EurOpen.CZ
Česká společnost uživatelů otevřených systémů
www.europen.cz

XXIII.konference
Hotel Flag
Strážnice
28.9. – 1.10.2003

Programový výbor

Dostálek Libor, PVT a.s., České Budějovice
Felbáb Jiří, ICZ a.s. Praha
Novotný Jiří, Masarykova univerzita Brno
Pavlík Roman, Trusted Network Solutions, Bílovice nad Svitavou
Rudolf Vladimír, Západočeská univerzita Plzeň

Vážení kolegové, vážené kolegyně

pozvání na podzimní konferenci je pro mne spojeno s nádvořím novohradského hradu a posezením, které bylo součástí letošní jarní konference. Tam vykrystalizoval program akce, který držíte v rukou.

U jednoho stolu se zrodil základ celé úterní sekce soustředěné na projekt Liberouter, u druhého se zformovala sekce středeční zaměřená na IP telefonii a Voice over IP. Probrali jsme řadu dalších témat a určitě mnohá budou zařazena na některé z dalších konferencí.

Stejně důležitý byl i zájem kolegů, kteří se ozvali osobně nebo mailem a nabídli zajímavá témata.

Program konferencí odráží současné trendy vývoje informačních technologií. Jeho skladba je jistě výsledkem dramaturgického plánu programového výboru, ale odraz aktuálních trendů se automaticky prosazuje i v nabídkách příspěvků, tak jak je dostáváme, a má podstatný vliv na jeho konečnou podobu. Díky tomu se do programu konference podařilo zařadit mimo jiné Multimedia Home Platform, zabývající se problematikou, o které na konferenci nebyla řeč velmi dlouho.

Strážnická konference je v jednom směru průkopnická. Celá úterní sekce je věnována původnímu řešení spojujícímu základní a aplikační výzkum a vyvinutého spojenými silami akademických institucí a účelových organizací Zaznamenali jste někdy, jaký podíl zaujímají podobné příspěvky například na konferencích Usenixu?

Úvodní slovo docenta Štyse v Nových Hradech bylo pro většinu účastníků objevné. Budování regionálního nadnárodního akademického centra je činnost jistě velmi motivující. Podle ohlasů se jednalo o jeden z nejvýše hodnocených příspěvků. Úvodní slovo strážnické konference toto téma dále rozvíjí a bude nepochybně také velmi zajímavé.

Tutoriál měl v Nových Hradech obrovský úspěch. Byl beznadějně zaplněn krátce po zveřejnění programu a všechny zájemce nebylo možné uspokojit, přestože byl díky ochotě Petra Břehovského zopakován ještě jednou ve středu odpoledne. Téma ASN.1, BER a DER není jistě tak atraktivní jako typy internetových útoků, ale je stejně podstatné. Přednášející v anotaci přesně vystihl, oč jde: „pro pochopení principů bezpečnosti TCP/IP je nutná znalost těchto standardů. Avšak tyto standardy jsou považovány za jedny z nejnezáživnějších a tak ten, kdo nemusí, se jejich studiu vyhýbá.“ PKI tutoriál kolegy Dostálka na konferenci v Jetřichovicích byl velmi zajímavý a jisté je, že že i tento tutoriál by bylo škoda si nechat ujít.

Pomalé kouření dýmky, závěrečný příspěvek pondělního odpoledne, jistě vyvolá živou diskusi. Velmi se na ní těším.

Tradičně je zařazena i večerní sekce, tentokráte zaměřena na antickou filosofii a její vztah k dnešní době. Nepochybně i ta povede k zajímavé diskusi. Do té si dovolím příspěvek předem. Pobavil mě nedávno jeden z hrdinů knihy ‘Mr. Sammler‘s Planet‘ Američana Saula Bellowa, nositele Nobelovy ceny za literaturu. Ten pragmaticky nahlas uvažuje: “’All men by nature desire to know’. That’s the first sentence of Aristotle’s *Metaphysics*. I never got much farther, but I figured, that the rest must be out of date anyway.” Má pravdu?

Samostatnou součástí konference je Key Signing Party, která se uskuteční v pondělí 29.září v hotelu Flag ve Strážnici. Garantem akce je Roman Pavlík a veškeré podrobnosti lze najít na adrese http://www.gpg.cz/~rp/keysigning2/ i v tomto programu. Pro účast na party není podmínkou účast na konferenci.

Konferenci jistě netvoří pouze příspěvky. Večerní přátelská posezení bývají velmi zajímavá – vybavuji si namátkou Třeboň, Malou Úpu, Velké Bílovice, Znojmo či naposledy právě Nové Hrady. Ani ve Strážnici to jistě nebude jiné. 80 sklepů zasazených ve stínu staletých listnáčů ve svahu poblíž Petrova nabízí k takovému posezení velmi inspirující prostředí.

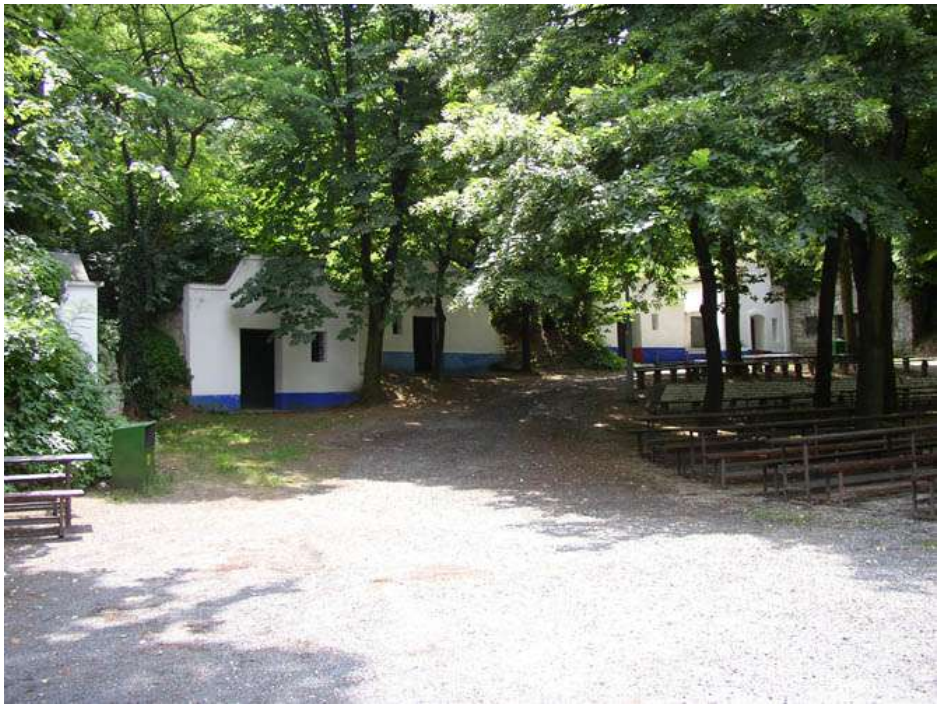
Nelze zde opomenout ani Strážnici a její blízké okolí: zámek, skanzen, Baťův kanál, Bílé Karpaty a řadu dalších míst v bezprostředním okolí, které představují velmi atraktivní prostředí.

