HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

VPN servis putem SSL protokola

CCERT-PUBDOC-2003-11-47

CARNet CERT u suradnji s LS&S

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

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Tehnologije i rješenja koja korisnicima omogućuju udaljeni i "siguran" pristup informacijskim resursima putem nesigurne javne računalne mreže, kao što je Internet, sve su popularnije i traženije. Tradicionalna rješenja udaljenog pristupa više nisu dostatna, pogotovo ukoliko se u obzir uzmu strogi sigurnosni zahtjevi koji se danas postavljaju pred informacijske sustave. Povjerljivost, integritet i autentičnost podataka postali su neizbježni zahtjevi, pogotovo kada se radi o pristupu povjerljivim korporativnim podacima, čije otkrivanje predstavlja ozbiljan sigurnosni rizik. U doba kada je obavljanje poslovnih zadataka putem Interneta postalo dio svakodnevnice, problemi udaljenog pristupa još su naglašeniji.

Jedno od najpopularnijih rješenja koje se danas koristi u ovu svrhu su virtualne privatne računalne mreže (engl. *Virtual Private Networking*), tehnologija koja se bazira na konceptu tuneliranja mrežnog prometa, i koja je razvijena isključivo kako bi korisnicima omogućila udaljeni i siguran pristup internim resursima. Protokoli na kojima počiva tehnologija virtualnih privatnih računalnih mreža su IPSec, L2TP i PPTP, od kojih je IPSec trenutno najzastupljeniji. Na tržištu je danas dostupan velik broj komercijalnih rješenja koja omogućuju VPN pristup, a najpoznatija su ona velikih proizvođača kao što su Cisco, CheckPoint, NetScreen i dr. Postoji i nekoliko *open-source* projekata u ovome smjeru, ali su ona daleko manje popularna u odnosu na komercijalne proizvode. Osnovni razlog tome je činjenica što komercijalne tvrtke uz svoje proizvode nude kompletnu uslugu instalacije, održavanja i administracije sustava, što je posebno važno kod velikih tvrtki gdje uređaji moraju biti raspoloživi u svakom trenutku. Besplatna rješenja za sada ovakvu podršku ne nude, što im je osnovno ograničenje za širu primjenu. Jedan od najvećih nedostataka komercijalnih VPN proizvoda je njihova prilično visoka cijena (do nekoliko tisuća američkih dolara), što predstavlja ozbiljan problem za manje tvrtke, koje si tako velike troškove ne mogu priuštiti.

Jedno od alternativnih rješenja, koje može smanjiti troškove uvođenja i održavanja VPN sustava te ih na taj način približiti tvrtkama s manjim budžetom opisano je u nastavku dokumenta. Radi se o VPN rješenju baziranom na SSL protokolu, pri čemu se karakteristike istoga koriste u svrhu zaštite mrežnog prometa za vrijeme njegovog tranzita putem Interneta. Biti će opisani osnovni koncepti ove tehnologije, zajedno sa njenim prednostima i nedostatcima, kao i mogućnosti njene primjene.

2. Zahtjevi

Kako bi se uopće moglo raspravljati o prednostima, nedostatcima i ostalim problemima pojedinih tehnologija za pristup udaljenih korisnika, potrebno je ustanoviti koji su općeniti zahtjevi postavljeni pred takve sustave. Neki od njih biti će navedeni i ukratko opisani u nastavku poglavlja.

- **Sigurnost**

Bez obzira o kojem se rješenju ili tehnologiji radi, sustav udaljenog pristupa mora osigurati tzv. *end to end* sigurnost, od klijentske aplikacije za udaljeni pristup do resursa kojemu se pristupa. Sigurnosni problemi, prijetnje i rizici koji se javljaju u ovom smislu su višestruki. Potrebno je osigurati snažnu autentikaciju korisnika (engl. *authentication*), povjerljivost (engl. *confidentiality*) i integritet podataka (engl. *integrity*) koji se razmjenjuju, a također je potrebno voditi računa i o mehanizmima bilježenja i praćenja aktivnosti korisnika (engl. *accountability*). Sve su ovo aspekti o kojima je potrebno voditi računa ukoliko se želi implementirati pouzdan i kvalitetan sustav udaljenog pristupa te nisu nimalo jednostavni za rješavanje. Sigurnost sustava za udaljeni pristup posebno je osjetljivo područje informacijske sigurnosti, budući da se u slučaju kompromitiranja istog neovlaštenim korisnicima omogućuje izravan pristup internim resursima, što predstavlja neprihvatljiv sigurnosni rizik za organizaciju.

