekonomski bilo vrlo nepovoljno rešenje.

---

<sup>3</sup>Andrew S. Tanenbaum, Computer Networks, Third edition, Prentice-Hall, Inc., 1996.

Plaćanje iznajmljenih linija bi iziskivalo znatna materijalna sredstva, pogotovo u slučaju organizacionih jedinica smeštenih u različitim državama. Troškovi povezani sa potrebom za odgovarajućom opremom i neophodnim angažovanjem odgovarajućeg osoblja, koje bi se staralo o njenom održavanju su još jedna mana. Sledeći nedostatak tradicionalnih privatnih mreža jeste njihova nefleksibilnost. Povezivanje velikog broja zaposlenih, klijenata i partnera na korporacijsku privatnu mrežu (što je naravno i cilj) bi zahtevalo postojanje velikog broja pristupnih tačaka koje bi se još i dinamički menjale, što jednu takvu mrežu čini praktično nemogućom za realizaciju. Usled svega toga je rešenje potraženo u VPN mrežama, koje koristeći javnu infrastrukturu, u današnje vreme omogućavaju praktično globalnu povezanost. Tarifiranje u ovom slučaju se svodi na cenu lokalnog povezivanja sa provajderom koji omogućava pristup javnoj infrastrukturi. Osim toga, formiranje i održavanje VPN mreže se može prepustiti provajderu usluga, što može u finansijskom i tehničkom pogledu relaksirati korisnike.

Prednosti virtuelnih privatnih mreža su:<sup>4</sup>

- Povećanje geografske pokrivenosti,
- Uštede u iznajmljenim linijama,
- Uštede u udaljenim i međunarodnim dial – up povezima,
- Mogućnost brzog dodavanja novih udaljenih korisnika,
- Smanjenje potrebne opreme za remote – access,
- Uštede u ljudstvu.

Postoje i nedostaci virtuelnih privatnih mreža, a to su:

- VPN mreže zahtevaju dobra znanja o *security*-ju (zaštiti podataka), prvenstveno u pogledu hakerskih napada i konfiguracije VPN uređaja za rad u sprezi sa firewall-ovima.
- Mogućnost korišćenja VPN-a (dostupnost i QoS) zavise od faktora van kuće (od kvaliteta usluge koju daje Internet Service Provider ISP) i naročito je izraženo u našim uslovima.
- Ukoliko VPN konekcija simulira rad računara u LAN-u, u zavisnosti od kvaliteta VPN servera i veze sa ISP-om, protok podataka između računara umreženih u VPN-u je osetno sporiji u odnosu na LAN.

---

<sup>4</sup><http://www.wikipedia.org> pregledano dana 05.10.2012.

- Pitanje interoperabilnosti raznih proizvođača. Ovo je izraženo za sve tehnologije u razvoju, a ima veliku ulogu pri izgradnji Extranet VPN-a gde svaki VPN segment (svaki partner, organizacija i sl) ima uređaje kupljene od različitog proizvođača.<sup>5</sup>

### **3.2. Klasifikacija virtuelnih privatnih mreža**

Virtuelne privatne mreže mogu se kategorisati na osnovu dve različite karakteristike – na osnovu nivoa sofisticiranosti i na osnovu bezbednosti. Nivoi sofisticiranosti se razdvajaju na osnovu toga gde je, tj. na kom nivou višeslojne arhitekture računarskih mreža, potrebno realizovati glavni deo poslova. Virtuelne privatne mreže sa mrežnog nivoa zahtevaju da se promene odvijaju u okviru mrežnih servisa samih operativnih sistema. Primeri ovakvih sistema su IPSec, OpenVPN i PPTP. Sa druge strane, virtuelne privatne mreže sa malim konfiguracionim zahtevima, zahtevaju da sam softver obavi sve potrebne aktivnosti i na taj način ostavlja operativni sistem i ostale aplikacije slobodnim. Primeri sistema čiji se rad zasniva na ovakvom principu su Skype i Hamachi.

Druga karakteristika na osnovu koje se virtuelne mreže mogu klasifikovati je bezbednost. Mnogo istaknutiji i značajniji od prethodnog kriterijuma. Virtuelne privatne mreže na osnovu njihove bezbednosti možemo da razdvojimo na poverljive i sigurne. Poverljive virtuelne privatne mreže se oslanjaju na fundamentalnu bezbednost mreže putem koje će saobraćaj biti prenošen; nema dodatnih aktivnosti koje se odvijaju sa ciljem da se zaštiti mrežni saobraćaj. Sa druge strane sigurne virtuelne privatne mreže primenjuju različite tehnike i postupke sa ciljem da štite privatnost podataka koje prenose. Sigurne virtuelne privatne mreže su mnogo opštije zato što se one mogu uspostavljati nad bilo kojim tipom računarskih mreža.<sup>6</sup>

### **3.3. Komponente virtuelnih privatnih mreža**

Da bi VPN postala važna platforma ona treba da bude pouzdana i upravljiva kroz celu mrežu i sigurna od napada. VPN rešenja takođe treba da poseduju Platform Scalability - mogućnost da se mreža adaptira od male kućne konfiguracije do velike biznis implementacije. Najvažnija odluka pre nego što se krene sa implementacijom je da VPN zadovolji sve zahteve korisnika i da bude kompatibilna sa već postojećom mrežom korisnika.

<sup>5</sup><http://www.e-drustvo.org> pregledano dana 05.10.2012.

<sup>6</sup><http://www.corecom.com> pregledano dana 05.10.2012.

Najznačajnije komponente VPN su:<sup>7</sup>

- 1) protokoli,
- 2) firewall,
- 3) bezbednost.

### **3.3.1. Protokoli**

Najvažnija stvar kod VPN-a je da ona mora biti zaštićena od upada raznih neautorizovanih korisnika. Samim tim, postoji više razvijenih tehnologija i protokola koje VPN koristi u većoj ili manjoj meri: Generic Route Encapsulation (GRE) je VPN tehnologija razvijena od strane CISCA i kasnije definisana sa dva IETF RFC-a i to 1701 i 2784. CISCO je razvio GRE kao enkapsulacioni metod da uzme pakete iz jednog protokola, enkapsulira ih u IP paket i transportuje enkapsulirani paket preko IP osnove. GRE se koristio, a i sada se koristi za konektovanje malih delova određenih protokola preko IP baziranih osnova bez dodatnog konfigurisanja tih osnova da bi se pokrenuli dodatni protokoli. GRE, koji je IP protokol trećeg nivoa može enkapsulirati sledeće protokole: AppleTalk, Banyan Vines, Layer2-bridged traffic, CLNP, DECNET, IP, IPX itd.<sup>8</sup>

Osnovni nedostatak GRE-a je nedostatak protekcije. On ne poseduje autentikaciju enkripciju i proveru integriteta paketa. Zbog ovih nedostataka ne koristi se za kompletna VPN rešenja već se u većoj ili manjoj meri koristi sa drugim rešenjima.

### **3.3.2. Firewall**

Firewall prati celokupan saobraćaj kroz mrežu i štiti mrežu od upada neautorizovanih korisnika. Organizacije treba da naprave mrežu koja će imati firewall na svakoj konekciji između njihove mreže i interneta. Dva najčešće korišćena firewall-a su:<sup>9</sup>

1. Filtriranje paketa zavisno o IP adresama odredišta tj. izvorišta - Filtriranje zavisno o IP adresama omogućava zabranu konekcija od ili prema određenim računarima i/ili mrežama, u zavisnosti od njihovih IP adresa.

<sup>7</sup> Krstajić B., Radulović A., Informacione tehnologije, Zbornik radova, Žabljak, 2010.

<sup>8</sup> Veinović M., Jevremović A., Računarske mreže, Univerzitet Singidunum, Beograd, 2011.

<sup>9</sup> Stallings W., Cryptography and Network Security - Principles and Practices, Prentice Hall, New Jersey, November 2005.

