

Data gram

zpravodaj sdružení CESNET

číslo 13

listopad 2006

CESNET a PlanetLab

V srpnu se sdružení CESNET stalo členem mezinárodního konsorcia *PlanetLab*. Jeho cílem je vývoj nových aplikací pro Internet budoucnosti, které vznikají ve velmi nestandardním prostředí experimentální sítě.

Konsorcium *PlanetLab* založila v roce 2002 trojice amerických univerzit: University of California at Berkeley, Princeton University a University of Washington. Většinu ze současných více než tři set členů stále tvoří univerzity z několika desítek zemí světa, výzkumné ústavy a provozovatelé národních či regionálních akademických sítí. Vedle nich do konsorcia vstoupily i významné firmy působící v oblasti síťových služeb (Google) či informačních technologií (Intel, HP).

Členové *PlanetLabu* společně provozují experimentální síť, určenou jako prostředí pro vývoj nových aplikací. Počet jejích uzlů již překročil 700 a najdete je po celé zeměkouli. Nejvíce se pochopitelně koncentrují v informaticky nejrozvinutějších oblastech - USA, západní Evropě a východní Asii:



Základním krédem sítě *PlanetLab* je virtualizace, která umožňuje koexistenci jednotlivých aplikací, aniž by se navzájem ovlivňovaly. Každá aplikace si může v síti vytvořit vlastní virtuální infrastrukturu s vlastní adresací i vlastními algoritmy vyhledávání dat. Celá síť se pak chová jako několik navzájem nezávislých sítí.

Jedním z nejvýznamnějších projektů *PlanetLabu* je *OceanStore* - globální systém pro spolehlivé ukládání dat, jehož uživatelé se nestarají o to, kde se jejich data fyzicky nacházejí. Na distribuci dat se zaměřuje i projekt *Coral* orientovaný na efektivní distribuci dat uživatelů s pomalým připojením. Několik projektů usiluje o zvýšení výkonu a spolehlivosti jednotlivých služeb pomocí paralelizace (*CoDeeN*, *CoDNS*, *CoBlitz*, *CoWeb* a další).

Prostřednictvím CESNETu mají nyní k těmto experimentům přístup i odborníci z České republiky.

Rozvoj sítě eduroam

V Datagramu číslo 9 jsme vás informovali o projektu *eduroam*, jehož cílem je usnadnit mobilitu akademických uživatelů. Jeho základem je propojená autentizační infrastruktura, díky níž se uživatel hostující v některé ze sítí zapojených do projektu autentizuje vždy ve své domácí instituci. V hostitelské síti pro něj není nutné nic nastavovat, jednoduše se připojí a komunikuje. Podobný model funguje například při roamingu mobilních telefonů.

Od svého vzniku se síť *eduroam* v České republice utěšeně rozrůstá. V současnosti je do ní zapojeno již více než patnáct institucí z osmi různých měst. Z valné většiny se jedná o univerzity, čestnými výjimkami jsou pražská Soukromá střední škola výpočetní techniky a Masarykova nemocnice v Ústí nad Labem.

Podpora Ministerstva informatiky

Významný přínos pro další rozvoj této sítě představuje úspěch ve výběrovém řízení Ministerstva informatiky na podporu vysokorychlostního Internetu. Náš *Projekt na podporu síťové infrastruktury v rámci akademického roamingového systému eduroam* se zařadil mezi necelou padesátku vybraných z téměř tří set uchazečů.

Ministerstvem přidělená dotace 2 miliony Kč bude investována především do rozšíření zapojených sítí a konsolidace autentizační infrastruktury.

Končí autentizace eduroam-simple

eduroam od svého vzniku nabízel tři alternativní způsoby autentizace: plně zabezpečený 802.1X, VPN tunel do domácí sítě a jednoduchý WWW formulář. Letos v červnu dospěla mezinárodní komunita koordinující jeho rozvoj k rozhodnutí zachovat pouze první z nich.

Hlavním problémem VPN tunelů je špatná škálovatelnost, díky níž se tato varianta prosazovala jen ve velmi omezené míře. Autentizace WWW formulářem (nazvaná *eduroam-simple*) naproti tomu trpí vážnými bezpečnostními nedostatky. Nelze v ní zabránit úniku důvěrných uživatelských dat.

Rozhodnutí o ukončení autentizace *eduroam-simple* bylo velmi bolestné, protože je pro svou jednoduchost mezi uživateli oblíbená. Autoři projektu však dospěli k názoru, že ohrožuje důvěryhodnost celého projektu a musí být nejpozději do 1. října 2007 ukončena. Podrobnější informace i zdůvodnění najdete na stránkách www.eduroam.cz.

Certifikáty GlobalSign pro vaše servery

Řada služeb poskytovaných uživatelům vyžaduje v určitých fázích přenos důvěrných dat, jako jsou uživatelská jména a hesla. Aby se zabránilo jejich odposlechu, bývá taková komunikace šifrována (HTTPS, IMAPS a podobně).

