CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Virtual Network Computing

NCERT-PUBDOC-2010-03-295

Nacionalni CERT

u suradnji s

LSS

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

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

Nacionalni 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

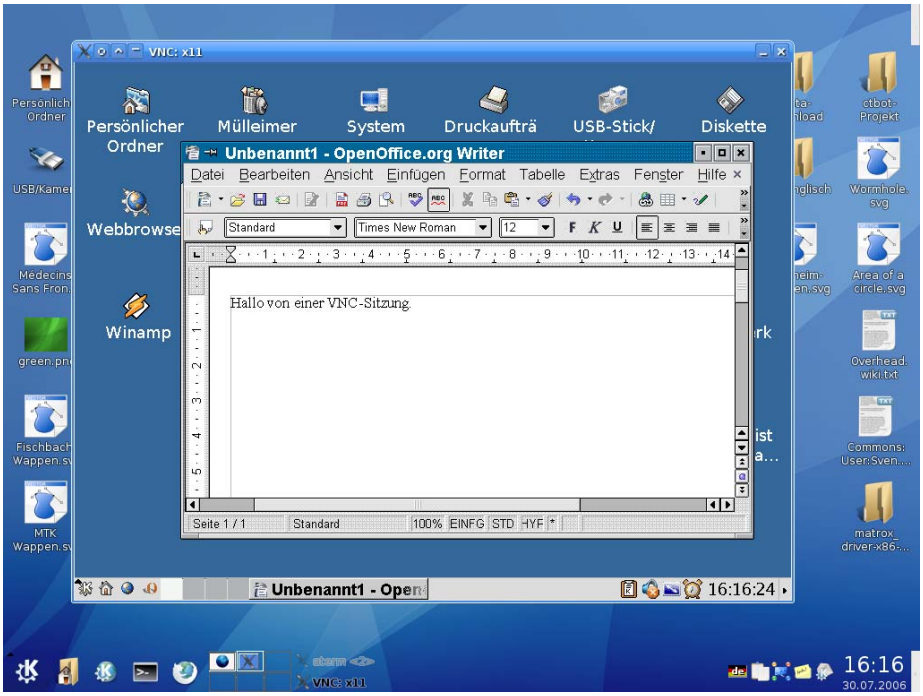
U svojim svakodnevnim situacijama korisnici računala često imaju potrebu pristupiti udaljenim računalima kako bi ostvarili prijenos datoteka, ispisali dokumente na daljinu ili odradili neki drugu korisnu radnju. Upravo zato su razvijeni posebni sustavi namijenjeni udaljenom spajanju te kontroli zaslona i događaja na udaljenom računalu. Jedan od takvih sustava je VNC (eng. *Virtual Network Computing*) sustav zasnovan na RFB (eng. *remote framebuffer*) protokolu. Radi se o vrlo jednostavnom protokolu koji obavlja prijenos događaja između klijenta i poslužitelja te definira smještaj prenesenih podataka na zaslonu. Sadrži mnoge metode kodiranja koje omogućavaju bolje iskorištavanje resursa mreže jer klijent i poslužitelj sve parametre veze dogovaraju prije njene uspostave.

Implementacija opisanog sustava zahtjeva puno pažnje, kao i provođenje određenih sigurnosnih mjera. Od razvoja prvih inačica otkriveni su neki sigurnosni problemi poput mogućnosti otkrivanja osjetljivih podataka (npr. korisničke lozinke). Kao jedno od mogućih rješenja ovih sigurnosnih nepravilnosti nameće se primjena SSH (eng. *Secure Shell*) protokola. Radi se o uspostavljanju tunela između poslužitelja i klijenta te prijenosu podataka na sigurniji način. Razvijene su mnoge programske implementacije VNC sustava poput aplikacija RealVNC, TightVNC, UltraVNC i EchoVNC. Svaka od ovih aplikacija sadrži brojne napredne značajke za udaljeni rad, ali i neke ozbiljne sigurnosne rizike. Takve nedostatke u implementaciji i dizajnu napadači mogu zlouporabiti za pokretanje proizvoljnog programskog koda, izvođenje DoS (eng. *Denial of Service*) napada ili povećanje prava na sustavu. Osim VNC-a, postoje sustavi sa sličnim funkcijama, a to su RDP (eng. *Remote Desktop Protocol*) i ICA (eng. *Independent Computing Architecture*). Osim sličnih namjena i funkcionalnosti, oni sadrže slične sigurnosne nedostatke kao i VNC sustav.

Ovaj dokument donosi opis funkcionalnosti, sigurnosnih problema i implementacija VNC sustava. Također, predstavljene su osnovne programske implementacije zajedno s njihovim sigurnosnim nedostacima. Na kraju su dani opisi sustava RDP i ICA, kao i usporedba s VNC implementacijama te osvrt na očekivani razvoj u budućnosti.

2. Virtual Network Computing

VNC (eng. *Virtual Network Computing*) je sustav za udaljeno povezivanje koji koristi RFB (eng. *remote framebuffer*) protokol za upravljanje udaljenim računalom. On obavlja prijenos događaja s jednog računala (npr. ulaza s tipkovnice ili miša) na drugo omogućavajući prikaz promjena na zaslonu. Neovisan je o platformi, što znači da se VNC preglednik na jednom operacijskom sustavu može povezati s VNC poslužiteljem na istom ili bilo kojem drugom operacijskom sustavu. Također, više korisnika može se povezati s istim VNC poslužiteljem istovremeno. Popularna uporaba ove tehnologije uključuje udaljenu tehničku podršku i pristup datotekama na radnom računalu s kućnog računala. Primjer sučelja prikazan je na Slika 1.



Slika 1. Sučelje VNC sustava
Izvor: Wikipedia

2.1. Povijest

Sustav VNC je kreiran u laboratoriju ORL (Olivetti & Oracle Research Lab) koji je tada bio u vlasništvu korporacije „Olivetti and Oracle Corporation". 1999. godine organizacija AT&T preuzela je laboratorij te tri godine kasnije obustavila istraživački projekt iz kojeg je VNC nastao. Nakon zatvaranja projekta nekoliko stručnjaka koji su radili na njemu osnovalo je tvrtku RealVNC kako bi nastavili razvijati VNC program (komercijalna inačica i inačica otvorenog koda). Neki od članova tima koji su nastavili razvoj proizvoda su Tristan Richardson (izumitelj), Andy Harter (vođa projekta), James Weatherall i Andy Hopper.

Razvoj VNC sustava potaknula je želja da se proširi funkcionalnost prikaza korisničkog sučelja na udaljenim računalima. Prva inačica ovog sustava, tzv. *Teleporting System*, bila je ograničena značajkama X sustava (računalni program koji pruža grafičko korisničko sučelje za umrežena računala) iz kojeg je inicijalno i razvijen. Nekoliko godina kasnije, ORL je razvio Videotile kao *ultra-thin-client* tehnologiju. Radi se o uređaju s LCD zaslonom, olovkom i ATM (eng. *Asynchronous Transfer Mode*) mrežnom vezom. Dizajniran je za prikaz video zapisa visoke kvalitete te interakciju s aplikacijama. Najveći problem ovog rješenja bila je uporaba velike količine resursa što ja zahtijevalo dodatne izmjene u aplikaciji. Time je omogućeno tretiranje video zapisa na način da se prenose samo oni dijelovi koji se mijenjaju, a ideja je dalje razvijena u prvi VNC sustav.

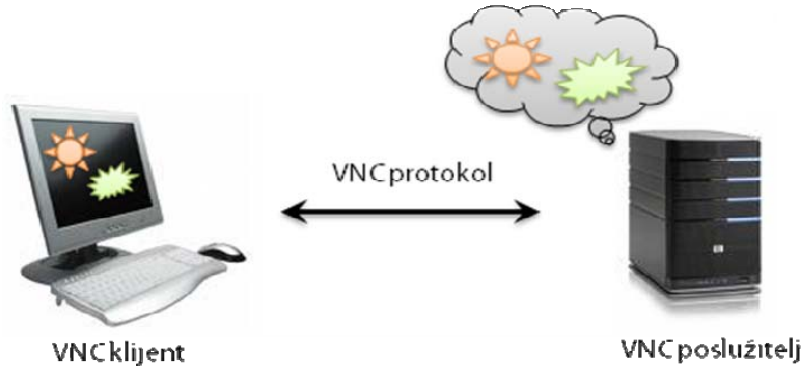
Nekoliko besplatnih i komercijalnih inačica VNC-a razvijeno je iz originalnog GNU GPL izvornog koda. Ipak, izraz VNC je danas registrirana oznaka za RealVNC Ltd.