Ukoliko administrator želi zaštititi mrežu od neovlašćenih zlonamernih napadača, on može zabraniti promet mrežnih paketa koje kao odredište imaju određene IP adrese. To je poprilično beskorisno jer napadači mogu promeniti IP adrese. Zbog toga je puno bolje dozvoliti pristup mreži samo određenim paketima koji kao odredište imaju određene sigurne IP adrese.

Normalno ukoliko se napadač domogne i tog popisa on može paketima pridružiti kao odredišnu IP adresu neku iz tog popisa. Mana je što ne proverava sadržaj paketa ili zašto je on poslat i resursi koji su onemogućeni su vidljivi svim korisnicima.

2. Filtriranje paketa u zavisnosti od odredišnih tj. izvorišnih portova - Prilikom spajanja jednog računara na drugi i jedan i drugi koriste određene pristupne portove. Sve ukupni broj pristupnih portova je 65536. Prva 1024 porta su rezervirana za određene aplikacije i ne mogu se koristiti za neke druge. Administrator nezavisno od aplikacija može ograničiti pristup mrežnim paketima. Neki aplikacijski protokoli su izrazito osetljivi na mrežne napade pa je potrebno onemogućiti pristup istima (Telnet, NetBIOS Session, POP, NFS, X Window, ...). Ti portovi su osobiti osetljivi na napad zbog velikog nivoa kontrole koju pružaju napadaču. Neki drugi portovi mogu biti iskorišteni da bi se uništile određene bitne informacije. Prednosti ovog tipa firewall-a su kontrola nivoa pristupa korisnika i kontrola nivoa resursa koji se dele. Samo resursi koji su autorizovani su pristupačni. S druge strane korisnici moraju da koriste dodatne passworde da bi pristupili internetu.

#### **4. Bezbednost virtuelnih privatnih mreža**

Bezbednost virtuelnih privatnih mreža se u zavisnosti od arhitekture mreže ostvaruje na različite načine. Na primer, pristup sa udaljenog radnog mesta može zahtevati snažnije mehanizme zaštite tajnosti podataka koji se prenose za razliku od onih koji se koriste u internim mrežama. Razlog za ovako nešto je očigledan. Naime, pristup sa udaljenog radnog mesta se najčešće ostvaruje putem mnogo ranjivije javne mreže koja se nalazi izvan naše privatne mreže. Sa druge strane mrežni nivo omogućava tunelovanje koje obezbeđuje dodatnu sigurnost.

Različite arhitekture povlače za sobom i različite cene, i tako pružaju mogućnost da se implementiraju različiti bezbednosni mehanizmi. Neke od arhitektura koje su ovde prikazane su: arhitektura zasnovana na internim mrežama, arhitektura zasnovana na eksternim mrežama, arhitektura zasnovana na sistemima sa udaljenim pristupom, arhitektura virtuelnih privatnih

mreža na mrežnom nivou OSI referentnog modela, kao i arhitektura virtuelnih privatnih mreža na nivou veze podataka.

#### **4.1. Virtuelne privatne mreže zasnovane na internim mrežama**

Arhitektura virtuelnih privatnih mreža zasnovana na internim mrežama predstavlja oblik „site-to-site“ arhitekture putem koje neka kompanija može međusobno povezati više statičnih lokacija preko Interneta.<sup>10</sup> Ukoliko neka organizacija ima jednu ili više udaljenih lokacija tada ih ona može pripojiti jedinstvenoj privatnoj mreži.<sup>11</sup>

Organizacija može kreirati virtuelnu privatnu mrežu u svojoj internoj mreži kako bi međusobno, na bezbedan način, povezivala lokalne računarske mreže. Različita odeljenja jedne iste kompanije, koja su prostorno odvojena, mogu se međusobno povezati upotrebom ovog servisa. Daleko jeftiniji od iznajmljenih privatnih linija, ovakav servis može međusobno da poveže različita odeljenja u okviru jedne kompanije.

Na primer, male poslovnice se mogu vezati sa glavnom poslovnicom. Glavna poslovnica se može, putem ovakvih servisa, povezati na centralnu upravu kompanije.

#### **4.2. Virtuelne privatne mreže zasnovane na eksternim mrežama**

Slično arhitekturi virtuelnih privatnih mreža zasnovanih na internim mrežama, arhitektura zasnovana na eksternim mrežama predstavlja drugačiju formu „site-to-site“ arhitekture. Ukoliko neka kompanija (organizacija) ima blisku saradnju sa nekom drugom kompanijom, kao što je na primer saradnja kupac – prodavac, one mogu da uspostave jednu arhitekturu virtuelne privatne mreže zasnovanu na eksternoj mreži kojom se lokalna mreža jedne kompanije povezuje sa lokalnom mrežom druge kompanije. Na ovakav način pomenute kompanije su u mogućnosti da sarađuju u jednom kolaborativnom okruženju. Ovakva arhitektura pruža mogućnost spoljašnjim prodavcima, dobavljačima i potencijalnim kupcima da pristupaju lokalnoj mreži kompanije domaćina u za to specifično predviđenoj oblasti koja je poznata pod nazivom demilitarizovana

<sup>10</sup>Tyson J., How Virtual Private Networks Work, 2007.

<sup>11</sup>Krstajić B., Radulović A., Informacione tehnologije, Zbornik radova, Žabljak, 2010.

zona. Ovakve konekcije je obično moguće ostvarivati u posebno definisanim vremenskim periodima.

Ukoliko jedna kompanija pokušava da se konektuje na lokalnu mrežu druge kompanije, bilo da to pokušava iz svoje sopstvene lokalne mreže ili pokušava da uspostavi udaljenu konkekciju putem javne mreže, mora da uspešno zadovolji sva pravila određenog skupa autentikacionih mehanizama i firewall-a koji omogućavaju prvoj kompaniji da nesmetano pristupi demilitarizovanoj zoni druge kompanije. Da bi se postigla veća ekonomičnost, ovakve arhitekture se često sreću u nekim oblastima elektronske trgovine kao i u razmeni elektronskih podataka.<sup>12</sup>

### **4.3. Virtuelne privatne mreže zasnovane na sistemima sa udaljenim pristupom**

Virtuelne mreže zasnovane na sistemima sa udaljenim pristupom, poznatije pod imenom dial-up virtuelne privatne mreže (VPDN – *Virtual Private Dial-up Network*), predstavljaju oblik „korisnik–lokalna mreža“ arhitekture povezivanja kojom kompanija omogućuje svojim zaposlenima da pristupe privatnoj lokalnoj mreži kompanije sa različitih udaljenih lokacija. U situacijama kada je potrebno da se napravi ovakva arhitektura privatne mreže kompanije najčešće svoja ovlašćenja delegiraju nekom od provajdera takvih servisa.<sup>13</sup> Provajder servisa u toj situaciji uspostavlja server za pristup mreži i distribuira korisnički aplikativni softver potencijalnim korisnicima – zaposelnima u kompaniji. Tako zaposleni upotrebom aplikativnog softvera mogu da se preko servera za pristup mreži povežu sa privatnom lokalnom mrežom svoje kompanije. Ovakva arhitektura ima nisku cenu koštanja ali je osetljiva što se tiče bezbedonosnih karakteristika.

### **4.4. Virtuelne privtne mreže na mrežnom nivou OSI referentnog modela**

Virtuelne privatne mreže na mrežnom nivou baziraju se na IP protokolu (IP – *Internet Protocol*). Ovakve virtuelne privatne mreže se mogu implementirati na dva načina: tunelovanjem ili šifrovanjem na mrežnom nivou.

<sup>12</sup> Venkateswaran R., *Virtual private networks*, 2000.

<sup>13</sup> Jovanović B., *Različite arhitekture virtuelnih privatnih mreža*, Centar za primenjenu matematiku i elektroniku, Beograd, 2010.

Tunel povezuje dve tačke virutelne privatne mreže preko deljene infrastrukture određene mreže. U tunel modu, krajnje tačke tunela su zajednička mesta spajanja virtuelne privatne mreže i deljene mrežne infrastrukture.