- **Jednostavnost korištenja**

Jednostavnost korištenja također je jedan od zahtjeva o kojem je potrebno voditi računa prilikom odabira i implementacije sustava za udaljeni pristup. Kompleksni i neintuitivni sustavi, komplicirani za korištenje, osim što će korisnicima otežati korištenje sustava, također ih može natjerati na zaobilaženje definiranih sigurnosnih mjera te korištenje alternativnih mehanizama udaljenog pristupa kojima se može ugroziti sigurnost ostatka sustava (npr. modemski *dial-in* pristup). Klijentska

aplikacija korisniku mora omogućiti jednostavno provođenje aktivnosti na udaljenom sustavu, slično kao što to čini kada se on nalazi na internoj računalnoj mreži.

- **Jednostavnost uvođenja, administracije i održavanja**

Inicijalno uvođenje (engl. *deployment*) i instalacija sustava, i na strani klijenta, i na strani poslužitelja (VPN koncentratora) mora biti što jednostavniji i vremenski što manje zahtjevan postupak. Pristup internim resursima trebao bi za korisnika biti što je moguće više transparentan te zahtijevati što manje interakcije u smislu održavanja i administracije klijentske aplikacije. Slično vrijedi i za dio sustava na strani organizacije. Složene i neintuitivne konfiguracije, osim što su sklone pogreškama koje mogu ozbiljno ugroziti sigurnost sustava u cjelini, također su i teške za uočavanje i otklanjanje. Važan faktor je i podrška proizvođača, pogotovo u okruženjima gdje je udaljeni pristup informacijama usko vezan uz obavljanje poslovnih zadataka, i gdje nemogućnost pristupa informacijama u danom trenutku predstavlja ozbiljne novčane gubitke.

- **Integracija s ostalim komponentama informacijskog sustava**

Kako bi se izbjegli suvišni problemi i nepotrebne izmjene u postojećoj konfiguraciji informacijskog sustava, poželjno je sustav za udaljeni pristup što više uskladiti sa postojećim tehnologijama i navikama korisnika. Uvođenje novih tehnologija i sustava, koje se znatno razlikuju u odnosu na postojeća rješenja, mogu unijeti brojne poteškoće, pogotovo u okruženjima s većim brojem korisnika. U obzir je također potrebno uzeti i pravila definirana sigurnosnom politikom i ostalim pravilnicima organizacije, budući da sustav mora biti u potpunosti u skladu s istima.
U nastavku dokumenta biti će pokazano kako se VPN sustavi bazirani na SSL protokolu uklapaju u navedene zahtjeve i na koji su način riješeni.