2.2. Opis

Jedan VNC sustav sastoji se od tri komponente (Slika 2):

1. VNC poslužitelj – program na računalu koji služi za pružanje kontrole klijentu.
2. VNC klijent (ili preglednik) – program koji služi za pregled, kontrolu i interakciju s poslužiteljem.
3. VNC protokol – RFB protokol, vrlo jednostavni protokol za prijenos slike ili poruka o događajima između poslužitelja i klijenta.

Komunikacija se odvija tako da se klijent poveže s poslužiteljem preko priključka (obično 5900). Alternativa je povezivanje preglednika s poslužiteljem kada se koristi priključak 5800, ili povezivanje poslužitelja s klijentom u „modu za slušanje" na priključku 5500. Prednost tog načina rada je što poslužiteljska strana ne mora imati konfiguriran vatrozid za omogućavanje pristupa na priključku 5900 ili 5800.



Slika 2. Komponente VNC sustava

Poslužitelj šalje male podatkovne blokove (eng. *rectangles of the framebuffer*) klijentu. U najjednostavnijem obliku VNC protokol koristi puno resursa pa su razvijene metode kodiranja tj. efikasnijeg prijenosa podataka. VNC protokol omogućuje klijentu i poslužitelju dogovaranje oko metode kodiranja koja će se koristiti. Najjednostavnije kodiranje, koje podržavaju svi klijenti i poslužitelji, je kodiranje reda (eng. raw encoding). Radi se o metodi kod koje se podaci o pikselu (najmanji grafički element slike) šalju u redoslijedu od lijeve strane prema desnoj, a nakon slanja cijele slike šalju se samo dijelovi koji se mijenjaju. Ovo kodiranje je korisno i efikasno samo ako se mali dijelovi slike mijenjaju od okvira do okvira. To je slučaj kod pomicanja miša na statičnoj pozadini ili upisa teksta u okvir. Međutim, kod velikih promjena slike, kao kod pregleda video zapisa, ova metoda postaje neuporabljiva.

Uporaba VNC-a preko Interneta je moguća ako korisnik ima širokopojasnu vezu na strani klijenta i poslužitelja Međutim, kako bi se ostvarila veza ponekad je potrebno konfigurirati NAT (eng. *Network Address Translation*), vatrozid ili usmjeritelj. Neki korisnici mogu odabrati uporabu VPN (eng. *Virtual Private Network*) mreža za lakše korištenje VNC-a preko Interneta. Alternativno, VNC veza može se ostvariti kao LAN (eng. *Local Area Network*) veza.

2.3. RFB protokol

RFB je jednostavan protokol za udaljeni pristup računalu koji pruža grafičko korisničko sučelje. Budući da je implementiran na tzv. *framebuffer* razini (logički sloj za prikaz grafičkih promjena na uređajima), dostupan je za sve sustave (X11 za Linux, Windows i Macintosh inačice) te aplikacije. Proširen je s dodatnim značajkama (poput funkcije prijenosa podataka) i puno sofisticiranijim postupcima za kompresiju te sigurnosnim tehnikama. Kako bi se omogućila kompatibilnost više različitih inačica klijenata i poslužitelja, uveden je postupak dogovaranja parametara veze prije povezivanja. Pri tome klijent i poslužitelj dogovaraju inačicu RFB kodiranja, najprikladniju kompresiju i najbolje sigurnosne opcije koje podržavaju obje strane.

Protokol je prvotno razvijen kao tehnologija za udaljene zaslone koju bi koristio klijent s ATM (eng. Asynchronous Transfer Mode) vezom. Sljedeću i najznačajniju ulogu, protokol RFB pronašao je u VNC sustavu kada je objavljen kao slobodan i besplatan za uporabu.

2.3.1. Rukovanje podacima i sjednicom

Dio protokola za prikaz podataka izveden je prema jednostavnom pravilu:

```
Smjestiti pravokutnik piksela podataka na danu x,y poziciju.
```

Na prvi pogled, ovo pravilo izgleda kao nepraktičan način prikaza nekih komponenata korisničkog sučelja. Međutim, upravo ovakav način rukovanja podacima omogućava razne sheme za kodiranje piksela što pruža veliki stupanj fleksibilnosti u odrađivanju parametara poput brzine obrade podataka poslužitelja i klijenta. Osnovni postupci kodiranja zajedno s podacima koje koriste prikazani su u Tablica 1.

Kodiranje	Opis
Kodiranje reda (eng. *row encoding*)	Kodiranje niza piksela od lijeva prema desno.
CopyRect kodiranje	Kodiranje x,y koordinata kao podataka s koje pozicije treba kopirati piksele podataka.
RSE kodiranje	Kodiranje podjelom pravokutnika piksela u grupe s jednakom vrijednošću.
Hextile kodiranje	Kodiranje podjelom pravokutnika piksela u područja 16x16 bita.
ZRLE kodiranje	Kodiranje područja veličine 64x64 piksela uz uporabu kompresije.
Pseudo-kodiranje	Opis
Pokazivač (eng. *cursor*)	Kodiranje koje omogućava lokalno iscrtavanje pokazivača miša.
DesktopSize	Kodiranje koje omogućava izmjenu veličine zaslona.

Tablica 1. Vrste kodiranja

Unos podataka temelji se na modelu standardne radne stanice s tipkovnicom ili sličnim ulaznim uređajem. Klijent šalje ulazne događaje poslužitelju svaki put kada korisnik pritisne neku tipku ili pomakne miša. Međutim, ulazni događaji mogu biti sintetizirani s nekog nestandardnog ulazno/izlaznog uređaja. Na primjer, moguće je koristiti uređaj sličan olovci koja se koristi na zaslonu, a služi za generiranje događaja.

Kako bi se uspostavila veza između poslužitelja i klijenta, poslužitelj prvo zahtjeva autentikaciju klijenta koristeći shemu zahtjev-odgovor. Korisnik se autenticira preko klijenta upisom lozinke. Nakon uspostave veze, poslužitelj i klijent izmjenjuju poruke kako bi dogovorili veličinu zaslona, format piksela i metodu kodiranja. Kada klijent primi podatke za potpuni prikaz, sjednica počinje. Bilo koja strana u komunikaciji može inicirati prekid sjednice u bilo kojem trenutku.

3. Sigurnosni aspekti VNC sustava

Protokol VNC je po svojoj prirodi nesiguran. Usmjeren je na učinkovit prijenos poruka između korisnika i poslužitelja. Postupci autentikacije i šifriranja nisu uključeni u izvornu inačicu protokola. Ranije inačice su posebno ranjive na otkrivanje osjetljivih podataka ili njihovo dešifriranje. Kako bi se podigla razina sigurnosti moguće je uspostaviti komunikaciju preko protokola SSH (eng. *Secure Shell*).

3.1. Dešifriranje lozinki

Prije uspostave veze između poslužitelja i klijenta, korisnik mora proći postupak autentikacije upisom odgovarajuće lozinke. Ovo pruža napadaču mogućnost napada dešifriranjem lozinki.

