ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • duben 2006 • roč. XVI • č. 4

Deset let CESNETu

Pavel Satrapa, CESNET

6. března 2006 oslavilo sdružení CESNET deset let své existence. Kulatá výročí vybízejí k ohlédnutí a rekapitulaci, proto jsme se i my pokusili shrnout vývoj, kterým za tu dobu prošlo sdružení samotné a akademické sítě obecně.

1 Před CESNETem

Počítačové sítě k nám přišly společně s demokracií a se zapojováním republiky do infrastruktur svobodného světa. Již v roce 1990 byl v Praze díky podpoře nadace z USA zprovozněn uzel sítě EARN (European Academic and Research Network), evropské odnože sítě BITNET. Zhruba o rok později došlo k posílení mezinárodní přístupové trasy do rakouského Linze a jejímu rozdělení na dva nezávislé kanály: jeden zůstal pro síť EARN, na druhém se začalo experimentovat s Internetem.

K oficiálnímu zahájení provozu Internetu v tehdejší Československé republice došlo počátkem roku 1992. Tou dobou se již čile scházela skupina technických odborníků a plánovala, jak jej zprostředkovat vysokým školám na našem území. Výsledkem byl projekt republikové akademické sítě *FESNET (Federal Education and Scientific NETwork)* předložený do Fondu dynamického rozvoje vysokých škol při Ministerstvu školství, mládeže a tělovýchovy.

Projekt byl přijat, ovšem vzhledem k rozdělení republiky došlo k jeho významné změně. Omezil svou působnost pouze na území nově vzniklé České republiky a v souladu s tím i jméno. Během prvního čtvrtletí roku 1993 pak byla síť *CESNET (Czech Academic and Education NETwork)* uvedena do provozu a propojila Brno, České Budějovice, Hradec Králové, Liberec, Olomouc, Ostravu, Plzeň a samozřejmě Prahu.

Její tehdejší parametry dnes budí pousmání. Většina tras (včetně zahraniční) měla kapacitu pouhých 19,2 kb/s, pouze páteř Praha-Brno disponovala 64 kb/s. První krok však byl učiněn a síť začala utěšeně růst.

2 Založení sdružení

V době vzniku sítě CESNET byl u nás nemalý zájem o přístup k Internetu, jenž vysoce přesahoval nabídku. Proto Výpočetní centrum ČVUT, které síť CESNET tehdy provozovalo, získalo v roce 1994 licenci pro poskytování neveřejných datových služeb a začalo přístup k Internetu nabízet komerčním subjektům. Cílem bylo financovat ze zisků finančně náročný provoz a rozvoj sítě.

CESNET však tou dobou byl pouze jménem sítě. Formálně mělo připojování nových účastníků k síti podobu vedlejší hospodářské činnosti jedné vysoké školy. S rostoucím počtem připojených subjektů bylo zřejmé, že takový model přestává být udržitelný. Vznikla proto pracovní skupina hledající vhodné uspořádání pro další roz-

voj akademické sítě. Dospěla jednoznačně k závěru, že nejlepším řešením bude založit samostatný právní subjekt.

6. března 1996 proto zástupci 27 domácích univerzit a Akademie věd ČR podepsali zakladatelskou smlouvu. Vznikl tak *CESNET, zájmové sdružení právnických osob*, který se měl nadále starat o provoz a další rozvoj akademické sítě ČR i veškeré s ním související aktivity.

Založení sdružení představovalo velmi významnou změnu a odstranilo řadu překážek. Vztahy s připojenými zákazníky se zjednodušily. Radikálně se změnilo financování ze strany vysokých škol – zatímco dříve síť dotovalo centrálně ministerstvo školství, nyní museli jednotliví členové platit členské příspěvky. V celkovém souhrnu představovalo založení CESNETu významný krok vpřed.

3 Orientace na výzkum

Poskytování Internetu na komerční bázi sice bylo ekonomicky zajímavé a představovalo důležitý vedlejší zdroj příjmů pro rozvoj sítě, v jeho důsledku se však původně novátorský experiment postupně měnil na rutinní infrastrukturu. Odborníci sdružení proto přivítali evropský projekt *TEN-34*, jehož cílem bylo povýšit evropskou akademickou páteř na úroveň srovnatelnou s USA.

České republice se prostřednictvím CESNETu podařilo zapojit se do projektu – jako jediné zemi za bývalou železnou oponou. Cílem TEN-34 bylo propojit účastnické země mezinárodní páteří s přenosovou kapacitou 34 Mb/s. Podmínkou účasti bylo vybudování adekvátní sítě v národním měřítku. Proto souběžně vznikl domácí projekt TEN-34 CZ s cílem vybudovat rychlou akademickou páteř ČR. Ve veřejné soutěži na jeho řešení CESNET zvítězil.

V roce 1996 tak začala vznikat akademická síť nové generace, jejíž provoz byl oficiálně zahájen v červnu 1997. Jak výjimečná byla nejlépe ilustruje srovnání se sítí CESNET z doby založení sdružení (viz Obr. 1). Její nejrychlejší spoje měly kapacitu 512 kb/s. Nová síť proti nim představovala zrychlení téměř sedmdesátinásobné.

Financování z veřejných prostředků s sebou ovšem neslo i určitá pravidla pro její využití. Ta vycházela z pravidel evropských a omezovala účastníky na vědecké, výzkumné a vzdělávací instituce, či takto zaměřené části komerčních subjektů. Všichni členové sdružení pochopitelně přešli do atraktivnější sítě TEN-34 CZ a původní síť CESNET se změnila na síť ryze komerční, jež měla sloužit výlučně jako doplňkový zdroj financování.

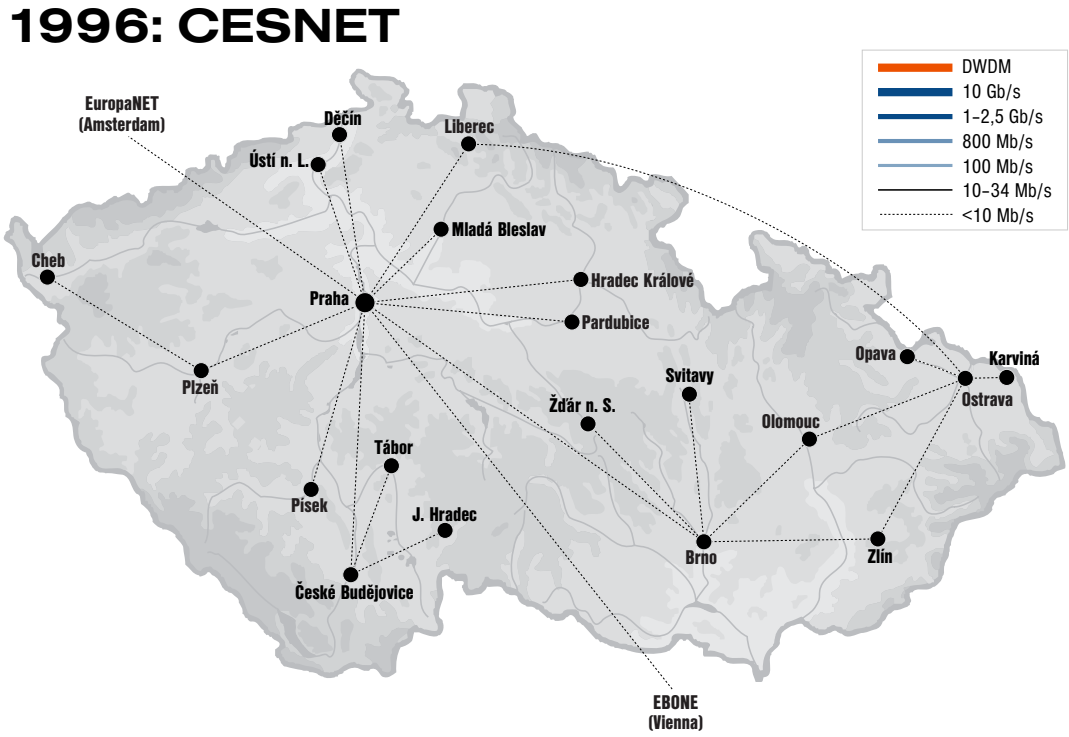
Tuto roli ale hrála stále obtížněji. Ve druhé polovině 90. let vstoupilo na náš internetový trh několik silných mezinárodních společností. Vzniklo tak velmi konkurenční prostředí, v němž sdružení nemohlo dlouhodobě obstát. Proto bylo rozhodnuto komerční síť odprodat. Jejím kupcem se v roce 2000 stala společnost Contactel a CESNET přestal poskytovat připojení k Internetu na komerční bázi. Od roku 2000 se sdružení věnuje výlučně rozvoji národní akademické sítě a souvisejícímu výzkumu komunikačních technologií a jejich aplikací.

4 Výzkumný záměr

Projekty TEN-34 a TEN-34 CZ skončily v roce 1998. Na evropské úrovni navázal projekt *QUANTUM*, v jehož rámci vznikla páteřní síť *TEN-155* postavená na technologii ATM a nabízející přenosovou rychlost 155 Mb/s. Sdružení CESNET se do něj zapojilo a začalo připravovat národní síť TEN-155 CZ.

Velmi zásadně se však změnilo financování jejího vzniku. Od roku 1999 probíhalo v rámci výzkumného záměru *Vysokorychlostní síť národního výzkumu a její nové aplikace*, který sdružení získalo. Vedle poskytnutí špičkové komunikační platformy, nezbytné pro rozvoj vědy a výzkumu v ČR, a především pro plnohodnotnou odbornou spolupráci se zahraničím, se sdružení mělo věnovat i vlastní výzkumné činnosti v oblasti pokročilých síťových technologií a jejich aplikací.

Klíčovým úkolem však stále zůstávala páteřní síť, která zvolna začala vykračovat směrem ke gigabitovým technologiím. Koncem roku 1999 jsme připravili nasazení první pilotní trasy, která počátkem roku 2000 propojila Prahu s Brnem rychlostí 2,5 Gb/s. Jednalo se o první případ, kdy CESNET vzbudil mezinárodní rozruch, protože přenosová trasa této kapacity vyhrazená výlučně



Obrázek 1: Síť CESNET v roce 1996

pro IP byla tou dobou raritou i mezi nejvyspělejšími zeměmi.