Tunelovanje, kao proces enkapsulacije i prenosa paketa podataka nekog određenog protokola (protokol klijent) kroz neki drugi protokol (protokol domaćin), predstavlja fundamentalni postupak koji je osnova svih tehnologija virtuelnih privatnih mreža. Protokol tunelovanja podatke i informacije iz zaglavlja koji su sastavni deo paketa transmisionog protokola klijenta jednostavno obmotava novim zaglavljem protokola domaćina kojim se obezbeđuju informacije neophodne za usmeravanje podataka kroz mrežu i njihovo dospevanje na željeno odredište. Ovakav tunel ne obmotava korisne informacije samo da bi one dospele na željeno odredište, već se ovakvim tunelovanjem postiže određen stepen pouzdanosti da su podaci bezbedno i bez greške stigli na odredište a da su pri tome prenošeni javnom mrežom.

Prenos podataka preko Interneta ili neke druge javne mreže putem tunela virutelne privatne mreže može se realizovati korišćenjem nekoliko različitih tehnika tunelovanja, kao na primer: PPTP (PPTP – *Point-to-Point Tunneling Protocol*), L2FP (L2FP – *Layer 2 Forwarding Protocol*), L2TP (L2TP – *Layer 2 Tunneling Protocol*) ili IPSec (IPSec – *IP Security*). IPSec predstavlja proširenje IP protokola sa mrežnog nivoa koje dodaje podatke potrebne za autentifikaciju kao i zaštitu tajnosti podataka u samom tunelu čime se postiže dodatna bezbednost.

Ovakva virtuelna privatna mreža predstavlja kolekciju tunela koji su uspostavljeni preko deljene mrežne infrastrukture. Paket sa mrežnog nivoa napusta čvor virtuelne privatne mreže na jednom kraju tunela sa dodatim IP zaglavljem čija adresa odredišta predstavlja drugu stranu tunela. Takav paket se zatim usmerava pomoću zajedničke mrežne infrastrukture na osnovu tako modifikovane adrese odredišta. Na drugoj strani tunela vrši se odbacivanje dodatog IP zaglavlja i ponovno kreiranje početnog paketa.

IETF (IETF – *Internet Engineering Task Force*) je standardizovao bezbednu arhitekturu na mrežnim nivou, poznatiju kao IPSec protokol. IPSec protkol predstavlja kolekciju protokola, autentikacionih mehanizama i mehanizama za šifrovanje.

### **4.5. Virtuelne privatne mreže na nivou veze podataka OSI referentnog modela**

Ukoliko se zajednička mrežna infrastruktura zasniva na komutiranim tehnologijama na nivou veze podataka, virtuelne privatne mreže implementirane direktno na ovim tehnologijama nazivaju se virtuelne privatne mreže na nivou veze podataka.

Međutim, sa pojavom svičeva-rutera i protokola kao što je MPLS (MPLS – *Multi-Protocol Label Switching*) ili MPOA (MPOA – *Multi-Protocol over ATM*) više ne postoji jasna linija koja razgraničava virtuelne privatne mreže na različitim nivoima višeslojnog modela.<sup>14</sup>

Veze koje su namenjene ovom vidu virtuelnih privatnih mreža imlementiraju se kao virtuelna kola na drugom nivou. Virtuelno kolo predstavlja osnovnu apstrakciju protokola orijentisanog na uspostavljanje veze. Kada se uspostavi virtuelno kolo, ono opstaje do eksplicitnog zatvaranja. Prednost virtuelnih kola je u tome što su ona daleko jeftinija i fleksibilnija od iznajmljenih linkova. Virtuelna kola dolaze sa određenim nivoom garancije njihovih performansi.

Ova vrsta virtuelnih privatnih mreža nije idealno povoljna za dial-up servise jer veliki broj provajdera internet usluga svoje servise zasniva na IP protokolu. Bez obzira što dial-up servisi nude primetno smanjenje troškova, IP bazirane virtuelne privatne mreže su mnogo atraktivnije IT menadžerima te su zbog toga i zastupljenije.

Kao i sa tunelima, ovde je zastupljen problem kada će virtuelna kola sa drugog nivoa biti prilagođena da omoguće uspostavljanje potpune meš (full-mesh) topologije računarske mreže kako bi povezale sve moguće parove čvorova u virtuelnoj privatnoj mreži. Da bi se ovakav problem prevazišao, u obzir se uzimaju drugi oblici fizičkih arhitektura kao što je na primer parcijalni meš (partial mesh) ili topologija zvezde.

## **5. Kontrola pristupa u VPN**

Pristup zaštićenim informacijama mora da bude ograničen samo na osobe koje su autorizovane za pristup tim informacijama. Računarski programi, a u mnogim slučajevima i sami računari koji obrađuju podatke moraju takođe da budu autorizovani. Ovo zahteva postojanje mehanizama koji su u stanju da kontrolišu pristup zaštićenim informacijama. Sofisticiranost mehanizama za kontrolu pristupa treba da se uporedi sa vrednošću informacija koje se štite. Osetljivije i dragocenije informacije treba da imaju jače mehanizme zaštite. Temelji na kojima počivaju mehanizmi kontrole pristupa su identifikacija i autentifikacija.<sup>15</sup>

<sup>14</sup>VPN Connections Options Expand, Info World, 2001.

<sup>15</sup> Deal R., The Complete Cisco VPN Configuration Guide, Cisco Press, December 2005.

Identifikacija je tvrdnja ko je zapravo neko i šta je u stvari nešto. Ako se osoba predstavi svojim imenom i prezimenom neko mora da potvrdi da je ta izjava istinita. Međutim, ovakva tvrdnja može biti istina ili ne. Pre nego što nekoj osobi bude dozvoljen pristup zaštićenim informacijama neophodna je verifikacija odnosno provera informacija o toj osobi.

### **5.1. Autentifikacija u virtuelnoj privatnoj mreži**

Autentifikacija je čin verifikacije tvrdnje o identitetu. Kada neko ode u banku da obavi neku novčanu transakciju on se predstavlja bankarskom službeniku imenom i prezimenom (tvrdnja o identitetu). Na zahtev službenika da svoj identitet potvrdi nekim dokumentom on prezentuje ličnu kartu. Službenik zatim proverava podatke i upoređuje fotografiju iz lične karte. Ukoliko fotografija i podaci odgovaraju osobi koja ih je prezentovala službenik je izvršio autentifikaciju odnosno potvrdio je da se radi o toj konkretnoj osobi.<sup>16</sup>

Postoje tri različita tipa informacija koje mogu da se koriste za autentifikaciju: ono što znate, ono što imate i ono što ste. Primer za “ono što znate” je najčešće PIN ili lozinka. Primer za “ono što imate” uključuje ličnu kartu ili platnu karticu. Biometrija u stvari govori “ono što ste”. Primeri biometrije uključuju otisak dlana, otisak prsta, snimak glasa i skeniranje mrežnjače oka. Snažna autentifikacija eng. strong authentication zahteva obezbeđivanje informacija iz dva od tri različita tipa informacija. Na primer “ono što znate” i “ono što imate”. Ovo se naziva dvofaktorna autentifikacija eng. two-factor authentication.

U računarskim sistemima koji su danas u upotrebi korisničko ime je najčešći način za identifikaciju, a lozinka je najčešći način za autentifikaciju. Korisničko ime i lozinka služili su svojoj svrsi ali u savremenom svetu oni više nisu adekvatan oblik identifikacije i autentifikacije i polako bivaju zamenjeni sofisticiranijim mehanizmima kao što su smart kartice ili biometrija.

Protokol za autentifikaciju je vrsta kriptografskog protokola. On služi da autentifikuje entitete koji žele da uspostave bezbednu međusobnu komunikaciju. Postoji veliki broj različitih protokola za autentifikaciju a neki od najčešće korišćenih su:

- Challenge-handshake authentication protocol (CHAP)
- CRAM-MD5
- Diameter

<sup>16</sup>Grubor G., Miloavljević M., Osnovi zaštite informacija, Univerzitet Singidunum, Beograd, 2010.