Kao jedna od osnovnih metoda dešifriranja lozinki javlja se tzv. *brute force* napad. Radi se o napadu koji se koristi kao strategija dešifriranja podataka isprobavanjem svih mogućih kombinacija ključa dok se ne „pogodi" točan. Uspješnost ovih napada uvelike ovisi o duljini lozinke koju se želi dešifrirati. Ključ duljine n bita sadrži 2^n mogućih ključeva. Prema tome se vidi kako broj ključeva jako raste povećanjem broja bitova lozinke. Smatra se kako je broj operacija (2^{128}) potreban za proboj ključa od 128 bita neizvediv u stvarnom vremenu uz uporabu svih konvencionalnih tehnika digitalnih računala. Ipak, rastom mogućnosti obrade kod suvremenih računala postaje moguće izvesti neke napredne algoritme (poput Groverovog algoritma [22]) kako bi se ugrozila sigurnost ovakvih lozinki. Zbog toga stručnjaci savjetuju uporabu ključeva duljine 256 bita, tj. korištenje lozinki duljine 8 znakova. Neke inačice VNC sustava zahtjevaju uporabu lozinki duljine od najmanje 8 znakova, dok se kod ostalih to samo preporuča.

Osim izvođenja *brute force* napada, napadač može ostvariti pristup računalu žrtve te otkriti lozinku zapisanu u operacijskom sustavu korisnika, točnije u registrima u slučaju Windows operacijskih sustava. Razvijeni su neki alati koji omogućuju dešifriranje takvih oblika lozinki.

Alat VNCPwdump omogućuje otkrivanje i dešifriranje ključa u registrima koji sadrže kriptirane VNC lozinke. Dešifriranje se obavlja na nekoliko načina:

- odbacivanje trenutnog korisničkog ključa u registrima,
- otkrivanje ključa iz datoteke „NTUSER.DAT",
- dešifriranje naredbe koja sadrži kriptiranu lozinku te
- pokretanje VNC procesa i odbacivanje lozinke korisnika.

Novije inačice alata sadrže funkcionalnost izmjene lozinki, a više informacija moguće je naći na stranici:

http://www.cqure.net/wp/index.php?s=vnc

Također, Jonas Piela je objavio programski kod koji služi za dešifriranje istih lozinki zahvaljujući ranjivostima VNC sustava.

http://www.jonaspiela.de/code.html#vncdec

3.2. Šifriranje komunikacije

Šifriranje je proces transformacije informacija uporabom nekog algoritma kako bi se one učinile razumljivim samo onim korisnicima kojima su namijenjene. Provodi se uporabom određenog ključa, a rezultat postupka je šifrirana poruka. Svaki korisnik koji poznaje ključ može pokrenuti obrnuti postupak te dešifrirati izvornu poruku. Koristi se za zaštitu podataka od nedozvoljenog pregledavanja.

Rad VNC sustava zasniva se na prijenosu podataka preko mreže. Na takve podatke nužno je primijeniti neki postupak šifriranja kako bi se spriječilo njihovo presretanje. Komercijalne inačice VNC sustava uglavnom sadrže funkcionalnost šifriranja podataka za prijenos, dok se kod besplatnih inačica ne provodi nikakvo šifriranje.

Slika 3 prikazuje situaciju gdje je implementirana zaštita komunikacije. Napadač koji presreće komunikaciju ne može dešifrirati poruke.

Slika 3. Šifriranje komunikacije kod VNC-a

Šifriranje štiti povjerljivost poruke, ali potrebne su dodatne tehnike za zaštitu integriteta i autentikaciju. Također, vrlo je važno pravilno primijeniti postupak šifriranja kako bi se navedeni zahtjevi ostvarili.

3.3. Osjetljivi podaci

Osjetljive informacije su one informacije čije otkrivanje neovlaštenim ili nepovjerljivim korisnicima može rezultirati smanjenjem razine sigurnosti sustava. Gubitak, izmjena ili neautorizirani pristup osjetljivim informacijama može utjecati na privatnost individualnih, poslovnih ili trgovačkih tajni. Ovisno o prirodi i osjetljivosti podataka, napadač može uzrokovati neznatnu, ali i veliku štetu organizaciji ili pojedincu.

Zaštita osjetljivih podataka mora spriječiti (Slika 4):

- neautorizirani pristup – mogućnost pregleda podataka,
- neautoriziranu uporabu – uporaba podataka na sustavu (npr. njihovo umnožavanje),
- prekid – nemogućnost pristupa podacima za legitimne korisnike,
- izmjenu – izmjena podataka pohranjenih na sustavu,
- uništavanje – brisanje ili neki drugi oblik trajnog uništavanja podataka.

Slika 4. Zaštita osjetljivih podataka

Inačice VNC sustava do 4.0 nisu vodile računa o sigurnoj pohrani podataka. Novije inačice sustava pohranjuju povjerljive podatke (poput lozinki) s odgovarajućim sigurnosnim pravima pristupa kako bi se spriječio pristup neautoriziranim korisnicima.

3.4. Zaštita komunikacije preko SSH protokola

VNC sustav koristi metodu zahtjev-odgovor za pružanje osnovne autentikacije koja omogućava povezivanje klijenta i poslužitelja. Ovakva metoda ne zahtjeva prijenos lozinki preko mreže što predstavlja dobru praksu u zaštiti sustava. Ipak, nakon uspostavljanja komunikacije ne pruža se nikakva vrsta šifriranja prometa. Napadač pri tome ima mogućnost snimanja ili presretanja svih poruka koje se izmjenjuju između poslužitelja i klijenta. Kako bi se izbjegao ovaj problem, moguće je zaštititi komunikaciju uporabom SSH protokola.

SSH protokol je mrežni protokol koji omogućava razmjenu podataka uporabom sigurne veze između dva mrežna uređaja. Šifriranje koje se koristi kod protokola SSH pruža povjerljivost i integritet podataka preko nesigurnih mreža (poput Interneta). U osnovi je razvijen za operacijske sustave Unix, dok za platforme Windows, Mac i sl. postoje samo komercijalne inačice poslužitelja. Međutim, korisnici koji koriste operacijske sustave Windows mogu implementirati usmjeravanje prometa preko Unix računala kako bi zaobišli ovaj problem.

3.4.1. Implementacija i obilježja

SSH protokol obično pruža prozor za prijavu na udaljenom računalu. Sav promet je šifriran između dva računala uporabom tehnika šifriranja uz javni ključ što otežava napade kriptoanalize (dešifriranja poruke bez poznavanja ključa). Nakon instalacije, računalu je moguće pristupiti preko SSH klijenta, a za uspješno povezivanje korisnik mora upisati ispravnu lozinku.

VNC protokol obično koristi priključak 59xx, gdje „xx“ predstavlja broj zaslona na poslužitelju. Ukoliko je VNC poslužitelj pokrenut na platformi Windows, obično se koristi priključak 5900.

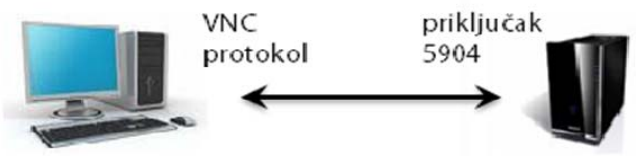
Osim toga, SSH protokol ima neka dodatna obilježja poput:

- zahtijevanja slušanja na određenom priključku lokalnog računala te prosljeđivanje prometa preko sigurne mreže,
- mogućnosti kompresije podataka – korisno ako je veza između korisnika i poslužitelja spora (poput modemske), ali može povećati brzinu prijenosa i kod nešto bržih mreža te
- prosljeđivanja prometa na treće računalo koje ne sadrži VNC poslužitelj.

3.4.2. Uporaba na Windows sustavima

U slučaju uporabe operacijskog sustava Windows, korisnici mogu implementirati usmjeravanje preko računala s Unix platformom. Razlog tomu je postojanje besplatnih inačica SSH klijenta i poslužitelja za Unix platforme.

