ÚVT MU

zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • duben 2005 • roč. XV • č. 4

Rada informačních technologií Masarykovy univerzity v Brně

Luděk Matyska, ÚVT MU

Rozhodnutím rektora Masarykovy univerzity v Brně, prof. Petra Fialy, byla loni na podzim ustavena *Rada informačních technologií* (viz `http://www.muni.cz/misc/itboard.html`) jako rektorův poradní orgán pro oblast informačních a komunikačních technologií. Analogická Rada existovala v letech 1991 až 1998 a její existence přispěla k rozvoji informačních technologií na MU, definici postavení a úkolů ÚVT a položila základy současného vysoce efektivního využití informačních a komunikačních technologií na MU v současnosti.

Hlavním úkolem současné Rady je zajištění koncepce rozvoje informačních a komunikačních technologií na Masarykově univerzitě v Brně tak, aby nasazení těchto technologií v maximální míře přispívalo k integraci a dalšímu rozvoji MU i jejích jednotlivých součástí (fakult, ústavů, . . .). Informační technologie tvoří jeden ze základů univerzitní infrastruktury a např. prostřednictvím Informačního systému studia (IS MU) v posledních letech velmi výrazně přispěly k přijetí nové struktury studia (model 3-2-3) a současné vysoké propustnosti studia na univerzitě. Neméně významné, přestože z pohledu běžného pracovníka či studenta univerzity méně patrné, jsou však i další informační systémy, které umožňují administraci osob (personalistika) či majetku (účetní a inventární systémy) křížově přes celou univerzitu.

Dalším integračním procesem je propojení telefonních ústředen a využití principů Internetové telefonie (VoIP, Voice over IP). Přes fyzickou distribuci jednotlivých budov má dnes univerzita jednotný číslovací systém a telefonické hovory nejen uvnitř univerzity, ale prostřednictvím počítačové sítě CESNET2 i mezi univerzitami jsou dnes zdarma (resp. za cenu paušálních poplatků, jejichž výše není přímo úměrná počtu protelefonovaných minut).

Rada má za úkol hledat nové možné oblasti nasazení informačních a komunikačních technologií ve střednědobém a dlouhodobém horizontu. Do působnosti Rady nepatří běžná operativa (tomu ani neodpovídá složení Rady), ale strategické návrhy. Těmi může být např. identifikace nových oblastí, v nichž může univerzita nasazením odpovídajících technologií získat předpoklady k dalšímu rozvoji (aktuální otázkou je např. oblast elektronické podpory výuky, abychom nemluvili jen o informačních systémech). Další oblastí je ale samozřejmě i kritické hodnocení stávající situace na MU a návrhy dalších postupů i v těch oblastech, kde již dnes MU patří přinejmenším v ČR v nasazení informačních technologií k naprosté špičce.

Kromě koncepce rozvoje technologií na MU mezi další konkrétní úkoly Rady patří:

– Posuzování *priorit úkolů* v oblasti informačních a komunikačních technologií z hlediska dlouhodobé prospěšnosti MU, resp. jejích strategických činností, tj. výuky a výzkumu. Rada by do rozhodovacích procesů měla vnést silnější akcent potřeb akademické obce MU, tak aby další rozvoj byl skutečně v souladu se zájmy a potřebami MU jako akademické instituce.
– Posuzování *rozsahu a využití finančních prostředků* vynakládaných na celouniverzitní úrovni v oblasti informačních a komunikačních technologií. Toto je jak krátkodobý – posouzení aktuálního rozpočtu pro daný rok – tak i dlouhodobý úkol – hledání vhodné úrovně finančních prostředků s ohledem na celkový rozpočet MU.
– Posuzování *záměrů v oblasti transformačních a rozvojových projektů* MU s celouniverzitní působností v oblasti informačních a komunikačních technologií. Předkladatelé projektů i vedení MU by tak mělo získat partnera při posuzování možného dopadu na další rozvoj univerzity u velkých a finančně náročných projektů.

Přestože Rada informačních technologií nemá žádnou rozhodovací pravomoc a pouze předkládá návrhy rektorovi, může sehrát významnou roli v dalším rozvoji MU, pokud se jí podaří vystihnout nejdůležitější trendy využitelnosti informačních technologií na rozvoj velkých univerzit. Členové Rady[1] proto nereprezentují konkrétní fakulty či ústavy (s výjimkou úřadujícího ředitele ÚVT), ale jsou významnými reprezentanty akademické obce univerzity. □

Bezpečnost v distribuovaném prostředí

Daniel Kouřil, ÚVT MU

V současných vědeckých disciplínách lze najít řadu oblastí, které se neobejdou bez ohromné výpočetní síly, kterou dnešní počítače nabízejí. Příkladem může být oblast výpočetní chemie, fyziky vysokých energií nebo biomedicíny. Některé úlohy jsou však tak rozsáhlé, že jejich řešení by na běžně používaných počítačích zabralo velmi dlouhou dobu, proto se často používají superpočítače nebo clustery, které nabízejí výrazně vyšší výkon. Protože s jídlem roste příslovečná chuť, uživatelům často nestačí ani výkon těchto systémů a hledají ještě výkonnější varianty, které by byly schopné efektivně zpracovávat jejich náročné úlohy.

Oblast náročných výpočtů dnes směřuje k budování a podpoře tzv. *Gridů*[1]. Zjednodušeně lze říci, že gridy umožňují uživatelům využít výpočetní kapacity z různých institucí a přitom uživateli vytvářejí jednotné prostředí a skrývají rozdíly mezi jednotlivými systémy. Jednotlivé systémy zapojené v gridu jsou však stále autonomní a jejich administrátoři mají nad nimi plnou kontrolu. Gridy jsou charakteristické dynamickým prostředím, kdy připojení i odpojení zdrojů je velmi dynamický proces. Stejně tak se může část gridové infrastruktury stát dočasně nedostupná, například kvůli problémům se síťovou konektivitou. Gridová infrastruktura se však snaží zajistit, aby takové dynamické změny minimálně ovlivnily práci uživatele i zpracování jeho úloh.

Takové rozsáhlé a dynamické prostředí přináší nové bezpečnostní problémy, pro které je nutné najít spolehlivá řešení. Na následujících řádcích se snažím zprostředkovat čtenáři pohled na problematiku bezpečnosti v dnešních systémech pro řešení náročných úloh, zejména s důrazem na rozsáhlé projekty, které spojují mnoho různých institucí a často přesahují území jednotlivých států, či kontinentů.

1 Autentizace

Autentizace je proces ověření identity uživatele nebo služby. Nejčastěji používanou metodou autentizace v dnešních počítačových systémech je kombinace uživatelského jména a hesla, které se

[1] K 1.dubnu 2005 pracovala Rada informačních technologií v následujícím složení: Doc. Luděk Matyska (ÚVT, FI – předseda), Prof. Josef Bejček (PrF), Doc. Ladislav Dušek (PřF, LF), Prof. Jozef Gruska (FI), Prof. Jaroslav Koča (PřF), Prof. Jiří Kroupa (FF), Prof. Ivo Možný (FSS), Doc. Václav Račanský (ÚVT).

[1] jazykové puristy odkazuji na diskusi o správném českém překladu tohoto termínu na `http://meta.cesnet.cz/cs/grid.html`

ověřuje proti nějaké databázi. Vzhledem k organizačním a geografickým vzdálenostem, ve kterých se gridové projekty realizují, ale tato metoda není vhodná. Bylo proto potřeba najít autentizační metody, které budou dostatečně jednoduché na používání, ale přitom škálovatelné a interoperabilní a které bude snadné administrovat. V gridech se proto používají technologie založené na PKI (*Public Key Infrastructure*), kdy každý uživatel a služba vlastní certifikát veřejného klíče podepsaný některou důvěryhodnou certifikační autoritou (CA). Tento certifikát spolu s odpovídajícím soukromým klíčem pak používá pro svou autentizaci. Technicky je tento mechanismus léta znám a používán, zejména v menším měřítku. V gridovém prostředí je ale potřeba stabilní produkční prostředí, které zajistí maximální interoperabilitu mezi zúčastněnými stranami. Bylo proto potřeba definovat pravidla, která musí splňovat každá certifikační autorita a mechanismy, které ověří, že tato pravidla jsou opravdu dodržována. Minimální požadavky jsou nastaveny tak, aby zajišťovaly důvěru v informace v certifikátu, zejména v to, že fyzický majitel certifikátu je skutečně osoba nebo služba v certifikátu uvedená. Mezi minimální požadavky na CA patří zejména nutnost předložení osobních dokladů žadatele při podávání žádosti o certifikát, dále tyto požadavky vyžadují, aby počítač, na kterém se provádí operace s podepisovacím klíčem CA, nebyl připojen k žádné počítačové síti, vyžadují aby všechny operace s tímto klíčem byly logovány, kladou důraz na včasné vydávání revokačních listů apod.

Velkým úspěchem gridových aktivit je vytvoření prostředí, které takovou klasifikaci certifikačních autorit umožňuje. V současné době je v každém evropském státě, který má nějakého účastníka gridových aktivit, alespoň jedna certifikační autorita, která splňuje takové minimální požadavky. V České republice máme CA[2], kterou vybudovalo a provozuje sdružení CESNET a která umožňuje všem členům české akademické obce získat certifikát uznávaný všemi významnými gridovými projekty v Evropě. Protože podobné aktivity pro definování minimálních požadavků existují i v zemích severní Ameriky a Asie, lze čekat, že v horizontu několika let bude možné použít certifikát vydaný CA CESNET pro přístup ke gridovým službám na celém světě. Zároveň je snaha přenést tyto aktivity i do prostředí, které s gridy přímo nesouvisí, příkladem může být projekt TACAR[3], který pod záštitou sdružení TERENA buduje adresář důvěryhodných evropských CA a je z velké části založen na gridových autoritách. V budoucnu by tak mělo být možné používat certifikát od CA CESNET pro přístup k řadě akademických služeb v rámci celé Evropy, později i jinde ve světě.