Vlastní šifrování však zajišťuje jen utajení přenášených dat. Zůstává jiné nebezpečí: falešný server. Pokud by se někomu podařilo vydávat se např. za univerzitní webmail, mohl by získat přihlašovací údaje mnoha uživatelů.

Certifikáty

K odstranění tohoto problému se server prokazuje certifikátem, což bývá standardní součástí navázání komunikace některým z šifrovaných protokolů. *Certifikát* je digitální verze osvědčení o pravosti, kterým jistá instituce potvrzuje, že certifikát skutečně náleží serveru uvedeného jména a že tento server používá pro kryptografické účely veřejné klíče obsažené v certifikátu. Tyto údaje jsou potvrzeny digitálním podpisem dotyčné instituce, kterou je tak zvaná *certifikační autorita (CA)*.

Jestliže klient důvěřuje dotyčné certifikační autoritě (zná ji a má k dispozici její veřejné klíče), bude věřit jí vydaným certifikátům a bude proto považovat údaje o serveru za ověřené. Jestliže klient tuto certifikační autoritu nezná, může požádat o její certifikát, jímž autentičnost certifikační autority ověřuje jiná, nadřazená certifikační autorita. Tímto způsobem lze budovat tak zvaný řetězec důvěry – sekvenci certifikátů vedoucí od některé z klientovi známých autorit až po cílový server, v níž jednotlivé certifikáty postupně stvrzují platnost údajů o dalším členovi řetězce.

Každý klient bývá od výrobce vybaven údaji o některých zavedených certifikačních autoritách. Jejich přehled můžete v MS Internet Exploreru získat, když z hlavního menu zvolíte *Nástroje/Možnosti sítě Internet*. Na kartě *Obsah* pak stisknete tlačítko *Certifikáty* a v dialogovém okně vyberte kartu *Důvěryhodné kořenové certifikační úřady*. Pokud používáte Firefox, vyberte z menu *Nástroje/Možnosti*. Na kartě *Rozšířené* zvolte podkarty *Šifrování* a na ní tlačítko *Certifikáty*. Objeví se nový dialog, jehož karta *Certifikační autority* vás dovede k cíli. Serverům, jejichž certifikáty dokáže ověřit řetězcem vycházejícím z některé z těchto autorit, klient důvěřuje.

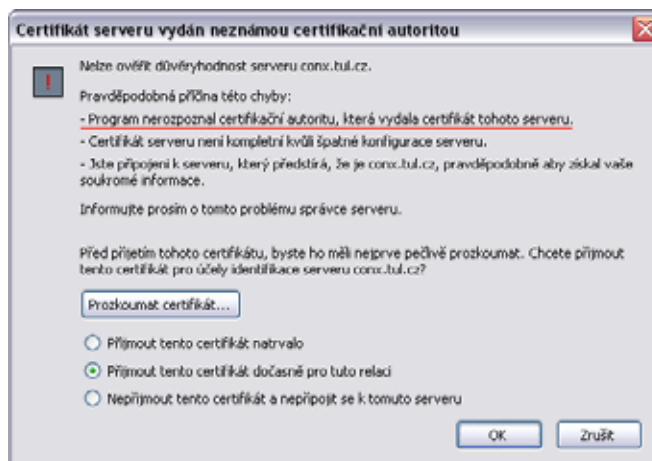
CESNET CA

Sdružení CESNET provozuje certifikační autoritu CESNET CA, jež poskytuje služby členům sdružení. Těmi nejběžnějšími je vydávání certifikátů, a to jak serverových, tak osobních.

CESNET CA však sama není certifikována žádnou z globálních autorit, známých klientům ve výchozí konfiguraci. Důvodem jsou především finanční nároky takové certifikace, které by znamenaly, že certifikáty vydávané CESNET CA by musely být zpoplatněny. Takovou službu CESNET nemá zájem provozovat.

Mají-li klientské programy pro WWW, elektronickou poštu a další služby akceptovat certifikáty CESNET CA, je třeba do nich instalovat její kořenový certifikát. Lze jej získat na adrese <http://www.cesnet.cz/pki/cs/ch-CRT-CRL.html>. Postup instalace se liší v závislosti na konkrétním programu.

Pokud klient nezná kořenový certifikát CESNET CA, vyvolá pokus o připojení k serveru certifikovanému touto autoritou varovný dialog s upozorněním, že nelze ověřit autentičnost cílového serveru.



To je jednak nepříjemné, ale především se tím podporuje nebezpečný uživatelský návyk potvrzovat dialogy ohlašující bezpečnostní problémy bez hlubšího zamyšlení, co je způsobilo. Všimněte si také, že dialog je obecný – stejné hlášení klient vydá i v případě, že certifikát byl padělán (čímž se problém falešných serverů vrací zpět do hry).

Řešením je instalovat kořenový certifikát CESNET CA. To však vyžaduje součinnost mnoha uživatelů (často laických), navíc je třeba postup opakovat po reinstalaci systému.

