ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • červen 2006 • roč. XVI • č. 5

PlanetLab – model budoucího Internetu

Jiří Navrátil, CESNET z.s.p.o.

Bude se Internet podstatně měnit?

V poslední době se v odborných kruzích stále více hovoří o nutnosti změnit základy Internetu, protože s jeho růstem se objevuje stále víc a víc problémů. Nové aplikace, které zajímají miliony lidí, a trvalé zvyšování přípojných kapacit, které umožňuje realizovat přenosy ohromných objemů dat velkými rychlostmi, přináší nejen nové možnosti, ale prohlubují i palčivé problémy, které jsou známy již mnoho let: nedostatečný adresový prostor, přetížení některých fundamentálních služeb, pomalé vyhledávání zdrojů, nespolehlivá stabilita přenosových cest, stále častější pirátské útoky na servery… Jedním z důvodů tohoto stavu je fakt, že mnohé služby a protokoly, které se v Internetu používají, jsou staré desítky let a vzhledem k tomu, že na nich stojí celý Internet, tak se nemohly principiálně změnit, ale jen postupně modifikovat.

PlanetLab `http://www.planet-lab.org` je první „organizace“, která si ve svých cílech vytyčila změnu Internetu. Podívejme se proto, co je to vlastně za organizaci, jaké je její poslání, v jakých směrech se angažuje, co umožňuje a jaké aplikace jsou na ní vyvíjeny a testovány. PlanetLab vznikla v průběhu roku 2002 jako konsorcium několika amerických universit (University of California at Berkeley, Princeton University a University of Washington) [1] a postupem času do ní vstoupily další university z celého světa. Jejími členy se stala i významná výzkumná pracoviště firem z oblasti IT (jako jsou HP, Intel, France Telecom), organizace zajišťující provoz Internetu v akademických komunitách (jako jsou Internet2-USA, Canarie-Kanada, Cernet-Čína) a další národní pracoviště se širokým výzkumným posláním (INRIA-Francie, GIST-Korea) atd. Konsorcium PlanetLab představuje jednak celosvětovou distribuovanou laboratoř pro výzkum a ověřování nových typů síťových aplikací v planetárním měřítku, současně jde ale i o unikátní síť, samostatnou infrastrukturu, která má 631 uzlů distribuovaných ve všech částech světa. Evropa má v síti asi 100 uzlů, ale ČR a ani Slovensko v ní zatím zastoupeny nejsou.

Akademické prostředí bylo vždy na čele rozvoje komunikačních systémů a stálo i u zrodu Internetu. Žádná universita a ani žádný stát nebude mít nikdy dostatek prostředků a lidí na to, aby mohl samostatně vytvořit laboratoř, která bude působit v celosvětovém měřítku. To, že se to v projektu PlanetLab podařilo, je velkým krokem vpřed a svědčí to o tom, že PlanetLab má zajímavý a široký program. V minulosti již bylo několik pokusů takové experimentální celosvětové sítě vytvořit, ale ty se většinou zaměřovaly jen na monitorování provozu Internetu (NIMI, Surveyor)

a brzy zanikly, protože jejich poslání bylo příliš úzké. Za experiment v tomto směru se dá považovat i propojení gridů. Tam však v konečném řešení půjde o vytvoření produkční sítě, která bude sloužit především pro zajištění dostatečných výpočtových kapacit komunitě uživatelů z oblasti fyziky vysokých energií, pro NASA, chemiky, atd. PlanetLab je něco jiného, je to otevřená laboratoř se širokým posláním pro tvůrce síťových aplikací, tedy prostředí pro implementace návrhů nových komunikačních protokolů, metod distribuovaného zpracování a uchovávání dat – a jejich testování.

Internet se mění stále

Původní představa a dlouholetý provoz Internetu byly postaveny na konceptu, kdy na jedné straně existuje množina uživatelů (klienti) a na druhé straně stojí servery, které poskytují informace a zajišťují služby. Kdysi dávno to byly jen služby spojené s elektronickou poštou a zajištěním přístupu k výpočetním serverům, později se služby rozšířily do sféry bankovní, knihovní, komerční a administrativní. Před několika lety to byl web, který zajistil, že se Internet stal přitažlivým pro širokou uživatelskou komunitu. Pořád to však byl provoz typu klient-server. V posledních letech však i toto schéma bylo překonáno. V podstatě „přes noc“ se začal masivně prosazovat provoz typu P2P („peer to peer“), neboli provoz mezi samotnými účastníky Internetu, bez nutnosti služeb poskytovaných nějakými „centrálními“ servery. Podle některých odhadů tvoří dnes takovéto peer to peer aplikace 50–70 % celkového objemu přenosu dat v Internetu.

Tuto novou éru odstartoval na přelomu tisíciletí program Napster, který umožnil masové přenosy hudebních nahrávek. Jeho popularita během několika málo měsíců vzrostla natolik, že vážně ohrozil celý multimediální průmysl a hudební nakladatelé nakonec dosáhli toho, že Napster musel skončit svoji činnost. To však vůbec neznamenalo konec aplikací typu P2P, spíše naopak. Vývojáři aplikací i uživatelé si uvědomili, jaký vnitřní potenciál Internet má, a že se vůbec nemusí data soustřeďovat na jednom místě, aby byla přístupná mnoha uživatelům. Pokud jsou data zajímavá, pak si je ti, kteří o ně mají zájem, najdou sami – a sami jsou ochotni si je také vzájemně vyměňovat. Legální aspekty výměny dat, které jsou předmětem licencí, je jiná otázka, o té zde nebudeme hovořit. Krátce po „pádu“ Napsteru se objevily jiné programy, které uživatelům zajistily totéž, co dělal Napster. Pracovaly na mnohem promyšlenější strategii, která dovolovala vytvářet distribuované virtuální společenství uživatelů. Programy DirectConnect, Kazaa, Gnutella, BitTorrent a mnoho dalších jejich odvozenin umožňují přenos dat v dynamicky vytvářených virtuálních sítích, podle příslušnosti ke komunitě dané protokolem přenosu. Většinou jde o přenosy velkých objemů dat, kterými jsou hudební a video nahrávky (MP3, DVD), ale i další objemově náročné informace – databáze, velké softwarové balíky, atd. V mezičase pokročila i technologie digitálního zpracování zvuku a videa a jejich přenos po Internetu, a tak se technologie P2P začíná uplatňovat i v této oblasti. Vznikla např. první celosvětová síť Skype, která umožňuje telefonování po Internetu. Skype má dnes kolem 5 milionů uživatelů, a po jeho úspěchu se objevují další sítě podobného typu. Uvedené aplikace P2P jsou samozřejmě ty nejznámější, protože jsou hodně medializovány. Existují však také aplikace, které byly vyvíjeny pro oblasti spojené s metropolitními informačními systémy, výzkumem klimatu apod. Dá se říci, že P2P sítě jsou stejnou revolucí v Internetu, jakou do něho před několika lety přinesl WEB. Jsou to velice spolehlivé distribuované sítě s automatickými funkcemi vyhledání partnera, buď úplně distribuované nebo jen s minimálními vazbami na nějaké centrum.

Každá z těchto sítí používá trochu jinou strategii vyhledávání partnerů i přenosu dat mezi nimi. To mělo samozřejmě svoji odezvu v akademické oblasti, protože zmíněné problémy vedou k velice zajímavým vědeckým teoriím a řešením obecných problémů, které jsou spojeny s teorií grafů, pravděpodobností, spolehlivostí, plánovacími strategiemi apod. Svědčí o tom velké množství prací, které byly v posledních 5 letech publikovány ve významných časopisech a na odborných konferencích z oblasti počítačových věd. Vytvořit síťovou aplikaci není vůbec jednoduché

a pokud by to měla být aplikace, která má fungovat v globálním měřítku, sloužit milionům uživatelů, tak je nutné její funkčnost ověřit v reálném prostředí. Jak ukazují zkušenosti, tak právě „reakce reálného prostředí“ Internetu je katalyzátorem pro ty nejatraktivnější komerční projekty. Vývoj je tak rychlý, že ani velké nadnárodní společnosti a tvůrci komerčních internetových aplikací nemají mnoho času si dělat vlastní základní výzkum v této oblasti a stále více se opírají o teorie, principy, výsledky měření nebo pilotní návrhy, které byly vytvořeny v akademickém prostředí. Dá se říci, že do jisté míry k úspěšnému rozvoji této oblasti přispěla i Planetlab. Existuje dlouhý seznam vědeckých prací, které byly publikovány na základě výsledků z experimentování na PlanetLab. Ve většině těchto prací i v popisu nových projektů dominují problémy související s hledáním informací v rozsáhlých sítích, sdílením a replikací dat, návrhy vhodných struktur a adresací objektů. Často se zde řeší problémy nových metod přenosu dat, využití možných redundantních spojení, což je často (přímo i nepřímo) spojeno s důležitou problematikou směrování.

