ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • červen 2007 • roč. XVII • č. 5

Jednotná informační brána jako nástroj vyhledávání informací

Jindřiška Pospíšilová, Karolína Košťálová, Hana Nemeškalová, Národní knihovna ČR

Projekt Jednotné informační brány vznikl v roce 2002 jako společný projekt Národní knihovny ČR a Ústavu výpočetní techniky Univerzity Karlovy, od roku 2004 se stal projektem národním. V současné době je do projektu zapojeno 59 informačních institucí, včetně Masarykovy univerzity. Jeho hlavním úkolem je zpřístupnit uživatelům různorodé (heterogenní) informační zdroje přes jednotné prostředí. Dalším velmi důležitým záměrem je zpřístupnit na jednom místě informace o existujících zdrojích, a tím pomoci nejen uživatelům při uspokojení jejich informačních potřeb, ale také tyto zdroje propagovat a nabídnout široké veřejnosti k užívání.

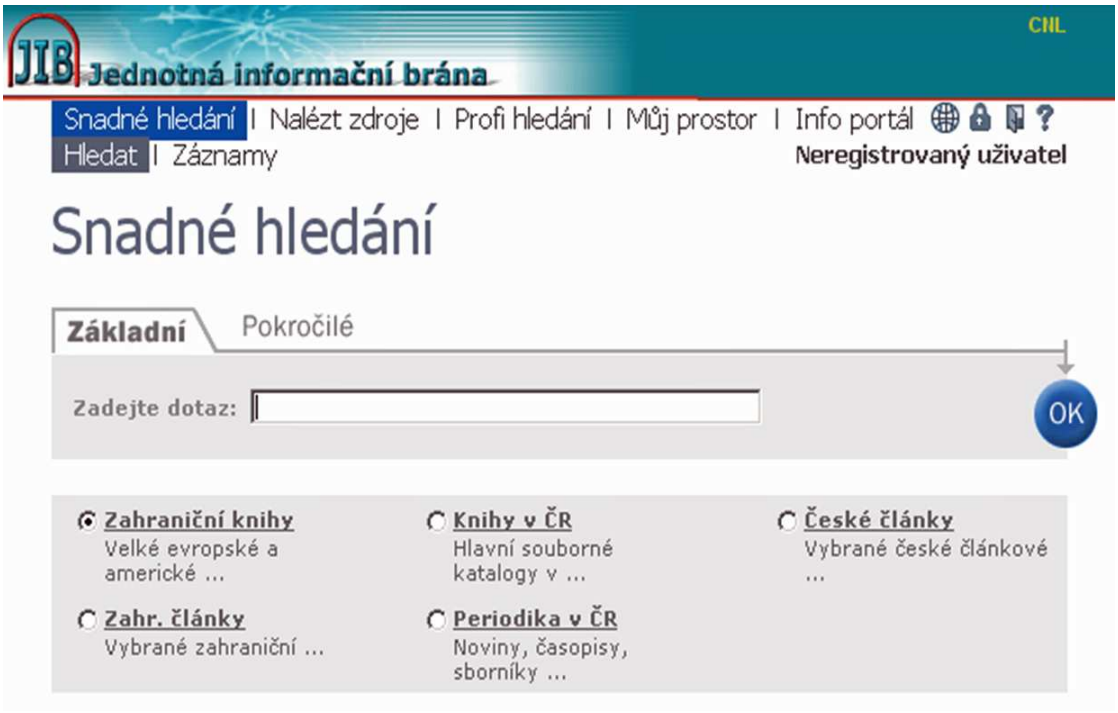
Portál Jednotné informační brány `http://www.jib.cz` (dále jen JIB) umožňuje uživatelům využívat z jednoho místa a jedním vyhledávacím rozhraním různé české a zahraniční informační zdroje: katalogy knihoven, souborné katalogy, plnotextové databáze, atd. Zdroje, které portál zpřístupňuje, lze rozdělit na volně dostupné a licencované (dostupné pouze z určitých předem nadefinovaných IP adres). Z jiného pohledu lze zdroje rozdělit na ty, které lze v rámci JIB přímo prohledávat (jejich počet je 105) a na ty, které jsou zapojeny jako odkazové, kdy uživatelé získávají na jednom místě informace o existujícím zdroji, k vyhledávání však musí použít rozhraní tohoto konkrétního zdroje. Využívat volně dostupné zdroje JIB může každý, bez ohledu na místo pobytu či současnou registraci v knihovně. Licencované zdroje může naopak využívat jen ten, kdo je registrovaný v knihovně, která licencované zdroje zpřístupňuje (vlastní), a zároveň pracuje na počítačích z povolených IP adres.

Po zadání adresy `http://www.jib.cz` uživatelé ihned vstupují do prostředí portálu JIB. Zde se mohou pohybovat pomocí odkazů na horní liště. Těmito odkazy se budeme nyní podrobněji zabývat.

Snadné hledání

Snadné hledání obsahuje několik skupin předem vytipovaných zdrojů, tzv. *předvybrané sady* – Zahraniční knihy, Knihy v ČR, Zahraniční články, České články, Periodika v ČR. Registrovaní uživatelé[1] si mohou vytvářet vlastní skupiny zdrojů, které pak využívají nejen ve Snadném ale i v Profi

[1] Jednotnou informační bránu mohou používat i neregistrovaní uživatelé. Avšak registrace v JIB umožní uživateli využívat její pokročilejší služby – vytváření osobních profilů, sestavování vlastních skupin oblíbených zdrojů, uchovávání výsledků vyhledávání, ukládání formulací dotazů, atd. Registrace je užitečná zejména pro ty uživatele, kteří pracují s JIB pravidelněji. Pro registraci klikněte na ikonu zámku (Přihlásit se) v pravé horní části obrazovky.



Obrázek 1: JIB – vstupní stránka

hledání. Po kliknutí na název skupiny se vždy zobrazí přehled zařazených zdrojů. Základním znakem Snadného hledání tedy je, že pro vyhledávání není nutné vybírat žádné konkrétní zdroje (katalogy, databáze…), stačí si zvolit některou z předvybraných sad, které jsou předem připraveny. Vyhledávání dotazu ve Snadném hledání probíhá ve všech zdrojích vybrané skupiny, nalezené záznamy se zobrazí souhrnně pro všechny vybrané zdroje v rámci sady.

