Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Matěj Vaněček

Nástroje pro vzdálenou správu a jejich využití

Remote control tools and theirs usage

Bakalářská práce

Praha 2009-08-11

Vedoucí bakalářské práce: Mgr. Jan Pokorný, Ph.D.

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze, 11.8. 2009

……..

podpis studenta

Identifikační záznam

VANĚČEK, Matěj. *Nástroje pro vzdálenou správu a jejich využití [Remote control tools and theirs usage]*. Praha, 2009. 46 s. Bakalářská práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Mgr. Jan Pokorný, Ph.D.

Abstrakt

Tématem bakalářské práce je vzdálená správa počítačů. Práce popisuje nástroje a technologie, které lze pro vzdálenou správu použít. Zároveň uvádí přímé zkušenosti se vzdálenou správou a její vliv na současnou a budoucí podobu informační společnosti. Bakalářská práce je rozdělena do šesti hlavních kapitol, které jsou rozděleny dle oblastí použití nástrojů vzdálené správy. Úvodní kapitola se zabývá uvedením do problematiky vzdálené správy. Druhá kapitola shrnuje tuto problematiku v operačních systémech Microsoft Windows. Třetí kapitola je věnována vzdálené správě operačních systémů platformy UNIX. Čtvrtá kapitola představuje další technologie vzdálené správy, které lze využít. Pátá kapitola mapuje webové nástroje vycházející ze vzdálené správy. V rámci kapitoly je též provedeno praktické srovnání. Závěrečná kapitola shrnuje problematiku vzdálené správy v prostředí moderních komunikačních zařízení, které ilustruje obrazovými přílohami.

Abstract

The aim of this bachelor thesis is to discuss the available methods for remote administration. It also provides experiences with remote administration tools and theirs impact on information society. Thesis is divided into six main chapters, which are divided according to areas of useability of remote administration tools. The first chapter is entry into the remote administration. The second chapter summarizes this issue in Microsoft Windows operating systems. The third chapter is about the remote administration in UNIX operating systems. The fourth chapter presents additional remote administration technologies. The fifth chapter is about webtools that are based on the remote administration. Some practical comparison is also as part of this chapter. The final chapter summarizes the issues of remote administration in modern communication devices.

Klíčová slova/Keywords

vzdálená administrace, vzdálená plocha, vzdálená správa, remote administration, remote control, remote desktop, telecontrol, teleoperation

Obsah

Předmluva

Bakalářská práce analyzuje způsoby využití informačních technologií v procesech, které se dají zahrnout pod společný jmenovatel vzdálená správa.

Zpracování tématu bakalářské práce probíhalo v několika fázích. Tématem vzdálené správy jsem se již částečně zabýval ve druhém ročníku bakalářského studia v rámci výběrové přednášky *ICT* (Information and Communication Technologies) *pro provoz informačních zdrojů*. Součástí atestace předmětu bylo vypracování seminární práce. Zde jsem se věnoval fenoménu Web 2.0, kde jsem mimo jiné zmínil trend přechodu nástrojů vzdálené správy do webového prostředí. Zároveň tak byla tato práce impulsem, díky kterému jsem se rozhodl zabývat se problematikou vzdálené správy i ve své bakalářské práci. Ve třetím ročníku bakalářského studia jsem zpracovával, pro účely atestace předmětu *Bibliografické rešeršní služby*, bibliografický soupis zaměřený na prostředky vzdálené správy.

Cílem bakalářské práce je zmapovat problematiku vzdálené správy a poskytnout tak pokud možno komplexní přehled o informačních zdrojích z prostředí osobních počítačů a nejčastějších operačních systémů osobních počítačů, kde je vzdálená správa důležitou součástí procesu zpracování a sdílení dalších informací, a je zároveň trendem, ke kterému vývoj v celé informační společnosti v posledních letech směřuje.

Obsah práce je rozdělen pomocí kapitol, které jsou rozlišovány dle oblastí použití nástrojů vzdálené správy.

Práce je rozdělena do šesti hlavních kapitol. První kapitola je úvodem k tématu vzdálené správy. Druhá kapitola shrnuje možnosti a prostředky vzdálené správy v prostředí operačních systémů Microsoft Windows. Třetí kapitola se zabývá operačními systémy platformy UNIX. Čtvrtá kapitola pojednává o dalších technologiích vzdálené správy, jichž je možné v rámci vzdálené správy využít. Pátá kapitola mapuje webové nástroje vycházející ze vzdálené správy, včetně praktického srovnání. Šestá kapitola zmiňuje využití vzdálené správy v prostředí moderních komunikačních zařízení, které ilustruje obrazovými přílohami, na nichž jsou zobrazeny náhledy aplikací pracujících v systémech těchto moderních komunikačních zařízení.

Pro potřeby této práce jsem zvolil citaci v textu pomocí prvního údaje záznamu a data vydání, známé též jako „Hardvardský systém“. V odkazu je uveden vždy první prvek bibliografické citace tzn. většinou autor, korporace nebo akce (pokud je název korporace nebo akce příliš dlouhý jsou použity jen první dvě nebo tři slova z názvu), popřípadě název (nebo zkrácený název). Druhá část odkazu obsahuje datum publikování (popř. copyrightu) a třetí část čísla stránek (popř. článku nebo odstavce), pokud je lze určit. Místo kulatých závorek je v textu užito závorek hranatých, neboť kulatých závorek je využíváno za účelem doplňování textu o další podrobnější nebo osvětlující informace. Bibliografické záznamy citované literatury jsou v závěrečném seznamu literatury řazeny abecedně dle prvního údaje v záznamu. Záznamy byly vytvořeny v souladu s pravidly uvedenými v českých překladech mezinárodních norem ISO 690 a ISO 690-2:

- ČSN ISO 690. *Dokumentace – Bibliografické citace – Obsah, forma a struktura*. Praha : Český normalizační institut, 1996. 31 s.
- ČSN ISO 690-2. *Informace a dokumentace – Bibliografické citace – Část 2: Elektronické dokumenty nebo jejich části*. Praha : Český normalizační institut, 2000. 22 s.

Celkový rozsah bakalářské práce je 46 stran.

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce Mgr. Janu Pokornému, Ph.D. za náměty a rady poskytnuté v průběhu jejího zpracovávání. Poděkování též patří kolegyni Bc. Zuzaně Fialové, za zapůjčení přístroje Apple iPhone, který posloužil pro testování nástrojů vzdálené správy v praxi.

1 Úvod

Vzdálená správa počítače (dále v textu jen jako vzdálená správa) v sobě jako obecný termín zahrnuje téměř jakýkoli způsob kontroly, případně specifické administrace počítače, ze vzdáleného místa (za vzdálené se v takovéto situaci považuje, jakákoli vzdálenost, od centimetrů po tisíce kilometrů, rozhodující je fakt, že uživatel fyzicky nemůže kontrolovat počítač prostřednictvím jeho vstupních periferií, nejčastěji klávesnice a polohovacího zařízení).

Bez nástrojů vzdálené správy si v dnešní době nedokáže provoz například firemních výpočetních technologií nikdo představit. Řešení pro vzdálenou správu totiž výrazně šetří čas a ve svém důsledku také kapacitu potřebných specialistů. Vzdálená správa však již dávno není pouze výdobytkem specializovaných firem. Poměrně široká počítačová veřejnost dnes stále častěji vstupuje do sfér vzdálené správy. Vzniká tak řada především softwarových nástrojů, které tito uživatelé mohou využívat. Začínáme stále více žít fenoménem distančního aparátu, čímž přímo ovlivňujeme podobu a budoucí vývoj celé informační společnosti.

Své uplatnění samozřejmě nalézá vzdálená správa i v knihovnách a informačních institucích, neboť ty také využívají řadu počítačů nejen ke zpřístupňování elektronických informací samotným uživatelům, ale i k vedení své interní agendy, včetně tvorby takových specifických produktů, jimiž jsou katalogy či databáze. Pro mnohé z knihoven a informačních institucí může vzdálená správa jejich počítačů fungovat jako služba dodavatelské firmy, a samy instituce tak nemusí zaměstnávat specializovaného technika, čímž lze ušetřit řadu finančních prostředků.

Rozvoj postupů a nástrojů vzdálené správy šel v ruku v ruce s rozvojem počítačových technologií, především sítí, ať již lokálního (např. LAN) či rozsáhlejšího charakteru (ARPAnet, NSF-NET, Internet). Významným přínosem pro rozvoj všech sítí, a tedy i pro budoucí využití vzdálené správy, byla standardizace přenosového protokolu TCP/IP. Ten mimo jiné umožnil identifikaci počítačů pomocí IP adres (IPv4, dnes pozvolný přechod na IPv6). Tímto krokem byl umožněn vznik Internetu jako takového, a standardizovala se tak i identifikaci jednotlivých počítačů nejen v rámci lokálních sítí (v letech 1980 až 1994 převládala v sítích LAN identifikace

pomocí protokolu IPX/SPX). Standardizovaná jednoznačná identifikace je základním krokem, který je pro vzdálenou správu zapotřebí. Musíte s jistotou vědět, co chcete ovládat (který počítač), abyste mohli přemýšlet nad tím, jak to ovládat.

Hlavním cílem pro vznik vzdálené správy pak bylo právě využití jejich možností v již zmíněných firemních sítích. Postupem času se tak podařilo maximálně omezit fyzickou přítomnost techniků a specialistů při údržbě firemní výpočetní infrastruktury. Specializované softwarové nástroje, které jsou navržené pro účely vzdálené správy, totiž dokážou řadu problémů vyřešit distančně, tedy přímo z počítače firemního počítačového specialisty (poskytují takovou sadu příkazů a opravných procedur, které může technik spustit ze svého počítače, na kterémkoli počítači, ke kterému má virtuální přístup). Počítač vykazující závadu však musí být dostupný prostřednictvím počítačové sítě (standardně LAN, v dnešní době i WAN). Těmito zásahy na dálku lze ušetřit mnoho času, protože řada incidentů (nejčastěji softwarové konflikty) nevyžaduje fyzickou přítomnost technika u problémového počítače. Na dálku lze takto spravovat počítače jakéhokoli uživatele bez ohledu na to, jestli používá desktop, notebook či kapesní počítač. Jedinou podmínku reprezentuje pouze zmiňované připojení k síti. Počítač tedy samozřejmě musí být v takové hardwarové kondici, která mu spuštění sekvence pro připojení se k síti umožní (zpravidla tedy i spuštění operačního systému alespoň v nějakém nouzovém módu). Vyřešení softwarového problému na počítačích s fungujícím připojením k síti je pak většinou otázkou několika minut. V dnešní době lze dokonce i zautomatizovat řešení některých běžnějších problémů bez přímé asistence (stále virtuální, nikoli fyzické) výpočetního specialisty, především pomocí předem definovaných opravných skriptů.

Mezi další výhody vzdálené správy patří schopnost urychlit analýzu problému i v případě, že není možná okamžitá náprava. To je například běžné u konfliktů způsobených selháním hardwaru. Specialista se může na budoucí fyzický zásah lépe připravit, vezme s sebou potřebný náhradní díl hardware, neztrácí tak čas neustálým vracením se do své kanceláře.

Vzdálená správa nalézá dnes široké uplatnění v celé společnosti, tedy i v našich domácnostech. Jedná se totiž o velmi silný způsob nejen administrace, ale i využívání prostředků (někdy jen k pouhému usnadnění života), které nám ta která potencionální síť nabízí. Vzdálené vypínání či restartování serveru, nebo počítače, jenž vám

distribuuje připojení k Internetu, můžete využít právě třeba doma. Mnoho lidí má dnes kromě stolního počítače také notebook či jiné přenosné zařízení, které si rád vezme například do postele, a při surfování po Internetu využívá, právě služeb distribuovaného připojení přes jejich stolní počítač. Aby si ušetřili každý den jednu noční cestu ke svému počítači, neboť člověk je v dnešní době přeci jen pohodlný, raději si nainstalují některý z programů umožňující vzdálenou správu, a tak ve chvíli, kdy je přemůže únava, jednoduše mají možnost vypnout ze svého lůžka oba počítače.

Dalším trendem poslední doby je využití vzdálené správy v rámci zajištění bezpečnosti objektů či majetku. Ten využívají například nejrůznější bezpečnostní agentury, které jsou schopny zachytávat videa z vašeho bezpečnostního okruhu (termín pro bezpečnostní zařízení složené z videokamer, mikrofonů a záznamového zařízení uloženého přímo v takto střeženém objektu) či ovládat jednotlivá zařízení a zajišťovat tak bezpečnost vašeho majetku a koordinaci zásahových prostředků (vyslání zásahové jednotky, kontaktování policie) ze vzdáleného umístění, tedy z relativního bezpečí. Výhodou je zde zejména obtížnější deaktivace systému a lidského faktoru. Systém totiž ovládá někdo, kdo není přímo v ohrožené lokalitě a nemůže být tedy snadno omráčen, jak se tomu někdy stává, sedí-li noční hlídač v budce plné monitorů přímo na daném místě. Sofistikované moderní systémy díky tomu často odhalí a umožní včasným informováním patřičných složek zadržení vetřelce předtím, než způsobí reálnou škodu či hrozbu.