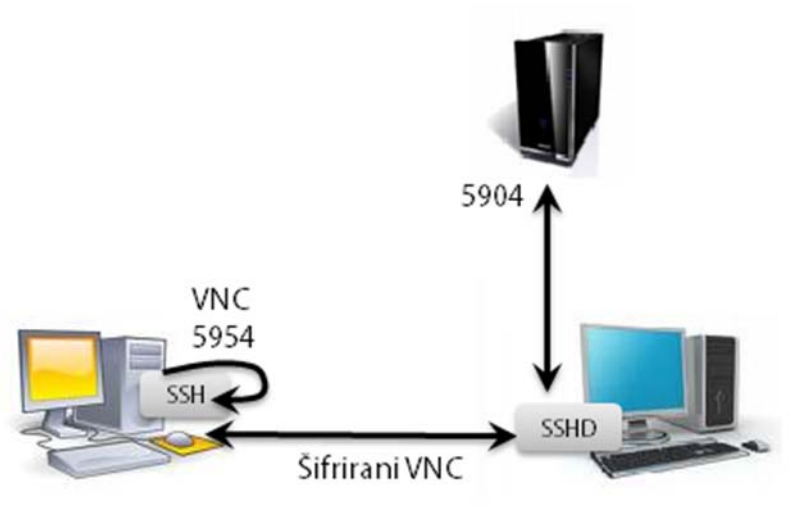
Slika 5 prikazuje slučaj izravnog povezivanja računala s operacijskim sustavom Windows i VNC poslužitelja. Vidljivo je kako se povezivanje odvija preko priključka 5904 i nesigurne veze. Ukoliko napadač presretne komunikaciju između klijenta i poslužitelja, on ima pristup svom sadržaju koji se prenosi u nešifriranom obliku.



Slika 5. Izravno povezivanje bez SSH

Ako se želi uvesti zaštita preko SSH protokola potrebno je iskoristiti dodatno računalo s operacijskim sustavom Unix. Korisnik (*localhost*) se tada povezuje s proizvoljnim priključkom, na primjer 5954. Protokol SSH se koristi za tuneliranje (preusmjeravanje priključaka) do „pomoćnog“

Unix računala te računala s VNC poslužiteljem (na priključak 5904) što rezultira šifriranom, sigurnom vezom. Kako bi opisani postupak funkcionirao, na pomoćnom računalu mora biti pokrenut servis *sshd* (eng. *Secure Shell Daemon*). Radi se o upravljačkom programu za protokol SSH. Komunikacije se dalje odvija preko lokalnog prosljeđivanja (eng. *local forward*) jer je na korisničkom računalu stvoren „lažni" priključak. Opisani scenarij prikazan je na Slika 6.



Slika 6. Zaštita komunikacije preko protokola SSH

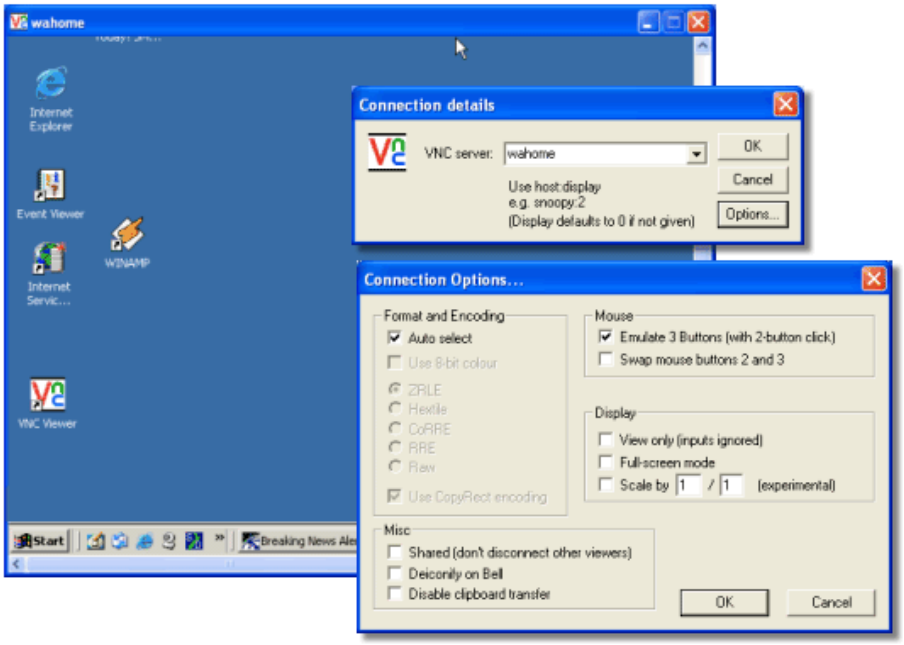
Lokalno prosljeđivanje omogućuje uspostavu sigurne SSH sjednice i tuneliranje proizvoljne TCP (eng. *Transmission Control Protocol*) veze preko nje. Tunel je moguće kreirati bilo kada što ga čini vrlo efikasnim. Budući da se radi o lokalnom prosljeđivanju, priključak je dostupan samo računalu na kojem je pokrenuto prosljeđivanje. To znači da druga računala ne mogu pristupiti tom priključku.

4. Programske implementacije

Originalna AT&T inačica VNC sustava nije više u širokoj uporabi jer su razvijene različite inačice s brojnim poboljšanjima. U nastavku su dani primjeri nekoliko besplatnih i komercijalnih implementacija VNC sustava.

4.1. RealVNC

RealVNC je aplikacija koja implementira VNC protokol za udaljenu kontrolu zaslona računala. Razvijen je za operacijske sustave Windows, Mac OS X te brojne sustave zasnovane na Unix platformi, kao i za Java i iPhone platforme. Sučelje aplikacije prikazano je na Slika 7.



Slika 7. RealVNC
Izvor: freeware365

Navedena aplikacija dolazi u tri inačice:

1. Besplatna inačica (eng. *Free Edition*) – inačica otvorenog programskog koda licencirana GNU GPL (eng. *General Public License*) licencom. Razvijena je za platforme Unix (Linux, Solaris, HP-UX, AIX) i Windows. Opisana inačica aplikacije je dosta zastarjela, posebno ona za sustave Windows.
2. Osobna inačica (eng. *Personal Edition*) – komercijalna inačica namijenjena malim poduzećima ili korisnicima. Uključuje postupke autentikacije i šifriranja, ali razvijena je samo za operacijske sustave Windows.
3. Poslovna inačica (eng. *Enterprise Edition*) – komercijalna inačica razvijena za velika poduzeća. Ima ugrađene postupke napredne autentikacije i šifriranja, a može se koristiti na sustavima Windows, Mac OS X te raznih sustavima zasnovanim na Unix i Linux platformama.

Trenutne inačice komercijalnih aplikacija uključuju:

- podršku za HTTP (eng. *HyperText Transfer Protocol*) posrednički poslužitelj,
- adresar,
- mogućnost izmjene poruka u stvarnom vremenu (eng. *chat*),
- udaljen ispis dokumenata i
- poruke s obavijestima o stanju na vezi.

Detaljnija usporedba značajki opisanih inačica dana je u tablici 2.

Značajka	Besplatna inačica	Osobna inačica	Poslovna inačica
Kompatibilnost s besplatnom inačicom	+	+	+
Windows NT 4, 2000, XP, Server 2003	+	+	+
Windows Vista, Server 2008	-	+	+
Unix (Linux, Solaris, HP-UX, AIX)	+	-	+
Mac OSX (x86 i PPC)	-	-	+
Autentifikacija preko RSA	-	+	+
Šifriranje sjednice preko AES-a	-	+	+
Udaljen ispis dokumenata	-	+	+
One-port HTTP	-	+	+
Podrška za HTTP posrednički poslužitelj	-	+	+
Pomoć i podrška korisnicima	-	+	+
Prijenos datoteka	-	+	+
Integrirani adresar	-	+	+
Prijenos poruka u stvarnom vremenu	-	+	+
Izmjena veličine zaslona	-	+	+
Alati za razvoj (samo platforme Windows)	-	-	+