Nalézt zdroje

Nalézt zdroje poskytuje několik možností, jak si vybrat zdroje pro vyhledávání. V záložce `Název` je možné listovat zdroji podle abecedy nebo hledat podle jednotlivých slov z názvu zdroje, záložka `Vyhledat` nabízí jednoduchý formulář pro hledání zdrojů podle jejich názvu, poskytovatele, kategorie, do které je zdroj zařazen, typu zdroje nebo podle libovolného slova z popisu zdroje a v záložce `Kategorie` lze zjistit, jaké zdroje jsou shromážděny v jednotlivých předmětových nebo speciálních kategoriích. Zdroje, které jsou označeny ikonkou 🔍, mohou uživatelé začít rovnou prohledávat. Ikona ⊕ slouží registrovaným uživatelům k přidání libovolného počtu zdrojů do `Mého prostoru >> Mých zdrojů`. Z těchto vybraných zdrojů si registrovaní uživatelé vytvářejí vlastní skupiny zdrojů, které pak využívají ve Snadném i Profi hledání.

Profi hledání

Rozdíl mezi Profi a Snadným hledáním spočívá především v rozdílném způsobu výběru zdrojů pro vyhledávání, a v rozšířených možnostech při práci s výsledky v Profi hledání. Prvním krokem v Profi hledání je výběr zdrojů podle různých kritérií v části *Určit zdroj*:

- Moje zdroje (pouze pro registrované uživatele)
- Předvybrané sady
- Kategorie
- Vyhledat

Pro zadání dotazu je možné i v Profi hledání použít Základní (obecně formulovaný dotaz) nebo Pokročilé vyhledání (podle autora, názvu, předmětu, roku vydání a ISBN/ISSN). Profi hledání poskytuje pro práci s nalezenými výsledky bohatší možnosti než hledání Snadné. Počet nalezených

výsledků je možné pomocí funkce `Upřesnit` rozšířit nebo zúžit. Profi hledání nabízí prohlížení vyhledaných záznamů buď podle jednotlivých prohledávaných zdrojů nebo ve sloučené množině, kde jsou automaticky odstraněny duplicity. Součástí Profi hledání je i přehled předchozích dotazů, registrovaní uživatelé si mohou jednotlivé dotazy uložit do `Mého prostoru >> Uložené dotazy` a zde z nich vytvářet tzv. *Avíza* (JIB automaticky provádí vybraný dotaz v předem stanovených časových intervalech a zdrojích, výsledky posílá na zadanou e-mailovou adresu).

Můj prostor

Zdroje a některé služby lze využívat volně, bez registrace (jako Neregistrovaný uživatel), všechna nastavení se však po odchodu z portálu JIB automaticky smažou. Všichni uživatelé si mohou služby JIB personalizovat, tedy vytvořit si vlastní prostor v rámci portálu. Tento tzv. `Můj prostor` – neboli uživatelské konto – získá uživatel po registraci do systému (registrace je zdarma). Můj prostor poskytuje následující typy služeb:

e-schránka: umožňuje ukládat a uchovávat nalezené záznamy, pracovat s nimi (zasílání e-mailem), vytvářet složky a plnit je vybranými záznamy z e-schránky;

moje-zdroje: vytváření vlastních skupin zdrojů z nabídky zdrojů JIB a manipulace s těmito skupinami zdrojů;

uložené dotazy: umožňuje uložit si dotazy z Profi vyhledávání pro další využití (vyhledávání a vytváření avíz);

předvolby: možnost přizpůsobit vzhled a chování JIB dle uživatelových preferencí (jazyk komunikace, formát zobrazení seznamu zdrojů, formát zobrazení nalezených výsledků, počty zobrazovaných výsledku, aj.).

Přidané SFX služby

Kromě vyhledávání ve zdrojích nabízí JIB také tzv. *přidané SFX služby*, které umožní uživateli získat na jeho dotaz více informací (plný text konkrétního dokumentu – je-li k dispozici, ověření dostupnosti dokumentu v konkrétní knihovně či na území ČR, objednání kopie dokumentů, získání informací o autorovi, získání dalších článků autora pomocí databáze Web of Science, apod.). Služba se aktivuje pomocí SFX-ikonek nebo S·F·X (SFX = Special Effects). V současné době je v rámci přidaných SFX služeb nabízeno 43 zdrojů, mezi nimi plnotextové databáze, souborné katalogy, knihovna elektronických časopisů EZB, portál STM (Science, Technology, Medicine), služba VPK pro elektronické dodávání dokumentů ze sítě technických knihoven ČR, a další.

Mimo portál JIB lze využít ikonku přidaných SFX služeb Získejte JIB i v jednotlivých databázích dostupných v ČR. Kromě katalogů knihoven jsou služby dostupné i v licencovaných zdrojích (jako např. EBSCO, Web of Science, souborný katalog WorldCat), ovšem za předpokladu, že administrátor příslušné báze vloží ikonku přidaných SFX služeb do systému a služby aktivuje.