Uvažujeme-li tedy o využití nástrojů vzdálené správy, ať už je naší motivací cokoli, musíme splnit následující požadavky:

- mít zapnutý cílový počítač
- počítač musí být v takovém hardwarovém stavu, že je schopen vytvořit a udržet připojení k síti (jinak jej nelze na dálku diagnostikovat a ovládat)
- připojení k síti, nejlépe pevnou linkou (vzdálená správa je méně praktická, pokud cílový počítač používá například dial-up modem, který není trvale on-line a často má dynamickou IP adresu)
- znát IP adresu cílového počítače
- nainstalovat nebo zavést potřebný software na hostitelském (cílovém) počítači a velmi často i na stanici, ze které chceme hostitelský počítač ovládat

2 Nástroje vzdálené správy v systémech Microsoft Windows

Operační systémy řady Microsoft Windows obsahují nativní nástroje pro vzdálenou správu (Terminálové služby) od roku 2000, tedy od uvedení verze Microsoft Windows Server 2000. Pro širokou uživatelskou veřejnost přišly tyto nástroje o rok později spolu s operačním systémem Microsoft Windows XP. I další následující operační systémy produktové řady Microsoft Windows (dále v textu uváděno jen jako Windows) obsahují zmiňované nástroje pro vzdálenou správu. Jmenovitě se jedná o deriváty operačního systému Windows XP pro další typy informačních technologií, Media Center a Tablet PC Edition, dále pak Windows Vista v edicích Ultimate, Business a Enterprise, a samozřejmě serverové operační systémy Windows Server 2003 a Windows Server 2008. Je také nyní již jisté, že nadcházející verze operačního systému označovaná jako Windows 7 bude tyto nástroje pro vzdálenou správu také obsahovat.

V dalším textu se zaměříme především na systémy Windows XP, jako zástupce operačního systému pro běžného desktopového uživatele a Windows Server 2003, jako zástupce serverových systémů. Windows XP byly vybrány vzhledem k jejich širokému rozšíření mezi uživateli, neboť Windows Vista se ukázaly v nejednom ohledu jako krok špatným směrem, a panuje všeobecná nevole operační systémy rodiny Windows Vista využívat. Část věnovaná serverovým systémům, které měl reprezentovat pouze Windows Server 2003, byla rozšířena oproti původnímu plánu o novinky, které přinesl Windows Server 2008. Ten si v posledních pár měsících získal mnoho spokojených uživatelů, a bylo by tak na škodu jeho možnosti alespoň v krátkosti nezmínit.

2.1 Možnosti vzdálené správy v operačních systémech Windows XP a Windows Server 2003

Vzdálená správa v systémech Windows je umožněna především díky implementacím protokolu RDP (Remote Desktop Protocol), jemuž bude podrobněji věnována zvláštní část textu.

„Se vzdálenou správou jsou nejlepší zkušenosti a nejmenší komplikace tehdy, když je v řídícím počítači používaném k provádění vzdálené správy stejný operační systém jako ve vzdáleně spravovaném počítači“ [How to use..., 2008].

Toto tvrzení firmy Microsoft je však poněkud zavádějící. Ve skutečnosti jsou skvělé praktické zkušenosti se vzdálenou správou Windows serverů z počítačů Apple. (V této souvislosti je zajímavé podotknout, že implementace RDP protokolu pro počítače platformy Apple, kterou vytvořili samy vývojáři Microsoftu, je v mnoha ohledech lépe udělána, než pro samotné operační systémy Microsoft Windows.) Instalační média systému Windows Server 2003 (Instalační CD) ve skutečnosti obsahují takové grafické nástroje správy a nástroje charakteru příkazového řádku, které je možné využít ve většině případů ke vzdálené správě operačních systémů různé provenience či edice s vysokým stupněm schopnosti budoucí vzájemné spolupráce [How to use..., 2008].

2.1.1 Vztah nástrojů vzdálené správy v operačních systémech Windows XP a Windows Server 2003

Windows XP přicházejí poprvé s vestavěnými nástroji pro vzdálenou správu pro takzvaného běžného uživatele, ty se v české verzi jmenují Vzdálená pomoc a Vzdálená plocha. Ve své podstatě to jsou omezené verze nástrojů v té době ještě neexistujícího serverového Windows Server 2003. Při bližším zkoumání zjistíme, že Terminálové služby operačního systému Windows Server 2003, jsou dostupné v celé své šíři i pro Windows XP. Pomocí poměrně jednoduchých patchů je možné upravit jakýmsi "odemknutím" Windows XP na plně vybavený Terminálový server (vysvětleno v části Windows Server 2003). [Terminal Server Patch, 2008]

2.2 Windows Server 2003

Windows Server 2003 přichází s vestavěnými nástroji pro vzdálenou správu, včetně webové aplikace, které zahrnuje příslušná zavedená verze Terminálových služeb (nejnovější je Remote Desktop Services ve verzi 6.0.6001.18000 z 24.května 2008). Komunikaci, či chcete-li zasílání zpráv mezi serverem a klienty je zajištěno v systému Microsoft Windows 2003 Server nativně prostřednictvím protokolu RDP v. 5.2 (Remote Desktop Protocol verze 5.2) [How to enable..., 2006]. (Terminálová

služba Windows 2003 Server byla vytvořena tak, že může být nezávislou na RDP protokolu. Obsahuje totiž jakousi flexibilní platformu, která umožňuje ostatním výrobcům vývoj alternativních protokolů, k využívání funkce Terminálové služby [Remote Desktop Protocol, 2008].) Terminálová služba systému Windows Server 2003 obsahuje dvě následující součásti: Vzdálená plocha pro správu a Terminálový server [How to enable..., 2006].

2.2.1 Vzdálená plocha pro správu

Vzdálená plocha pro správu umožňuje spravovat vzdáleně servery se systémem Microsoft Windows 2000 a Windows Server 2003 z libovolného klienta Terminálové služby. Pro účely demonstrace a spolupráce mohou jednu relaci sdílet dva správci. Správce se také může vzdáleně připojit ke skutečné konzole serveru příkazem -console. Ve výchozím nastavení se součást Vzdálená plocha pro správu nainstaluje společně se systémem Windows Server 2003. Vzdálená plocha pro správu je však z bezpečnostních důvodů prioritně zakázána.

2.2.2 Terminálový server

Terminálový server umožňuje současný přístup více vzdálených klientů k programům pro systém Windows, které jsou na tomto serveru spuštěny. Toto je standardní použití Terminálového serveru.

Součástí Windows Server 2003 je i služba Active Directory. Active Directory umožňuje administrátorům nastavovat síťovou politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Primární role Active Directory je poskytování centrálních služeb pro autentizaci a autorizaci, tedy jakousi správu účtů a uživatelů. Zároveň je adresářovou službou příslušné sítě. Adresář pak obsahuje uložené soubory informací o objektech v síti a jejich vzájemných vztazích. Doména Active Directory je pak v podstatě skupinou počítačů sdílejících společnou adresářovou databázi. Díky tomu tak lze Active Directory také využít k vzdálené správě počítačů, které přísluší do jedné společné domény, a to včetně editace registrů či úpravy systémových služeb [ALLEN, 2003].

2.3 Terminálové služby Windows Server 2008

Windows Server 2008 přináší výrazný upgrade terminálových služeb. Terminálové služby podporují Remote Desktop Protocol 6.1, který je odvozený od verze 6.0 uvedené spolu s operačním systémem Windows Vista. Nejvýznamnější změnou oproti verzím protokolů RDP řady 5 je možnost sdílet samostatnou aplikaci přes připojení vzdálené plochy namísto sdílení celé plochy. Tato vlastnost se nazývá Terminal Services Remote Programs. Dalšími rozšiřujícími prvky jsou Terminal Services Gateway a Terminal Services Web Access. První z nich umožňuje autorizovaným počítačům bezpečné připojení k terminálovému serveru nebo vzdálené ploše přes Internet. K tomuto účelu slouží využití protokolu RDP skrze HTTPS připojení bez nutnosti předchozího vytvoření VPN (Virtuální privátní sítě). Není ani nutné otvírání dalších portů na firewallu, protože RDP protokol pomocí zmíněného HTTPS vytváří tunel využívající přímo port 443 (nativní port HTTPS, zajišťující bezpečnou komunikaci s využitím TLS/SSL). Terminal Services Web Access pak umožňuje plnohodnotný webový přístup k Terminálový službám s využitím rozhraní webového prohlížeče. [Microsoft, 2009]

2.4 Remote Desktop Protocol

Zhruba v květnu 1997, začal Microsoft rozvíjet protokol pro výměnu informací mezi terminálovými servery a jejich klienty, který chtěl použít pro implementaci terminálových služeb v nových operačních systémech. Tento protokol dostal název Remote Desktop Protocol a vycházel ze standardů Mezinárodní telekomunikační unie (ITU, International Telecommunication Union), z rodiny protokolů T.120. Především implementoval protokol T.125 (MCS) a protokol T.128 (Application Sharing), na kterém byly založeny komunikační mechanismy, provozované v té době pro výměnu dat v rámci Microsoft NetMeeting (systém využívaný například pro videokonference). Nakonec byl Remote Desktop Protocol (RDP) poprvé uveden v operačním systému Windows NT 4.0, v edici Terminal Server Edition, která přišla na trh v roce 1998 a byla prvním operačním systémem, do kterého se dalo standardně přihlašovat vzdálenými procedurami [Remote Desktop Protocol, 2008]. Není bez zajímavosti v této souvislosti uvést, že tato první verze protokolu RDP dostala označení 4.0 (nikoli

1.0 jak by se nabízelo)a to právě podle verze operačního systému Windows NT, ve kterém byl protokol RDP poprvé uveden.

RDP se tak stal jedním z často užívaných síťových protokolů. Také proto, že umožňuje uživateli ovládat vzdálený počítač prostřednictvím připojení ke grafickému rozhraní pracovní plochy vzdáleného počítače. Vzdálená správa především v operačních systémech Windows se poté odvozovala umožněna především díky implementacím RDP protokolu.

Připojení pomocí RDP pracuje na principu klient a server. Uživatel na svém počítači využívá nejčastěji nativního programového klienta (tím je pro operační systémy rodiny Windows, Remote Desktop Connection – RDC či Terminal Services Client - TSC) pro zobrazení grafického uživatelského prostředí, které je spuštěno na vzdáleném počítači. Jakékoli zařízení může být klient, pokud má obrazovku, myš a klávesnici a je zároveň schopné komunikovat po síti pomocí protokolu RDP. Postupem času vzniklo několik různých implementací i pro operační systémy na platformě UNIX a v neposlední řadě i pro Mac OS X.

2.4.1 Architektura protokolu RDP

Protokol RDP umožňuje komunikaci prostřednictvím až 64.000 kanálů. Obrazovka vzdáleného počítače je přenášena jako rastrová grafika (bitmapová) ze serveru na klienta nebo na terminál. Od klienta se přenáší interakce klávesnice a myši se serverem. Tato komunikace je ve své podstatě velmi asymetrická, neboť většina údajů je přenášena ze serveru ke klientovi.

Protokol RDP byl prapůvodně určen na podporu různých síťových topologií, avšak v současné podobě ho lze využívat pouze přes TCP/IP sítě, právě díky normám ITU, a je vnitřně rozdělen do několika vrstev. V primární vrstvě využívá protokol RDP čtyř základních služeb. Tři z nich jsou určeny pro správu připojení: požadavek na připojení, potvrzení spojení, a požadavek na odpojení. Požadavky na připojení i odpojení přicházejí ale vždy od klienta. Když ukončí spojení server, není to klientovi nijak zvlášť oznámeno. Čtvrtou základní službu využívá protokol RDP k samotnému přenosu dat.

Další vrstva protokolu RDP rozhoduje o multicastingu, tedy zda budou data přeposílána z jednoho zdroje skupině více koncových stanic. Zvláštní bezpečnostní

vrstva zahrnuje veškeré šifrování a podpisy služeb. Zabraňuje neoprávněným uživatelům sledování připojení přes RDP protokol a brání také úpravě přenášených dat neautorizovaným uživatelem. Pro šifrování používá RC4 algoritmus, a podpisy, kterým chrání onu manipulaci s daty, skládá díky kombinaci algorithmů MD5 a SHA-1. Navíc vrstva zabezpečení spravuje autorizaci a autentizaci.