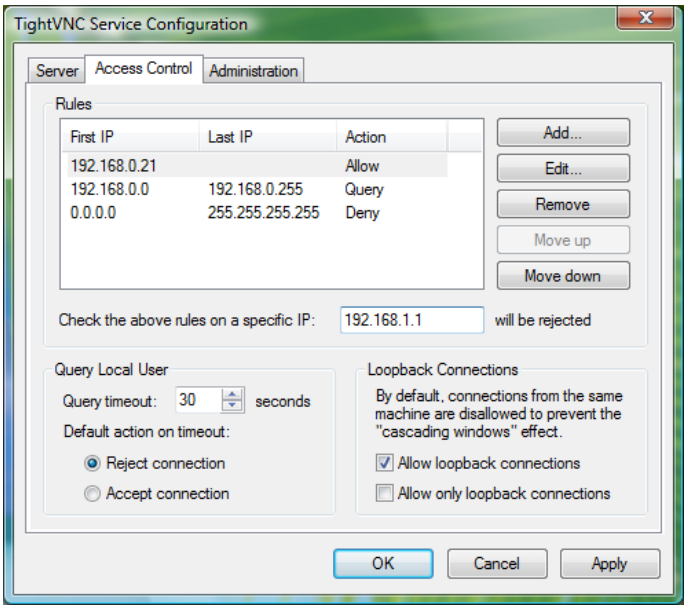
Tablica 2. Usporedba inačica aplikacije RealVNC

4.2. TightVNC

TightVNC je aplikacija otvorenog koda koja koristi i proširuje RFB protokol za upravljanje zaslonom na udaljenom računalu. Osnovno obilježje ove aplikacije je novi oblik kodiranja, tzv. *tight encoding* koje daje bolje performanse VNC vezama. Radi se o efektivnoj kombinaciji JPEG kompresije i drugih oblika kodiranja. Budući da ovaj oblik kodiranja ne podržava većina današnjih sustava, potrebno je koristiti aplikaciju TightVNC na oba računala koja komuniciraju. Sučelje za konfiguraciju aplikacije TightVNC prikazuje Slika 8.

Opisana aplikacija također uključuje:

- mogućnost prenošenja datoteka,
- podršku za upravljački program Windows DFMirage kako bi se detektirala promjena na zaslonu,
- mogućnost povećanja slike (eng. *zoom*) i
- automatsko tuneliranje preko SSH protokola na Unix platformama.



Slika 8. Aplikacija TightVNC
Izvor: TightVNC

Neke aplikacije nastale iz aplikacije TightVNC su:

1. RemoteVNC – sadrži dodatne funkcije automatskog omogućavanja NAT sustava i vatrozida.
2. TightVNC Portable Edition – prijenosa inačica programa koja je također i komercijalna.
3. TigerVNC – preuzima poboljšanja iz aplikacije TurboVNC.

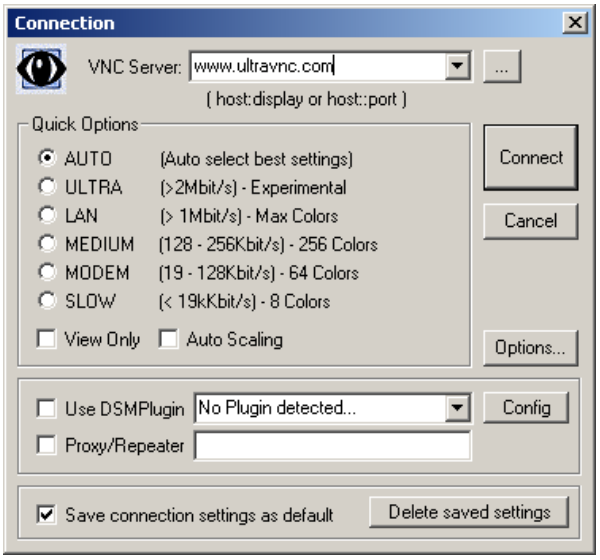
4.3. UltraVNC

UltraVNC je aplikacija otvorenog koda za operacijske sustave Windows koja koristi protokol VNC za kontrolu zaslona na udaljenom računalu. Distribuirana je pod GNU GPL licencom, a razvijena u programskim jezicima C, C++ i Java.

Sadrži sljedeća obilježja:

- dodatak za šifriranje veze između klijenta i poslužitelja,
- podršku za prijenos datoteka,
- funkcije za izmjenu poruka u stvarnom vremenu te
- razne metode autentikacije.

Slika 9 daje prikaz klijentskog dijela aplikacije UltraVNC prilikom uspostave veze s udaljenim računalom.



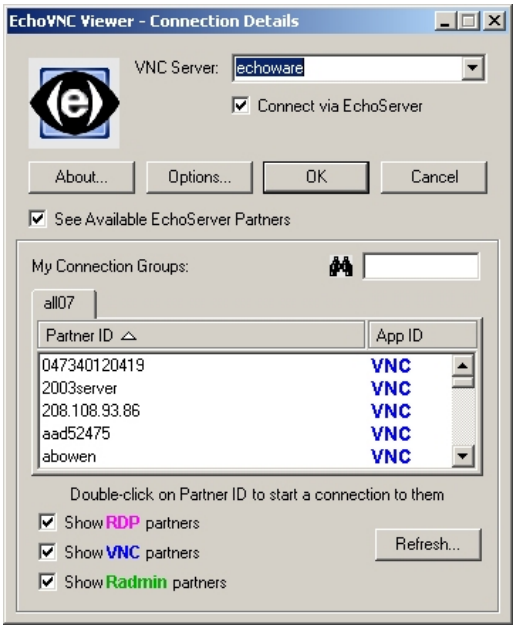
Slika 9. Aplikacija UltraVNC
Izvor: UltraVNC

4.4. EchoVNC

EchoVNC je alat otvorenog koda za udaljenu kontrolu zaslona nekog računala. Sadrži podršku za protokole VNC i RDP (eng. *Remote Desktop*) te RAdmin poslužitelj i preglednik. Razvijen je za platforme Windows i Mac OS X, a veze se mogu ostvariti bez obzira na konfiguraciju vatrozida, usmjeritelja ili posredničkog web poslužitelja. Na Slika 10 prikazano je sučelje ovog alata.

Alat EchoVNC razlikuje se od ranije opisanih aplikacija i ostalih VNC platformi po dvije značajke:

- Razvijen je skupom alata echoWare kako bi se dobila veza između poslužitelja i klijenta koja ne ovisi o značajkama vatrozida.
- Omogućuje veze s drugim uslugama za udaljeno upravljanje zaslonom uključujući druge poslužitelje VNC, RDP te RAdmin.



Slika 10. Alat EchoVNC
Izvor: sourceforge

4.5. Sigurnosni nedostaci

4.5.1. Pokretanje proizvoljnog programskog koda

Pokretanje proizvoljnog programskog koda označava mogućnost napadača da pokrene bilo koju naredbu na ciljanom računalu ili u ciljanom procesu. Napadač obično dobije tu mogućnost iskorištavanjem nekih od nedostataka u sustavu. Većina tih ranjivosti omogućava pokretanje strojnog koda, ali neke se mogu iskoristiti i za pokretanje malih dijelova koda koji pak kao posljedicu imaju mogućnost pokretanja bilo kojeg koda (npr. pokretanje prozora za unos naredbi).

Najopasniji utjecaj koji iskorištavanje ovakvih ranjivosti može imati je napadačevo potpuno preuzimanje kontrole nad ranjivim procesom. To mu dalje daje i mogućnost preuzimanja kontrole nad cijelim ranjivim sustavom.

Napad se obično izvodi izmjenom zapisa u PC (eng. *program counter*) brojaču pokrenutog procesa. Riječ je o brojaču koji označava koju naredbu proces treba izvesti. Kontroliranje vrijednosti tog brojača omogućava kontrolu nad time koja se naredba izvodi sljedeća. Prema tome, nakon umetanja zlonamjernog koda, napadač mijenja vrijednost PC brojača. Budući da brojač pokazuje na umetnuti kod, on se automatski pokreće.