- Extensible Authentication Protocol (EAP)
- Host Identity Protocol (HIP)
- Kerberos
- MS-CHAP and MS-CHAPv2 variants of CHAP
- NTLM also known as NT LAN Manager
- Password-authenticated key agreement protocols
- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- RADIUS
- Secure Remote Password protocol (SRP)
- TACACS
- TACACS+
- RFID-Authentication Protocols

## **5.2. Autorizacija u virtualnoj privatnoj mreži**

Nakon što su osoba, program ili računar identifikovani i autentifikovani treba odrediti kojim resursima im je dozvoljen pristup i koje akcije su im dozvoljene za izvršenje (pokretanje, pregled, kreiranje, brisanje ili izmena). Ovaj proces se naziva autorizacija.

Autorizacija za pristup informacijama I drugim računarskim servisima započinje administrativnim politikama I procedurama. Politike propisuju ko može da koristi koje informacije I računarske servise I pod kojim uslovima. Mehanizmi kontrole pristupa su konfigurisani tako da primoravaju na poštovanje uspostavljenih politika.

## **5.3. Accounting u virtualnoj privatnoj mreži**

Evidencija o pokušajima pristupanja sistemu i pojedinim servisima na njemu naziva se accounting. Ovakve evidencije se vode u log fajlovima i veoma je važno da administratori što češće kontrolišu ove fajlove jer u njima mogu naći važne informacije o eventualnim nepravilnostima koje se tiču autentifikacije i autorizacije. Ukoliko redovno vrše kontrolu log fajlova mogu blagovremeno da spreče neželjne posledice koje mogu veoma ozbiljno ugroze sistem koji održavaju.

Remote Authentication Dial In User Service (RADIUS) je mrežni protokol koji omogućava računarima centralizovanu autentifikaciju, autorizaciju i accounting (AAA) da bi mogli da se konektuju i koriste mrežne servise. RADIUS je razvila kompanija Livingston Enterprises, Inc. 1991 godine kao serverski protokol za autentifikaciju i accounting, a kasnije je unet i u IETF standarde.

Zbog široke podrške koju ima RADIUS protokol često koriste ISP i kompanije za upravljanje pristupom Internetu ili internoj mrežom, wireless mreži i integrisanim e-mail servisima. Ove mreže mogu u sebi da sadrže modeme, DSL, pristupne tačke, virtualne privatne mreže, mrežne portove, web servere i drugo.

RADIUS je klijent/server protokol koji se pokreće u sloju aplikacije OSI modela, koristeći UDP protokol za transport. Serveri za pristup mreži (*Network Access Server* u daljem tekstu NAS server) predstavljaju mrežni prolaz koji kontroliše pristup mreži i moraju da imaju RADIUS klijent komponentu koja komunicira sa RADIUS serverom. RADIUS server je proces koji se odvija u pozadini i koji je pokrenut na Linux ili Windows platformi i ima tri osnovne funkcije:<sup>17</sup>

1. Da autentifikuje odnosno da identifikuje korisnike ili uređaje pre nego što im dopusti da pristupe mreži
2. Da autorizuje odnosno da privilegije korisnicima ili uređajima za bezbedan pristup mrežnim servisima
3. Da radi accounting odnosno izveštava o korišćenju ovih servisa

RADIUS server koristi AAA koncept za upravljanje pristupom mreži koristeći proces koji je poznat pod nazivom „AAA transakcija“. AAA je skraćenica za autentifikaciju, autorizaciju i accounting. Karakteristike autentifikacije i autorizacije su opisane u dokumentu RFC 2865 dok je accounting opisan u dokumentu RFC 2866.

Korisnički računar šalje zahtev NAS serveru da bi dobio pristup određenom mrežnom resursu koristeći parametre za pristup. Ovi parametri za pristup se prosleđuju NAS serveru preko link-layer protokola, Point-to-Point Protocol (PPP) u slučaju dial-up konekcije ili DSL provajdera, a takođe mogu biti poslani i kao HTTPS Web forma.

NAS server šalje zatim RADIUS Access Request poruku RADIUS serveru zahtevajući dobijanje pristupa preko RADIUS protokola. Ovaj zahtev sadrži parametre za pristup u formi korisničko ime i lozinka ili digitalni sertifikat koji poseduje korisnik.

<sup>17</sup><http://telekomunikacije.etf.bg.ac.rs> pregledano dana 10.10.2012.

Dodatno, zahtev može da sadrži i druge informacije koje NAS server zna o korisniku kao što je njegova mrežna adresa kao i informacije koje imaju veze sa korisnikovom fizičkom lokacijom sa koje pristupa NAS serveru.

RADIUS server zatim proverava, koristeći šeme za autentifikaciju kao što su PAP, CHAP ili EAP, da li su informacije koje su mu prosledjene korektne. Nekada su RADIUS serveri proveravali korisničke informacije u lokalnoj bazi podataka smeštenoj u flat datoteci. Moderni RADIUS serveri da rade ovo isto ali isto tako mogu da se referenciraju porema spoljašnjim izvorima, a najčešće se koriste: SQL, Kerberos, LDAP ili Active Directory servisi.

RADIUS server zatim vraća jedan od tri moguća odgovora NAS serveru:

1. Access Reject
2. Access Challenge
3. Access Accept

**Access Reject** – Korisniku je bezuslovno zabranjen pristup svim zahtevanim mrežnim resursima. Razlozi mogu da razni od grešaka prilikom dokazivanja korisnikovog identiteta pa do neaktivnog ili nepoznatog korisničkog naloga.

**Access Challenge** – Zahtevaju se dodatne informacije od korisnika kao što su: ponavljanje lozinke, PIN, token ili smart kartica. Access Challenge se takođe koristi u složenijim dijalozima za autentifikaciju u kojima se uspostavlja bezbednosni tunel između korisničkog računara i RADIUS servera u slučaju kada su parametri za pristup sakriveni od NAS servera.

**Access Accept** – Korisniku je dozvoljen pristup. Kada se korisnik uspešno autentifikuje RADIUS server proverava njegova prava ili privilegije da pristupa određenim mrežnim servisima. Na primer korisniku može biti dozvoljeno da koristi wireless mrežu u kompaniji, ali ne i njene VPN servise. Informacije o autorizaciji, kao što je napomenuto, mogu da se čuvaju lokalno ili u nekom od spoljnih izvora kao što su SQL, LDAP ili Active Directory. Autorizacija će biti detaljnije opisana kasnije, a sada može da se zakluči da svaki od ova tri odgovora RADIUS servera uključuje Reply-Message attribute koji mogu da sadrže razlog za odbijanje, zahtev za dodatnim informacijama ili poruku dobrodošlice za uspešnu autentifikaciju. Tekst sa atributima prosleđuje se korisniku preko Web stranice koju dobija kao odgovor od NAS servera.

RADIUS server isporučuje attribute za autorizaciju NAS serveru, a on zatim generiše termine koji korisniku služe za pregovaranje prilikom pristupa. Na primer neki od sledećih atributa može da se pojavi kao Access-Accept odgovor.

Portal koji bi se korisniku otvorio posle uspešne autentifikacije prikazivao bi linkove prema servisima na koje taj konkretan korisnik ima pravo, a to bi bilo generisano na osnovu komunikacije između SSL VPN uređaja i RADIUS servera.

Posle toga za proveru privilegija za pristup pojedinim servisima bili bi odgovorni Web server i RADIUS server. To bi funkcionisalo tako što bi Web server svaki zahtev za pojedinim servisom proveravao na RADIUS serveru odnosno u bazi podataka koja se koristi kao njegovo proširenje.