Důležitou je také vrstva, která zajišťuje přenos vstupních zařízení, myši a klávesnice, a vstupního a výstupního zobrazení. Tento mechanismus je však pro obecný popis poměrně složitý. Spokojme se s tím, že zde dochází ke cacheování a případné komprimaci některých informací, což snižuje výrazně výsledné zatížení sítě.

Jak již bylo řečeno, data jsou přenášena z RDP protokolu přímo do protokolu sítí TCP/IP. Nejprve jsou data nasměrovaná na určitý kanál, zašifrována, rozdělena do předdefinovaných částí, přizpůsobena pro síťový protokol, adresována, a odeslána. Na opačném konci tento proces probíhá v přesně obráceném pořadí, takže data jsou k dispozici přímo cílovému program, který je na dané straně otevřen. Ve své podstatě RDP protokol umožňuje distribuci datových proudů z jednoho zdroje do mnoha cílových destinací, aniž by musel posílat data zvlášť. Žádost totiž může být zrcadlena na jiného uživatele. Dokonce i místo vstupu může být převedeno v případě potřeby z jednoho uživatele na druhého. [Remote Desktop Protocol, 2008]

2.4.2 Domlouvání podmínek komunikace s klientem

Terminálový server neví a ani nemůže běžně vědět, jaký typ klienta se s ním kdy spojí. Proto všechny parametry, které charakterizují klienta a popisují jeho schopnosti (vlastnosti), musí být předány při připojování. Znalost schopností klienta totiž terminálového serveru umožňuje pružně reagovat na požadavky klienta. Proto je využívána jakási sada předdefinovaných vlastností, které musí server u klienta ověřit a domluvit se na konkrétní specifikaci jejich používání [Remote Desktop Protocol, 2008].

a) Všeobecné znalosti o klientovi: jakou využívá platformu a operační systém, kterou verzi protokolu RDP, a jaká komprese dat je podporována.

b) Způsob vykreslování: zde se dojednává velikost rozlišení pracovní plochy, preferovaná barevná hloubka, podporované barevné hloubky, a bitmapová komprese.

c) Znakové příkazy: například způsob textové výstupu či vykreslování panelů.

d) Cacheování bitmap: vyjednává se o dočasném nebo trvalém ukládání často používaných bitmap na počítači klienta.

e) Barevné tabulky: rozhoduje se podpoře jednotlivých barevných palet pro vykreslování jednotlivých pixelů.

f) Aktivace panelů: jak se budou zobrazovat ostatní ovládací prvky mimo aktivní okna.

g) Vzdálená správa: nastavuje se podpora vzdálené správy, umožňuje tak klientovi, být kontrolován ze vzdáleného místa.

h) Nastavení kurzoru: určuje barvu a grafické vlastnosti kurzoru myši.

2.4.3 Nejužívanější verze protokolu RDP v dnešní době

Protokol RDP verze 5.1 vznikl jako nedílná součást operačního systému Windows XP. S příchodem serverového systému Windows 2003 Server byl mírně rozšířen o funkci automatického znovu připojení přerušené komunikace do podoby verze 5.2. Díky rozšíření těchto systémů mezi většinou uživatelů je zatím nejčastěji využívanou verzí protokolu verze 5.1/5.2, to však nebude mít zřejmě dlouhého trvání. S příchodem nového operačního systému Windows Vista v roce 2006 vznikla již významně vylepšená nová podoba protokolu RDP, verze 6.0. Ta byla opět lehce upravena do verze 6.1 pro serverový systém Windows 2008 Server. Díky postupnému a stále častějšímu přechodu na podařený operační systém Windows 2008 Server, byly vydány aktualizace protokolu RDP verze 6.1 i pro starší operační systémy. Předpokládá se tedy, že brzy tato verze protokolu získá převahu [Remote Desktop Protocol, 2009].

Specifikace protokolu RDP verze 5.1:

- barevná hloubka 8, 15, 16, 24 či 32 bitů
- 128bitové šifrování algoritmem RC4 (starší klienti mohou použít slabší kódovaní)
- podpora Transport Layer Security

- Audio Redirection – přesměrování výstupu zvuku umožňuje uživateli spustit program na vzdálené ploše s výstupem zvuku na svém lokálním počítači
- File System Redirection – umožňuje použít lokální soubor, který je umístěný na klientově počítači, i na počítači vzdáleném
- Printer Redirection – umožňuje použít lokální tiskárnu pro tiskový výstup programů spuštěných na vzdáleném počítači
- Port Redirection – umožňuje použít lokální sériový a paralelní port pro programy spuštěné na vzdáleném počítači
- schránka pro kopírování textu muže být sdílena mezi vzdáleným počítačem a lokálním počítačem

Specifikace protokolu RDP pro verzi 6.0 byla rozšířena o tyto vlastnosti:

- Vylepšené šifrování a podepisování, protokol RDP by již neměl být napadnutelný útokem typu man in the middle (Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem, na jednu stranu se tváří, že je oprávněný uživatel, pro druhou si pak hraje na jeho server.)
- Terminal Services Remote programs – vzdálené programy jsou asociovány se soubory umístěnými na lokálním počítači, je tak možné sdílet samostatnou aplikaci namísto sdílení celé plochy
- Seamless Windows – vzdálené aplikace mohou běžet na počítači klienta v okně, jako by byly spuštěny lokálně
- Terminal Services Gateway – zajišťuje bezpečné připojení k terminálovému serveru nebo vzdálené ploše přes Internet prostřednictvím portu 443 (HTTPS)
- podpora Windows Aero a technologie ClearType
- podpora WPF efektů pro aplikace .NET 3.0
- přesměrování zařízení bylo přepsáno pro zajištění větší flexibility a zpřístupnění více zařízení

- všechny terminálové služby jsou plně konfigurovatelné a skriptovatelné pomocí WMI
- vylepšená adaptace RDP klientů pro aktuální šíři přenosového pásma
- šifrování pomocí Transport Layer Security (TLS) 1.0 jako implicitní (povinně zahrnuté) pro server i klienta
- podpora více monitorů – relace může být rozdělena mezi dva monitory

3 Vzdálená správa a UNIX

UNIX byl poprvé představen v roce 1974 v článku:

THOMPSON, Ken; RITCHIE, Dennis M. The UNIX Time-Sharing System, *Communications of the ACM*. 1974, vol. 17, no. 7, s. 365-375. ISSN 0001-0782.

Práce na tomto systému však byly zahájeny již v roce 1964 v rámci projektu MULTICS (MULTiplexed Information and Computing Service), na kterém spolupracovaly MIT (Massachusetts Institute of Technology), GE (General Electrics) a Bell Telephone Laboratories. Cílem tohoto projektu bylo poskytnout široké skupině uživatelů simultánní počítačový přístup, velký výpočetní výkon a efektivní uložení dat s možností jejich sdílení. Do konce roku 1969 však neposkytoval zdaleka všechny služby, pro které byl vytvářen. Jeho vývoj v Bell Telephone Laboratories a posléze i v GE byl tedy ukončen (do roku 1988 se o jeho podporu stále snažily na MIT, poslední známý počítač se systémem MULTICS byl vypnut 30. září. 2000).

Bývalí programátoři MULTICSu, vedení Kenem Thompsonem a Denisem Ritchieem, navrhli v roce 1970 nový operační systém UNICS (UNIversal Information and Computing Service), který byl MULTICSem inspirován, avšak kladl vyšší důraz na jednoduchost. Později byl přejmenován na UNIX. Celý operační systém byl charakteristický tím, že byl víceúlohový, víceuživatelský, textově orientovaný (později s možností grafického rozhraní X Windows), vynikal přenositelností a snadnou modifikovatelností, a nativně podporoval práci v síti. UNIX byl v počátku navržen především pro servery (operační systémy Windows a MacOS naopak vznikali nejprve pro desktopy), vzdálenou správu tak již od raných verzí podporuje přirozeně. [Thompson, 1974]

UNIX byl také licencován univerzitám, komerčním firmám a vládním organizacím. Licence zahrnovala všechny zdrojové kódy operačního systému. To mělo za následek velké rozšíření ve využívání tohoto operačního systému, zároveň to znamenalo i vznik mnoha různých verzí UNIXU. Ty vznikali nejen uvnitř samotných Bell Telephone Laboratories, ale i na univerzitách (nějznámějším je asi operační systém BSD vyvíjený na univerzitě Berkeley v Californii).

Začátkem roku 1984 bylo celosvětově instalováno asi 100 000 UNIXů různé provenience, které běžely na strojích velice rozmanitého výkonu - od mikropočítačů až po velké sálové počítače. V témže roce vzniká sdružení GNU (GNU is Not UNIX), které podporuje tzv. svobodný software a vytváří legislativní prostředek pro zaručení svobodného softwaru, General Public License (GPL). Vzniká tak spousta systémů odvozených od UNIXu (tzv. UNIX-like). Příkladem může být LINUX, vytvořený finským studentem Linusem Torvaldsem v roce 1992. Svět dnes eviduje přes 250 operačních systémů, které samy sebe charakterizují jako UNIXové nebo právě UNIX-like. Díky tomu si dnes pod pojmem UNIX hodně lidí představí spíše obecné označení rodiny operačních systémů, než jeden konkrétní produkt.

3.1 Shell

Abychom mohli dále rozvinout výklad ohledně systémů odvozených od UNIXu, musíme nejdříve přejít k vysvětlení tzv. shellu, neboť tento termín se nám bude nyní častěji objevovat. Shell je poměrně unikátní součástí operačního systému UNIX, protože je jedním z hlavních způsobů, jak komunikovat se systémem. Jedná se o jakési textové uživatelské rozhraní na bázi příkazové řádky, které je předchůdcem grafického uživatelského rozhraní. Shell je spuštěn po přihlášení uživatele do systému, poté vytvoří příkazový řádek, pomocí kterého uživatel může ovládat počítač, vyvolávat další funkce a jeho ukončením je uživatel ze systému odhlášen [Maxwell, 2002].

3.2 UNIX vzdáleně pomocí „r“ utilit

Sada tzv. „r“ utilit či nástrojů je sada, které umožňuje základní nezabezpečenou správu UNIXových operačních systémů pomocí zřízení vzdáleného Shellu. Svůj prapůvod má v roce 1983 v UNIXovém operačním systému 4.2BSD (Berkeley Software Distribution), od té doby byla tato sada zahrnuta do většiny pozdějších UNIXových operačních systémů. Jednotlivými součástmi jsou rlogin, rcp, rsh, rwho a rexec, které lze vyvolat pomocí stejně psaných příkazů. [Maxwell, 2002] Věnujme se těm, které lze využít ke vzdálené správě.

3.2.1 Rlogin

Tento název v sobě kromě samotného softwarového nástroje zahrnuje i síťový protokol, který využívá rozhraní TCP/IP sítí, kde standardně naslouchá na TCP portu číslo 513.

3.2.1.1 Protokol rlogin

Při sestavování spojení klient posílá čtyři řetězce dat na server. První je prázdný neboli nulový řetězec (skládá se pouze z jediného nulového bytu), následují ho tři nenulové řetězce:

- Přihlašovací jméno uživatele na klientském počítači.
- Přihlašovací jméno, které uživatel chce použít na serveru (což je často stejné jako uživatelské jméno na klientovi, ale ne vždy).
- Kontrolní informace, jakými jsou především typ a rychlost terminálu.

Server vrací klientovy opět prázdný řetězec, tedy nulový byte, kterým dává najevo, že obdržel základní čtyři řetězce a je nyní v režimu pro přenos dat. Po této počáteční výměně informací lze ještě vyjednávat o velikosti okna či obrazovky, tedy kolik se má zobrazovat řádků, jaký počet znaků na řádek, počet obrazových bodů ve směru X a počet obrazových bodů ve směru Y. Poté je obvykle od uživatele vyžádáno zadání hesla pro přihlášení se ke vzdálenému počítači (serveru). Za předpokladu, že heslo je správné, je uživatel přihlášen na vzdáleném počítači a lze jej používat pomocí příkazů, jako kdyby byl přihlášen lokálně. [RFC 1258, 1991]

Klient může pracovat s příkazy ve dvou režimech. V tzv. cooked režimu může pomocí příkazů start a stop, které nejsou odesílány na server, místně přerušit či zase obnovit výstup dat ze serveru na lokální terminál. V tzv. raw režimu jsou přenášeny i příkazy start a stop přímo na server, které tak lze využít například k samotnému řízení toku dat na serveru. [RFC 1258, 1991]

Uzavřít TCP spojení pomocí protokolu rlogin lze v obou směrech, od klienta i od serveru. Ten, který proces řádně ukončuje, posílá oznámení uživateli nebo procesům serveru těsně před uzavřením spojení v opačném směru.