Před pár lety se mi na závěr konference sdružení NLUUG v předsálí konferenčního centra v Maastrichtu zeptal neznámý kolega se slušností Holanďanům vlastní - víceméně aby „řeč nestála“ - jak se mi konference líbila. „Byla velmi zajímavá“, odpověděl jsem, „Eric Allman a další celebrity a řada zajímavých příspěvků“. „Určitě!“, řekl. „ale já sem jezdím hlavně kvůli setkání s lidmi – ať už jsou to noví známí nebo ti, se kterými se leckdy celý rok nevidím“.

Děkuji všem přednášejícím, kteří přijali naše pozvání, všem, kteří se podíleli na přípravě konference i všem, kteří se participují na zajištění chodu sdružení.

Přeji vám, aby konference byla obsahově podnětná, profesionálně motivující a společensky uvolněná. A také abychom se sešli s těmi, se kterými nemáme možnost se jindy setkat, a aby tato setkání byla obohacující.

Jiří Felbáb
předseda rady sdružení EurOpen.CZ



Vinné sklepy v Petrově

Neděle 28.9.	Tutorial	
13:00 17:00	**ASN.1, BER a DER**	**Libor Dostálek** PVT a.s.

Pondělí 29.9.	Multimedia Home Platform	
9:00	**Úvodní slovo**	**Jiří Felbáb** EurOpen.CZ
9:05	**Role výzkumu a univerzit v EU**	**František Ježek** Fakulta aplikovaných věd ZČU Plzeň
10:05	Přestávka na kávu	
10:30	**Úvod do MHP jakožto standardu digitální televize**	**Dušan Juhás** Panasonic Europe Software Development Laboratory (PESDL) s.r.o.
11:30	**Vývoj aplikací pro digitální televizi na platformě MHP**	**Daniel Štefl** Panasonic Europe Software Development Laboratory (PESDL) s.r.o.
12:45	Dotazy a závěr dopolední části	
13:00	**Oběd**	
14:00	**DVB, linux a bussiness**	**Jan Petrouš** UniBase Softwares.r.o.
15:00	**Amatérské řešení lokální sítě s využitím Wi-Fi**	**Jiří Kašpar**
15:45	Přestávka na kávu	
16:15	**Pomalé kouření dýmky a internetové technologie**	**Tomáš Novotný, Jiří Novotný**
17:15	Diskuse a závěr prvního dne	
17:30	**Key signing party**	
18:30	**Večeře**	
19:30	**Valná hromada členů EurOpen.CZ**	
20:00	**Vybrané aspekty antické filosofie a dnešek**	**Josef Petželka** Katedra filosofie Filozofická fakulta MU Brno

Úterý 30.9.	Projekt Liberouter	
9:00	**HW/SW Co-Design of Routers**	**Otto Fučík** Fakulta informačních technologií VUT v Brně
9:45	**Vyhledávání v IPv6 směrovači implementovaném v hradlovém poli**	**David Antoš** Fakulta informatiky MU v Brně **Vojtěch Řehák** Fakulta informatiky MU v Brně **Jan Kořenek** Fakulta informačních technologií VUT v Brně
10:30	Přestávka na kávu	
11:00	**Vývoj nanoprogramů pro procesory implementované v hradlovém poli**	**Filip Hőfer** Fakulta informatiky MU Brně
11:45	**Netopeer - konfigurační systém pro směrovače a sítě IP**	**Ladislav Lhotka** CESNET, z.s.p.o. Praha
12:45	Dotazy a závěr doplední sekce	
13:00	Oběd	
13:45	Práce v sekcích	
18:00	Večeře s posezením ve vinných sklepích v Petrově	

Středa 1.10	Voice over IP	
9:00	**IP telefonie a její praktické využití**	**Jiří Novák** NET-SYSTEM s.r.o., Liberec
10:15	**Hlasové služby v síti CESNET2**	**Miroslav Vozňák** Vysoká škola báňská – Technická univerzita Ostrava Fakulta elektrotechniky a informatiky
11:00	Přestávka na kávu	
11:30	**VoIP a zkušenosti při implementaci v praxi**	**Vladimír Toncar** Kerio Technologies s.r.o. Plzeň
12:20	Závěr třetího dne a zakončení konference	
12:45	Oběd	

ASN.1, BER a DER

Libor Dostálek
PVT a.s. České Budějovice
dostalek@pvt.cz

Tutoriál bude věnován ASN.1, BER a DER. Na těchto standardech stojí většina z těch protokolů rodiny TCP/IP, které řeší bezpečnost. Proto pro pochopení principů bezpečnosti TCP/IP je nutná znalost těchto standardů. Avšak tyto standardy jsou požadovány za jedny z nejnezáživnějších, a tak kdo nemusí, tak se jejich studiu vyhýbá.

Cílem tutoriálu je populární formou probrat tyto důležité standardy. Bude probírán jazyk ASN.1, který popisuje datové struktury. Dále bude probráno kódování datových do BER i DER. Jelikož čeština nevystačí s ASCII znaky, tak se dále budeme zabývat i kódováním textů v UTF-8.

Součástí tutoriálu bude i ukázka programů, které řeší zobrazení binárně kódovaných dat (BER či DER) zpět do ASN.1, tj. do tvaru čitelného pro člověka.

Libor Dostálek
(*1957) vystudoval Matematicko-fyzikální fakultu UK. Dvacet let se věnuje vývoji a výuce programového vybavení. Nyní pracuje jako vedoucí konzultačního oddělení PVT,a.s. a je členem dozorčí rady PVT,a.s. Specializuje se na e-commerce a e-banking. Byl správcem firewallu, hostmasterem PVTnet a architektem řady aplikací v oblasti elektronického bankovnictví. Podílel se i na projektu I. Certifikační autority.