5 Gigabitové sítě

V roce 2001 došlo k rychlému šíření gigabitových přenosových rychlostí. Na evropské úrovni vznikl projekt *Géant* a s ním spojená páteřní síť *GÉANT*. Díky nad očekávání dobré nabídce přenosových služeb síť již v okamžiku spuštění disponovala na páteřních linkách kapacitou 10 Gb/s. CESNET byl opět členem řešitelského týmu. Dobrá pozice České republiky se potvrdila i tím, že pražský uzel byl zahrnut do desetigigabitové páteře. Vedly od nás celkem tři spoje: do Německa (10 Gb/s), Polska (2,5 Gb/s) a na Slovensko (2,5 Gb/s).

Souběžně vznikala i domácí síť nové generace, nazvaná *CESNET2*. Do provozu byla oficiálně uvedena v říjnu 2001 a její základní charakteristikou byla přenosová rychlost 2,5 Gb/s na linkách propojujících nejvýznamnější uzly.

Potřeba poskytovat stále rychlejší přenosové trasy při prakticky konstantním financování nás vedla k uplatnění přístupu *CEF (Customer Empowered Fibre networks)*, kdy si zákazník pronajímá od telekomunikačního operátora pouze přenosová vlákna (tzv. temná vlákna), která si osazuje vlastní technologií. CESNET patří k průkopníkům tohoto principu, který hraje významnou roli při výstavbě současných akademických sítí.

Právě nutnost osazovat vlastní zařízení vedla ke zvýšenému zájmu o optické přenosové technologie. Hlavním zájmem úsilí CESNETu bylo prodloužení jejich dosahu a omezení (pokud možno úplná eliminace) zařízení nutných na trase. Pro tuto oblast se vžilo označení *NIL (Nothing In-Line)* a CESNET v ní dosahuje mezinárodně respektovaných výsledků.

V roce 2004 byl spoj Praha-Brno povýšen na 10 Gb/s a o rok později byl dokončen optický přenosový systém DWDM (Dense Wavelength Division Multiplexing) v kruhové topologii Praha-Brno-Olomouc-Hradec Králové-Praha. K tomu došlo již v rámci následného výzkumného záměru, jehož název *Optická síť národního výzkumu a její nové aplikace* signalizuje větší orientaci na optické technologie.

Jak je vidět, CESNETu se po celou dobu jeho existence dařilo držet krok s vyspělými zeměmi Evropy. Výsledky, kterých se daří dosahovat ve výzkumu komunikačních technologií a služeb, dávají dobrý předpoklad, že tomu tak bude i nadále. □

Převzato ze zpravodaje Datagram-Cesnet, únor 2006, `http://www.cesnet.cz/doc/datagram`

CESNET – výzkum sítě a síť pro výzkum

Gabriela Krčmařová, CESNET

1 Úvod

Dne 6. března 2006 oslavilo sdružení CESNET (Czech Education and Scientific Network) přesně deset let od svého založení. Sdružení CESNET založené v roce 1996 všemi vysokými školami České republiky společně s Akademií věd České republiky provozuje a rozvíjí síť národního výzkumu a vzdělávání CESNET2. Síť CESNET2 je integrovaným síťovým prostředím, kde je jednak předmětem zkoumání a vývoje síť sama o sobě – probíhá zde výzkum, vývoj a testování nových služeb a aplikací a jejich nasazování do provozu – a jednak je provozována národní síť pro výzkum (NREN – National Research and Education Network). Sítě národního výzkumu (NREN) jsou součástí Internetu, ale mají podstatně lepší parametry služeb poskytovaných svým uživatelům, zejména rychlost přenosu dat, spolehlivost a garantovanou kvalitu služeb umožňující například multimediální aplikace.

2 Výzkum sítě

Významnou složkou činnosti sdružení CESNET jsou výzkumné aktivity v oblasti pokročilých síťových technologií a aplikací, které tyto technologie využívají. V současnosti výzkumné činnosti probíhají v souladu s řešením sedmiletého výzkumného záměru „*Optická síť národního výzkumu a její nové aplikace*“ (2004 – 2010). Sedmileté období je dostatečně dlouhé pro zahájení a úspěšné dokončení rozsáhlých výzkumných činností, které jsou v současné době rozděleny do dvanácti tematicky vymezených aktivit.

2.1 Rozvoj páteřní sítě CESNET2

Cílem aktivity je vybudovat moderní a vysoce výkonnou síť národního výzkumu a vzdělávání, která bude svým uživatelům poskytovat nejnovější služby a technologie. Nedílnou součástí aktivity je spolupráce se sítí GÉANT2 a ostatními evropskými NREN pro zajištění interoperability, která je nezbytná pro poskytování pokročilých služeb v mezinárodním měřítku. Aktivita zahrnuje nejen výzkum a implementaci nových technologií v prostředí sítě národního výzkumu, ale rovněž i veškeré podpůrné činnosti pro zajištění kvalitních a stabilních služeb pro ostatní aktivity i uživatele.

2.2 Optické sítě

Aktivita Optické sítě se zabývá výzkumem a vývojem CEF (Customer Empowered Fibre) sítí, zejména metodami přenášení dat, přenosovými zařízeními, přenosy vzduchem v první míli a spoluprací na rozvoji nových aplikací užívajících GLIF (Global Lambda Integrated Facility). Výsledky výzkumu se ověřují a uplatňují v laboratorních podmínkách i v rozlehlých experimentálních sítích, a následně pak v produkčních sítích. Řešitelé spolupracují na ověřování s projektanty a provozovateli sítí v různých zemích značně odlišných svými podmínkami.

2.3 Programovatelný hardware

Cílem aktivity je vývoj specializovaných síťových zařízení založených na programovatelném hardwaru, především hradlových polích. U zrodu této aktivity stála snaha postavit kvalitní směrovač pro protokol IPv6 (Internet Protocol version 6) na bázi osobního počítače. Vznikl projekt Liberouter s cílem vytvořit jednak hardwarový akcelerátor směrování, umožňující provádět řadu směrovacích rozhodnutí přímo na kartě rozhraní, jednak konfigurační systém usnadňující a integrující správu takového zařízení. Výsledkem projektu je karta COMBO6 a k ní přidružené karty rozhraní – nejprve se čtyřmi gigabitovými Ethernety, později s jedním desetigigovým.Vzhledem ke značnému potenciálu karty COMBO6 a k nemalému zájmu o ni od řady zahraničních institucí se připravuje její výroba ve větších sériích.

2.4 Sledování infrastruktury a provozu sítě

Oblast sledování infrastruktury představuje vývoj monitorovacích systémů, které shromažďují, zpracovávají a prezentují informace primárně získané z aktivních prvků sítě (směrovače, přepínače, atd.). Na rozdíl od ostatních měřících systémů se zde analyzují dlouhodobé trendy chování síťové infrastruktury a je poskytován primárně souhrnný pohled na příslušné veličiny nebo síťové parametry včetně jejich limitních hodnot, a to převážně v agregované podobě. Oblast sledování provozu je zaměřena na vývoj nástrojů pro efektivní zpracování specifických elementárních informací (flow) o provozu sítě. Masivní nárůst provozu v současných sítích směřuje tuto problematiku k distribuovaným systémům s výkonnými klasifikačními a filtračními mechanismy a inteligentním způsobem uchování dat.

2.5 Sledování a optimalizace výkonnostních charakteristik

Obecným cílem aktivity je výzkum a vývoj směřující k zajištění požadovaných výkonnostních charakteristik komunikace v rozlehlých vysokorychlostních sítích. Aktivita zahrnuje vývoj prostředků pro monitorování síťového provozu a jejich použití, a spolupráci na výzkumu v rámci mezinárodního projektu LOBSTER (Large Scale Monitoring for Broadband Internet Infrastructure).

2.6 AAI (autentizační a autorizační infrastruktura) a mobilita

Cílem aktivity je vývoj a implementace „interdomain“ distribuované infrastruktury poskytující autentizační a autorizační služby pro podporu spolupráce uživatelů registrovaných v různých domovských institucích. Tato infrastruktura by měla být využívána zejména WWW aplikacemi, službami poskytování konektivity v hostitelských sítích (roaming) a některými službami IP telefonie (registrace uživatelů, výstup hovoru do veřejné telefonní sítě). Základním požadavkem na budovanou infrastrukturu je kompatibilita s obdobnými řešeními vyvíjenými v evropských NREN a ve světě.

Jako vzorový příklad služby vyžadující distribuovanou autentizační a autorizační infrastrukturu lze uvést řízení přístupu „mobilních“ uživatelů do internetu prostřednictvím bezdrátových (WiFi) sítí hostitelských organizací (tzv. roaming). V současné době je v evropských sítích národního výzkumu uváděna do provozu pilotní AA infrastruktura postavená na stromové struktuře RADIUS serverů; v rámci projektu *eduroam* je podporována IP mobilita a roaming v těchto sítích. Přestože toto konkrétní řešení může být v budoucnosti nahrazeno obecnou AAI, očekáváme, že implementace a provoz takto široce pojaté služby přinesou zkušenosti využitelné jak v technické tak i v organizační přípravě AA služeb nové generace.

2.7 IP telefonie

Cílem výzkumné aktivity IP telefonie je rozvoj a zkvalitnění služeb IP telefonní infrastruktury. V rámci aktivity lze vysledovat několik směrů: výzkumy zaměřené na kvalitu služby (QoS, alternativní výstupy ze sítě, pokročilé signalizační mechanismy), rozšíření o podporu nových protokolů a služeb (SIP, ENUM, atd.), podpora IP telefonů, integrace a především přechod k moderní technologii NGN (SS7).

2.8 MetaCentrum

Aktivita se věnuje rozvoji a správě českého akademického gridového prostředí a souvisejícímu výzkumu ve vybraných oblastech. Vlastní aktivita je rozdělena do čtyř základních oblastí: zajištění vlastního provozu, uživatelská podpora včetně podpory konkrétních aplikací, výzkum a vývoj v oblasti monitorování distribuované gridové infrastruktury a bezpečnost distribuovaného prostředí. Součástí aktivity je rovněž zapojení v rozsáhlém projektu 6. rámcového programu EU *EGEE (Enabling Grids in EuropE)*, který pokrývá všechny čtyři výše zmíněné oblasti. Od 1. 1. 2005 je součástí aktivit MetaCentra i účast na národním projektu *MediGRID*, zaměřeném na podporu distribuovaného prostředí pro lékařské disciplíny.