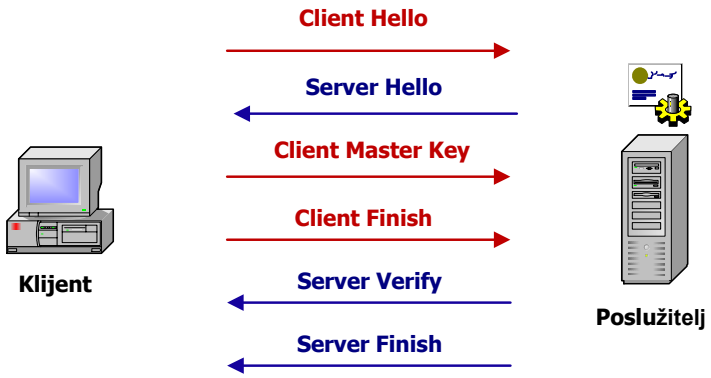
3. Secure Socket Layer

Implementacija VPN servisa putem SSL protokola bazira se na njegovim svojstvima koja osiguravaju povjerljivost, autentičnost i integritet podataka koji se razmjenjuju između klijenta i poslužitelja. Budući da je osnovna namjena VPN servisa osigurati sigurnu komunikaciju putem nesigurne javne mreže kao što je Internet, svojstva koja posjeduje SSL protokol čine ga idealnim za primjenu u ovakvim situacijama.
U ovome poglavlju ukratko je opisan način rada SSL (engl. *Secure Socket Layer*) protokola, kako bi se na taj način uočila njegova osnovna svojstva te mogućnost njihove primjene u svrhu implementacije VPN sustava.
SSL protokol razvijen je od strane tvrtke Netscape i danas je postao *de facto* standard za sigurnu komunikaciju putem Interneta. Prema OSI modelu SSL protokol nalazi se između aplikacijskog i transportnog sloja i kao takav nije isključivo vezan uz HTTP protokol, kao što se to vrlo često pogrešno pretpostavlja. Bez obzira što se HTTP danas najčešće koristi u kombinaciji sa SSL protokolom, isti je jednako tako moguće primijeniti i na bilo koji drugi servis.
U svrhu autentikacije, SSL protokol koristi svojstva asimetrične kriptografije (kriptografija javnog ključa, engl. *public key cryptography*), dok se za enkripciju podataka koriste svojstva simetrične kriptografije (kriptografija tajnog ključa, engl. *secret key cryptography*). Ovakav pristup danas je vrlo čest, budući da se njime iskorištavaju dobre, a uklanjaju loše strane oba pristupa. Problemi razmjene i dogovaranja ključeva rješavaju se korištenjem asimetrične kriptografije (infrastruktura javnog ključa, certifikati) , dok se problemi performansi rješavaju korištenjem simetričnih algoritama koji su poznati po znatno većim brzinama u odnosu na asimetrične algoritme, što ih čini pogodnima za enkripciju veće količine podataka.
U sljedećoj tablici (Tablica 1) navedeni su algoritmi i protokoli koje SSL protokol koristi u svrhu razmjene ključeva te osiguravanja integriteta i povjerljivosti podataka.

Razmjena ključeva	Povjerljivost	Integritet
- RSA - Diffie-Hellman - FORTEZZA	- RC4 - IDEA - DES, 3DES	- SHA - MD5

***Tablica 1** - Algoritmi i protokoli podržani od strane SSL algoritma*

U prvoj fazi komunikacije, jednim od navedenih algoritama za razmjenu ključa dogovara se tajni ključ sjednice (engl. *session key*), nagon čega se isti koristiti za šifriranje podataka u daljnjem tijeku komunikacije.
Na sljedećoj slici (Slika 1) dan je pojednostavljeni prikaz SSL komunikacije između klijenta i poslužitelja.