Role výzkumu a univerzit v EU

František Ježek
Fakulta aplikovaných věd ZČU Plzeň
JEZEK@KMA.ZCU.CZ

Diskutována je pozice ČR v rámci EU a pozice EU v rámci zemí OECD z hlediska konkurenceschopnosti vázané na výzkum. Uvedena je role univerzit z hlediska prosperity země tak, jak je popsána ve strategických dokumentech EU. Formulovány jsou hypotézy dalšího rozvoje vědy a její infrastruktury v ČR.

Příspěvek obsahuje i zamyšlení nad rolí informačních technologií ve vědě a terciárním sektoru vzdělávání. Vysvětlen je historický vývoj počítačové podpory tvůrčí technické práce s tím, že příspěvek je uzavřen popisem strategie PLM (product lifecycle management).

František Ježek
Působení na ČVUT a ZČU jako učitel v oblasti geometrie, matematiky, informatiky, počítačové grafiky a geometrického modelování. Zkušenosti z celoživotního vzdělávání v oblasti ICT. Účast na samosprávě vysokého školství (Rada vysokých škol) a činnost v radách infrastrukturních a vědeckých programů.

Úvod do MHP jakožto standardu digitální televize

Dušan Juhás
Panasonic Europe Software Development Laboratory (PESDL), s. r. o.
juhas@panasonic-software.cz

Standard MHP (Multimedia Home Platform) bude zasazen do kontextu digitální televize. Stručně budou popsány důvody vzniku MHP, jeho historie, současnost a možná budoucnost. Posluchači se dozvědí odpověď na otázku: „Kdo může čerpat z výhod otevřeného standardu MHP?“ Výklad bude obsahovat základní rozdělení a strukturu standardu. Klíčovým komunikačním prostředkem v MHP je v současnosti programovací jazyk Java. Některým účastníkům prezentace budou možná známa aplikační rozhraní Javax a HAVI, která jsou ve standardu použita. Podrobněji budou popsány podstatné pasáže týkající se např. grafického rozhraní, bezpečnosti, DSMCC (nebo-li souborového systému na multimediální úrovni) apod. Protože se jedná o poměrně širokou problematiku, bude v závěru uveden obsáhlejší seznam odkazů na další informace.

Dušan Juhás
V roce 1998 vystudoval informační a řídicí techniku na ZČU v Plzni. Později do roku 2002 pracoval v ICZ, kde získal menší zkušenosti s většími databázovými systémy. Od roku 2002 pracuje jako sw. vývojář, správce CVS a nástěnkář ve firmě s neuvěřitelně dlouhým názvem Panasonic Europe Software Development Laboratory (PESDL), kde se podílí na vývoji software pro digitální televize. Je nadšeným příznivcem a věčným nedoukem Perlu. Tu a tam také fušuje do CMS PostNuke a překladů počítačové literatury.

Vývoj aplikací pro digitální televizi na platformě MHP

Daniel Štefl

Panasonic Europe Software Development Laboratory (PESDL), s. r. o.

stefl@panasonic-software.cz>

Kromě sledování televizních pořadů umožňuje digitální televize i běh interaktivních aplikací v digitálním televizním přijímači. Pokud má být možné spouštět na přijímačích od různých výrobců aplikace vysílané různými televizními společnostmi, je třeba, aby se všichni shodli na jednotném aplikačním rozhraní. Takovým obecným rozhraním je Multimedia Home Platform (MHP), vytvořená konsorciem Digital Video Broadcasting (DVB). Vývojem MHP aplikací zajímavých pro televizní diváky, s ohledem na možnosti současného hardware digitálních televizních přijímačů, se zabývá tento článek. Jsou diskutovány vývojové nástroje a techniky používané pro tvorbu MHP aplikací v jazyku Java. Dále je představen vývojový kit usnadňující vývoj, testování a ladění. Také je zmíněno rozhraní Xlet, používané pro kontrolu životního cyklu MHP aplikace firmwarem digitálního televizního přijímače.

Daniel Štefl
Pracuje jako vývojový inženýr v laboratořích společnosti Panasonic, kde se zabývá vývojem aplikací pro digitální televizi. V minulosti se podílel na realizaci kitu určeného pro efektivní vývoj MHP aplikací. V rámci doktorandského studia na Západočeské univerzitě zkoumá rozhraní člověk-technický systém, zejména s ohledem na ovládání digitálních televizních přijímačů.

DVB, linux a bussiness

Jan Petrouš
UniBase Software s.r.o.
hop@unibase.cz

Rozmach (nejenom satelitního) digitálního vysílání videa nemohl minout ani svět otevřených systémů. Příspěvek je jemným úvodem do problematiky standardu DVB. Nechybí ani popis současných "komputerizovaných" řešení: PCI karta do PC nebo komerční set-top-box poháněný linuxem.

Jan Petrouš
Pracuje jako systémový specialista v UniBASE Software s.r.o. Ve firmě je zodpovědný za implementace síťových technologií (Cisco, Linux firewalling, VPN) a operačních systémů (Linux, Solaris, HP/UX, Unixware). Specializuje se na implemetace obecně nestandardních komunikačních prvků, např. ovladače pro čtečky smart karet apod.

Amatérské řešení lokální sítě s využitím Wi-Fi

Jiří Kašpar
jira.kaspar@volny.cz

Příspěvek popisuje praktické zkušenosti s vytvořením lokální sítě na sídlišti s cílem sdílet trvalé internetové připojení. Řešení není profesionální, cílem je co nejúspornější řešení. Připojení k Internetu je realizováno linkou 128kbps s jedinou IP adresou. Router, firewall a síťová topologie je směsí nejnovějších (v době pořízení) zařízení pro bezdrátové sítě Wi-Fi, 100Mb přepínaného Ethernetu, tenkého Ethernetu (BNC), vyřazených Pentií 100 a 486 s Linuxem i Windows 95 a různým software zdarma. Součástí úsporného kutilství je i amatérská stavba antén.
Příspěvek si neklade za cíl přinést nějaké nové odborné informace, ale spíš popsat amatérskou praxi a dát případným zájemcům o následování nějaké ty užitečné tipy.

Jiří Kašpar
Programátor a realizátor webových aplikací se stal v soukromém životě klientem H-Systému. Přes veškerou nepřízeň osudu a státu se převážná většina klientů zkrachovalé společnosti sdružila v družstvu Svatopluk, které svépomocí rozestavěné stavby dokončilo. V Horoměřicích je přes 60 bytů i kancelář družstva a autor příspěvku zde ve volných chvílích rozvíjí a spravuje počítačovou síť.

