Videokonference za zdí

Eva Hladká, Petr Holub,
Michal Procházka, ÚVT a FI MU

S intenzivnějším využíváním sítí roste i potřeba zabezpečit lokální sítě a síťové aplikace. Dochází k uzavírání lokálních sítí za tzv. firewally (doslovně „ohnivé zdi", odtud název tohoto článku) za účelem omezení nežádoucích přístupů do lokální sítě [1]. Dalším dnes již obvyklým jevem je použití překladu adres – NAT (Network Address Translation) [2], kdy je celá lokální síť s privátním adresním rozsahem skryta za jednu či více veřejných IP adres. Praktickým důsledkem použití NATu je, že s počítači za NATem nelze z venku přímo navázat spojení.

Obě dvě tyto techniky – firewally i NATy tedy omezují komunikaci a je nutné se s nimi ve videokonferenčních aplikacích vypořádat. Problémy s uzavřeným prostředím ovšem nejsou specifické pouze pro videokonference, ale pro všechny aplikace vyžadující přímou komunikaci, např. pro některé typy distribuovaných výpočtů.

Tento článek je určen těm uživatelům, a také správcům LAN, kteří v prostředí sítí omezených NATy a firewally pracují a chtěli by využívat možností videokonferencí. Nabízené řešení bylo vytvořeno pro dva projekty 6. Rámcového programu EU pro oblasti lékařství a genetiky a je tedy prověřené ve velmi restriktivním prostředí klinických pracovišť v rámci téměř celé Evropy.

1 Kolaborativní prostředí

Videokonferenční systémy existují mnoho let a počet jejich uživatelů stále stoupá. Dnes to, co videokonferenční systémy nabízejí, překonalo pouhou komunikaci zvukem a obrazem a proto je lépe mluvit o kolaborativních prostředích, tedy systémech na podporu vzdálené spolupráce. Zde, ve Zpravodaji ÚVT, průběžně vychází články mapující tuto oblast a přinášející čtenářům informace o možnostech tohoto způsobu komunikace na MU. Přesto v tomto článku alespoň krátce zmíníme systémy, které zde dosud popsány nebyly.

Mezi v současnosti nejúspěšnější kolaborativní systémy široce rozšířené mezi uživateli patří ICQ [3] a Skype [4].

Systém ICQ je primárně určen k textové komunikaci, v současné verzi podporuje i hlasovou a video komunikaci. Videokonferenční systém založený na ICQ nelze použít k propojení více než dvou účastníků. Dále nesplňuje požadavky na provoz kolaborativního prostředí ve výše popsaném síťovém prostředí s NATy a firewally, protože protokol pro video i audio komunikaci není dostatečně robustní a vyžaduje přímé propojení mezi účastníky. Přenos dat není žádným způsobem zabezpečen[1] a množství nahlášených bezpečnostních incidentů v síti ICQ ukazuje, že tento systém není pro bezpečnou komunikaci vhodný.

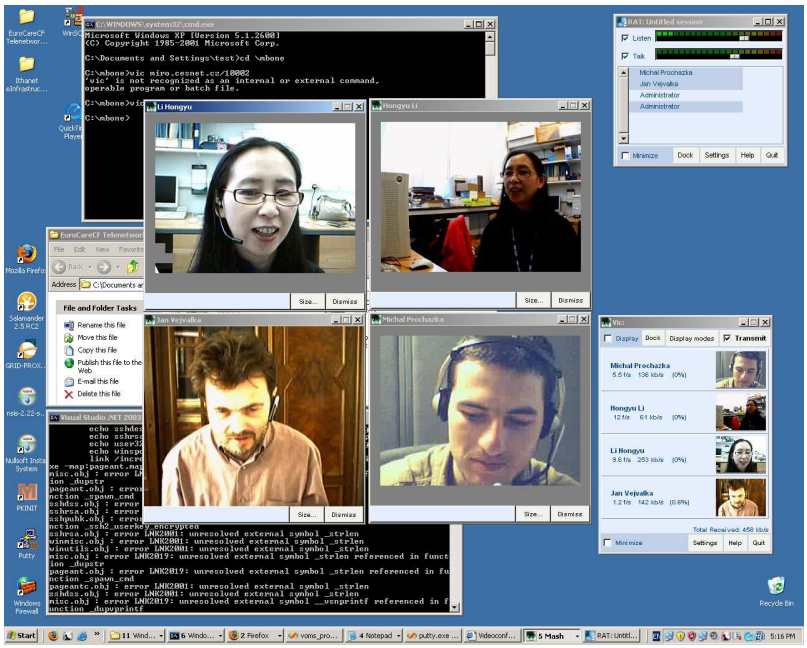
Síť Skype je primárně určena pro hlasovou komunikaci. V posledních verzích se objevila i podpora přenosu videa. K výhodám Skype patří šifrovaný přenos dat a možnost prostupovat firewally a NAT. Přes tyto výhody existuje také několik podstatných nevýhod. Protokol je jednak proprietární, a proto je velmi obtížně přesvědčovat síťové administrátory, aby ho povolili v omezené síti, řada pracovišť ho přímo zakázala. Navíc komunikace dvou účastníku, kteří jsou oba za NATem, je z technických důvodů možná jen proto, že přenos je realizován přes dalšího účastníka systému Skype, který má veřejnou IP adresu. Proto se všichni klienti systému Skype s veřejnou IP adresou stávají potencionálními prostředníky komunikace kterýchkoli ostatních klientů. Problémy sítě Skype byly podrobně popsány v několika článcích [5], [6].