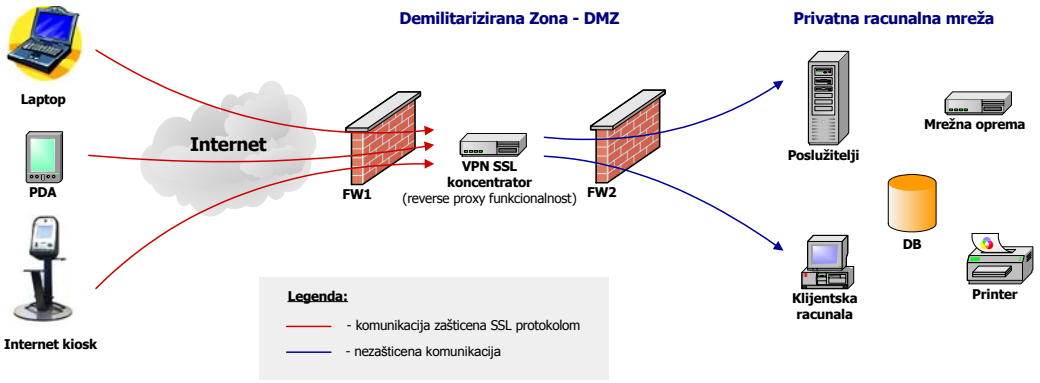


Slika 1: *SSL komunikacija*

U prvoj fazi komunikacije klijent i poslužitelj dogovaraju protokole koji će se koristiti za autentikaciju korisnika i enkripciju podataka (`Client Hello` i `Server Hello` paketi). U sklopu `Server Hello` paketa poslužitelj klijentu šalje certifikat u kojem se nalazi javni ključ poslužitelja, zajedno s ostalim podacima.
U sljedećoj fazi klijent odabire glavni ključ (engl. *master key*) na temelju kojeg će u narednom koraku i klijent i poslužitelj generirati simetrični ključ za enkripciju podataka. Odabrani ključ kriptira se javnim ključem poslužitelja, dobivenim iz primljenog certifikata, te se formira odgovarajući `Client Master Key` paket koji se vraća poslužitelju. Dobiveni paket poslužitelj dekriptira odgovarajućim tajnim ključem (koji je samo njemu poznat) te na temelju njega generira *session key* koji će se koristiti za enkripciju prometa. U sljedećem koraku poslužitelj klijentu vraća paket s kojim provjerava valjanost konekcije, a u istom koraku poslužitelj može zatražiti autentikaciju klijenta, ukoliko aplikacija to zahtjeva. Komunikacija se završava slanjem `Server Finish` paketa kojim poslužitelj dovršava ovu fazu komunikacije.
U ovom trenutku i klijent i poslužitelj posjeduju isti simetrični ključ, koji će se u kombinaciji sa odabranim algoritmom koristiti za enkripciju mrežnog prometa.

4. Princip rada

Osim SSL protokola, koji se koristi u svrhu autentikacije i enkripcije podataka, VPN SSL sustavi karakteristični su po tome što gotovo uvijek primjenjuju i tehnologiju reverznih *proxy* poslužitelja u svrhu ostvarivanja željene VPN funkcionalnosti. Radi se o konceptu vrlo sličnom onome kod klasičnih, tzv. *forward proxy* poslužitelja, ali u nešto drukčijem smislu i s nešto drukčijim ciljevima.
Za razliku od klasičnih *forward proxy* poslužitelja, koji se ponašaju kao posrednici za konekcije inicirane od strane klijenta prema poslužitelju, *reverse proxy* tehnologija koristi obrnuti pristup, otkuda i dolazi sam naziv reverzni *proxy* poslužitelj. U ovom slučaju *proxy* poslužitelj prima konekcije udaljenih klijenata te ih na temelju definiranih pravila prosljeđuje internim resursima. Ovakav pristup ima brojne prednosti (mogućnost raspoređivanja prometa prema opterećenju - *load balancing*, dodatni nivo zaštite prema internim resursima, mogućnost centralne kontrole pristupa, itd...), a pokazao se i dobrim rješenjem u svrhu implementacije VPN sustava putem SSL protokola.
Na sljedećoj slici (Slika 2) prikazan je koncept reverznih *proxy* poslužitelja, primijenjen na VPN SSL sustave.



Slika 2: *Primjena reverse proxy tehnologije na VPN SSL sustav*

Uloga VPN SSL uređaja u ovakvom scenariju je da udaljenim korisnicima omogući siguran i autorizirani pristup internim resursima organizacije. Korištenjem reverse *proxy* funkcionalnosti, zahtjevi klijenata presreću se na samom VPN SSL uređaju, gdje se nakon odgovarajućih provjera prosljeđuju internim resursima, odnosno servisima koje je klijent zatražio. Komunikacija između klijenta i VPN koncentratora (koja se odvija putem nesigurne javne mreže) zaštićena je SSL protokolom, dok se promet internom mrežom šalje u nekriptiranom obliku. Enkripcija, odnosno dekripcija mrežnog prometa, provodi se na samom VPN SSL koncentratoru, zajedno sa autentikacijom i autorizacijom korisnika.

Na vatrozidima je potrebno podesiti odgovarajuću sigurnosnu politiku, koja će pristup dozvoliti samo onim resursima i servisima kojima je to potrebno. Iako su na slici prikazana dva vatrozida, treba napomenuti da je istu funkcionalnost moguće postići korištenjem samo jednog vatrozida sa tri mrežna sučelja (interno, javno i DMZ) sučelje, pri čemu je VPN koncentrator potrebno postaviti u DMZ zonu, na isti način kao što je to prikazano na prethodnoj slici.