Každý gridový uživatel tedy má certifikát, jehož odpovídající soukromý klíč má uložen na disku a zašifrován heslem. Aby uživatel nemusel zadávat toto heslo při každém přístupu k gridovým službám, nabízí gridová infrastruktura rozšíření klasické podoby PKI formou tzv. *proxy certifikátů*. Proxy certifikát je nově vygenerovaný certifikát, který není podepsaný žádnou CA, ale uživatelovým vlastním soukromým klíčem. Tento certifikát má platnost několik málo hodin (zpravidla deset nebo dvanáct) a jeho soukromý klíč je uložen na disku nešifrovaně v souboru, který je čitelný pouze majiteli certifikátu. Uživatel tak nemusí zadávat heslo ke svému privátnímu klíči při každém použití gridu. Krátká doba platnosti proxy certifikátu snižuje riziko plynoucí z případného ukradení takového nešifrovaného certifikátu. Gridová infrastruktura také poskytuje nástroje na automatické přenášení proxy certifikátů mezi různými počítači v sítí, které uživatel nebo jeho úloha pravě používá. Tato technika se obecně označuje jako princip *single sign-on* a umožňuje, aby se uživatel do gridu přihlásil pouze jednou a pak již po určitou dobu nemusel explicitně zadávat své autentizační údaje, protože lokální systém si jeho identitu pamatuje a umí ji použít transparentně. Výrazně se tím usnadňuje použití gridu a zvyšuje to i bezpečnost uživatelova certifikátu, protože se téměř po celou dobu pracuje pouze s krátkodobým proxy certifikátem.

Vedle PKI podporují gridy i jiné autentizační metody. Existuje například služba, která umožňuje integrovat PKI infrastrukturu s prostředím, kde

[2] `http://www.cesnet.cz/pki/`

[3] `http://www.terena.nl/tech/task-forces/tf-aace/tacar/`

je používán autentizační mechanismus Kerberos. Tato služba generuje certifikáty na základě kerberovských lístků a umožňuje tak snadnější připojení uživatelům z organizací, které používají Kerberos. Dalším trendem současné gridové bezpečnosti je zavádění jednorázových hesel, tj. hesel, která lze použít pro jedinou autentizaci.

2 Autorizace

Autorizace je proces, ve kterém služba ověřuje, že autentizovaný klient má oprávnění použít danou službu. Na rozdíl od oblasti autentizace, kde gridová infrastruktura od počátku stavěla na dostupných technologiích, se gridové autorizační služby začaly budovat na zelené louce. Žádná z dostupných autorizačních metod totiž neposkytovala funkcionalitu, která je pro gridy požadována. Jako příklad lze uvést autorizaci založenou na adresářové službě LDAP, která je hojně využívaná, zejména v organizačně uzavřených prostředích (např. v rámci jedné univerzity). V LDAPu lze definovat skupiny uživatelů, kteří mají právo použít určitou službu. Tato služba při každém přístupu klienta nejprve zjistí, zda klient je uveden v příslušné skupině a rozhodne tak, zda klientovi službu poskytne či ne. Tento způsob je jednoduchý a dobře funguje v relativně malém prostředí, postrádá však např. mechanismus delegování práv, kdy by uživatel mohl předat část svých oprávnění jinému uživateli (např. kolegovi, který by chtěl zpracovat data, která jsou čitelná pouze jejich majiteli), vyžaduje časté dotazy na LDAP server a není dostatečně škálovatelný.

Proto vznikly a stále se vyvíjejí sofistikované gridové autorizační služby, které poskytují efektivnější nástroje pro řešení autorizační problematiky v oblasti gridů. Řada těchto služeb poskytuje funkcionalitu vypůjčenou ze světa PKI, kdy každý projekt spravuje jeden nebo více tzv. *atributových serverů* vydávající uživatelům atributové certifikáty, kde je zapsáno členství uživatele ve skupinách, případně přímo aktuální role uživatele. Uživatel s administrátorskými právy tak může pracovat se svou běžnou identitou a oprávněním a pouze pro úkony související se správou použít administrátorský certifikát. Snižuje se tak riziko zneužití nebo chyby, kterou uživatel může udělat. Atributový certifikát je podepsán službou, která jej vydala a koncový server nemusí kontaktovat žádnou třetí službu, jen ověří podpis na atributovém certifikátu a zkontroluje příslušné atributy. Klient posílá svůj atributový certifikát jako součást autentizačního procesu, zpravidla je zakódován v uživatelově proxy certifikátu, takže nejsou potřeba ani žádné změny na úrovni komunikačního protokolu. Takové prostředí umožňuje flexibilní správu uživatelských oprávnění, uživatel si může vybrat jaké skupiny nebo role z přiřazených právě potřebuje pro svou práci. Příslušné atributové certifikáty lze často také delegovat i jiným uživatelům, kteří tak mohou používat služby, ke kterým má přístup původní uživatel. Tyto delegační certifikáty jsou zpravidla časově omezené.

V gridovém prostředí bývá také problém vůbec zapsat přístupovou politiku, protože faktorů, které ji ovlivňují, může být velmi mnoho a jsou velmi různorodé. Často nelze vystačit s jednoduchým statickým seznamem uživatelů, příp. skupin, který je zapsán v konfiguraci služby, ale výsledná přístupová politika je výsledkem vyhodnocení řady dílčích pravidel. Například vedoucí gridového projektu může definovat skupinu uživatelů, kteří mohou používat výpočetní prostředky přiřazené tomuto projektu, ale lokální správci těchto prostředků mohou definovat vlastní přístupovou politiku, která musí být vyhodnocena též. Častým příkladem může být situace, kdy lokální správce chce preferovat uživatele pocházející z lokální instituce před ostatními, kterým je přístup povolen pouze v okamžiku, kdy výpočetní prostředky nejsou zatížené. Takových pravidel může být celá řada, mohou být definovány na více místech a vyhodnocování přístupové politiky pak může být velmi složitý proces. Tyto problémy vyústily v definování jazyků založených na XML, které umožňují standardizovaným způsobem zapsat i složité přístupové politiky a rovněž nabízejí nástroje pro efektivní zpracování těchto pravidel.

V oblasti autorizace se gridový svět snaží přiblížit a využít výsledků, které jsou dostupné v oblasti webových služeb (*Web services*). Zejména zmíněné zpracování pravidel pro řízení přístupu

je založeno na výsledcích z oblasti webových služeb a standardů, které odtud pocházejí.

Současná gridová řešení se v maximální míře snaží podporovat interoperabilitu mezi různými organizacemi. V oblasti autorizace se proto zkoumají přístupy, které jsou schopné využít autorizační mechanismy z různých institucí, pokud možno bez zásahu uživatele tak, aby uživatel mohl volně využívat různé služby nabízené různými organizacemi a přitom zůstalo zachováno požadované zabezpečení a princip single sign-on.

Tento přístup je velmi dobře využitelný i mimo gridové prostředí, jak ukazuje například projekt Shibboleth[4], který vznikl pro podporu digitálních knihoven a má řadu faktorů společných s gridovou problematikou. Shibboleth je orientován na prostředí webu a umožňuje, aby uživatel, který přistupuje k webovému serveru, byl autorizován pomocí informací, které jsou spravovány jeho domovskou institucí. Umožňuje tak, aby uživatel přistupoval k elektronickým zdrojům odkudkoliv bez potřeby dodatečného hesla. Organizace tak například nemusejí nutit uživatele, aby používali proxy servery pro přístup k digitálním knihovnám, ale uživatel může přímo přistupovat k serveru knihovny, který jménem uživatele kontaktuje uživatelův „domovský“ autorizační server a je schopný převzít a zpracovat výsledek autorizačního procesu. Z pohledu uživatele je důležité, že celý proces je maximálně transparentní. Vzhledem k podobným cílům, které Shibboleth a gridy mají, vznikl nový projekt GridShib, který se snaží o větší propojení gridů a principů, na kterých je Shibboleth založen.

3 A co uživatel?

Cílem systémových správců by měl vždy být spokojený uživatel, pro bezpečnost to platí dvojnásob. Bezpečné totiž nemusí znamenat uživatelsky složité, naopak systém by měl být od počátku navržen tak, aby umožňoval snadné použití ze strany uživatelů. Průzkumy ukazují, že bezpečnostní incidenty jsou z velké části zapříčiněny uživateli a jejich nesprávným chováním, nikoliv problémy v infrastruktuře. Systém může používat i sofistikované bezpečnostní mechanismy, ale pokud uživatel nebude dostatečně opatrovat své autentizační údaje, bude celkově systém daleko zranitelnější.

Pokud například uživatel používá několik příbuzných webových stránek, kam je přístup chráněn různými hesly, velmi pravděpodobně uloží tato hesla do každého klienta, kterého použije, přes veškerá varování, že tak nemá činit. Pokud však tyto webové stránky budou podporovat princip single sign-on, kdy uživatel zadá heslo jen jednou a infrastruktura v pozadí zajistí, že jeho identifikace se bude předávat transparentně bez nutnosti opakovaného zadávání hesla, je pravděpodobné, že patřičně poučený uživatel heslo opravdu napíše pokaždé z klávesnice.

Pokud se taková infrastruktura navíc propojí i s newebovým prostředím, např. pomocí gridových technologií a uživatel tak skutečně bude své heslo zadávat pouze jednou za den, výrazně se tak zvýší nejen pohodlí uživatelů, ale zejména bezpečnost celého systému. Vybudování takového systému sice stojí více úsilí, ale vrátí se ve vyšší úrovni bezpečnosti a uživatelského pohodlí. Jedním z podstatných cílů gridových technologií je poskytnout nástroje pro vybudování takového prostředí.

Dalším problémem, který přímo souvisí s gridy, je správa soukromých klíčů uživatelů. Zatímco jméno a heslo si je každý uživatel schopen zapamatovat, privátní klíč o velikosti 1024 bitů si nezapamatuje nikdo. Musí být proto uložen na nějakém médiu, nejčastěji disku uživatelské stanice. To přináší riziko jeho prozrazení, zejména v dnešní době, kdy je k Internetu připojena řada počítačů, které nejsou aktualizovány, případně jsou napadeny nejrůznějšími viry, a soukromý klíč se tak může dostat do nepovolaných rukou útočníka. Současné gridy se proto snaží nabídnout řešení, které uživatelům umožní uložit svůj soukromý klíč na specializovaný server, který uživatelům vydává pouze krátkodobé proxy certifikáty. Přestože takový server obsahuje klíče řady uživatelů, což je v přímém rozporu s klasickým pohledem na PKI, ukazuje se, že je to bez-

[4] http://shibboleth.internet2.edu/

pečnější řešení, než ponechávat klíče u uživatelů, kteří o jejich zabezpečení nemají vědomosti či zájem. Další možností, která umožňuje odstranění uživatelského klíče je použití čipových karet, které se postupně začínají v gridovém prostředí prosazovat.

4 Síťová kontrola aneb firewall

Slovo firewall je zaklínadlem, které se objevuje snad v každém článku o bezpečnosti, a proto mu nemůžeme nevěnovat aspoň krátkou zmínku ani zde. Firewallem máme na mysli zařízení umístěné mezi komunikujícími stranami, které monitoruje síťovou komunikaci a je schopno tuto komunikaci ovlivnit. Nejčastěji se tento prostředek používá pro izolování lokální sítě tak, aby např. lokální počítače nebyly dostupné z Internetu.