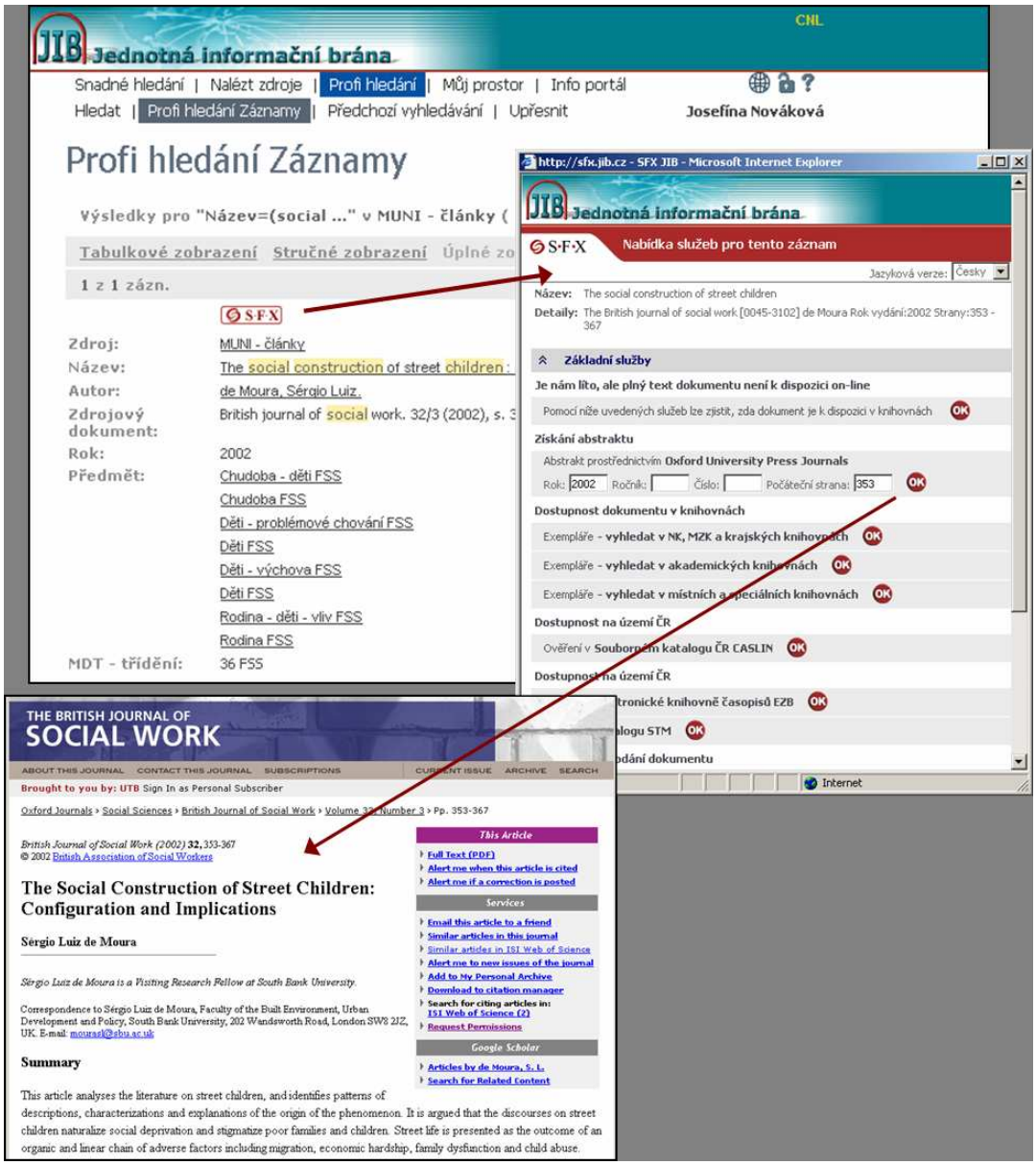
Přidané SFX služby jsou řešeny pomocí nástroje typu *link server*. Úlohou link serveru je nabídnout co nejúplnější a nejpřesnější nabídku přidaných služeb k danému dokumentu. Link servery nabízí prostřednictvím OpenURL[2] odkazy na různé typy služeb, mimo již výše zmíněné i na získání citace, recenzí v internetovém knihkupectví, encyklopedické informace o autorech, související dokumenty na Internetu, apod.

Některé další služby

Již jen velmi stručně zmiňme některé další služby, které portál JIB svým uživatelům nabízí:

CitationLinker: pokud uživatel zná alespoň některé základní informace o hledaném dokumentu, může bez nutnosti vyhledávat v dostupných informačních zdrojích aktivovat přidané SFX služby a vytvořit si jednoduše pomocí nástroje CitationLinker nabídku SFX se všemi relevantními přidanými službami.

[2] OpenURL je standard pro zakódování popisných metadat webového zdroje do jeho URL. Umožňuje přenos metadat z SFX zdroje na SFX server, který na základě zpracování OpenURL nabídne uživateli SFX menu s odkazy na SFX cíle. Pro získání OpenURL konkrétního dokumentu (např. pro webové stránky) použijte v SFX menu odkaz na službu *SFX Citation Capture*.



Obrázek 2: SFX služby v JIB

Seznamy e-časopisů: Další velkou pomůckou pro uživatele jsou seznamy e-časopisů automaticky generované podle nastavení portfolií. Tyto seznamy obsahují časopisy přístupné prostřednictvím SFX a jsou vytvořeny na základě informací dodaných knihovnami. Seznamy jednotlivých knihoven obsahují časopisy knihovnami předplácené v plných textech nebo abstraktech článků a dále také časopisy volně přístupné.

Přímé vyhledávací odkazy: MetaLib (softwarové řešení portálu JIB) nabízí v nové verzi možnost spouštět předdefinované dotazy z externího prostředí pomocí přímých vyhledávacích odkazů URL. Tato funkce najde široké uplatnění pro tvůrce webových informačních systémů. Přímý vyhledávací odkaz umožňuje koncovému uživateli přeskočit fázi přihlášení se do JIB, výběru zdrojů a definice dotazu. Výsledkem klepnutí na odkaz je spuštění dotazu přímo v prostředí JIB, který vrátí na výstupu seznam nalezených záznamů. Práce s JIB se tak pro koncového uživatele maximálně zjednoduší, odpadne

pro něho zejména volba rešeršní strategie, která často vyžaduje určitou znalost daného zdroje. Tímto způsobem lze např. dynamicky generovat seznamy tématicky relevantních dokumentů, ověřovat vlastnictví dokumentů ve fondech apod.

Portál JIB poskytuje širokou škálu služeb, jejichž úkolem je pomoci uživateli při řešení jeho informačních potřeb. Podrobné informace o portálu JIB a všech jeho službách lze získat na **InfoPortálu JIB** – `http://info.jib.cz`.

Závěr

Knihovny jsou po staletí vnímány jako místa zpřístupňování tištěných dokumentů, jako místa pro klidné studium knihy nebo periodika. S rozvojem a využíváním moderních informačních a komunikačních technologií se knihovny stále více zaměřují v nabídce svých služeb i na ty uživatele, kteří knihovnu nevyužívají standardně, tedy na ty, kteří ji navštíví pouze nahodile, omylem či dokonce vůbec ne. Portál JIB je jedním z příkladů řešení moderního zpřístupnění informačních zdrojů knihoven. Pro jeho další rozvoj je však důležité nejen trvale rozšiřovat počet zapojených zdrojů a služeb, ale i navázat komunikaci s koncovými uživateli portálu a rozvíjet ho dále ve vzájemné spolupráci tvůrců a uživatelů.

Bonus:

Jako jakýsi bonus navíc uveďme formou obrázku 2 příklad využití možností přidaných SFX služeb v JIB – získání abstraktu k záznamu článku v článkové databázi budované Masarykovou univerzitou. □

Virtualizace výpočetního prostředí – přínosy

Luděk Matyska, ÚVT MU

Virtualizace výpočetního prostředí, jejíž všeobecné koncepty i konkrétnější technické informace byly obsahem předchozích dvou článků, není jen zajímavou oblastí výzkumu, ale má jednoznačný praktický přínos. V prvním přiblížení nám virtualizace zvyšuje počet počítačů, se kterými můžeme při plánování počítat. Máme-li zajistit provoz čtyř služeb (např. DNS server, webový server, mail server a ftp server), doporučení odborníků platné před návratem virtualizace říkala, že potřebujeme čtyři počítače, každý právě pro jednu službu. Jedině tak jsme mohli zajistit prostředí optimální pro každou ze služeb a současně garantovat její bezpečnost. Virtualizace umožní opět každou službu uzavřít v „jejím" počítači, avšak virtuálním. A všechny tyto virtuální počítače pak můžeme spustit na jednom fyzickém, čímž ušetříme nejen prostředky na nákup tří počítačů, ale i náklady na jejich provoz (elektřina, chlazení) a správu.

