ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • únor 2006 • roč. XVI • č. 3

Elektronické diplomky a bakalářky na ESF MU: dokončená mise

Jaroslav Nekuda, Jiří Poláček, ESF MU

Prolog

Psal se rok 2002 a jeden z autorů tohoto článku procházel ráno, ještě před otevřením knihovny (SVI) Ekonomicko-správní fakulty Masarykovy univerzity v Brně, mezi regály s knihami, diplomovými a bakalářskými pracemi. Jeho pozornost zaujala převeliká, ještě neuklizená a nezařazená hromada závěrečných prací. Zablikalo červené světýlko: *Bože, kdo má ty hromady rozkrámovaných věcí pořád dokola uklízet?* A jen co se uklidí, hned je zase studenti – v lepším případě – *roztahají*, v tom horším se pak budou snažit je, buď celé nebo jejich části, odnést z knihovny navěky. Nejlepší by bylo, kdyby tady ty věci snad ani nebyly. Ale co lepšího místo nich? Třeba jen elektronické obrazy? A jako obvykle: zrozen z přirozené lidské snahy o eliminaci zbytečné a otravné práce – nápad byl na světě!

Tak byl odstartován příběh, který došel ke svému úspěšnému završení na sklonku roku 2005. Na jeho konci je knihovna, v níž fyzicky nejsou závěrečné studentské práce v klasické, papírové podobě. Byly nahrazeny elektronickými formami. Část z nich je dokonce zcela volně k dispozici v síti Internet.

Koho by zajímal takový příběh se šťastným koncem, může ve čtení pokračovat.

Fáze I. Definování úlohy, hledání zdrojů a podpory

Myšlenku, která tak náhle spatřila světlo světa, bylo třeba maličko domyslet, zvážit celou logistiku projektu, kvantifikovat potřebné zdroje a najít pro ni – řekněme – politickou podporu. Díky značné míře osvícenosti tehdejšího vedení fakulty se všeho podařilo v poměrně krátké době dosáhnout. „Moderní“ myšlenka dopadla ve správný čas na úrodnou půdu a bylo možné začít ve věci konat. Pro představu – na regálech v té době ležely téměř dvě tisícovky diplomových a bakalářských prací publikovaných od roku 1996. Ty jsme se rozhodli zpětně digitalizovat a počínaje již rokem 2002 jsme chtěli zahájit vybírání závěrečných prací nejen v klasické papírové, ale i v elektronické podobě.

Fáze II. Zachytit včas to, co by mohlo vbrzku uniknout

Počátkem roku 2002 bylo třeba bezodkladně učinit opatření k zachycení právě dopisovaných závěrečných prací v elektronické podobě. Byl přichystán pokyn děkana, který specifikoval standardy odevzdávaní závěrečných kvalifikačních prací. Ukládal studentům mimo jiné též povinnost odevzdávat práce i v elektronické podobě v obvykle užívaných formátech (Word, MS Works,

WIN-602, Open Office apod.). Později se tento pokyn (každoročně ještě podle okolností upřesňovaný) stal standardní součástí studijních předpisů. Kromě toho byl vytvořen i jednoduchý formulář, v němž budoucí absolventi vyjadřovali svou vůli, zda bude možné jejich práce (hned anebo se zpožděním 1–3 let) volně vystavovat v síti Internet. Těmito dvěma akty bylo o budoucnost plně postaráno. Co by bývalo mohlo v dané etapě nenávratně uniknout, bylo pevně zachyceno, a tak bylo možné se naplno věnovat aktivitám ve stylu „retro".

FÁZE III. Dvojí kouzlo „retro"

Oříškem byl způsob, jak se zmocnit té velké hromady starých papírových prací a převést je do elektronické podoby. Zvolili jsme dvojí cestu. Hromadným dopisem jsme se obrátili na bývalé absolventy a požádali je, aby nám své práce – pokud je ještě mají v elektronické podobě – poslali. Daný způsob se ukázal být docela plodným, neb se nám takto podařilo získat celkem 160 dokumentů. Nedobytný zbytek jsme digitalizovali opět dvojím způsobem. Buď na velkém knižním skeneru nebo – v případě, že existovaly dva výtisky od práce – jsme druhý výtisk jsme prostě a jednoduše rozřezali a práci skenovali na skeneru s podavačem, což bylo samozřejmě mnohem elegantnější a rychlejší. Bakalářské práce jsme řezali bez ohledu na to, zda existoval nebo neexistoval druhý výtisk. Nedobrovolně se tak staly aktéry příběhu *plného násilí na knihách*. Vlastní retro-digitalizace trvala zhruba jeden rok.

FÁZE IV. Finále a rutinní provoz

Koncem roku 2005, kdy jsme získali a zpracovali poslední elektronické dokumenty z podzimních termínů obhajob, byly vytvořeny všechny předpoklady pro finalizaci projektu. Tedy odstěhování papírových prací do odlehlého a potemnělého skladu a zpřístupnění jen elektronických forem akademické obci v knihovně. A – samozřejmě – také veřejné prezentaci závěrečných prací, u kterých jsme získali souhlas autorů k publikování na Internetu. Vedení fakulty závěrečný krok odsouhlasilo a tak dne 29. 11. 2005 byla část prací „se souhlasem" zveřejněna i na Internetu (zde – `http://www.econ.muni.cz/svi/zaverecne_prace/`). Popisovaná mise byla z tohoto pohledu ukončena. Informace o projektu proběhly v denním tisku, informoval i týdeník Ekonom a další periodika. Z archivu bylo za první měsíc volného provozu zpřístupněno přes 1 200 prací, denně je prohlédnuto nebo staženo průměrně 55 dokumentů. Celkově je potěšitelné, že v dlouhodobé perspektivě získáváme souhlas cca 85 % posluchačů k publikování závěrečných prací na webu. Situaci v posledních 4 letech ukazuje tabulka:

	2002	2003	2004	2005
DP se souhlasem	141	226	218	174
DP bez souhlasu	44	24	31	62
BP se souhlasem	76	170	148	206
BP bez souhlasu	22	15	19	31

Technické a administrativní specifikace projektu

Sjednocen byl také prezentační formát – veškeré práce v archívu jsou předkládány ve formátu PDF. Do tohoto formátu jsou ručně převáděny buď „tiskem" z textového editoru, pokud byla práce získána v elektronické podobě, nebo přímým skenováním v programu Adobe Acrobat, pokud byla práce k dispozici již jen v papírové podobě. Veškeré práce jsou pak digitálně podepsány a interním mechanismem formátu PDF zabezpečeny tak, že zakazují prohlížeči souborů PDF tisk těchto prací a kopírování částí jejich obsahu.

Patrně technicky nejzajímavější komponentou archívu ZP je jejich zpřístupnění v terminálovém režimu ze všech počítačů v knihovně ESF. Využívá se technologie NX společnosti No Machine; konkrétně je implementována volně dostupná aplikace FreeNX na linuxovém serveru, ke kterému se lze připojit jak z linuxových, tak windowsových stanic. Princip terminálového přístupu spočívá ve skutečnosti, že uživatel se na terminálový server přihlásí výhradně skrze speciálního klienta, který na klientskou stanici pouze přenáší obraz toho, co má na serveru spuštěno – a zde je uživateli dovoleno spustit pouze prohlížeč Adobe Reader a v něm otevírat závěrečné práce přístupné v režimu pro

čtení. Jinými slovy uživatel nemá možnost kopírovat si soubory závěrečných prací ze serveru někam „k sobě“. Terminálový režim tak čtenářům knihovny umožňuje nahlížet do prací, ke kterým nebyl dán souhlas s publikováním na Internetu.

Prozatím zůstává vyhledávání v archivu ZP oddělené od knihovního katalogu, podnikáme však kroky k tomu, aby se elektronický archiv časem stal jeho transparentní součástí. V současné době tedy přebíráme částečně automatizovaným způsobem záznamy z knihovního katalogu a konvertujeme je do podoby souborů XML, které tvoří obsah vlastního vyhledávacího systému.

Postupem času jsme do naší rutinní administrativní agendy také zařadili tzv. Licenční smlouvy (vzor je k nalezení zde – `http:www.econ.muni.cz/data/vzorLS.doc`), které lépe a přesněji vymezovaly autorsko-právní stránku vztahu mezi absolventy a užitím jejich děl na půdě fakulty i povolení k eventuálnímu vystavení dokumentů na webu. Byla také vytvořena obecná ilustrativní šablona pro závěrečné studentské práce (k nahlédnutí zde `http://www.econ.muni.cz/data/vzorDP.doc`), aby tyto splňovaly jisté minimální standardy administrativní „štábní kultury“.

Závěrečné poznámky

Při snaze o ušetření lidské práce jí bylo třeba vynaložit *mnoho a mnoho*. Je jen obtížně odhadnutelné, kdy náklady a pracnost projektu budou v budoucnosti – obrazně řečeno – „zaplaceny“ původně zamýšlenou úsporou práce spojenou s tříděním, ukládáním a manipulací. Dost možná, že to ani vbrzku nebude.

Avšak uživatelský komfort, přímý internetový přístup, úspora místa, ochrana původních dokumentů a celkově přitažlivý design celého modernizačního projektu jsou faktory, které jasně dominují na straně profitů. Nezanedbatelným pozitivem může být koneckonců i jistý prestižní moment plynoucí z faktu, že se s velkou pravděpodobností jedná o první ucelený a plně funkční projekt tohoto druhu v ČR.

Zajímavý prvek do celé této oblasti vnáší aktuální novela Zákona o vysokých školách, která v § 47b Zveřejňování závěrečných prací stanoví, že vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Bude zajímavé sledovat, jak se k této novince vysoké školy postaví a jakých nových počinů budeme v této – tak náhle l iberalizované – oblasti svědky.

Literatura

[1] J. Nekuda. Retrodigitalizace diplomových a bakalářských prací v SVI ESF MU aneb od papíru k elektronickým obrazům? Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč. 15, č. 1, s. 9-11. □

S čárovými kódy na majetek

Jana Kohoutková, Zdeněk Machač, ÚVT MU

Ve čtvrtém čísle loňského ročníku Zpravodaje (přibližně před rokem) vyšel článek o elektronické podpoře evidence majetku na MU, rekapitulující dané téma od počátku jeho historie po současnost. Článek skončil výhledy do roku 2005 a příslibem, že se téma na stránky Zpravodaje vrátí. V těchto dnech, kdy se na MU účetně uzavírá rok 2005, je vhodná doba slib splnit a ohlédnout se, co se v loňském roce kolem majetku událo.

1 Jak jsme začínali

Do roku 2005 vstupovala MU s veškerým majetkem uloženým ve společné celouniverzitní databázi, tedy s úplnou elektronickou evidencí jak nemovitostí tak investičního i drobného movitého majetku. Tento majetek byl a je spravován jednak aplikacemi modulu *Majetek* ekonomického informačního systému *Magion*[1] (primárně určenými správcům majetku na úrovni hospodářských středisek MU[2]) a dále aplikacemi *Inetu MU*(určenými správcům majetku na úrovni

[1] EIS Magion společnosti Magion Vsetín provozuje MU od roku 1998.