Iako ovakav pristup na prvi pogled djeluje prilično jednostavno i privlačno, u nastavku će biti pokazana ograničenja i nedostaci koja otežavaju širu primjenu ovakvih rješenja.

4.1. Prednosti

Jedna od najvećih prednosti VPN sustava baziranih na SSL protokolu je ta što ona ne zahtijevaju zasebnu klijentsku aplikaciju za pristup internim resursima organizacije. Dovoljan je Web preglednik sa ugrađenom SSL podrškom, što većina današnjih Web preglednika zadovoljava. To znači da je pristup moguć s bilo koje lokacije gdje postoji veza na Internet i mogućnost korištenja Web servisa (Web caffe, Internet kiosci, PDA uređaji i sl.). Kao što će se kasnije pokazati, ovakav pristup za sobom povlači brojne sigurnosne probleme koje je potrebno riješiti, ukoliko se sustav želi koristiti u široj primjeni.

Upotreba Web preglednika kao VPN klijenta automatski eliminira potrebu za konfiguracijom i održavanjem klijentske aplikacije, što također treba navesti kao jednu od prednosti. Iz navedenih podataka, može se zaključiti da je i cijena ovakvih rješenja nešto niža nego što je to slučaj kod klasičnih VPN sustava baziranih na IPSec protokolu.

Budući da VPN SSL sustavi koriste tehnologiju reverznih poslužitelja, također su naslijeđene sve njene prednosti koje svakako treba uzeti u obzir. Više informacija o reverznim *proxy* poslužiteljima, načinu njihova rada i mogućnostima primjene moguće je naći na CERT-ovim Web stranicama u dokumentu pod nazivom "Reverzni *proxy* poslužitelji", (www.cert.hr).

4.2. Nedostaci

Osim problema sigurnosti prisutnih na strani klijenta i poslužitelja (VPN koncentratora), koji će biti opisani poglavljima 5.1 i 5.2, SSL VPN tehnologija posjeduje nekoliko ozbiljnih tehničkih nedostataka koje treba napomenuti.

Na prvome mjestu treba spomenuti probleme pristupa aplikacijama koje nisu vezane uz HTTP (HTTPS) protokol, odnosno Web servis. Pristup Web aplikacijama i servisima putem VPN SSL tehnologije i ne donosi neka posebna poboljšanja, budući da je ista funkcionalnost sama po sebi već dostupna putem SSL protokola (enkripcija, integritet i autentičnost podataka). Mogućnosti raspodjele prometa prema opterećenju između različitih Web poslužitelja (engl. *load balancing*), centralna kontrola pristupa internim resursima te brojne druge prednosti koje donose reverzni *proxy* poslužitelji također ne predstavljaju veliku novost, budući da danas postoji velik broj aplikacija (komercijalnih i *open source*) koje nude iste funkcionalnosti.
Problem postoji u slučajevima kada je pristup potrebno osigurati drugim aplikacijama i servisima kao što su SAP, dijeljenje resursa, baze podataka i sl. U ovom segmentu brojni proizvodi su prilično ograničeni, a oni koji nisu najčešće zahtijevaju instalaciju određenih programa na strani klijenta. Ovaj problem se uglavnom rješava tako da se sa VPN koncentratora dohvati programski kod (najčešće u obliku *Java appleta*) koji će Web pregledniku dodati nove funkcionalnosti potrebne za pristup zatraženim resursima. Problem je posebno naglašen kod "nestandardiziranih" aplikacija i servisa razvijenih za specijalne primjene.

5. Sigurnosni problemi

U ovome poglavlju biti će opisani sigurnosni problemi koji se javljaju kod virtualnih privatnih računalnih mreža baziranih na SSL protokolu. Iako se ovakav način udaljenog pristupa na prvi pogled čini vrlo atraktivnim i praktičnim, u nastavku će biti navedeni neki od problema koji u ovakve sustave unose određeni sigurnosni rizik i o kojima je potrebno voditi računa prilikom implementacije konkretnih rješenja.
Problemi će biti podijeljeni u dvije skupine, od kojih jedna predstavlja probleme koji se javljaju na strani poslužitelja, odnosno VPN SSL koncentratora, a druga probleme na strani klijenta.