Protokol rlogin je standardně implementován tak, že umožňuje uživateli nastavit třídy důvěryhodných uživatelů a počítačů, které budou mít možnost přihlásit se bez hesla. Přestože je to nesmírně pohodlné, představuje to oslabení zabezpečení (které samo o sobě v tomto protokolu v podstatě stejně neexistuje) Vynechání hesel od důvěryhodných uživatelů otevírá všechny takto nakonfigurované systémy, ke kterým se připojujete, i když je zasažen útokem jen jediný. Rlogin také standardně nešifruje žádná data odesílaná do sítě a to včetně loginů a hesel. [RFC 1258, 1991]

3.2.1.2 Porovnání protokolu rlogin s protokolem Telnet

Z praktického hlediska jsou příkazy protokolu rlogin mnohem jednodušší než příkazy protokolu Telnet. Rlogin také nepodporuje tak rozsáhlé struktury příkazů, ani možnosti nastavení, o kterých jedná Telnet v rámci vyjednávání doplňkových parametrů NO (podrobněji v kapitole Telnet). Klient je schopen pomocí protokolu rlogin odeslat na server jedinou klíčovou informaci: aktuální velikost okna či obrazovky, které využívá. Server je schopen sdělit klientovi aby zapnul nebo vypnul řízení toku dat, a požádat ho, aby klient poslal aktuální velikost okna či obrazovky.

3.2.2 Rsh

Rsh neboli Remote Shell je počítačový program příkazového řádku typu Shell, který umožňuje spouštět Shell příkazy na vzdáleném počítači, který je propojený s lokálním počítačem přes počítačovou síť (využívá TCP portu 514). Na vzdáleném systému, na který rsh směřuje příkazy, musí být spuštěn program typu daemon označovaný jako rshd, který zpracovává přicházející rsh spojení. Rsh ve skutečnosti posílá dvě uživatelská jména na rshd, remuser a locuser.

Remuser je vaše uživatelské jméno, kterým jste právě přihlášeni do klientského stroje. Nazývá se remuser podle pohledu rshd, protože z pohledu rshd je klientův počítač vzdáleným strojem.

Locuser je uživatelské jméno, které rshd používá k provedení příkazů na serveru. Opět je pojmenováno dle rshd, protože z rshd je server místním počítačem.

3.2.3 Rwho

Jedná se o příkaz, který vypíše seznam vzdáleně přihlášených uživatelů a všechny počítače přihlášené do stejné sítě. Pokud není zpráva od vzdáleného počítače přijata do 11 minut rwho předpokládá, že je vzdálený počítač vypnutý, a neposílá již dále seznam uživatelů, kteří k tomuto počítači byli připojeni. Když uživatel nenapsal systému ke kterému je připojen déle než minutu, začne rwho sledovat tuto nečinnost. Stane-li se pak, že tento monitorovaný úsek nečinnosti překročí jednu hodinu, rwho již uživatele dále nesleduje, považuje ho za odpojeného, a to do chvíle dokud nepošle serveru zprávu, že je aktivní, prostřednictvím příkazu –a.

3.2.4 Rexec

Remote Process Execution funguje na podobném principu jako rsh, s tím rozdílem, že kromě loginů používá k autentizaci i hesla (vzhledem k nezabezpečenosti celého připojení tak případný útočník získá oproti rsh navíc i hesla). Rexec standardně naslouchá na TCP portu 512.

3.3 Možnosti Vzdálené plochy v UNIXovém prostředí

Většina administrátorských činností v UNIXových operačních systémech nevyžaduje grafické uživatelské prostředí, známé pod zkratkou GUI, přesto tato otázka zajímá řadu běžnějších uživatelů, kteří by rádi spouštěli na vzdáleném počítači především nejrůznější aplikace.

Nabízí se nám tedy hned několik možných protokolů a na nich postavených řešení. Protokol X11, který je nativní UNIXový, protokol NX, který je optimalizovaným derivátem protokolu X11, protokol RDP, který je nativní pro MS Windows a byl již zmiňován, a v neposlední řadě protokol RFB, vyznačující se nezávislostí a multiplatformalitou.

3.3.1 Protokol X11

X11 je síťově transparentní protokol využívaný v prvních UNIXových grafických uživatelských rozhraních pro přenos obrazu na obrazovky. Počítačový software založený na tomto protokolu a poskytující takovéto grafické prostředí se

nazývá X Window System. Protokol X11 je založen na modelu klient-server, což je pro zobrazovací mechanismy poněkud nestandardní postup, zároveň však tímto umožňuje jeho využití pro vzdálené sdílení pracovní plochy. Program X server běží na počítači s grafickým displejem a komunikuje s různými klientskými programy, ty mohou být spuštěné jak na místním, tak na vzdáleném počítači. X server funguje jako prostředník mezi uživatelem a klientskými programy, přijímá žádosti o grafický výstup od klientských programů a ty zobrazuje na obrazovce a v opačném směru posílá uživatelské příkazy z klávesnice a myši na klientské programy. Zajímavostí je, že obvyklá architektura typu klient-server je brána z opačného pohledu než u protokolu X11, kde je serverem vždy lokální uživatelský počítač, zatímco klienty se stávají programy, které může uživatel z lokálního umístění spustit i na vzdáleném počítači. Opačný pohled na architekturu klient-server vznikl z důvodu pohledu místního počítače, kde se vychází z principu, že vzdáleně spuštěné programy odesílají data, které lokální počítač zobrazuje na obrazovku, tedy že lokální počítač je serverem zpracovávajícím žádosti o zobrazení. Výhodou protokolu X11 pro využití k přenosu vzdálené plochy v prostředí UNIXových operačních systému je to, že je tento protokol pro ně již nativní a většina ze současných distribucí ho využívá k zobrazování vlastních grafických uživatelských prostředí. Zajišťuje tak snadné a rychle vytvořené propojení i mezi různými distribucemi operačních systémů UNIX. Nevýhodami jsou vysoké nároky na rychlost a stabilitu připojení (při výpadku spojení se klientské programy ihned ukončí) a poněkud vágní přístup k síťové bezpečnosti. Spojení pomocí protokolu X11 je totiž standardně nešifrované využívá se však několika druhů zabezpečení pomocí autorizace, aby se kterýkoli klient nemohl připojit kamkoli. Původní omezení na IP adresy podle předem zadaného seznamu uživatelů používané již v UNIXovém protokolu rlogin, má stejné, v předcházející kapitole zmíněné, bezpečnostní nedostatky. Autorizace pomocí cookies bohužel nakonec neslavila úspěch, protože je přenášena v otevřené podobě (absence šifrování) a neochrání tak před útoky s využítím techniky sniffing. Sniffing je technika, při které dochází k ukládání a následnému čtení TCP paketů. Dá se tak mimo diagnostiku sítě využít i k odposlechu cizí datové komunikace (jedním z druhů sniffingu je i klasický útok man-in-the-middle). Z toho důvodu se začalo pro potokol X11 využívat symetrické šifry DES a či symetricky šifrovaného protokolu Kerberos. [Scheifler, c1994]

Tato zabezpečení však v druhé polovině devadesátých let převálcoval protokol SSH, který umožňuje snadné vytvoření zabezpečeného tunelu, kterým lze posílat nezabezpečená data (více v kapitole SSH).

3.3.2 Protokol NX

NX protokol vznikl jako optimalizační protokol pro běh systémů postavených protokolu X11. Tento protokol byl vyvinut v italské softwarové firmě Nomachine. Při jeho vzniku se důraz kladl na vylepšení slabých míst protokolu X11. Především šlo o zlepšení přenosu protokolu X11 na linkách s pomalým síťovým připojením a eliminaci ztráty spuštěných klientských programů přerušením síťového spojení. Přidána nakonec byla i podporu zvuku a integrace SSH šifrování. Přestože klíčové komponenty jsou open-source, stejně jako původní protokol X11, kompletní systémové řešení postavené na protokolu NX pro rozsáhle korporátní sítě je pouze komerční. Běžnému uživateli však dobře poslouží již volně šiřitelné komponenty. Řešení vzdálené plochy postavené na NX protokolu funguje tak, že mezi X server na lokálním počítači a klientské programy na vzdálených počítačích vloží dalšího prostředníka s názvem NXproxy (jak název napovídá, supluje tím v podstatě funkci klasického aplikačního proxy serveru). Nxproxy provádí inteligentní kompresi dat odesílaných protokolem X11 a zároveň cacheuje grafické objekty (například menu). Další součástí je ještě NXagent, který se zavádí (spouští) na vzdálené straně a má za úkol udržovat relaci v případě přerušení připojení a umožnit tak vyřízení požadavků klientských programů. Výhody oproti původnímu X11 protokolu jsou tak zřetelné. NX protokol je výkonnější na sítích s pomalejším připojením zejména díky vysoké účinnosti komprese a cacheování grafických objektů. Výpadek spojení už nezavře všechny programy a můžete tedy navázat v práci tam, kde jste skončili. Připojení je již standardně šifrováno SSH tunelem, který stačí doplnit vlastními klíči a získat tak velmi bezpečný způsob komunikace. Navíc přenáší i zvuk a lze ho použít dokonce i pro kopírování souborů mezi vzdálenými počítači. [NoMachine]

3.3.3 Implementace protokolu RDP pro UNIX

V kapitole věnující se operačním systémům rodiny Microsoft Windows byl již protokol RDP podrobně popsán. Připomeňme si tak jen jeho možnosti. Protokol RDP je standardně šifrovaný, cacheuje některé z přenášených informací, čímž je výrazně

méně náročný pro linky s pomalým síťovým připojením a lze jeho prostřednictvím přenášet zvuk a využívat vzdálené soubory i tiskárny. Implementace pro operační systémy na bázi UNIXu obsahuje dvě části: xrdp pro UNIXové servery a rdesktop pro UNIXové klienty.

3.3.4 Protokol RFB

RFB (Remote Framebuffer) vyvinutý v roce 1998 je jednoduchý protokol určený pro vzdálený přístup ke grafickému uživatelskému rozhraní (GUI) nejčastěji prostřednictvím počítačové sítě. RFB protokol je používán programem VNC (Virtual Network Computing)a jeho odvozeninami. RFB protokol jak název napovídá je založen na využití framebufferu. Framebuffer je zařízení, které obstarává obrazové výstupy přenášením obrazových informací z vyrovnávací paměti (bufferu). Taková informace ve vyrovnávací paměti se obvykle skládá z číselných hodnot barev pro každý obrazový bod, který se zobrazuje na obrazovce. Barevné hodnoty jsou nejčastěji ukládány jednobitově (monochromatický režim), čtyřbitově s paletou, osmibitově s barevnou paletou, 16-bitově (highcolor) či 24-bitově (truecolor). Lze také využívat tzv. alfa kanál pro uchování informace o průhlednosti obrazového bodu. [Richardson, 2009, s. 4]

Architektura klient-server je tentokráte implementována standardně. RFB klientem je tak nazýván počítač, u kterého uživatel sedí před obrazovkou s klávesnicí a myší. Koncový bod odkud pocházejí změny framebufferu (tedy všeho co se děje na obrazovce vzdáleného operačního systému a jeho aplikací) a které jsou sítí distribuovány pomocí RFB protokolu, se říká RFB server. Při navrhování RFB protokolu byl kladen důraz na to, aby bylo vyvíjeno co nejméně požadavků klienta a klienti tak mohli běžet na co možná nejširší škále dostupného hardware a operačních systémů. Tento protokol rovněž umožňuje klientovi pokračovat v rozdělané práci, pokud se odpojí a znovu připojí. Dokonce lze takto předat připojení ke vzdálenému serveru z jednoho klienta na druhého.

Při počáteční interakci mezi klientem a serverem prostřednictvím protokolu RFB dochází k vyjednávání o formátu a druhu kódování, které se použijí pro reprezentaci obrazových bodů. Toto vyjednávání bylo opět navrženo tak, aby co nejvíce ulehčilo práci klientovi. Pointa je v tom, že server musí být vždy schopen

dodávat obrazová data v takové podobě, kterou klient chce. Avšak v případě, že je klient schopen zpracovávat odpovídajícím způsobem několik různých formátů či kódování, může si server zvolit takovou kombinaci, která je pro něj jednodušší z hlediska produkce.

Protože RFB vznikl jako poměrně jednoduchý open-source protokol, postupem času na jeho základě vzniklo několik různě pokročilých verzí, ve kterých byl základní RFB protokol obohacen o další funkce jakými jsou přenos souborů, sofistikovanější komprese či nejrůznější zabezpečovací techniky přenosu. Proto v zájmu zachování kompatibility mezi mnoha různými VNC klienty a jejich serverovými implementacemi, obsahují tyto programy informace o několika verzích RFB protokolu. To umožňuje klientům a serverům vyjednávat o vzájemném propojení pomocí takové verze, aby mohla být zvolena co nejvhodnější komprese a bezpečnostní možnosti, a zároveň byl zajištěn vysoký standard vzájemné komunikace. [Richardson, 2009]

Výhody lze u protokolu RFB najít v podobě jednoduché instalace, možnosti funkčního nastavení i pro linky s pomalým síťovým připojením, možnost sdílení jedné plochy více uživateli a skutečnost, že přerušení spojení nevede k automatickému ukončení programů. A protože je RFB protokol založen na framebufferu, který je využíván napříč platformami pro reprezentaci obrazu, je možné ho použít v nejrůznějších systémech, které pracují v grafickém režimu a používají okna (tedy včetně X Window System, Microsoft Windows a Mac OS X). Při využití RFB protokolu ale nelze dynamicky měnit velikost plochy a objektová grafika (například menu) je přenášena pouze bitmapově (vykreslováním jednotlivých obrazových bodů), což zvyšuje náročnost přenosu.