[2] Hospodářskými středisky MU jsou rektorát, fakulty, ústavy a pracoviště s celouniverzitní působností.

dílčích pracovišť, vedoucím těchto pracovišť a jednotlivým osobám, které za majetek odpovídají).

Majetek je až na odůvodněné výjimky fyzicky označen evidenčními/inventárními štítky a jednou ročně, na podzim, probíhá inventura toho, zda evidovaný majetek na MU skutečně existuje a v kladném případě zda se nachází na předpokládaném místě. Tradičně se inventura provádí odškrtáváním nalezených předmětů majetku v papírových seznamech, v posledních letech se však na MU uchytila myšlenka využívat snímače čárového kódu. Několik fakult tuto myšlenku zrealizovalo v podobě lokálních softwarových řešení a polepilo čarokódovými inventárními štítky své majetky. Bylo však jasné, že duplicitně (jak centrálně tak lokálně) lze evidenci majetku vést jen velmi dočasně a v malém rozsahu, a že je potřeba navrhnout a zrealizovat vhodné centrální řešení.

Takto tedy vypadala situace před rokem, kdy jsme se do úkolu centrálně zavést do evidence a inventarizace majetku MU čárový kód pustili. Hned zkraje je třeba říci, že „my“ znamená tým složený z pracovníků RMU (ekonomického a provozního odboru) a ÚVT, referentů majetku na fakultách (děkanátech i katedrách) a zaměstnanců dvou externích dodavatelských firem (již zmíněné společnosti Magion a společnosti ICS, o níž bude řeč dále).

2 Jak jsme pořídili kódy

Kódy, které jsou ve výsledku vytištěny na štítcích v čárové podobě, jsou v evidenci majetku nutné dvojí: jednak pro vlastní *předmět* majetku a dále pro *lokalitu* (zpravidla místnost), v níž se majetek nachází.

U lokalit byla situace MU jednodušší v tom, že v rámci pořízení stavebního pasportu v roce 2004 byly jednotně a centrálně nadefinovány a přiděleny tzv. *polohové kódy* budov a místností a tyto mohly být (a byly) použity pro vytvoření čárového kódu. Při vzniku a zaevidování nových budov a místností se nyní polohové neboli čárové kódy přidělují průběžně. [3]

U předmětů bohužel žádný z existujících údajů nebyl pro účely čárových kódů vhodný, takže jim musel být hromadně vygenerován zcela nový údaj – *čárový kód* majetku. Situaci zpestřila skutečnost, že fakulty, které začaly čárový kód zkoušet již dříve a lokálně, měly u svých starších předmětů kódy již vygenerovány – přirozeně každá fakulta se svým prefixem, takže o souvislé řadě čárových kódů k majetkům nemohlo být ani řeči. (Variantu vygenerovat znovu všechny kódy v souvislé řadě a existující štítky přelepit jsme zavrhli dříve, než by ji – i s námi – zavrhly fakulty.) Kódy k již existujícím předmětům byly proto nejprve přeneseny z lokálních úložišť fakult do centrální databáze a následně hromadně dogenerovány pod několika dohodnutými prefixy (obojí zajistil ÚVT). Kódy k nově pořizovaným a evidovaným předmětům se od konce loňského května automaticky generují v EIS Magion s dříve nepoužitým prefixem „6“ (jak si mohou čtenáři ověřit na nejnovějším vybavení svých kanceláří), což zajišťuje jedna z funkcí EIS Magion, realizovaná loni na jaře na objednávku MU.

3 Jak se tiskne a tisklo

Máme-li kódy, můžeme tisknout štítky. Do hry tím vedle dodavatele EIS Magion vstoupil druhý externí dodavatel, jímž se na základě výběrového řízení stala pražská společnost ICS Identifikační systémy. Tento dodavatel dodal MU především softwarové vybavení pro snímače čárového kódu (o nichž si povíme dále) a také parametrizovatelné šablony pro tisk evidenčních štítků – různé pro místnosti (lokality) a pro předměty. Vlastní softwarové řešení tisku bylo vytvořeno v ÚVT. A jak to celé funguje?

Především musí být k uživatelské stanici připojena specializovaná tiskárna a dále musí být nainstalována tisková komponenta vytvořená v ÚVT. Na straně serveru je nutná formátovací komponenta, která přijímá na vstupu údaje pro potisk štítku (jednoho nebo více), obalí je příslušnou šablonou a vytvoří tak tiskový soubor pro tiskovou komponentu. Pro tisk štítků lokalit je formátovací komponenta součástí aplikace *Přehledy budov a místností* Inetu (což je jedna z aplikací pro fakultní správu nemovitostí), pro tisk

[3] Polohové kódy musely být hromadně vygenerovány a musí být dále průběžně generovány i pro místnosti v cizích budovách, které MU nevlastní, pouze užívá.

štítků předmětů je nainstalována na terminálových serverech Rumbur, kde je volána z aplikací Magionu (jimiž je zajišťována fakultní správa majetku).

Aplikace *Přehledy budov a místností* je dostupná jak v sekci *Ekonomika → Majetek*, tak v sekci *Služby ICT/FM → Facility Management* a umožňuje tisk štítků pro jednotlivé místnosti nebo pro celá podlaží budov. Kliknutím na příslušnou ikonu se vygeneruje tiskový soubor, jehož otevřením se aktivuje tisková komponenta. Aplikace správy majetku v Magionu pracují poněkud složitěji, především kvůli vzájemnému odstínění dvou nezávislých externích dodavatelů, kteří chtěli zůstat nezávislými, a také díky technickým omezením terminálového serveru. Kliknutím na funkci tisku pro předem vybranou skupinu předmětů se údaje pro potisk vygenerují do souboru, spustí se formátovací komponenta a výsledek se odešle uživateli jako soubor v příloze e-mailu. Kliknutím na tuto přílohu se opět aktivuje tisk.

Popsaným způsobem se od loňského května tisknou štítky u nově zaváděných lokalit a předmětů, ke starším byly štítky vytištěny hromadně a externě. Etapu, která následovala po hromadném vytištění štítků a jejich distribuci na jednotlivá hospodářská střediska, raději nebudeme více rozebírat a omezíme se jen na vyjádření úcty k mravenčí práci všech těch, kdo během letních prázdnin umístili na správné předměty a dveře místností desetitisíce čárokódových štítků.

4 Jak pracují čtečky

Máme-li štítky, můžeme je číst – opět díky externímu dodavateli ICS a jeho programovému řešení mobilních snímačů čárového kódu, které ve stručnosti pracuje takto: Snímač se nejprve hromadně naplní údaji z centrální evidence majetku o lokalitách a předmětech, které by v nich měly být, a předá je tomu, kdo provádí inventurní kontrolu. Kontrolor pak prochází jednotlivé lokality a postupně snímá čárové kódy – vždy nejprve kód lokality a poté kódy všech v ní umístěných předmětů. Snímač údaje zaznamenává a zpracovává (včetně průběžného upozorňování na nenalezené předměty) a v konečném výstupu poskytuje čtyři druhy seznamů: seznam předmětů nalezených v očekávaném umístění, seznam předmětů nalezených v jiném umístění (tzv. přesuny), seznam nenalezených předmětů (tzv. manka) a seznam předmětů nalezených nad rámec očekávání (tzv. nálezy). Tyto seznamy se hromadně předávají přes komunikační modul zpět do centrální databáze majetku k dalšímu zpracování.

5 Jak se inventarizuje ponovu

Inventarizace „ponovu“ znamená, že se k již popsanému softwarovému vybavení snímačů vytvoří podpora pro export a přenos dat z centrální databáze, pro přenos a import dat do centrální databáze a pro zpracování naimportovaných dat v centrální databázi. Pro MU byla veškerá tato podpora vytvořena v ÚVT jako součást Inetu v sekci *Ekonomika → Majetek*, s využitím komponenty pro komunikaci se čtečkami (předávání a přebírání dat do/ze čteček), rovněž externě dodané společností ICS.

V Inetu tak vznikla trojice aplikací, pracující nad tzv. *inventurní databází*, která se každý rok při zahájení inventury musí hromadně naplnit z centrální databáze aktuálními údaji o veškerém majetku, který je k datu inventury, tedy k 30. září, v užívání. Aplikacemi, o nichž je řeč, jsou *Export dat ze snímače*, *Import dat ze snímače* a *Inventurní sestavy*. Aplikace pro export a import umožňují vygenerovat, předat a převzít soubory dat o majetku užívaném na jednotlivých *inventárních úsecích*, což jsou předem určené (a schválené) skupiny pracovišť MU (pro každý rok se inventární úseky vytvářejí a schvalují znovu). Inventurních sestav je celkem šest typů – *Počty majetků v místnostech*, *Soupisy nedohledaného/přebývajícího majetku*, *Změny umístění*, *Manka vs. Přebytky*, *Soupis nedohledaného majetku dle místností* a *Statistika průběhu inventury* – a jsou k dispozici k prohlížení i pro tisk (ve formátu pdf).

Inventura je zahajována a ukončována jednotně pro celou MU – ukončením se znepřístupní aplikace exportu a importu dat, zatímco sestavy zůstávají dostupné až do další inventury. Po ukončení inventury se hromadně aktualizuje centrální databáze majetku podle zjištěných přesunů (tzv. *neúčetní převody*) majetku… a obnovuje se

její běžný provoz. Údaje o mancích a nálezech slouží jako podklady pro následné účetní operace – tedy *účetní převody* majetku mezi různými pracovišti a řešení *ztrát* (škod).

Všechny vyjmenované aplikace jsou určeny referentům majetku a běžný uživatel Inetu k nim nemá přístup. Jako bonus – aby to uživatelům nebylo líto a hlavně pro svou užitečnost – vznikla v Inetu v souvislostí s inventarizací ještě jedna aplikace, dostupná všem – *Informace o nalezeném majetku*.

6 Jak se inventarizovalo v roce 2005

Na závěr se sluší uvést několik souhrnných a statistických údajů.

V roce 2005 se na MU inventarizovalo částečně tradičně a částečně nově. „Postaru“, způsobem papír+tužka, inventarizovali na LF, PřírF, FF, FSS a v SKM. Tato hospodářská střediska dostala pro rok 2005 výjimku z povinnosti přejít u majetku na evidenci a inventarizaci čárovým kódem kvůli probíhajícím rekonstrukcím a rozsáhlému stěhování osob a majetku, kdy nebylo myslitelné nalepit (a posléze nasnímat) desetitisíce čárokódových štítků. Všechna ostatní hospodářská střediska MU již inventarizovala čárovým kódem.

Celkem bylo hromadně vytištěno a v průběhu prázdnin nalepeno asi 4 400 evidenčních štítků místností a více než 62 000 inventárních štítků předmětů.

Jako vedlejší aktivita ÚVT bylo rovněž v letních měsících přeneseno přibližně 191 000 záznamů majetku uložených v centrální databázi ze starého úložiště (databáze Informix na samostatně provozovaném serveru) do nového (databáze Oracle na dvojici serverů provozovaných v klastru zajišťujícím bezvýpadkový provoz) včetně celého ekonomického systému Magion.