Firewall je často považován za synonymum pro zabezpečenou síť a bývá také automaticky doporučován téměř jako všelék na veškeré problémy s bezpečností. Zkušenosti z gridového prostředí však ukazují, že firewally nezřídka přinášejí více problémů než užitku, a proto by jejich nasazení mělo být vždy velmi pečlivě uváženo. Firewally zpravidla implementují politiku „co není povoleno je zakázáno“ která je však velmi nepřirozená pro gridové prostředí, protože povolení každé nové služby je dlouhotrvající proces, který špatně zapadá do dynamického gridového světa.

Řada gridových projektů dnes spravuje různé seznamy portů a IP adres, které musí být povoleny v konfiguracích firewallů, aby bylo možné vybudovat a udržet funkční infrastrukturu. Přestože definují minimální požadovanou funkcionalitu, jsou tyto seznamy zpravidla tak rozsáhlé, že v podstatě stírají význam firewallu. Stačí také drobná opomenutí v konfiguraci pro částečné, či úplné vyřazení určité funkcionality.

Firewally by proto měly být nasazovány jen v situacích, kdy opravdu mohou přinést zvýšení bezpečnosti i v reálném provozu a co nejméně omezovat legitimní uživatele. O to více úsilí by mělo být věnováno zabezpečení služeb samotných, než omezování přístupu k nim. □

Zavolej mi ...

Stanislav Kala, ÚVT MU

Na telefonování po místních pobočkách v rámci celé Masarykovy univerzity jsme si už zvykli. Pominulo zdlouhavé hledání příslušné fakulty ve Zlatých stránkách a většinou i následné přepojování na příslušnou osobu někde z vrátnice. I volání z venku je podstatně jednodušší. Budování hlasové sítě MU bylo dokončeno a nastala další fáze: běžný provoz, užívání a vylepšování. Je proto vhodné zmínit se o některých zkušenostech, doporučeních a dalších záměrech při využívání hlasové sítě MU. V minulém čísle Zpravodaje bylo popsáno Spojovací a informační centrum MU [1]. Tentokrát se zaměříme více na technickou stránku hlasových služeb.

Jsme připojeni na několik operátorů

Technické řešení hlasové sítě MU umožnilo zrušit a odhlásit jednotlivá připojení ústředen na staré kabely Českého Telecomu po celém městě, omezit tím paušální poplatky a soustředit se na ekonomickou výhodnost každé přípojky v daném období. Původní zůstaly pouze telefonní linky u malých lokalit a také ty, které jsou nutné pro zabezpečení objektů, nouzová volání apod. Významně se tím zlepšila pozice Masarykovy univerzity při každém výběru majoritního operátora na příští období (jedenkrát ročně) a při uzavírání smluv o cenách hovorů. Myslím, že tohoto výsledku už si povšimla většina uživatelů na svém telefonním účtu.

Dnes jsme optickými kabely přímo propojeni s těmito telefonními operátory:

- GTS – v současnosti náš *majoritní operátor*, na kterého jsme přenesli naše číslo 54949xxxx
- Cesnet – využívaný hlavně pro bezplatná volání v rámci akademických institucí
- Eurotel – přímé připojení do sítě GSM přes naše číslo 72749xxxx
- T-Mobile – přímé připojení do sítě GSM přes naše číslo 73609xxxx

I další operátoři nám nabízeli své služby se stejným rozhraním a ve stejném místě a jsou připraveni pro příští výběrová řízení. K čemu nám

může být znalost o připojovacích číslech jednotlivých operátorů užitečná, se dozvíme níže v tomto textu.

Směrování hovorů

V prvním období provozu nové telefonní ústředny bylo dodavatelem technologie doporučeno využít zkušeností několika jiných vysokých škol, včetně VUT Brno, a nastavit směr volání přes IP technologii prostřednictvím Cesnetu přímou volbou směru **0*8**. Tuto možnost volby operátora jsme sice nastavenou nechali, VUT ji používá stále, ale následným rozborem statistik jsme zjistili, že tato volba není využívána dostatečně. Je jasné, že není v silách každého uživatele, aby se při své práci podstatně odlišného charakteru ještě zajímal o to, zda cenový vývoj hovorného zrovna někam nepokročil. Proto jsme se rozhodli nechat ruční volbu směru jen jako nouzovou a všechny hovory směrovat na nejvhodnějšího operátora *automaticky*.

Ať vytočíte jakékoliv telefonní číslo, buďte ujištěni, že už se někdo zamýšlel nad ekonomickou i kvalitativní výhodností směru, kterým bude hovor vyslán z naší ústředny. Směr nebo přesněji směrování odchozích hovorů na bránu příslušného operátora je voleno obvykle podle nejnižších cen. Rozlišení cíle volání je dáno prvními číslicemi, které říkají, zda voláte město, meziměsto, a podobně (2 Praha, 602 Eurotel). Tato čísla jsou vypsána ve směrové tabulce telefonní ústředny, a jsou stále aktualizována. Malá akademická pracoviště mohou mít třeba jen jednu nebo dvě linky přes Cesnet za nulovou cenu hovorného. Proto jsou do směrové tabulky zahrnuta i jednotlivá konkrétní telefonní čísla podle seznamu, který nám dává Cesnet k dispozici.

Dnes je cenově například výhodnější směrovat hovory do Prahy přes Cesnet a na Středočeský kraj přes GTS, zítra to může být opačně. Toto stálé porovnávání a nastavování platí jak pro místní či meziměstské, tak i pro mezinárodní volání.

I přesto se může stát, že chcete pro svůj hovor zvolit jiného operátora, než jakého by zvolila ústředna MU. Stává se to například u faxů do zahraničí. Zahraniční volání bývá nejlevnější s využitím IP telefonie, kterou pro nás zprostředkovává Cesnet. Je tak proto nastaveno i implicitní směrování. Jenže komunikační protokoly a časová zpoždění v každém směru, nebo také vzájemná konverze protokolů na rozhraní různých prostředí nebo států, mohou vyhovovat srozumitelnosti mluveného slova, ale nemusí již být vhodné pro fax[1]. Buď časové zpoždění způsobí, že váš fax naváže spojení, přenese zprávu, ta je přijata, ale potvrzení už nedojde (a vy pro ohlášený „error“ posíláte zprávu zbytečně znovu a znovu), nebo, což je častější, se prostě faxy nespojí. Pro tento případ lze použít předvolbu **0*7**, kterou hovor nebo žádost o faxové spojení nasměrujete přes majoritního operátora, bez ohledu na cenu. Tradiční operátoři s použitím klasické telefonní technologie podporují faxový přenos zpráv při všech používaných rychlostech přenosu.

Je ještě jedna možnost volby odchodu na operátora, kterou má uživatel. Je to především u soukromých hovorů. Buď spojení prostě vytočíte a označíte jedním z možných způsobů uvedených na `http://www.ics.muni.cz/services/phones/shovorne.html` – a o směru odchodu vašeho hovoru rozhodne nejnižší cena; hovor pak uhradíte Masarykově univerzitě. Nebo máte druhou možnost, předplatitelskou *Kartu X* u vámi zvoleného operátora. Karta X má své vlastní číslo předvolby a tím je vlastně zvolený operátor vybrán a jemu také platíte.

Přenos informace o číslu

Tuto službu nejdříve nabídli operátoři sítí mobilních telefonů GSM. U pevných linek to ještě dlouho nebyla taková samozřejmost. Teprve technologie ISDN (Integrated Service Digital Network) přinesla možnost přidat k hovoru na pevných linkách další doplňující informace. Mimo čísla volaného a volajícího jsou to ještě časové a tarifikační údaje.[2]

[1] Částečně se touto problematikou zabýval článek [2]

[2] Aby mohl uživatel tyto nové možnosti vidět a využívat, musí mít k dispozici telefonní přístroj, který danou funkcionalitu podporuje. Protože v ČR nebyl nikdy velký tlak na masivní výměnu původních telefonů (i ty staré stále

Telefonní ústředna MU je s operátory propojena několika PRI (Primary Rate Interface) toky vždy s 30 linkami (ISDN30), a samozřejmě dostává číslo volajícího i odesílá své při volání ven. Bylo by to prosté, kdyby v tom nebyla nějaká klička. Volaný vlastně uvidí číslo, které máme u příslušného operátora a to ještě v případě, že je to desetitisícová série. Nejlépe si to ukážeme na příkladu. Předpokládejme, že volám z pobočky MU *2114* některému účastníkovi mimo MU:

- zavolám-li kohokoliv v Brně, on uvidí, že ho volá číslo **54949***2114*. Volal jsem totiž přes majoritního operátora GTS. Volaný účastník se vytočením tohoto čísla dovolá zpět na mou pobočku na MU;
- zavolám-li někoho v Praze, uvidí volaný číslo +420234680111 a zpět na MU se tímto číslem nedovolá. Zobrazené číslo je totiž číslo brány Cesnetu v Praze, a to je stejné pro celý akademický svět v této oblasti. Nelze prostě tolik institucí obsloužit tak, aby dostal každý svých 10 000 možných čísel. Při volání zpět musí volaný vytočit **54949***2114*. Je to bohužel daň za příznivější ceny hovorů;
- zavolám-li 602123456, což je číslo Eurotelu, na displeji volaného mobilu se objeví **72749***2114*. Volal jsem totiž přímo přes pevné připojení Eurotelu. Volání zpět funguje, volaný se dovolá zpět na stejný telefon *2114*. Prakticky totéž platí i pro T-mobil, jen se volanému ukáže **73609***2114* a tímto číslem se zpět dovolá;
- zbývá ještě uvést, že Český mobil přímé připojení na ústřednu MU nemá, voláním na telefon v síti Oskar je odesláno číslo **54949***2114* a tímto se volaný dovolá zpět stejnou cestou.

V obráceném směru je situace jednodušší. Číslo volajícího zvenčí dostaneme na svůj telefon na MU správně (za předpokladu, že náš konkrétní telefonní přístroj přenos informací o čísle podporuje), jen může být ve formátu 511 111 111 nebo mezinárodním 00420 511 111 111 – podle nastavení u daného operátora. Pokud nevolá někdo ze zahraničí, je informace, dá se říci, rovnocenná.

splňují základní funkci – možnost se dovolat), většina telefonních účastníků u nás si tyto možnosti neuvědomuje a zatím je nevyužívá.

Další využití čísla, kterým se volající prezentuje, je spíše otázka našeho vybavení. Digitální telefon s displejem číslo ukáže. Jenže je „hloupý“ a drahý. Veškerá jeho chytrost je v ústředně a obrovskou škálu jeho možností a služeb snižuje částečně to, že výběr a nastavení funkcí musí dělat centrálně technik a pro uživatele zůstává prakticky možnost jen některou z přednastavených funkcí vypnout nebo zapnout.