Toto naivní využití možností virtualizace však má i svá úskalí a nedostatky. Hlavní problém je v robustnosti – všechny čtyři služby sdílí stejný počítač, pokud dojde k jeho výpadku, přestanou fungovat všechny služby současně. Virtualizace nám však umožní řešit efektivně i tento problém. Představme si, že místo jednoho použijeme dva fyzické počítače. Pokud vše funguje, na každém z těchto počítačů poběží dva virtuální stroje se dvěma funkcemi. Dojde-li k výpadku jednoho fyzického počítače, dojde k výpadku pouze dvou služeb. Hlavní výhoda se však projeví v nápravě (recovery) tohoto výpadku. Ty dva virtuální stroje, k jejichž výpadku došlo v důsledku zhroucení jednoho fyzického počítače, můžeme s co nejmenší časovou ztrátou spustit na tom zbývajícím počítači, aniž bychom jakkoliv zasáhli do na něm již běžících služeb. Dojde sice k určitému poklesu výkonu všech čtyř služeb, ale jsme schopni všechny služby provozovat s minimálním přerušením. A zejména nijak nemusíme měnit konfigurace jednotlivých služeb a jejich počítačů – řešení je v podstatě ekvivalentní tomu, že máme stále k dispozici záložní fyzický počítač.

Virtualizace nám tak nejen umožnila snížit počet fyzických počítačů, ale současně velmi efektivně reagovat na případné výpadky bez nutnosti držet si záložní počítače. Držíme si pouze záložní *virtuální* počítače a dokud máme alespoň jeden fyzický počítač, jsme schopni zajistit funkci všech poskytovaných služeb.

Tento přístup můžeme dále rozšířit. Namísto pevného mapování virtuálních počítačů na fy-

zické můžeme rozhodovat dynamicky, zpravidla podle aktuální zátěže. Již v našem modelovém případě dvou počítačů a čtyř služeb můžeme třeba v době vyšší zátěže webového serveru jeho virtuální počítači přidělit jeden fyzický stroj a ostatní tři virtuální počítače (a jejich služby) ponechat na druhém. Při poklesu zátěže webové serveru pak můžeme nějaký z těch tří virtuálních strojů přesunout a zvýšit tak poskytovaný výkon všech tří služeb.

V předchozím odstavci jsme použili obrat *přesun virtuálního počítače*. To je další oblast, ke nám virtualizace nabízí dříve (téměř) nedostupné možnosti. Každý virtuální počítač běží v prostředí nějakého hypervizoru (VMM, Virtual Machine Monitor), který mimo jiné rozhoduje o přidělení procesoru a také má plně pod kontrolou všechna virtuální rozhraní (především přístup na disk či do počítačové sítě). Jestliže hypervizor odebere konkrétnímu virtuálnímu počítači procesor, virtuální počítač se zastaví, ale „neví" o tom. V tomto stavu můžeme virtuální počítač „uklidit", tj. vzít veškerou paměť, kterou používá, a zkopírovat ji na disk. Takto vytvoříme *obraz* virtuálního počítače ve stavu, který odpovídá hibernaci operačního systému (bez virtualizace). Proti hibernovanému stavu, který zpravidla nelze spustit jinde než na tom počítači, kde došlo k hibernaci, můžeme virtuální obraz přesunout na jiný počítač a spustit jej tam – přesunuli (migrovali) jsme tak celý virtuální počítač na jiný fyzický, aniž by jakkoliv došlo k narušení vnitřního stavu virtuálního počítače. Samozřejmě reálná situace je komplikovanější kvůli vstup/výstupním operacím. Systém souborů můžeme přesunout též (s tím přesuneme i otevřené soubory), skutečný problém je však se síťovou komunikací. Pokud virtuálnímu počítači odebereme procesor, ztratí přirozeně schopnost přijímat data – pokud mu nějaký jiný (virtuální) počítač pošle paket, ten paket nemůže být přijat. Naštěstí toto může zajistit hypervizor. Pakety přichází na fyzickou síťovou kartu, hypervizor je přesunuje do virtuálního síťového rozhraní konkrétního virtuálního počítače. Hypervizor „ví", že konkrétní virtuální počítač je přesouván, může proto pro něj určené pakety ukládat do bufferu a tento buffer rovněž přesunout na cílový počítač (do odpovídajícího bufferu cílového hypervizoru). Tímto způsobem je možné zajistit i bezeztrátovost síťové komunikace. Samozřejmě zůstává nebezpečí, že druhá strana čeká na odpověď a pokud ji nedostane v nějakém konečném časovém intervalu, spojení přeruší. Toto nebezpečí můžeme minimalizovat rychlostí přesunu virtuálního stroje a jeho rychlým znovu spuštěním. Toto schéma funguje pouze při přesunu v rámci lokální sítě, kdy nemusí dojít ke změně IP adresy virtuálního stroje.

Pokud máme k dispozici obraz virtuálního stroje, nemusíme jej pouze přesouvat, ale můžeme jej i kopírovat. Tímto způsobem si můžeme udělat *vzorovou instalaci* (gold image) a kdykoliv budeme potřebovat výpočetní prostředí s těmito parametry, vytvoříme kopii vzorové instalace virtuálního počítače a tu spustíme na vhodném fyzickém počítači. Kromě rychlosti nám tento přístup zejména zaručuje naprostou identitu všech spuštěných strojů. Dokonce si můžeme dovolit konkrétní virtuální počítač po použití (např. realizaci konkrétního výpočtu) zrušit a příští výpočet spouštět opět v „čistém" prostředí původní vzorové instalace. Můžeme tak minimalizovat riziko ovlivnění následných použití virtuálního počítače (např. problémy způsobené chybnou implementací nějakých funkcí jádra, které mohou vést k postupnému vyčerpání paměti, zániku některých funkcí atd.).

Možnosti, které nabízí virtualizace, však zdaleka nejsou omezeny jen tím, co jsme prozatím diskutovali. Některé z těch pokročilejších si uvedeme dále.