Inventuru provádělo 85 inventarizačních komisí na stejném počtu inventárních úseků, které měly k dispozici ke své práci 35 snímačů čárového kódu. První export provedlo dne 11. 10. několik inventarizačních komisí Pedagogické fakulty (PedF se mimochodem projevila jako nejobratnější čárokódující fakulta) a Fakulty sportovních studií. Datum posledního exportu dat do snímače bylo 14. 11. a jednalo se (nepřekvapivě) o majetek UKB.

A na úplný závěr: Do řešení projektu byl investován nemalý, blíže neevidovaný počet hodin. Autoři článku by proto rádi využili této příležitosti k poděkování všem, kdo se na práci podíleli. Myslíme si – a věříme, že nejen my – že se jedná o zdařilé dílo jak z pohledu výsledků, tak z pohledu pracovní atmosféry, ve které vznikalo. □

Do Gridu snadno a rychle – prostředí VOCE

Daniel Kouřil, Jan Kmuníček, ÚVT MU

Pojem *Grid* se objevil v devadesátých letech minulého století jako nová forma distribuovaného zpracování informací a řešení složitých problémů. Gridy se zpočátku soustředily primárně na oblast náročných výpočtů, ale postupně pronikají i do jiných oblastí, které mohou profitovat z řešení, která byla vytvořena v rámci rozvoje Gridů. Za všechny lze jmenovat např. oblast digitálních knihoven, e-learningu nebo kvalitních videokonferenčních či multimediálních nástrojů. Gridy se také vždy pohybovaly na horní hranici technologických možností a přitahovaly pozornost řady odborníků jak z akademického prostředí tak z IT průmyslu. Více informací o Gridech, jejich možnostech a vývoji lze nalézt v článku „Gridy jako klíčový fenomén informačních technologií nového tisíciletí“ v předchozím čísle Zpravodaje.

Po řadě let intenzivního vývoje se v současné době Gridy dostávají do fáze, kdy se přibližují běžným uživatelům, kteří tak mohou začít využívat možností, které gridová prostředí nabízí. Vzhledem k enormnímu zájmu, který o gridové technologie panuje, a obrovskému úsilí a množství prostředků, které byly do jejich vývoje investovány v minulém desetiletí, nabízí současné Gridy velmi širokou škálu možností a mechanismů, což zároveň nutně vede k tomu, že současná gridová řešení jsou velmi komplexní a

s pozvolnou učící křivkou. Zejména řadoví uživatelé, kteří nemají zkušenost z podobného distribuovaného prostředí, se mohou cítit zaskočeni komplexností Gridů. Gridové prostředí je náročné i z hlediska administrativy, protože obsahuje množství služeb, často se složitou konfigurací, které nemají mimo gridový svět obdobu. Administrátoři proto potřebují hodně času a úsilí k instalaci aspoň základních služeb a zejména k jejich rutinnímu provozu.

Noví uživatelé, kteří se chtějí seznámit s Gridy a začít je používat pro řešení svých problémů, tak často naráží na velkou bariéru. V lepším případě mají dostupné nějaké gridové prostředí (zpravidla postavené pro některý existující gridový projekt), v horším případě začínají na zelené louce a snaží se o vybudování infrastruktury (nebo aspoň její části) vlastními silami. V obou případech je velmi často složitost a množství všech potřebných kroků odrazující a uživatelé se často vracejí ke svým zaběhlým zvyklostem, které jim poskytují zajištěné zázemí, přestože pomocí gridových technologií by bylo často možné řešit jejich problémy efektivněji.

V současnosti se věnuje netriviální úsilí tomu, aby se Gridy staly přístupnější pro širší skupiny uživatelů. Ve zbytku tohoto článku poskytneme popis prostředí *VOCE (Virtual Organization for Central Europe)*, které bylo vybudováno pro maximální usnadnění přístupu nových uživatelů ke gridovým technologiím a plně funkční gridové infrastruktuře. Prostředí je budováno jako součást projektu EGEE[1], jehož hlavním cílem je vytvoření produkční panevropské gridové infrastruktury. VOCE je aktivita Středoevropské federace EGEE, kterou tvoří instituce z České republiky, Maďarska, Polska, Rakouska, Slovenska a Slovinska. Vývoj VOCE je koordinován sdružením CESNET, který v projektu zastupuje Českou republiku.

1 VOCE

Cílem VOCE je poskytovat všem uživatelům ze středoevropského regionu plně produkční gridové prostředí (tzv. *virtuální organizaci*). Vybudovaná infrastruktura VOCE obsahuje všechny potřebné gridové služby a je v maximální možné míře nezávislá na komponentách, které by poskytovala nějaká třetí strana mimo region. Chod jádra infrastruktury je zajišťován sdružením CESNET, výpočetní zdroje a úložiště dat poskytují všichni účastníci. V současnosti je k dispozici přes 500 procesorů a téměř 6 TB úložného prostoru. Přestože jsou tyto kapacity zpravidla sdíleny i s jinými projekty a nejsou dedikovány výhradně pro VOCE, mají tak uživatelé VOCE přístup k velmi výkonnému prostředí.

Zájem VOCE se primárně soustředí na dvě skupiny uživatelů. První skupinou jsou noví uživatelé, kteří nemají žádnou zkušenost s Gridy a chtějí rychle proniknout do základů gridových technologií bez toho, aby sami museli konfigurovat a udržovat vlastní infrastrukturu, domlouvat využití zdrojů s jinými institucemi apod. Další cílovou skupinou jsou uživatelé, kteří již mají nějakou předešlou zkušenost s Gridy a mají také konkrétní aplikace, které by rádi v Gridu vyzkoušeli, ale zároveň nemají kapacity (časové, finanční, lidské) na vybudování vlastní infrastruktury. Těmto uživatelským skupinám VOCE umožňuje, aby mohly rychle vyzkoušet, jak zapojit své stávající aplikace do gridového prostředí. VOCE nabízí všem těmto zájemcům snadnou proceduru pro získání účtu a rychlého připojení do plně funkčního gridového prostředí. Díky tomu, že VOCE provádí outsourcing celého provozu a administrativy gridové infrastruktury, se uživatelé mohou plně soustředit na řešení svých problémů, aniž by byli zatěžováni problémy, které se týkají správy.

Infrastrukturu VOCE lze vedle vyzkoušení Gridů použít i pro plně produkční provoz. Uživatelé, kteří se již seznámili s gridovým prostředím a mají své aplikace připraveny pro běh v Gridu, mohou použít VOCE pro jejich rutinní provoz. VOCE tak umožňuje uživatelům hladký přechod od prvního seznamování se s gridovými nástroji až po produkční použití, vše ve stejném prostředí bez nutnosti dalšího přeškolování. V případě, že prostředí VOCE přestane některé skupině stačit a bude vyžadovat více zdrojů, příp. větší garanci jejich dostupnosti, předpokládáme, že si vybuduje vlastní infrastrukturu. Infrastruktura VOCE je založena na nejrozšířenějším gri-

[1] `http://www.eu-egee.org/`

dovém middleware dneška, je proto velmi pravděpodobné, že nově ustavené prostředí bude poskytovat totožnou funkcionalitu jako VOCE a pro uživatele bude velmi snadné začít pracovat v nové infrastruktuře na základě znalostí získaných ve VOCE.

Přestože VOCE poskytuje platformu, kde si uživatelé mohou vyzkoušet možnosti Gridů, liší se od jiných testovacích infrastruktur v tom, že zajišťuje alespoň minimální úroveň bezpečnosti. Současná prostředí, která se používají pro demonstraci a testování Gridů, umožňují v podstatě anonymní přístup, kdy v zájmu jednoduchosti povolují přístup uživatelům, jejichž identita není důvěryhodně ověřitelná (zpravidla se přístup povoluje na základě e-mailové komunikace). Tento stav samozřejmě vede k tomu, že počet dostupných zdrojů a jejich rozšiřitelnost je omezená. Vlastníci prostředků totiž nemají zájem vkládat své zdroje do infrastruktury, která nezajistí, že případně problémový uživatel je jednoduše dohledatelný. VOCE naproti tomu striktně vyžaduje, aby registrovaní uživatelé měli certifikát vydaný některou akreditovanou gridovou certifikační autoritou. Přísné požadavky na akreditaci certifikačních autorit zajišťují, že uživatelé jsou spolehlivě identifikovatelní v průběhu jejich pohybu po Gridu.

Na rozdíl od většiny současných virtuálních organizací, není VOCE spjato s žádnou konkrétní aplikační skupinou. Naopak VOCE se snaží přitáhnout různé aplikace a podporovat široké portfolio aplikačních uživatelů. Vývojáři VOCE jsou schopni podat pomocnou ruku v přenosu aplikací do prostředí Gridu nebo také pomoci zprostředkovat kontakty na jiné podobně zaměřené aplikační skupiny v gridovém světě.

V současné době má VOCE propracovaný systém podpory, který slouží pro efektivní řešení uživatelských problémů. VOCE disponuje experty z různých oblastí gridových technologií a je schopno poskytovat svým uživatelům plnou podporu.

2 VOCE z pohledu uživatele

VOCE je otevřeno všem uživatelům z akademického prostředí ČR. Pravidla pro registraci jsou uvedena na portálu VOCE[2], v této kapitole uvádíme jejich shrnutí a popis vlastností, které VOCE nabízí svým uživatelům.

Základním předpokladem pro získání členství ve VOCE je vlastnictví certifikátu veřejného klíče, který vydala certifikační autorita sdružení CESNET. Tato autorita je uznávaná v celosvětovém gridovém prostředí a držitelé jejích certifikátů mají tedy usnadněný přístup ke spolupráci se zahraničními partnery. Více informací o certifikátech lze nalézt např. v [1].

Pro získání certifikátu je nutná osobní návštěva pracoviště Registrační autority CESNET CA, která ověří patřičné doklady. Pro pracovníky a studenty MU je k dispozici pobočka na Superpočítačovém centru ÚVT[3].

Zájemci o zapojení do VOCE musí vyplnit registrační formulář na webu, kde uvedou základní kontaktní informace. Pro přístup k formuláři se vyžaduje autentizace pomocí uživatelského certifikátu. Po vyplnění elektronické přihlášky je nejvýše do tří kalendářních dnů zřízen účet uživatele ve VOCE a lze začít s použitím Gridů. VOCE je od počátku spjato s projektem *META Centrum*[4], který nabízí infrastrukturu pro náročné výpočty v České republice. Českým uživatelům proto doporučujeme požádat o členství v *META Centru* a v rámci této žádosti uvést také zájem o zapojení do VOCE. Uživatelům se tak otevře bohatší prostor pro realizaci výpočtů a získají přístup k více zdrojům. Přihlášení do *META centra* však není nutné pro členství ve VOCE.