PlanetLab řeší aplikace budoucnosti

Vyjmenujme si jen několik konkrétních příkladů služeb a aplikací, které v PlanetLab dnes pracují, a které spoluvytváří nové prostředí a tím pomáhají řešit síťové problémy s jistou abstrakcí. Následující příklady jen ilustrují tematiku a ukazují dimenze veličin, se kterými projekty kalkulují:

- Jeden z největších projektů je OceanStore [11] – globální paměť, v níž se uživatelé nestarají o to, kde jsou jejich data uložena.
- Distribuční systém Coral `http://www.coralcdn.org` je určen pro efektivní distribuci dat uživatelů, kteří mají pomalé připojení k síti a potřebují informace vystavené na jejich počítačích (webových serverech) distribuovat širokému okruhu dalších.
- Služba CoDNS zajišťuje v síti distribuovaný DNS, který je odolnější proti útokům a nespolehlivosti serverů `http://codeen.cs.princeton.edu/`.
- CoBlitz, CoWeb a CoDeploy jsou služby, které využívají distribuovanou síť pro paralelní přenos velkých objemů dat, např. pro distribuci zdrojů operačních systémů.
- Projekt RON (Resilient Overlay Network) se zaměřuje na tvorbu a optimalizaci směrovacích tabulek s využitím redundance a interního monitoringu dostupných cest v síti [6].
- Projekt DHARMA (Distributed Home Agent for Remote Mobile Access) řeší situace zajištění mobilního přechodu z různých sítí bez nutnosti opětně navazovat spojení `http://dharma.cis.upenn.edu/`.

Mnoho z těchto služeb a aplikací je přímo svázáno nebo navazuje na další výzkumné projekty, které byly a jsou podporovány nadací NSF (National Science Foundation), jako jsou např. Tapestry, Chord, Pastry, OpenDHT – což jsou projekty patřící do třídy DHT (Distributed Hash Table) [7, 8, 9]. Tyto metody jsou dnes jednou z nejvíce se rozvíjejících oblastí základního výzkumu, a také oblastí s největším publikační aktivitou. HT – neboli asociativní paměti – zná každý programátor, který pracuje s Perlem a ví, jak užitečné jsou tyto funkce při práci s datovými strukturami. Zjednodušeně se dá říci, že nahrazují dlouhé hledání objektu tím, že objekt má přidělen jednoznačný klíč, který se dá spočítat. Nalezení objektu je pak vlastně ve většině případů realizováno v jednom kroku. Stejný princip se používá i při lokalizaci objektu v síti.

Řada projektů řešených v PlanetLab je podporována nebo realizována s účastí firem jako jsou HP, Microsoft, Intel apod. Například s podporou firmy Intel bylo testováno prostředí pro projekt IrisNet (Internet-scale Resource Intensive Sensor Network Services), což je síť osobních WEB kamer, u níž se předpokládalo, že by v ní mohlo být zapojeno až 300 milionů lidí! Skromnější modely uvažovaly jen o metropolitních dimenzích s 1,5 milionem lidí, avšak s mnoha typy serverů, které by mohly hlásit stav obsazenosti parkovišť, stav provozu na křižovatkách apod. V tom případě by jen udržování informace o lokalizaci objektů vyžadovalo asi 25000 aktualizací za sekundu [12]. Pro Wikipedia, což je dnes nejrozšířenější světová encyklopedie, se zde testují možnosti efektivní distribuce velkých objemů dat k co nejšir-

šímu okruhu uživatelů s použitím několikastupňové replikace.

Síť PlanetLab používá mnoho uživatelů i pro měření charakteristik chování Internetu – například Google zde má otevřený projekt, který vyhodnocuje dostupnost jejich serverů z různých částí světa. Jiný projekt z této oblasti, který se zaměřil na vzájemnou dostupnost účastníků z různých domén, řeší HP.

Proč je PlanetLab právě tím vhodným prostředím, kde se takovýto výzkum dá provádět? Její přednost spočívá především v tom, že umožňuje uživatelům vytvářet nezávislé aplikace, které mohou běžet v celé sítí vedle sebe a vytvářet tak ucelené virtuální vrstvy sítě. Vrstvy používají společné uzly bez toho, že by se při jejich užití jakkoliv vzájemně ovlivňovaly. Tvůrce nebo uživatel aplikace si může v síti vytvořit svoji vlastní strukturu, se kterou pak může pracovat. Nezřídka takové struktury obsahují stovky uzlů PlanetLabu. Pro identifikaci objektů a uzlů v síti používají vlastní adresaci i vlastní metody vyhledávání dat a směrování toku informací mezi objekty a uzly. Některé z nich používají i vícevrstvovou architekturu. Použijí některý z dostupných nástrojů typu DHT jako obecný základ pro adresaci a vyhledávání objektů a teprve nad ní budují vlastní aplikaci zpracování dat. Příkladem takovéhoto použití je projekt OceanStore nebo projekt Shuttle (bezpečná decentralizovaná distribuce zpráv), který používá v nižší vrstvě systém Tapestry.

Co říci závěrem?

V této prvním informaci o Planetlabu jsme přinesli několik nových informací o tom, jakým směrem se ubírá výzkum v oblasti síťových technologií ve světě. Je tak trochu překvapivé, že o popisované směry výzkumu se v ČR dosud skoro nikdo nezajímal. Asi jsme příliš malá země, kterou v poslední době zajímala především snaha o to, jak se nejlépe prosadit na gigabitových spojích, a samozřejmě také celosvětová gridomanie.

Síť PlanetLab je zajímavá i z mnoha jiných aspektů. Jedním z nich je třeba to, jak byla taková síť postavena, na jakých principech realizuje svoji virtualitu, a proč se stala modelem pro NGI (Next Generation of Internet). Technické řešení Planetlabu si ukážeme v některém z pokračování tohoto článku.

Neméně zajímavá je také skutečnost, že PlanetLab je velice vstřícná ke všem partnerům, kteří ji chtějí používat. Jejím členem se může stát každá akademická organizace, která do ní vloží svůj uzel. Této příležitosti využil i CESNET; nakoupil požadovanou techniku a podal přihlášku, která se v současné době vyřizuje. Doufáme, že během léta se stihnou realizovat všechny instalační práce a od září bude mít i ČR zastoupení v této unikátní celosvětové laboratoři. V naší akademické komunitě se tím významně rozšíří podmínky pro výzkum v dané oblasti. Není to ale jen záležitost CESNETu, který se přímo zapojí do dnes prováděných experimentů. Je to i výzva pro výzkumné a vědecké týmy z našich vysokých škol a vědeckých pracovišť, aby se začlenily s vlastními projekty. PlanetLab nabízí ideální prostředí pro řešení diplomových nebo disertačních prací i pro navázání přímých kontaktů s předními světovými odborníky.

Literatura

[1] Andy Bavier, Mic Bowman, Brent Chun, David Culler, Scott Karlin, Steve Muir, Larry Peterson, Timothy Roscoe, Tammo Spalink, Mike Wawrzoniak. Operating Systém Support for Planetary-Scale Network Services. `http://www.planet-lab.org/`

[2] P.Barham, B.Dragovic, K.Fraser, S.Hand, T.Harris, A.Ho, R.Neugenbauer, I.Pratt and A.Warfield. Xen and the Art of Virtualization. In Proc. 19th SOSP, Lake Georgie, NY, Oct 2003

[3] A.Bavier, T.Voigt, L.Peterson, M.Wawrzoniak. SILK: Scout Path in the Linux, Technical Report. 2002-009, Department of Information Technology, Uppsala University, Uppsala, Sweden 2002

[4] Linux VServers Project, `http://linux-vserver.org/`

[5] Hary Balakrisnan, Frans Kaashoek, David Karger, Robert Morfia and Ion Stoica. Looking up Data in P2P System. Communications of ACM, February 2003, Vol 46, No. 3

[6] D. Anderson, H. Balakrisnan, F. Kaashoek and R. Morris. Resilient Overlay Network. In Proc. 18th SOSP, pages 131-145, Banff, Alberts, Canada, Oct. 2001