Výše uvedený způsob migrace virtuálního počítače má charakter „ulož a přesuň" (store and forward). Možná je ale i tvorba kopie v reálném čase, kdy začneme kopírovat běžící virtuální počítač a dosáhneme stavu, kdy na dvou fyzických strojích máme dva identické virtuální počítače (ve stejném stavu rozpracování). Pouze jeden z těchto počítačů však skutečně „počítá" (výpočet druhého je simulován tím, že se v něm zaznamenávají změny stavu toho aktivního virtuálního počítače). A ve vhodném okamžiku se přepne řízení a nově vytvořená kopie převezme aktivitu a původně virtuální počítač skončí. Při

pečlivé práci s buffery je možné garantovat přesun v rámci lokální sítě se ztrátou nejvýše jednoho paketu, což odpovídá skutečně okamžité migraci.

Použití virtuálních počítačů a jejich migrace můžeme použít i k velmi významné *úspoře spotřeby elektrické energie*. Použijme opět původní příklad, ale při startu služeb spusťme všechny čtyři virtuální počítače na jednom fyzickém a druhý fyzický buď ponechme úplně vypnutý nebo jej držme v nějakém energeticky úsporném režimu. Dokud bude stačit výkon prvního fyzického počítače, pouze ten spotřebovává energii (a generuje teplo). teprve při jeho přetížení aktivujeme druhý počítač. Tento model můžeme rozšířit na více služeb, resp. jejich kopie a tím dosáhnout skutečně významných úspor elektrické energie. Např. velké webové servery běží na velkých clusterech, přitom jen část dne je pro obsluhu uživatelských požadavků skutečně třeba plný výkon všech uzlů. Virtualizace umožňuje využít v každém okamžiku optimální počet uzlů, ostatní mohou být vypnuté. Přitom díky kopírování a migraci virtuálních počítačů je možné velmi rychle reagovat na změny zátěže.

Virtualizace umožňuje také *zvýšit spolehlivost konkrétních výpočtů*. Snímek stavu virtuálního počítače nemusíme vytvářet jen když jej chceme migrovat, během výpočtu můžeme pravidelně vytvářet snímky stavu (checkpoints) a ty ukládat. Dojde-li z nějakého důvodu ke zhroucení počítače, můžeme aktivovat nějaký z předchozích snímků a výpočet dokončit s minimální ztrátou. Snímek celého virtuálního počítače nám poskytuje vyšší záruku spolehlivosti proti situaci, kdy se snažíme vytvořit pouze snímek (checkpoint) běžící aplikace (nemusíme speciálně kopírovat vnitřní stavy struktur jádra operačního systému, ukládáme celý operační systém i s jádrem). S rostoucí rychlostí a zejména kapacitou disků nevadí vyšší režie tohoto přístupu (vytváříme snímek celého virtuálního počítače, jeho paměti a případně i systému souborů).

Zajímavou oblastí je i využitelnost virtuálních oblastí pro *interaktivní práci*. Máme-li jeden počítač (s jedním procesorem) a spustíme-li na něm dva virtuální počítače, budou vzájemně soupeřit o výkon procesoru. Hypervizor však může nejen zvýšit prioritu jednoho virtuálního počítače (na úkor druhého), ale může změnit i parametry předávání procesoru mezi oběma virtuálními počítači (např. velmi snížit dobu, po kterou má virtuální počítač procesor garantován). Tímto způsobem můžeme dosáhnout toho, že jeden z obou virtuálních počítačů může být vysoce interaktivní, vhodný pro přímou práci uživatele, a přitom spotřebováva jen malou část celkového výkonu procesoru (v literatuře jsou popsány experimenty, kdy interaktivní virtuální počítač spotřebuje jen cca 10 % celkového výkonu a přitom uživatel má pocit, že počítač je pouze jeho a má vynikající odezvu.

Interaktivitu je možné zkombinovat s migrací: v první fázi všechny virtuální počítače běží na jednom fyzickém. Jakmile se uživatel připojí na virtuální počítač (např. `ssh`), tomu je přidělen fyzický počítač a na něj je příslušný virtuální počítač odmigrován. Proces přihlášení trvá déle, ale fyzické počítače jsou použity až skutečně podle potřeby – kromě úspory elektřiny je možné i optimalizovat sdílení výpočetní infrastruktury mezi interaktivními a dávkovými úlohami.

Virtuální počítače, resp. virtualizace výpočetní infrastruktury nejen pomáhá řešit řadu existujících problémů, ale otevírá i prostor pro zcela nové způsoby využití výpočetních infrastruktur. Způsoby použití zmíněné v tomto článku představují jen část již známých možností – nezmínili jsme např. vazbu na virtualizaci sítě, nové možnosti paralelních a distribuovaných výpočtů ve virtualizovaném prostředí – představují však určitý reprezentativní výsek a demonstrují, že s virtualizačními technologiemi i technikami jejich využití se budeme v budoucnosti stále více setkávat. Lze dokonce očekávat, že postupně převážná většina výpočtů bude probíhat ve virtualizovaném prostředí a uživatelé nebudou příliš přicházet do přímého kontaktu s fyzickým prostředím. □

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.

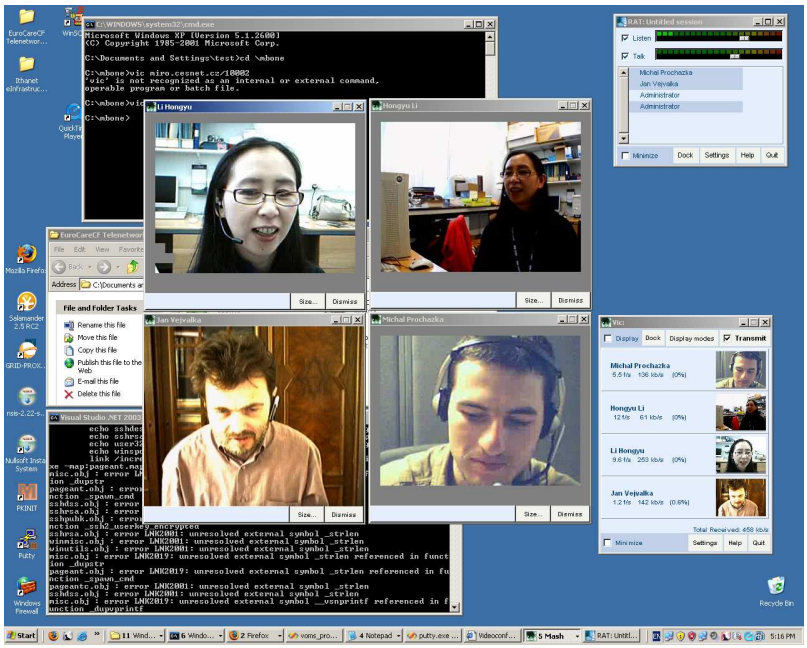
Síť Skype je primárně určena pro hlasovou komunikaci. V posledních verzích se objevila i podpora přenosu videa. K výhodám Skype patří šifrovaný přenos dat a možnost prostupovat firewally a NAT. Přes tyto výhody existuje také několik podstatných nevýhod. Protokol je jednak proprietární, a proto je velmi 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.