Pro přístup ke gridovému prostředí VOCE je vyhrazen zvláštní počítač (tzv. *User Interface – UI*), kde je nainstalován veškerý software potřebný k použití gridových prostředků. Zřízení účtu na tomto stroji je také součástí registrační procedury VOCE. Od okamžiku, kdy je uživateli aktivován účet ve VOCE, je možné přihlásit se na tento stroj (skurut4.cesnet.cz) pomocí protokolu ssh a otevřít tak bránu do gridového světa. Z UI se zadávají úlohy, které jsou následně spouštěny na některém z volných strojů v Gridu bez ohledu

[2] `http://egee.cesnet.cz/cs/voce/`
[3] Případnou návštěvu doporučujeme domluvit předem.
[4] `http://meta.cesnet.cz/`

na to, zda stroj je v Praze, Krakově nebo Košicích. Stejně tak lze průběh úlohy monitorovat a sledovat, jak prochází jednotlivými gridovými komponentami až do okamžiku, kdy skončí a uživatel si stáhne výsledek úlohy. UI dále obsahuje příkazy pro přístup k datovým úložištím, které umožňují snadno využít velkou diskovou kapacitu, která jsou ve VOCE dostupná.

Základní operace pro využití gridové infrastruktury jsou popsány v dokumentaci dostupné na portálu VOCE. Příprava a spuštění jednoduchých úloh je tak otázkou krátkého času. Podobně přístup k nabízeným úložištím je jednoduchý a základní operace lze zvládnout poměrně rychle. I uživatel, který neměl žádné znalosti gridových technologií, si může osvojit základní gridové operace během velmi krátké doby.

Pro přístup ke zdrojům VOCE lze také použít specializované webové portály, které skrývají technické detaily a nabízí snadnější přístup k infrastruktuře. Pro VOCE jsou dostupné portály GILDA a P-GRADE. První byl vytvořen primárně pro účely demonstrací a byl vyvíjen s důrazem na použití ve výuce. Druhý nabízí sofistikovanější prostředky, zejména řízení workflow, tj. vztahů mezi více úlohami, které tvoří jeden celek.

Po zvládnutí základů použití Gridů se mohou uživatelé pustit do přenášení svého aplikačního portfolia. Mohou buď využít zmíněné portály nebo hledat vlastní řešení pomocí nativních gridových příkazů. Pro VOCE je také k dispozici unikátní systém Charon[5], který vznikl na Národním centru pro výzkum biomolekul na Přírodovědecké fakultě MU. Nejdříve byl vytvořen pro účely *META Centra*, později byl upraven i pro VOCE. Charon tvoří vrstvu na pomezí mezi webovými portály a čistými prostředky gridového middleware. Skrývá řadu detailů nižších úrovní, takže uživatel se nemusí učit často komplexní syntax příkazů ani pronikat do detailů spletité gridové architektury. Poskytuje jednoduché řádkově orientované rozhraní, které je dostatečně silné na práci s širokou škálou úloh. Výhodou v našem prostředí je to, že Charon lze používat jak v *META Centru* tak ve VOCE, takže uživatelé mohou používat úplně stejné příkazy pro práci v těchto, jinak velmi odlišných, infrastrukturách.

[5] `http://egee.cesnet.cz/cs/voce/Charon.html`

I když na první pohled složité, gridové prostředí dneška je poměrně vstřícné a nabízí velké množství nástrojů pro řešení úloh, které jsou náročné na čas, síťovou kapacitu, úložné prostory nebo schopnosti administrátorů. VOCE bylo vytvořeno pro podporu řešení těchto problémů a je otevřeno všem uživatelům, kteří potřebují bohaté prostředí, které Gridy nabízí.

Literatura

[1] D. Kouřil. „Bezpečnost v distribuovaném prostředí.“ *Zpravodaj ÚVT MU*. 2005, roč. 15, č. 4, s. 2–6. □

Videokonference s vysokou kvalitou

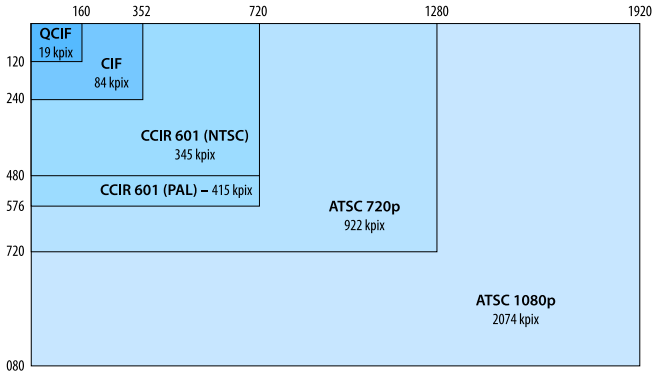
Eva Hladká, Petr Holub, FI a ÚVT MU

Videokonference se staly jednou z běžně využívaných technologií pro komunikaci jedinců i týmů. V řadě kanceláří se kromě telefonu a počítače nachází též videokonferenční zařízení nebo doplňky umožňující jako videokonferenční zařízení využívat počítač. Navzdory této skutečnosti, a nebo spíše právě kvůli ní, se i v oblasti videokonferencí bádá, vyvíjí a testuje. Zkoušejí se nové přístupy a vyšší kvalita obrazu a zvuku. Tento vývoj je na jedné straně urychlován rozvojem síťové infrastruktury a dostupností šířky použitelného pásma, na druhé straně jej vyžadují uživatelé, pro které je ergonomie a co největší přiblížení k realitě u videokonferencí velmi důležité. Přes veškerý pokrok je totiž videokonferenční komunikace pro zúčastněné namáhavější než běžná schůzka. Proto se v tomto příspěvku zaměříme na videokonference s vysokou kvalitou videa a zvuku. Je to vývojový trend, který se na MU za podpory VZ *Optická síť národního výzkumu a její nové aplikace* úspěšně rozvíjí.

1 Video

Na tomto místě si čtenáři dovolíme připomenout několik základních parametrů, které ovlivňují výslednou kvalitu videokonference. Jedná se o kvalitu videa, šířku datového toku a zpoždění.

Kvalita videa: Použijeme-li pro videokonferenci zde již mnohokrát popsané Mbone Tools, potom malý obrázek v základním menu (QCIF) má 180×144 bodů, zvětšený obrázek (CIF) má 360×288 bodů. Pro srovnání – televizní přenos v normě PAL má 720×576 bodů[1]. Mluvíme-li o videu s vysokým rozlišením, míníme tím v rámci tohoto článku některý z rodiny formátů dle standardu HDTV, kde snímek má rozlišení buď 1280×720 nebo 1920×1080 bodů. Pro větší názornost jsou jednotlivé formáty srovnány na obrázku 1.



Obrázek 1: Porovnání velikosti video obrazu pro různé formáty.

Celkovou kvalitu videa samozřejmě neovlivňuje pouze jeho velikost, ale i další faktory, jako barevná hloubka obrazu či použití ztrátové komprese. Zatímco běžné počítačové grafické karty pracují při přehrávání videa s 8 bity na barevný kanál, profesionální nasazení používá nejméně 10 bitů, což při třech barevných rovinách rozšiřuje barevnou škálu 64×. Ztrátová komprese zejména při použití vysokého kompresního poměru často vede na různé artefakty v obraze: v lepším případě je to jen ztráta ostrosti detailů, v horším pak na posterizace obrazu (rozpad obrazu do čtvercových bloků).

Šířka datového toku: V předchozím odstavci byla uvedena rozlišení základních videoformátů. Abychom měli představu o tom, kolik dat je třeba přenášet, chybí další parametr, a tím je počet obrázků za časovou jednotku, typicky sekundu – odtud anglická zkratka fps, neboli frames per second. Tento parametr ovlivňuje plynulost pohybu v přenášeném videu. U statické snímané scény je možné počet snímků omezovat často až k 1 fps, pro plynulost pohybu u běžně komunikujících osob postačí 5–15 fps, ale pro skutečně plynulý pohyb dynamické scény je třeba přenášet 30 fps nebo i více. Výsledný datový tok pro HD formát v rozlišení 1920×1080 dle HDTV normy se 60 prokládanými snímky za sekundu a 10 bity na barevný kanál je celkem 1,5 Gb/s[2]. Na první pohled se může zdát, že přenos takového množství dat je nereálný. Současné experimentálně-provozní sítě však mohou přenášet až desítky Gigabitů. Navíc, není-li striktně požadována maximální kvalita obrazu, minimální zpoždění a nezávislost jednotlivých snímků, lze videodata efektivně komprimovat. Z jednoho nekomprimovaného streamu lze získat například 25 Mb/s stream komprimovaný ve formátu HDV.

Zpoždění: Základní vlastností přirozené komunikace je zdánlivě okamžitá odezva. U videokonferencí je potřeba počítat se zpožděním (latencí), které vzniká zpracováním videosignálu u vysílající stanice, dobou potřebnou pro přenos dat sítí ke koncové stanici a zpracováním a zobrazením dat na koncové stanici. , viz obr. 2.

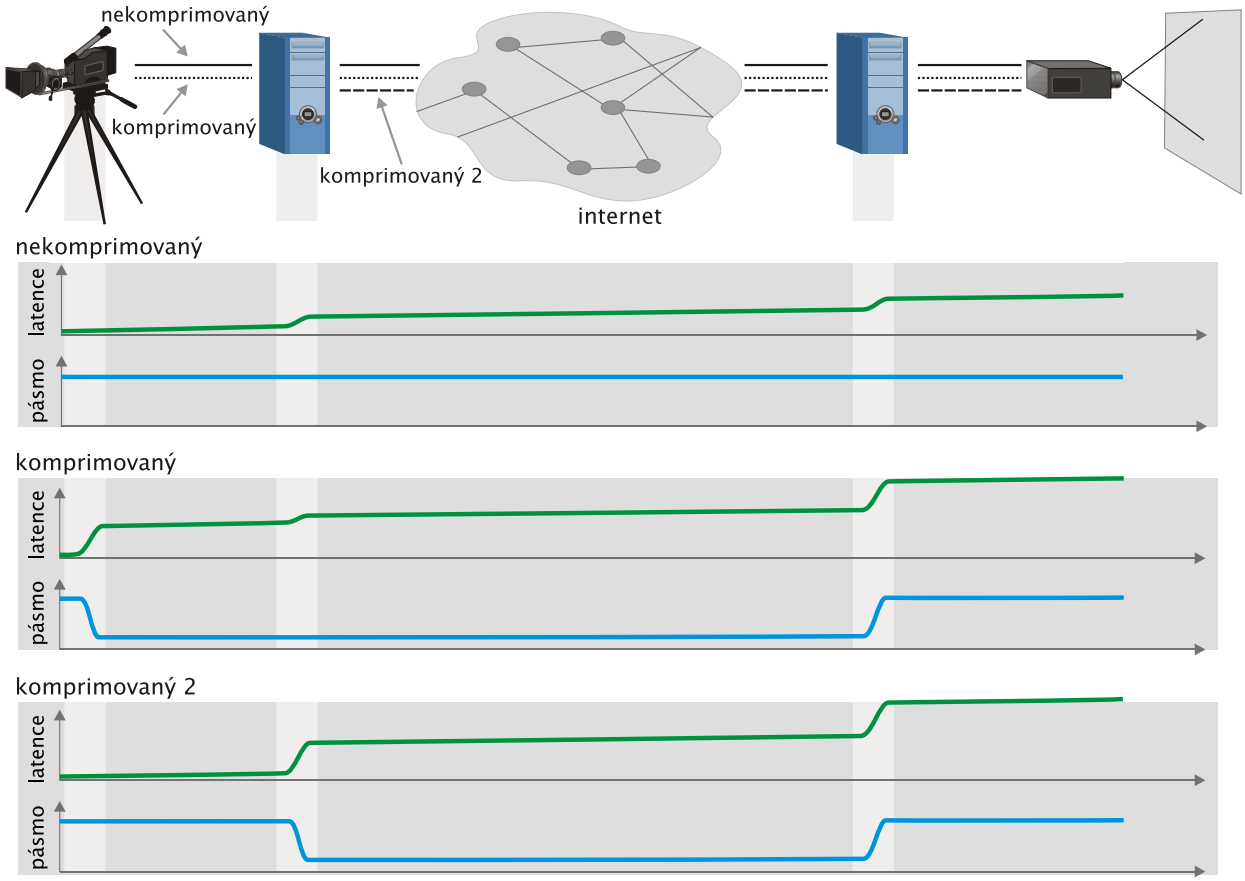
Počítáme-li s objemem dat 1,5 Gb/s, potom zpracování a přenos daného objemu bude vyžadovat netriviální kapacity a čas. Čím ovšem bude delší zpoždění, tím méně přirozená a tedy kvalitní bude komunikace. Lidské smysly (a ty jsou zde podstatné, protože koncovým uživatelem je člověk, nikoliv stroj) mají různou schopnost zaznamenat zpoždění. Při komunikaci je zapojen zrak i sluch a tím citlivějším a tedy směrodatným je sluch. Schopnost zvukové synchronizace

[1] Technicky vzato je rozlišení 720×576 platné pouze pro zařízení s obdélníkovými body jako jsou například televize. V případě zařízení se čtvercovými body, např. počítačové obrazovky, je rozlišení 768×576 bodů.