5.1. Sigurnosni problemi na strani poslužitelja

U nastavku će biti ukratko opisani neki od sigurnosnih problema koji su prisutni na strani VPN koncentratora, odnosno na strani privatne mreže organizacije.

- **Propuštanje prometa na vatrozidu**

Analizirajući primjer dan na prethodnoj slici (Slika 2) moguće je jasno uočiti kako se komunikacija između udaljenog korisnika i internih resursa može razložiti na dva dijela. Prvi je konekcija između udaljenog korisnika i VPN SSL koncentratora, dok drugi dio čini komunikacija između istog koncentratora i određenog internog resursa kojem korisnik pristupa.
Za svaki od internih servisa kojem se želi omogućiti pristup, potrebno je na vatrozidu koji odvaja DMZ zonu i internu mrežu (FW2 na gornjoj slici) propustiti odgovarajući promet. Ukoliko se radi o povjerljivim internim servisima kao što su MS Exchange, SAP, Active Directory, baze podataka i sl., propuštanje pripadajućih konekcija iz DMZ zone može biti vrlo opasno. Ukoliko neki od poslužitelja (ili sam VPN koncentrator) u DMZ zoni bude kompromitiran, neovlašteni korisnik imati će u tom slučaju mogućnost pristupa povjerljivim internim računalnim resursima, što predstavlja iznimno visok sigurnosni rizik. Osim toga, dozvoljavanje prometa prema kritičnim internim resursima predstavlja ozbiljno kršenje sigurnosne politike organizacije (ukoliko ista postoji), što je ujedno i nepremostivo ograničenje za implementaciju ovakvog rješenja.
Ove probleme moguće je riješiti korištenjem specijalnih arhitektura koje će omogućiti komunikaciju između udaljenih korisnika i internih resursa organizacije, a da se pritom na vatrozidu ne propušta "sumnjiv" promet koji predstavlja potencijalni sigurnosni rizik. Jedna od takovih arhitektura je tzv. Air Gap arhitektura, tehnologija koja omogućuje odvajanje interne i privatne računalne mreže, na način da se između njih dozvoljava samo razmjena podataka na aplikacijskoj razini. Zaglavlja paketa, kontrolne informacije, sumnjive naredbe i sl. automatski se blokiraju, čime se privatna mreža dodatno štiti od potencijalnih malicioznih aktivnosti. Komunikacija između internih i javnih resursa odvija se putem specijaliziranog uređaja s ugrađenom Air Gap funkcionalnošću, koji u jednom trenutku može komunicirati samo sa jednom od mreža s kojima je povezan. Podaci koji se razmjenjuju najčešće se zapisuju u RAM memoriju uređaja putem SCSI protokola, čime se dobiva na performansama. Više informacija o Air Gap tehnologiji moguće je naći na adresi http://www.giac.org/practical/gsec/Michael_Hurley_GSEC.pdf.

Budući da implementacija Air Gap sustava u određenoj mjeri komplicira stvari i unosi dodatne troškove (što je jedna od osnovnih prednosti VPN SSL sustava), opisani sigurnosni rizik ili se prihvaća, ili se primjenjuju manje zahtjevne metode njegovog umanjivanja. Ovakve metode najčešće uključuju dodatnu segmentaciju ili reorganizaciju strukture računalne mreže, korištenje samo neophodnih servisa za koje je moguće prihvatiti rizik, stroga kontrola i filtriranje prometa i sl.