Takođe treba reći da zbog svoje osetljivosti podaci koji se nalaze na RADIUS serveru, a to su korisnički sertifikati i privilegije svakog pojedinačnog korisnika, treba da budu dobro čuvani. Najbolja zaštita bi bila da administrator ukoliko želi promenu podataka na RADIUS serveru koristi dodatnu autentifikaciju uz pomoć smart kartice, a po potrebi i digitalno potpiše te promene. Za sve ostale korisnike i servise ovi podaci nisu dostupni za izmenu već oni mogu samo da ih čitaju odnosno da oni za njih budu read-only.

Kada je odobrio korisniku pristup mreži NAS server šalje RADIUS serveru Accounting Start (*RADIUS Accounting Request* paket koji sadrži *Acct-Status-Type* atribut koji ima vrednost "start") kao signal za pokretanje korisničkog pristupa mreži. Paket "Start" sadrži korisničku identifikaciju, mrežnu adresu, način konekcije i jedinstveni identifikator sesije.

Za vreme korisničkog pristupa mreži, NAS server šalje RADIUS serveru Interim Update slogove (*RADIUS Accounting Request* paket koji sadrži *Acct-Status-Type* atribut koji ima vrednost "interim-update") da bi ga ažurirao statusom aktivne sesije. "Interim" slogovi dogovaraju trajanje tekuće sesije kao i informacije o podacima koji se trenutno prenose.

Na kraju, kada se zatvori korisnički pristup mreži NAS server isporučuje RADIUS serveru Accounting Stop slog (*RADIUS Accounting Request* paket koji sadrži *Acct-Status-Type* atribut koji ima vrednost "stop") koji obezbeđuje informacije o vremenu konekcije, poslatim podacima, razlozima za prekid konekcije kao i drugim informacijama važnim za korisnički pristup mreži.

## **6. Zaštita virtuelne privatne mreže**

Internet Protocol Security (IPsec) protocol je rešenje za zaštitu podataka koji se prenose korišćenjem IP protokola. Ovaj system je realizovan setom protokola kojima se ostvaruje šifrovanje, provera autentičnosti i izvora i integriteta poruka koje se prenose. Dodatno, IPsec system koristi i protocol za razmenu ključeva na početku sesije.<sup>18</sup>

IPsec system se može koristiti za zaštitu komunikacije između krajnjih učesnika, između krajnjeg učesnika, sa jedne strane, i podrazumevanog mrežnog prolaza, sa druge strane, ili između podrazumevanih mrežnih prolaza sa obe strane. U skladu sa tim IPsec podržava dva režima rada: transportni i tunelski.

Za razvoj IPsec sistema zaštite zvanično je zadužena IETF grupa. Sam IPsec system zaštite je naslednik ISO standardizovanog NLSP (*Network Layer Security Protocol*) protokola baziranog na SP3 protokolu, kojeg je prvi objavio američki NIST – a inicijalno je dizajniran od strane američke nacionalne bezbednosne agencije (NSA). Postoji veliki broj dokumenata kojim je IPsec system zaštite dokumentovan i standardizovan.

Jedna od značajnih prednosti IPsec sistema zaštite u odnosu na druge popularne sisteme zaštite (SSL, TLS...) je rad na niskom nivou u odnosu na OSI i TCP/IP referentne modele. Ovakva pozicija obezbeđuje fleksibilnost u pogledu zaštite velikog broja protokola viših nivoa.

Osnovne komponente IPsec sistema zaštite su Internet Key Exchange (IKE, IKE2) – system za upravljanje ključevima i uspostavljanje bezbednosnih asocijacija, Authentication Header (AH) – protocol za obezbeđivanje autentičnosti i integriteta i Encapsulating Security Payload (ESP) – protocol za obezbeđivanje poverljivosti, autentičnosti i integriteta.

Još jedna značajna karakteristika IPsec sistema zaštite je i podrška za IPv6 protokol. Ustvari, IPsec je podrazumevani deo ovog protokola i inicijalno je i razvijan na njemu a naknadno je portovan na verziju 4.

Za uspešno korišćenje IPsec protokola neophodno je uspostavljanje pravilnih bezbednosnih asocijacija. Bezbednosne asocijacije predstavljaju pravila po kojima će se uspostaviti bezbedna komunikacija između učesnika.

---

<sup>18</sup>Veinović M., Jevremović A., Računarske mreže, Univerzitet Singidunum, Beograd, 2011.

U bezbednosnim asocijacijama mogu biti direktno postavljeni ključevi koji će se koristiti za šifrovanje a u tu svrhu se može iskoristiti I protocol za razmenu ključeva putem Interneta.

IPsec system zaštite se može posmatrati kao jednostavno I efikasno rešenje za zaštitu komunikacija baziranih na IP protokolu. Važna karakteristika ovog sistema jeste otvorenost I dokumentovanost kroz RFC I druge dokumente. Izbor IPsec sistema zaštite kao nosioca realizacije sopstvenog rešenja baziranog na sopstvenom algoritmu, rezultat je dugortajnog I temeljnog ispitivanja postojećih alternativa.

## **7. Mere za poboljšanje bezbednosti WLAN**

Mere za zaštitu bežične računarske mreže se mogu sprovoditi na upravljačkom, operativnom i tehničkom nivou.

### **7.1. Upravljačke mere za zaštitu bezbednosti WLAN**

Upravljačke mere za zaštitu bezbednosti počinju sa obuhvatnom politikom bezbednosti. Politika bezbednosti je dokument na osnovu kojeg su ostale mere bezbednosti, operativne i tehničke usklađene i implementirane. Bezbednost bežične mreže uključuje sledeće odrednice:

Ovlašćenja i odgovornosti korisnika - Politika prikazuje šta je sve u nju uključeno, zašto je ona neophodna i šta se dešava ako se ona prekrši. Ona takođe definiše odgovornost službi i pojedinaca, posebno korisnika uopšte, odeljenja IT I kontrolora.

- 1) Sredstva koja se štite - Politika bezbednosti može identifikovati ili ukazati na osetljive informacione resurse, komunikacione kanale i sisteme koje treba zaštititi u bežičnoj mreži.
- 2) Pretnje i slabosti - Politika bezbednosti može da uključi i deo u kojem se identifikuju pretnje po bežičnu mrežu.
- 3) Analiza napada - Politika bezbednosti može identifikovati posledice koje nastanu u slučaju narušavanja bezbednosti bežične mreže.
- 4) Postupci i odgovornosti - Politika bezbednosti bi trebalo da identifikuje i definiše bezbednosne procedure za sledeće slučajeve:

- Kreiranje naloga za nove korisnike.
- Politiku lozinki i njihovo obnavljanje.
- Autentikaciju.
- Pristup opremi i prostorijama.
- Izveštavanje o narušavanju bezbednosti.
- Raspolaganje sa osetljivim podacima.

Planiranje odgovora na narušavanje bezbednosti - Može biti opisano uključujući i planove odgovora na različite incidente, spisak osoba koje treba pozvati u slučaju incidenta i njihovu odgovornost, proces ispitivanja uzroka incidenta, process oporavka sistema, popis izveštaja koji se moraju podneti posle incidenta.

Prihvatljivo korišćenje - Politika bezbednosti može da se kreira tako što bi bile definisane dozvoljene aktivnosti na bežičnoj mreži (npr. pristup internetu, razmena elektronske pošte i poslovna primena). Politika takođe može da definiše aktivnosti koje su izričito zabranjene na bežičnoj mreži sa objašnjenjem potrebe da se zaštite resursi korisnika i održi integritet mreže. Bezbednost na krajnjim tačkama - Kontrola bezbednosti na radnim stanicama, laptop računarima, PDA i drugim bežičnim uređajima koji su uključeni u politiku bezbednosti bežične mreže. Zahtevi za često čak i dnevno ažuriranje softvera, namensko korišćenje bezbednosnog softvera (npr. VPN klijenti, anti-virus i firewall), treba da budu uključeni. Lista za kontrolu bezbednosti može da ima razne oblike prema mogućnostima pristupa krajnjoj opremi, na lokaciji opreme ili preko mreže. Uputstvo za uvođenje WLAN - Politika treba da obezbedi uputstvo za implementaciju i razmeštaj delova bežičnih sistema. Treba da odredi ko može da instalira pristupne tačke i drugu bežičnu opremu i da obezbedi ograničenja za lokacije i fizičku bezbednost za pristupne tačke. Takođe može da obezbedi podrazumevane konfiguracije za pristupne tačke (koristeći WPA2/802.11i) i krajnje uređaje (koristeći VPN), autentikaciju (koristeći autentikaciju na osnovi 802.11X) i mehanizam poverljivosti, zahteve za upravljanje ključevima, i zahteve za fizičko raspoređivanje uređaja i mreže.