Pomalé kouření dýmky a internetové technologie

Tomáš Novotný
Gymnázium Křenová, Brno
tomas@novotny.cz

Jiří Novotný
ÚVT MU, Brno
novotny@ics.muni.cz

V příspěvku popisujeme program pro zpracování soutěží v pomalém kouření dýmky, který byl použit (mimo mnoha domácích soutěží) na Mistrovství světa v pomalém kouření týmů ve Windsoru. Jde o první program tohoto druhu, který je postaven na principu internetových technologií a je koncipován jako server - klient. Systém pracuje na internetovém serveru, klienty jsou počítače s libovolným webovým prohlížečem (Netscape, Opera, Mozilla, Internet Explorer). Vlastní program je napsán v PHP a používá databáze PostgresSQL. Součástí systému je modul v jazyce Java pro elektronické zpracování času, který je funkční i na velmi nekvalitních linkách. V příspěvku bude diskutováno použití Javy v prostředí různých webových klientů.

Tomáš Novotný
studuje druhý ročník čtyřletého studia na gymnáziu Křenová v Brně. Programováním se zabývá od svých 13ti let. Programuje v jazycích Java, PHP a využívá databází MySQL a PostgreSQL v prostředí operačního systému NetBSD.
Je správcem internetových serverů na Gymnáziu Křenová, autorem mnoha webových stránek a programátorem systému pro zpracování výsledků v pomalém kouření dýmek.

Jiří Novotný
pracuje na Masarykově univerzitě od roku 1981, kde začínal jako technik sálových počítačů. Později se věnoval návrhu a vývoji hardware i software pro osobní počítače (8bitové i PC). V roce 1992 položil společně s předčasně zesnulým RNDr. Ivo Černohlávkem základy metropolitní počítačové sítě BAPS (Brněnská Akademická Počítačová Síť) včetně jejího připojení na Internet. V letech 1998-2001 spolupracoval pracoval na vývoji vícefunkční PCI karty pro firmu Terabeam. V současné době se stará o provoz části routerů BAPS, vývojem v oblasti hradlových polí a je zástupcem vedoucího strategického projektu CESNETu „Implementace IPv6 v síti CESNET2“.

Vybrané aspekty antické filosofie a dnešek

Josef Petrželka
Katedra filosofie, Filozofická fakulta MU Brno
josef.petrzelka@phil.muni.cz

Přednáška se stručně dotkne několika témat z antického (především řeckého myšlení), jež mají nějakým způsobem blízko k současnému poznání či myšlení. Nastíní tématickou odlišnost antické a současné filosofie; podněty řecké přírodovědy a kosmologie pro další zkoumání podstaty světa a vesmíru a srovnání antického a novověkého popř. současného uvažování o společnosti.

Josef Petrželka
(*1971)
1998: postgraduální studium, filosofie, Ph.D., Filosofování jako životní styl. Sókratés, Platón. Katedra filosofie FF MU.
1995: magisterské studium, filosofie-historie, Mgr., Pojetí člověka u F. M. Dostojevského. Katedra filosofie FF MU.

1999- : odborný asistent na Katedře filosofie FF MU.
1999-1999: odborný asistent na Katedře občanské výchovy PdF UP Olomouc.

Pedagogická činnost
Dějiny antické a středověké filosofie
Úvod do řecké a latinské filosofické terminologie
Filosofie pro společný základ
Platónova teorie idejí

HW/SW Co-Design of Routers

Otto Fučík
Fakulta informačních technologií VUT v Brně
fucik@fit.vutbr,.cz

Routers presents typical real-time high-performance embedded systems that are implemented as mixed software-hardware systems. Generally, embedded systems utilize both hardware and software parts but are neither used nor perceived as computers. Rather, dedicated hardware is used for performance, while application specific software is used for features and flexibility. Design of embedded systems is subject to many different types of constraints, including timing, throughput, reliability, and cost. Contemporary design methods for embedded systems tends to specify and design hardware and software separately which leads to difficulties in verifying the entire system. Also when HW/SW partition is made in advance, the final system implementation can be sub-optimal with lower performance to price ratio and longer time-to-market. In the proposed Liberouter project: (1) we are exploiting many useful futures of FPGA technology used as a basic hardware component, (2) the router design can be seen as an unified problem where software and hardware functions presents implementation alternatives for the same specification. Thus during each incremental design step, it can be carefully decided how the router's architecture can be partitioned and which parts will be better to implement in hardware or software to obtain better router's performance, lower cost, and shorter design time.

Otto Fučík
Education
- 97-98, Postdoctoral study, University of Wyoming, USA.
- 97, Doctor of Philosophy in Cybernetics, VUT v Brně.
- 90, Ing. (Master of Science in Computer Engineering)

Research Interests
- Re-configurable computer architecture
- Hardware/software co-design methodology and algorithms
- Real-time digital signal processing

Hardware descriptive languages

Vyhledávání v IPv6 směrovači implementovaném v hradlovém poli

David Antoš,
Fakulta informatiky Masarykovy univerzity v Brně
antos@fi.muni.cz

Vojtěh Řehák
Fakulta informatiky Masarykovy univerzity v Brně
rehak@fi.muni.cz
Jan Kořenek
Fakulta informačních technologií VUT v Brně
korenek@liberouter.org

Článek popisuje design vyhledávacího procesoru v Combo6 IPv4/IPv6 směrovací akcelerační kartě. Směrování a filtrování IPv6 vyžaduje prověření více než 440 bitů hlaviček. Jako výhodné se zde jeví použití asociativní paměti CAM. Bohužel největší na trhu dostupné CAM nemají dostatečnou šířku pro pokrytí této úlohy. Navrhujeme proto vyhledávací procesor (LUP) založený na CAM kombinované s dohledáváním ve stromové struktuře.
Popíšeme design hardwarové jednotky realizující vyhledávání údajů z hlaviček paketů a podpůrný software, který vytváří obsah vyhledávacích tabulek („vyhledávacích nanoprogramů“) ze směrovací tabulky a nastavení paketového filtru.
Při vývoji jsme aplikovali metody formální verifikace (model checking). Modelovali jsme navržený algoritmus přístupu ke sdíleným pamětem a korektnost jeho chování jsme prověřili systémem NuSMV pro formální verifikaci.
Vývoj probíhá v rámci otevřeného projektu Liberouter

David Antoš
je postgraduálním studentem Fakulty informatiky MU, zabývá se vyhledáváním ve směrovačích.