[7] I. Stoica, R.Morris, D. Karger, F. Kaashoek and H. Balakrishnan: „Chord: A scalable Peer-to-peer Lookup Service for Internet Applications“. ACM SIGCOMM, San Diego CA, 2001

[8] V. Ramasubramanian and E.G.Sirer. Behive: Expoiting Power Law Query Distributions for O(1) Lookup Performance in Peer to Peer Overlays. MIT, Cambridge, MA

[9] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp and Scotty Shenker. A scalable content-addresable network. In Proc. ACM SIGCOMM 2001, August 2001

[10] M. Harren, J.M. Hellerstein, R. Huebsh, D.T. Loo, S. Shenker and I. Stoica. Complex Querries in DHT-based Peer-to-Peer Networks. In Proc. 1st Int. Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA, Mar 2002

[11] J. Kubiatowitz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Goels, R. Gummandi, S. Rhea, H. Wheatherspoon, W. Wemer, C. Wells and B. Zhao. OceanStore: An Architecture for Global-Scale Persistent Storage. In Proc. 9th ASPLOS, pages 190-201, Cambridge, MA, Nov 2000

[12] Philip B. Gibbons, Bred Karp, Yan Ke, Suman Nath and Srinivasan Seshan. IrisNet: An Architecture for WorldSensorWeb. IEEE CS and ComSoc. Pervasive Computing, OCT-DEC 2003

[13] J. Navrátil, M. Neuman, K. Smejkal. Síť ČVUT v roce 2001. Pražská technika, 2001/4, str. 31-36, ISSN 1213-5348. □

Jak spolupracují Magion a Inet

Jana Kohoutková, ÚVT MU

O tom, že na MU nějakým způsobem spoluexistují informační systémy Magion (specializovaný ekonomický systém) a Inet (intranet pro obecnou komunitu uživatelů MU), vědí čtenáři Zpravodaje z různých článků, za všechny jmenujme alespoň [1] a [2]. Nakolik je však tato spoluexistence řízená a smysluplná, jsme dosud ve Zpravodaji nerozebírali – a tento článek by to měl napravit. Pojďme tedy dát věci do souvislostí a ukázat, že se nedějí živelně (jak jde život a jak usoudí externí dodavatel), ale podle určitých záměrů a systematicky.

1 Nejprve trocha povinné teorie

Při budování informační infrastruktury je nutno brát v potaz řadu hledisek, k nimž v prvé řadě patří tato čtyři:

1. *komu je určena*,
2. *jaké věcné oblasti má pokrývat*,
3. *v jakých technologiích bude realizována*,
4. *kdo budou autoři po stránce a) obsahové neboli metodické, b) informatické*,

jinými slovy *uživatele*, *aplikační oblasti*, *informační technologie* a *dodavatele*.

Ad 1) Uživatelé: Podle rozsahu přístupů k informacím lze *uživatele* univerzitních informačních systémů typově rozdělit do pěti úrovní:

- úroveň „*rektorátu*“, zahrnující vedení univerzity a odborné pracovníky na úrovni rektorátu, kteří mají mít přístup k datům celé univerzity (v aplikační oblasti nebo oblastech, v nichž se pohybují);
- úroveň „*fakulty*“, tedy vedení a odborní pracovníci jednotlivých součástí univerzity, kteří mají mít přístup k datům celé součásti (opět ve „svých“ aplikačních oblastech);
- úroveň „*pracoviště*“, tedy vedení, sekretariáty a odborní pracovníci jednotlivých pracovišť (typicky například referenti majetku či zadavatelé docházky), kteří mají mít přístup k datům v rozsahu svého pracoviště;
- úroveň „*osoby*“, což jsou jednotliví zaměstnanci, studenti a spolupracovníci MU s přístupem k informacím, jež potřebují ke své práci, nebo které se jich týkají či o nich vypovídají,
- úroveň „*světa*“, tedy veřejnosti s přístupy k veřejně publikovatelným datům.

Uživatelů na prvních dvou úrovních je na MU několik set, na třetí úrovni více než tisíc (dílčích pracovišť má MU přibližně 450), na čtvrté úrovni

desetitisíce a na poslední úrovni je počet uživatelů opět o řád vyšší[1].

Ad 2) Aplikační oblasti: Za základní *aplikační oblasti* lze v univerzitním prostředí označit těchto sedm:

- studium a výuka,
- věda a výzkum,
- ekonomika a účetnictví,
- lidské zdroje (personalistika a mzdy),
- knihovny a správa dokumentů a spisů,
- vnější vztahy,
- technické a provozní služby.

Na MU je informační podpora budována ve všech těchto oblastech, přirozeně ve snaze pokrýt je jak šířkou záběru tak kvalitou práce s daty.

Ad 3) Informační technologie: Z *informačních technologií* zmíníme jen přístupy k datům, tak jak to potřebuje hlavní dějová linie tohoto článku, a odborný výklad ponecháme povolanějším autorům, ať již prostřednictvím Zpravodaje nebo jiných médií (o technologiích Inetu pojednávají například články [3] a [4], další informace lze najít přímo v Inetu, v sekci *O Inetu → Všeobecné informace*). Přístupy uživatelů k datům rozdělme na „webové“ a „newebové“. První jsou realizovány prostřednictvím webového (html) prohlížeče a nejlépe splňují požadavek „přístup kdykoli odkudkoli bez bariér“. Druhé jsou realizovány prostřednictvím specializovaných klientů – ať již tzv. *lehkých* v rámci 3vrstvé architektury, nebo *těžkých* ve 2vrstvé architektuře – a jejich síla tkví v „rychlosti a výkonnosti práce s daty“. Webové přístupy nejsou vhodné tam, kde je rozhraní pro přístup k datům velmi členité a dynamické (u takového rozhraní lze s běžným webovým prohlížečem a jazykem html vystačit jen velmi těžko), a naopak jsou nutné tam, kde se jedná o velké počty uživatelů a je vyloučen jiný typ klienta než běžný html prohlížeč – z důvodů licenčních a kapacitních resp. výkonnostních[2].

Ad 4) Dodavatelé: A konečně k *dodavatelům*, tedy k často diskutované otázce, zda „koupit nebo vyvíjet“ neboli kudy vést hranici mezi vlastním vývojem a externími dodávkami: Při šíři záběru aplikačních oblastí, jak byly výše vyjmenovány, není myslitelné, aby si veškerou informační podporu vyvíjela univerzita vlastními silami, a je nutné vhodně zkombinovat vlastní vývoj s pořizováním informačních subsystémů od externích dodavatelů. Externí dodávky jsou rozumné tam, kde je aplikační oblast nějakým způsobem typizovaná, na softwarovém trhu podporovaná, a dodavatel dává záruku odborné specializace a sledování vývoje oblasti včetně vývoje souvisejících předpisů a legislativy; naopak vlastní vývoj je žádoucí tam, kde se jedná o řešení na míru, k němuž univerzita v každém případě musí dodávat analýzu.

Jestliže nyní zkombinujeme, co bylo až dosud napsáno, vycházejí pro uživatelské přístupy k datům závěry:

1. Pro uživatele na úrovni rektorátu a fakult nemůže existovat jeden „všeobjímající“ informační systém vyvíjený vlastními silami MU. Realita je taková, že vedle sebe musí spoluexistovat vícenásobné a úžeji specializované subsystémy, kombinující webové a newebové přístupy (vzhledem k povaze – tj. komplexnosti a náročnosti – prováděných operací převládají přístupy newebové) a vyvíjené dílem vlastními silami, dílem externími dodavateli.
2. Naopak pro uživatele na úrovni dílčích pracovišť, jednotlivých osob a samozřejmě světa se budují integrované, průřezové systémy, a to – vzhledem k počtu uživatelů – jednoznačně ve webových technologiích, tedy strukturovaný intranet[3] a veřejná internetová prezentace. Přirozeně převládá snaha budovat tyto systémy vlastními silami, aby uživatelé měli informace pod co nejmenším počtem střech.

A pro vlastní vývoj nastávají tyto úkoly:

- *rozšiřovat přístup k informacím* na katedry, k osobám a do světa tam, kde přístupy

[1] Od konce roku 1998 byly zaznamenány přístupy na stránky www.muni.cz z více než půl miliónu různých počítačů (IP adres).

[2] Příkladem ze života je tady limitovaná kapacita terminálových serverů, na nichž jsou na MU provozováni klienti systému Magion.