Politika razvijanja - Trebalo bi povesti računa o uvođenju promena u već razmeštenoj infrastrukturi, kao što je registracija uređaja, procedure za dogradnju uređaja, uklanjanje i dodavanje uređaja, kao i testiranje interoperabilnosti uređaja.

Verifikacija i usaglašavanje - Politika treba da uključuje zahteve za dnevničke revizije i obračuna troškova, uključujući i specifikacije akcija i događaja koje treba zabeležiti, kao i učestalost pregleda dnevnika. Politika treba da sadrži predviđenu učestalost i opseg bezbednosnih procena za uključivanje pristupne tačke.

- Nametanje politike – Politika treba da definiše odgovornost za nadziranje zaposlenih, i treba da do detalja definiše aktivnosti na disciplinovanju prekršioca i ponovljenih prekršioca.
- Obaveze prema regulativi – Politika bezbednosti WLAN mora uzeti u obzir bilo koji relevantni industrijski standard (npr. Payment Card Industry Data Security Standard (PCI-DSS)) ili uputstva za očuvanje i zaštitu privatnosti podataka.
- Obuka i podizanje nivoa svesti o bezbednosti – Zajedno sa jasnim delokrugom politike bezbednosti, organizacije koje koriste WLAN treba takođe da obezbede da svo kritično osoblje bude na odgovarajući način obučeno za korišćenje bežične tehnologije.

Administratori mreže treba da budu potpuno svesni bezbednosnih rizika koje sa sobom nose mreža i uređaji. Oni moraju da rade kako bi garantovali primenu politike bezbednosti i da znaju koje korake treba da preduzimaju u slučaju napada. Svi korisnici WLAN treba da budu upozoreni na svoju odgovornost kada koriste bežične mreže unutar organizacije na koju se odnosi politika bezbednosti ili kada koriste mobilne bežične uređaje za povezivanje na druge bežične mreže, van organizacije.

## **7.2. Operativne mere za zaštitu bezbednosti WLAN**

Fizička bezbednost je osnovna mera kojom se obezbeđuje da samo autorizovani korisnici imaju pristup bežičnoj računarskoj opremi. Fizička bezbednost podrazumeva mere kao što su:

- Kontrola pristupa – Identifikacija propusnicama, pristup uz identifikaciju putem čitača kartica, identifikacija biometrijskim uređajima su metode koje smanjuju mogućnost neovlašćenog pristupa opremi za bežičnu računarsku mrežu.
- Lična identifikacija.
- Zaštita na više nivoa – zaključavanje vrata, instalacija video nadzora za nadgledanje prostora oko objekata u kojima je postavljena WLAN. Na taj način se odvrćaju potencijalni napadači na pristupne tačke.

Svaka od navedenih mera je važna, ali napadač na bežičnu mrežu se može nalaziti van objekta u kojem se koristi bežična mreža, a da ipak bude u dometu te mreže, sa mogućnošću upada u nju. Da bi se to sprečilo, koristi se alat za procenu bezbednosti bežične mreže (npr. procena povredivosti) i sprovođenje bezbednosne procene se obavlja redovno. Bezbednosne procene se vrše kako bi se osigurala usaglašenost opreme i ponašanja zaposlenih sa politikom

bezbednosti. Testiranje na probijanje zaštite bežične mreže se takođe pojavljuje kao mogućnost da se bezbednost bežične mreže održi u okviru predviđene tolerancije rizika.

### **7.3 Tehničke mere za zaštitu bezbednosti WLAN**

Tehničke mere zaštite obuhvataju korišćenje hardverskih i softverskih rešenja. Softverske mere zaštite uključuju pravilno konfigurisanje pristupnih tačaka (AP), instaliranje softverskih zavrta i nadgradnju softvera, autentikacija, sistemi za detektovanje upada (IDS), lični firewall za bežične uređaje i šifrovanje komunikacija. Hardverska rešenja uključuju smart kartice, virtuelne privatne mreže (VPN), infrastrukturu sa javnim ključem (PKI), segregaciju mreže, i biometrijske metode zaštite. Treba primetiti da se neka od ovih rešenja pojavljuju i kao hardverska i kao softverska. Tehničke mere zaštite bi trebalo da uključuju podršku šifrovanjem i kontrolu autentikacijom što je opisano u svakom od standarda za bežične mreže.

Šifrovanje u bežičnim komunikacijama se koristi prvenstveno da zaštiti poverljivost poruka i podataka za podešavanje konekcije koji se šalju preko mreže. Autentikacija u bežičnim mrežama se pojavljuje da bi se proverila veza između jednog i drugog uređaja, ili da se potvrdi da je korisnik ovlašćen da se konektuje na određenu mrežu. Protokoli za šifrovanje koji se koriste u starijim standardima za bežične mreže su bili implementirani na neodgovarajući način a kao posledica toga je njihovo lako probijanje (npr. WEP RC4). Korišćenje najnovije verzije standarda za bežične mreže je preporučljivo, pošto one imaju tendenciju da koriste protokole za šifrovanje koji nisu podložni probijanju (npr. WPA2, AES). Izbor protokola za šifrovanje zavisi od raspoložive infrastrukture. Postojeći uređaji, nasledeni od ranije, mogu samo da podrže WEP/TKIP, ali ne i WPA/WPA2. AES zahteva veću procesorsku snagu.

Najbolja praksa po pitanju bezbednosti WLAN-a je korišćenje WPA2 i AES. Mnoge bežične tehnologije dozvoljavaju upotrebu više modova za autentikaciju, čime se nudi različita čvrstina autentikacije. Na primer WPA i WPA2 se mogu postaviti u lični ili kompanijski mod. Lični mod koristi slabiju PSK autentikaciju, a kompanijski mod zahteva mnogo čvršći 802.1x/EAP metod. U zavisnosti od poslova koji se obavljaju, može se odrediti prikladnost svake od metoda autentikacije. Za veće mreže koje zahtevaju više upravljanja, centralizovana autentikacija i upravljanje korišćenjem 802.1X uz odgovarajući izbor EAP se preporučuje. Za male privremene mreže, metoda deljenog ključa može da obezbedi odgovarajuću zaštitu. Najbolja autentikacija u praksi za WLAN je trenutno WPA2 uz korišćenje 802.1X/EAP.

Stariji sistemi ili uređaji nisu kompatibilni sa većinom novijih standarda, i ostala infrastruktura (npr. server za autentikaciju) može takođe biti ograničenje za uspešnu implementaciju bezbednosnih protokola novije generacije. Dobra praksa je onemogućavanje network service set identifer SSID broadcast. Na taj način se pristupna tačka čuva od nepotrebnog oglašavanja svog prisustva.