Vojtěch Řehák
je postgraduálním studentem Fakulty informatiky MU, zabývá se formální verifikací.

Jan Kořenek
dokončuje inženýrské studium na FIT VUT, je autorem hardwarového návrhu vyhledávacího procesoru.

Vývoj nanoprogramů pro procesory implementované v hradlovém poli

Filip Hőfer
Fakulta informatiky Masarykovy univerzity v Brně
fil@liberouter.org

Jedním z důležitých rysů vývoje v rámci otevřeného projektu Liberouter je koncept nanoprocesorů a nanoprogramů. Jedná se o procesory implementované v hradlových polích, tedy v programovatelném hardwaru. Tyto procesory představují novou platformu, která umožňuje efektivní běh specializovaných nanoprogramů. Zároveň se však jedná o platformu, pro kterou nelze použít běžné vývojové nástroje. Proto bylo vyvinuto křížové programové vybavení, které dovoluje odladit nanoprogramy na PC a zkompilovat je do binárního kódu konkrétního nanoprocesoru. Jelikož jsou průběžně vylepšovány nejen nanoprogramy, ale i nanoprocesory, byl zvolen návrh dostatečně robustní, aby každá změna v hardwaru nevynucovala přepsání nanoprogramů. Prezentovaný nástroj je generickým simulátorem nanoprocesorů.

Filip Hőfer
Filip Hőfer dokončuje bakalářské studium a je externím vyučujícím na Fakultě informatiky Masarykovy univerzity v Brně. V rámci otevřeného projektu Liberouter se zaměřuje zejména na vývoj simulátorů hardwaru. V současné době se věnuje také vývoji hardwaru samotného, konkrétně vývoji vstupní jednotky směrovače.

Netopeer - konfigurační systém pro směrovače a sítě IP

Ladislav Lhotka
CESNET, z.s.p.o. Praha
Lhotka@cesnet.cz

Softwarový systém Netopeer je součástí projektu Liberouter. Původní motivací bylo vytvoření konzistentního rozhraní pro konfiguraci PC směrovačů, systém je však nyní koncipován jako platformně nezávislý systém pro konfiguraci směrovačů i celých sítí IPv4 a IPv6. Data jsou v interním formátu XML uchovávána v centrálním uložišti, které nabízí i správu verzí na bázi CVS. Uživatel (správce sítě) komunikuje se systémem pomocí front-endů, které umožňují

různým způsobem vytvářet a upravovat konfigurace. K dispozici jsou front-endy vlastního řádkového rozhraní, WWW a Cisco IOS. Vyzvednutí zvolené konfigurace a její prezentace v konfiguračním jazyku cílové platformy je úkolem back-endů – k dispozici jsou verze pro Cisco IOS, NetBSD a Linux. Ve vývoji je též modul *metakonfigurace* , který umožní konfigurovat celou síť na vyšší úrovni abstrakce – konkrétní konfigurace jednotlivých směrovačů se pak vygenerují automaticky.

Ladislav Lhotka
(*1959) vystudoval matematické inženýrství na FJFI ČVUT a poté se více než deset let věnovat matematickému a simulačnímu modelování ekologických systémů. Po příchodu Internetu do ČR se zapojil do budování akademických sítí a to se mu postupně stalo hlavním zaměstnáním. V současné době pracuje v útvaru výzkumu a vývoje sdružení CESNET, kde vede strategický projekt IPv6 a podílí se též na spolupráci v mezinárodních projektech GÉANT a 6NET. K jeho odborným zájmům patří kromě síťových technologií operační systém Linux, programování v Pythonu a systémy pro zpracování textu (XML, TeX).

IP telefonie a její praktické využití

Jiří Novák
NET-SYSTEM s.r.o., Liberec
j.novak@netsystem.cz

Posluchač se během přednášky dozví, jak se jeho hlas dostane při použití VoIP technologie z jednoho sluchátka přes datovou síť do sluchátka druhého. Bude popsán v krátkosti algoritmus převodu z hlasu na data, komprese hlasu a to, jak se VoIP zařízení vyrovnávají s různými problémy datových sítí - zpoždění, ztráty apod. Současné hlasové a datové sítě jsou složeny z mnoha komponent. Budou ukázány rozdíly i podobnosti a jejich dopad na VoIP. V další části bude ukázán možný postup při integraci stávající datové a hlasové sítě do jednoho funkčního celku s ohledem na praktické zkušenosti. A na závěru budou diskutovány přínosy i nové problémy VoIP.

Jiří Novák
(*1975) Vystudoval Střední průmyslovou školu v Liberci, obor Automatizace a Výpočetní technika. Potom pokračoval na FEL ČVUT v Praze, obor Systémové programování, kde získal titul Ing.
Pracuje jako systémový inženýr/konzultant v NET-SYSTEMu v Liberci. Zabývá se datovými sítěmi od návrhu po implementaci včetně VoIP, převážně na technologiích Cisco. Je držitelem CCNA. Věnuje se problematice VoIP a vývoji aplikaci pro toto prostředí.

Hlasové služby v síti CESNET2

Miroslav Vozňák
Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky, Katedra elektroniky a telekomunikační techniky
miroslav.voznak@vsb.cz

Techniky přenosu hlasu v sítích IP označované jako VoIP (Voice over IP) se stávají základní platformou komunikace v řadě moderních sítí. Ve druhé polovině roku 1999 začal CESNET vytvářet podmínky pro provozování IP telefonie mezi členy sdružení a vytvořil pracovní skupinu, která se začala zabývat problematikou technologie VoIP. Prvním výstupem projektu bylo propojení ústředen ČVUT v Praze a VŠB-TUO v Ostravě přes síť národního výzkumu a vzdělávání, dnes má možnost volat zdarma v rámci sítě sdružení několik desítek tisíc účastníků, jejichž přístroje jsou součástí ústředen zapojených do projektu. Výrazný potenciál snížení nákladů na hovorné je i v realizovaném výstupu do veřejné sítě s nízkými cenami za spojení, ale přitom s kvalitou srovnatelnou s běžným hovorem přes veřejnou síť. Sdružení CESNET IP telefonii neprovozuje za účelem dosažení zisku, ale poskytuje členům sdružení přístup ke službě, která usnadňuje a zefektivňuje hlasovou komunikaci. Cílem příspěvku je informovat o stávajícím stavu, aktuálně řešených technických úkolech a nově připravovaných službách v projektu IP telefonie.