3.3.5 Přístup mezi operačními systémy odlišných platforem

Uživatelé se také často setkávají se situacemi, kdy potřebují využít vzdálené plochy mezi operačními systémy různých platforem. V kanceláři mají například korporátně (zaměstnavatel si koupil multilicenci) nainstalovaný operační systém z rodiny Microsoft Windows, ale ve skutečnosti jsou zarytými milovníky UNIXu, a tak ho používají doma. Internetová fóra tak plní dotazy jak nejlépe vyřešit takovouto situaci. Odpověď je bohužel značně nejednoznačná. Velmi záleží na konkrétních

verzích jednotlivých operačních systémů, které mají do takovéto komunikace vstupovat. Propojit vzdáleně plochy různých operačních systému lze, a dokonce existují varianty pro každý z výše jmenovaných protokolů. Žádné řešení však není takové, aby se o něm dalo říci, že zrovna ono bude zaručeně a vždy fungovat. Při propojování vzdálených ploch různých operačních systémů je tedy nejdůležitější trpělivost, protože často musíte vyzkoušet mnoho různých protokolů a jejich implementací, než dosáhnete kýženého výsledku.

4 Další technologie vzdálené správy

4.1 Specifikace protokolu Telnet

Telnet (Telecommunication Network) protokol je jeden z nejstarších protokolů sítí TCP/IP. Účelem vzniku tohoto protokolu bylo poskytnout obousměrné komunikační rozhraní, které by mohlo mít poměrně obecné využití i mezi systémy rozdílných základů a platforem. Jeho hlavním cílem bylo umožnit standardní způsob propojení koncových neboli terminálových zařízení a terminálově orientovaných procesů navzájem. Při jeho vzniku se již předvídalo, že tento protokol může být použit jak pro komunikace ve smyslu terminál - terminál , tak pro komunikace mezi jednotlivými terminálovými procesy (například pro distribuované výpočty). Uživateli tak umožňuje ovládat nejen vzdálené zařízení pomocí terminálu s příkazovým řádkem, ale může zajišťovat i komunikaci mezi programy.

Telnet protokol je postaven na třech hlavních myšlenkách. První z této trojice je koncept síťového virtuálního terminálu NVT (Network Virtual Terminal). Druhou je zásada vyjednávání doplňkových parametrů NO (Negotiating Options), kde se jedná o vyjednávání klienta a serveru o nastavení určitých voleb. Poslední myšlenkou pak je symetrické zobrazení terminálů a procesů. Tyto základní tři postupy jsou definovány v dokumentu RFC 854, který se díky využívání postupů v něm popsaných stal jakýmsi standardem pro tento protokol. [RFC 854, 1983, s. 1]

Síťový virtuální terminál NVT je imaginární obousměrné znakové zařízení vytvořené na obou koncích spojení, které zajišťuje průhlednost všech operací vůči uživateli. Nejsou zde rozdíly mezi jednotlivými komunikujícími zařízeními [RFC 854, 1983, s. 4]. Virtuální terminál poskytuje obecnou sadu příkazů pro všechny typy zařízení a také se zabývá prezentací dat. To znamená, že zajišťuje v jaký bajt se má změnit například písmeno A, aby na druhém konci síťového spojení bylo interpretováno opět jako A. (Není bez zajímavosti, že právě protokol NVT je použit v omezené míře pro prezentaci dat v mnoha dalších protokolech, jakými jsou například FTP, POP3, SMTP, NNTP či HTTP) [Dostálek, 2003, s. 54]. Klient Telnet přijímá znaky a řídící kódy od specifického vzdáleného terminálu, transformuje je do jednotného tvaru NVT a v tomto tvaru je odesílá na server Telnet. Na straně serveru

musí být zajištěno mapování kláves a řídících kódů síťového terminálu NVT do formy požadované terminálové emulace. Údaje jsou od klienta protokolu Telnet přenášena jako sedmibitové kódy ASCII pro znaky a zobrazení s přidaným osmým bitem rozlišujícím přenášený znak nebo řídící povel (0-znak, 1-povel). Server standardně naslouchá na TCP portu číslo 23. Po vytvoření TCP spojení jsou přenášená data mezi vzdáleným terminálem a počítačem po řádcích nebo po znacích spolu s řídícími znaky protokolu Telnet. Server Telnet odevzdává přenášená data přímo aplikaci, s kterou virtuálně komunikuje vzdálený terminál. [RFC 854, 1983]

Abychom správně pochopili smysl a roli virtuálního terminálu NVT je velmi důležité si uvědomit, že každý virtuální terminál vždy omezuje individualitu či specifičnost konkrétních terminálů a redukuje jejich vlastnosti a schopnosti na takovou úroveň, která může být společná prakticky všem fyzicky existujícím terminálům, které jsou schopny se komunikace určitého druhu zúčastnit. Nejinak je tomu i v případě virtuálního terminálu NVT, který si proto můžeme představit jako největší společný jmenovatel všech ještě použitelných terminálů. Díky tomuto definovanému formátu NVT může Telnet operovat na různých operačních systémech [Peterka, 1993].

Vyjednávání doplňkových parametrů NO umožňuje rozšířit možnosti protokolu o další potřebné parametry. Bezprostředně po navázání spojení totiž obě strany mohou používat právě a pouze to, co jim zaručuje virtuální terminál NVT. Vzájemné domlouvání na použití různých rozšíření obvykle probíhá okamžitě po navázání spojení, ale není to nutnou podmínkou. Doplňkové parametry může požadovat server i klient, přičemž libovolný z nich může žádost o zavedení volitelných parametrů akceptovat nebo zamítnout. To se děje i přesto, že definice protokolu předpokládá, že obě komunikující strany jsou vybaveny NVT. Proto proběhne nejdříve výměna údajů, ve které se obě strany dohodnou na určitých parametrech a volbách komunikace. Pokud jedna strana neumí použít danou volbu, požadavek zamítne. Jak už bylo řečeno, strany však musí dodržet minimální standard NVT. Díky vyjednávání doplňkových parametrů NO je možné komunikovat i s terminály, jejichž skutečné schopnosti nepřesahují minimum, požadované virtuálním terminálem NVT, a na druhé straně je možné efektivně využít možnosti a schopnosti lépe vybavených terminálů.

Existují čtyři možné požadavky v rámci vyjednávání doplňkových parametrů NO:

WILL - odesílatel chce danou volbu zapnout

DO - odesílatel chce, aby příjemce danou volbu zapnul

WONT - odesílatel chce danou volbu vypnout

DONT - odesílatel chce, aby příjemce danou volbu vypnul

[RFC 854, 1983]

4.1.1 Problematika bezpečnosti protokolu Telnet

Telnet byl poprvé vyvinut v roce 1969. V této době přistupovala většina uživatelů do počítačových sítí na univerzitách, ve vládních úřadech nebo ve velkých společnostech. Tato skutečnost tak byla jedním z hlavních důvodů, proč nebyla bezpečnost brána tak vážně jako po celosvětovém rozmachu Internetu. Jak se zvyšoval počet uživatelů Internetu, rostl také počet těch, kteří se zkoušeli nabourat do serverů ostatních. Tím vzrostla potřeba šifrování.

Experti na počítačovou bezpečnost a s tím v ruku v ruce jdoucí počítačovou kriminalitu tak doporučovali distancování se od používání protokolu Telnet pro vzdálený přístup k serverům. Důvodem pro tato doporučení či varování byla především skutečnost, že protokol Telnet standardně nešifruje žádná data odesílaná do sítě a to včetně loginů a hesel. Často se tak dala a dá takováto komunikace přímo odposlouchávat. Zneužití takto získaných loginů a hesel je nasnadě, kdokoliv kdo má přístup do routeru, switche nebo hubu umístěného na síti mezi dvěma zařízeními, kde je Telnet používán ve své standardní nerozšířené podobě, může zachytit celou jejich komunikaci a získat tak hesla a vše co bylo napsáno použitím několika běžných programů pro sledování činnosti sítě.

Tyto bezpečnostní nedostatky způsobily rapidní ústup při využití protokolu Telnet. Zvláště pak v prostředí internetu, kde se vzdálené přístupy začaly realizovat s využitím protokolu SSH, který byl poprvé uvolněn v roce 1995. SSH poskytovalo většinu funkcí protokolu Telnet a navíc silné šifrování, které bránilo v získávání hesel a veřejný klíč, který sloužil k ověření vzdáleného počítače. Další možností jak zvýšit

bezpečnost přenosu protokolu Telnet je jeho „zapouzdření“ v rámci VPN (Virtual Private Network). [Dostálek, 2003]

4.2 SSH (Secure Shell)

4.2.1 Terminologický úvod

Secure Shell protokol byl vynalezen v roce 1995 Tatu Ylönenem, který pracoval jako výzkumný pracovník v Helsinki University of Technology ve Finsku. Vytvořil tento protokol po sérii bezpečnostních incidentů v univerzitní síti, aby zajistil šifrování přenášených dat, včetně hesel. Bohužel však první program, který implementoval tento protokol, nazval jednoduše dle názvu protokolu jako SSH. Neúmyslně tak dalším generacím zajistil jakési zmatení jazyků. Když dnes v informatice řeknete SSH, tak si nikdo nemůže být hned jistý, o čem to vlastně chcete mluvit. Zda o programu, či o zabezpečeném komunikačním protokolu. Je nutné podotknout, že k záměnám dochází naneštěstí i v některých publikacích či statích, které se tváří na první pohled odborně. Abych se vyvaroval podobných chyb, rozhodl jsem se využít označení, převzaté z následující publikace:

BARRETT, Daniel J.; SILVERMAN, Richard E. *SSH : The Secure Shell : The Definitive Guide*. 2nd ed. Sebastopol, CA : O’Reilly, 2005. xviii, 645 s. ISBN 0-596-00895-3.

Primárně bude popisován protokol SSH a jeho verze, a to následujícím způsobem:

SSH-1, pro 1. verzi protokolu SSH, jejíž tvůrcem je Tatu Ylönen

SSH-2, pro 2. verzi protokolu SSH, v současnosti téměř výhradně používaná verze

V omezené míře budou zmiňovány i konkrétní implementace, které mohou mít podobný název, jako název protokolu. Pro odlišení budiž:

SSH1, program SSH Tatu Ylönena, implementující protokol SSH-1

SSH2, program SSH Secure Shell z roku 1998, implementující protokol SSH-2.

4.2.2 Protokol SSH

SSH protokol specifikuje jak vytvořit zabezpečené spojení přes veřejnou síť, tím také umožňuje jistou míru bezpečné komunikace mezi dvěma počítači. Dalo by se také říci, že zajišťuje vzdálené spojení s poměrně vysokou garancí, že propojuje takové dvě strany, které jsou oprávněné spolu komunikovat. SSH protokol je používán jako bezpečná náhrada starších protokolů (jakým je například Telnet) a nabízí i některé nové vlastnosti (především v závislosti na verzi) [Barret, 2005].

Hlavními přednostmi protokolu SSH jsou zajištění důvěrnosti dat, zajištění integrity komunikace, autentizace komunikující stran, autorizace přístupů a tzv. tunelování spojení. Všechny tyto zmíněné funkce přináší ve své podstatě až SSH-2. Díky jistým rozšířením pak i SSH-1, v podstatě však až od verze 1.5 (SSH-1.5), zde však hraje jistou roli i použitý program a tedy implementace samotného protokolu (například OpenSSH přinášela více možností než *SSH1,* přestože oba dva implementovali protokol SSH-1*).*

V současnosti je SSH-1 jen jakousi relikvií, protože není zdaleka tak flexibilní jako SSH-2, má řadu neopravitelných bezpečnostních slabin a je již několik let zastaralá. Proto je všeobecně v dnešní době užíván jako standard právě protokol SSH-2. [Barret, 2005, s. 45].

SSH-2

Již zmiňovaná flexibilita protokolu SSH-2 oproti verzi SSH-1 je dána především modularitou protokolu SSH-2. Ten ve své specifikaci má navrženou architekturu rozdělenou na 3 hlavní části, transportní vrstvu, vrstvu autentizace uživatele a vrstvu spojení.