Dodatne mere bezbednosti se mogu primenjivati pored već uključenih bezbednosnih funkcionalnosti prema bezbednosnim standardima i njima pridruženim tehnologijama. U mnogim slučajevima, ti dodaci mogu značajno da povećaju nivo bezbednosti. Dodatne mere uključuju:

- Korišćenje virtualne privatne mreže (VPN) kojom se dodaje još jedan nivo bezbednosti za daljinski pristup. Kada se koristi bežična mreža ili hotspot koji ne pripadaju organizaciji (npr. kućna ili javna WLAN), upotreba VPN je veoma preporučljiva. Taj dodatni nivo zaštite omogućava jaču autentikaciju i šifrovanje za korisnike koji imaju daljinski pristup.
- Sistem za detekciju upada u bežičnoj mreži (IDS) je tehnologija iskorišćena da detektuje napade karakteristične za bežičnu mrežu. Korišćenje bežičnog IDS sistema dozvoljava organizaciji koja štiti svoju mrežu da reaguje na napad što je ranije moguće i tako minimizuje bilo koje oštećenje na mreži. Bežični IDS se dalje može koristiti da poveća mogućnost predviđanja napada i za upravljanje procedurom isključenja korisnika, kao što je blokiranje ili deautentikacija sumnjivih korisnika, ili promena bežičnih kanala kako bi se iskoristilo slabljenje signala, i tako onemogućio pristup napadaču.
- Šifrovanje podataka na hard disku je veoma preporučljivo za osetljive informacije koje se čuvaju na nekom od uređaja koji ima pristup bežičnoj mreži.
- WEP nije siguran, nije dizajniran kao potpuno rešenje za obezbeđivanje mreže, već mu je namena samo da podigne nivo bezbednosti na nivo kakav je postojao u ranijim kablovskim mrežama. Postoji veliki broj programa koji "provaljuju" WEP algoritam a lako su dostupni na internetu. Ako oprema nije zastarela preporučuje se WPA2 umesto WEP-a.
- Kada se radi o mreži sa mnogo korisnika, preporuka je da se izvrši njena segmentacija. To je tehnika koja predstavlja razdvajanje računarske mreže u podmreže. Tako se postižu bolje performanse i povećava bezbednost takvih podmreža, zato što se postavljaju dodatna pravila za deo mreže u kojem se nalaze kritične komponente. Segmentacija se najčešće ostvaruje pomoću mrežnih uređaja bridge, switch, i router.

- Ako se omogućava broadcast SSID, ne koristiti imena firme ili imena po kojima bi neko lako mogao da utvrdi o čijoj se mreži radi za SSID (service set identifier) I AP. Ta imena se ne šifruju u hederu 802.11x paketa podataka, tako da svako može da ima podatak o kojoj se mreži radi, a napadaču je značajno olakšan posao kada tačno zna gde i šta treba napasti.
- Ne dozvoliti da bilo ko vidi MAC adresu AP-a iako mnogi proizvođači opreme ugrađuju mogućnost automatskog prepoznavanja adrese.
- Menjanje ključa s vremena na vreme ne donosi neku zaštitu jer hakeri ključ mogu “provaliti” u roku od par minuta, a promena se mora ručno izvršiti na svakom AP-u u mreži. Iz tog razloga su razvijeni automatski izmenjivači ključa koji ga menjaju dosta često na svim AP-ovima istovremeno.
- Postaviti AP tako da pokriva svu potrebnu površinu ali da signal što manje napušta zgradu ili okruženje u kojem se radi.
- Pre prve instalacije AP-a obavezno promeniti šifru i IP adresu.
- Ne koristiti DHCP (Dynamic Host Configuration Protocol) na WLAN-u.

Pronalaženje postojeće IP adrese u mreži kada se koristi DHCP je veoma jednostavno.<sup>19</sup>

- Postoji mogućnost korišćenja boja za zidove koje blokiraju wireless signal. Boja sadrži okside gvožđa i aluminijuma i apsorbuje talase frekvencije do 128 GHz.
- Merenjem jačine signala pomoću više prijemnika, utvrđuje se lokacija klijenta koji se prijavljuje na AP i na osnovu toga dozvoljava ili odbija pristup mreži. Postoje HW/SW alati za takvu zaštitu, koriste se za zaštitu velikih bežičnih mreža.

#### **7.4. Honeypot tehnologija za zaštitu bežične mreže**

Za razliku od firewall-a ili IDS, honeypot ne rešava samo jedan specifičan problem. To je veom fleksibilan alat kojim se mogu obavljati poslovi od otkrivanje napada na IPv6 mrežama do hvatanja prevara sa kreditnim karticama on-line. Uopštena definicija koja pokriva sve manifestacije, honeypot je resurs informacionog sistema čija je vrednost u neovlašćenom korišćenju tog resursa. Kao i svaki koncept i ovaj ima svoje prednosti i nedostatke.

<sup>19</sup>[www.sec.gov](http://www.sec.gov) pregledano 15.10.2012.

Prednosti honeypot tehnologije:<sup>20</sup>

- Mali skup podataka od velike važnosti: Honeypot prikuplja veoma malo podataka. Skup podataka koje prikupi za jedan dan ne prelazi veličinu reda MB (kod drugih sistema je to reda GB). Prosečno generiše desetak upozorenja dnevno. Honeypot prikuplja samo maliciozne i neautorizovane aktivnosti. To značajno smanjuje potrebno vreme i troškove analize podataka.
- Novi nestandardni alat i taktika odbrane od napada na mrežu.
- Zahteva upotrebu minimalnih resursa: Računar klase PII sa 128 MB RAM-a može bez poteškoća da opslužuje mrežu klase B na ovim poslovima.
- Šifrovanje ili IPv6: Za razliku od većine drugih tehnologija (kao što su IDS sistemi) honeypot radi bez problema u šifrovanom ili IPv6 okruženju. Bez obzira kakve podatke napadač ubacivao u honeypot, on će ih detektovati i sakupiti.
- Jednostavnost: Konceptualno je honeypot veoma jednostavan. Nema složenih algoritama u razvoju, glomaznih tabela za održavanje niti dodataka i ispravki za update. Što je jednostavnija tehnologija to je manje mogućnosti za grešk ili pogrešno konfigurisanje alata za zaštitu.

Nedostatci honeypot tehnologije:

- Ograničen opseg vidljivosti: Honeypot može da registruje aktivnosti koje su direktno ka njemu usmerene, a ne može da registruje napade na druge sisteme oko sebe, ako nije i sam obuhvaćen tim napadom.
- Rizik: Sve tehnologije za zaštitu bezbednosti su obuhvaćene rizikom. Firewall je pod rizikom da bude probijen, šifrovanje da bude razbijeno, IDS senzori mogu da propuste registrovanje napada. Honeypot ima rizik da bude iskorišćen od strane napadača za napad na druge sisteme. Taj rizik zavisi od vrste honeypot sistema i njegove konfiguracije.

Vrste honeypot zaštita:

Honeypot se pojavljuje u više oblika i veličina kako bi se otežalo prepoznavanje ovih sistema od strane napadača. Generalno postoje dve kategorije, sa niskom interakcijom i sa visokom interakcijom. Interakcija definiše nivo aktivnosti koji honeypot dozvoljava napadaču.

<sup>20</sup> Jevremović A., Veinović M., „Zaštita podataka na IP nivou pod Linuks OS“, Zbornik radova 50. konferencije Etran, Beograd, 2005.

Honeypot sa niskom interakcijom radi sa emulacijom servisa i operativnih sistema. Aktivnosti napadača su ograničene na nivo emulacije, na primer emulirani FTP servis sluša na portu 21 i može samo da emulira FTP prijavljivanje i eventualno još nekoliko jednostavnijih komandi u FTP. Prednost ovakvog sistema je njegova jednostavnost, lako se instalira i održava, sa minimalnim rizikom. Uvođenje ovakvih honeypot obuhvata instalaciju softvera, izbor operativnih sistema i servisa koje treba emulirati kao i monitor aktivnosti napadača. Sve ovo je veoma jednostavno i dostupno širem krugu zainteresovanih organizacija koje štite svoju bežičnu mrežu. Emulacija servisa smanjuje rizik od neželjenih aktivnosti napadača, tako da on ne može preuzeti ovakav honeypot tj. njegov operativni sistem i sa te pozicije dalje napadati ostatak štićene mreže. Glavni nedostatak honeypot sa niskom interakcijom je što beleži samo ograničen skup informacija već unapred poznatih aktivnosti koje napadač sprovodi.