2 Řešení

Kolaborativních systémů existuje celá řada, naším cílem je ale nabídnout řešení pro čtenáře, který pracuje v omezeném síťovém prostředí. Dalším omezením je i cenová dostupnost řešení a poměr ceny a výkonu.

Protože bylo jasné, že nic z dostupných systémů nesplňuje na 100 procent naše požadavky,

[1] Neaplikuje-li ovšem uživatel některý z dodatečných nástrojů jako PGP-ICQ (`http://www.samopal.com/soft/pgpicq/`) pro šifrování zpráv pomocí PGP.



Obrázek 1: EuroCareCF videoconference screenshot.

rozhodli jsme se pro vytvoření nového systému, který maximálně využije existující technologie a nástroje tak, abychom se mohli soustředit zejména na řešení problémů s omezeními síťové vrstvy.

Následující odstavce jsou věnovány spíše síťovým administrátorům a laický čtenář ho může projít velmi zběžně.

2.1 Požadavky

Systém musí poskytovat zabezpečený přenos dat. Celý systém musí být postaven na otevřených a ověřených formátech, protože přes tento systém budou data proudit z i do omezených vnitřních sítí. Otevřenost formátů je zejména důležitá pro síťové i systémové administrátory, kteří mohou protokol otestovat zda neporušuje lokální pravidla pro provoz aplikací. Na straně uživatele musí být samozřejmostí jednoduché ovládání a dostatečná škála poskytovaných služeb. Z aplikačního pohledu musí být systém dostatečně flexibilní, aby byl schopen poskytovat nejen audio a video přenosy, ale například také sdílenou pracovní plochu a instant messaging (posílání textových zpráv jako Jabber, IRC či ICQ). Flexibilita je zapotřebí i na úrovni jednotlivých aplikací. Například pro video přenosy nesmí být systém postaven pouze na jednom konkrétním video formátu, protože musí dostát požadavkům na přenos video signálu ve vysokém rozlišení a zároveň s nízkými nároky na přenosovou kapacitu – pro uživatele, kteří nemají dostatečně kapacitní připojení k síti.

Pro splnění výše zmíněných požadavků jsme celý systém rozdělili do tří vrstev. Síťová vrstva poskytne spojité síťovou infrastrukturu mezi všemi komunikujícími klienty pomocí přesně definovaného protokolu, který lze jednoduchými pravidly povolit na institucionálních firewallech. Musí také řešit problém s průchodností NATu a v neposlední řadě zajistit šifrovaný přenos dat. Síťová vrstva musí počítat s požadavkem, kdy nesmí existovat možnost jak klienta kontaktovat z veřejné sítě. Druhá vrstva distribuce dat poskytuje služby pro zprostředkování vzájemné komunikace klientských aplikací. Poslední vrstva se sestává ze samotných klientských aplikací a nástrojů. Aplikace by měly být jednoduše instalovatelné na klientský počítač a také jednoduše ovladatelné. Pro uživatele by se celá infrastruktura měla tvářit transparentně.

2.2 Síťová vrstva

Pro realizaci první vrstvy, tj. síťové vrstvy, jsme zvolili software OpenVPN [7]. OpenVPN je open source projekt, jehož hlavním cílem je vytvořit

vysoce bezpečnou virtuální privátní síť (VPN). Pro vytvoření této VPN sítě se nevyužívá běžný PPTP (Point To Point Protocol) protokol [8], ale síť je vybudována nad TCP nebo UDP protokolem, tzn. na aplikační vrstvě ISO/OSI modelu. OpenVPN splňuje námi kladené požadavky a to ve všech bodech. Protokol, který OpenVPN používá je zdokumentován a prakticky dobře ověřen, protože OpenVPN je již několik let velice aktivně používáno. Data mezi klientem a serverem jsou šifrována na úrovni TLS (Transport Layer Security). Pro autentizaci se využívá sdílený klíč nebo lépe infrastruktura veřejných klíčů (PKI - Public Key Infrastructure), kdy je každý uživatel vybaven vlastním osobním certifikátem, kterým prokazuje serveru svoji identitu. Jelikož server disponuje také certifikátem je autentizace oboustranná a uživatel si je jist, že komunikuje se správným VPN serverem a server ví kdo komunikuje s ním.