[3] Na MU jsou provozovány dva průřezové celouniverzitní intranety, a sice IS MU (přednostně zaměřený na oblast studia a výuky) a Inet MU (specializující se na oblast ekonomiky, personalistiky a mezd). Oba systémy používají společnou – centrální – evidenci osob a osobních přístupových atributů (loginů a hesel) a řadu dalších integrujících prvků.

na úrovni rektorátu a fakult obhospodařují subsystémy externích dodavatelů;
- *budovat informační podporu* pro všechny úrovně uživatelů v těch oblastech, které jsou *specifické* pro univerzitní prostředí, anebo pro ně neexistuje kvalitní nabídka podpory na softwarovém trhu;
- *zajišťovat integrační vazby* mezi dílčími subsystémy.

Tímto shrnutím budiž teorii učiněno zadost, a nyní se již pojďme podívat, jak se teorie snoubí s praxí v jedné z klíčových aplikačních oblastí – ekonomické.

2 Obrázek z praxe: Magion a Inet

Informační podporu v oblasti ekonomiky a účetnictví primárně poskytuje Masarykově univerzitě Ekonomický informační systém Magion (dále *EIS Magion* nebo jen *Magion*) externího dodavatele Magion System, a.s. Systém, implementovaný ve 2vrstvé architektuře (aplikace těžkého klienta komunikují přímo s databází), je provozován na klastru terminálových serverů a má v současné době okolo 350 uživatelů, převážně z Ekonomického odboru RMU, z ekonomických oddělení děkanátů fakult a z centrálních ekonomických útvarů dalších součástí MU.

Duálním systémem k EIS Magion je Inet MU, vyvíjený na ÚVT MU a řešený v 3vrstvé architektuře, jejíž front-end tvoří html prohlížeč (prohlížeč komunikuje s aplikačním serverem a ten s databází). Provozní statistiky ukazují, že Inet používá téměř 80% zaměstnanců MU, zhruba 60% studentů a okolo 40% externistů (tj. pracovníků na dohody), tedy celkem více než 20 tisíc osob.

EIS Magion tvoří moduly *Hlavní účetní kniha*, *Pohledávky*, *Závazky*, *Cestovní náhrady*, *Pokladna*, *Banka*, *Majetek*, *Sklady*, *Objednávky* a *Rozpočty*. Ekonomickou sekci Inetu tvoří podsekce *Banka*, *Pokladna*, *Účetní sestavy*, *SUPO*, *Majetek*, *Pohledávky* a *Projekty*. V následujících odstavcích se na spolupráci Magionu a Inetu v jednotlivých ekonomických podoblastech podíváme zblízka.

2.1 Účetní sestavy

Účetní sestavy byly historicky první aplikací ekonomické sekce Inetu, a Inet jimi plní svou úlohu *rozšiřovat přístup k datům*, kmenově udržovaným v EIS Magion, na další uživatele. Dalšími uživateli jsou v tomto případě *osoby* (*Účetní sestavy za zakázky* jsou určeny vedoucím zakázek a osobám jimi delegovaným) a *pracoviště* (*Účetní sestavy za pracoviště* jsou určeny vedoucím pracovišť a opět jimi delegovaným osobám).

Účetní sestavy jsou určeny pouze pro čtení a jejich obsah je získáván z dat EIS Magion, stejně jako jsou z dat Magionu (resp. z dat personálního systému) získávána implicitní přístupová práva; Inet vede ve své vlastní režii pouze data o explicitních přístupových právech[4]. Poznamenejme, že v EIS Magion pojem implicitního přístupového práva neexistuje – tam je nutno explicitně přidělit přístup k zakázce každému vedoucímu zakázky, jakkoli je v systému jako vedoucí zakázky evidován, a podobně je nutno explicitně přidělit přístup k pracovišti každému vedoucímu pracoviště, jakkoli je jako vedoucí pracoviště evidován v personálním systému. Stačí si uvědomit, kolik je na MU pracovišť a zakázek[5], aby bylo zřejmé, že zpřístupnění účetních sestav všem vedoucím pracovišť a zakázek by prostřednictvím Magionu nebylo administrovatelné a že role Inetu je tu nezastupitelná. Nicméně hlavním důvodem pro existenci účetních sestav v Inetu stále zůstává záměr budovat přístup k informacím na úrovni jednotlivých osob a pracovišť pod co nejméně střechami, tedy v jednotném prezentačním a navigačním prostředí.

2.2 Banka a pokladna

Aplikace Banky a Pokladny vznikly v ekonomické sekci Inetu poměrně nedávno, v souvislosti s vývojem systému SUPO, o němž bude řeč dále v části 2.5 Inet jimi plní úlohu *zajišťovat integrační vazby* mezi dílčími subsystémy a v rámci integrace přidává další velmi podstatné hodnoty.

[4] Přístupová práva mohou být *implicitní* (vyplývající z nějakého kontextu, například právo vedoucího pracoviště k účetním sestavám za pracoviště nebo právo vedoucího ekonomického útvaru fakulty k účetním sestavám za všechny zakázky fakulty apod.) nebo *explicitní* (jmenovitě přidělená – delegovaná, například právo přístupu k účetním sestavám za zakázku delegované vedoucím zakázky další osobě).

[5] Zakázek je aktuálně více než dva tisíce.

Aplikace Banky zajišťují provoz tzv. *bankovního rozhraní*, jímž se do modulu Banka EIS Magion hromadně předávají bankovní příkazy k inkasu či úhradě z jiných, externích systémů a naopak externím systémům se hromadně předávají informace o výsledku provedení těchto příkazů, přičemž párování bankovních výpisů (tj. informací o výsledku provedení příkazů) na bankovní příkazy provádí právě bankovní rozhraní. Vedle systému SUPO využívá bankovní rozhraní stipendijní systém (pro výplaty stipendií s výjimkou ubytovacích) a studijní systém IS MU (pro výplaty ubytovacích stipendií), do budoucna se počítá s využitím bankovního rozhraní například pro platby za přijímací řízení.

Aplikace Pokladny, obdobně jako v případě Banky, zajišťují propojení mezi modulem Pokladna EIS Magion a systémem SUPO. Implementují jak příjmovou tak výdajovou pokladnu, jíž lze do systému SUPO vkládat nebo z něj vydávat finanční hotovost, se všemi potřebnými vazbami do EIS Magion. Těchto pokladen je na MU jen omezený počet a ani do budoucna se nepočítá s jejich významným nárůstem, o širším až širokém využití pokladních aplikací Inetu se však uvažuje v souvislosti se zákonnou povinností zavést od ledna 2007 registrační pokladny.

2.3 Majetek

První aplikace Majetku vznikly v Inetu v létě 2003, a od té doby se vytrvale dožadují pozornosti vývojářů; nejneodbytnějšími se staly v loňském roce v souvislosti se zaváděním čárového kódu pro evidenci a inventarizaci majetku. V oblasti majetku plní Inet ve vztahu k Magionu všechny tři úlohy vyjmenované na konci první části tohoto článku, tedy *rozšiřující*, *vývojovou* i *integrační*.

Úlohu *rozšiřovat přístup k informacím* kmenově spravovaným v EIS Magion plní jednak výpisy a sestavy (osobní přehledy, nálezy majetku, sestavy majetku za pracoviště), a dále aplikace pro práci s majetkem (přiřazování osob a místností, editace technických parametrů, zpracování návrhů a protokolů k převodům nebo vyřazení majetku, tisky inventárních štítků s čárovým kódem). Tyto aplikace slouží – podobně jako účetní sestavy diskutované v části 2.1 – jak jednotlivým *osobám* tak *pracovištím* (vedoucím pracovišť a referentům majetku).

Úlohy *budovat specifickou informační podporu* se Inet ujal loni, v souvislosti s inventarizací majetku za pomoci snímačů čárového kódu. Tuto činnost EIS Magion nijak nepodporoval a ani o ní neuvažoval, a vybraný dodavatel programového vybavení snímačů neměl s Magionem žádné obchodní vztahy. Implementaci tedy zajistil Inet. O výsledku dosti podrobně referoval článek [5], proto jen zopakujme, že se jedná o aplikace sloužící jak úrovním rektorátu a fakult tak úrovni pracovišť, a doplňme, že k loňským aplikacím pracujícím nad inventurní databází (která se jednou za rok, k datu zahájení podzimní inventury, účelově vytváří exportem dat z centrální databáze majetku) přibyly letos aplikace pro celoroční práci se snímačem přímo nad centrální databází majetku.

Úloha *zajišťovat integrační vazby* mezi dílčími subsystémy opět souvisí s čárovým kódem a inventarizací – Inet slouží jako prostředník pro přenos dat mezi EIS Magion (inventurní resp. centrální databází majetku) a programovým vybavením snímačů.