Miroslav Vozňák
absolvoval katedru elektroniky a telekomunikační techniky na VŠB-TUO v roce 1995, po ukončení studia zůstal na katedře a nastoupil na místo odborného asistenta. V rámci kombinovaného postgraduálního studia absolvoval v roce 2000 doktorskou zkoušku a v roce 2002 obhájil disertační práci na téma „Optimalizace hlasového provozu v sítích s technologií VoIP“. Od roku 1995 je pod hlavičkou firmy Siemens školitelem v oblasti komunikačních systémů Hicom300, HiPath4000 a HiPath5000, odborné kurzy probíhají ve školících střediscích na VŠB-TUO nebo v Praze Klánovicích. Dlouholeté zkušenosti a získané know-how se staly základem i odborné spolupráce mezi katedrou zaměstnavatele a firmou Siemens, spolupráce probíhá v oblasti vývoje aplikací, řešení technických problémů a testování nových produktů. V roce 1999 se stal zakládajícím členem řešitelské skupiny IP telefonie v rámci sdružení CESNET a na tomto úkolu pracuje i dnes jak ve výzkumné, tak i v provozní části projektu.

VoIP a zkušenosti při implementaci v praxi

Vladimír Toncar, Kerio Technologies s.r.o.
vtoncar@kerio.com

Příspěvek podává přehled Voice over IP protokolů H.323 a SIP. Je zmíněna jejich historie a filozofie návrhu. Jsou diskutovány problémy implementace VoIP v praxi, např. kompatibilita různých zařízení a problém časování hlasových paketů na různých výpočetních platformách. Závěr příspěvku je věnován open-source implementacím VoIP protokolů, zejména projektům OpenH323 a Vovida.

Vladimír Toncar
Absolvoval inženýrské a postgraduální studium v oboru Informatika a výpočetní technika na FAV ZČU v Plzni. Nyní pracuje ve společnosti Kerio Technologies ČR, kde se zabývá návrhem a vývojem aplikací Voice over IP a specializuje se zejména na protokol H.323

-

Druhé OpenPGP Keysigning Party

OpenPGP Keysigning Party se bude konat při příležitosti XXIII. konference uživatelů otevřených systému EurOpen.CZ. Účast na Keysigning Party není podmíněna účastí na konferenci. Jednací jazyk pro druhé OpenPGP Keysignig Party je čeština.

Kde?

Hotel Flag, restaurace GALERIE
Předměstí 3
696 62 Strážnice
tel: +420 518 332 059
fax: +420 518 332 099

Kdy?

Pondělí, 29. září 2003
od 17.30 do 18.30 CEST (GMT+2)
Keysigning party začne v 17.30. Bude rozdán seznam účastníků a neprodleně zahájen vlastní proces podepisování klíčů.

Co musím udělat, abych se mohl keysigning party zúčastnit?

1. Všichni účastníci zašlou **nejpozději do úterý, 23. září do 23.59 CEST** své veřejné klíče společně s key ID, typem klíče, fingerprintem a informací o velikosti klíče na adresu koordinátora, kterým je Roman Pavlík <rp@tns.cz> Roman připraví seznam účastníků keysigning party (MD5 a SHA1 hash seznamu účastníků). Na seznamu bude uveden key ID, typ klíče, fingerprint a velikost klíče každého účastníka keysignig party. Tištěnou podoba seznamu obdrží každý účastník neprodleně po zahájení keysignig party. Klíčenka s veřejnými klíči všech účastníků bude k dispozici na adrese http://www.gpg.cz/~rp/keysigning2/pubring.asc nejpozději 24. září v 11.00 CEST.

2. Přijít **včas** na keysigning party.

3. Přinést sebou:

   - Platný občanský průkaz nebo cestovní pas platný v České republice.
   - Papír s následujícími údaji o vlastním klíči: key ID, typ klíče, fingerprint, velikost klíče a uživatelský identifikátor (uid). Je nutné, abyste tyto údaje získali z klíče uloženého na vaší **vlastní klíčence.**
   - Pero nebo tužku na psaní.
   - **Rozhodně ne počítač.**

Proces podepisování klíčů

1. Po začátku keysignig party obdrží každý účastník od koordinátora tištěný seznam, který obsahuje key ID, typ klíče, fingerprint a velikost klíče každého z účastníků. U každého klíče na seznamu je vlevo značka "[ ]". U každého uživatelského identifikátoru (uid) je vlevo značka "( )". Účastníci značky použijí při kontrole správných údajů o klíči (key ID, typ klíče, fingerprint a velikost klíče) a při kontrole identity majitele klíče.

2. Ve směru hodinových ručiček každý účastník vstane a zřetelně nahlas přečte key ID, typ klíče, fingerprint, velikost klíče a uživatelský identifikátor pro svůj klíč. Tyto údaje přečte z papíru, který si na keysigning party sám přinesl a který obsahuje údaje získané z jeho vlastní klíčenky. Toto opatření je nezbytné pro odhalení chyb, které byly úmyslně

či neúmyslně zaneseny do tištěného seznamu účastníků, které na začátku keysigning party rozdal koordinátor. Při čtení může také každý řici, který uživatelský identifikátor (uid) má být podepsán a který nikoliv. Každý z účastníků keysigning party pozorně poslouchá a kontroluje, zda informace, které přednáší majitel klíče, souhlasí s informacemi, které jsou uvedeny v tištěném seznamu, který obdržel. Pokud jsou informace shodné, vepíše do značky "[ ]" vedle klíče fajfku.

3. Po té co své klíče přečetli všichni účastníci keysignig party, připraví si všichni občanský průkaz nebo cestovní pas platný v ČR. Každý z účastníků předá svůj pas sousedovi po pravé ruce. Nyní každý z účastníků překontroluje identitu toho, jehož občanský průkaz nebo pas právě drží v ruce. Pokud jste si jistí, že zkoumaná osoba je skutečně ta, za kterou se vydává a že klíč, který je uveden na seznamu je skutečně její, vepište do značky "( )" vedle příslušného uid fajfku. Po té předejte občanský průkaz nebo pas sousedovi po pravé ruce. Tento krok se opakuje tak dlouho, dokud každý neobdrží zpět svůj občanský průkaz nebo pas.

4. Skončil-li předešlý bod, je formální část keysignig party u konce. Výsledný tištěný seznam s vašimi poznámkami dobře uschovejte, je to nejcennější výsledek, který si z keysignig party odnášíte. Nyní můžete odejít nebo zůstat a diskutovat otázky kolem PGP, ochraně elektronické komunikace nebo cokoliv jiného.