2.9 Virtuální prostředí pro spolupráci

Virtuální prostředí pro spolupráci je aplikační aktivitou využívající vysokorychlostních sítí pro sdílení multimediálních dat; a to jak synchronně formou videokonferencí a sdílených aplikací tak i asynchronně formou streamingu vysílání. Cílem aktivity je výzkum a vývoj kolaborativních technologií od přenosových protokolů pro multimediální data, jejich sdílení a ukládání i aplikační využití. Jedná se především o vývoj technologií navazujících na videokonferenční aktivity a rozvíjející je, a dále pak o zpracování videostreamů a jejich zpřístupňování.

2.10 Podpora distančního vzdělávání

Základním cílem je kvalitativní posun elektronické podpory výuky na vysokých školách s maximálním využitím současných možností v oblasti progresivních síťových i lokálních digitálních technologií, jako jsou nástroje pro záznamy, zpracování, ukládání a prezentaci multimediálních dat a nástroje pro vzdálenou spolupráci.

2.11 CESNET CSIRT (Computer Security Incident Response Team)

Cílem aktivity CESNET CSIRT je dosáhnout lepší úrovně interní organizace v oblasti bezpečnosti sítě CESNET2, služeb na ní provozovaných a v řešení vzniklých bezpečnostních incidentů. Cílem je vybudování týmu pro příjem a řešení nahlášených bezpečnostních incidentů a ustanovení pravidel pro komunikaci mezi institucemi připojenými k síti CESNET2 při řešení bezpečnostních incidentů, dále potom poskytnout těmto institucím návody, informace, pravidla a motivaci pro zřízení bezpečnostních týmů.

2.12 Medicínské aplikace

Hlavními úkoly této aktivity jsou aplikace z oblasti zdravotnictví. Řeší se projekty formalizace dat onkologických pacientů, podpora open source nástrojů a systémů ontologie nad medicínskými daty a zpracování medicínských obrazových dat. Výsledky této aktivity jsou přímo využitelné v rámci akčního plánu e-Health, který v roce 2004 vyhlásila Evropská unie. Hlavním cílem programu e-Health, který přináší kvalitativní zlom v lékařské péči, je vytvořit do roku 2010 tzv. Evropský bezhraniční prostor pro informace o zdraví.

Na webových stránkách sdružení CESNET (`http://www.cesnet.cz`) lze nalézt podrobné informace o aktuálních výsledcích jednotlivých výzkumných aktivit v rámci Zprávy o řešení výzkumného záměru za rok 2005.

3 Spolupráce na mezinárodních výzkumných projektech

Jak z výše uvedeného vyplývá, výzkumné aktivity sdružení CESNET zahrnují oblasti od nejnižších přenosových vrstev počítačových sítí, přes middleware, autentizaci a autorizaci, bezpečnost, až po výzkum a vývoj nových aplikačních služeb. Značný důraz se klade na mezinárodní spolupráci a na zapojení především do projektů v rámci 6. rámcového programu Evropské unie. V současné době jsou zástupci sdružení CESNET úspěšně zapojeni do několika významných mezinárodních projektů. Jsou to například:

3.1 GN2 – Multi-Gigabit European Academic Network

Kontinuita rozvoje evropské infrastruktury pro výzkum a vzdělávání je zajištěna realizací tohoto čtyřletého projektu 6. rámcového programu, který byl oficiálně zahájen 1. 9. 2004 a jeho cílem je vybudovat moderní, vysoce výkonnou infrastrukturu (*Géant2*) umožňující poskytovat uživatelům přístup k jejich pracovnímu prostředí (ve smyslu informačních zdrojů, výpočetních kapacit, atd.) v reálném čase odkudkoliv v rámci tzv. Evropského výzkumného prostoru (European Research Area - ERA). Velký důraz se přitom klade na podporu služeb zajišťujících zaručenou konektivitu mezi koncovými zařízeními a na vyřešení problémů spojených s mobilitou.

3.2 EGEE – Enabling Grids for E-SciencE

Projekt EGEE 6. rámcového programu Evropské unie patří mezi největší mezinárodní projekty jak počtem partnerů tak finančním krytím, které EU poskytuje. Dvouletý projekt byl pod vedením CERNu zahájen 1. května 2004 a zahrnuje 70 partnerů prakticky ze všech zemí Evropy

včetně Ruska. Zapojeny jsou i instituce z USA, byť bez přímého finančního příspěvku EU. Zájem o spolupráci mají i asijské země, především Korea a Japonsko. Cílem projektu je vybudování celoevropského Gridu, propojitelného s obdobnými mimoevropskými infrastrukturami. EGEE Grid bude tvořen propojenou sítí datových úložišť a počítačů, především clusterů s architekturou Intel IA-32 a IA-64 či kompatibilními architekturami procesorů AMD. Projekt zajistí tzv. middleware, tj. programové vybavení, které umožní propojit jednotlivé počítače či dnes již existující tematické, regionální či národní Gridy do jednotného celoevropského systému.

3.3 LOBSTER – Large Scale Monitoring for Broadband Internet Infrastructure

Projekt LOBSTER navazuje na projekt SCAMPI (Scaleable Monitoring Platform for the Internet), který vyvinul hardwarově akcelerovanou platformu pro pasivní monitorování vysokorychlostních sítí. Cílem dvouletého projektu LOBSTER, který byl zahájen v září 2004, je instalovat síť monitorovacích uzlů založených na platformě SCAMPI v evropském měřítku. Jeho konsorcium tvoří instituce z pěti evropských zemí a z Nového Zélandu. Své zastoupení v něm mají sítě národního výzkumu, univerzitní výzkumná pracoviště a partneři z komerční sféry.

4 Síť pro výzkum

Nasazované síťové aplikace a služby, jako výsledky výzkumných aktivit, je žádoucí provozovat ve vysoce výkonném a spolehlivém síťovém prostředí. Tedy tak, aby vyhověly aktuálním požadavkům vědecko-výzkumné uživatelské komunity ze všech oblastí výzkumu a vývoje. Výzkumná síť CESNET2 poskytuje realizovaným výzkumným záměrům a výzkumným projektům přímou podporu formou nadstandardního informačního prostředí se specifickým akcentem v oblasti mezinárodní spolupráce (tj. v rámci 5. a 6. rámcového programu EU). Jako vedlejší efekt přenáší toto prostředí běžný provoz univerzit, výzkumných a vzdělávacích institucí, a to převážně formou přímé podpory vědecko-výzkumného a vzdělávacího procesu.

Síť CESNET2 je určena pro potřeby výzkumu, vývoje a vzdělávání v ČR a tomu, kromě jiného, odpovídají její technické parametry. Její páteř propojuje okruhy s vysokými přenosovými rychlostmi největší univerzitní města České republiky. Kromě kvalitního připojení k Internetu a velkých přenosových kapacit (2,5 Gb/s) umožňuje síť CESNET2 především pro vědecké a výzkumné účely realizovat i některé pokrokové, kapacitně velmi náročné služby – například distribuované počítání, úložné/skladové služby nebo multimediální služby.

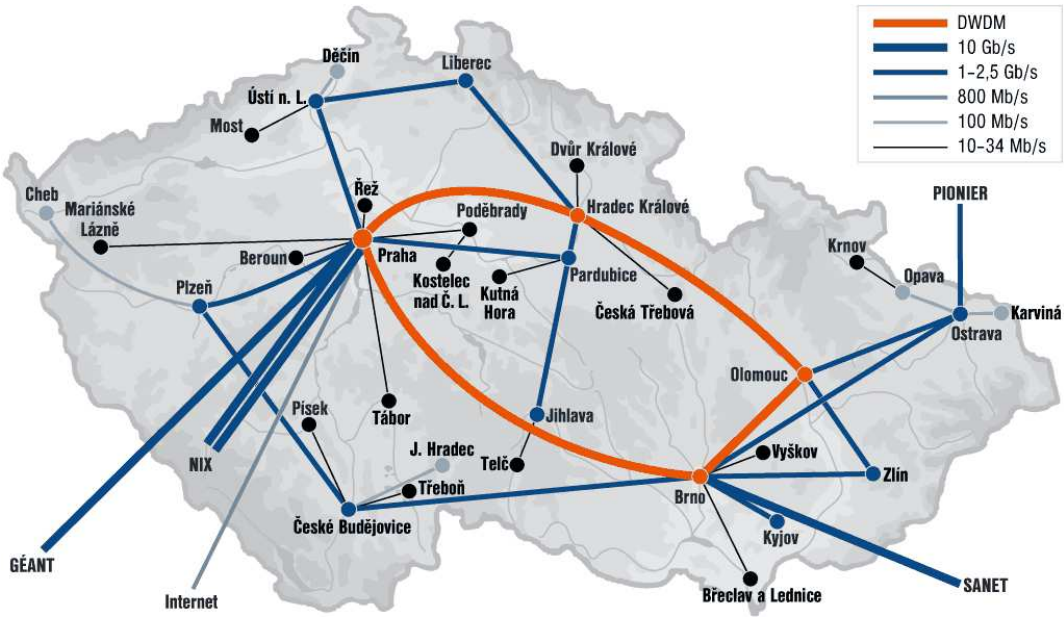
Síť CESNET2 poskytuje přímý přístup do světového výzkumného informačního a komunikačního prostoru i do běžného Internetu.

Koncem roku 2005 byl na síti CESNET2 dostavěn optický přenosový systém DWDM (Dense Wavelength Division Multiplexing) v kruhové topologii Praha–Brno–Olomouc–Hradec Králové–Praha s přenosovou kapacitou 10 Gb/s. Síť disponuje čtyřmi nezávislými zahraničními spoji. Jeden vede k pražskému uzlu evropské výzkumné sítě GÉANT. Má kapacitu 2,5 Gb/s a zprostředkuje přímý přístup do mezinárodního vědecko-výzkumného prostředí. Druhá zahraniční linka má přenosovou rychlost 800 Mb/s a slouží jako hlavní zahraniční spoj sítě CESNET2 pro komunikaci s běžným Internetem, další přímé spoje jsou do Polska a na Slovensko.