Ranjivosti koje su omogućavale pokretanje proizvoljnog programskog koda kod VNC programa su:

- Pogreška u provjeri podataka RFB protokola koji dolaze s poslužitelja kod paketa RealVNC.
- Neispravno rukovanje određenim oblicima kodiranja u paketu RealVNC.
- Nepravilnost u funkciji „CMsgReader::readRect“ VNC preglednika u paketima RealVNC VNC Free Edition inačice 4.0 do 4.1.2, Enterprise Edition inačice E4.0 do E4.4.2 i Personal Edition inačice P4.0 do P4.4.2.
- Neodgovarajuća provjera ulaznih vrijednosti komponente „vncviewer“ u radu paketa RealVNC.
- Pojava cjelobrojnog prepisivanja u datoteci „ClientConnection.cpp“ kod paketa TightVNC koja se očituje prilikom povezivanja sa zlonamjernim poslužiteljem.
- Prepisivanje memorije u funkciji „ClientConnection::NegotiateProtocolVersion“ prilikom uporabe paketa UltraVNC u slučaju rada u „LISTENING“ načinu ili korištenja DSM dodatka.
- Ranjivosti koje uzrokuju nepravilno određivanje veličine spremnika na stogu kod paketa UltraVNC i TightVNC.
- Pojava prepisivanja memorije zbog nepravilne provjere podataka koje unosi korisnik prije njihova kopiranja u spremnike neodgovarajuće veličine kod paketa EchoVNC inačica prije 1.1.2.
- Prepisivanje memorije uređene po principu stoga u datoteci „echoware/Logger.cpp“ u paketu EchoVNC inačica prije 1.1.2.

4.5.2. DoS napad

DoS (eng. Denial of Service) je napad u kojem se pokušava učiniti računalne resurse nedostupnim za njihove legitimne korisnike. U osnovi se sastoji od napora jednog ili više napadača da spriječe efikasno funkcioniranje (privremeno ili trajno) Internet stranice ili usluge. Ciljevi napada su obično popularni i često korišteni web poslužitelji poput onih u vlasništvu banaka ili važnih državnih tijela.

DoS napadi se provode navođenjem ciljanog računala na ponovno pokretanje (eng. *restart*) ili na iskorištavanje svih raspoloživih računalnih resursa čime se onemogućava ispravan rad sa ostalim klijentima. Osnovna metoda napada je slanje velikog broja zahtjeva za uspostavu komunikacije prema ciljanom poslužitelju kako ono ne bi moglo odgovoriti na upite drugih (legitimnih) korisnika (ili bi komunikacija s drugim korisnicima trajala jako dugo). Opisani scenarij prikazuje Slika 11.

Slika 11. DoS napad

Ranjivosti koje su omogućile DoS napad kod implementacija VNC sustava:

- Neodgovarajuća provjera ulaznih podataka kod komponente „vncviewer“ paketa RealVNC.
- Pogreška u datoteci „common/rfb/CMsgReader.cxx“ prilikom obrade nekih tipova kodiranja podataka u paketu RealVNC inačica 4.x.
- Višestruke pogreške u funkcijama „ClientConnection::CheckBufferSize()“ i „ClientConnection::CheckFileZipBufferSize()“ koje uzrokuju cjelobrojno prepisivanje kod paketa TightVNC.
- Pojava prepisivanja memorije u funkciji „ClientConnection::NegotiateProtocolVersion“ datoteke „vncviewer/ClientConnection.cpp“ kod paketa UltraVNC.
- Pogreška u definiranju granica pri unosu korisničkih podataka koja izaziva prepisivanje memorije u paketu EchoVNC.

4.5.3. Povećanje prava na sustavu

Povećanje prava na sustavu je čin iskorištavanja ranjivosti ili pogreške u dizajnu programa kako bi se pristupilo resursima koji su inače zaštićeni. Rezultat uspješnog napada je izvođenje akcija s višim korisničkim pravima. Pojavljuje se kod sustava koji sadrže nedostatke koji mogu dovesti do zaobilaženja definiranih sigurnosnih prava na sustavu. Ovakvi napadi predstavljaju vrlo ozbiljan problem jer mogu rezultirati zlouporabom podataka ili sustava.

Ranjivosti koje omogućavaju povećanje prava na sustavu u paketima koji implementiraju VNC protokol su:

- Pogreška u rukovanju zahtjevima za autentifikacijskom lozinkom omogućuje zaobilaženje autentifikacije te pristup bez poznavanja VNC lozinke. Ovaj propust uočen je kod paketa Real VNC inačica 4.x.
- Nepravilnosti u postupku dogovaranja postupka autentifikacije između klijenta i poslužitelja kod paketa RealVNC.
- Nepravilnosti u implementaciji protokola RFB omogućuju klijentu navođenje poslužitelja na nekorištenje autentifikacije u paketu RealVNC.
- Pogreška u obradi konfiguracijske naredbe „QueryAllowNoPass“ kod poslužitelja paketa TightVNC.
- Pojave cjelobrojnog prepisivanja kod više funkcija paketa TightVNC.

- Nepravilnost u datoteci „echoware/Logger.cpp“ koja se manifestira pojavom prepisivanja memorije u radu paketa EchoVNC.

Važno je napomenuti kako su svi pobrojani sigurnosni propusti uočeni u starijim inačicama navedenih programskih paketa. U najnovijim inačicama svi ti propusti su ispravljeni, ali kako se svakodnevno otkrivaju novi, svim korisnicima se savjetuje instalacija objavljenih zakrpi kao i praćenje informacija koje se objavljuju na referentnim izvorima. Također, poželjno je implementirati i dodatne elemente zaštite (poput definiranja IP adresa s kojih se korisnik smije spajati) kako bi se povećala razina sigurnosti cijelog sustava.

5. Ostali sustavi za udaljeno spajanje na računalo

5.1. RDP sustav

RDP (eng. *Remote Desktop Protocol*) protokol razvila je tvrtka Microsoft, a služi za pružanje grafičkog sučelja na udaljenom računalu. Razvijen je za većinu inačica operacijskog sustava Windows, ali i za platforme Linux, Unix, Mac OS X te druge moderne operacijske sustave. Svaka inačica operacijskog sustava Windows nakon inačice XP uključuje RDP klijent i poslužitelj programe.

Prva inačica RDP protokola, pod nazivom Terminal Services, razvijena je prema specifikaciji ITU-T T.128 koja definira protokol za dijeljene aplikacije. Ova je inačica bila sastavni dio paketa Windows NT 4.0 Server, Terminal Server Edition. U operacijski sustav Windows XP Professional uključena je inačica 5.1., pod nazivom RDP, koja sadrži podršku za 24-bitne boje i zvukove. Najnovija inačica (7.0) izdana je u srpnju 2009. godine, a uključena je u pakete Windows Server 2008 R2 i Windows 7. Ova je inačica donijela mnoge napredne funkcionalnosti poput podrške za više zaslona.

Osnovna obilježja nove inačice RDP paketa su:

- podrška za 8-bitne, 15-bitne, 16-bitne, 24-bitne i 32-bitne boje,
- šifriranje preko algoritma RC4 uz uporabu ključa duljine 128 bita,
- funkcija „*Audio Redirection*“ – pokretanje audio programa na udaljenom računalu te prenošenje zvuka na lokalno računalo,
- funkcija „*File System Redirection*“ – uporaba lokalnih datoteka na udaljenom računalu,
- funkcija „*Printer Redirection*“ – mogućnost uporabe lokalnog pisača,
- funkcija „*Port Redirection*“ – mogućnost aplikacije izravno pristupi lokalnim serijskim i paralelnim priključcima,
- mogućnost razmjene sadržaja preko funkcije „*clipboard*“ između lokalnog i udaljenog računala,
- funkcionalnost „*Seamless Windows*“ – udaljene aplikacije moguće je pokrenuti na računalu koje sadrži RDP vezu.
- NLA (eng. *Network Level Authentication*) – tehnologija koja zahtjeva autentikaciju prije uspostave sjednice s poslužiteljem.
- podrška za udaljene „*Aero Glass*“ teme,
- podrška za Windows PE (eng. *Presentation Foundation*) aplikacije,
- podrška za protokol TLS (eng. *Transport Layer Security*) 1.0 na klijentu i poslužitelju te
- podrška za više zaslona.