2.4 Pohledávky

Aplikace Pohledávky je v Inetu téměř neviditelná, nicméně nesmělá úvaha vývojářů, že by se bez ní MU mohla obejít (a to tak, že by zjednodušenou podobu požadované funkcionality zajistil Magion), byla loni v létě zastavena hned v zárodku. Jedná se opět o *integrační vazbu* na Magion s nezanedbatelnou přidanou hodnotou v podobě důkladných datových kontrol, tentokrát z lokálního systému jednoho pracoviště MU, kde se vede evidence o skladovaném zboží, zákaznících, objednávkách a vystavených fakturách. Údaje o pohledávkách vázaných k lokálně vystaveným fakturám se prostřednictvím Inetu dávkově přenášejí do Magionu, kde již jejich úhrady sleduje ekonomické oddělení příslušné fakulty. Inetovská aplikace, která umožňuje převzít dávku dat, zkontrolovat ji a vložit do databáze Magionu, slouží zatím jen jednomu lokálnímu systému, ale je obecně využitelná libovolným dalším systémem generujícím pohledávky.

2.5 SUPO

Systém SUPO (neboli Systém úhrad pohledávek za osobami, dříve nazývaný Clearing) je budován pod střechou Inetu jako nedílná součást ekonomického systému MU, podrobněji viz [6]. Inet tady opět plní úlohu *budovat specifickou informační podporu*, která není pokryta EIS Magion ani na úrovni rektorátu a fakult, a rovněž úlohu *integrační*.

Ve vztahu k Magionu představuje SUPO specializovaný modul, který vede evidenci o „atomických" pohledávkách za osobami, zajišťuje hromadné úhrady těchto pohledávek (přednostně bezhotovostní cestou), zpřístupňuje informace o pohledávkách i úhradách a poskytuje prostředky pro předávání souhrnných informací do účetnictví Magionu. Pohledávky přitom SUPO sbírá z různých externích systémů evidujících služby poskytované Masarykovou univerzitou osobám, a informace o provedených úhradách pak těmto systémům poskytuje zpět. Systém je určen všem úrovním uživatelů z MU – od odborů rektorátu (ekonomického, personálního, právního aj.) přes odborné útvary součástí (opět ekonomické, personální aj.), dílčí pracoviště až po jednotlivé osoby (klienty SUPO, jimiž jsou především studenti a zaměstnanci MU).[6]

2.6 Rozpočty a projekty

Nejmladším reprezentantem spolupráce mezi Magionem a Inetem jsou Projekty, které rozšířily ekonomickou sekci Inetu před dvěma měsíci. Jedná se zatím jen o zárodek budoucího systému ISEP (Informačního systému pro evidenci projektů), který má podobně jako SUPO sloužit všem úrovním uživatelů z MU (k odborným útvarům se tu řadí i útvary pro vědu a výzkum, na úrovni osob se jedná o řešitele projektů), a rovněž veřejnosti (informace o řešených vědecko-výzkumných projektech mají i svou veřejnou část, určenou k publikování na `www.muni.cz`).

Úlohou Inetu je tady jak *rozšíření přístupu k informacím* kmenově spravovaným v EIS Magion na další uživatele tak *vybudování specifické informační podpory* pro všechny úrovně uživatelů. Ve vztahu k Magionu se jedná o to, aby rozpočtové sestavy projektů řešených na MU (v prvé řadě vědecko-výzkumných projektů, ale obecně jakýchkoli ekonomicky podchycených aktivit), které čerpají data z ekonomické databáze Magionu, byly dostupné všem úrovním uživatelů – podobně jako je tomu u účetních sestav, o nichž jsme mluvili v části 2.1. Samotné čerpání dat z databáze Magionu však zcela jistě nebude stačit. V uživatelských požadavcích je totiž zahrnuta i možnost modelovat čerpání rozpočtů, což znamená kombinovat data z rozpočtů, účetnictví a objednávek (všechna získávaná z databáze Magionu) s plány budoucího čerpání, které si budou řešitelé projektů udržovat prostřednictvím Inetu mimo databázi Magionu.

3 Výhledy do budoucna

Spolupráce mezi Magionem a Inetem, jak byla popsána v předchozích odstavcích, zatím probíhá pouze na úrovni surových dat, uložených v relačních datových strukturách. Aplikace Inetu tedy čtou data přímo z databáze Magionu, a také do ní přímo zapisují, „povolení" čtení a zápisu je dáno pouze neformální dohodou mezi firmou Magion a vývojovým týmem Inetu. V právě probíhající diskusi o zpřístupňování dat rozpočtů (viz 2.6) se však na straně Magionu objevují první vlaštovky ochoty vyvážet i části programového kódu. Vývoz by měl mít podobu webových služeb (o technologii viz například [7]), jimiž by se na vyžádání poskytovala již nikoli surová, ale potřebně předzpracovaná data, a to v dokumentované a stabilizované formě. Inet coby odběratel by tím byl odstíněn od případných změn ve vnitřních strukturách vyvážených dat a programů. Pokud s těmito vlaštovkami skutečně přijde jaro, bude to pro spolupráci Magionu s Inetem znamenat kvalitativní skok kupředu – a rádi o tom ve Zpravodaji podáme svědectví.

[6] Ve vztahu k SUPO zastupuje nyní součásti pouze SKM (coby provozovatel ubytovacího systému), dílčími pracovišti jsou jednotlivé koleje a osobami ubytovaní studenti. Do budoucna je však SUPO otevřeno libovolnému systému, který vede evidenci o službách poskytovaných osobám, a jehož provozovatel má zájem přenést na SUPO pracnost a režii související se zajišťováním úhrad za tyto služby a jejich účetním zpracováním.

Systém Magion, provozovaný na MU, zatím pokrývá oblast ekonomiky a účetnictví (včetně správy majetku, skladové evidence, objednávek a rozpočtování). V březnu letošního roku uzavřela MU se společností Magion smlouvu o dodávce dalších modulů, a sice modulů pro podporu personalistiky a mezd[7]. Nové moduly mají být uvedeny do plného provozu tak, aby zajistily zpracování mezd od ledna 2007, a bude pro ně platit totéž co pro moduly ekonomické: budou poskytovat informační podporu uživatelům na úrovni rektorátu a fakult, zatímco dalším úrovním uživatelů bude přístup k personálněmzdovým datům poskytovat Inet (pracovištím a osobám) resp. www.muni.cz (světu). Je tedy otázkou jen několika málo měsíců, než se aplikace vybudované nad datovou základnou systému Magion objeví i v personálně-mzdové sekci Inetu a nahradí stávající aplikace pracující nad databází Informix. I o tomto rozšíření spolupráce Magionu s Inetem, jakmile bude hotovo a v provozu, budeme na stránkách Zpravodaje rádi referovat.

Literatura

[1] P. Vokřínek. *EIS Magion na MU*. Zpravodaj XV, č. 5, s. 1–4.

[2] J. Kohoutková. *Informační infrastruktura na MU*. Zpravodaj XI, č. 5, s. 5–8.

[3] J. Měcháček. *XML a Java*. Zpravodaj XII, č. 2, s. 9–12.

[4] J. Ocelka. *Poskytnutí autentizace v informačních systémech*. Sborník *DATAKON 2003*, 259–264.

[5] J. Kohoutková, Z. Machač. *S čárovými kódy na majetek*. Zpravodaj XVI, č. 3, s. 3–6.

[6] A. Jurtíková, J. Ocelka, J. Staudek. *Clearing MU – zúčtovací systém pro bezhotovostní uhrazování poskytovaných služeb*. Zpravodaj XVI, č. 1, s. 11–13.

[7] M. Kuba. *Web Services*. Zpravodaj XIII, č. 3, s. 9–14.