[2] Pokud by laskavému čtenáři nevycházel výpočet potřebného datového toku z výše uvedených hodnot, pak je na správné stopě. V rámci výkladu jsme se dopustili dvou zjednodušení – skutečné HDTV rozlišení včetně tzv. mazacích řádků je 2200×1125. Dále se pro snížení datového toku využívá menší citlivosti lidského oka na barvy než na jas, a proto je barevný prostor YCrCb vzorkován 4:2:2, což sníží datový tok na 2/3. Správný výpočet je tedy

$$2200 \times 1125 \times 30 \times 30 \times 2/3 = 1,485\,\text{Gb/s}.$$

Tento formát se také označuje jako HD-SDI specifikovaný v normě SMPTE 292M [1].



Obrázek 2: Nárůst latence u videopřenosu. Vodorovná osa na obrázku odpovídá poloze videa v řetězci zpracování, jak je uveden v horní části obrázku. Rozdíl mezi komprimovaným videem a komprimovaným videem 2 spočívá v tom, že v prvním případě probíhá komprese přímo v kameře, kdežto ve druhém případě jde video z kamery nekomprimované a ke kompresi dochází teprve v počítači.

se dá u člověka vytrénovat, ne nadarmo dosahují v tomto ohledu vynikajících časů například hudebníci hrající v komorních orchestrech, kde se přesnost synchronizace udává až kolem 5 ms. Běžně se doporučuje pro kvalitní komunikaci nepřekročit hranici 100 ms a proto je nutno minimalizovat časy nutné na zpracování obrazu na obou koncích. Za předpokladu, že používané sítě mají dostatečnou propustnost, je možné ušetřit čas odstraněním komprese. Zvláště pro přenosy na vzdálenosti v řádu deseti a více tisíc kilometrů[3], kde i rychlost přenosu dat není zanedbatelnou položkou v celkovém zpoždění.

2 Zvuk

Zatím jsme explicitně nezmínili zvuk, i když jeho kvalita je pro úspěšnost a ergonomii videokonference podstatná. U videokonferencí s vysokou kvalitou obrazu je rozhodující právě rozlišení videa, kvalita zvuku však nesmí komunikaci negativně ovlivnit.

[3]Při rychlosti světla 300 000 km/s urazí světlo vzdálenost 10 000 km za 33 ms. Je však nutno vzít v potaz, že světlo se v optickém kabelu nešíří stejně rychle jako ve vakuu, ale 1,5-násobně pomaleji, a tudíž stejnou trasu urazí za zhruba 50 ms.

K HDTV obrazu muže být připojeno prakticky libovolné audio, takže lze využít například nejvyšší kvality dle standardu High-Definition Multimedia Interface (HDMI) [2], tj. nízkolatenční nekomprimovaný zvuk s 24 bitovým kvantováním, vzorkováním 192 kHz a s 8 (7.1) kanály, což dává 36,8 Mb/s. I v této značně maximalistické kvalitě však představuje zvuk pouze malý zlomek přenášených dat v porovnání s nekomprimovaným HDTV videem.

Vezmeme-li v potaz skutečnost, že lidský sluch je na zpoždění mnohem vnímavější než zrak, nabízí se na první pohled lákavá možnost posílat zvuk nekomprimovaný s co nejnižší latencí, zatímco obraz by se extenzivně komprimoval pro zmenšení nároků na přenosovou kapacitu. Zde však narazíme na další záludnost lidského vnímání: podobně jako je lidský sluch citlivý na celkové zpoždění, je zrak citlivý na synchronizaci mezi zvukem a obrazem – v angličtině se běžně užívá termínu "lip synchronization", tedy synchronizace na rty. Hranice citlivosti na desynchronizace obrazu a zvuku se pohybuje opět přibližně kolem 100 ms a nekomprimované video se z tohoto pohledu opět ukazuje jako vhodný formát.

3 Komunikační schéma

Zatím jsme nezmínili mezi kolika účastníky může HD videokonference probíhat, tedy jaké komunikační schema lze použít. Základním omezujícím faktem je, že koncové místo vysílá 1,5 Gb/s a nejméně stejný objem dat přijímá. Maximální počet účastníků tedy omezuje kapacita koncové linky. Dalším problémem je replikace. Pokud bude počet účastníků větší než dva, je třeba vysílaná data replikovat tak, aby je dostala všechna přijímající místa. Řešení známá z videokonferencí v běžné kvalitě zde selhávají. Skupinová komunikace v podobě multicastu není adaptována na potřebné objemy dat zejména v prostředí heterogenních sítí stejně tak jako MCU jednotky známé z H.323 videkonferencí.

Problém komunikace mezi více účastníky lze řešit za použití speciálně upravených vysoce výkonných reflektorů multimediálních datových toků [3] nebo přímé multiplikace signálu na optické vrstvě pomocí splitterů. Výhoda optických spliterů je v tom, že nepřidávají zpoždění a jsou takřka nezávislé na přenosové rychlosti (a dokonce mohou být širokospektrální a dělit více vlnových délek najednou), problémem je však jejich malá flexibilita a zatím pouze experimentální dostupnost.

4 Závěrem

Zejména výše uvedené problémy s vícebodovou distribucí zatím využití rozsáhlejších videokonferencí na bázi nekomprimovaného videa značně omezují. Prvními vlaštovkami v tomto směru mohou být demonstrace na workshopu iGrid 2005 popsané v samostatném článku v tomto čísle Zpravodaje, kde dva týmy nezávisle na sobě tyto technologie demonstrovaly.

HD videokonference a jejich další zlepšení posunují oblast prostředí pro virtuální spolupráci ke stále reálnějšímu a přirozenějšímu vjemu účastníků. V brzké době umožní přenosy z míst, kde je kvalita detailu obrazu velmi důležitá, např. z operačních sálů do poslucháren. Pro nás představují mnoho výzev a ukazují mnoho problémů, které je třeba řešit. Na rutinní využití těchto technologií si ještě budeme muset nějaký čas počkat, ale do budoucna je třeba s nimi vážně počítat.

Literatura

[1] Society of Motion Picture and Television Engineers. *Bit-Serial Digital Interface for High-Definition Television Systems.* SMPTE 292M-1998.

[2] *High-Definition Multimedia Interface* (HDMI). `http://www.hdmi.org/`

[3] E. Hladká, P. Holub. „Zrcadla v počítačové síti." *Zpravodaj ÚVT MU.* ISSN 1212-0901, 2002, roč. 12, č. 5, s. 7–10. □

iGrid 2005

Petr Holub, Eva Hladká, Luděk Matyska, ÚVT a FI MU

Jen velmi málo aplikací je schopno využít potenciál, který nabízí optické sítě svou vysokou pře-

nosovou rychlostí a velmi nízkou latencí. Zpravidla je jejich kapacita využita pouze pro přenos agregovaných proudů dat bez specifických požadavků na rychlost nebo kapacitu sítě. Ukázat skutečné možnosti vysokorychlostních optických sítí bylo cílem workshopu iGrid2005, který se konal v září 2005 v San Diegu v Kalifornii (USA) a kterého jsme se i my aktivně účastnili.

Setkání iGrid2005 spolupořádaly tři organizace: Electronic Visualization Laboratory (EVL) z Univerzity Illinois v Chicagu, Cal-(IT)^2 z University of Califonia San Diego a GLIF, Global Lambda Integrated Facility. Druhá z jmenovaných organizací byla současně hostitelem celé akce. Všechny tři pořádající instituce patří mezi nejvýznamnější „hráče“ v oblasti optických sítí: EVL operuje StarLight, mezinárodní spojovací bod optických sítí, a je současně vedoucím pracovištěm v oblasti vizualizace velkých objemů dat, pro něž je nezbytná i odpovídající vysokokapacitní síťová infrastruktura. Cal-(IT)^2 je vedoucí organizací projektu OptiPuter, studujícího zcela nové způsoby uživateli řízeného přepínání optických tras. GLIF je pak sdružení hlavních vlastníků a operátorů akademických optických tras, které má přirozený zájem na hledání a podpoře nových aplikací vysokorychlostních sítí.

Workshopy iGrid mají již určitou tradici – první byl pořádán jako součást konference SuperComputing'98 v Orlandu na Floridě, další pak v roce 2000 v Yokohamě v Japonsku a v roce 2002 v Amsterodamu v Holandsku. Série worshopu iGrid současně dokumentuje prorůstání Gridů – původně chápaných velmi úzce jako distribuované výpočetní systémy – a vysokorychlostních sítí. Stále více se dnes hovoří o integrovaném heterogenním prostředí, které je tvořeno sítěmi a jimi propojenými nejrůznějšími zdroji (výpočetního výkonu, dat, znalostí, ale i přístroji a lidmi), a které má charakter prostředí podporujícího spolupráci geograficky vzdálených týmů nad společnými problémy.

Workshop iGrid2005 [1] tvořilo 45 demonstrací, několik zvaných přednášek a několik panelů. Spolupráce se projevila i zde – prakticky všechny demonstrace byly představovány týmy zastupujícími několik institucí. Nejvíce demonstrací bylo samozřejmě koordinováno partnery z USA, celkem se jednalo o 28 takto koordinovaných demonstrací. Po třech demonstracích koordinovaly týmy z Kanady, Japonska, Polska, dvě demonstrace pak tým z Holandska a jednu „vlastní“ demonstraci pak měly týmy z České republiky, Číny, Koreje, Spojeného království a z Taiwanu. Českou republiku zastupoval tým tvořený pracovníky a doktorskými studenty Masarykovy univerzity (z Fakulty informatiky a Ústavu výpočetní techniky) a sdružení CESNET (jeden ze zakládajících členů GLIFu). Ve skutečnosti se tento tým podílel na celkem třech demonstracích – kromě výše zmíněné „vlastní“ demonstrace to byly akce vedené polským a americkým týmem.