Certifikáty SureServer EDU

Stejně problémy trápí i další národní sítě pro vědu, výzkum a vzdělávání. Proto se dohodlo osm jejich provozovatelů na společném postupu. Sdružili své prostředky a vypsalí výběrové řízení s cílem uzavřít smlouvu s některou z certifikačních autorit uznávaných klientskými programy ve výchozím nastavení. Ze soutěže nakonec vyšla vítězná autorita GlobalSign.

K uzavření smlouvy došlo na jaře letošního roku. Následoval pilotní provoz ověřující funkčnost celého systému a od podzimu jsou certifikáty nazvané SureServer EDU k dispozici pro servery členů sdružení. Jejich hlavní výhodou je, že jsou akceptovány běžnými klientskými programy, aniž by uživatel musel cokoli instalovat či nastavovat. Stejně jako certifikáty CESNET CA jsou členům sdružení vydávány bezplatně. Doporučujeme všem správcům služeb v síti CESNET2, aby je začali používat.

K jejich získání musí nejprve daná instituce vstoupit do certifikačního programu. V době vzniku tohoto textu byly zapojeny Akademie múzických umění, Slezská univerzita, Technická univerzita v Liberci, Univerzita Karlova a Vysoká škola chemicko-technologická. Vstup do programu certifikátů SureServer EDU vyžaduje jen, aby statutární zástupce instituce jmenoval administrativní kontakty. Jedná se o osoby zodpovědné za schvalování žádostí o certifikáty pro servery dané instituce.

Jakmile se instituce zapojí do programu, je získání certifikátu zcela jednoduché. Správce serveru prostřednictvím WWW formuláře vytvoří a odešle žádost o certifikát. Administrátor je systémem požádán o vyjádření a pokud přidělení certifikátu schválí, je žádost po kontrole pracovníkem CESNETu předána GlobalSign. Zde je vytvořen certifikát a odeslán správci serveru k instalaci. WWW rozhraní umožňuje i odvolání certifikátu, pokud by se dostal do nepovolaných rukou. Vše potřebné najdete na adrese

<http://www.cesnet.cz/pki/cs/st-guide-gs.html>

CEF Networks Workshop 2006

Pražský *CEF Networks Workshop* se stal již pravidelným záznamem v diářích odborníků zaměřených na nasazení optických přenosových technologií v počítačových sítích. Ten letošní se konal od 29. do 31. května a sjelo se na něj 43 účastníků z řady evropských zemí, USA a Kanady.

Většina z celkového počtu devatenácti příspěvků popisovala zkušenosti s budováním optických sítí provozovaných zákazníky v jednotlivých státech a oblastech. Jejich počet i obsah svědčí o tom, že koncept CEF (Customer Empowered Fiber) se úspěšně prosazuje v sítích všech velikostí - od městských až po kontinentální. Vedle univerzit a národních sítí pro vědu, výzkum a vzdělávání dnes CEF sítě nasazují i instituce místní samosprávy, nemocnice či komerční subjekty.

Účastníci semináře formulovali závěry, v nichž doporučili pro další rozvoj CEF sítí podporovat:



- průzkum dostupnosti nenasvícených vláken a zavádění sítí CEF pro výzkumné a vzdělávací účely ve zbývajících státech a regionech, včetně nenasvícených vláken překračujících hranice států,
- vyhodnocování a zavádění pokročilých technologií nasvícování vláken pro výzkumné a vzdělávací sítě,
- specifikaci požadavků na interoperabilitu a pravidel pro nákup vybavení a přístrojů a standardizační práce,
- výzkum počítačových sítí včetně vývoje rozlehlých testbedů na bázi nenasvícených vláken,
- zdokonalování sdílení a nasvícování vláknové základny pro výzkumné činnosti,
- vzájemnou výzkumnou spolupráci,
- pokračování výměny informací.

Účastníci se také shodli na kladném hodnocení prezentací i přípravy semináře a doporučili jeho další pokračování.

Seminář IP telefonie

Značný zájem odborné veřejnosti vzbudil náš seminář věnovaný IP telefonii. Zúčastnilo se jej bezmála sto odborníků z univerzit, výzkumných ústavů, ale i komerčních firem. Otázka využití Internetu pro přenos telefonních hovorů i dalších audiovizuálních služeb je v současnosti velmi aktuální.

Přednášející představili základní technologické prvky IP telefonie, jako je signalizační protokol SIP či systém ENUM využívající doménová jména (DNS) pro ukládání informací relevantních pro IP telefonii.

Zazněly i příspěvky praktičtější orientované, v nichž se účastníci seznámili s nejoblíbenějšími volnými programy z této oblasti, jimiž jsou SIP Express Router a softwarová ústřena Asterisk.

Ukázkou využití moderních technologií byl popis projektu IP telefonie Západočeské univerzity v Plzni, který kombinuje SIP s bezdrátovou počítačovou sítí (Wi-Fi). Hybridní mobilní telefony umožňují využít v areálu univerzity místní bezdrátovou síť jako médium pro běžná volání.