Transportní vrstva zajišťuje počáteční výměnu klíčů, serverovou autentizaci, a ověření integrity. Volitelně může také poskytovat bezztrátovou kompresi přenášených dat. Transportní vrstva také zajišťuje opětovnou výměnu klíčů, pro zajištění vyšší bezpečnosti. Standardně po 1 GB přenesených dat či po uplynutí 1 hodiny. Záleží zde pak na tom, co nastane dříve.

Vrstva autentizace uživatele zajišťuje autentizaci klientů. Samotná autentizace je řízena SSH klientem, server pouze reaguje na autorizační požadavky od SSH klienta.

Vrstva spojení definuje koncept kanálů. Jedno SSH spojení může hostovat více kanálů zároveň, kdy každý může přenášet data v obou směrech. [RFC 4251, 2006]

4.2.3 Přednosti protokolu SSH

Důvěrnost dat

Tento princip by měl ochraňovat soukromá data před odhalením nežádoucí třetí osobou. Typická počítačová síť nezajišťuje soukromí. Kdokoli, kdo přistupuje do takovéto sítě, může být schopen s pomocí více či méně sofistikovaných nástrojů vidět nebo získávat všechna data procházející touto sítí, a to včetně loginů a hesel. SSH zajišťuje soukromí a důvěrnost dat díky šifrování těch dat, které jsou prostřednictvím SSH mezi koncovými subjekty sítě distribuovány. Toto zašifrování mezi koncovými body takovéto komunikace je založeno na náhodných klíčích, které jsou vyjednány v rámci bezpečného propojení pouze pro dané sezení (session), po jeho skončení tyto klíče zanikají. SSH podporuje mnoho rozličných způsobů šifrování dat distribuovaných během jednotlivých sezení. Mezi nejběžněji užívané patří například AES, ARCFOUR, Blowfish, Twofish, IDEA, DES, a triple-DES (3DES).

Integrita komunikace

Integrita komunikace znamená, že musí být zajištěno, aby údaje přenášené z jednoho konce připojení k síti dorazily v nezměněné podobě na konec druhý. Vrstva protokolů TCP/IP, přes které SSH přistupuje, má sama o sobě kontrolu integrity vzhledem k síti jako takové (elektrické šumy, ztracené pakety z důvodu přetížení sítě apod.). Tyto metody však pro zajištění integrity dat nestačí. Kdyby totiž SSH pouze zašifrovalo komunikaci, a případný útočník by tedy nevěděl, která data konkrétně napadá, mohl by mezi ně poslat jakýsi datový odpad, který kontrola integrity TCP/IP neodhalí (nemá na to prostředky, kontroluje pouze správné doručení jednotlivých paketů), a vám přijdou nesmyslná, poškozená či nevyžádaná data, nebo o některá již stažená data přijdete (závisí na zdatnosti útočníka). SSH protokol proto využívá takovou kontrolu integrity, která ověří obě nejdůležitější vlastnosti přenášených dat. Že přenášená data nebyla pozměněna, a že skutečně pocházejí od odesílatele. Využívá k tomuto účelu tzv. hash algoritmy, fungující zjednodušeně na principu kontrolního součtu.

Autentizace komunikující stran

Autentizace znamená ověření něčí identity. Každé spojení prostřednictvím protokolu SSH zahrnuje dvě autentizace. Klient ověřuje identitu SSH serveru (server authentication), a server ověřuje identitu uživatele, který žádá o přístup (user authentication). Autentizace serveru (server authentication) zajišťuje, že SSH server je pravý, a brání tak například před útoky přesměrováním připojení k síti na jiný server. Dále chrání i před útoky typu man-in-the-middle. Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem, na jednu stranu se tváří, že je oprávněný uživatel, pro druhou si pak hraje na jeho server.

Ověření uživatele (user authentication) je tradičně prováděno hesly, která bohužel jsou slabým autentizačním prostředkem, především díky uživatelům samotným (1234 ,ABCD , jméno manželky ani datum narození opravdu nejsou bezpečnými hesly). Díky SSH šifrování jsou samotná hesla chráněna během přenosu, což je oproti běžným prostředkům vzdáleného přístupu typu Telnet či FTP poměrně pokrok (Jak již bylo řečeno, tyto prostředky posílají loginy a hesla tak jak jsou, a je možné je tedy zachytávat a krást.) Samotné šifrování hesla by však nemuselo stačit. Proto SSH využívá dalšího postupu, autentizace pomocí veřejného klíče, obecně známého jako asymetrické šifrování. Nejběžnější verzí asymetrického šifrování je využívání dvojice klíčů, veřejného a soukromého. Šifrovací klíč je veřejný, majitel klíče ho volně uveřejní, a kdokoli jím může šifrovat jemu určené zprávy. Dešifrovací klíč je naopak soukromý, majitel jej drží v tajnosti a pomocí něj může jemu určené zprávy dešifrovat. Pro zvýšení bezpečnosti se mohou SSH klient a server dohodnout na použití nějakého pokročilejšího způsobu autentizace, či na několikanásobném ověření pomocí různých postupů.

Autorizace přístupů

Autorizace spočívá v rozhodnutí, zda existuje oprávnění pro danou činnost, pro toho kterého uživatele. Nastává vždy po autentizaci, neboť nemůžete nikomu přiřknout privilegia, pokud si nejste jistí, že je tím, za koho se vydává. SSH servery mají velké množství způsobů jak garantovat práva uživatelů, a umožňovat či omezovat konkrétní jejich akce. Velice přitom záleží na konkrétní programové implementaci SSH, kterou server využívá, i na metodě autentizace, kterou se uživatel prokázal (lze

v případě potřeby nastavit, více úrovní vstupu, podle toho jakou autentizaci má uživatel zrovna použít v závislosti na kvalitě připojení apod.).

Tunelování spojení

Tunelování či směrování spojení znamená, že posíláte jinou službu založenou na TCP, například Telnet, prostřednictvím SSH sezení (session). To přenáší výhody SSH i na ostatní služby TCP, které tímto prostřednictvím budete využívat. Například se z obyčejného Telnetového spojení, které přenášelo loginy a hesla tak jak jsou, stane spojení se šifrovanými daty a s ověřenou integritou komunikace, která je navíc autentizována pomocí SSH klíčů. [Barret, 2005, s. 37-39]

Stejně jako každý šifrovaný protokol, může být i SSH považováno za bezpečnostní riziko pro firmy nebo vlády, které nevěří svým zaměstnancům a chtějí mít jejich komunikaci pod kontrolou. Navíc má SSH v sobě zabudované jednoduché mechanismy pro vytváření tunelovaných spojení, skrze které lze přenášet velké objemy dat a vytvářet tak nežádoucí vstupní body, které mohou sloužit k úniku důležitých informací nebo k průniku do vnitřní sítě. Stejně tak mohou být tytéž vlastnosti užitečné (např. již zmíněné šifrování služeb jako je POP3 nebo IMAP prostým použitím SSH tunelu), protože je u jiných protokolů nenajdeme.

5 Vzdálená správa v prostředí webových aplikací

Posledních deset let je ve znamení rapidního rozvoje Internetu a jeho masivního pronikání k běžným domácím uživatelům, jejichž počet přesahuje nyní již miliardu. Neustálé zkvalitňování připojení k Internetu, jeho dostupnost a rychlost se tak nutně musely projevit i na podobě Internetu samotného. Nastal tak příhodný čas pro rozvoj služeb a aplikací nejrůznějšího druhu a vývojáři na celém světě tak stále přicházejí s novými nástroji, které ovlivňují ve svém důsledku i trendy využívání Internetu. Vznikají tak i webové aplikace a služby vzniklé na modelu vzdálené správy, využívající nejrůznějších postupů a technologií.

5.1 Vzdálené správa prostřednictvím browseru

Politika podobných služeb, které využívají na klientské straně pouze browseru (webového prohlížeče) je jednoduchá, browser je dostupný na každém počítači s připojením k Internetu, a tak spravovat vzdálené počítače můžete například z jakékoli internetové kavárny a nemusíte nikdy instalovat žádný klientský software (takovou instalaci by vám totiž někdy ani nemuseli dovolit). Zároveň může být takovýto vzdálený přístup k určitému počítači jedinou možností, to zejména v případě nemá-li tento počítač veřejnou IP adresu (není přímo viditelný a dostupný z Internetu). Pro takovéto případy existuje několik komerčních služeb. Například GoToMyPC od společnosti Cytrix či LogMeIn od společnosti 3am Labs (nyní LogMeIn Inc.). Pouze LogMeIn však má i bezplatnou variantu pro běžného uživatele, na které si každý můžeme zmapovat prostředky a funkce této služby.

5.1.1 LogMeIn

Společnost 3am Labs uvedla službu LogMeIn (http://www.logmein.com) na trh v září roku 2004 (díky velkému úspěchu tohoto produktu se v roce 2006 přejmenovala na LogMeIn Inc.). Její funkční řešení se skládá ze serverové části (LogMeIn host), která běží na PC vzdáleně spravovaném, ze samotné služby běžící na serverech společnosti LogMeIn Inc. a z klienta, kterým je dostupný prostřednictvím každého běžného browseru. [LogMeIn, 2009]

Klient i server komunikují prostřednictvím centrálního serveru společnosti LogMeIn Inc. (Gateway Server). LogMeIn host navazuje a udržuje stálé SSL zabezpečené spojení s obslužným Gateway Serverem. Spojení je iniciováno LogMeIn hostem pomocí přidružené aplikace, která se po nainstalování může spouštět automaticky při každém startu počítače či manuálně (využití pro správu cizího počítače pro případ vzdálené pomoci). Vůči všem firewallům a dalším případným síťovým kontrolorům jde tedy o povolené odchozí spojení, které není důvodu nijak zamezovat. Po přihlášení klientského browseru, které je zabezpečeno přihlašovacím heslem na vzdálený počítač který chceme ovládat, je komunikace mezi klientem a hostem (obsah pracovní plochy, klikání myší i stisky kláves) zprostředkována centrálním serverem. Komunikaci tak lze snadno navázat i v případě, že klientský i vzdálený počítač jsou skryty za firewallem, či v hluboké struktuře sítě s nejrůznějšími bezpečnostními prvky.

Webové rozhraní je velmi názorné, po přihlášení se z libovolného počítače uvidíte seznam všech svých instalovaných hostů a jejich stav (online/offline). Kliknutím na odpovídající odkaz se připojíte k cílovému počítači, po zadání ověřovacího přístupového hesla. Po úspěšném připojení k cílovému počítači se vám v okně prohlížeče objeví jeho vzdálená plocha. V menu v horní části obrazovky můžete nastavit vlastnosti zobrazení, kterými jsou rozlišení, barevná hloubka, celoobrazovkový režim, přepínání mezi více obrazovkami (pokud je cílový počítač má), které hlavně ovlivňují rychlost a kvalitu zobrazení.

Z hlediska bezpečnosti je celá komunikace mezi klientem a serverem šifrována s využitím SSL protokolu. Ten využívá zabezpečeného HTTPS spojení, (port 443) a SSL/TLS certifikátů k ověření přístupu. Certifikáty aktuálně využívají 2048 bitů dlouhý RSA klíč (ve své podstatě vlastně dvojici klíčů, veřejný a privátní). Šifrování zajišťuje, že komunikace nebude odposlechnuta či pozměněna, a to dokonce ani serverem LogMeIn, který funguje ve všech případech jako prostředník. K autorizaci přístupu slouží oddělená hesla k LogMeIn účtu a k autorizaci vstupů do jednotlivých vzdálených počítačů. LogMeIn používá nyní standardně 256-bitové šifrování. Zlepšená bezpečnost je pak dostupná v placených verzích. Ty kromě standardní vzdálené plochy, kterou přináší volně dostupná varianta, nabízejí i přenos souborů

mezi počítači, možnost synchronizace dat ve vybraných složkách a lokální tisk souborů ze vzdáleného počítače.

Ve srovnání s jinými řešeními, kde musíte pro propojení dvou vzdálených skrytých (bez veřejné IP) počítačů nejprve mezi nimi vytvořit například virtuální privátní síť (což není vždy reálně uskutečnitelné) a teprve poté použít specializovaný program pro vzdálenou správu nebo vzdálenou plochu, vyniká služba LogMeIn velkou jednoduchostí instalace. Jako klienta lze použít libovolný počítač či dokonce PDA, SmartPhony a mobilní telefony, vybavené webovým prohlížečem (není nutná instalace žádného klientského software, pouze přítomnost podpory Javy). Výhodou integrace webové služby jako přenosového prostředku je i to, že službu LogMeIn je možné využívat i pro správu počítačů mezi operačními systémy různých platforem.