[7] Moduly nahradí a rozšíří současný personálněmzdový systém MU, realizovaný v jazyce 4GL nad databází Informix, což je platforma, kterou se MU před dvěma lety rozhodla opustit ve prospěch perspektivnější Oracle. S přechodem na Oracle je bohužel nutno opustit i nadstavbu ve 4GL…

Tipy z Inetu: Rezervace on-line

Jana Haluzová, ÚVT MU

Redakční poznámka:

Na Masarykově univerzitě jsou provozovány a rozvíjeny dva celouniverzitní intranetové systémy, které přes web poskytují služby autentizovaným uživatelům: systém ***IS MU*** *(primárně zaměřený na studijní oblast a vyvíjený týmem na FI MU) a systém* ***Inet*** *(primárně zaměřený na správně-ekonomickou oblast a vyvíjený týmem v ÚVT MU). Oba systémy jsou dnes již značně rozsáhlé a nabízejí svým uživatelům velmi bohaté spektrum služeb. Zejména pro nové uživatele nemusí být vždy snadné se v nabízených službách zorientovat a naučit se jich využívat. Proto ve Zpravodaji ÚVT otevíráme nový seriál článků s cílem představit uživatelům MU vybrané služby správně-ekonomického systému Inet. Jako první jsme zvolili aplikaci zaměřenou na rezervace místností a předmětů, uvedenou do provozu před několika týdny.*

Rezervace on-line ve dvou větách

Jedná se o systém umožňující rezervovat vybrané místnosti nebo předměty v majetku MU, určený fakultám nebo pracovištím MU, které místnosti či majetek užívají. Aplikace je přístupná všem zaměstnancům MU na adrese `https://inet.muni.cz/app/provoz/rez_obj` (menu Inetu: Služby ICT/FM → Provozní služby → Rezervace).

Podrobnější popis aplikace

Předchůdcem a inspirací aplikace *Rezervace online* bylo programové vybavení vytvořené v roce 2001 pro potřeby Ústavu výpočetní techniky jako součást jeho lokálního intranetu. Kterákoli osoba z ÚVT mající přístupová práva do intranetu si mohla zarezervovat místnost (zasedačku ÚVT) nebo předmět majetku (dataprojektor) a „své“ záznamy mazat. Zároveň byli určeni „superuživatelé“ (pracovnice sekretariátu) mající právo provést rezervaci i za jiného člověka a – popřípadě – kterýkoli záznam rezervace smazat. V celouniverzitní rezervační aplikaci byly oba tyto principy zobecněny tak, aby vyhovovaly očekávaným požadavkům uživatelů z celé MU.

Účelem aplikace je umožnit lidem zaměstnaným na určitém pracovišti nebo pracovištích MU rezervovat si v časové ose nějakou místnost či předmět, určený k vypůjčení. Jde tedy o princip „kdo – co – kdy“ (kdo si zarezervuje, co si zarezervuje a v jakém čase), jímž se k danému objektu rezervace vytvoří fronta požadavků.

- Pod pojmem KDO jsou implicitně míněni zaměstnanci v pracovním poměru nebo na dohodu, právo však lze přidělit i dalším osobám (za podmínky, že jsou vedeny v centrální evidenci MU). Přístup osoby k objektu tedy buď automaticky vyplývá z pracovního poměru, nebo je speciálně přidělen.
- CO znamená objekt rezervace. Místnosti mohou být jak v budovách, které jsou majetkem MU, tak v budovách pronajatých; podmínkou je existence místnosti v centrální evidenci MU (viz `https://inet.muni.cz/app/fm/prehled_mistnosti`). Předmětem v majetku MU jsou pak míněny movité majetky, typicky notebooky nebo dataprojektory. Obecně lze rezervovat jakoukoliv místnost evidovanou v číselníku místností nebo jakýkoliv movitý majetek vedený v evidenci majetku MU.
- KDY je interval doby výpůjčky. Ten je dán počátečním a koncovým datem a časem rezervace. Aplikace obsahuje škálu kontrol zajišťujících smysluplnost a konzistenci časových intervalů (jeden interval se nesmí překrývat s druhým, nelze provádět rezervace do minulosti, nevyplněné údaje se odhadují a automaticky doplňují).

Přístupy k objektu (resp. práva k rezervaci) jsou dvojího druhu a každý z nich má tři varianty:

Hromadný přístup zaměstnanců pracoviště: Právo k objektu rezervace se přiděluje pracovišti, s implicitní působností na všechny zaměstnance (podle celouniverzitní evidence pracovních poměrů a dohod), a může být nastaveno následovně:

- pouze prohlížení,
- zápis/rušení „vlastních“ záznamů a prohlížení „cizích záznamů“,
- zápis/rušení všech záznamů (právo „superuživatele“).

Individuální přístup osoby: Právo k objektu se přiděluje osobě explicitně, bez ohledu na její pracovní poměr. Právo má opět tři varianty jako u předešlého přístupu.

Vylepšením přístupových práv prvního typu je možnost přidělit právo k objektu pracovišti včetně podpracovišť, což znamená zaměstnancům pracoviště i jeho podpracovišť na všech úrovních podřízenosti. Vyskytne-li se případ, že osoba má k objektu více práv, ať již z titulu příslušnosti k pracovišti nebo z titulu speciálních práv, uplatní se u ní vždy právo nejsilnější.

Praktické použití

V současné době je rezervační aplikace využívána na ÚVT MU. Všichni zaměstnanci ÚVT mají možnost rezervovat na své jméno zasedací místnost a přenosný dataprojektor, superuživatelské právo mají pracovnice sekretariátu. Kromě toho mají pracovníci dvou menších podpracovišť ÚVT možnost rezervovat si „cestovní“ notebook, k němuž jiná pracoviště přístup nemají; právo superuživatele má v tomto případě pracovník, jemuž je notebook svěřen (má jej v inventárním soupisu).

Jak již bylo řečeno, aplikace byla vytvořena tak, aby ji mohlo používat kterékoliv pracoviště MU. Je svázána s celouniverzitními číselníky osob, místností a předmětů v majetku MU, a je přístupná všem zaměstnancům univerzity na adrese uvedené v úvodu, s implicitně prázdnou nabídkou rezervovatelných objektů. K plnohodnotnému využití stačí málo: do nabídky objektů k rezervaci vložit požadovanou místnost nebo předmět a do evidence práv přidat potřebná práva. Obojí provedou na vyžádání správci systému Inet.

Zkuste si sami pro své akce rezervovat přes web potřebnou místnost nebo potřebný předmět z majetku MU. Požádat o vložení objektu a přístupových práv lze e-mailem na adrese `maj-inet@ics.muni.cz`. □

Další krok v záznamu přednášek

Pavel Šiler, FI MU

1 Úvod

Každá činnost, které se skupina lidí po nějakou dobu věnuje s invencí a pílí, má za následek rozvoj a zdokonalení. Tento článek se čtenáře pokusí přesvědčit, že nejinak je tomu i v oblasti záznamů přednášek [1]. Důkazem dokumentujícím nové možnosti a kvalitativní zlepšení bude popis konkrétního provedení záznamu vybraného přednáškového cyklu.

Během podzimního semestru 2005 jsme v rámci e-learningového kurzu k předmětu M1510 *Matematická analýza 1* za podpory rozvojového projektu „E-learning na MU: Multimediální a IT podpora“ prof. RNDr. Zuzany Došlé, DrSc. přikročili k nahrávání uceleného cyklu přednášek. Jednalo se celkem o záznam v rozsahu 12 dvouhodinových přednášek.

Zpočátku tento projekt vypadal jako rutinní záležitost. Záznam přednášek matematiků však patří k těm nejproblémovějším, protože je nutné kromě ostatních multimediálních podpor výuky (projektor, vizualizér, Mimio, ...) co nejlépe zaznamenat i klasický zápis křídou na tabuli. Zde nastává řada problémů s kontrastem, leskem a rozlišením. Proto snaha o co nejlepší záznam tohoto kurzu vedla k řadě nových poznatků a zkušeností a sehrála jednu z klíčových rolí pro rozvoj našich dalších schopností.

2 Režie záznamu

Po rozhodnutí zaměřit se na kurz M1510 bylo nutno zamyslet se nad celkovým přístupem k práci a zvolit optimální způsob režie. První možností bylo využít automatický záznam pevně zabudovanými prostředky učebny D3 na Fakultě informatiky MU, druhou (pracnější) variantou bylo natáčet vše ručně.

Prof. Došlá využívá při svých přednáškách pouze tabuli a její projev je poměrně dynamický. Proto jsme hned upustili od automatizovaného záznamu. Tento způsob byl sice technicky možný, ale nastavení kamery tak, aby bylo dokonale čitelné písmo na tabuli, by se rozcházelo s dynamickým projevem přednášející. Přestože by byl takový postup technicky zcela v pořádku, výsledek by neodpovídal celkovému záměru díla.

Rozhodli jsme se tedy přistoupit k ručnímu natáčení. Navíc jsme jednoznačně upřednostnili čitelnost písma na tabuli před sledováním výkladu přednášející. Filmařsky by sice bylo správné sledovat při výkladu prof. Došlou, ale významově, bez použití slidů, bylo nutné dopřát divákovi dostatek času na vstřebání faktů psaných na tabuli. Automatický záznam se také pořizoval, ale pouze jako záloha a pro srovnání a ověření správnosti předpokladů uvedených výše.