IP telefon, tj. telefon volající po datové síti, číslo volajícího ukazuje a u většiny typů se dá s tímto číslem dále pracovat. Ukládat do seznamu, pojmenovat a ze seznamu vytáčet. Nasazení IP telefonů však vyžaduje další speciální nastavení a úpravy na datové síti, proto je používáme jen v nezbytných případech, kde není ekonomicky výhodné budovat klasickou telefonní ústřednu.

Poměrně dobře – v poměru ceny a užitné hodnoty – jsou na tom telefony se službou *CallerID*, čili identifikací volaného. Český Telecom tuto službu ve své síti nazývá „CLIP“. Informace o čísle volajícího nebo číslo a jméno pobočky se na displej telefonu přenáší mezi prvním a druhým zazvoněním. Telefony obvykle umí spárovat číslo se záznamem v seznamu osob a dokážou volajícího pojmenovat. Zpětné vytočení zobrazeného čísla bývá otázkou jednoho nebo dvou stisknutí tlačítka. Pouze nulu, která se při volání z venku neukazuje, musíte před hovor vložit ručně. Někdy je dokonce lepší mít takový telefon než hlasovou schránku, protože i u zmeškaných hovorů je zaznamenán čas a číslo volajícího přímo na telefonu a naopak u hlasové schránky bývá velmi často zaznamenáno jen anonymní položení sluchátka, ke kterému se navíc dost pracně dostáváte. Zaznamenané číslo můžete pochopit stejně jako vzkaz na záznamníku s tímto oznámením: „*Zavolej mi na toto číslo . . .*“.

Telefonů CallerID je na trhu celá řada a jejich cena bývá do 1000 Kč. Bohužel tato vymoženost je zatím odepřena účastníkům Ekonomicko správní fakulty na Lipové a většině pracovníků Přírodovědecké fakulty na Kotlářské. V těchto lokalitách byly totiž do nového systému hlasových služeb MU zařazeny původní ústředny, které tuto službu ještě nepodporovaly.

Poslední možnost, jak se na MU dozvědět číslo volajícího, je na osobním účtu

na webu `https://inet.muni.cz/app/telef/tarifikace/osoba`. Informace o uskutečněných hovorech jsou pravidelně přenášeny do serveru Inetu. U každého uskutečněného hovoru se eviduje čas, délka hovoru, číslo volaného a volajícího a nejprve předběžná, po přepočítání nákladů pak konečná cena hovoru, viz [3]. V tabulce na webu se, na rozdíl od CallerID telefonu, neobjevují zmeškané hovory. Zato je tam velice přehledně nastřádána určitá historie a také možnost si jednou použitá čísla pojmenovat a ušetřit si tak někdy opětovné hledání v seznamech.

Jméno volajícího

Spolu s přenášeným číslem volajícího se v rámci hlasové sítě Masarykovy univerzity přenáší i jméno. Do údajů o každé pobočce MU je správcem telefonní ústředny zapsán text 27 znaků bez diakritiky. Digitální telefony mají možnost seznam jmen prohledávat a volat pobočku podle vyťukaných prvních písmen jména. Aby bylo možné tuto funkci efektivně využívat, byla na MU pro zápis jmen nebo názvů poboček stanovena určitá pravidla. Pokud je pobočka registrována na osobu, je údaj zapsán ve formátu: `PRIJMENI,Jmeno Fak`. Fakultu na konci je důležité psát zejména u učeben, vrátnic a laboratoří, které se jinak jmenují téměř stejně na celé univerzitě.

Jméno pobočky se přenáší, jak už bylo zmíněno výše, na digitální telefony, ale také na IP telefony a analogové CallerID přístroje. Ne každý telefon však umí zobrazit všech 27 znaků, některé třeba jen 15. I to je třeba brát v úvahu při popisu a začínat tak vždy nejdůležitějším údajem. Šíření jména volajícího mimo MU je vypnuto.

Literatura

[1] Z. Malčík. Spojovací a informační centrum MU. Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. 15, č. 3, s. 4–6.

[2] V. Lorenc. Dovolali jste se na číslo 10.0.1.12 .... Zpravodaj ÚVT MU. ISSN 212-0901, 2004, roč. 14, č. 4, s. 5–9.

[3] J. Ocelka, J. Kotrba. Budování hlasové sítě MU: podpora telefonie v informačních systémech. Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč. 14, č. 4, s. 1–5. □

Pasportizace budov a místností MU

Petr Glos, ÚVT MU

1 Úvod

V roce 2004 proběhla na Masarykově univerzitě pasportizace budov a místností, přesněji řečeno byl aktualizován stavební a technologický pasport budov a místností (dále jen pasport). Pasportizační týmy firmy IB Structure a.s. zaměřily místnosti budov MU a pořídily jejich popisné atributy. Výsledkem provedených prací je popisná a grafická část pasportu včetně metodik použitých při jeho pořízení.

1.1 Popisná část pasportu

Popisná část pasportu obsahuje následující *údaje o jednotlivých budovách* (uložené v textových souborech):

- základní stavební informace – identifikace budovy, adresa, počet podlaží, aj.
- rozšířené stavební informace – údaje o konstrukci budovy, aj.
- základní a rozšířené technologické informace – údaje o zásobování palivy a energiemi, vytápění, klimatizaci, aj.

Součástí popisné části jsou dále informace o jednotlivých *místnostech a budovách* uložené v `xls` souborech:

- identifikační údaje budov – kód číselníku budov a místností MU, polohový kód
- identifikační údaje místností – kód číselníku budov a místností MU, polohový kód, označení místnosti, její účel a typizace, a další
- technické údaje místností – plocha, výška, typ a plocha podlahové krytiny, počty dveří, oken, údaje o površích stěn a stropů, aj.

1.2 Grafická část pasportu

Grafická část pasportu obsahuje výkresy ve formátu `dwg` (obecně uznávaný standard pro elektronickou výkresovou dokumentaci) pro jednotlivá *podlaží budov* a jsou v ní zakresleny:

- půdorysy místností a stavebních konstrukcí (nosných stěn, příček, schodišť,..)
- okna a dveře v místnostech.

Další součástí grafické části pasportu jsou dwg výkresy znázorňující:

- pohledy na budovy
- řezy budovami.

2 Pasport a EIS

Pozorný čtenář jistě nepřehlédl zmínku o stávajícím číselníku budov a místností Ekonomického informačního systému MU (EIS) v článku J.Haluzové a Z.Machače o elektronické podpoře evidence majetku MU v tomto čísle Zpravodaje. Od počátku prací na aktualizaci pasportu byl kladen maximální důraz na integraci tohoto číselníku používaného na veřejných www stránkách MU (viz např. http://wwwdata.muni.cz/misc/address_list.asp), i v ekonomických (viz např. https://inet.muni.cz/app/majetek/prehbudov) a mapových aplikacích MU (viz např. https://maps.muni.cz/ArealyBudovyMU). V současné době probíhá převod a verifikace části popisných dat do databázových struktur napojených na zmíněné číselníky. Za touto nenápadnou větou je ukryto nemalé a často téměř detektivní úsilí pracovníků oddělení EIS ÚVT při pátraní, které dvě místnosti (z pasportu a číselníku) jsou vlastně tou stejnou (místností).

Výsledkem integračního úsilí bude databáze budov a místností ve vlastnictví MU, která bude poskytovat data pro aplikace realizující zpřístupnění a aktualizaci dat pasportu, a bude propojená s geografickou databází budov a místností. Tuto databázi budeme samozřejmě dále rozšiřovat podle aktuálních potřeb uživatelů (například pro aplikace typu facility management – o tom ale jindy).

3 Pasport a GIS

Grafika pasportu obsahuje i vybrané identifikační a technické údaje budov a místností dostupné při prohlížení jednotlivých elektronických výkresů. Pro oprávněné uživatele jsou výkresy budov zpřístupněny prostřednictvím aplikace GIS (geografické informační systémy) na terminálovém serveru tsbaps.ics.muni.cz – uživatelé tedy nemusejí na svých počítačích instalovat žádné další programové vybavení.

Navigační část aplikace umožňuje vybrat požadovanou budovu pomocí výběru z číselníku, zadáním adresy nebo vyhledáním půdorysu budovy na mapovém podkladu orientačního plánu města Brna, jak jej známe v tištěné podobě, či nad ortofotomapou města (ortofotomapa je speciálně upravený kolmý letecký snímek zemského povrchu). Pro mimobrněnské budovy lze k navigaci využít přehlednou mapu České republiky a ortofotomapy okolí Telče a Cikháje. Navigační část aplikace je v podstatě totožná s aplikací pro vyhledávání a zobrazování půdorysů budov MU https://maps.muni.cz/ArealyBudovyMU. Pro realizaci navigační části aplikace je využito programové vybavení firmy ESRI, a to ArcSDE pro správu prostorových dat v relační databázi a ArcIMS pro publikaci prostorových dat v prostředí WWW.

Po výběru hledané budovy je spuštěna část aplikace pro prohlížení a tisk grafiky již konkrétní budovy. Symbolika jednotlivých grafických prvků odpovídá předaným dwg výkresům a je přístupná v legendě. Uživatel si může zobrazovat jednotlivá podlaží budov, zvětšovat výkresy půdorysů jednotlivých podlažích, nastavovat přesná měřítka pro zobrazení a tisky, vypínat a zapínat zobrazení jednotlivých skupin prvků ve výkresech (čarová kresba, popisky, kóty,...). Jednotlivé místnosti lze vyhledávat podle polohového kódu či podle jejich skutečné polohy v rámci budovy. Pro tiskové výstupy může uživatel použít tiskárny, které má připojeny ke své pracovní stanici. Pro realizaci této části aplikace slouží ArcReader firmy ESRI, bezplatný prohlížeč mapových kompozic připravených v prostředí ArcGIS.

Uvedené řešení pro zpřístupnění grafické části dat pasportu si nevyžádalo žádné finanční prostředky na pořízení software a hardware, bylo využito stávajícího programového a technického vybavení. Jsme si plně vědomi, že se jedná o první, či spíše nultou verzi řešení a očekáváme, že bude podrobena tvrdé a konstruktivní kritice z řad uživatelů.