5.1.1. Sigurnost

RDP koristi šifriranje što ga čini dosta pouzdanijim od mnogih jednostavnih VNC implementacija. Međutim, bez dodatnih sigurnosnih mjera ranjiv je na MITM (eng. *man-in-the-middle*) napad, aktivno prisluškivanje u kojem napadač uspostavlja veze s žrtvama te ih navodi da misle kako komuniciraju izravno. Razlog tomu je što ne koristi certifikate za autentikaciju poslužitelja. Znači, ukoliko se korisnik poveže se udaljenim poslužiteljem, ne postoji sigurnost da se sadržaj ne bilježi na nekom sustavu koji se nalazi između klijenta i poslužitelja. te da su lozinke sigurne (iako je sjednica šifrirana).

Na sustavima Windows XP nije ugrađena podrška za certifikate u RDP pa je potrebno upotrijebiti SSH tuneliranje preko VNC veza. Međutim, Windows Server 2003 pruža podršku za autentikaciju preko TLS protokola.

Još jedna ranjivost kod sustava RDP vezana je uz samu implementaciju protokola, a omogućava napadaču pokretanje DoS (eng. *Denial of Service*) napada. Problem se javlja u načinu rukovanja zahtjevima udaljenog računala, a moguće ga je zlouporabiti preko posebno oblikovanih zahtjeva.

Nepravilnosti u dizajnu RDP protokola donose još neke sigurnosne probleme kao što su. otkrivanje informacija o sadržaju kriptiranih paketa preko sume za provjeru (eng. *checksums*). Zahvaljujući tome, napadač ima mogućnost pregleda paketa te manipulacije prometom.

Kako bi se izbjegli opisani propusti, korisnicima se preporuča primjena odgovarajuće nadogradnje te pravilna konfiguracija postavki za autentifikaciju i šifriranje komunikacije.

5.1.2. Programske implementacije

Jedna od implementacija RDP protokola je *rdesktop*, besplatni klijent otvorenog programskog koda prikazan na Slika 12. Distribuiran je pod GNU GPL licencom i dostupan za sustave temeljene na platformi Unix (poput BSD-a ili neke od inačica Linuxa).

Uključuje sljedeće značajke:

- preusmjeravanje priključaka,
- korištenjem proizvoljne konfiguracije tipaka na tipkovnici (znakovi se ispravno prenose bez obzira na raspored tipki na tipkovnici klijenta),
- kompresiju i šifriranje prometa,
- automatsku autentikaciju,
- podršku za pametne kartice.

Slika 12. Rdesktop
Izvor: Sun Microsystems

Još jedna od implementacija istog protokola je poslužitelj *xrdp* koji se temelji na aplikaciji *rdesktop*. Radi se o implementaciji otvorenog koda čiji je cilj stvaranje poslužitelja za operacijski sustav Linux sa svim potrebnim funkcijama za povezivanje s RDP klijentom.

5.2. ICA sustav

ICA (eng. *Independent Computing Architecture*) je protokol koje je razvila tvrtka Citrix Systems za razmjenu podataka između poslužitelja i klijenta. Neovisan je o platformi, a sadrži funkcije slične sustavu X Windows System.

Osnovna obilježja ICA sustava su:

- Neovisnost o platformi – primjenjivost na razne sustave uključujući UNIX, Linux, Macintosh, Java, Symbian OS, PocketPC, Windows CE, OS/2 i MS-DOS uz mogućnost pristupa aplikacijama temeljenim na platformama Windows, Java i Unix s gotovo svakog uređaja.
- Jedinstveni klijent – rad sa posljednjim Windows, Unix i Java aplikacijama uz mogućnost razvoja dijela klijentskog programa.
- Neovisnost o protokolu – dizajniran za ran preko svih standardnih protokola uključujući TCP/IP, NetBEUI, NetBIOS i IPX/SPX te komunikacijskih protokola PPP, ISDN, Frame Relay, ATM te raznih bežičnih protokola.
- Podrška na klijentu – ICA podržava skoro sve tipove uređaja.
- Prilagodba stanju na vezi – uporaba malo mrežnih resursa.

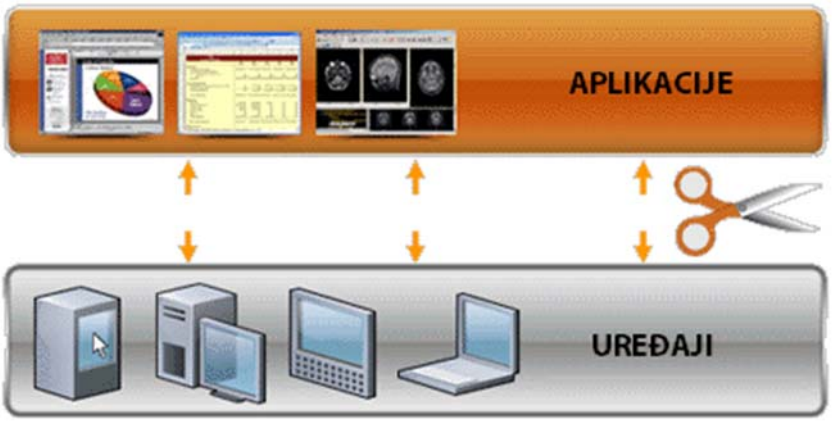
5.2.1. Sigurnost

Prve inačice protokola ICA uključivale su slabe algoritme za šifriranje kako bi se zaštitila korisnička autentikacija. Radi se o jednostavnom algoritmu koji se zasniva na XOR funkciji pa može biti jednostavno probijen. Uspješan napad omogućuje snimanje lozinki te pregled prometa koji izmjenjuju klijent i poslužitelj. Osim toga, moguće je izvesti MITM napade ili krađu sjednice (iskorištavanje valjanje sjednice za povećanje prava pristupa informacijama ili uslugama na računalnom sustavu). Kasnije su uvedene sigurnije inačice šifriranja koje koriste algoritam Diffie-Hellman (kriptografski protokol koji omogućava uspostavu sigurnog dijeljenog ključa preko nesigurne mreže između dvije strane) za razmjenu ključa i RC5 za šifriranje prometa. Međutim, iako ovi algoritmi daju dodatnu razinu sigurnosti, i dalje predstavljaju slabu točku za MITM napade.

Također, javljaju se dodatni sigurnosni problemi ukoliko se koriste protokoli TLS ili SSL za zaštitu autentikacije. Napadač ga može iskoristiti stvaranjem posebno oblikovanog certifikata kako bi uspješno oponašao neki SSL/TLS poslužitelj. Ovo omogućuje lažiranje identiteta poslužitelja.

5.2.2. Programske implementacije

Najpoznatija implementacija opisanog protokola je aplikacija Citrix XenApp koja omogućuje povezivanje s korporativnim aplikacijama. Može posluživati aplikacije na središnjem poslužitelju ili omogućiti korisnicima udaljenu interakciju s njima. Osnovno svojstvo je upravo razdvajanje korisničkog sučelja od obrade aplikacija koje se nalaze na središnjem poslužitelju (Slika 13).



Slika 13. Razdvajanje aplikacija i uređaja
Izvor: Ipsintegration

Za razliku od VNC protokola, umjesto grafičkih informacija obavlja se prijenos informacija s razine prikaza (slično kao kod protokola X11). Aplikacija je dostupna za nekoliko operacijskih sustava uključujući Microsoft Windows, Mac OS, Linux te druge zasnovane na platformi Unix (HP-UX, Solaris, AIX). Uključuje podršku za protokole TCP, HTTP, HTTPS, SMB te CIFS. Postoji web inačica

klijenta, besplatno dostupna na Internetu, pod nazivom „Web Interface for XenApp“. Koristi se za pružanje ICA posredničkog poslužitelja preko HTTPS protokola.

Još jedna implementacija protokola ICA je program AnywhereTS, namijenjen operacijskim sustavima Microsoft Windows.

Osnovna obilježja:

- pretvaranje računala u tzv. *thin* klijenta,
- pokretanje klijenta s tvrdog diska, CD (eng. *Compact Disk*) ili USB (eng. *Universal Serial Bus*) uređaja,
- pokretanje preko mreže uporabom okruženja PXE (eng. *Preboot eXecution Environment*),
- ugrađeni TFTP (eng. *Trivial File Transfer Protocol*) i DHCP (eng. Dynamic *Host Configuration Protocol*) poslužitelji,
- podrška za RDP i ICA protokole,
- preusmjeravanje zvuka i serijskih priključaka i
- preusmjeravanje na USB uređaj.