4.1 CESNET Conference 2006

V souvislosti s 10. výročím svého založení uspořádalo sdružení CESNET mezinárodní odbornou konferenci CESNET Conference 2006, jejímž mottem bylo „Síť pro výzkum, výzkum pro síť“. Konference, jejíhož zahájení se ujala ministryně školství, mládeže a tělovýchovy Petra Buzková, se konala ve dnech 6.- 8. března 2006. V Modré posluchárně Univerzity Karlovy v Praze se setkaly špičky internetového výzkumu z celého světa. Vysokou odbornou kvalitu programu konference zajistili odborníci v oblasti informačních a komunikačních technologií z České republiky, Evropy i USA.

Na stránkách konference (`http://www.ces.net/conference06/`) jsou k dispozici nejen anotace a prezentace jednotlivých přednášek, ale také videozáznam celé akce. □



Obrázek 1: Současná topologie sítě CESNET2

Konference CESNET 2006

Eva Hladká, Luděk Matyska, FI MU a CESNET

Sdružení CESNET slaví v tomto roce 10 let své existence. O tom jaká to byla léta a čeho CESNET za tuto dobu dosáhl se můžete dočíst v tomto čísle Zpravodaje v jiném článku. Tento příspěvek je věnován hlavní události oslav desátých narozenin CESNETu, která se konala přesně den po onom desetiletém výročí.

CESNET se za těch deset let své existence postupně posouval z organizace, která zajistila vybudování a následný rozvoj špičkové infrastruktury počítačových sítí v České republice, získala nemalé ostruhy i na poli komerčním (a včas svou tyto aktivity opět prodala), směrem k organizaci s výrazným výzkumným a vývojovým potenciálem. Nepřekvapí proto, že hlavní událostí oslav desetiletého výročí byla mezinárodní konference, která proběhla v Praze a která svým rozsahem i zaměřením pokrývala většinu výzkumných aktivit sdružení CESNET.

1 Místo a čas

CESNET byl oficiálně založen 6. března 1996, konference se konala 7. a 8. března v Praze, v prostorách Modré posluchárny Karlovy univerzity. Úvodní recepce proběhla v předvečer vlastního odborného jednání konference v prostorách Obecního domu v Praze, přesně na den deset let po založení sdružení CESNET, a byla tak skutečnou a důstojnou oslavou narozenin. Zřejmě i letošní zima projevila sdružení svou přízeň a v jednací dny bylo v Praze chladné, ale slunečné počasí.

2 Odborný program

Odborný program konference byl zahájen a zakončen rozsáhlými zvanými „keynote“ přednáškami, mimo nich posluchači měli možnost vyslechnout další zvané přednášky, některé dokonce videokonferenčně. Hlavní program konference byl pak postaven na přednášek, které z nabídky zaslaných příspěvků vybral mezinárodní programový výbor.

2.1 První den

První den byl slavnostně zahájen projevem kvestora hostitelské university Josefa Kubíčka a ministryně školství, mládeže a tělovýchovy Petry Buzkové. Paní ministryně ve svém projevu velmi

trefně srovnávala historii vývoje CESNETu a aktivity známé pro jménem INDOŠ (zavádění Internetu do škol) a kladně ocenila CESNET za vykonanou práci i způsob, jak se k ní staví.

Na oficiální zahájení navázal blok zvaných přednášek. První klíčovou přednášku přednesl předseda sdružení DANTE a současně technický ředitel DFN, organizace zajišťující vysokorychlostní akademické sítě v Německu, Klaus Ullman. Jeho přednáška byla věnována budoucnosti evropských akademických sítí a směrům dalšího rozvoje. Následovala přednáška ředitele sdružení CESNET, věnovaná přehledu aktivit sdružení a jeho výzkumným plánům do budoucna.

Šíři zájmů a aktivit sdružení ilustroval následující blok, tvořený směsí zvaných a vybraných přednášek věnovaných gridům a specifickým problémům rozsáhlých distribuovaných systémů a prostředí. Součástí tohoto bloku byly i přednášky věnované konkrétním požadavkům gridů a distribuovaných prostředí na počítačové sítě a tomu, jak tyto požadavky ovlivňují další vývoj v oblasti počítačových sítí.

2.2 Videokonference

První den byl zakončen dvěma zvanými přednáškami, přednášenými „na dálku“, videokonferenčně. Oba přednášející – Ana Preston a Mike Wellings – jsou domovem v USA a z časových důvodů se nemohli zúčastnit jednání konference osobně. Sdružení CESNET se videokonferencemi dlouhodobě zabývá, využili jsme proto této příležitosti a dohodli využití odpovídajících technologií tak, aby obě přednášky bylo možno realizovat.

První z nich, přednáška Any Preston o rozvoji optických sítí, byla realizována technologií H.323 [1], zařízením Polycom FX po běžné produkční síti. Slidy k přednášce byly promítány druhým projektorem z kopie zaslané předem do Prahy, posluchači tak na dvou plátnech mohli sledovat jak přednášející, tak i doprovodný materiál. Přednáška proběhla bez výpadků a problémů a pro přednášce následovala živá diskuze.

Druhá z videokonferenčně realizovaných přednášek patřila tomu technicky nejpokročilejšímu, čeho jsme dnes v oblasti videokonferencí v současné době schopni [2]. Jednalo se o unikátní videokonference při použití videa ve velmi vysoké (high-definition, HD) kvalitě, o vůbec první veřejnou demonstraci videokonference tohoto typu v České republice a o jednu z prvních v rámci Evropy. Přednášková místnost Univerzity Karlovy v Celetné ulici, vybavená zapůjčeným prototypem HD projektoru s nativním HD rozlišením 1920×1080, byla propojena přes akademické vysokorychlostní sítě s pracovištěm Research Channel v Seattlu (USA, stát Washington). Bohužel se nepodařilo realizovat tuto přednášku nad nekomprimovaným HD datovým tokem – důvodem byl určité problémy v zajištění požadované kapacity sítě, především v USA – a přednáška byla realizována pomocí HDV (High Definition Video) komprese. Přesto mezi oběma koncovými místy byl po dobu půlhodnové přednášky přenášen datový tok 25 Mbps. Přenos byl realizován bez jakékoliv dedikace pásma, pouze za použití mezinárodní infrastruktury akademických sítí (CESNET2, GEANT, Internet2/Abilene), posluchači mohli proto pozorovat i důsledky občasné ztráty paketů, ke které docházelo při přenosu síti Internet2. Tyto ztráty se projevovaly viditelnými výpadky makrobloků, větších či menších čtvercových a obdélníkových oblastí v přenášeném obraze.

2.3 Druhý den

Druhý den přednášek byl zahájen blokem věnovaným hardware, a to jak kartám s programovatelnými hradlovými poli, která se využívají v aktivních síťových prvcích, tak i optickým zesilovačům. V odpoledním bloku pokračovaly přednášky z oblasti videokonferencí, P2P sítí, bezpečnosti a dalších aktuálních síťových témat.

Konference byla zakončena druhou klíčovou přednáškou, kterou prezentoval zástupce švýcarské sítě národního výzkumu SWITCH Simon Leinen a věnoval ji dlouhodobému sporu o základní koncepci počítačových sítí – přepínání okruhů proti nespojovaným službám.

Jednání konference shrnuli ve svých vystoupeních ředitel sdružení Jan Gruntorád a předseda programového výboru, Luděk Matyska.

3 Konference on line

Nejenom živé jednání konference bylo CESNETu ke cti. Tak jako se dlouho před vlastní konferencí připravoval program a organizace, připravovaly se i technologie a scénáře, jak konferenci zpřístupnit i dalším účastníkům, kteří se nemohli jednání zúčastnit osobně. Protože CESNET ve svých aktivitách tyto technologie rozvíjí a uvádí do českého akademického prostředí, byla během konference využita celá škála možných prostředků pro záznam konference a příspěvků, včetně streamování konference v reálném čase v několika formátech.

Celý průběh konference byl živě vysílán do Internetu ve formátech RealMedia, WindowsMedia a také pomocí technologie MediaSite (současný záznam živého obrazu a slidů). Záznam konference je k dispozici jak ve standardní, tak i v high-definition kvalitě na adrese `http://videoserver.cesnet.cz/videoarchiv.php`.

4 Závěrem

Mezinárodní konference v oblasti počítačových sítí s více než stem účastníků, řadou zahraničních účastníků včetně zahraničních (i zámořských) přednášejících otevřela novou kapitolu v historii CESNETu. Konference byla úspěšná, ať už úspěch měříme počty posluchačů na přednáškách, živými diskuzemi nebo tím, že ani jedna přednáška ohlášená na programu nechyběla. Všechny on-line technologie splnily očekávání, záznamy přednášek jsou k dispozici. Vedení sdružení CESNETu spolu s členy programového výboru teď konferenci vyhodnocuje a zvažuje nejvhodnější formu jejího pokračování tak, aby bylo možno za několik let říci, že ta první, narozeninová konference otevřela cestu k uznávané mezinárodní události v oblasti počítačových sítí a jejich aplikací. Můžeme společně sdružení CESNET přát, aby se tento narozeninový sen splnil.

Pokud vás informace o konferenci zaujaly a chcete se dozvědět více, kompletní program konference včetně prezentací přednášek a fotodokumentace naleznete na [3]. Kompletní příspěvky naleznete ve sborníku [4].

Literatura

[1] P. Holub, E. Hladká. VIMM a Megaconf III – virtuální konference celosvětového měřítka. Zpravodaj ÚVT MU. ISSN 1212-0901, 2001, roč.12, č.2, s.3-6.

[2] E. Hladká, P. Holub. Videokonference s vysokou kvalitou. Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč.16, č.3, s.9-12.

[3] `http://www.ces.net/conference06/prog/`

[4] G. Krčmářová, P. Sojka (Eds.): First CESNET Conference on Advanced Communications and Grids Proceedings, CESNET, 2006. □

Sdružená matrika studentů po 6 letech

I. Burian, J. Šmerda, ÚVT MU

Bylo nebylo, dávno tomu. Před více než šesti lety byl na stránkách zpravodaje ÚVT MU (viz článek [1]) představen projekt SIMS, neboli databáze *Sdružených Informací Matrik Studentů*. Jde o projekt (nyní již rutinně provozovanou službu) řešený na Ústavu výpočetní techniky MU pro MŠMT ČR na základě výběrového řízení z roku 1998. Po tak dlouhé době je slušné zastavit se v každodenním běhu světem IT, ohlédnout se zpět a bilancovat – co a jak se podařilo a co nás v nejbližší době čeká.