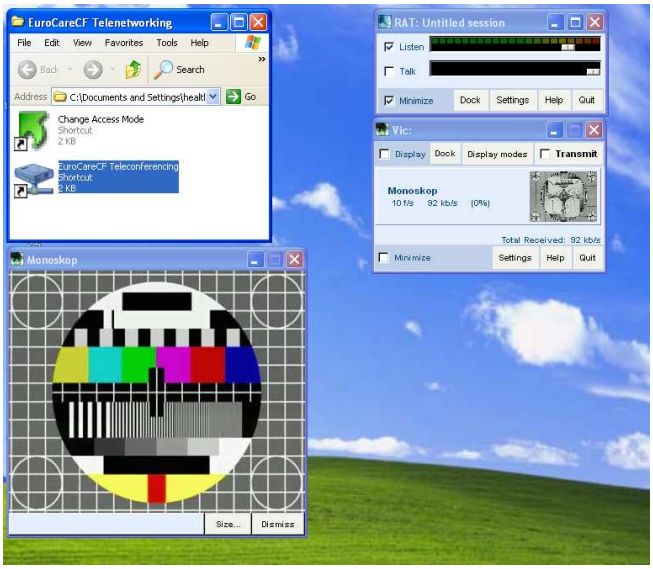
3.1 Pilotní provoz

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. □

Na pohádky s vtipem, na bezpečnost s čipem!

Václav Lorenc, ÚVT MU

Laskavý čtenář promine, ale dnešní příspěvek o bezpečnější autentizaci začneme poněkud netradičně, pohádkovým vstupem.

Bylo, nebylo...

V učebnicích a skriptech o počítačové bezpečnosti je možné najít tři základní způsoby prokázání identity jedince. Zkusme se tedy společně podívat na konkrétní případy a zmínit si jejich výhody, nevýhody a případná možná vylepšení.

Popořadě tedy – prokázat svoji identitu mohu něčím (a) co znám, (b) co mám, (c) čím jsem. Zabrouzdejme tedy do zmiňovaného pohádkového světa a pokusme se podpořit stručný výčet vhodnými ilustracemi.

Velice pěkný příklad něčeho, *co známe*, jsou hesla, v pohádkách známá již přinejmenším tisíc a jednu noc. Vzpomeňme na Alibabu a jeho pohádkovou jeskyni plnou pokladů. Přístup k ní nebyl chráněn ničím jiným, než právě heslem. A to ne zrovna slabým – „Sezame, otevři se". Heslo to není triviální, nedostatečně dlouhé, ba dokonce i vůči slovníkovému útoku tehdejší doby by jistě obstálo.

Příběh sám nám však dává odpověď na otázku, má-li tento způsob přihlašování slabiny. Bohatě totiž postačí, když si dotyčné heslo někdo poslechne, a jeho prostým zopakováním se dostane do zabezpečené jeskyně. Samotná hesla tedy moc bezpečí nepřinesou, nezdaří-li se je vhodně ochránit.

Prokazování se něčím, *co mám*, je trochu větší oříšek. Často k tomuto účelu slouží tzv. tokeny, tedy klíče nebo královské pečeti, rozličné šátky, prsteny, královští koně a nebo dostatečně vznosné oblečení. Ostatně rozlišit lháře od pravého zachránce se na královské hostině zadaří právě pomocí prstenu, který statečný kovář Mikeš dostal od princezny při jejím zachraňování (tábor příznivců Bajaji si vzpomene na podobnou situaci, kde však hrál hlavní roli šátek).

I tato metoda má však svoje nedostatky. Jak například postupovat v případě krádeže? Jak zabezpečit, aby dotyčná věc byla natolik jedinečná, aby nešla zfalšovat? Vždyť nejedna pohádka dokonce začíná touto premisou, kdy důkaz původu získá nesprávná osoba. Je tedy často nutné obezřetně volit, co použijeme v roli tokenu.

Nu a třetím případem, moderně zvaným biometriky, je autentizace něčím, *co jsme*, nějakou vlastností, kterou si neseme stále s sebou. I tento způsob není v pohádkách nikterak neobvyklý. „Šaty s vlečkou, stříbrem vyšívané, ale princezna to není, jasný pane." Vzpomínáte? Vměstnat se do miniaturního střevíčku dokázala z celého království pouze jediná slečna, byť měla tváře od popela umazané. A právě neobvykle malá velikost Popelčiny nohy je v tomto případě onou biometrikou.

Najít však dostatečně charakteristický znak pro každou pohádkovou bytost by bylo více než obtížné. A to ani nezvažujeme nutnost nejen získat, ale i uchovat střevíc každé osoby v království, pokud bychom tuto metodu chtěli použít plošně.

Současně vyvstává i poměrně přirozená otázka – je možné jednotlivé metody kombinovat? Ale dozajista! Takový přístup je velice důležitý pro zvýšení bezpečnosti celého řešení. Ostatně i tady máme velice pěkný příklad. Tři kůzlátka, zavřená v domečku, se snaží odhalit, je-li osoba za dveřmi jejich maminka, nebo zlý a hladový vlk. Vlk, pamětliv Alibaby, odposlechne heslo a okamžitě zkouší, bude-li fráze „Kůzlátka, kůzlátka, otevřete vrátka..." dostatečným oprávněním ke vstupu. Ale ouha, je třeba navíc prokázat, že i

hlásek má vlk natolik tenounký, aby zněl stejně jak maminka koza.

V království plném bitů…

V tuto chvíli však opustíme pohádkový svět a vrhneme se do vod kruté digitální reality, v němž je magie v mnohém nahrazena matematikou a fyzikou.

Na výše uvedených příkladech je vidno, že ačkoliv se jednotlivé metody dají samy o sobě poněkud vylepšit, jejich kombinace se prokazují jako mnohem odolnější vůči útokům. Zkusme si ukázat i příklady bezpečnější autentizace v běžném životě.

Typickým případem je přihlašování se k počítači. Je již zažitým zvykem používat pro takovou situaci kombinaci jména a hesla, v lepším případě s nějakou politikou změny hesla, jeho minimální délky či odhadované odolnosti vůči slovníkovému útoku.

Navíc není neobvyklé, že mnoho lidí mívá přístup do různých systémů. Jedno heslo pak používá pro přihlášení se ke svému osobnímu počítači, jiné pro přístup k e-mailu, další pak pro přístup k elektronickému bankovnictví či k účetnímu programu. V lepším případě jsou tato hesla různá a nadprůměrně kvalitní, v horším to končívá jedním jednoduchým a snadno zapamatovatelným heslem, které je ke všemu napsané na papírku u monitoru.