2.3 Videokonferenční server

Druhá vrstva, která poskytuje službu videokonferenčního serveru, se sestává z komunikačního zrcadla [9]. Tento software slouží k distribuci dat mezi účastníky videokonference. Zrcadlo běží na stejném stroji jako OpenVPN server a veškerá audiovizuální komunikace mezi uživateli probíhá přes toto zrcadlo. Uživatelé se připojí do konference spuštěním videokonferenčních nástrojů, které kontaktují komunikační zrcadlo a to jim začne přeposílat data od ostatních přihlášených účastníků. Zrcadlo může být zkonfigurováno tak, aby provádělo manipulaci s daty ve smyslu překódování video streamu, synchronizaci audio a video kanálu, normalizaci zvuku apod. Každý klient, který chce využívat služeb zrcadla musí mít jedinečnou IP adresu z pohledu komunikačního zrcadla. Tento požadavek byl vyřešen použitím "bridged" režimu tunelu OpenVPN, kdy každý klient obdrží IP adresu z rozsahu veřejných adres, ale tyto IP adresy nejsou směrovány do Internetu[2].

[2]Tento na první pohled komplikovaný přístup se využívá z toho důvodu, že v různých participujících institucích se využívají různé rozsahy privátních IP adres a těžko bychom mohli spolehlivě vybrat nekonfliktní privátní rozsah adres přidělovaná tunelem OpenVPN. Proto jsme zažádali o veřejný segment, který je pro účely kolaborativního prostředí blokován jednou z participujících institucí a tím pádem nesmí být použit jinde.

2.4 Klientské aplikace

Klientská vrstva je v současné implementaci realizována videokonferenčními nástroji MBone Tools. Obsahují nástroje pro audio přenos dat RAT (Robust Audio Tool) a video přenos dat VIC (Video Conference Tool). Oba nástroje využívají protokol UDP a pro vícebodovou distribuci dat komunikační zrcadlo.

Součástí implementace bylo také vytvoření instalačních balíčků, které mají umožnit jednoduché nasazení videokonferenčního systému na klientské stanice. V první fázi jsou vytvořeny balíčky jen pro operační systém Microsoft Windows. Instalační balíček byl rozdělen na dva: pro administrátory a pro uživatele. Rozdělení bylo nezbytné, protože uživatelé počítačů obvykle nedisponují administrátorskými právy a instalace OpenVPN tato práva vyžaduje. Po instalaci je uživateli poskytnuto rozhraní, které mu dovoluje se k videokonferenci připojit a odpojit, kroky spojené s navázáním spojení a spuštěním videokonferenčních nástrojů se dějí plně automaticky.

3 Ověření

První, co asi pozorného čtenáře napadne, bude otázka o použitelnosti. Řešení splňuje požadavky, je dostatečně jednoduché pro uživatele, ale bude dostatečně výkonné? Pro komunikaci platí poměrně přísná omezení týkající se zpoždění [10]. Kdyby díky popsanému mechanismu mělo zpoždění narůst nad přípustnou mez, byl by celý systém k ničemu. Proto bylo provedeny testy a jejich výsledky jsou shrnuty v tabulce 1.

Je vidět, že řešení je přijatelné a použitelné a nezhorší nad vnímatelnou mez kvalitu komunikace.