4 Co dál

V dalším období plánujeme integraci uvedené grafické části pasportu s atributovou (databázo-

vou) částí pasportu a to v souvislosti s převedením grafické části do databáze. Tomuto převodu bude předcházet *rektifikace výkresů* pasportu – jejich umístění do správné polohy v prostoru tak, aby i například půdorysy jednotlivých místností v různých podlažích téže budovy opravdu ležely nad sebou. Správná poloha budov a místností bude důležitá i pro další aplikace – např. v IS BAPS bude možno zakreslovat reálnou polohu kabelů i uvnitř budov. Neméně důležitá bude správná poloha budov a místností i při další etapě pasportizace budov, tentokrát s důrazem na *technologický pasport* – rozvody energií, zásobování teplem, klimatizace, vzduchotechnika. □

Elektronická podpora evidence majetku na MU v Brně

Jana Haluzová, Zdeněk Machač, ÚVT MU

1 Něco málo z historie

Informační podpora evidence majetku na MU prošla za dobu své existence několika technologickými etapami. Do roku 1990 se evidence majetku vedla centrálně na tehdejším sálovém počítači EC. Od roku 1991 se postupně data předávala jednotlivým součástem univerzity (hospodářským střediskům, tj. fakultám a celouniverzitním pracovištím) a jejich pracovištím, kde se zpracovávala pomocí SW vytvořeného na MU (technologie Foxpro). Data majetku pro účetní evidenci byla vedena na každém hospodářském středisku centrálně, ale operativní evidence (umístění majetku) byla distribuována na jednotlivá pracoviště (katedry). Celkem tedy bylo na MU asi 150 instalací tohoto SW. Aby byl obrázek pestřejší, přešlo později SKM na lokální SW externího dodavatele (technologie Clipper).

V roce 2002 byl zprovozněn modul *Majetek* grafické verze Ekonomického informačního systému firmy Magion (EIS Magion v technologii Power Builder). V témže roce byl do centrální databáze přenesen investiční majetek a v roce 2004 se k němu přidal majetek drobný. Údaje o majetku jsou v současné době z centrální databáze přístupné jednak ekonomickému systému EIS Magion a dále SW vytvořenému v ÚVT – Inetu MU (technologie Java). V další části textu se podrobněji zaměříme na proběhnuté konverze, stav elektronické podpory evidence majetku dnes a výhledy a plány do budoucna.

2 Konverze dat majetku v roce 2004

Jak již bylo řečeno, byla v loňském roce převedena veškerá data drobného majetku uložená v lokálních evidencích do společné centrální databáze MU. Konverze se týkala centrálních databází všech hospodářských středisek (13 instalací SW) a lokálních databází vybraných pracovišť velkých fakult. K investičnímu majetku asi v počtu 15 000 záznamů se postupně přidávaly záznamy neinvestičního majetku v celkovém počtu asi 160 000 kusů. Akce byla náročná jak ze strany fakult, které musely data majetku k danému dni srovnat s účetními záznamy, tak pro ekonomy rektorátu, kteří akci řídili metodicky, a v neposlední řadě také pro ÚVT, který akci zajišťoval pomocí svých vlastních aplikací a skriptů s mnoha kontrolními prvky a výstupy. Při nesrovnalostech s účetnictvím se musela zdrojová data ekonomy upravit (hledaly se nesrovnalosti i u jednotlivých kusů majetku) a konverze provádět opakovaně. U vybraných pracovišť s majetkem nad 400 záznamů (přes 50 instalací) se k převedeným datům navíc přenášely údaje o umístění, tj. identifikace místnosti (kde je majetek fyzicky umístěn) a označení osoby (jíž je majetek svěřen do užívání).

Z velké většiny se nejednalo o údaje svázané s celouniverzitními číselníky, proto vzápětí po přenesení dat do centrální databáze nastala pro referenty majetku a ÚVT další náročná část konverze – změna umístění ze starých popisných údajů na údaje z celouniverzitních číselníků, tj. číselníku budov a místností a číselníku osob. Pro potřeby inventarizace byl číselník budov a místností pročišťován a rozšiřován o chybějící místnosti a zejména o budovy (a místnosti v nich) nepatřící do vlastnictví MU (budovy nemocnic a jiné cizí budovy, jež MU užívá). Po konverzi mohla fakulta (hospodářské středisko) začít vkládat nové majetky již do centrální databáze a tam s nimi dále pracovat prostřednictvím EIS Magion.

Pro referenty majetku na pracovištích byla vytvořena sada aplikací na univerzitním intranetu Inet a v průběhu června až srpna 2004 proběhl cyklus 15 pravidelných školení, v nichž 3 pracovníci ÚVT proškolili více než 150 pracovnic a pracovníků (většinou sekretářek kateder ve funkci referentek majetku) v používání těchto aplikací.

Termínem dokončení všech činností týkajících se konverzí byla fyzická inventura majetku k 30.9.2004. Úkol byl splněn a inventura byla provedena již z centrální databáze.

3 Současný stav evidence majetku

Správa majetku se skládá z účetní a operativní evidence. Referenti majetku hospodářských středisek (pracovníci děkanátů fakult) zajišťují účetní i operativní evidenci s pomocí programového vybavení EIS Magion („těžký klient“). Provozováno je na terminálových serverech Rumbur1 a Rumbur2, které jsou v loadbalancingovém zapojení pro vyrovnávání zátěže, testovací verze je na serveru Cvibur. Zde se s majetkem provádějí účetní operace, jako je zařazení a vyřazení majetku, jeho přesuny v rámci pracovišť a účetní i daňové odpisy u investičního majetku. K operativní evidenci, kterou zajišťují zejména referenti pracovišť (vesměs kateder) a také koncoví uživatelé (vedoucí pracovišť a jednotliví zaměstnanci MU), slouží programové vybavení realizované v rámci Inetu MU, běžící nyní na serveru Oberon. Inet je vlastnictvím univerzity, je dostupný na adrese `https://inet.muni.cz/` a jeho tvůrci jsou pracovníci Ústavu výpočetní techniky.

Majetkové aplikace jsou přístupné prostřednictvím webového klienta („tenký klient“) v sekci *Ekonomika MU* v podsekci *Evidence majetku* (internetová adresa je `https://inet.muni.cz/app/index.jsp?id=ekon.majetek`). V této podsekci jsou jednak aplikace určené všem, kdo mají do Inetu přístup, a také aplikace pro oprávněné uživatele. Do první skupiny patří aplikace:

- *Přehled práv referentů majetku* – seznam majetkových referentů za jednotlivá pracoviště, na něž se mohou zaměstnanci obracet při problémech
- *Přehledy budov a místností MU* – seznam všech budov a místností z číselníku univerzity
- *Osobní přehled majetku* – přehled majetků svěřených přihlášenému uživateli.

Do druhé skupiny patří čtyři aplikace:

- *Přehledy majetku MU* poskytují základní přehledy určené pouze k prohlížení na obrazovce a jsou přístupné referentům majetku a vedoucím pracovišť. Majetky lze seskupovat podle místností nebo osob.
- Podobně aplikace *Tiskové sestavy majetku MU* vytváří stejné sestavy, ale výsledek je ve formátu PDF a je připraven k tisku.
- *Přidělování práv referentům majetku*, jak název napovídá, slouží majetkovým referentům na děkanátech fakult pro přidělování a odebírání práv ke správě majetků vybraným osobám na katedrách.
- Nejsložitější a jedinou aplikací, která může data majetku měnit, je *Změna osob a místností majetku*. V ní lze vyhledávat majetky dle různých kritérií a nad vybranými majetky provádět neúčetní operace, jako je změna osoby, místnosti a vybraných technických parametrů (v současné době výrobní číslo, následovat budou rozměry, poznámky aj.), tisknout návrhy na vyřazení nebo převody majetku (opět ve formátu PDF).

Za účelem efektivního využívání aplikačního serveru byla implementována fronta požadavků na generování PDF dokumentů (a dalších déle trvajících úloh). Požadavky nejsou tedy vyřizovány souběžně, ale postupně, a po dokončení je výsledek na serveru k dispozici po nejméně 24 hodin. Šetří se tak výpočetní prostředky strojů a většinou i čas a nervy uživatelů.

Úložištěm majetkových dat je v současné době server Bombur (DB Informix). Během letošního roku jej vystřídá dvojice serverů Amber1 a Amber2 (DB Oracle), zapojených v clusteru pro zajištění bezvýpadkového provozu.

V současnosti se loni pročištěný číselník budov a místností postupně aktualizuje daty z proběhnuté pasportizace (viz článek P.Glose v tomto čísle Zpravodaje) a pracuje se na projektu *zavedení čárových kódů* majetku v rámci MU. Jedná se o plošné označení nemovitého a movitého majetku štítky s čárovým kódem a stanovení celouniverzitní metodiky práce se čtečkami čáro-

vého kódu (terminály) s cílem automatizovat proces fyzické inventarizace majetku. Pětice hospodářských středisek, jmenovitě Fakulta informatiky, Filosofická fakulta, Fakulta sociálních studií, Právnická fakulta a Rektorát, již čárové kódy využívají, avšak za pomoci systému externího dodavatele, který má jen lokální charakter a není na všech fakultách aktivní. V projektu se proto počítá s konverzí již dříve vygenerovaných kódů do centrální databáze, aby na zmíněných fakultách nebylo nutné již dříve nalepené štítky s čárovými kódy vyměňovat. Autoři článku pevně věří, že toto budou již poslední konverze, které budou s majetkem prováděny.

4 Výhled do budoucnosti

Na nejbližší měsíce je v souvislosti se správou majetku naplánována řada postupných akcí. Nejprve budou již použité čárové kódy (jejich číselná podoba) převedeny z lokálních systémů do centrální databáze majetku. V centrální databázi budou k takto získaným kódům jednorázově vygenerovány nové čárové kódy tak, aby jednoznačný čárový kód měly všechny majetky MU, a to majetky movité i nemovité. Aplikace EIS Magion pak bude u nově zaváděných majetků automaticky přidělovat čárový kód ihned po přidělení inventárního čísla.

V současnosti probíhá výběrové řízení na dodavatele softwaru pro již zakoupené čtečky čárového kódu. Dále bude nutné provést dotisk štítků s čárovými kódy pro celou MU a zajistit polepení majetků těmito štítky. EIS Magion a případně i Inet budou rozšířeny o podporu práce se čtečkami. Nejnáročnější etapou však bude zaškolení uživatelů v používání terminálů, aby s jejich pomocí provedli konečnou inventarizaci včetně zpracování získaných dat a promítnutí výsledků zpět do centrální databáze. O výsledcích naplánovaných úkolů si povíme v některém z dalších Zpravodajů. □

Mobilita napříč sítěmi

Eva Hladká, Luděk Matyska, FI MU

V roce 2001 byly na tomto místě prezentovány dva články zaměřené na mobilitu a bezdrátové sítě [1, 2]. V letech, která od publikace obou příspěvků uplynula, se vývoj nezastavil a je na místě se k problematice vrátit a univerzitní veřejnost seznámit se současným stavem podpory mobility v akademických sítích. Stejně jako v původních příspěvcích se omezíme především na podporu mobility v oblasti bezdrátových sítí, protože se jedná o oblast, s níž se každodenně může potkat každý z nás.