1 „Naše“ demonstrace

Jak bylo řečeno v úvodu, hlavním cílem workshopu byla demonstrace co nejpokročilejších aplikací optických sítí. Převážná většina demonstrací se věnovala přenosu obrazových dat, které potřebují vysokou přenosovou kapacitu a při interaktivní práci i velmi nízkou latenci. Do této kategorie patřila i demonstrace *CZ101* s názvem *HD Multipoint Conference*, jejímž prostřednictvím jsme představili výsledky společné práce MU, CESNETu a spolupracující Louisiana State University (LSU) v Baton Rouge. High-definition (HD) video poskytuje při rozlišení 1920×1080 bodů velmi kvalitní obraz, schopný zachytit i velmi malé detaily. Použití HD videa pro videokonference však naráží na problém jeho zpracování: pokud použijeme příliš vysokou kompresi, musíme se smířit se ztrátami v kvalitě obrazu a tím de facto přijdeme o přednosti vysokého rozlišení. Velmi kvalitního obrazu je možno dosáhnout při použití HDV komprese, která vyžaduje přenosové pásmo 25 Mbps. Zásadní nevýhodou HDV komprese je však velmi vysoká latence při vlastním kódování videa, která může dosáhnout více jak 1,5 sekundy. To je samozřejmě zcela nepoužitelné pro skutečnou videokonferenci, pro kterou potřebujeme dosáhnout zpoždění nejlépe v řádu 100 ms. Variantou je použití nekomprimovaného videa dle standardu HD-SDI, kde je ovšem šířka datového toku zhruba 1,5 Gbps. Dvoubodová videokonference, kdy je třeba každým směrem přenášet těchto

1,5 Gbps, byla poprvé realizována na podzim 2001 mezi Tokiem a prefekturou Chiba v Japonsku a přibližně o měsíc později jiným nezávislým týmem mezi Seattlem a Denverem v USA. Rozšíření na tři a více konferujících míst bránil jednak nedostatek přenosové kapacity, jednak chybějící nástroje na co nejrychlejší duplikaci datových proudů při této přenosové rychlosti.

Aktivní prvky, které používáme pro vícebodový přenos dat při běžných videokonferencích [6] jsme adaptovali tak, aby byly schopné s minimální latencí duplikovat datové proudy do přenosové rychlosti 2 Gbps. Pro tento účel používáme servery vybavené dvěma procesory AMD64 Opteron, ve kterých je 10 GE karta firmy Chelsio. Jeden server je schopen beze ztrát duplikovat jeden proud, tj. z jednoho vstupního proudu vytvoří dva výstupní. Tyto aktivní prvky tvořily základ distribuční sítě vlastní demonstrace.

Snímání dat a generování datového proudu o kapacitě 1,5 Gbps, stejně jako jeho zpracování na druhém konci přenosového kanálu rovněž vyžadovalo velmi výkonné výpočetní systémy. Pro snímání HD videa jsme použili kameru Sony HVR-Z1E, která byla přímo připojena k převodníku AJA HD10A, který převáděl analogový signál kamery na HD-SDI proud. Ten byl dále zpracován kartou DVS Centaurus, zabalen do UDP/IP paketů a poslán přes 10 GE Chelsio kartu do vysokorychlostní sítě. Obsluhující počítač byl opět server se dvěma procesory AMD64 Opteron, konkrétně jsme použili typ 250 s frekvencí 2,4 GHz. Na druhé straně přenosové trasy byl analogický počítač, avšak bez DVS karty a místo toho vybavený grafickou kartou schopnou zobrazit HD rozlišení. Při laboratorním uspořádání jsme naměřili zpoždění 175 ms – je to čas od okamžiku zachycení přes zpracování a přenos až po zobrazení na HD LCD obrazovce. Podrobnější technické informace je možno nalézt na webové stránce `https://sitola.fi.muni.cz/igrid/` a stručný popis pak v článku *Videokonference s vysokou kvalitou* v tomto čísle Zpravodaje.

Samotná demonstrace pak propojila tři místa: Brno (ČR), LSU (Luisiana) a San Diego (Kalifornie). Všechna data procházela StarLightem v Chicagu, kde jsme měli k dispozici tři aktivní reflektory (duplikátory) popsané výše. Všechna místa byla propojena optickými trasami s kapacitou 10 Gbps. Optické trasy poskytl GLIF, konkrétně CzechLight (Brno–Praha–Amsterodam), NetherLight (Amsterodam–Chicago), CAVEWave (Chicago–San Diego) a National Lambda Rail (Chicago–Baton Rouge). Každé místo bylo vybaveno vlastní HD kamerou, signál byl z každého místa přenášen do Chicaga, kde byl zdvojen a poslán na zbývající dvě místa. Takto jsme vytvořili plnohodnotné videokonferenční prostředí.

Pro vlastní demonstraci byly k dispozici třikrát 2 hodiny, vždy ráno kalifornského času. Čas jsme vyplnili přednáškami, a to jak na místě tak i z obou připojených míst – z MU přednášel například prof. Gruska a prof. Slovák. HD kamera byla schopná beze ztráty detailu sejmout celé plátno se slidy a přenést je na vzdálená místa v plné kvalitě. Fotografie zobrazování HD videa na zapůjčených 63” plazmových obrazovkách v San Diegu je na obr. 1.

Ne všechno však proběhlo podle plánu. Zaměřili jsme se primárně na zpracování a přenos videodat a podcenili jsme kvalitu přenášeného zvuku. Výsledkem byl vynikající obraz a spíše nekvalitní zvuk – použili jsme pouze zapůjčené vybavení, které jsme ani předem nijak nespecifikovali. Daleko větší problém ale způsobily dva hurikány, které přešly přes Lousianu a Texas (jeden z nich byl hurikán Katrin, který zničil New Orleans). Jedna karta DVS Centaurus, kterou jsme nechali poslat českým dodavatelem na LSU byla zadržena při celním odbavování: původně měla jít přes New Orleans, po jeho zatopení byla přesunuta do Houstonu, ten však byl ohrožen druhým hurikánem a i jeho celnice byla zavřena. Bez této karty však nebylo možné generovat HD nekomprimovaný proud z LSU. Realizovali jsme proto náhradní řešení, kdy LSU posílala pouze HDV komprimovaný proud. Díky tomuto řešení jsme mohli přímo na místě demonstrovat zpoždění, způsobené zpracováním (kompresí a dekompresí) HDV proudů. To dosahovalo hodnoty 2 sekund a bylo v ostrém kontrastu s méně jak půl sekundovou latencí z ČR (přestože se jednalo o mnohem větší vzdálenost). Pozorovaná téměř 500 ms latence přenosu nekomprimovaného HD videa mezi Brnem a San Diegem se

Obrázek 1: Ukázka u demonstrace CZ101 – HD Multipoint Conference.

skládala ze 175 ms latence zpracování videosignálu a 102 ms latence přenosové trasy. Zbývajících více jak 200 ms pak měla na svědomí vlastní duplikace dat v StarLightu.

Druhá demonstrace, na které jsme se podíleli, nesla název *Interactive Remote Visualization across the LONI and the National LambdaRail* a byla organizována našimi partnery na LSU. Cílem zde bylo předvést interaktivní vizualizaci, která je zobrazována na více místech současně, a všichni, kteří ji sledují, s ní také mohou interagovat (např. měnit úhel pohledu, přiblížení, ale i některé parametry modelu, který představuje). Propojena byla opět stejná tři místa jako v předchozím případě, každé však mělo navíc k dispozici dvě speciální zařízení pro interakci, nazývané *tangible*. Každé z těchto zařízení bylo napojeno na jeden parametr vizualizace a pohybem se zařízením bylo možno tento parametr měnit. Tato demonstrace měla dva cíle. Jedním bylo využití výpočetních prostředků státu Louisiana propojených optickou sítí (Louisiana Optical Network Initiative, LONI[1]) a vytvoření superpočítače vybaveného velkou pamětí. Druhým cílem byl pak přenos vizualizace jako HD video proudu, tj. nikoliv speciálním protokolem. Podařilo se vytvořit počítač s více jak 320 GB paměti, jehož jednotlivé uzly zpracovávaly a posílaly data rychleji, než by bylo možné dosáhnout použitím i jediného superpočítače s lokálními disky. Přenosová infrastruktura byla identická předchozímu případu. Nedodaná karta DVS Centaurus způsobila, že místo přímo generovaného HD video proudu musela být vizualizace zobrazena lokálně na LCD panelu v Luisianě, tam sejmuta HD kamerou a přenášena dále jako HDV komprimovaný proud. Přes toto omezení se podařilo demonstrovat použitelnost celého přístupu. V plné podobě se pak společně podařilo tento systém demonstrovat o dva měsíce později na konferenci SuperComputing'05 v Seattlu (stát Washington), kam se podařilo přivést dva plné HD video proudy (vizualizace z LSU a živý obraz z MU v Brně) a jeden živý HDV proud z LSU.

[1] `http://www.cct.lsu.edu/projects/loni/index.php`

Cílem poslední demonstrace, které jsme se zúčastnili – *Large-Scale Simulation and Visualization on the Grid with the GridLab Toolkit and Applications* – bylo předvedení výsledků spolupráce v rámci EU projektu GridLab [7].

2 Kontext ostatních demonstrací

Během workshopu iGrid proběhla celá řada dalších videokonferenčních demonstrací, ovšem pouze demonstrace ResearchChannel byla rovněž věnována vícebodovému HD video přenosu, v ostatních případech šlo pouze o dvoubodové spojení. Za zmínku stojí demonstrace japonské skupiny *Digital Media and Content* z Keio University. Ta používala pro přenos komprimovaného videa v rozlišení 4K (4096×3112) hardwarový kodek JPEG2000. V této kvalitě byly přenášeny jak počítačové animace tak i živé 4K video z experimentální digitální kamery firmy Olympus. V San Diegu byl pro zobrazení použit prototyp 4K projektoru SONY. Jedna z prezentací byla věnována Gutenbergově bibli, kde byly možnosti 4K projekce demonstrovány na detailech iluminací.

Pravděpodobně nejsilnější skupinu demonstrací představovaly vizualizace. Velmi zajímavé byly demonstrace využívající 100 Megapixelovou zobrazovací plochu, tvořenou celkem 55 běžnými LCD panely (5×11). Tato plocha má využití např. při detailním studiu satelitních snímků a obrazů z geografických informačních systémů. Plné video na této ploše zatím není možné – bez komprese by vyžadovalo datový tok cca 1 Tbps – i zobrazení „pouze“ statických obrazů v plném rozlišení s možností pohybu v obraze a interaktivního zoomu generuje datové toky řádu gigabitů za sekundu. K vidění byly i různé druhy stereoskopických a holografických projekcí, či snímání trojrozměrných objektů pomocí CT skenování v reálném čase.