5. Překontrolujte, zda informace o klíči, který se chystáte podepsat, odpovídají informacím, které jsou uvedeny na tištěném seznamu. Pokud ano, můžete přistoupit k vlastnímu podpisu uid. Podepsat byste měl/měla pouze taková uid, kde je fajfka ve značce "( )" i ve značce "[ ]" u příslušného klíče.

6. Všechny klíče, které jste podepsal, **pošlete zpět na adresu koordinátora.** Roman aktualizuje pubring.asc, který obsahuje veřejné klíče všech účastníků keysignig party. Výsledek bude ke stažení na adrese http://www.gpg.cz/~rp/keysigning2/pubring.asc

Proč si nemám brát počítač?

Existuje řada důvodů, proč to nedělat. Krátká odpověď je, že to může být nebezpečné a kontraproduktivní. Pro ty, kteří nesouhlasí, uvádíme několik argumentů:

- Někdo by mohl modifikovat programy, operační systém nebo hardware, aby tak získal nebo modifikoval klíče.

- Pokud si lidé vyměňují diskety se svými klíči, může se snadno roznést virová nákaza.

- Pokud si účastníci přinesou sebou své privátní klíče s cílem podepisovat přímo na keysigning party, otevírá se řada možností, jak získat jejich passphrase (útoky key-loggin , shoulder-surfing atd).

- Je mnohem lepší vyměnit si pouze informace o klíčích a ověřit identitu účastníků a vlastní podepisování nechat na doma, kde máte k dispozici důvěryhodný počítač.

- Někdo Vám může počítač polít pivem.

- Někdo může Váš počítač shodit se stolu.

- Další důvody, které nejsou publikovatelné.

Kde získat více informací o podepisování klíčů?

Můžete si přečít Keysigning Party Howto (http://www.gpg.cz/~rp/keysigning2/). Tento dokument vysvětluje pojem pavučina důvěry, kterou pomocí podepisování klíčů budujeme.

Více informací o GnuPG. (http://www.gpg.cz/)

Pro lepší orientaci

Konference se koná v hotelu Flag, který, ač je jeho adresa Předměstí 3, se nachází přímo v centru Strážnice. Ubytování je ve dvoulůžkovýh pokojích s veškerým zajištěním služeb v rámci hotelu.

Úterní posezení se koná v Petrově, který je zhruba 3 kilometry od Strážnice (viz mapka na následující straně). Je možné i dojít pěšky po polní cestě podél železniční tratě.

Příjezd od Prahy je nejjednodušší po brněnská dálnici, ze které se odbočí na sjezdu směr Hodonín. Jak stručně shrnul pan provozní v hotelu Flag: „Z Prahy je nejlepší jet po dálnici, první obec na cestě je Petrov a druhá Strážnice“.

Pro lepší orientaci uvádíme opět polohu obou objektů, jak ji zaměřil Dolf při návštěvě Strážnice

souřadnice hotelu Flag	souřadnice vinných sklepů Petrov
N 48° 53.979	N 48° 52.642
E 17° 18.867	E 17° 16.275
nadmořská výška 179m	nadmořská výška 163m

Hotel Flag

Strážnice

Město Strážnice bylo založeno v polovině 13. století jako stráž na pomezí – pevnost na ochranu zemských hranic. Díky této exponované poloze prožívalo město slavnou i pohnutou minulost, v níž se střídaly doby klidného rozvoje a válečných katastrof. Největší rozkvět prožívala Strážnice v 16. století, kdy patřila k nejlidnatějším moravským městům.

Strážnický zámek – původní gotický vodní hrad byl založen ve stejné době jako město. Prošel mnoha stavebními úpravami, jeho současná podoba je výsledkem klasicistní přestavby v polovině 19. století.

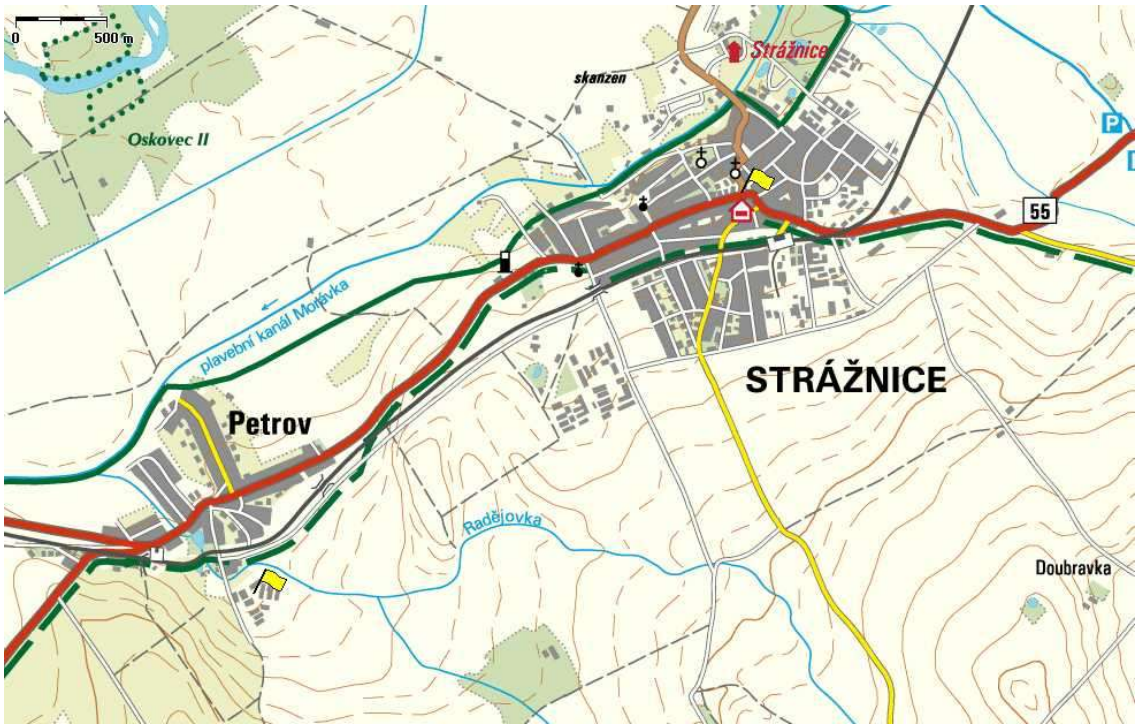
Ze starší doby se zachovaly zbytky městského opevnění, Veselská a Skalická brána, které tvořily součást fortifikace vybudované v 16.století před tureckým nebezpečím. V baroku vznikla dnešní podoba původně gotického kostela sv. Martina s věží a kaple sv. Rocha. Během 18.století byl také postaven rozsáhlý areál piaristických budov s chrámem Nanebevzetí Panny Marie a klášterem. K významným stavebním památkám patří také synagoga se židovským hřbitovem a skanzen obsahující ukázky lidové architektury z celého Slovácka.