Celá situace se ještě trochu zamotá, přidáme-li digitální identitu člověka a s ní související elektronický podpis. Pamatovat si odpovídající podepisovací klíče, reprezentované několika tisíci jedniček a nul, již opravdu není v silách běžného uživatele, proto bývají uloženy někde na disku. A právě obrana elektronické identity by měla být prioritou - nikdo by nebyl rád, kdyby se jeho jménem páchaly digitální zločiny.

Zatímco u klasických klíčů je jejich krádež a kopírování přinejmenším zjistitelné, neb je bude jejich majitel po nějakou dobu pohřešovat, u digitálních je situace mnohem horší. Pořídit digitální kopii dat je možné nepozorovaně a s téměř nulovými náklady, v případě klíčů pak i velice rychle. Ideální úložiště důvěrných dat (klíčů) by tedy mělo být takové, které by umělo chránit libovolná data do něj vložená, a v případě nutnosti provádět nad těmito daty požadované kryptografické operace tak, aby uchovávané tajemství žádným způsobem toto úložiště neopustilo. Ačkoliv to zní jako úkol pro chytrou horákyni, taková zařízení existují.

Jsou jimi kryptografické čipy. Běžněji se s nimi potkáte v nově vydávaných platebních kartách, kde nahrazují funkci nepříliš důvěryhodného magnetického proužku, v dobách předmobilních se s nimi mnoho lidí potkávalo v předplacených telefonních kartách, dnes v podobě SIM karet, v bezkontaktní podobě i v nedávno zavedených elektronických kartách Českých drah.

Pro potřeby bezpečného přihlašování a podepisování dat na počítači existují speciální USB zařízení, která právě takovou funkci poskytují. Obsahují kryptografický čip s bezpečným úložištěm dat, jejich podpora v operačních systémech se různí, ale zlepšuje se, a zejména jsou to zařízení natolik přenosná, že jejich nošení u klasických klíčů od bytu či auta nečiní problémy. A ač se taková zařízení často neliší vzhledem, liší se právě svým obsahem, tedy klíči na nich uloženými. Jedná se tedy o variantu tokenu.

Pozorní čtenáři si jistě uvědomili, že spousta z výše jmenovaných zařízení, neposkytuje své funkce každému na potkání. Stejně jako byl Golem spouštěn svým šémem, kryptografické čipy často požadují autentizaci uživatele předtím, než začnou pracovat. Ta se děje nejčastěji za pomoci tzv. PINu, tedy nějakého číselného kódu rozumné délky.

Tím jsme se v pohádkovém i reálném světě dostali ke stejnému poznatku – kombinaci více faktorů při prokazování identity uživatele. Nikoliv však hláskem a heslem, ale v tomto případě PINem a odpovídajícím USB tokenem. Potenciální zákeřný lupič tak musí nejen ukořistit přístupový PIN, ale i token samotný, což mu rozhodně lup neusnadní.

Bylo by příjemné říci, že jsme se tímto dostali k nejvyspělejší technologii bez jakýchkoliv chyb, nebyla by to však pravda. Právě masivnější rozšíření kryptografických USB tokenů ukazuje, že

ač je míra jimi poskytované bezpečnosti obvykle opravdu vyšší, je stále řada nedořešených otázek. V prostředí úkolů řešených ve spolupráci s Masarykovou univerzitou jsou to např. projekty Medimed a provázané gridové aplikace. Objevuje se potřeba důvěryhodných vstupů a výstupů tak, aby bylo zařízení schopno pracovat i v nedůvěryhodném prostředí, tedy obchodech, internetových kavárnách nebo učebnách. Tedy i v takových situacích, kdy je samotný počítač napadený virem nebo pod kontrolou útočníka, a přesto by bylo vhodné nějakým způsobem zabránit úniku důvěrných informací.

To jsou témata, nad kterými v současnosti probíhá výzkumná práce a objevují se prototypy nových zařízení. Doba prostých hesel však již pomalu končí a je třeba se dívat do budoucnosti, se všemi jejími klady i zápory.

Zazvonil zvonec...

Pohádkou jsme začali, pohádkou skončíme. Vždyť i bájné království, které se snažilo předejít strašlivé sudbě, nakonec neuspělo pro jednu jedinou růži či kolovrátek. A že jim odstranění problému trvalo sto let? Budiž to pro nás poučením – každý řetěz je jen tak silný, jak silný je jeho nejslabší článek... □

Tipy z Inetu: Evidence zahraničních služebních cest

Ivan Burian, ÚVT MU

1 Rozsah evidence

Tématem dnešních tipů z Inetu je evidence údajů a výpisy parametrizovaných sestav o zahraničních služebních cestách. Evidence zahraničních služebních cest je primárně určena personalistkám, pracovníkům oddělení vědy, výzkumu a zahraničních vztahů či jiným specializovaným pracovníkům MU, ale obsahuje také *Osobní přehled zahraničních cest*. Soubor aplikací se skládá z těchto čtyř částí:

- *Zadávání zahraničních cest* (`https://inet.muni.cz/app/ces/form`) – slouží k základnímu zadávání informací o zahraniční služební cestě;
- *Přehled výjezdů do zahraničí* (`https://inet.muni.cz/app/ces/vystupy`) – vypisuje parametrizované sestavy o zahraničních cestách pro specializované pracovníky MU;
- *Osobní přehled zahraničních cest* (`https://inet.muni.cz/app/ces/vystupy_user`) – vypisuje informace o osobních zahraničních cestách pro konkrétního přihlášeného zaměstnance (studenta, dohodáře);
- *Přehled zahraničních měst a organizací* (`https://inet.muni.cz/app/ces/prehmest`) – doplňková aplikace vypisující seznam měst a navštívených (evidovaných) organizací pro potřeby zadávání zahraničních služebních cest.

Aplikace se v Inetu nachází v podmenu *Ekonomika*, sekci *Služební cesty*.

2 Pohled do historie

Jednotlivé aplikace vznikaly postupně během roku 2002. Nejdříve to byla základní aplikace pro *Zadávání zahraničních cest* a následně *Přehled výjezdů do zahraničí*. Aplikace byly koncem roku 2002 napojeny na elektronický docházkový systém, takže již není potřeba u služebních cest zaměstnanců zadávat základní údaje – jméno, příjmení, pracoviště a termín cesty – přímo, protože se tyto údaje přebírají z docházkového systému. U zahraničních služebních cest studentů (převážně doktorandů) se však tyto údaje zadávat musí, neboť nejsou obsaženy v docházkovém systému. Následně byly v roce 2003 přidány aplikace *Osobní přehled zahraničních cest* a *Přehled zahraničních měst a organizací*.