Autoři článku mají své domovské pracoviště v areálu FI MU na Botanické 68a, kde byla vybudována první bezdrátová síť v rámci celé Masarykovy univerzity [3] i ostatních vysokých škol (přinejmenším co se rozsahu pokrytí celého areálu fakulty týče). V současné době je v tomto areálu, kde kromě Fakulty informatiky sídlí i Ústav výpočetní techniky a Středisko podpory handicapovaných studentů, zprovozněno několik bezdrátových sítí. Další bezdrátové sítě byly vybudovány i v ostatních lokalitách Masarykovy univerzity [6, 7], která navíc samozřejmě nezůstala jedinou vysokou školou, jejíž pracoviště zajišťují přístup do Internetu tímto způsobem.

Bezdrátová síť již sama o sobě zajišťuje jistou úroveň mobility. V první úrovni umožňuje volný pohyb s trvalým přístupem k Internetu tam, kde je dostupný signál přístupového bodu. Větší prostor může být pokryt soustavou přístupových bodů, které zprostředkovávají dostupnost jednoho síťového segmentu – to je např. případ sítě FI, která v celém areálu vytváří uniformní prostředí z pohledu hierarchie IP sítí. I v tomto případě zůstává problém připojení při vlastním pohybu – nastavení přístupových bodů musí umožňovat dynamické předávání pohybujícího se klienta (např. notebooku). Pokud mobilitu omezíme na možnost přihlásit se kdekoliv v pokrytém areálu (i při omezené pohyblivosti po přihlášení), pak to nevyžaduje žádné dodatečné schopnosti bezdrátové sítě. V celém prostoru je k dispozici jednotný prostor IP adres a přístup do sítě se neliší podle místa připojení.

Problém nastává tam, kde musíme přecházet mezi bezdrátovými sítěmi s různou administrativou. V tomto případě pravděpodobně přecházíme do jiného prostoru z pohledu IP sítě a je pravděpodobné, že mechanismus přístupu k síti – tedy způsob, jak získáme povolení síť

používat – se bude lišit. Pokud víme předem, že se v prostoru nové sítě budeme pohybovat, musíme si zpravidla pamatovat nový způsob přihlašování, včetně např. přihlašovacího jména (login) a hesla, ale pokud se v prostoru nové sítě ocitneme neočekávaně, pak zpravidla nejsme schopni ji využít, přestože obecná politika dané sítě tuto možnost nevylučuje.

Existuje celá řada autentizačních mechanismů, které umožňují zpřístupnit bezdrátovou síť předem známým – zaregistrovaným – osobám. Skutečná mobilita však vyžaduje možnost alespoň dočasného využití i sítí organizací, u nichž uživatel není předem registrován. Možným řešením je projití registrační procedurou „na místě“, to však s sebou nese nejméně dva problémy: (i) vlastní registrační proces může být poměrně zdlouhavý a nemusí být tedy vhodný pro skutečně dočasné použití, (ii) hostující organizace si musí vést registrační údaje o všech hostech, což v podstatě zbytečně zatěžuje její administrativu (a v konečném důsledku snižuje ochotu zpřístupnit svou síť návštěvníkům).

Ideálním řešením by se mohl stát jediný bezdrátově pokrytý prostor nejenom v rámci jedné lokality MU či MU jako celku (kde virtuální privátní síť MU již tuto možnost poskytuje), ale celé akademické sítě a případně i celků větších. Je však zřejmé, že tento přístup nemůže být centralistický (s jedinou databází informací o všech potenciálních uživatelích) a je třeba hledat vhodnější přístupy.

Východiskem našich úvah je tedy existence organizací, ochotných v principu zpřístupnit si vzájemně své bezdrátové sítě, ovšem bez administrativní zátěže spojené se sdílením databází přístupových oprávnění.

1 Projekt EduRoam

Řešením problému uvedeného na konci předchozího odstavce se zabývá aktivita *Mobility Task Force* sdružení TERENA (organizace sdružující akademické sítě Evropy) [4] od začátku roku 2003. Cílem je výzkum síťových architektur, autentizačních a autorizačních technologií pro transparentní zpřístupnění bezdrátových (a případně dalších) sítí studentům, učitelům a vědeckým pracovníkům participujících organizací tak, aby jednotliví uživatelé mohli bez dalších kroků přistupovat k síti kdykoliv se ocitnou v prostoru pokrytém sítí alespoň jednoho z účastníků (není třeba se dopředu registrovat apod.). Pro tyto účely se řešitelé shodli na označení *EduRoam*, které se současně stalo synonymem pro hostitelskou mobilní infrastruktur (Educational Roaming).

Infrastruktura EduRoam vychází ze základní myšlenky, že autentizační proces konkrétního uživatele je realizován pouze u jedné organizace, nezávisle na tom, kde se uživatel právě nachází. Autentizační infrastruktura musí za zadaných autentizačních informací rozpoznat, kde je ona domovská organizace, té autentizační údaje předá a podle verdiktu (autentizován nebo nikoliv) pak zajistí přístup do lokální sítě. Konkrétně se využívá hierarchicky propojený systém autentizačních serverů RADIUS, neboť ty jsou zpravidla využívány pro autentizace v rámci jednotlivých organizací a podporované protokoly umožňují jejich vzájemné propojení způsobem popsaným výše.

Konkrétní autentizace se pak dělá protokolem 802.1x, případně přes webová rozhraní, podstatný je ale přenos autentizačního dotazu domovské organizaci uživatele. Ta je dána formátem použitého „průkazu“ (credentials), zpravidla pak přihlašovacího jména, jehož součástí je i jednoznačně vymezená identifikace domény (např. `matyska@ics.muni.cz` jako login jméno ukazuje, že autentizaci je nutné provést v doméně `ics.muni.cz`). Aby systém mohl fungovat, musí se jednotlivé organizace předem dohodnout na vzájemné důvěře a tom, že budou takto delegovanou autentizaci uznávat. V současnosti je do aktivity Mobility Task Force připojeno 13 národních sítí, ovšem žádná národní síť nepokrývá všechny byť jen akademické instituce dané země.

2 EduRoam v české akademické síti

Česká republika se prostřednictvím sdružení CESNET připojila k projektu EduRoam hned v jeho počátku. V rámci výzkumného záměru *Vysokorychlostní síť národního výzkumu a její nové aplikace* byla založena aktivita s cílem vybudovat

národní infrastrukturu a připojit ji k ostatním evropským sítím. Výsledkem práce je definice roamingové politiky (tedy kdo, kdy a za jakých podmínek je oprávněn tuto službu používat – zpravidla je taková politika velmi blízká roamingovým politikám, které známe od mobilních operátorů telefonních sítí) a konkrétní implementace EduRoam infrastruktury v České republice [5]. Současně CESNET garantuje propojení národní infrastruktury na evropské úrovni.

Na národní úrovni je do aktivity EduRoam.cz připojena již řada organizací. Kromě sídla CESNETu v Praze na Zikově ulici je třeba zmínit např. UK (rektorát a řada fakult, např. FF, PRF a FAF), FEL ČVUT, UJEP, VŠCHT, ZČU, UHK. Technické podrobnosti o podmínkách provozování RADIUS serverů (jak se k EduRoamu připojit), včetně jejich doporučené topologie, je možné najít na části webu EduRoam určené správcům infrastruktury.

EduRoam řeší problém hostujících účastníků v síti zcela přirozeným způsobem. K autentizaci stačí autentizace uživatelským jménem a heslem ze své domovské organizace.

3 Rizika spojená s provozováním EduRoamu

Jak jste si možná všimli, mezi národními organizacemi zapojenými do aktivity EduRoam nebyla zmíněna Masarykova univerzita v Brně. Jedním z důvodů je standardní problém těch, kteří začali příliš brzy – bezdrátové sítě na MU jsou staršího data a používají autentizační mechanismy, které nejsou jednoduše propojitelné s požadavky EduRoam. Dalším, podstatnějším důvodem je ale právní nevyjasněnost – člen EduRoam musí zpřístupnit svou síť uživatelům z ostatních organizací. To ovšem znamená přizpůsobit bezpečnostní a přístupovou politiku požadavkům EduRoam, což v případě MU není jednoduché rozhodnutí, mimo jiné opět proto, že na MU mají formálně ustavené politiky přístupu k síti jednu z nejdelších tradic v rámci akademického prostředí ČR. V rámci realizace politiky je pak třeba ošetřit případy, kdy jednotlivec – „návštěvník“ – poruší její pravidla. Má se v takovém případě zakázat přístup všech uživatelů ze stejné domovské organizace? Pokud ne, pak jakým způsobem budou drženy údaje o „nežádoucích“ uživatelích – nebudeme si muset vytvářet vlastní databáze, jejichž existenci a správě jsme se chtěli vyhnout?

Nejproblematičtějším místem sjednocení politik je otázka přístupu k vnitřním zdrojům univerzity. EduRoam sám nedefinuje, jakou IP adresu (ve vztahu k adresnímu prostoru hostující organizace) „návštěvník“ získá, nicméně jednoduché a často používané řešení přiděluje IP adresu přímo z rozsahu IP adres hostující organizace. To ovšem v dnešním světě, kde je stále řada přístupů kontrolována na základě IP adresy, znamená, že takový uživatel získá přístup ke stejným službám a informačním zdrojům jako vlastní student nebo zaměstnanec. Tím zpravidla dojde k rozporu s licenční politikou třeba elektronických databází – MU má zakoupeno právo přístupu vlastních studentů a zaměstnanců, nikoliv však studentů a zaměstnanců ostatních vysokých škol či dalších akademických institucí. Tento problém lze řešit vyčleněním bezdrátové sítě z rozsahu sítí, zpřístupňujících takové zdroje – pokud ovšem stejnou síť použije oprávněná osoba, pak rovněž ztrácí možnost přístupu (nebo ten musí byt realizován dalším stupněm autentizace, což je samozřejmě pro vlastní uživatele nepohodlné).

Použití Virtuální privátní sítě tento problém může řešit, vyžaduje však netriviální technickou podporu všech účastníků aktivity EduRoam a ochotu implementovat příslušné nástroje. Dalším možným řešením je zlepšení mechanismů *autorizace*, tedy oprávnění přistupovat ke konkrétním zdrojům.