5.3. Usporedba s VNC implementacijama

Slika 1Tablica 3 daje usporedbu svih opisanih implementacija protokola VNC, RDP i ICA. Većina sustava pruža osnovnu zaštitu komunikacije putem šifriranja podataka (osim nekih besplatnih inačica paketa). Također,skoro svi paketi sadrže podršku za neke napredne funkcionalnosti poput višestruke sjednice te prijenos datoteka. Za razliku od tih značajki, samo neki paketi (rdesktop, Citrix XenApp te AnywhereTS) uključuju podršku za prijenos zvučnih zapisa.

Većina paketa implementira klijenta i poslužitelja, dok paketi rdesktop i AnywhereTS omogućuju samo klijentski dio, a xrdp poslužiteljski.

Paket	Šifriranje	Prijenos datoteka	Audio podrška	Višestruke sjednice	Klijent/ Poslužitelj
RealVNC besplatna inačica	-	.	-	+	+
RealVNC osobna inačica	AES-128	+	-	+	+
RealVNC poslovna inačica	AES-128	+	-	+	+
TightVNC	-	+	-	+	+
UltraVNC	uz dodatak	+	-	+	+
EchoVNC	+	+	-	+	+
Rdesktop	+	+	+	+	samo klijent
xrdp	+	-	-	+	samo poslužitelj
Citrix XenApp	SSL, TLS	+	+	+	+
AnywhereTS	SSL, TLS	+	+	+	samo klijent

Tablica 3. Usporedba sustava

6. Očekivanja u budućnosti

Sustavi za udaljenu kontrolu računala razvijaju se vrlo brzo te postaju zastupljeni na gotovo svim platformama. Već sada neke inačice sadrže podršku za većinu modernih operacijskih sustava, a očekuje se usmjeravanje razvoja prema mobilnim i sličnim uređajima. Razlog tome je sve veća uporaba takvih uređaja za pristup Internetu i uslugama koje on nudi. Udaljeni pristup računalima te upravljanje zaslonom omogućilo bi korisnicima rad neovisno o položaju te pružilo veću pokretljivost i prenosivost usluga. Osim primjenjivosti na nove platforme, sustavi će uključivati podršku za povezivanje s raznim sustavima i implementacijama drugih protokola za udaljeni rad.

Također, većina sustava usmjerava se prema adekvatnoj zaštiti podataka. U budućnosti se očekuje razvoj sigurnijih sustava koji imaju ugrađene pouzdanije metode autentikacije i šifriranja. Razlog tomu je pronalaženje postupaka za probijanje popularnih kriptografskih algoritama te implementacija novih tehnika za snimanje prometa, krađu podataka ili izvođenje nekih drugih napada na komunikaciju, podatke i sustav.

Očekuje se i ugradnja dodatnih naprednih funkcionalnosti kao što su prijenos audio zapisa s udaljenih računala ili ispis datoteka na drugim računalima. Takve značajke čine sustave privlačnim korisnicima, ali i efikasnim i primjenjivim u raznim situacijama za razne potrebe. Međutim, uz razvoj sustava koji će sadržavati sve opisane pozitivne značajke, može se očekivati i veći broj komercijalnih inačica ovakvih sustava.

7. Zaključak

Sustavi za udaljeno spajanje na računalo ili VNC sustavi donose mnoge napredne funkcionalnosti. Neke od važnijih su mogućnost sigurnog prijenosa datoteka, podrška za višestruke sjednice te razmjena audio zapisa. Ovakve funkcije korisnicima omogućavaju jednostavno i efikasno obavljanje raznih aktivnosti na udaljenim računalima. Dostanu prednost uporabi ovakvih sustava donosi zastupljenost na gotovo svim poznatijim operacijskim sustavima. Uz to, većina implementacija uključuje neovisnost o platformi što znači da je moguće ostvariti konekcije sa sustavima zasnovanim na sličnim protokolima ili primijenjenim na druge platforme.

Osim prednosti koje donose sofisticiranim funkcijama, ovi sustavi nose i određene sigurnosne rizike. Među ozbiljnijima je mogućnost dešifriranja komunikacije koja se razmjenjuje preko mreže između klijenta i poslužitelja. Zlouporabom takvih propusta napadači bi mogli presresti komunikaciju te saznati sadržaj na udaljenom računalu. Kako bi se spriječili napadi usmjereni na otkrivanje prometa između klijenta i korisnika moguće je komunikaciju provoditi kroz sigurnije veze. Riječ je o primjeni SSH protokola koji omogućuje uspostavu sigurnog tunela kroz nesigurnu mrežu te prosljeđivanje svog prometa kroz taj tunel. Osim spomenutog VNC sustava, slične funkcije ali i slične ranjivosti sadrže i sustavi RDP i ICA. Znači, kako bi korisnik nekog sustava zaštitio podatke koje izmjenjuje preko mreže, savjetuje se uspostava sigurnih veza bez obzira na razinu šifriranja ugrađenu u sustave.

Daljnjim razvojem ovih proizvoda očekuje se umjeravanje prema modernim uređajima (poput mobilnih uređaja). Također, očekuje se implementacija sigurnijih algoritama za šifriranje komunikacije i veća razina zaštite svih podataka koji se koriste pri radu. Međutim, razvoj naprednijih alata za udaljeni rad mogao bi donijeti i komercijalizaciju sada besplatnih inačica.

8. Reference

[1] VNC, http://en.wikipedia.org/wiki/Vnc, ožujak, 2010.

[2] Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper, Virtual Network Computing, http://www.cl.cam.ac.uk/research/dtg/attarchive/pub/docs/att/tr.98.1.pdf, IEEE Internet Computing, siječanj/veljača, 1998.

[3] RFB protokol, http://en.wikipedia.org/wiki/RFB, ožujak, 2010.

[4] Tristan Richardson, The RFB Protocol, http://www.realvnc.com/docs/rfbproto.pdf, RealVNCLtd, studeni, 2009.

[5] Making VNC more secure using SSH, http://www.hep.phy.cam.ac.uk/vnc_docs/sshvnc.html, ožujak, 2010.

[6] Securing your VNC connection using SSH, http://www.linux-tip.net/cms/content/view/333/26/, prosinac, 2007.

[7] RealVNC, http://en.wikipedia.org/wiki/RealVNC, ožujak, 2010.

[8] TightVNC, http://en.wikipedia.org/wiki/TightVNC, ožujak, 2010.

[9] UltraVNC, http://en.wikipedia.org/wiki/UltraVNC, ožujak, 2010.

[10] EchoVNC, http://en.wikipedia.org/wiki/EchoVNC, ožujak, 2010.

[11] RealVNC nedostatak, http://secunia.com/advisories/20107/, svibanj, 2005.

[12] VNC nedostatak, http://www.coresecurity.com/content/vnc-integer-overflows, veljača, 2009.

[13] RealVNC propust, http://isc.sans.org/diary.html?storyid=1331, svibanj, 2006.

[14] RDP, http://en.wikipedia.org/wiki/Remote_Desktop_Protocol, ožujak, 2010.

[15] Massimiliano Montoro, Remote Desktop Protocol, the Good the Bad and the Ugly, http://www.oxid.it/downloads/rdp-gbu.pdf, svibanj, 2005.

[16] rdesktop, http://en.wikipedia.org/wiki/Rdesktop, ožujak, 2010.

[17] xrdp, http://en.wikipedia.org/wiki/Xrdp, ožujak, 2010.

[18] Citrix XenApp, http://en.wikipedia.org/wiki/Citrix_XenApp, ožujak, 2010.

[19] AnywhereTS, http://en.wikipedia.org/wiki/AnywhereTS, ožujak, 2010.

[20] ICA, http://en.wikipedia.org/wiki/Independent_Computing_Architecture, ožujak, 2010.

[21] Comparison of remote desktop software, http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software, ožujak, 2010.

[22] Grover-ov algoritam, ožujak, 2010, http://en.wikipedia.org/wiki/Grover%27s_algorithm