3 Problém kvality zvuku

Hned po první přednášce se ukázalo, že kvalita záznamu neodpovídá našim představám. Zatímco obraz dosahoval běžného standardu a odpovídal použitým prostředkům, zvuk ve své kvalitě, dané vestavěným mikrofonem v kameře, za obrazem silně pokulhával.

Tomu, kdo není seznámen s využíváním záznamů, se může zdát řešení problému kvality zvuku zbytečně složité. Zde je však třeba připomenout, že kvalitní zvuk je základním ergonomickým požadavkem. Zvuk je nositelem značné části informace v záznamu a jeho kvalita je pro kvalitu záznamu velmi důležitá. Předpokládáme, že záznamy budou sledovány až několik hodin souvisle a nekvalitní zvuk negativně ovlivňuje vnímání posluchače a zvyšuje jeho únavu.

Co tedy vlastně máme k dispozici? Základní a nejjednodušší způsob je použití vestavěného mikrofonu v kameře. Další možností je použít kombinaci směrových a všesměrových mikrofonů.

V prvních záznamech byl tedy původní zvuk pořízený vestavěným mikrofonem nahrazen zvukovou stopou z automatického záznamu. Ta je pořizována klopovým bezdrátovým mikroportem SENNHEISER a výsledná kvalita je o několik řádů vyšší. Celkově byl tento způsob sice funkční, leč poněkud neproduktivní, protože konečné zpracování se protáhne o několik hodin práce ve střižně při synchronizaci nové zvukové stopy s obrazem.

Obecně lze říct, že špatná zvuková kvalita je průvodním znakem téměř veškeré video tvorby prováděné mimo velká studia. Tvůrci se zaměřují

především na obrazovou kvalitu a zvuk ponechávají většinou na vestavěných mikrofonech kamer nebo na jednoduchých mikrofonech připojených ke kameře.

Použití směrového mikrofonu jsme také zavrhli, a to z obavy nestejné úrovně hlasitosti při sledování tabule a přednášející. Štáb pro pořizování záznamu by se musel rozšířit o mikrofonistu, více či méně úspěšně sledujícího pohyb přednášející a kamery. Podle našich představ by měl stačit pro pořízení záznamu jeden člověk.

Při přednášení se však používá bezdrátový mikroport SENNHEISER špičkových kvalit, jehož přijímací jednotka je napevno zabudována v katedře. Uvědomili jsme si, že počet přijímačů, které snímají vysílání jednoho mikrofonu, není omezen. Proto jsme úspěšně odzkoušeli použití dalšího přijímače naladěného na stejnou frekvenci jako použitý klopový mikrofon a připojeného ke kameře. Tímto jsme dosáhli stejné kvality zvuku jako u záznamu automatizovaného, bez nutnosti záznamy ručně synchronizovat.

Podobná konfigurace nebyla nikdy předtím použita. Zpočátku bylo pracné najít vhodné nastavení, protože přijímač mikroportu není určen pro přímé připojení ke kameře. Další zvýšení kvality přineslo zakoupení zvukového mixážního pultu MACKIE CFX12 MKII. Dovoluje nám totiž odstranit zvuky v těch frekvenčních rozsazích, kde působí pouze rušivě. Dnes toto zapojení používáme zcela standardně, podle okolností i bez mixážního pultu.

Použitý mikroport velice důrazně potlačuje okolní prostředí, takže v záznamu je hlas přednášejícího dominantní. Při nahrávání přednášky je tento jev žádoucí, při pořizování záznamu jiného charakteru by bylo třeba použít ještě všesměrového mikrofonu a ruch okolního prostředí do záznamu řízeně přimíchávat.

4 Režijní zkušenosti

Další velmi zajímavou zkušenost jsme získali při vlastní režii záznamu. Prof. Došlá se na poli e-learningu aktivně angažuje a v minulosti již natočila několik matematických přednášek na video. Tyto nahrávky byly více či méně uměle režírovány. Výsledky, hlavně s vysloveně studiově komponovanými záznamy, byly poměrně rozpačité a působily velmi nepřirozeně. Naproti tomu přednáška provedená a zaznamenaná v přirozeném prostředí s běžnými studenty v publiku snesla i ta nejpřísnější kritéria. Projev před kamerou a bez kamery byl zcela shodný.

Z našich zkušeností vyplývá, že nejlepšího výsledku se dosáhne při natáčení ve zcela přirozeném prostředí pro přednášejícího, pokud možno bez omezujících požadavků. Vyučující, i když je dokonale schopen veřejné prezentace, není herec, a nelze po něm chtít okamžitou adaptaci na jakékoliv prostředí. Učitel má navíc za cíl, aby divák shlédl jeho vystoupení jednou a nabyté poznatky mu vydržely pokud možno do konce života. V herectví je taková snaha poněkud kontraproduktivní. Herec se navíc může spolehnout na režiséra, kostymérku a konečně i autora, takže případný neúspěch se rozdělí. Učitel naproti tomu prezentuje výhradně sám sebe a svoje nabyté znalosti, což jej samozřejmě nutí být ve svém projevu značně opatrným.

Tato teorie se potvrdila při nutnosti přetočit jednu z prvních přednášek pro indispozici přednášející. Repríza se konala opět s publikem, v posluchárně plně obsazené studenty, kteří si tak přišli část látky na konci cyklu zopakovat. Rozdíl je patrný pouze v zimním stylu oblečení přítomných, ale celkový dojem je stejný jako u přednášek točených „v premiéře“.

Dalším podstatným vylepšením bylo pořizování záznamu přímo v digitálním streamu na harddisk notebooku bez použití kazet. Disponujeme maximálně 80minutovými kazetami a přerušení přednášky při výměně kazety je velmi rušivé. Přednášející si potřebuje udělat pauzu podle svého plánu, nikoliv tehdy, kdy nám dojde kazeta. Navíc dosáhneme velké úspory času, protože převedení záznamu z pásku na harddisk počítače pro další zpracování trvá stejně dlouho jako samotný záznam.

Zpracování ve střižně a kódování výsledného produktu již probíhalo běžnými postupy. Na poslední chvíli jsme se ještě rozhodli ke zpracování celého cyklu přednášek v DVD kvalitě a vytvoření šesti DVD, vždy po dvou přednáškách.

5 Závěr

Co tedy provedení tohoto záznamu přineslo? Hlavně poznání, že jakékoliv podobné dílo je našimi prostředky proveditelné. Ze strany přednášejícího se není čeho bát, protože vliv standardního prostředí zcela překryje negativní působení přítomnosti kamer, a jeho projev je zcela přirozený.

Technicky je třeba nasadit ty nejlepší prostředky, jak pro video a hlavně pro audio část. Právě audio bývá dost často podceňováno a v kontrastu s dobře provedeným videem dokáže celkový dojem hodně pokazit.

Celá akce musí být dobře naplánována. Nahrávací řetězec se stává při použití pokročilých postupů dost složitý, a pokud chceme dobrý výsledek, musí být vše dobře odzkoušeno. Při samotném průběhu natáčení není vhodné cokoliv zásadního měnit. Přináší to pak rozdíl mezi jednotlivými částmi záznamu a i přechod k vyšší kvalitě působí negativně. Velmi důležité pak je počítat s dobou pro provedení změn, a to i přetočení některé části záznamu. Může se vyskytnout jak indispozice přednášejícího tak problém samotné techniky.

Musí být vždy zcela jasné, k čemu bude záznam použit. Jen tak se dá zvolit vhodný způsob a režie záznamu, a také formát a komprese výsledného díla. Důležité je dohodnout i takové detaily, jako například přesné znění a tvar titulků. Jen tak se lze vyhnout případnému rozčarování po dokončení práce, kdy je provedení změn nejobtížnější. Drobná změna ve znění titulku znamená mnoho hodin práce navíc, celý export totiž musí proběhnout znovu.

Vzhledem k tomu, že naše vybavení je na dostatečné technické úrovni, lze ostatní podmínky splnit. Proto můžeme zodpovědně říct, že přípravě další podpory pro e-learningové kurzy v cestě nic nestojí.