Na úvod malá rekapitulace toho, co vlastně matrika studentů je a k čemu slouží: SIMS je intranetový informační systém, který shromažďuje a zpracovává informace o studentech a jejich studiích na veřejných i soukromých vysokých školách ČR (výjimku tvoří pouze školy státní, jako je např. Univerzita obrany). Výsledky zpracování jsou poskytovány jednak školám, a dále samozřejmě také ministerstvu školství. Pro ministerstvo jsou z matričních dat vytvářeny výstupy, na jejichž základě jsou – mimo jiné – vysokým školám rozdělovány finanční prostředky. Aby byl informační systém užitečný, je třeba, aby data v něm obsažená a zpracovávaná byla správná a aktuální. Aktuálnost je zajištěna sběry, které probíhají čtyřikrát ročně – školy musí poslat přírůstkové aktualizace dat o všech svých studentech. Datové soubory jsou šifrovány a opatřeny

elektronickým podpisem, čímž je zajištěna jejich důvěrnost a nepopiratelnost. Kromě sběrů mají správci dat jednotlivých škol možnost dělat opravy i v období mezi sběry a udržovat tak data maximálně aktuální.

1 Minulost

Minulý článek sledoval historii SIMS od jeho začátku koncem roku 1998 až do druhého testovacího sběru dat a končil výhledem na první závazný sběr dat k 31.10.1999. Jelikož z tohoto sběru měly být poprvé generovány podklady pro financování veřejných vysokých škol na následující kalendářní rok, byla znát nervozita ve všech táborech. Nebudeme napínat: první sběr i zpracování údajů proběhly dle přání a očekávání všech spoluautorů. Nudné statistické záznamy hovoří o tom, že prvního ostrého sběru dat do centrální matriky studentů se zúčastnilo 23 veřejných vysokých škol, do databáze byly uloženy informace o 216 279 studentech, o 240 273 jejich studiích a o 296 648 etapách historií studií. Následující sběr v prosinci 1999 byl již v podstatě rutinní záležitostí.

2 Jak šel čas

V průběhu let došlo k mnoha rozšířením, vylepšením a doplněním, ale základní principy fungování centrální databáze a sběrů dat zůstaly zachovány – jsou popsány v článku z roku 1999 [1]. Z mnoha změn realizovaných v následujících letech uvádíme jen ty nejzákladnější:

V roce 2000 vznikla aplikace „Info Student“ zobrazující o konkrétní studentce či studentovi veškeré informace zaznamenané v SIMS a pro správce byla implementována možnost automaticky provádět v poslaných datech základní opravy. Vznikly základní typy výstupů – chybových, matričních (datových) a statistických. V roce 2001 byl zaveden cyklus pravidelných čtvrtletních sběrů dat (k 31.3., 30.6., 31.10., 31.12.), který je dodržován dodnes; původním důvodem pro tento cyklus bylo čtvrtletní vyplácení stipendií doktorským studentům. Nově byla vytvořena agenda přestupů, implementováno generování matričních výstupů studií na jiných vysokých školách a vznikl i „Průvodce SIMS pro nové uživatele“. Poprvé se sběru dat účastnily také některé soukromé vysoké školy.

V roce 2003 byla rozšířena struktura sbíraných dat v oblasti tzv. přidaných položek a došlo k přečíslování kódů studijních programů. V následujícím roce proběhla atestace systému SIMS na shodu se standardem ISVS (Informační systém veřejné zprávy) pro náležitosti životního cyklu IS. Tímto atestem musí projít ze zákona všechny veřejné informační systémy úřadů státní správy.

V loňském roce pak došlo k přečíslování kódů územní identifikace obcí a částí obcí, byla doplněna evidence a generování podkladů pro ubytovací stipendia a evidence pro krátkodobé stipendijní pobyty.

3 Matrika v číslech

První souhrnný ukazatel, který by jistě každého v souvislosti s matrikou studentů napadl, je počet studentů a studií v čase. V následující tabulce je uveden počet aktivních studentů a studií – oba údaje se vztahují vždy ke sběru 31. října v daném roce. Je uveden také počet vysokých škol, které údaje do matriky poskytly.

	Aktivních studií	Aktivních studentů	Počet VŠ: veřejné / soukromé
1999	191 726	199 699	23/0
2000	197 858	207 472	23/0
2001	211 045	220 949	24/5
2002	231 550	243 512	24/21
2003	256 015	269 194	24/27
2004	279 792	293 465	24/30
2005	306 611	320 652	25/36

Z tabulky je zřejmý každoroční nárůst počtu studentů i jejich studií. Po roce 2000 rostl meziročně počet studentů zhruba o 10%. Obdobně rostl i počet aktivních studií. Celkově podle matriky SIMS studovalo v roce 2005 na českých vysokých školách o 60% více studentů než v roce 1999.

Co se týče počtu vysokých škol, je vidět značný rozdíl v dynamice počtu veřejných vysokých škol oproti počtu soukromých vysokých škol. Zatímco počet veřejných VŠ zůstává víceméně konstantní (za 6 let přibyly pouze dvě – Univerzita Tomáše Bati ve Zlíně v roce 2001 a Vysoká škola

polytechnická Jihlava v roce 2005), nárůst počtu soukromých VŠ má velmi strmý charakter. K 31.10.2005 přispívalo do matriky celkem již 36 soukromých vysokých škol. Pokud ovšem porovnáme celkový počet studentů studujících na obou typech vysokých škol, je převaha na straně veřejných VŠ, kde v loňském roce studovalo 92% všech aktivních vysokoškolských studentů v ČR.

Další tabulka charakterizuje celkový rozsah databáze SIMS v jednotlivých letech. Uvádí kumulované počty záznamů studentů, jejich studií a historií studií (tj. informace i o případných přerušeních a obnoveních v rámci jednoho studia) od počátku matriky k 31.10. daného kalendářního roku.

	počet záznamů v SIMS		
	Student	Studium	Historie studií
1999	216 279	240 273	296 648
2000	253 331	306 656	410 847
2001	299 002	381 978	532 856
2002	351 663	470 892	661 811
2003	407 922	565 766	784 916
2004	473 450	672 765	940 569
2005	544 323	790 889	1 104 638

4 Z každodenního života matriky

Za téměř sedm let se na ÚVT v práci na matrice vystřídalo několik lidí a hlavně se sama matrika musela průběžně měnit a vyvíjet podle aktuálních požadavků. Mediálně nejznámějším požadavkem bylo zřejmě loňské zpracování dat za účelem určení, kteří vysokoškolští studenti mají či nemají nárok na ubytovací stipendium a proč tomu tak je. Díky ubytovacím stipendiím se například přišlo na to, že zdaleka ne všechny školy vedou své matriky studentů na 100% správně, a též se objevil problém s tzv. prázdninovými studii (student se zapsal a ukončil studium ještě před začátkem vlastní výuky), která kvůli podmínce, že student má nárok na ubytovací stipendium, pouze pokud studuje první studium na VŠ ČR, spoustu studentů z nároku vyloučila. Studenti proti tomu celkem pochopitelně vznesli na svých školách námitky a školy se pak nějakou dobu pokoušely odkazovat tyto námitky na nás jakožto správce matriky, dokud se nepřesvědčily, že za správnost vložených dat odpovídají pouze ony samy. Poměrně kuriózním případem byla také neohlášená návštěva otce studentky jedné pražské vysoké školy, kterého k nám do Brna jednoho letního odpoledne poslali ze studijního oddělení. Šlo o to, že studentka studovala déle, než bylo přípustné, škola na její studium přestala dostávat státní příspěvek a žádala úhradu školného. S lítostí jsme museli potvrdit, že v matrice máme přesně stejná data, jaká má škola, a že v Brně se problém nevyřeší... Za šest let provozu a vývoje matriky jsme zažili i situace, kdy jsme se o oficiálních změnách, určených ministerstvem, dozvěděli až z dotazů škol na to, kdy budou změny konečně provedeny.

5 Malý výhled do budoucnosti

Na závěr se zmíníme o nejbližší budoucnosti matriky. Matrika je realizována na platformě Microsoft (databází je MS SQLServer) v aplikačních technologiích, které pomalu ustupují do pozadí, takže hlavním úkolem letošního roku je dokončit vývoj nové verze systému, realizované v technologii .NET, a tuto zprovoznit. Během letošního roku proběhne také přechod na XML formát pro sběry a opravy dat matriky, a samozřejmě musíme počítat s dalšími úpravami, které matrice přinesou čas, zákonodárci a ministerstvo.

Literatura

[1] P. Koudelka, J. Kohoutková. Sdružená matrika studentů. Zpravodaj ÚVT MU. ISSN 1212-0901, 1999, roč. 10, č. 1, s. 5–9. □

Projekt e-learning 2006 – pilotní kurzy

Nina Hrtoňová, Anna Váňová, Luděk Matyska, ÚVT MU

Také v letošním roce pokračuje na Masarykově univerzitě e-learningový rozvojový projekt, tentokrát pod názvem „*Elektronické výukové materiály a komplexní podpora jejich tvorby*“. Na projekt loňský navazuje v několika hlavních rovinách: v rozvoji zázemí technologického, metodického a koncepčního, rozvojem personální

podpory a v oblasti technického vybavení (podrobně jsme o projektu informovali v prosincovém Zpravodaji ÚVT [3]). V rámci projektu je dále podporován rozvoj prostředí IS MU pro elektronickou výuku (tzv. IS LMS) jako integračního nástroje, který sdílí celá univerzita. Explicitní podporu poskytuje projekt i širšímu využívání IS prostřednictvím fakultních e-techniků. Projekt bude i nadále pokračovat v rozvoji prostředí a nástrojů pro záznam, zpracování a zpřístupnění záznamů přednášek, přístup k záznamům bude probíhat přes rozhraní IS. Podpora bude poskytována i zpracování a ukládání dalších video a případně audiomateriálů, které vzniknou v rámci přechodu dalších kurzů do digitální podoby. Velká pozornost bude v průběhu roku věnována také autorským systémům. Koordinaci všech těchto činností a zpracování získaných zkušeností tak, aby mohly být využity celou univerzitou, bude i nadále zabezpečovat *Centrum pro podporu e-learningu MU* (eCentrum).