Po rozsáhlém testování, které spočívalo v použití nejrůznějších počítačů, přístrojů, a browserů, a během něhož byla kapitola o LogMeIn psána vzdáleně (ovládán počítač na platformě Windows se spuštěným textovým editorem Microsoft Word), pokud to bylo v daném přístroji jen trochu technicky možné, jsem dospěl k následujícím zjištěním. Log Me In browser klient naprosto bezchybně funguje ve všech posledních třech verzích Microsoft Internet Exploreru (IE 6,7 a 8) i v Mozilla Firefoxu (verze 2, 3 a Portable). Bohužel použití Opery (všech derivátů, včetně verze Mini pro mobilní telefony), Google Chrome a Safari (ve verzi pro PC) doporučit nelze. Zde se podaří přihlásit k účtu, zobrazí se jednotlivé pracovní stanice, ale samotné přihlášení k nim se většinou ani nezinicializuje (většinou ztroskotají na firewallu). Celkově lze nejvíce doporučit Mozillu Firefox ve verzi 3.5, která je dostupná pro všechny tři hlavní platformy (Windows, UNIX, Mac OS) a zároveň byla dle mých subjektivních zjištění odezva při práci na vzdáleném počítači nejkratší (například při zmiňovaném psaní textu této kapitoly byly prodlevy v zobrazení znaků naprosto ojedinělé). Vzdálená správa prostřednictvím mobilních telefonů je u této služby poměrně malichernou záležitostí, neboť jakési základní využití práce s GUI ovládaného počítače lze pozorovat až od displeje charakteristikami srovnatelného s přístrojem Apple iPhone (velikost úhlopříčky 3,5 palce, rozlišení 320 × 480 pixelů).

5.2 Webové služby inspirované prostředky vzdálené správy

Vývojáři webových služeb však přicházejí i s různými alternativními řešeními sdílení dat a dokumentů, a nechávají se přitom volně inspirovat prostředky vzdálené správy. Velký rozvoj těchto služeb přišel s rozvojem Web 2.0 a následného vlivu, který tento fenomén měl na podobu celého Internetu. S příchodem nových vývojových prostředků jakými jsou AJAX (Asynchronous Java Script and XML), hojně využívaného právě u Web 2.0 služeb využívajících prioritně browser, nebo AIR (Adobe Integrated Runtime), který naopak přináší webové služby přímo na plochu jako aplikace, vzniká ve světě mnoho zajímavých produktů doslova každým dnem. Nejsou to sice stále plnohodnotné nástroje vzdálené správy, ale přesto nám mohou nastínit principy, na kterých by mohly fungovat technologie a nástroje budoucnosti.

5.2.1 AJAX

Téměř až mystérii obestřená a do nebe vynášená je někdy tato technologie vývoje interaktivních webových aplikací. Nelze jí samozřejmě upřít jakýsi nový pohled na věc a pokrok, který přinesla spolu s produkty Web 2.0, ale větší střízlivost by přeci jen neškodila. AJAX je vlastně jen spojením starých známých technologií XML, JavaScript, HTTP a (X)HTML. Hlavní zmiňovaná deviza AJAXu, komunikace s webovým serverem na pozadí, díky které nemusí být stránka neustále znova překreslována, existovala už v mnoha produktech před AJAXem. Popularitu AJAXu nakonec nejvíce podpořil fakt, že ho k vývoji svých webových aplikací a služeb začali používat vývojáři firmy Google. Snad už se ale pomalu dostáváme z fáze euforie, kdy je AJAX používán téměř všude, do fáze kdy bude využíván jen pro projekty, kde je opravdu funkčně vhodné jej použít. [Holzner, 2007]

5.2.2 Webtop jako specifický pohled na vzdálenou správu

AJAX našel velmi vhodné využití u Webtop (Web Desktop) služeb. Tyto webové služby si berou inspiraci v konkrétním používání vzdálené správy, kterou uživatelé často využívají jako prostředku k dosažení uživatelovi vlastní ovládací plochy a jeho dokumentů a aplikací ze vzdáleného umístění. Webtop služby nabízejí personalizovanou virtuální plochu, dostupnou z browseru, přístupnou přes počítač všech platforem využívající připojení k Internetu. Aplikace, data, soubory,

konfigurace, nastavení i přístupová oprávnění jsou uložena na síti ve vašem účtu konkrétní služby. Nemusíte tak sebou vozit žádné zařízení na přenos dat, stačí jakýkoli počítač s připojením k Internetu, na který nejsou kladeny prakticky žádné hardwarové nároky. Veškeré aplikace, a tedy značná část výpočetních procedur, probíhají na serverech Webtop služeb. Klientský počítač pouze využívá browser pro zobrazení prostředí a distribuuje pokyny zadané klávesnicí a polohovacím zařízením. Jednotlivé služby jsou v různých stádiích vývoje a nabízejí tak nesrovnatelně rozdílné možnosti. Z obecnějšího pohledu však mění pohled na klasické paradigma chápání dnešních počítačů, a mohou být prvním krokem posunu k budoucím formám informační společnosti, jak jí charakterizují mnohé predikce nejrůznějších teoretiků (např. Petříček, 1998, Gibson,1984, Wooley 1993).

5.2.3 AIR

Tvůrci technologie AIR (Adobe Integrated Runtime) chtějí dosáhnout splynutí webu a uživatelského prostředí naopak takovým způsobem, že odstraní browser jako distributora dat z Internetu. Jednotlivé webové nástroje (jejich webová podoba), naprogramované v HTML a využívající Javascript (tedy i AJAX), Flash či Adobe Flex se dají převést ve vývojovém prostředí AIR do desktopové aplikace konkrétní webové služby. Tato aplikace pak komunikuje se serverem sama, nevyužívá pro zobrazování dat browser a není tedy omezována jeho rámci, což jim umožňuje prakticky libovolný vzhled či jakoukoli strukturu menu. To se odráží v lepší ovladatelnosti a dostupnosti některých funkcí konkrétních služeb. Výhodou zůstává, že i po oficiálním uvedení stabilní verze AIR v únoru 2008, je tato technologie zdarma, a dochází tak stále častěji k implementacím webových služeb, což stimuluje vývoj celého Internetu. [Adobe, 2009]

Zajímavý vliv má tento trend na tvůrce webových služeb pro monitorování serverů a podnikových sítí. Ti začínají tvořit vlastní AIR aplikace, kterými přenášejí monitorovací funkce z webového prostředí přímo na ovládací plochu. V těch pak lze komplexněji a variabilněji nastavovat zobrazování jednotlivých parametrů, dle potřeb každého administrátora, což dříve ve webovém prostředí nebylo možné, neboť každá stránka zobrazovala konkrétní monitorované vlastnosti. Nyní si v AIR aplikacích těchto webových služeb můžete vyčlenit prioritní servery, o jejichž změně stavu chcete být automaticky informováni, přiřadit jim atributy na které má brát aplikace

obzvlášť zřetel, a podobně. V případě práce na jiném úkolu pak mohou tyto aplikace běžet na pozadí a informovat vás o své činnosti prostřednictvím ikon a zpráv zobrazovaných v oznamovací oblasti systémové lišty (tzv. system tray).

6 Využití moderních komunikačních zařízení ke vzdálené správě

Termín moderních komunikační zařízení je v této kapitole chápán jako nadřazený pojem zastupující řadu nejrůznějších mobilních telefonů a zařízení, včetně tzv. Smartphonů a přístrojů typu PDA. Tato zařízení se v současné době vyznačují vysokou mobilitou, snadnou dostupností, a stále dokonalejšími technickými a softwarovými komponenty. Vybavení kvalitním přístupem k Internetu se stává standardem současných mobilních telefonů a integrovaný webovým browser má prakticky každé moderní komunikační zařízení. S postupným rozvojem bezdrátových sítí Wi-fi současně přichází na trh stále více přístrojů podporujících i tuto technologii (dokonce již i některé osobní multimediální přehrávače). Všechny tyto aspekty tak dohromady umožňují přístup k Internetu prakticky kdekoli. Tato skutečnost má vliv nejen na samotný chod informační společnosti, ale samozřejmě i na praktické využívání nástrojů vzdálené správy.

Administrátoři počítačových sítí využívají těchto možností moderních komunikačních zařízení především v okamžicích nenadálé situace, kdy není možné se v přijatelném čase přihlásit ke vzdálené správě pomocí plnohodnotného počítače. Je třeba si uvědomit, že s rostoucí mobilitou zařízení, úměrně klesá komfort využívání nástrojů vzdálené správy za pomoci některého z moderních komunikačních zařízení. Tento fakt je dán především miniaturizací displejů těchto přístrojů, neboť v porovnání se standardní počítačovou obrazovkou, se dá jakýkoli mobilní displej považovat za maličký. Z tohoto důvodu tak lze tyto moderní komunikační zařízení opravdu využít jen v případech nouze, neboť jakákoli dlouhodobější práce je velmi uživatelsky nepohodlná.

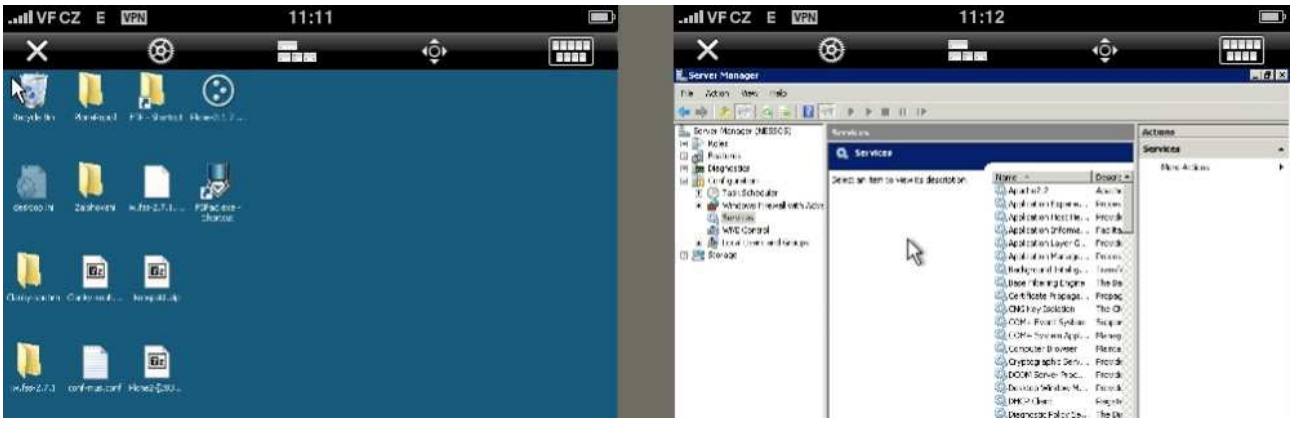
Pro konkrétní příklad si demonstrujme použitelnost nástrojů vzdálené správy na přístroji Apple iPhone. Ten je vybaven kvalitním displejem o velikosti úhlopříčky 3,5 palce, s rozlišení 320×480 pixelů. Zároveň lze orientovat obraz na displeji dle potřeb uživatele na výšku (vertikálně delší obraz), či na šířku (horizontálně delší obraz), což zvyšuje jeho využitelnost pro aplikace, které jsou v prostředí osobních počítačů standardně tvořeny právě pro delší horizontální stranu. Ovšem i u tohoto displeje můžeme narazit na překážky způsobené zmiňovanou miniaturizací. Nejlépe

lze tato omezení zmapovat na konkrétních případech, které jsou zdokumentovány vloženými obrázky, které svými rozměry odpovídají skutečné velikosti zobrazení na přístroji Apple iPhone.

Práci se vzdálenou plochou jsou reprezentovány obrázky pořízené při běhu aplikace Jaadu RDP, která je vytvořena jako iPhoneovský klient pro správu počítačů a serverů platformy Microsoft Windows.