Literatura

[1] E. Hladká, M. Liška. *Přednášky ze záznamu na FI MU.* Zpravodaj Ústavu výpočetní techniky Masarykovy univerzity v Brně, Brno, Masarykova univerzita v Brně. ISSN 1212-0901, 2003, vol. XIII, no. 4, s. 6–8. □

Bezpečná komunikace v praxi – první krůčky

Kamil Malinka, ÚVT MU

V minulém čísle Zpravodaje ÚVT byl zveřejněn článek [1], který se zabýval problematikou bezpečnosti elektronických dat a elektronické komunikace. Vyvolal poměrně velkou čtenářskou odezvu. Řada lidí se cítila článkem oslovena; netušila ale, jak zásady bezpečné komunikace uvést do praxe na svém vlastním osobním počítači. Tento článek má za úkol poskytnout jakýsi jednoduchý návod pro první praktické seznámení s bezpečnostní technologií v oblasti e-mailové komunikace. Je zaměřen na uživatele operačního systému MS Windows používající – na MU hojně rozšířené – poštovní klienty ThunderBird resp. Mozilla.

Enigmail

Enigmail je open-source rozšíření (plugin) e-mailového klienta ThunderBird resp Mozilla, který umožňuje uživateli přístup k ověřování a šifrování zpráv prostřednictvím volně dostupného softwaru GnuPG (multiplatformní implementace standardu OpenPGP – viz RFC2440, nahrazujícího komerční šifrovací software PGP). Tento plugin umožňuje kompletní správu OpenPGP klíčů, šifrování/podepisování zpráv při odesílání a dešifrování/ověřování zpráv při jejich přijímání.

Pro využívání Enigmailu je třeba nejprve nainstalovat GnuPG, a dále přímo v aplikaci ThunderBird přidat samotné rozšíření. Českou lokalizaci a všechny potřebné instalační balíčky lze získat například na serveru `http://enigmail.spi.cz`. Po instalaci doplňku a následném restartu poštovního klienta se v nástrojové liště objeví nová záložka – OpenPGP. Pomocí ní lze provádět veškeré požadované funkce, především:

a) podepisovat své e-maily elektronickým podpisem; ten umožňuje příjemci ověření autentičnosti (autorství e-mailu nelze zpochybnit) a ověření integrity (e-mail nebyl cestou od odesílatele k adresátovi změněn);
b) šifrovat obsah e-mailu (utajení obsahu zprávy pro kohokoliv kromě adresáta);

c) ověřovat autentičnost/integritu přijatých e-mailů opatřených elektronickým podpisem;
d) dešifrovat obsah přijatých zašifrovaných e-mailů;
e) kompletní správu OpenPGP klíčů (jak vlastních privátních klíčů tak i cizích veřejných klíčů).

Elektronický podpis a šifrování zpráv – stručné opáčko

Zopakujme stručně jak funguje elektronický podpis u e-mailových zpráv:

- u odesílatele se pomocí hashovací funkce vypočítá z textu zprávy kontrolní součet;
- tento kontrolní součet je zašifrován privátním klíčem odesílatele a odeslán e-mailem jako podpis;
- příjemce rozšifruje podpis veřejným klíčem odesílatele (ověření autentičnosti), a získá tím kontrolní součet obdržené zprávy;
- příjemce vypočítá vlastní kontrolní součet přijaté zprávy a oba kontrolní součty porovná (ověření integrity).

Postup při výměně šifrovaných zpráv je následující:

- odesílatel zašifruje data veřejným klíčem příjemce a odešle je na adresu příjemce;
- příjemce vezme svůj privátní klíč a zprávu rozšifruje.

A jak to celé funguje v praxi

První věc, kterou je po instalaci Enigmail třeba udělat, je vygenerovat svou dvojici klíčů. Jedním z dvojice je klíč *veřejný*, o jehož distribuci budeme dále hovořit. Tento klíč má každý k dispozici, aby vám mohl zasílat zašifrované zprávy. Zašifrované zprávy může dešifrovat pouze držitel odpovídajícího *soukromého* klíče (tato druhá část vašeho klíče by zcela jistě neměla být k dispozici ostatním a je nezbytné ji mít bezpečně uloženu). Ovšem tyto vlastnosti již byly diskutovány v minulém čísle, takže se jimi nebudeme dále zabývat.

V nabídce ThunderBirdu zvolte možnost Správa OpenPGP klíčů. Zde můžete využít služeb průvodce, který vás provede celou procedurou. Zvolíte identity, které mohou využívat vygenerované klíče, dále přístupové heslo a několik dalších vlastností. Průvodce je do detailu popisuje a jsou poměrně intuitivní, takže není třeba se jim hlouběji věnovat. Defaultní nastavení by mělo být dostatečné pro počáteční používání, přesto doporučujeme zvážit modifikaci následujících možností:

- *Doba platnosti klíče* – jak již název napovídá, určuje dobu platnosti. Technologie elektronického podpisu je založena na výpočetní složitosti. S technickým vývojem se zrychlují výpočetní možnosti strojů, a je tedy nutno brát tento fakt v potaz. Nedoporučuji tedy volit nějaké přehnaně velké hodnoty.
- *Velikost klíče* – určuje i odolnost klíče vůči útokům, kde čím delší klíč tím bezpečnější. Platí zde totéž co pro čas. Jen nutno brát v potaz vývoj a v současnosti se již nedoporučuje používání klíčů menších než 2048 bitů. Na druhou stranu, čím delší klíč, tím delší dobu trvá šifrování a ostatní funkce.

Po vygenerování soukromého a veřejného klíče budete vyzváni k vytvoření *revokačního certifikátu*. Tento certifikát může být použit pro zneplatnění klíče, např. při ztrátě soukromého klíče.

Vytvořený klíč je uložen ve správci pluginu Enigmail a pomocí něj provádíte příslušné operace. Jak již bylo zmíněno výše, váš veřejný klíč by měl být k dispozici ostatním uživatelům, aby si byli schopni ověřit vaši identitu. Jedním z možných způsobů je využití tzv. *keyserveru*. Uložením vašeho veřejného klíče na některém keyserveru umožníte ostatním využívat ho pro komunikaci s vámi. Pro ukládání veřejného klíče lze doporučit například server `pgp.mit.edu` nebo `pks.gpg.cz`. Další možností je zveřejnění klíče na vašich osobních webových stránkách. Zde ovšem člověk, který s vám chce komunikovat, nemá žádnou jistotu o pravosti tohoto klíče. Je několik možností, jak si ji ověřit. Jednou z možností je vytvoření tzv. *sítě důvěry* (web of trust). Váš veřejný klíč může být podepsán třetí osobu, např. kolegou z práce, a tím získává na jisté důvěryhodnosti; vytváří se tak jakási síť klíčů, které si navzájem věří. Jinou možností je vytvoření otisku vašeho klíče, tzv. *fingerprint*, a předání tohoto otisku bezpečnou cestou osobě, která s vámi chce komunikovat. Pomocí tohoto

otisku lze ověřit pravost veřejného klíče. Zde už se ovšem dostáváme k otázkám distribuce veřejných klíčů, které jsou mimo rámec našeho článku.

Vraťme se tedy zpět k použití vygenerovaných klíčů. Při instalaci pluginu je nastaveno, že veškeré odchozí e-maily budou podepisovány vaším soukromým klíčem. Při tvorbě e-mailu si dále můžete přes nastavení OpenPGP nastavit i šifrování zprávy.

Výhodou rozšíření Enigmail je uživatelská transparentnost. Pokud vám dojde podepsaný resp. zašifrovaný e-mail a vy máte veřejný klíč odpovídající odesílateli, dojde k automatickému ověření resp. dešifrování zprávy, a vám se v aplikaci zobrazí již přímo text e-mailu. Tato možnost se dá volitelně vypnout – pak si můžete vychutnat pohled na zašifrovaný tvar zprávy.

Pomocí správy klíčů samozřejmě můžete vytvářet další klíče, pro odlišné scénáře použití. Například soukromý a pracovní, nebo můžete importovat již vytvořené veřejné klíče jiných účastníků komunikace; ale to je již běžná praxe.

Závěr

Práce s rozšířením Enigmail poštovního klienta ThunderBird/Mozilla je velmi intuitivní a po počátečních nastaveních nevyžaduje téměř žádnou režii. Co dodat závěrem? Pokroky v této oblasti jdou mílovými kroky vpřed a bezpečnostní technologie se začínají dostávat k masám. Pokud jste s nimi neměli dosud žádné zkušenosti, měl by vám tento článek pomoci při prvních krůčcích směrem k vyšší bezpečnosti vaší elektronické komunikace.

Literatura

[1] A. Kropáčová. *Bezpečnost elektronických dat a elektronické komunikace.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. 16, č. 4, s. 15–20. □

Obsah

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