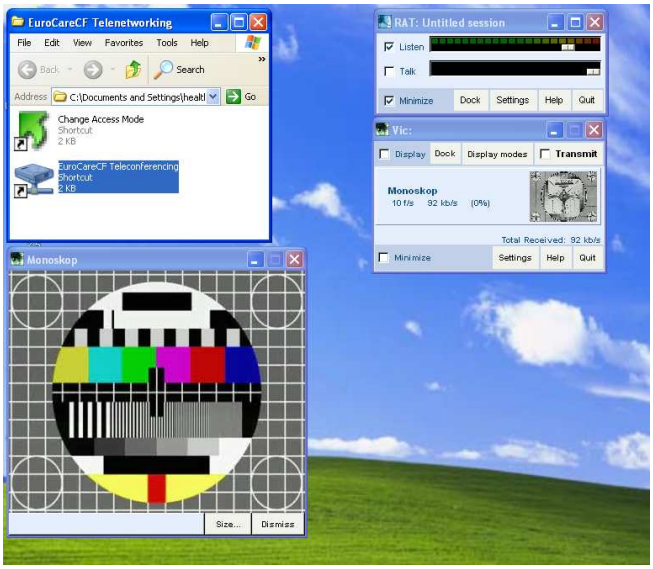
3.1 Pilotní provoz

Jak už bylo řečeno v úvodu, systém vznikal pro dva medicínské projekty 6. RP EU a byl tedy ověřen v geograficky rozsáhlém a přitom velmi omezeném síťovém prostředí, navíc v uživatelské komunitě, která není zaměřena technicky. Za 6 prvních měsíců provozu se podařilo pokrýt zhruba 50 % řešitelů projektů, uskutečnilo se 214

	bez VPN	UDP VPN	TCP VPN	TCP VPN + HTTP proxy
pchar latency [ms]	3.51	3.69	3.94	3.93
iperf jitter [μs]	6	6	9	13
pchar capacity est. [Mb/s]	39.8	35.2	20.1	19.8
iperf packet loss @ 30 Mb/s [%]	0.0	0.0	0.0	0.0
iperf CPU idle @ 30 Mb/s [%]	48.9±0.2	41.7±0.4	44.5±0.4	42.6±0.4

Tabulka 1: Testy přenosu dat přes OpenVPN server

připojení na komunikační zrcadlo (videokonference + testy) a 51 videokonferencí. Pro potřeby testování byla na zrcadle zřízena komunikační smyčka, která vysílá obraz monoskopu a umožňuje testovat a ladit spojení nezávisle na dalších účastnících.



Obrázek 2: Monoskop pro testování.

4 Závěr

Videokonference představují kolaborativní prostředí, které si klade za cíl umožnit komunikaci lidem v různých oblastech. Se současnými prostředky je však stále poměrně náročné vytvořit zabezpečené kolaborativní prostředí, které bude schopno pracovat na jakémkoli typu sítí – od pomalých a mobilních až po vysokorychlostní.

Nabízíme čtenáři a potenciálnímu uživateli pohled na systém, který poskytuje konferenční nástroje pro omezené síťové prostředí, ověřený na příkladu nemocnic a výzkumných laboratoří, kde je kladen velký důraz na bezpečnost. Systém také splňuje požadavky na jednoduché ovládání, které je v prostředí uživatelů s jiným než technickým zaměřením nezbytné. Pilotní testování ukázalo, že je tento systém použitelný a akceptovatelný nejen ze strany uživatelů, ale i systémových administrátorů. Obecná nechuť administrátorů povolovat komunikaci s vnějším světem pro uživatele uvnitř omezených sítí je tak poněkud zmírněna jednoduchostí technického řešení, navíc s jasnou a přehlednou informací pro správce sítí o tom, že po takto vytvořeném OpenVPN spojení budou posílána pouze data pro spojení se zrcadlem a že provoz této sítě nebude dále šířen do veřejného Internetu.

Literatura

[1] Rychnovský L., *Počítačová bezpečnost.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI, č. 1, s. 13–16.

[2] NAT: `http://www.abclinuxu.cz/slovnik/nat`

[3] ICQ: `http://www.icq.com`

[4] Skype: `http://www.skype.com`

[5] Biondi P., Desclaux F., *Silver needle in the Skype*, BlackHat Europe. `http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf`, Duben 2007.

[6] Baset S.A., Schulzrinne H., *An analysis of the Skype peer-to-peer internet telephony protocol*, INFOCOM 2006, Barcelona, Španělsko. `http://www1.cs.columbia.edu/~salman/publications/skype1_4.pdf`, Duben 2007.

[7] Hosner Ch., *OpenVPN and the SSL VPN Revolution*, Sans Institute, Březen 2004. `http://www.sans.org/reading_room/`

whitepapers/vpns/1459.php, Duben 2006.

[8] Hamzeh K., Pall G., Verthein W., Taarud J., Little W., Zorn G., *Point-to-Point Tunneling Protocol (PPTP)*, RFC 2637. ftp://ftp.isi.edu/in-notes/rfc2637.txt, Duben 2006.

[9] Hladká E., Holub P., *Zrcadla v počítačové síti*, Zpravodaj ÚVT MU. ISSN 1212-0901, 2002, roč. XII, č. 5, s. 7–10.

[10] Holub P., Hladká E., Matyska L., *iGrid2005*, Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVI, č. 3, s. 12–16. □