Související skupinou demonstrací byla vzdálená manipulace s unikátními přístroji (mikroskopy, observatořemi, rentgeny atd.). V rámci projektu NEPTUNE, který se zabývá výzkumem mikroorganismů žijících ve velkých hloubkách na vulkanicky a geotermálně aktivních oblastech oceánského dna, byly předvedeny HD přenosy videa a současná interakce s přístroji umístěnými na mořském dně.

Speciální skupina demonstrací byla věnována přímé manipulaci lambda služeb (pro úvod do této problematiky viz. např. [2, 3]). Cílem bylo ukázat nástroje pro sestavení a dynamickou (re)konfiguraci dle požadavků aplikací a uživatelů. Jedna z demonstrací například využívala protokolu GMPLS [4, 5] pro dynamickou konfiguraci lambda sítě za účelem sběru velkého množství astronomických dat z radioteleskopů rozmístěných v USA, Japonsku, Švédsku, Spojeném království a v Holandsku. Snímaných dat se následně využívá k přesné analýze pohybu Země ve vesmíru.

3 Shrnutí

Během workshopu iGrid2005 bylo na relativně velmi malém prostoru shromážděno velké množství unikátní techniky. Workshop byl proto záměrně zakončen speciální sekcí *Lessons Learned*, kde se otevřeně diskutovaly úspěchy, ale i problémy, které se během realizace všech demonstrací vyskytly. Značné množství problémů bylo způsobeno chybějící technikou – hurikány a americkou celnicí jsme zdaleka nebyli postiženi pouze my. Organizátoři akce se snažili v maximální možné míře pomoci a zapůjčili neuvěřitelné množství techniky, aby tyto problémy pomohli překonat. Workshop rovněž prokázal, jak nezbytný je další výzkum v oblasti konfigurace a správy lambda služeb – během workshopu byly všechny okruhy sestavovány a rušeny ručně, což představovalo prakticky kontinuální práci týmu více jak 5 lidí po celou dobu. Navíc v případě problémů manuální zásah v Evropě či Asii zpravidla znamenal probuzení lokálně odpovědné osoby.

Workshop iGrid2005 ukázal, kudy se ubírají špičkové aplikace využívající v maximální možné míře možností optických sítí a gridových systémů nad nimi budovaných. Není překvapením, že převážná většina aplikací pracuje s obrazovou informací ve velmi vysokém rozlišení a využívá jak vysoké kapacity optických sítí tak i velmi nízké latence k podpoře virtuálních pracovních skupin, jejichž členové jsou distribuováni ve více lokalitách po světě. Z jistého úhlu pohledu můžeme demonstrace na iGridu vidět jako části

(jednotlivé stavební kameny) velmi pokročilého prostředí pro spolupráci. Zde se otevírá možnost pro další zapojení týmů z ČR, jejích univerzit a akademických ústavů – špičková věda spočívající ve spolupráci několika vědeckých týmů nutně generuje nové nároky na optické sítě a Gridy. Taková vědecká pracoviště nepochybně v ČR jsou, chybí „jen“ jejich lepší propojení se síťovou a gridovou komunitou. Pokud se toto podaří, bude zastoupení České republiky na příštím iGridu mnohem rozmanitější.

Literatura

[1] *iGrid 2005*, http://www.igrid2005.org

[2] P. Holub. „Lambda služby.“ *Zpravodaj ÚVT MU.* ISSN 1212-0901, 2004, roč. 15, č. 2, s. 8–13.

[3] P. Holub, J. Radil. „Akademické lambda sítě u nás a ve světě.“ *Zpravodaj ÚVT MU.* ISSN 1212-0901, 2005, roč. 15, č. 3, s. 6–12.

[4] *GMPLS*, http://www.polarisnetworks.com/gmpls/, http://www.polarisnetworks.com/gmpls/gmpls_drafts.html

[5] A. Banerjee, J. Drake, J. P. Lang, B. Turner, K. Kompella, Y. Rekhter, „Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements“, *IEEE Comm. Mag.*, January 2001, http://www.calient.net/files/GMPLS.pdf

[6] E. Hladká, P. Holub. „Zrcadla v počítačové síti.“ *Zpravodaj ÚVT MU.* ISSN 1212-0901, 2002, roč. 12, č. 5, s. 7–10.

[7] *GridLab – A Grid Application Toolkit and Testbed*, http://www.gridlab.org/ □

Uživatel a počítačová bezpečnost

Andrea Kropáčová, CESNET CERTS[1]

Nejslabším článkem počítačové bezpečnosti obecně je vždy uživatel. Proto by měl být průběžně vzděláván a je nutné mu neustále připomínat základní pravidla pro bezpečné používání počítačů a služeb. Tento článek není návodem jak zajistit bezpečnost celé sítě nebo počítače, ani návodem na jejich bezpečnou konfiguraci. Je zaměřen na základní rizika a pravidla, která by měl každý uživatel znát a dodržovat tak, aby jeho prostřednictvím nedošlo k narušení bezpečnosti ať už konkrétně jeho dat nebo celého systému.

Základní pravidlo

Každý uživatel by měl vědět, že je nedílnou součástí širší počítačové bezpečnosti. Že bezpečnost jeho stanice není záležitostí pouze správce, nýbrž že on sám se na bezpečnosti své pracovní stanice i celé sítě aktivně podílí. Každá koncová stanice s narušenou bezpečností se může stát přestupním prvkem pro útok na ostatní zdroje v síti. Proto se počítačová bezpečnost týká všech prvků, i té nejobyčejnější pracovní stanice. *Každý systém je nejsnáze napadnutelný zevnitř.*

Vhodná volba hesla a jeho pravidelná změna

Pro automatické nástroje není problém vyzkoušet během několika minut stovky tisíc hesel; jako heslo nejsou tedy vhodná běžná slova (vyskytující se ve slovníku). Optimální nejsou ani jména oblíbených filmových či knižních hrdinů, záměna znaků s diakritikou za numerické symboly ležící na stejné klávese nebo použití dat identifikujících uživatele (adresa, čísla dokladů, data narození apod.). Hesla by měla pokud možno obsahovat i jiné než jen alfanumerické znaky (např. znaky `,.:;-=+_`). Měla by být také adekvátně dlouhá – řekněme alespoň 8 znaků – a je třeba je občas změnit.

Ochrana hesel a klíčů

Není vhodné si heslo v otevřené textové podobě kamkoliv poznamenávat – do diáře, na papírky, na doklady, na nástěnku, na stůl, na displej počítače. Pokud uživatel nevěří své paměti, je vhodné chránit heslo například další šifrou a pro uložení použít externí médium (disketu, CD-ROM, DVD, CF, Palm), které je pak třeba adekvátně ochránit před zcizením. Heslo samozřejmě není žádoucí komukoliv sdělovat a také obráceně – nedovolte, aby někdo sděloval své heslo vám!

[1] CERTS – Computer Security Incident Response Team

V případě přístupu k více službám nebo strojům, které nejsou autentizovány centrálně, není dobré používat všude stejné heslo. Pamatovat si pro různé služby různá hesla je sice trochu nepohodlné, ale nižší uživatelský komfort vynahradí vyšší bezpečnost vašich dat a programů.

Je třeba také dbát na správné používání hesla. Jestliže máte například heslo pro přístup k poště, není dobré zkoušet toto heslo ad-hoc pro jiné služby – obzvláště ne ty, o kterých nic nevíte nebo které jsou z principu nešifrované (FTP). Obecně platí, že je dobré zeptat se správce, který vám heslo vydal, ke kterým službám je možné je používat.

Mnoho uživatelů používá pro zjednodušení přístupu na vzdálené servery ssh klíče – typicky v případě, kdy potřebují pracovat s více vzdálenými servery, na kterých jsou hesla spravována individuálně. V těchto případech je nutné pečlivě zvážit, kde je možné uložit privátní klíč. Optimální je mít privátní ssh klíč uložen pouze na své pracovní stanici, byť to může komplikovat přenos dat mezi vzdálenými servery navzájem.

Ochrana obsahu zprávy a identity

Uživatelé si často neuvědomují, jak jednotlivé služby fungují. To je vede k mylné představě třeba o tom, kdo se může k jejich datům dostat a jak. Asi nejtypičtějším příkladem je elektronická pošta. Většinu běžných uživatelů šokují především dvě zjištění:

- že k obsahu jejich zpráv se může dostat každý, kdo má potřebné znalosti a možnosti (například odposlechem síťové komunikace nebo přímým přístupem k souborům na poštovním serveru). Jedinou skutečně spolehlivou cestou jak ochránit data posílaná elektronickou poštou, je jejich *šifrování*. Optimální ochranu poskytují metody založené na *asymetrické kryptografii*, například *PGP klíče a X.509 certifikáty*.
- že kdokoliv na světě může poslat e-mail, který bude mít jako odesilatelskou adresu uvedenu adresu jejich. To, že do položky *Odesilatel* může každý vložit cokoliv, se uživatel většinou dozví až v okamžiku, kdy jim od nich samých přijde nesmyslný e-mail, o kterém ví, že si jej určitě neposlali. Stejně jako v případě ochrany obsahu zprávy, i tento problém má řešení – tím je *elektronický podpis*. Elektronický podpis je navíc řešením i při ochraně integrity zprávy. Umožňuje totiž zjistit, jestli zpráva nebyla cestou změněna.

O problematice šifrování zpráv a elektronického podpisu se podrobněji zmíníme v některém z dalších článků.

Ochrana certifikátů a revokační klíče

K používání elektronického podpisu a šifrování obsahu zpráv nás motivuje snaha ochránit svá data, jejich integritu a svoji identitu. Neméně nutné je ovšem chránit privátní části klíčů (PGP, X.509 certifikátů) a být připraven na možnost zcizení nebo zničení privátního klíče. V takovémto případě je důležité klíč co nejrychleji revokovat. Revokací (zneplatněním) vlastník klíče nebo certifikátu říká, že jeho elektronickému podpisu již není možné dále věřit. Pro případ zničení privátního klíče je rozumné, aby se uživatel na tuto možnost včas připravil; např. tím, že již při generování klíčů si vygeneruje zároveň i příslušný revokační klíč.

V souvislosti s elektronickým podepisováním zpráv a jejich šifrováním je nutné dbát na pravidelnou kontrolu toho, jestli nedošlo ke zneplatnění některého z klíčů nebo certifikátů, které máme uloženy ve svém klientovi (veřejné klíče lidí, se kterými jsme v e-mailovém kontaktu). Certifikační Autority, které certifikáty vydávají, obvykle nějakou vhodnou formou zveřejňují seznam revokovaných certifikátů (například prostřednictvím svých webových stránek nebo el. poštou). Tyto seznamy by měly být v systémech uživatelů pravidelně aktualizovány.

Pečlivost a pozornost

Uživatelé by měli neustále dbát i na záležitosti typu *zamykání počítače* při opuštění pracoviště (a to i krátkodobém) a na *uzavření aplikací* typu poštovní klient před odchodem z práce. Rovněž například v internetových kavárnách, obecně u jakéhokoliv počítače, u kterého jste hostem, je

vhodné po skončení práce *vypnout spuštěné aplikace*. Je třeba být opatrný i při sdílení přenosových médií, například u médií vyměňovaných s kolegou. Obecně by měla být vždy aplikována zásada „důvěřuj, ale prověřuj“.