1 Tvorba výukových materiálů – dvě roviny podpory

Pro zajištění odpovídajících výstupů projektu je významná následující koncepce podpory tvorby výukových materiálů:

- na *úrovni fakultní* budou podporovány kurzy se základním využitím stávajících a dále rozvíjených možností IS LMS a autorských nástrojů
- na *úrovni celouniverzitní* bude poskytnuta větší podpora vybrané skupině kurzů, které svým rozsahem, novými či složitými postupy při zpracování, případně postupy metodickými, přesahují rámec běžných kurzů. Těmto kurzům bude poskytnuta finanční podpora, metodická podpora eCentra a v dostupném rozsahu i podpora vývojového týmu ISu.

Cílem tohoto řešení je rozvoj a ověření e-learningových technik a metodik na MU, rozvoj IS LMS a smysluplné používání externích autorských nástrojů, které povedou ke vzniku kvalitních e-learningových kurzů. S požadavkem na posun v celé oblasti tvorby a využívání elektronických výukových materiálů souvisí samozřejmě i upevnění pozice univerzitního IS LMS jako integračního a podpůrného prostředí (s tím ovšem souvisí i rostoucí tlak na vývojový tým IS LMS i nadále podporovat nové požadavky autorů kurzů). Jedním z přetrvávajících požadavků je potřeba zpřehlednit a zjednodušit práci v IS LMS při zpracování a zejména provozu kurzů. V současné době mohou uživatelé IS LMS využívat několik e-learningových nástrojů, rozdělených na jednotlivé agendy. Mezi ty základní patří:

- Agenda *Studijní materiály*, ve které může vyučující vystavovat soubory různých formátů a manipulovat s nimi.
- *Testovací* agenda umožňující změnou nastavení nad jednou sadou otázek vytvářet cvičení, testy, dotazníky nebo oživené texty.
- Poslední výraznou změnou při tvorbě elektronických podpor výuky v ISu je nové rozhraní kurzu (*Interaktivní osnova*), přes které může učitel ručně zpřístupnit studentům vybrané materiály a aktivity ve strukturované podobě.

Mnohé funkce agend jsou stále ve stadiu vývoje, a proto je cílem podpory kurzů na celouniverzitní úrovni také nasměrovat další rozvoj systému a prověřit funkčnost toho, co již systém nabízí.

2 Velké kurzy – soutěž

Pro výběr kurzů, které budou podporovány a sledovány na celouniverzitní úrovni, byla zvolena forma soutěže [1]. Soutěž byla vyhlášena na počátku roku 2006 s cílem zahájit řešení projektů v průběhu měsíce března. Celkem bylo podáno 39 návrhů ze všech fakult MU s výjimkou Právnické fakulty MU. Počet nabídek a zejména jejich kvalita jasně prokázaly, že myšlenka elektronické podpory výuky na MU již zapustila své kořeny. Na druhé straně návrhy kurzů potvrzují nezbytnost pokračující explicitní podpory na celouniverzitní úrovni, jako záruky postupující integrace celé univerzity i v této oblasti.

Vyhodnocení a výběru kurzů, které získají finanční podporu, se věnovala výběrová komise pod vedením prorektorky Brázdové a hlavního řešitele projektu. V komisi byly zastoupeny všechny fakulty z nichž vzešel alespoň jeden návrh projektu (včetně Centra jazykového vzdělávání MU), zástupce vývojového týmu ISu a zástupce eCentra. Po téměř měsíc trvajícím výbě-

rovém řízení, jehož součástí byla i prezentace užší skupiny 13 vybraných kurzů před členy komise, bylo vybráno celkem 8 kurzů, které dostanou v roce 2006 finanční podporu. Při výběru byl důležitý zejména inovativní přínos vybraných kurzů, a to jak při vytváření materiálů, tak při samotné výuce na úrovni metodické i organizační. S tím souvisí další společný rys podporovaných kurzů: výsledky práce by měly být využitelné i při tvorbě materiálů pro další předměty. Nové velké kurzy jsou otevřené studentům prezenčního, kombinovaného i celoživotního vzdělávání, některé z nich i pracovníkům MU nebo zájemcům mimo univerzitu. Za povšimnutí jistě stojí to, že řada autorských týmů je složena ze zástupců více fakult a členy týmů jsou v nezanedbatelné míře studující MU.

3 Podporované kurzy – seznamte se

Následuje stručné představení podporovaných velkých kurzů v abecedním pořadí:

Analytická chemie – modulárně zpracovaný kurz se speciálními samostatnými okruhy je určen primárně studentům Pedagogické a Přírodovědecké fakulty MU. Součástí kurzu je práce s grafickým materiálem, animacemi a videozáznamy z přednášek a dále názorné prezentace nástrojů používaných v analytické chemii. Kromě bohatého zařazení multimédií se autoři díky svým pedagogickým zkušenostem zaměří na zpracování netradičních metod výuky.

Angličtina online – kurz určený všem členům Masarykovy univerzity, jejichž jazyková úroveň neodpovídá požadovaným vstupním znalostem ke studiu odborné angličtiny, i těm, kteří si základní úroveň chtějí zlepšit či jen udržet. Kurz běží v Informačním systému od podzimního semestru 2005. V letošním roce půjde především o vyzkoušení řízení kurzu v různých rolích (autor, tutor nebo asistent učitele), propojení kurzu s komunikačními nástroji jiných systémů a spolupráci s vývojovým týmem ISu při dopracování testové agendy s protesty.

Effective Public Speaking – dvojjazyčný anglicko-český kurz se zaměřuje na zásady odborného mluveného projevu. Studující budou v jednotlivých lekcích vedeni ke konstruktivnímu studiu s množstvím původních videomateriálů a budou mít možnost vzájemně hodnotit svou práci.

E-learning v Matematice – zahrnuje původní návrh dvou samostatných matematických předmětů Matematická analýza 3 a Matematika III vyučovaných na Přírodovědecké fakultě a Fakultě informatiky MU. Hlavní výzvou při realizaci tohoto kurzu bude prototypové propojení testovacích položek agendy Informačního systému s aplikací MapleNet a rozšíření práce s TEXovou notací matematických výrazů zejména v testovacích otázkách.

Kurz práce s informacemi – „informační gramotnost srozumitelně a zábavně“. Interaktivní, prožitkový kurz, jehož cílem je studující zaujmout a podnítit jejich samostatnou práci s informačními zdroji. K tomu autoři kurzu využijí kombinaci textových a grafických materiálů s instruktážními ukázkami práce s aplikacemi.

Podpora výuky předmětů ošetřovatelství – kurz díky velkému množství informací ve videozáznamech, textových a obrazových materiálech povede k získání hlubších vědomostí a dovedností spojených s péčí o pacienty. Studující budou mít možnost získané znalosti intenzivně procvičovat, vzájemně svou práci hodnotit a diskutovat.

Project management – kurz pokrývá problematiku projektového řízení. Mezi přednosti kurzu patří především forma zpracování materiálů s důrazem na studium bez bariér, jazykových nebo fyzických. Absolventi budou mít možnost ucházet se o některý z mezinárodních certifikátů. Navazující výběrové lekce se zaměří na oblast životního prostředí, informačních a komunikačních technologií.

Zdravotní tělesná výchova – kurz je koncipovaný pro všestranné využití při péči o zdraví. V několika rovinách náročnosti poskytne teoretické informace z množství statického materiálu i videoukázek a umožní získat praktické dovednosti k posouzení funkčního stavu pohybového aparátu. Studující bude sám schopen vybrat vhodná vyrovnávací cvičení.

Podrobnější informace o pilotních kurzech jsou k dispozici na webových stránkách eCentra [1]. S vytvořenými kurzy se pak budete moci seznámit počátkem roku 2007, kdy proběhne jejich veřejná prezentace v rámci celouniverzitního semináře.

4 Pilotní kurzy a studující

Velkou pozornost si zasluhuje fakt, že na přípravě i průběhu výuky se stále větší měrou podílí samotní studující. Uplatňují se ve většině autorských týmů: při zpracování grafických materiálů, animací, stříhání videa, vytváření a zpracování testovacích položek, testování a tutorování kurzů. Za zvláštní zmínku přitom stojí právě tutorské zabezpečení průběhu výuky, protože jeho kvalita může konečný efekt nasazení elektronické podpory výuky zcela zásadně ovlivnit. Vzhledem k nárůstu počtu e-learningových kurzů a míře jejich využívání je určitě zajímavé pokusit se studující do tutorské práce zapojit.[1]

Literatura

[1] Informace o velkých kurzech, `http://www.ics.muni.cz/elearning/courses/`

[2] N. Hrtoňová: *Proč e-learning?*, Zpravodaj ÚVT, roč. 16, č. 2, s. 11–16 (`http://www.ics.muni.cz/bulletin/issues/vol16num02/hrtonova/hrtonova.html`) □

Bezpečnost elektronických dat a elektronické komunikace

Andrea Kropáčová, CESNET

Svět moderních počítačových technologií a Internetu je pro řadu uživatelů světem bez jasně daných pravidel a základních záruk, které znají z běžného života. Světem, kde je možné existovat pod smyšlenou identitou, vytvořit si identitu novou, popřít své činy a spoléhat se na anonymitu, nepostižitelnost a nedokazatelnost. Na druhou stranu ale existuje mnoho lidí, možná většina, kteří si uvedená fakta neuvědomují, a všem informacím vystaveným na Internetu či šířeným prostřednictvím elektronické pošty slepě a nekriticky věří. Přitom i v případě papíru, základního záznamového média lidstva, si obvykle uvědomují, že je to snadno zfalšovatelná věc. Že na papír je možné napsat cokoliv, že podpis je možné dokonale napodobit, a že i podepsaný dokument je poté možné modifikovat. Vždyť právě proto si lidé v průběhu staletí vypracovali řadu metod pro *ověření věrohodnosti obsahu, podpisu a integrity* psaných dokumentů. Každý jistě zná podpisové vzory vyžadované bankou, notářsky ověřený podpis, podpis potvrzený přítomnými svědky, soudně ověřený podpis, dokument prověřený pomocí metod grafologie a dalších věd, ověřené kopie dokumentů a další bezpečnostní technologie.