4 Autorizace – jak na ni?

Autorizace logicky následuje za autentizací – poté, co máme potvrzenu identitu konkrétního uživatele rozhodneme, co smí či nesmí v síti dělat. Ovšem aktivita EduRoam je založena na předpokladu, že lokální síť vlastně identitu nezná – pouze dostane od domovské organizace (které věří) potvrzeno, že ta konkrétního žadatele zná. Jak ovšem v takovém prostředí zajistit odpovídající autorizaci? Tato otázka zatím nemá jednoznačnou odpověď, nicméně v posledních letech se zdá, že by možným řešením mohl

být systém Shibolleth [8], který původně vznikl v USA (jakou součást aktivit kolem Internetu2) pro autorizaci přístupu k rozsáhlým elektronickým knihovním zdrojům.

Princip Shibollethu je obdobný principům, na nichž je založen EduRoam – definujeme autorizační skupiny (např. uživatelé konkrétní elektronické databáze) a na těchto skupinách se dohodneme s partnery. Autorizační požadavek pak opět řeší domovská organizace – té hostující předá autentizační údaje klienta a požadavek, aby domovská organizace potvrdila příslušnost k určité skupině (např. skupině zahrnující uživatele oprávněné používat konkrétní elektronickou databázi). Domovská organizace udělá kompletní ověření (autentizaci a následnou autorizaci) a hostující organizaci sdělí pouze výsledek: *ano* či *ne*. Hostující organizace si opět nemusí budovat vlastní databázi oprávnění, uživatel se nemusí předem registrovat, ...

Systém Shibolleth je dimenzován s ambicí sloužit celé akademické veřejnosti USA, v současné době je používán řadou univerzit s velmi dobrým ohlasem. I v ČR se začíná uvažovat o jeho experimentálním nasazení, ovšem plná implementace bude vyžadovat součinnost jak univerzit, tak i vlastních poskytovatelů obsahu a je to tedy běh na dlouhou trať.

5 Závěr

Jak je z popsaného patrné, podpora mobility postupně přerůstá z řešení čistě technických problémů do roviny politik, definujících oprávnění přístupu jak k síti, tak jednotlivým zdrojům touto sítí zprostředkovaným. Rostoucí počet případů zneužití volného přístupu k Internetu nutí i vysoké školy a další akademická pracoviště, aby ve zvýšené míře dbaly na nástroje a metody kontroly používání počítačové sítě. V příspěvku zmíněné přístupy se snaží překlenout rozpor, který je mezi snahou zpřístupnit Internet co největšímu počtu (akademických) uživatelů a snahou minimalizovat nebezpečí, která z neomezeného přístupu plynou. Aktivity EduRoam i Shibolleth jsou příkladem škálovatelných řešení, schopných pokrýt velmi rozsáhlé oblasti s minimem administrativy a byrokracie. Akademické sítě se snaží rozvíjet podporu mobility, nemohou však ignorovat problémy, které mobilita přináší. Je možné, že z projektu EduRoam vyroste v budoucnu jeden velký prostor pokrývající akademické prostředí a my budeme moci přecházet z jedné sítě do druhé bez ruční přeregistrace a bez obav z bezpečnosti (a provozovatelé sítí budou ochotni je otevírat, protože budou schopni vždy identifikovat případné narušitele provozu). Nepochybně se časem i MU připojí k aktivitám EduRoamu, aby svým zaměstnancům a studentům umožnila využití bezdrátových sítí i v dalších lokalitách, a aby současně vytvořila přívětivé prostředí pro své hosty. K tomu však bude ještě třeba kromě technických problémů vyřešit právě i otázky autorizace přístupu k licencovaným či jinak chráněným informačním a dalším zdrojům.

Literatura

[1] L. Matyska, E. Hladká. „Mobilní počítání.“ *Zpravodaj ÚVT MU*. 2001, roč. 11, č. 4 s. 1–3.

[2] L. Matyska, E. Hladká. „Mobilita v malém.“ *Zpravodaj ÚVT MU*. 2001, roč. 11, č. 5, s. 1–4.

[3] L. Matyska. „Bezdrátová síť Fakulty informatiky.“ *Zpravodaj ÚVT MU*. 2002, roč. 12 č. 3, s. 5–7.

[4] „TERENA mobility initiative“ `http://www.terena.nl/tech/index_mobility.html`

[5] „Projekt EduRoam České akademické sítě“ `http://www.eduroam.cz`

[6] D. Rohleder. „Bezdrátové sítě v prostředí MU.“ *Zpravodaj ÚVT MU*. 2004, roč. 14, č. 3, s. 18–19.

[7] J. Morávek, R. Peša. „VPN server Masarykovy univerzity.“ *Zpravodaj ÚVT MU*. 2003, roč. 14, č. 2, s. 10–12.

[8] „Shibolleth—authorization“ `http://shibboleth.internet2.edu/` □

Softwarové patenty

Luděk Matyska, ÚVT MU

Ladislav Lhotka ve svém posledním příspěvku věnovaném Open Software [1] zcela správně poukázal na to, že skutečným *nepřítelem* otevřených programů nejsou ti, kteří nechtějí zveřejnit zdrojové texty, ale ti, kteří se snaží o jejich „ochranu“

prostřednictvím *softwarových patentů*. Zatímco pouhé nezveřejnění v konečném důsledku vede k tomu, že stejnou věc někdo musí vymyslet znovu, softwarové patenty jsou úspěšnou cestou k zablokování tvůrčí invence a svobodného programování vůbec. Na historii a současný stav v této oblasti se proto zaměříme v tomto příspěvku.

1 Trocha historie

Patent v současnosti chápeme jako právo monopolní ochrany na určité dílo, produkt nebo proces (postup), který má autorovi zajistit příjem odpovídající nákladům, které musil vynaložit na jeho realizaci. Určitá forma monopolní ochrany – a s ní spojený monopolní zisk – pravděpodobně doprovází lidstvo již od starověku, patent v modernějším pojetí se objevuje v „Statute of Monopolies“, vydaném králem Jakubem I Anglickým v roce 1623, který v Anglii uzákonil právo na *patent* pro prvovynálezce a jejich ochranu po dobu 14 let. Z dnešního pohledu je ovšem zajímavý především důvod vydání tohoto nařízení: byla jím snaha omezit právo Koruny (tedy krále) vydávat „patenty“, práva na exkluzivní zboží či výrobky (na monopol). Udělení patentu bylo vždy chápáno jako privilegium, za které příjemce platí – buď přímo financemi (patenty byly nikoliv nevýznamný zdroj příjmů Koruny) nebo loajalitou. Tedy z jistého úhlu pohledu se jednalo o ochranu veřejnosti proti přílišnému počtu víceméně libovolně udělovaných „patentů“. Vydané královské nařízení, které tvoří faktický základ moderního anglo-amerického patentového systému, tedy omezovalo právo udělit patent jen těm, kteří nový produkt „vynalezli“, případně první do země přinesli.

Ochrana vynálezců je však mnohem starší, ovšem vždy byla spojena se zájmy společnosti. Již v roce 1474 vydala Benátská republika nařízení, požadující *registraci* vynálezů – částečně pro možnost poskytnout ochranu proti zneužití, fakticky ale proto, aby vynálezci si své vynálezy nenechali jen pro sebe a poskytli je veřejnosti (tedy *zveřejnili je*). Oplátkou za toto zveřejnění jim byla poskytnuta právní ochrana – monopol na zboží či proces. Společnost si tak de facto kupovala přístup k vynálezům.

Zatímco patenty na produkty a procesy mají tedy dlouhou historii, patentová ochrana programů – *softwarové patenty* – existuje pouze velmi krátkou dobu. První, kdo se otázkou patentové ochrany programů šířeji zabýval, byl samozřejmě americký Patentový úřad (přesněji U.S. Patent and Trademark Office). Ještě v sedmdesátých letech minulého století odmítal udělit patent v případě, že zahrnoval matematické postupy nebo výpočty (programy byly chápány jako vyjádření algoritmů, tedy matematických postupů). Změnu přístupu si vynutilo až rozhodnutí amerického Nejvyšší soudu v roce 1981, který v případu *Diamond v. Diehr* přikázal Patentovému úřadu vydat patent na nový způsob formování pryže řízený počítačem. Právě počítačový program (způsob řízení procesu formování) byl tím inovativním příspěvkem, proto dříve Patentový úřad odmítal patent udělit. Počátkem devadesátých let další americký soud (Federal Circuit) rozhodl, že zatímco samotný algoritmus zůstává nepatentovatelný, na patentovou žádost je třeba hledět jako na celek a patent udělit v případě, že počítačový postup zpracovává konkrétní, v reálném světě získaná data (např. počítačový program na zpracování elektrokardiografů). V roce 1995 pak vydává vlastní direktivu o zpracování patentových žádostí v oblasti software.

1.1 Situace v Evropě

Odhlédneme-li od národních zvyků, situaci v Evropě stále definuje Evropská patentová dohoda z roku 1973, která explicitně vyjímá matematické postupy, počítačové programy, obchodní postupy, intelektuální díla apod. z působnosti patentového práva – jsou zpravidla chráněny autorským právem. Nicméně rozšířené chápání patentového práva vedlo k tomu, že v Evropě začaly být přijímány patenty s netriviální počítačovou částí již koncem sedmdesátých let (první evropský programově orientovaný patent firmy IBM, ep0002365, je z roku 1979). Zatímco podle interních předpisů se od druhé poloviny osmdesátých let patentují postupy, jejichž součástí je počítačový program (nicméně program sám patentové ochrany nepožívá), v roce 1998 se Evropský patentový úřad rozhodl přijímat pod patentovou ochranu i programy, primárně v očekávání, že budou přijaty celoevropské direktivy, které

fakticky zruší vynětí softwarových patentů z působnosti patentového práva. K pokusu o nastolení takovéto direktivy došlo v roce 2002 z podnětu komisaře pro vnitřní trh (Frits Bolkenstein) formou návrhu 2002/0047 o „Patentovatelnosti počítačově implementovaných vynálezů“. V podstatě tato nová direktiva měla uzákonit praktiky realizované Evropským patentovým úřadem, nicméně stále vyjímala čisté programy z patentové ochrany. V září 2003 Evropský parlament velkou většinou přijal řadu pozměňovacích návrhů, které stav fakticky vrátily zpět do roku 1973. Pozměňovací návrhy byly podpořeny kulturním a průmyslovým výborem, pro původní znění byl pouze výbor pro legislativu.