## ZAKLJUČAK

Virtuelna privatna mreža ili VPN (engl. *Virtual Private Network*) je tehnologija koja zadnjih godina privlači pažnju mnogih kompanija i organizacija koje imaju za cilj proširenje i poboljšanje telekomunikacionih rešenja, uz istovremeno smanjenje troškova poslovanja. Ova tehnologija je primenljiva svuda, od udaljenih filijala do zaposlenih koji rade na terenu ili od kuće.

VPN po formi i funkcionalnosti predstavlja WAN mrežu. Glavna razlika je što se VPN uspostavlja kroz javnu telekomunikacionu infrastrukturu (Internet), umesto korištenja iznajmljenih veza (leased lines). Zaštita i privatnost podataka se ostvaruje korištenjem tuneliranja i enkripcije saobraćaja, kao i sigurnosnim procedurama koje garantuju sigurnost vaših podataka za vreme njihovog prenosa putem Interneta.

Virtuelna privatna mreža (VPN) omogućuje korisnicima da kroz privatnu računarsku mrežu povežu geografski udaljene filijale i radnike korištenjem Interneta kao infrastrukture za povezivanje. U tom smislu VPN služi kao vrlo prihvatljiva zamena za skupe stalne veze i iznajmljene linkove. VPN je fleksibilan način uspostavljanja komunikacija koji povećava produktivnost i delotvornost mreže, te korisniku štedi vreme i novac.

Višenamenska sposobnost VPN-a je od velike važnosti u današnjem mrežnom okruženju s obzirom na prirodu poslovnog uspeha, potreba razvoja korporacijskih mreža ka partnerima i kupcima i širenje opreme uz korporacijsku mrežu. Microsoft Windows je integrisao VPN tehnologiju i pomogao siguran, jeftin, daljinski pristup preko Interneta.

Budućnost je u integrisanim VPN mrežama koje zavise od toga kako će VPN industrija razviti svoj jedinstveni kvalitet kako bi omogućila jednim korisnicima lak način komunikacije sa drugim korisnicima. Stoga VPN pravi veliku multi-sajt mrežu koja omogućava da svaki uređaj bude jedinstveno adresiran iz bilo koje tačke u mreži. Ovo znači da se centralnim resursima može pristupiti iz bilo koje tačke u organizaciji ili iz bilo koje Internet povezane lokacije u celom svetu.

Tehnički problemi koji se odnose na konekciju stotina udaljenih sajtova ka centralnoj mreži su mnogobrojni. To obično uključuje kupovinu vrlo skupih backbone rutera ili upotrebu skupih frame - relay servisa. Ovi sistemi su teški za upotrebu i zahtevaju specijalna znanja. Takođe oni zavise od mogućnosti Intraneta i Ekstraneta kako bi ispunili svoje zahteve. Najvažnija stvar o kojoj VPN kompanije moraju razmišljati je ušteda u servisiranju VPN mreža. U globalu što kompanije budu jeftinije naplaćivale servis toliko će prodaja ići bolje, tako da će imati i veći profit nego da troše mnogo novca u razvoj visokokvalitetnih VPN-ova.

Načini implementiranja VPN konekcije su različiti. Generalno se prilikom kreiranja VPN konekcije koriste neki inicijalizacioni parametri koji se nalaze u nekom fajlu ako seimplementacija vrši na računaru. Često se u njemu nalazi putanja ka fajlu u kojem se nalazeključevi, sertifikati, šifre, tj. neki tajni podaci. Ti podaci su nekada javni (kao što je javniključ) ali veoma često, kada se ne koristi sertifikaciono telo, oni su tajni i od njihove tajnostizavisi uspešnost celokupnog procesa šifrovane VPN veze.

Kada se VPN aplikacija koristi na strani kompanije sa računara koji je fizički u prostorijamakompanije ne postoji tako velika bojazan za bezbednost fajla sa tajnim podacima. Problemnastaje kada se konekcija ostvaruje sa javnih mesta kao što su Internet kafei, aerodromi islično ili kada se laptop iznosi izvan prostorija kompanije. Tada je sadržaj fajla kojiomogućava otključavanje VPN konekcije mnogo ranjiviji. Posebno ako se on mora preneti nafajl sistem nebezbednog računara. Postoje razni scenarioji koji su realni i mogu dovesti dotoga da zlonamerna osoba dođe do sadržaja tog fajla.

Idealno rešenje za navedeni problemi jeste primena smart kartica. Kartica je izvan fajlsistema, pristup podacima je zaštićen *PIN* kodom, a podaci se mogu čuvati i razmenjivati ušifrovanom obliku. Ipak, i ovde postoje problemi u primeni. Čuvanje podataka na kartici zahteva njihovo čitanje od strane VPN aplikacije koja uspostavlja komunikaciju. Postoji puno različitih VPN aplikacija te postoji problem dorade svake aplikacije ponaosob sa funkcionalnošću korišćenja smart kartice.

Sa druge strane, pošto aplikacije standardno znaju da rade sa fajlovima i generalno očekuju inicijalizaciju preko fajlova u fajl sistemu moguće je primeniti virtuelni fajl sistem. On se instalira u radnoj memoriji računara i ponaša se regularno kao element fajl sistema. U ovom radu predloženo je moguće rešenje za čuvanje bezbednosno važnih parametara standardnih VPN aplikacija.

VPN su izvor budućih servisa. Ako su dobro implementirane one mogu omogućiti uprošćavanje mrežnih operacija, a u isto vreme smanjenje kapitalnih troškova. Za većinu kompanija najvažnija početna stavka je povezivanje široko rasprostranjene grupe ljudi na efikasan način koji bi omogućio velike prihode. Tu servis provajderi mogu puno pomoći u razvoju tehnologije pružajući usluge dodatnih servisa kao što su video konferencije, IP telefonija i sl. S druge strane VPN može pomoći servis provajderima u dobijanju novih kupaca omogućivši im sigurno poslovanje preko interneta.

## **Literatura:**

- (1) Andrea Bittau, Mark Handley and Joshua Lackey. The Final Nail in WEP's Coffin. Proceedings of the 2006 IEEE Symposium on Security and Privacy
- (2) Andrew S. Tanenbaum, Computer Networks, Third edition, Prentice-Hall, Inc., 1996.
- (3) Deal R., The Complete Cisco VPN Configuration Guide, Cisco Press, December 2005.
- (4) Grubor G., Miloavljević M., Osnovi zaštite informacija, Univerzitet Singidunum, Beograd, 2010.
- (5) Jevremović A., Veinović M., „Zaštita podataka na IP nivou pod Linuks OS“, Zbornik radova 50. konferencije Etran, Beograd, 2005.
- (6) Jovanović B., Različite arhitekture virtuelnih privatnih mreža, Centar za primenjenu matematiku i elektroniku, Beograd, 2010.
- (7) Krstajić B., Radulović A., Informacione tehnologije, Zbornik radova, Žabljak, 2010.
- (8) Opšta enciklopedija Larousses, LibrairieLarousse, Paris, 1967.
- (9) Simić N, Marić N, DoS Napadi na IEEE 802.11 Radio sisteme. Telfor, Beograd. 2004.
- (10) Stallings W., Cryptography and Network Security - Principles and Practices, Prentice Hall, New Jersey, November 2005.
- (11) Stojaković S. Č.; Building Secure Information Systems, dissertation. Prague. 2000
- (12) Toffler A., The Third Wave, A Bantam Books, USA, 1980.
- (13) Tyson J., How Virtual Private Networks Work, 2007.
- (14) Veinović M., Jevremović A., Računarske mreže, Univerzitet Singidunum, Beograd, 2011., str. 7
- (15) Venkateswaran R., Virtual private networks, 2000.

- (16) Veinović M., Jevremović A., Računarske mreže, Univerzitet Singidunum, Beograd, 2011.
- (17) VPN Connections Options Expand, Info World, 2001.

**Elektronski izvori:**

- 1) [www.sec.gov](http://www.sec.gov)
- 2) <http://www.wikipedia.org>
- 3) <http://www.e-drustvo.org>
- 4) <http://www.corecom.com>
- 5) <http://telekomunikacije.etf.bg.ac.rs>