- **Ranjivosti VPN SSL koncentratora**

Većina postojećih VPN SSL rješenja koristi neku vrstu Web poslužitelja na kojoj se bazira cijela arhitektura. Samim time, sve ranjivosti prisutne u programskom kodu Web poslužitelja (ili u bilo kojem drugom dijelu koda kojim je implementiran sustav) izravno utječu na sigurnost cijelog sustava. Ovaj problem posebno je naglašen, budući da kompromitiranje VPN SSL koncentratora neovlaštenom korisniku otvara iznimno velike mogućnosti za daljnje provođenje neovlaštenih aktivnosti. Identičan problem prisutan je i kod samog operacijskog sustava na kojem je sustav implementiran.
Iako danas postoji iznimno velik broj tehnika, alata i procedura za unaprjeđenje sigurnosti operacijski sustava, činjenica je da se novi sigurnosni propusti svakodnevno javljaju i da ove metode znaju vrlo često zakazati.
Još jedna od prijetnji vezana je uz činjenicu da neovlašteni korisnici mogu iskoristiti propuste u implementaciji, kojima će iskoristiti svojstva *proxy* poslužitelja te svoje maliciozne aktivnosti izravno usmjeriti na interne resurse. Ovakvi napadi mogu biti vrlo opasni i ukoliko su uspješno realizirani, mogu imati katastrofalne posljedice za organizaciju.
Od ovakvih problema najbolje se zaštititi redovitim i temeljitim održavanjem sustava, te strogom politikom filtriranja prometa prema VPN SSL koncentratoru. Potrebno je zabraniti sve potencijalno "sumnjive" konekcije te dozvoliti samo one koje su neophodne za ostvarivanje VPN komunikacije.

- **Autentikacija korisnika**

Općenito, kada se govori o mehanizmima udaljenog pristupa, jedan od vrlo važnih aspekata svakako je autentikacija korisnika. Budući da se radi o mogućnosti pristupa internim resursima organizacije, potrebno je realizirati kvalitetan sustav autentikacije korisnika, kojim će se provoditi pouzdana i snažna provjera identiteta. Ukoliko se uzme u obzir da VPN SSL sustavi pretpostavljaju pristup sa različitih lokacija, računala i IP adresa, ovaj je problem posebno važan.
U tom smislu preporučuje se korištenje snažnih metoda autentikacije upotrebom jednokratnih zaporki, tokena, pametnih kartica i sl. Također se preporučuje korištenje kombinacije dvije metode autentikacije korisnika, kako bi se na taj način smanjila mogućnost kompromitiranja sustava u slučaju da zakaže jedan od mehanizama.

- **Enkripcija podataka**

Budući da se podaci između udaljenog korisnika i privatne mreže razmjenjuju putem javne računalne infrastrukture (Internet), potrebno je na određeni način osigurati njihovu zaštitu od neovlaštenog promatranja. U slučaju SSL VPN sustava, enkripcija podataka postiže se korištenjem SSL protokola, opisanog u Poglavlju 5.
No, ono što je posebno važno, i što se vrlo često zaboravlja kada se govori o enkripciji i pripadajućoj zaštiti podataka, je činjenica da sama enkripcija ne vrijedi puno ukoliko nije pravilno implementirana. Korištenje snažnih algoritama i ključeva samo su neki od elemenata o kojima je potrebno voditi računa. Danas su dostupni brojni alati i tehnike koje omogućuju napadanje kriptografskih sustava te je stoga vrlo važno da se sustav načini otpornima na takve oblike napada. Loše i površno implementirani kriptografski sustav ostavlja lažan dojam sigurnosti, što može biti uzrok brojnih problema.

5.2. Sigurnosni problemi na strani klijenta

Slično kao i na strani poslužitelja, postoji skupina problema na strani klijenta, koja unosi određeni sigurnosni rizik u VPN sustave bazirane na SSL protokolu.

- **Problemi pohrane podataka na klijentskom računalu**

Jedan od ozbiljnijih sigurnosnih problema vezanih uz klijentsku stranu komunikacije je sam način pohranjivanja podataka na klijentskom računalu. Budući da je pristup moguć sa bilo koje javne lokacije koja posjeduje vezu na Internet i odgovarajući Web preglednik sa ugrađenom SSL podrškom (Internet kiosci, Intrenet kafići i sl.), ovaj je problem posebno izražen. Osim podataka kojima korisnik pristupa za vrijeme aktivne sjednice (datoteke, zapisi iz baza podataka, poslovni dokumenti i sl.),

također se misli i na podatke o samoj sjednici, budući da njihovo kompromitiranje neovlaštenom korisniku može omogućiti neautoriziran pristup sustavu. Ovaj problem identičan je onome vezanom uz upravljanje sjednicama kod Web aplikacija (engl. *Session Management*) i poznat je određeni broj napada koji iskorištavaju ovu ranjivost (Otimanje sjednica - *Session hijacking*, Lažiranje sjednica – *Session Spoofing*, Ponavljanje sjednica – *Session Replay* i sl.).
Još neki od podataka koji predstavljaju problem u ovom smislu su:

- URL adrese,
- privremene datoteke,
- Web kolačići,
- *history* podaci,
- vrijednosti polja Web formi i sl.

- **Maliciozni programi**

Opasnost od malicioznih programa (virusi, crvi, trojanski konji) sigurnosni je problem koji je dobro poznat i vrlo raširen, a prisutan je i kod VPN SSL sustava. U slučaju infekcije klijentskog računala, privatna mreža organizacije izravno je ugrožena, budući da se klijentsko računalo u tom trenutku tretira kao dio iste, što omogućuje jednostavno širenje malicioznih programa. Ukoliko se u obzir uzme činjenica da je pristup internim resursima moguć sa različitih "nepovjerljivih" lokacija, ovom problemu potrebno je posvetiti posebnu pažnju.
No, treba mati na umu jednu činjenicu koja umanjuje spomenuti problem. Budući da se udaljenim resursima u ovom slučaju pristupa putem Web preglednika i da se na taj način stvara siguran kanal između klijenta i poslužitelja, klasični maliciozni programi sami po sebi u ovom slučaju ne predstavljaju posebnu opasnost. No, uvijek treba imati na umu nove, modificirane i specijalno prilagođene inačice koje će znati iskoristiti ranjivosti u sustavu.

- **Otkrivanje informacija o internoj strukturi računalne mreže**

Budući da interne aplikacije i servisi mogu sadržavati informacije o ostalim internim resursima, koje inače nisu javno dostupne , korištenje SSL VPN sustava otvara mogućnost njihovog otkrivanja javnosti, što također predstavlja određeni sigurnosni rizik. Dolazak do ovakvih informacija, osim što neovlaštenom korisniku omogućuje preciznije usmjeravanje malicioznih aktivnosti, također omogućuje provođenje i tzv. *social engineering* napada.

6. Zaključak

Dokument opisuje VPN sustave bazirane na SSL protokolu, tehnologiju koja nudi alternativno rješenje sigurnog i udaljenog pristupa internim resursima u odnosu na postojeća VPN rješenja. Ideja se bazira na korištenju SSL protokola u svrhu ostvarivanja povjerljivosti, integriteta i autentičnosti podataka, a osnovna prednost joj je nešto niža cijena, te mogućnost pristupa putem standardnog Web preglednika sa ugrađenom SSL podrškom. Ovakvo rješenje umanjuje potrebu za instalacijom i održavanjem specijalizirane aplikacije na strani klijenta, a pristup sustavu moguće je ostvariti sa bilo koje lokacije koja ima vezu na Internet i odgovarajući Web preglednik. Osim navedenih prednosti, analize su pokazale da ovakav koncept VPN sustava posjeduje odgovarajuće nedostatke koji ograničavaju njegovu širu primjenu. Jedan od potencijalnih problema su brojna sigurnosna pitanja prisutna i na strani klijenta, i na strani poslužitelja, dok su drugi vezani uz probleme pristupa specijaliziranim aplikacijama kao što su npr. SAP, baze podataka i sl.
Može se zaključiti da se radi o vrlo zanimljivom i perspektivnom konceptu udaljenog pristupa, ali da još uvijek treba riješiti neke od navedenih problema, kako bi njegova upotreba zaživjela u punom smislu.

7. Reference

SANS, www.sans.org/rr/wp/SSL_VPN.pdf
Reviews: SSL VPNs, http://www.linuxsecurity.com/articles/network_security_article-8358.html
Aventail, http://www.aventail.com/
Alteon, http://www.nortelnetworks.com/products/01/alteon/sslvpn/