Podobným problémem, jakým je zajištění věrohodnosti dokumentu, je i *bezpečný přenos* dat. Při něm je žádoucí, aby přenášený obsah znali pouze odesílatel a příjemce. Pro mnoho uživatelů je obvykle šokující zjištění, že běžný přenos dat po Internetu je ve své podstatě nezabezpečený a data jsou přenášena v té podobě (obvykle otevřené), jakou jim dal uživatel. Nejvíce je tato neznalost patrná v prostředí elektronické pošty, kdy se často uživatelé diví, že obsah jejich zpráv si cestou může přečíst i někdo jiný, než pouze adresát.

Přitom i ve světě počítačů existuje bezpečný způsob, jak vybavit elektronické zprávy podpisem a pravost tohoto podpisu ověřit, či jak zajistit obsah přenášených dat před nežádoucími slídily. Je jím *elektronický podpis* a *šifrování obsahu zprávy*.

Zašifrování zprávy

Pro vytvoření bezpečné (šifrované) zprávy a elektronického podpisu se v současné době využívají principy tzv. *asymetrické kryptografie*, která pracuje s *dvojicí klíčů (keypair)*. Jeden z klíčů – *veřejný* – se užívá k zašifrování dat a je možné jej zveřejnit. Druhý z klíčů, tzv. *privátní*, je určen k dešifrování; ten musí být pečlivě chráněn

[1] Tutor: specifický termín přejatý z angličtiny. Umožňuje odlišit specifiku pedagogického pracovníka v distančním studiu od klasického učitele v prezenčním studiu. Tutor je metodický zprostředkovatel distančního studia a hodnotitel předběžných výsledků. Je v nejbližším kontaktu se studujícím.

a musí jej znát pouze jeho majitel. Dvojice privátní/veřejný klíč je navržena tak, že z klíče veřejného není možné žádným způsobem odvodit ani spočítat klíč privátní. To zaručuje, že pouze držitel privátního klíče může zašifrovanou zprávu dešifrovat a získat její obsah.

Výměna zabezpečené (zašifrované) zprávy mezi odesílatelem a příjemcem vypadá následovně: odesílatel zašifruje data veřejným klíčem příjemce a odešle je na adresu příjemce; příjemce vezme svůj privátní klíč a zprávu rozšifruje. Podmínkou takové komunikace ovšem je, že odesílatel má k dispozici veřejný klíč adresáta. Získat jej může např. tak, že před započetím šifrované komunikace si uživatelé vymění elektronicky podepsané zprávy, čímž si vzájemně vymění i své veřejné klíče.

Základní algoritmy pro šifrování jsou algoritmy RSA (pojmenované po autorech - Ron Rivest, Adi Shamir and Len Adleman), pro el. podpis pak DSA (Digital Signature Algorithm). Zašifrování obsahu zprávy řeší utajení jejího obsahu tak, aby jej znali pouze odesílatel a příjemce (majitel privátního klíče ke klíči veřejnému, kterým byla zpráva zašifrována).

Elektronický podpis

Elektronický podpis supluje u elektronických zpráv v počítačovém světě ručně vytvořený podpis na písemných dokumentech. Měl by tedy zajistit, že:

- uvedená osoba podepsala data vědomě;
- podepsaná osoba je el. podpisem dostatečně ověřena;
- dokument je pravý a nebyl následně modifikován.

Elektronický podpis je vlastně informace, která se připojuje k datům, aby identifikovala odesílatele. Při procesu vytvoření el. podpisu není podepisována samotná zpráva, jak je u mnoha uživatelů zakořeněno z ekvivalentu papír-tužka, ale ze zprávy se nejprve pomocí tzv. *hashovací funkce* spočítá kontrolní součet (message digest) a ten se zašifruje privátním klíčem odesílatele. Kontrolní součet zašifrovaný privátním klíčem odesílatele je požadovaný el. podpis zprávy. Hashovací funkce pro výpočet kontrolního součtu musí splňovat následující požadavky:

- pro stejnou zprávu spočítá hashovací funkce vždy stejný kontrolní součet;
- z kontrolního součtu není možné zjistit tvar vstupních dat, ze kterých byl kontrolní součet spočítán;
- dvě různé zprávy nesmí vést ke stejnému kontrolnímu součtu.

Důvod, proč se šifruje pouze otisk zprávy (kontrolní součet) a ne celá zpráva, je ryze praktický. Zašifrování celé původní zprávy by vedlo k jejímu zdvojnásobení, kdežto připojením podepsaného otisku se zpráva zvětší pouze o pár bytů. Pro výpočet kontrolního součtu se v současné době používají algoritmy SHA1 a SHA2, které nahradily dříve používaný algoritmus MD5.

Uživatel, který chce zprávu vybavit el. podpisem, k tomu použije svého privátního klíče. Každý, kdo zná jeho veřejný klíč, může pomocí tohoto klíče ověřit pravost připojeného el. podpisu. Přesný postup je následující:

Vytvoření elektronického podpisu: Z dat se pomocí hashovací funkce vytvoří kontrolní součet zprávy. Kontrolní součet zašifrovaný privátním klíčem je požadovaný elektronický podpis vstupních dat, který se připojí k podepsané zprávě.

Ověření elektronického podpisu: Při ověřování elektronického podpisu se postupuje tak, že se pomocí stejné hashovací funkce vypočte kontrolní součet zprávy, pomocí veřejného klíče osoby, která data podepsala, se dešifruje el. podpis a získá kontrolní součet zprávy. V případě, že se oba kontrolní součty shodují, je pravost elektronického podpisu potvrzena. Příjemce el. podepsané zprávy si tak ověří:

- Autenticitu podepisující osoby, protože zprávu mohl podepsat pouze ten, kdo má k deklarovanému veřejnému klíči odpovídající klíč privátní.
- Integritu zprávy. Je-li el. podpis vyhodnocen jako korektní, znamená to, že zpráva nebyla cestou v době mezi vytvořením el. podpisu a

jeho ověřením modifikována, protože hash je stejná jako při vzniku podpisu.
- Odpovědnost odesílatele. Protože privátní klíč zná pouze jeho držitel, je platný elektronický podpis důkazem, že danou zprávu opravdu vytvořil ten, kdo ji také podepsal.

Bezpečnost elektronického podpisu a šifrovaných zpráv

Z předchozího odstavce se může zdát, že el. podpis je plnohodnotným ekvivalentem ručně vytvořeného podpisu papírového dokumentu. Je ale nutné mít na paměti, že ruční podpis je výsledkem vědomé činnosti člověka, který drží v ruce psací pomůcku a v souladu se svými schopnostmi a vědomostmi za plného vědomí vytváří podpis. Kdežto elektronický podpis je řetězec dat, která vytváří software na základě vstupních dat a podmínek, které zná pouze podepisující se osoba.

Z výše popsaných principů el. podpisu a šifrovaných zpráv tedy plynou jeho bezpečnostní rizika a záruky, které jsou postavené především na ochraně privátního a veřejného klíče a bezpečnosti použitých algoritmů. Dá se tedy říci, že bezpečnost používání elektronického podpisu a šifrovaných zpráv je závislá na splnění následujících podmínek:

1. Nedošlo k narušení ochrany privátního klíče, tzn. může s ním disponovat pouze jeho držitel.
2. Nebyl prolomen algoritmus hashovací a šifrovací funkce.
3. Je zaručena a ověřena autenticita veřejného klíče ve vztahu k deklarovanému držiteli, tzn. je doložena pravost klíče (je nutné si být jistý na 100%, že daný klíč patří skutečně dané osobě).

V dnešní době supervýkonných počítačů, které usnadňují práci hackerů a lámání šifer, se kupodivu jako nejproblematičtější jeví podmínka číslo tři – ověření pravosti klíče a jeho vazby na deklarovaného držitele. Představte si, že byste rádi napsali šifrovanou zprávu člověku, který se jmenuje *Pepa Pádlo*, jeho adresa je možná *padlo@kajak.voda* a podaří se vám získat jeho veřejný klíč. Kdo vám ale zaručí, že je to opravdu Pepa Pádlo, a ne někdo, kdo se za něj poťouchle vydává? Tento problém je možné vyřešit v zásadě dvěma způsoby:

- Osobním předáním veřejného klíče danou osobou, kdy tato osoba vám osobně předá svůj veřejný klíč, např. na disketě, a vy máte zároveň možnost ověřit si její totožnost vyžádáním dokladu totožnosti.
- Poskytovatelem certifikačních služeb, tj. Certifikační autoritou.

V menším kolektivu lidí je možné jít první cestou a uživatelé mohou použít např. systém PGP (Pretty good privacy), kde je autentičnost veřejných klíčů postavena na vyslovené důvěře, kterou si držitelé klíčů vzájemně udělují.

V prostředí s velkým počtem uživatelů, kteří se často navzájem neznají, je vhodné jít cestou používání certifikátů a certifikační autority (CA).

Certifikát

Certifikát veřejného klíče je de-facto elektronický průkaz totožnosti, který spojuje člověka s jeho veřejným klíčem. Totožnost se prokazuje na základě znalosti soukromého klíče. Certifikát je podepsaný CA, která jej vydala.

Z hlediska počítačů je certifikát datová struktura obsahující informace o uživateli a především jeho veřejný šifrovací klíč. Nejrozšířenější je struktura certifikátu dle normy X.509 (zavedená doporučením ITU v roce 1988).

Kromě veřejného klíče obsahuje certifikát následující informace:

- Verzi vydaného certifikátu. Nula určuje, že se jedná o certifikát verze 1, jednička určuje verzi 2, dvojka verzi 3. Certifikáty verzí 2 a 3 jsou tzv. *rozšířené certifikáty*.
- Jednoznačné sériové číslo vydaného certifikátu. Je nutné, aby v rámci CA měl každý certifikát vydané unikátní číslo.
- Specifikaci algoritmu použitého pro el. podpis.
- Vymezení platnosti certifikátu od-do (data `notBefore` a `notAfter`). Před dosažením data `notAfter` by si uživatel měl nechat vystavit nový certifikát, z čehož vyplývá, že každý může vlastnit několik platných certifikátů současně.

– dentifikaci CA, která certifikát vydala.
– Identifikaci uživatele, pro kterého je certifikát vydáván, tzn. vlastníka dvojice veřejný/soukromý klíč.
– Alternativní jména/identifikátory subjektu (uživatele), např. e-mail adresu.