Pozměňovací návrhy dále zpracovávala speciální komise, ustavená radou ministrů – ta pak v roce 2004 vydala návrh nového znění připravované direktivy. Text fakticky zesiluje (a nikoliv zeslabuje) původní návrh komisaře Bolkensteina, neboť navíc vnáší i přímou patentovatelnost programů (tento nový návrh byl zveřejněn 18. května 2004). V současnosti je tento návrh předmětem ostrých sporů jak v odborné veřejnosti (která se ale kloní spíše k zamítnutí patentů, viz více jak 3000 podpisů ředitelů a jim na rovneň postavených pracovníků evropských firem pod peticí za nepřijetí návrhu), tak i mezi Evropskou komisí a parlamentem, kde lze velmi obecně říci, že Komise patenty podporuje, zatímco parlamentní většina nikoliv. Na úrovni vlád členských států je situace značně nejasná, i zde je často vidět rozpor mezi představami vlád (spíše vlažně pro) a národních parlamentů (často proti). Situaci navíc komplikuje proces vyjednávání, kdy státy jsou ochotny svou původně ostře formulovanou pozici přehodnotit na základě ústupků v jiných oblastech.

2 Qui bono

Přestože softwarové patenty mají chránit autory programů a mají zabezpečit prostor pro tvůrčí rozvoj, působí na první pohled poměrně překvapivě zjištění, že jsou to zpravidla právě samotní programátoři, případně (menší) firmy, které patří mezi největší odpůrce programových patentů. A naopak, za přijetí zákonů umožňujících patentovat samotné programy nejvíce lobují velké firmy. Vždyť patentová ochrana má poskytovat záruky samotným vynálezcům (tedy v tomto případě autorům programů) právě proti zvůli velkých firem. Jedná se tedy o paradoxní situaci, kdy velké firmy samy lobují za přijetí zákonů, které by omezily jejich možnosti? Samozřejmě nikoliv – ze softwarových patentů budou bohužel nejvíce těžit právě velké firmy, nikoliv samotní programátoři. Příčina je v samotné podstatě patentového procesu, pokud je aplikován na počítačové programy. Každý vynálezce se při vyplnění patentové přihlášky snaží definovat podstatu svého vynálezu tak, aby pokrývala co nejvíce možných budoucích užití a současně aby nezasahovala do prostoru vymezeného nějakým již přijatým patentu (pak by totiž byla přihláška po právu zamítnuta). Zatímco v případě klasických patentů mají patentové úřady vypracovány poměrně účinné metody definice „předchozích znalostí“ a také umí poměrně přesně vymezit zásah do předchozích patentů, v případě programů tomu tak není. Pokud patentové úřady posuzovaly patenty pouze proti existujícím předchozím patentům, pak samozřejmě zpočátku žádné předchozí patenty neexistovaly a jednalo se o nové vynálezy. Samozřejmě široce publikované algoritmy patentovány nebyly, ale to nebránilo firmám patentovat postupy, které zpočátku vypadaly pouze jako chytrá aplikace známých postupů v novém prostředí. Ovšem abstraktní charakter programů vede k tomu, že majitelé patentů se začínají domáhat široké patentové ochrany konkrétních obratů, použitých v již patentovaných programech. Tím samozřejmě pokrývají stále širší skupinu nových programů, které často s původním zaměřením patentu nemají nic společného, ale používají nějaký obrat, který byl takto patentován (slavný "single click" nebo patent na vyznačení změn v dokumentu pomocí barev – US patent No. 5,021,972 – jsou jen extrémním případem, na `http://webshop.ffii.org/` můžete najít příklady 20 programových patentů, které v podstatě ovládají přístup k webovým obchodům). To ovšem vytváří prostředí, kdy přestává být možné napsat nový počítačový program, aniž bychom v něm nepoužili nějaký obrat, který již nebyl patentován. Přitom

původní patent pravděpodobně pokrývá něco, co s novým programem nesouvisí, takže bez náročných – a patřičně drahých – hledání ve stávajících patentech nebude toto porušení patentu zřejmé.

Nebezpečnost programových patentů vyplývá právě z pokrytí běžných programových obratů a jejich skrytí pod nečekaným názvem patentu. To vede k následující politice majitelů patentů – namísto dalšího rozvoje nových vlastních aplikací prohledávají práce ostatních a hledají možné porušení patentu. Následně pod hrozbou právního sporu (což je zejména v Americe velmi drahé a pro menší firmy potenciálně bankrotující) požádají o platbu licenčních poplatků. Napadená firma zpravidla ustoupí, podobně jako ustoupí drobný živnostník, když na něm pouliční gang začne vymáhat „výpalné“.

Na tento postup nefunguje ani ochrana, kterou používají velké firmy. Ty jsou zpravidla majiteli velkého množství podobných programových patentů, takže jejich odborníci a právníci podrobí analýze produkt firmy, která je napadla a s vysokou pravděpodobností v ní najdou nějaký postup, který mají patentovaný. Pak vzájemným započtem patentů (resp. potenciálních licenčních poplatků) hrozbu „výpalného“ odvrátí. Pokud ovšem majitel patentu nemá vlastní produkt, nelze tento postup uplatnit.

Že se nejedná o hypotetický postup, je možno ilustrovat i na ve své podstatě bezelstném prohlášení, které pro časopis Think učinil v roce 1990 Roger Smith, pomocník hlavního poradce IBM pro otázky ochrany duševního vlastnictví. Ten říká, že již v roce 1990 přímé poplatky za licenční poplatky za patenty, které vlastní IBM, představují jen cca 10% zisků, které IBM celkově z patentů získává. Zbývajících 90% zisků představuje výhoda křížového licencování, tedy de facto bezplatný přístup k cizím patentům. Patenty tak ovšem nechrání malé firmy, které vlastní jeden nebo několik málo patentů – velká firma typu IBM si dokáže zajistit přístup k výsledkům tvůrčího procesu, aniž by za to jakkoliv zaplatila, právě mechanismem křížového licencování. Kdyby neexistovala možnost křížového licencování, musela by zřejmě IBM platit za „cizí“ patenty několikanásobně více, než kolik sama získá na licenčních poplatcích (to je samozřejmě poněkud zkreslené, neboť díky křížovému licencování klesají i zisky IBM, ovšem rozdíl v jednom řádu nasvědčuje tomu, že se principiálně nejedná o chybnou úvahu). Tedy i pro IBM by patrně bylo výhodnější, kdyby žádná patentová ochrana tohoto typu neexistovala – teď patentuje nikoliv kvůli ziskům za licenční poplatky, ale spíše jako ochrana proti uplatnění podobného práva jinými.

Zatímco IBM přesto patří k těm, kteří přesto programové patenty podporují, řada dalších firem – mezi nimi CISCO, Alcatel, Adobe (dokonce i Bill Gates v roce 1991) se k programovým patentům vyjadřuje negativně již delší dobu. Hlavním důvodem odporu je právě ona „časovaná bomba“ přiznaných patentů, pokrývajících zcela nečekané a ve své podstatě nesmyslné použití původně patentovaných programových postupů.

Ale i IBM se postupně dostává do vnitřně rozporného stavu ohledně programových patentů. Snaha podporovat Open Software se dostává do rozporu s další podporou patentů. Přestože poslední vývoj ve slavném případu SCO vs. „Linux“ zdá se naznačovat, že pozice firmy SCO zdaleka není tak pevná, jak si sama firma myslí, programové patenty jasně ohrožují možnost volné tvorby programů a tím samozřejmě ohrožují i ty firmy, které své podnikání staví kolem OpenSoftware (reálně ohrožují veškerý vývoj programů mimo největší firmy, které již dnes drží dostatek patentů jako ochranu proti potenciálním budoucím sporům – ovšem ukázali jsme, že tato ochrana postupně ztrácí na síle při rostoucí množině firem, které nic nevyvíjí a jen „sbírají“ patenty). IBM sama proto přišla s návrhem „patent commons“, tedy množiny patentů, kterou jejich majitelé veřejně poskytnou a zřeknou se práva na licenční poplatky. Přitom tyto patenty budou představovat ochranu proti pokusům o patentové vyděračství – při dostatečně rozsáhlé množině takto uvolněných patentů bude velmi pravděpodobné, že alespoň jeden z těchto patentů je novým patentovým vyděračem porušen [2]. Velmi to ovšem připomíná politiku *zastrašování*, která byla docela úspěšně použita proti SSSR. Ovšem všichni víme, že skutečným řešením není parita hrozeb, ale odstranění příčiny – v tomto případě pak programových patentů vůbec.

3 Závěrem

Programové patenty jsou však pouze specifickou, v mnoha ohledem značně extrémní cestou ochrany *duševního vlastnictví*. Jejich přinejmenším ambivalentní, ale dle názoru nejen autora tohoto článku silně negativní, vliv na tvůrčí procesy v návrhu a realizaci počítačového vybavení je poměrně dobře dokumentovatelný a je příčinou jasného odporu proti programových patentům v USA, Evropě i dalších zemích. Počítače, počítačové sítě a další zařízení však vedou k nutnosti předefinovat celou oblast duševního vlastnictví a její ochrany – jak ukazuje i kauza s programovými patenty, ta je v současnosti značně vychýlena ve prospěch majitelů duševního vlastnictví. I kdybychom se shodli na tom, že programy mají požívat ochrany pod hlavičkou autorského práva („copyrightu“), situace ani v této oblasti není jasná – počítače umožňují tak snadné šíření děl chráněných autorským právem, že je stále spornější, zda prohibiční taktika je skutečně správná a hodná dalšího rozvoje. Oblastí přístupu k autorským dílům se proto budeme věnovat v některém z dalších příspěvků.

Literatura

[1] L. Lhotka: *Svobodný software a základní otázka programování*, Zpravodaj ÚVT, 2005, roč. 15(3), s. 14–17.

[2] G. Goth: Open Source Infrastructure Solidifying Quickly, IEEE DS online.

Většina materiálu využitého v tomto příspěvku pochází z internetových zdrojů, zejména pak z serverů BitLaw (`http://www.bitlaw.com`), Software patents vs. Parliamentary democracy (`http://swpat.ffii.org`) a EuroLinux Alliance (`http://petition.eurolinux.org`). □

Obsah

Rada informačních technologií Masarykovy univerzity v Brně, *Luděk Matyska, ÚVT MU* **1**

Bezpečnost v distribuovaném prostředí, *Daniel Kouřil, ÚVT MU* **2**

Zavolej mi . . . , *Stanislav Kala, ÚVT MU* **6**

Pasportizace budov a místností MU, *Petr Glos, ÚVT MU* **9**

Elektronická podpora evidence majetku na MU v Brně, *Jana Haluzová, Zdeněk Machač, ÚVT MU* **11**

Mobilita napříč sítěmi, *Eva Hladká, Luděk Matyska, FI MU* **13**

Softwarové patenty, *Luděk Matyska, ÚVT MU* **16**

Editor: M. Bartošek • Vydavatel: Masarykova univerzita v Brně • 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