Přenosová média

Uživatelé by měli mít na paměti, že pravidelná antivirová ochrana jejich stanice je potřebná, není však univerzálním samospasitelným řešením. Používáme-li externí média, například při transporu dat mezi domácím a firemním počítačem, je nezbytné věnovat pravidelnou (antivirovou) péči i těmto médiím.

Archivace a šifrování citlivých dat

Pokud jsou výsledkem naší práce data, která nejsou určena pro každého a jejichž prozrazení by mohlo způsobit problémy, je vhodné data před uložením zašifrovat a mít je archivované pouze v šifrované podobě. K šifrování je možné použít např. již zmíněné PGP klíče nebo certifikáty. Dobrou volbou jak zvýšit bezpečnost dat je samozřejmě i *šifrovaný souborový systém*.

Znalost funkcionality používaných nástrojů a OS

Velkou bolestí současných technologií je skutečnost, že spolu se zvyšováním jejich uživatelské přítulnosti se zmenšuje povědomí uživatelů o tom, jak dané aplikace vlastně fungují a co jejich chování může způsobit. Pozdě se potom diví, jak je možné, že jejich „soukromý“ e-mail si může přečíst i někdo jiný než adresát, že data, která sami osobně smazali, jsou na pevném disku jejich stroje k nalezení ještě dlouho poté, co tak učinili, že se dopustili porušení autorských práv, že na jejich e-mailovou adresu chodí velké množství spamů, že mají zavirovaný počítač a podobně. Je proto vhodné znát následující pravidla a řídit se jimi:

- Nepoužívat zdánlivě užitečnou funkci zapamatovat heslo pro příští použití, kterou nabízí např. www-prohlížeč nebo poštovní klient. Uživateli tak sice přibude trocha práce navíc, ale ta za bezpečnost určitě stojí.
- Pro mazání souborů používat sofistikované metody, které zajistí skutečné fyzické smazání dat samotných, nikoliv pouze informací o nich. Zde je dobré zmínit, že je potřeba dát pozor na citlivá data například při reklamování vadného paměťového média. To, že médium nefunguje, neznamená, že data na něm jsou nečitelná. Vhodným řešením může být používání šifrovaného souborového systému nebo šifrování citlivých souborů.
- Pro bezpečnou elektronickou komunikaci používat šifrování zpráv, např. pomocí osobního X.509 certifikátu nebo pomocí PGP klíčů. Pro ochranu identity elektronické zprávy podepisovat.
- Neotevírat podezřelé e-maily a zvláště ne jejich přílohy. Na zjevný spam zásadně neodpovídat a nežádat o vyřazení z evidence, i když se to v dopise nabízí. V případě, že tak učiníte, jen potvrdíte funkčnost své adresy a podnítíte její zařazení do spamové databáze adres.
- Při používání klientů pro sdílení dat může dojít při špatné konfiguraci k tomu, že již v okamžiku stahování se data automaticky nabízí ke stažení jiným uživatelům; uživatel to často netuší a spoléhá se na to, že když stahuje autorským zákonem chráněná data výlučně pro osobní použití a nehodlá je distribuovat dál, tak se ničeho špatného nedopouští. Netuší, že jeho klient automaticky tato data zpřístupní již v okamžiku stahovací fáze.
- K většině důležitých služeb a nástrojů existují jejich zabezpečené verze. Například pro práci s elektronickou poštou jsou to protokoly IMAPS, POPS a SMTPS, pro přístup na vzdálené servery a přenos dat jsou protokoly SSH a SCP, což jsou zabezpečené obdoby nechráněných programů telnet a FTP.
- Instalovat programy pocházející jen ze spolehlivých zdrojů! Není-li si uživatel jist, měl by instalaci nových věcí nechat na správci.

Psychologický nátlak

Každý uživatel by měl vědět o možnostech psychologického nátlaku, kterého se může stát obětí i on samotný. Měl by vědět, že nikdo – kolega, správce, ani nadřízený – nemá právo po něm pod

jakoukoliv záminkou žádat sdělení hesla, a že taková žádost je nelegální, podezřelá a neměla by zůstat bez odezvy. Správce daného stroje heslo uživatele k ničemu nepotřebuje, protože má jiné prostředky, jak se v systému dostat tam, kam v souvislosti se svou rolí správce potřebuje. Nadřízený pracovník má zase k dispozici formální postupy, které může uplatnit v souladu s pravidly firmy. Nikdo nemá nárok, aby mu kolega prozradil heslo ke svému účtu, ke klíči a podobně. Vždy je vhodné si uvědomit paralelu z běžného života – souseda, nebo šéfa také neučíte svůj podpis podle bankovního podpisového vzoru. O možnostech a rizicích psychologického nátlaku by měli být informováni především začínající studenti a noví zaměstnanci.

Do této kategorie rovněž patří poplašné e-maily typu „honem si změň heslo na 'zbcdef', jinak dojde ke zneužití tvého účtu". Ke zneužití skutečně dojde, pokud takovéto výzvy uposlechnete.

Základní znalost práv, povinností a rizik

Uživatel se může dostat do vážných problémů i zdánlivě nevinnou činností jen proto, že nezná základní práva a povinnosti. Typickým příkladem je *porušení autorských práv* vystavením autorsky chráněných dat (filmů, hudby, software) na www-stránce nebo prostřednictvím klienta poskytujícího data veřejně ke stažení. Tímto činem se dopustí nelegálního šíření dat chráněných autorským zákonem a to může vést až k žalobě postiženou osobou a žádosti o finanční kompenzaci. Občas si uživatelé myslí, že se jim na poli autorkého práva nemůže nic stát, protože „Co mi může udělat firma z USA? Do České republiky na mě přece nedosáhne". Je to představa mylná; většina zemí včetně ČR má zákony, které postihují nelegální šíření dat chráněných autorským právem a každý (i osoby ze zahraničí) se jejich prostřednictvím mohou zneužití svých dat bránit.

Dalším poměrně častým prohřeškem, kterého se uživatelé dopouštějí, je spamování (spamming). Rozesláním například reklamních informací velkému množství příjemců se uživatel dopouští nejen prohřešku proti slušnosti a síťové etiketě, ale v některých případech také porušuje platné zákony.

Velkou bolestí je lehkomyslné zacházení s privátními údaji a daty. V posledních letech je velmi populární tzv. *phishing*, který svádí uživatele, aby sami prozradili svůj přístupový kód k bankovnímu účtu či jiným službám. Princip je velmi jednoduchý: uživateli přijde poplašná zpráva, že jeho bankovnímu účtu hrozí zneužití, ktere může vést ke ztrátě financí. Že tomu ale může zabránit tím, když okamžitě změní svůj přístupový kód – a to prostřednictvím uvedeného odkazu. Problém je však v tom, že příslušný odkaz nevede na stránky zmíněné banky (i když se tak tváří), nýbrž na stránky útočníka, kde je uživatel vyzván k vyplnění důležitých údajů. Pokud tak skutečně učiní, jeho osud je zpečetěn.

Na tomto poli je opravdu asi nejlepším doporučením chladná hlava, zdravý selský rozum a používání analogií z neinternetového života. Neznámému příchozímu, který by tvrdil, že vaše konto bude za 5 minut zneužito, ale on vás může zachránit když mu dáte své doklady a naučíte jej svůj podpis, také asi nebudete věřit, ale půjdete se informovat do své banky.

Spolupráce správce a uživatele

Velice důležitým bodem na poli bezpečnosti je komunikace mezi uživatelem a správcem. Uživatel by měl vědět, že správce je zde od toho, aby mu maximálním způsobem pomohl, obzvláště v případě problémů na poli bezpečnosti. Uživatelé se často stydí přiznat, že pravděpodobně udělali něco, co může vést k narušení bezpečnosti (např. kompromitace hesla) a tuto skutečnost tutlají – ať již ze strachu před správcem, před nadřízenými nebo z obavy o svou osobní prestiž. To je však zásadní chyba. Včasným a vhodným zásahem může správce ještě mnohé zachránit. Čím déle uživatel s upozorněním na svou chybu váhá, tím horší situace nakonec může být. Proto platí: správce se nebojte, zhřešivšího uživatele správce nezastřelí, ale pomůže mu.

Také je dobré si uvědomit, že i správce je jen člověk a není vševědoucí. Proto pojme-li uživatel podezření, že něco není s jeho počítačem nebo s konkrétní službou v pořádku, měl by vždy správci své podezření sdělit, byť by se nakonec ukázalo jako mylné.

Následky narušení bezpečnosti počítače/sítě

Uživatelé si často myslí, že bezpečnost jejich dat, počítače a sítě obecně se jich samotných netýká. Zvláště pak v případě, kdy jsou pouze „pasivními“ uživateli a o počítač, který při své práci používají, se stará „správce“. Mají pocit, že za vše zodpovídá správce a v případě narušení bezpečnosti se jim nemůže stát žádná újma a za nic neponesou odpovědnost. Jedná se samozřejmě o představu mylnou – i pasivní uživatel se může na porušení bezpečnosti svého počítače aktivně podílet. Například tím, že kolegovi „půjčí“ k použití svůj počítač nebo své heslo, použije zavirované přenosové médium nebo prostě jen svou naivitou a nevědomostí (porušení autorkých práv, spamming). Další mylnou představou, se kterou někteří uživatelé předem kalkulují, je, že v případě narušení bezpečnosti nelze zjistit, jak přesně k němu došlo a kdo je za problém zodpovědný. Většina zkušených správců ale je schopna tyto věci odhalit. Významnou pomoc v pátrání po slabém místě napadeného systému představují například systémy pro obnovu smazaných dat nebo centrální log-servery, které zaznamenávají důležité operace (jako například přihlášení do systému, změna dat a podobně). Uživatelé by o těchto technologiích měli vědět (stejně jako o faktu, že správce je člověk zvídavý a případy narušení bezpečnosti, když už nastanou, bere jako příležitost se něco nového naučit), zvyšuje to totiž jejich pocit odpovědnosti. Jakmile se dozvědí, že ve světě počítačů nic nemizí nenávratně, jejich přístup se změní ve prospěch bezpečnosti. Dále je vhodné informovat uživatele o možných důsledcích narušení bezpečnosti. Ty mohou být velice vážné – často jde o zneužití identity uživatele a jeho osobních dat například pro získání přístupu k privátním datům nebo k oklamání ostatních.

To všechno může vést k narušení soukromí, ke ztrátě osobní prestiže, dobrého jména, financí, k problémům v rodině a partnerském životě, k problémům v zaměstnání a následně jeho ztrátě, k vyloučení ze školy.

Obecný recept jak dosáhnout 100% zabezpečení asi neexistuje, co proto říct závěrem? Asi nejvýstižnější je pionýrské „buď připraven“ a v případě, že k narušení bezpečnosti dojde, reagovat rychle a efektivně se snahou odstranit vzniklý problém s co možná nejmenšími následky. Dále platí, že klíčem k bezpečnosti počítačů a aplikací je koncový uživatel. Čas vynaložený na jeho vzdělávání se určitě vyplatí – čili „se učit, se učit, se učit . . . “. □