Certifikační autority

CA (Certifikační autority) jsou důvěryhodné objekty, které vystavují certifikáty a ověřují totožnost žadatelů. Certifikační autorita plní dvě základní funkce:

– Certifikační – zaručuje, že deklarovaný veřejný klíč přísluší dané osobě.
– Validační – potvrzuje platnost certifikátu.

V případě certifikační role se jedná o vydávání certifikátů uživatelům, kdy certifikát je de-facto dokument, který potvrzuje, že veřejný klíč patří jednoznačně dané osobě. Certifikát je podepsán certifikační autoritou.

Obecně se tedy dá říci, že certifikát je zpráva podepsaná certifikační autoritou, která říká zhruba následující: „Člověku, který se jmenuje Pepa Pádlo, patří adresa padlo@kajak.voda a jeho veřejný klíč je ‘bflmpsvz’“.

CA ručí především za dvě věci – za jednoznačnost vydaných certifikátů a za svázání veřejného klíče s jeho držitelem.

CRL (Certificate Revocation List)

Certifikáty se obvykle vydávají na dobu určitou, tzn. že jejich platnost je omezena. Certifikát může ztratit svou platnost dvěma způsoby:

1. Vyprší, tzn. uplyne čas `notAfter`.
2. Je zneplatněn před časem `notAfter`, přičemž zneplatněn může být na základě žádosti vlastníka nebo na popud CA, která jej vydala.

Ke zneplatnění na žádost vlastníka dochází v okamžiku, kdy došlo např. k prozrazení, nebo zcizení privátního klíče a hrozí tedy zneužití identity, nebo při změně údajů souvisejících s certifikátem. CA může certifikát zneplatnit v okamžiku, kdy ze strany vlastníka dojde k porušení politiky CA (např. jeho nedovolené použití), při chybě způsobené CA, nebo při změně údajů. Certifikáty se také odvolávají v případě, že některý z uvedených identifikátorů subjektu už není platný (např. změna e-mail adresy, příjmení, vztahu k organizaci uvedené v subjektu apod.)

Zneplatněné certifikáty CA uveřejňuje v tzv. seznamu zneplatněných certifikátů – CRL (Certificate Revocation List). Postup, jakým vlastník certifikátu může požádat o jeho zneplatnění, je popsán v politice dané CA, která certifikát vydala.

CRL obsahuje sériová čísla zneplatněných certifikátů a může být i prázdný! Certifikáty revokované před naplněním data `notAfter` se v CRL zveřejňují až do vypršení jejich původní doby platnosti.

Součástí CRL jsou kromě sériových čísel ještě další údaje, např. datum vydání předchozího CRL a datum vydání následujícího CRL. Uživatel si tak může ověřit, jestli nepropásl vydání předchozího CRL. Další užitečná položka je položka `RevocationDate`, která říká, kdy byl certifikát zneplatněn, tzn. shledán podezřelým. Od tohoto data by všechny podpisy tímto certifikátem měly být považovány za nevěrohodné.

O způsobu zveřejňování CRL rozhoduje daná CA, která tak může učinit například prostřednictvím el. listů nebo vystavením na webu.

Je v zájmu každého uživatele, aby si seznamy zneplatněných certifikátů těch CA, jejichž certifikáty používá, pravidelně aktualizoval a používal je.

Použití certifikátu

Aby uživatel mohl certifikát úspěšně používat, musí být splněno několik podmínek:

– Certifikát musí být platný, tzn. čas je mezi `notBefore` a `notAfter` a není uveden v CRL (nesmí být revokovaný).
– Certifikát musí být podepsaný CA, které uživatel důvěřuje, a který tudíž má v seznamu důvěryhodných CA.
– Uživatel musí mít k dispozici veřejný klíč té CA, která certifikát vydala.

V případě komunikace mezi dvěma uživateli si uživatelé nejdříve ověří podpis svého protějšku

pomocí jeho veřejného klíče a posléze si ověří autentičnost veřejného klíče ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority, která jej vydala. V daném případě se požadavek na důvěryhodnost vztahuje pouze k certifikační autoritě.

V případě validace se uživatel dotazuje certifikační autority na platnost certifikátu svého protějšku. Dotazy mohou být kladeny on-line, nebo lze využít CRL.

CESNET CA

Certifikační autorita CESNETu byla založena v roce 2001, původně pro potřeby projektu DataGrid. Od roku 2003 poskytuje své služby členům sdružení CESNET z.s.p.o. CESNET CA (`https://www.cesnet.cz/pki`) nabízí v současnosti tři základní služby:

1. Vydávání osobních certifikátů – slouží pro zabezpečení komunikace prostřednictvím el. pošty (standard S/MIME) a autentizaci (např. k privátním WWW stránkám)
2. Vydávání certifikátů serverů a služeb – slouží k autentizaci služeb a počítačů, největší uplatnění mají při chráněné WWW komunikaci
3. Certifikuje další úřady – členové sdružení CESNET mohou založit vlastní certifikační autoritu, kterou CESNET CA certifikuje. Tím mezi certifikačními autoritami vzniká vazba, tzv. *řetězec důvěry*, což v praxi znamená, že ti uživatelé, kteří věří CESNET CA, budou automaticky věřit i nově vzniklé CA, která má certifikaci od CESNET CA.

Přínos el. podpisu a šifrování zpráv

Přínos šifrování zpráv je zřejmý: ochrana citlivých dat na cestě mezi odesílatelem a adresátem a tím minimalizování jejich zneužití.

Elektronický podpis má mnohem větší efekt a uplatnění, když si uživatel uvědomí všechny souvislosti; nikoliv pouze tu, že vybavení zprávy el. podpisem příjemci potvrdí odesílatele a ukáže, jestli zpráva nebyla cestou změněna (třeba ani ne úmyslně s cílem škodit, ale např. špatně nebo příliš restriktivně nakonfigurovanou antispamovou ochranou). Zřejmě každý, kdo používá elektronickou poštu, se již setkal s tím, že mu od něj samotného přišla zpráva, o které ví, že si ji neposlal. Nebo mu kolega sdělí, že od něj obdržel zprávu, kterou ale ve skutečnosti odesílatel uvedený v dopise neposlal. Je to důsledek problému nazývaného „spamming“ a faktu, že do položky „Odesilatel“ v prostředí e-mailové komunikace, může být vloženo cokoliv, tedy i adresa někoho úplně jiného, než kdo zprávu skutečně odesílá. Člověk pak může být obviněn z něčeho, čeho se nedopustil. Řešením je opět (částečně) el. podpis. Částečně proto, že tento případ již vyžaduje znalost a používání principů el. podpisu v širším měřítku. Představte si svět, ve kterém každý člověk používající el. poštu, má osobní certifikát a odesílanou poštu poctivě podepisuje. V takovém světě je pak ověření, jestli daná zpráva skutečně pochází od v ní uvedeného odesílatele, záležitostí vteřin. V případě, že dopis podepsán není nebo podpis není korektní, platí, že je nepravděpodobné, že zprávu skutečně odeslal uvedený odesílatel a tudíž jej za obsah zprávy není možné činit zodpovědným. Ano jistě, takový svět je teprve budoucností.

Uživatelé často kladou otázku „Kdy mám podepisovat a kdy mám šifrovat?“. Samozřejmě je možné obojí současně. Osobně *doporučuji podepisovat každou odesílanou zprávu, šifrovat je pak vhodné ty zprávy, které nesou citlivý obsah*, který by měl znát pouze příjemce.

K čemu se to dá použít dál?

Elektronický podpis a možnost zašifrovat zprávu posílanou el. poštou nejsou jedinými možnostmi jak využít veřejný a privátní klíč (X509 certifikát, nebo PGP). Elektronický podpis se dá využít např. také pro podepsání WWW stránky s citlivými údaji a obecně pro podepsání, a tím ochranu integrity jakýchkoliv el. dat – souboru, obrázku a podobně.

Osobní X509 certifikát nebo PGP klíč je možné použít také pro ochranu osobních dat na pracovní stanici a na záznamovém médiu. Stačí soubor s citlivými daty zašifrovat.

Dalším využitím je *autentizace*. Autentizace je proces ověření identity uživatele (nebo služby). Nejrozšířenější metodou autentizace je kombinace uživatelského jména (login) a hesla

(password), které se ověřují proti nějaké databázi. Autentizační mechanismy založené na PKI (Public Key Infrastructure), kdy každý uživatel (a služba) mají vydán vlastní certifikát veřejného klíče podepsaný důvěryhodnou CA, přinášejí do oblasti autentizace škálovatelnost, robustnost a usnadňují administraci.

Závěr

Možná vás po přečtení tohoto článku napadne otázka – „A jak vlastně ten elektronický podpis získám?“. Elektronický podpis sám o sobě samozřejmě získat nelze. Prvním krokem na cestě k jeho používání je získání PGP klíče nebo X509 certifikátu. V případě PGP klíčů doporučuji podívat se například na stránky `http://www.pgp.cz` a konzultovat to se zkušenějšími kolegy. V případě X509 certifikátů je zásadní otázkou „Na kterou CA se mohu obrátit se žádostí o certifikát?“ V tomto případě doporučuji porozhlédnout se v rámci university a zjistit, jestli ta CA neprovozuje.

Získání certifikátu veřejného klíče samozřejmě není pro ochranu dat a el. komunikace posledním krokem, není samospasitelné a určitě není jednorázovým řešením. Ruku v ruce s používáním certifikátu jde ochrana privátního klíče před zcizením a zničením. To v praxi znamená dobře uvážit, kde je možné privátní klíč uložit (pouze na zabezpečený stroj, který je plně pod vaší správou) a jak s ním nakládat (mít zálohu, nikomu jej „nepůjčovat“ a podobně). Samozřejmě je vhodné být připraven i na možnost zcizení privátního klíče a na tuto skutečnost rychle reagovat zneplatněním.

Co říci závěrem? Snad jen doporučení – podepisujte a šifrujte. Není tak daleko doba, kdy tyto mechanismy budou nedílnou součástí běžného života, a čím větší počet lidí si na jejich užívání navykne, tím bude efektivnější. Bezpečná komunikace už v dnešní době není planá fráze, ale nutnost a realita. □

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