Aplikace využívají řadu číselníků – Rámec cesty, Druh cesty, Státy, Města, Firmy a organizace. Číselníky Rámec cesty a Druh cesty byly vytvořeny pouze pro potřeby zahraničních služebních cest. Číselník firem a organizací je postaven na stejnojmenném číselníku ekonomického systému univerzity (IS Magion). Jedná se tedy hlavně o subjekty, s nimiž má nebo měla univerzita ekonomický styk. Tento číselník je však možné pro potřeby zadávání služební zahraničních cest rozšiřovat i o další „neekonomické" subjekty a akce. Pro pohodlnější zadávaní informací o cestách a následně pro tvorbu detailnějších výstupů byl na

základě číselníku firem a organizací vytvořen i číselník měst (číselník států je standardní číselník dle normy ISO 3166).

Při vývoji aplikace se počítalo s jejím rozšířením i do oblasti ekonomiky – o návaznosti na cestovní náklady, kapesné, diety atd. Tato část však nebyla realizována z důvodu absence přesné metodiky evidence a zpracování, v současné době tedy aplikace slouží pouze k evidenčním a statistickým účelům. Do budoucna se však plánuje propojení evidence zahraničních služebních cest s evidencí projektů, a tedy oživení ekonomických návazností.

3 Vybrané podrobnosti

Jak již bylo řečeno, aplikace slouží primárně pro potřeby specializovaných pracovníků a oddělení MU. Celé akademické obci jsou přístupny aplikace *Osobní přehled zahraničních cest* a *Přehled zahraničních měst a organizací*.

První z nich vypisuje stručný přehled všech zahraničních cest pracovníka uskutečněných od roku 2002 a ke každé cestě informace o navštívené organizaci či akci (samozřejmostí je název města a státu), rámci a druhu cesty. V případě, že doplňkové informace chybí, je vypsáno hlášení *„záznam o zahraniční cestě není doplněn"*. Pak je žádoucí požádat odpovědného pracovníka fakulty či ústavu o doplnění údajů.

Aplikace *Přehled zahraničních měst a organizací* vypisuje seznam všech organizací aktuálně použitelných pro doplňování informací o služební cestě. Po výběru a potvrzení státu se zobrazí seznam všech uložených měst. Při „rozkliknutí" názvu města se následně vypíší všechny evidované firmy a organizace. Chybějící organizace doplní na požádání pracovníci ÚVT, nebo je lze vkládat přes ekonomický systém Magion.

Pro specializované pracovníky jsou určeny další dvě aplikace. *Zadávání zahraničních cest* je základní část, sloužící pro vkládání, editaci či mazání doplňkových informací o služební cestě. Úvodní obrazovka se skládá ze tří částí:

- formulář pro změnu roku, pracoviště a vyhledání osoby (vyhledávají se pouze studenti, záznamy o cestách zaměstnanců se přebírají z docházkového systému);
- seznam uskutečněných a dosud nedoplněných zahraničních služebních cest zaměstnanců přebraný z docházky – záznamy je potřeba doplnit;
- seznam již doplněných služebních cest – záznamy je možné mazat nebo editovat.

V druhé obrazovce se již u konkrétní služební cesty vkládají nebo editují doplňující informace – stát, město, místo pobytu (akce, organizace nebo firma), druh a rámec pobytu. K druhu a rámci pobytu lze ještě přidat upřesňující textovou poznámku.

Specializovaným pracovníkům slouží také čtvrtá aplikace této sekce – *Přehled výjezdů do zahraničí* – poskytující parametrizované výpisy evidovaných zahraničních služebních cest. Ve vstupním formuláři je možno zadat výběrové kritérium a rozsah vypisovaných informací. Vypisovat lze cesty na konkrétním pracovišti, za definované období, pro určitou osobu, podle navštívené organizace (akce či firmy) a nebo v daném státě a městě. Povoleny jsou také vzájemné kombinace.

Stručná statistika počtu záznamů o zahraničních služebních cestách je uvedena v tabulce 1.

	Počty záznamů	
Rok	Z docházky	Doplněné
2002	440	134
2003	2076	1039
2004	2592	1063
2005	3293	1137
2006	4043	1294
2007	1282	242

Tabulka 1: Počty záznamů

Máte-li nějaké přání nebo náměty k evidenci zahraničních služebních cest, uvítáme je na e-mailové adrese `eko-inet@ics.muni.cz`. □

Obsah XVII ročníku Zpravodaje

Zpravodaj XVII/1, říjen 2006

Hektické léto v CPS MU 1
Zpravodaj na webu: včera a dnes 2
www.muni.cz ve verzi 200 4
Elektronické pasy 7
Zveřejňování závěrečných prací v IS MU 12
Tipy z Inetu: Nepřítomnost na pracovišti 14

Zpravodaj XVII/2, prosinec 2006

Zkušenosti s pořizováním videozáznamů na MU 1
Všichni chceme Eduroam! 4
www.muni.cz ve verzi 2006 (2) 6
Virtualizace výpočetního prostředí 9
Matematický systém Maple 11
Tipy z Inetu: Osobní přehledy a nálezy majetku 15

Zpravodaj XVII/3, únor 2007

Wikipedie – otevřená encyklopedie 1
Digitalizace v Archivu MU – první krůčky 5
Techniky virtualizace počítačů 9
Fotografování osob a výroba id-karet na MU 12
Kurz práce s informacemi 15
Tipy z Inetu: Účetní sestavy 18

Zpravodaj XVII/4, duben 2007

Spam – co s ním? 1
E-mail a centrální poštovní server MU 5
E-mail, spam a greylisting MU v číslech 8
Jak se chránit proti spamu 11
Nový personální a mzdový systém MU 14
Tipy z Inetu: Personální údaje a údaje o pracovních poměrech 18

Obsah

Jednotná informační brána jako nástroj vyhledávání informací, *Jindřiška Pospíšilová, Karolína Košťálová, Hana Nemeškalová, Národní knihovna ČR* **1**

Virtualizace výpočetního prostředí – přínosy, *Luděk Matyska, ÚVT MU* **5**

Videokonference za zdí, *Eva Hladká, Petr Holub, Michal Procházka, ÚVT a FI MU* **8**

Na pohádky s vtipem, na bezpečnost s čipem!, *Václav Lorenc, ÚVT MU* **12**

Tipy z Inetu: Evidence zahraničních služebních cest, *Ivan Burian, ÚVT MU* **14**

Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Grafex Blansko • *Neprodejné* • ISSN: 1212–0901