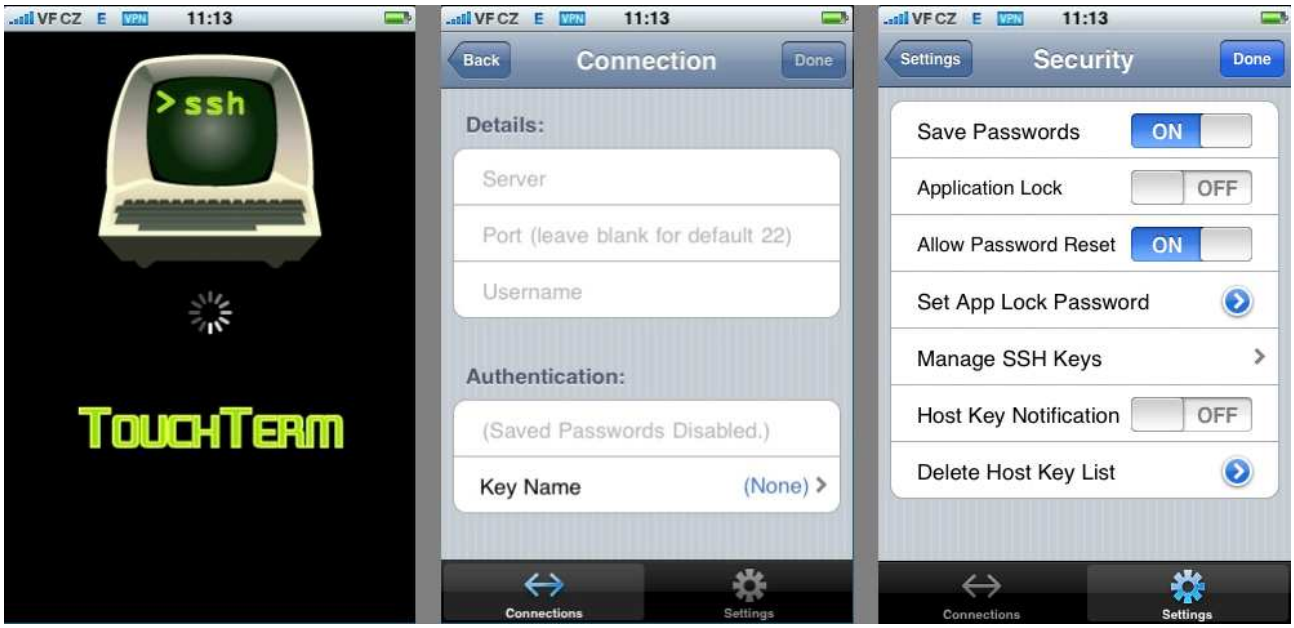
Obr. 1. Přihlašování ke vzdálené ploše aplikací Jaadu RDP pro Apple iPhone (zdroj: Mgr. Jan Pokorný, Ph. D.)

Na obr. 1. je názorně ukázán proces přihlašování klientské aplikace Jaadu RDP ke vzdálené ploše operačního systému Windows Web Server 2008. Při samotném přihlašování lze díky možnosti přibližování obrazu dosáhnout uspokojivé míry mezi zobrazením a uživatelským komfortem. Jistá omezení však přicházejí ihned po přihlášení.



Obr. 2. Vzdálená plocha v aplikaci Jaadu RDP pro Apple iPhone (zdroj: Mgr. Jan Pokorný, Ph. D.)

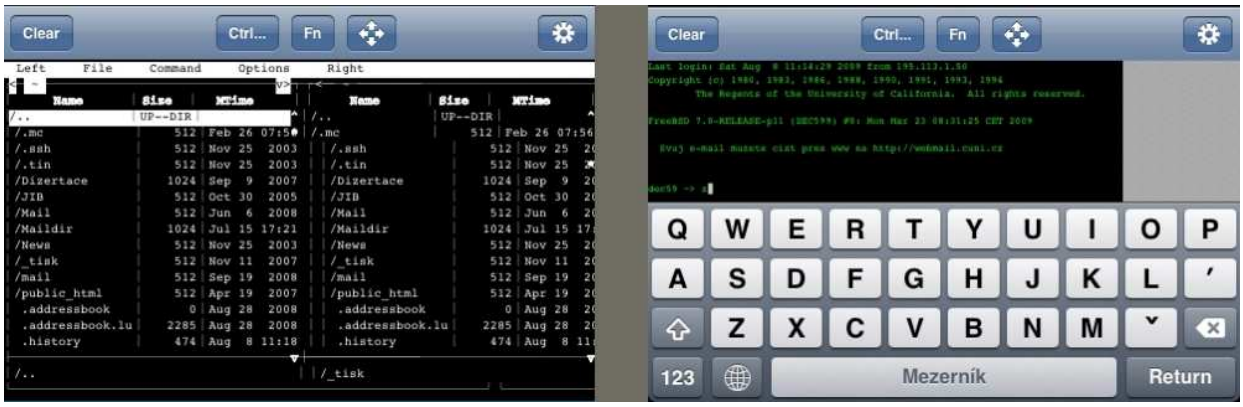
Zobrazení vzdálené plochy je i po změně orientace displeje nedokonalé (obr. 2.), neboť se zobrazuje jen část vzdálené plochy. Manipulace s ikonami na ploše je stále uživatelsky přijatelná, textové výpisy služeb běžících na vzdáleném počítači jsou však již mnohem méně přehledné. Daleko horší zkušenosti z hlediska uživatelského komfortu pak přinášejí aplikace využívající primárně textového rozhraní, jako jsou například terminálové služby. Jako příklad si předvedeme několik obrázků z aplikace TouchTerm, která poskytuje funkce zabezpečeného SSH terminálu pro Apple iPhone.



Obr. 3. Přihlášení a nabídková menu aplikace TouchTerm pro Apple iPhone (zdroj: Mgr. Jan Pokorný, Ph. D.)

Samotný proces přihlášení a případná volba nastavení je přehledná (obr. 3.). S přechodem do vlastního textového zobrazení terminálového okna však vznikají

první komplikace. To je dáno především pevnou šířkou okna. Přibližovat se zde nedá, pouze lze měnit velikost použitého fontu. Najít však vhodný kompromis mezi čitelností textu a dostatečnou mírou zobrazení je obtížné. Pokud si navíc zapnete klávesnici a chcete něco napsat, zmizí vám také více než polovina obrazu (obr. 4.).



Obr.4. Terminálové zobrazení v aplikaci TouchTerm pro Apple iPhone (zdroj: Mgr. Jan Pokorný, Ph. D.)

6.1 Vzdálená správa prostřednictvím služby SMS

V rámci vzdálené správy lze využít i v současnosti nejběžnější službu dostupnou na mobilních telefonech, službu krátkých textových zpráv (SMS). Specificky strukturované SMS zprávy odeslané na konkrétní přístupový bod, který je propojen s aplikací běžící na vzdáleném serveru a která interpretuje obdržené SMS zprávy jako textové příkazy, dokážou být šikovným nástrojem, když jsou ostatní technologie nedostupné (výpadek sítě Internet v okolí administrátora). S jejich pomocí lze obstarat ty nejdůležitější procesy, jako je například vytvoření nového uživatele, či restartování systému.

Závěr

Tato bakalářské práce analyzovala problematiku vzdálené správy počítačů se zaměřením na technologie a nástroje, které lze ke vzdálené správě využít. Zároveň však uvádí přímé zkušenosti se vzdálenou správou a její vliv nejen na současnou podobu informační společnosti, ale též nastiňuje možné budoucí trendy jejího vývoje.

V bakalářské práci je zpracována vzdálená správa několika typů, především v závislosti na nejvyužívanějších operačních systémech počítačů či konkrétních oblastech použití. Takovou oblastí využití je i samotný Internet, který je v současné informační společnosti považován za vůbec nejdůležitější a největší zdroj informací, především díky velmi krátké reakční době na aktuální dění. Tato aktuálnost by mohla být v případě výpadků technického rázu ohrožena, vzdálená správa jim jako jeden z nástrojů v rukou odborníků dokáže účinně předcházet, či je omezit na minimum.

Bez nástrojů vzdálené správy by byl v dnešní době provoz počítačových sítí obtížnější. Fyzická potřeba počítačových specialistů na každém jednotlivém bodě sítě, by prodražila veškeré služby, které jsou dnes na počítačové sítě jako takové přímo navázány. Zároveň tyto nástroje a služby mohou sloužit institucím, které zpřístupňují elektronické informace samotným uživatelům, a využívají větší množství síťově propojených počítačů pro vlastní agendu. Těmi jsou samozřejmě i knihovny, informační střediska a databázová centra, kterým může vzdálená správa ve formě služby ušetřit i finanční prostředky snížením přímých (mzdové, materiální) a nepřímých nákladů (minimalizace výpadků). Obecně lze říci, že se nevyplatí dedikovat interní pracovní sílu na správu počítačového vybavení, především menším knihovnám a takovým informačním institucím, které často nemění nastavení počítačových systémů či nevyvíjí extrémně specializované elektronické produkty.

Důležitým momentem se v celé společnosti stává situace, kdy si nástroje vzdálené správy postupně osvojuje i široká počítačová veřejnost. Ta dnes stále častěji vstupuje do těchto dříve výhradně specializovaných sfér. Tím si zároveň nevědomky zvyšuje svojí úroveň informační gramotnosti.

Seznam použitých zdrojů

- Adobe. *Adobe Labs*[online]. San Jose : Adobe Systems Incorporated, c2009 [cit. 2009-7-12]. Adobe AIR Technologies. Dostupný z WWW: < http://labs.adobe.com/technologies/air/>.

- ALLEN, Robbie; LOWE-NORRIS, Alistair G. *Active Directory.* 2nd ed. Sebastopol, CA : O'Reilly, 2003. xviii, 665 s. ISBN 0-596-00466-4.

- BARRETT, Daniel J.; SILVERMAN, Richard E. *SSH : The Secure Shell : The Definitive Guide.* 2nd ed. Sebastopol, CA : O'Reilly, 2005. xviii, 645 s. ISBN 0-596-00895-3.

- DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: Bezpečnost.* 2. vyd. Brno : Computer Press, 2003. 571 s. ISBN 80-7226-849-X.

- GIBSON, William. Neuromancer. 2nd ed. reprint. New York: Ace Books, 2000. ISBN 0-441-00746-5.

- HOLZNER, Steven. Mistrovství v AJAXu. 1. vyd. Brno : Computer Press, 2007. 591 s. ISBN 978-80-251-1850-4.

- How to enable and to configure Remote Desktop for Administration in Windows Server 2003. In *Microsoft Help and Support* [online]. Redmond : Microsoft Corporation, 2001- , last modif. on 30 October 2006 [cit. 2009-7-12]. Dostupný z WWW: < http://support.microsoft.com/kb/814590/en-us >.

- How to use the Administration Tools Pack to remotely administer computers that are running Windows Server 2003, Windows XP, or Windows 2000. In *Microsoft Help and Support* [online]. Redmond : Microsoft Corporation, 2001- , last modif. on 15 January 2008 [cit. 2009-7-9]. Dostupný z WWW: < http://support.microsoft.com/kb/304718/en-us>

- MAXWELL, Steve. *UNIX System Administration: A Beginner's Guide.* 1st ed. Osborne : McGraw-Hill, 2002. 675 s. ISBN 0-07-222833-4.

- Microsoft. *Windows Server 2008*[online]. Redmond : Microsoft Corporation, c2009 [cit. 2009-7-12]. Product Information. Technologies. Dostupný z WWW: http://www.microsoft.com/windowsserver2008/en/us/technologies.aspx

- NoMachine. *NX - Documentation* [online]. NoMachine, c2008 [cit. 2009-7-12]. Technology. Dostupný z WWW: http://www.nomachine.com/technology.php

- PETERKA, Jiří. Virtuální terminály. *Computerworld*. 1993, roč. 4, č. 23. ISSN 1210-9924.

- PETŘÍČEK, Miroslav. Síť aneb tělo bez orgánů. *Filosofický časopis*. 1998, roč. 46, č. 1. s. 67-71. ISSN 0015-1831.

- Remote Desktop Protocol. In *eTutorials.org* [online]. [S.l.] : eTutorials.org, 2008- , last modif. on 19 January 2008 [cit. 2009-7-19]. Dostupný z WWW: < http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+3+Communication+Protocols+and+Thin+Clients/Remote+Desktop+Protocol+RDP/>

- Remote Desktop Protocol. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001- , last modif. on 2 July 2009 [cit. 2009-7-12]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Remote_Desktop_Protocol >.

- RFC 1258. *BSD Rlogin* [online]. B. Kantor. September 1991 [cit. 2009-06-22]. 5 s. Dostupný z WWW: <ftp://ftp.rfc-editor.org/in-notes/rfc1258.txt>. ISSN 2070-1721.

- RFC 854. *Telnet Protocol Specification* [online]. J. Postel, J. Reynolds. May 1983 [cit. 2009-06-22]. 15 s. Dostupný z WWW: <ftp://ftp.rfc-editor.org/in-notes/rfc854.txt>. ISSN 2070-1721.

- RICHARDSON, Tristan. *The RFB Protocol.* Cambridge, 2009. 43 s. Technická zpráva. RealVNC Ltd.

- SCHEIFLER, Robert W. *X Window System Protocol***.** 1st ed. Massachusetts : MIT, c1994. 172 s.

- Terminal Server Patch. In *Sala Source* [online]. KOOD, 2003-2008, last modif. on 8 July 2008 [cit. 2009-7-15]. Dostupný z WWW: < http://www.kood.org/terminal-server-patch/>

- THOMPSON, Ken; RITCHIE, Dennis M. The UNIX Time-Sharing System, *Communications of the ACM*. 1974, vol. 17, no. 7, s. 365-375. ISSN 0001-0782.

- WOOLEY, Benjamin. *Virtual Worlds: A Journey in Hype and Hyperreality*.1st ed. NY: Blackwell, 1992. ISBN 0-14-015439-6.

Evidence výpůjček

Prohlášení:

Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze dne 9. 8. 2009

Matěj Vaněček

Jméno	Katedra / Pracoviště	Datum	Podpis