V bohatých kulturních tradicích města zaujímá přední místo školství. V roce 1577 byla otevřena vyšší bratrská škola, kterou v letech 1604 – 1605 navštěvoval J.A.Komenský. Piaristé se zasloužili o vznik gymnázia, založeného v roce 1634, které ve městě působilo 250 let. Mezi významnými profesory najdeme i jméno J.E.Purkyně, v roce 1864 – 1865 zde studoval také T.G.Masaryk.

Petrov

Historické vinné sklepy v petrovských Plžích. V roce 1983 byly tyto vinné sklepy z 18. a 19. století vyhlášeny Ministerstvem kultury za památkovou rezervaci. Tento komplex 80 vinných sklepů je ojedinělý v celé ČR.

Převzato z brožury Strážnice



Strážnice a blízké okolí

Předběžné oznámení o konání konference a žádost o příspěvky

XXIV. konference Českého sdružení uživatelů otevřených systémů
EurOpen.CZ (www.europen.cz) se bude
konat v květnu 2004
Místo i přesný termín bude upřesněno v průběhu měsíce září a oznámeno na konferenci ve Strážnici

Základní tematické okruhy příspěvků budou zaměřeny, ale nikoliv omezeny, na následující okruhy:

- portály a portálová řešení, obecné principy, oblasti nasazení, zkušenosti s volbou nástrojů, praktické zkušenosti s provozováním
- nástroje pro podporu vývoje softwarových projektů se zaměřením na podporu analýzy a implementace (modelování a vývojové prostředí)
- XML databáze
- vyhledávací stroje
- zkušenosti s vývojem a nasazováním aplikací na bázi J2EE technologií a aplikačních serverů

Příspěvky mohou být zaměřeny jak na popis architektury nástrojů či technologií, tak na jejich použití při vývoji reálných aplikací. Akceptovány budou pouze příspěvky technicky zaměřené, pokud se nejedná o příspěvky orientované na sociální či právní problémy dotýkající se informačních technologií.

Autorům přijatých příspěvků náleží autorský honorář obvyklý na konferencích EurOpen.CZ.

Stručnou anotaci příspěvku a stručný profesní životopis autora v rozsahu 10 - 15 řádků na standardním formuláři, který je k dispozici na www.europen.cz, je třeba zaslat nejpozději do 15.4.2004 buď e-mailem na adresu europen@europen.cz

nebo poštou na adresu.

Česká společnost uživatelů otevřených systémů
EurOpen.CZ
Univerzitní 8
306 14 Plzeň

Na webové stránce www.europen.cz je možno najít i anotace a profily autorů z minulých konferencí. Vyrozumění o zařazení příspěvku na program konference bude autorovi zasláno obratem, nejpozději do 22.4.2004

Příspěvky ve tvaru publikovatelném ve sborníku je třeba zaslat do 10.5.2004. Příspěvky neprocházejí redakční ani jazykovou úpravou. Sborník je zařazen do nomenklatury ISBN. Formát a rozsah příspěvku záleží na autorovi, může jít jak o text v běžném formátu (Word, PostScript a další), tak o kopii prezentace ve formátu ppt.

Program konference a pozvánky budou k dispozici do 30.4.2004 v papírové i elektronické podobě. Dotazy či případné žádosti o podrobnější informace je možné zasílat e-mailem na adresu europen@europen.cz.

Kdy	Tutorial se uskuteční v neděli 28.9. od 13 do 17 hodin
	Konference začíná v pondělí 29.5. v 9 hodin a končí ve středu 1.10. cca ve 13 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Hotel Flag Strážnice Předměstí 3 696 62 Strážnice email agflag@flag.cz www.flag.cz +420 518 332 099
Kam zaslat přihlášku	Vyplněnou přihlášku společně s oznámením o platbě zašlete na adresu: Anna Šlosarová EurOpen.CZ Univerzitní 8 306 14 Plzeň e-mail:europen@europen.cz tel.: 377 632 701
Co zahrnuje účastnický poplatek	vložné, sborník, stravné, raut, občerstvení během přestávek a ubytování
Úhrada poplatku	č.ú. 478928473 u ČSOB Praha 1, kód banky 0300 variabilní symbol 0250503 (nutno uvést), společnost EurOpen.CZ Univerzitní 8 Plzeň IČO: 61389081, DIČ: 010-61389081 Společnost EurOpen.CZ není plátcem DPH.
Neúčast	Při neúčasti se účastnický poplatek nevrací, ale sborník bude zaslán. Při částečné účasti se platí plný účastnický poplatek.
Doklad o zaplacení	Zašleme v rámci vyúčtování po skončení semináře.
Uzávěrka přihlášek	26.9.2003 nebo při naplnění ubytovací kapacity.
On-line přihlášky	Anotaci příspěvků i formulář přihlášky je možné najít na adrese: http://www.europen.cz V programu konference mùže dojít k drobným časovým i obsahovým změnám.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 100 účastníků
Další informace	Pořizování audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno.

Pozor, nová adresa pro zasílání přihlášek na konferenci je
Anna Šlosarová
EurOpen.CZ
Univerzitní 8
306 14 Plzeň

Konferenční poplatky

Vložné		
platba	tutorial	konference
členové		
do 20.9.	690	1 900
po 20.9.	790	2 150
ostatní		
do 20.9.	790	2 200
po 17.5.	890	2 450

Tutorial je možné objednat i samostatně, účast na konferenci není podmínkou pro účast na tutorialu.

Ubytování 350 Kč/den ve dvoulůžkovém pokoji.
Plná penze 310 Kč/den, snídaně 90,- Kč, oběd 100,- Kč, večeře 120 Kč
Ubytovací kapacita je zhruba 100 osob.

Ubytování a stravné	
od neděle 28.9.	1 980
od pondělí 29.9.	1 420

člen ano	platba do 20.9..ano	tutorial	konference Kč	ubytování od neděle	 Kč	celkem Kč

Zakřížkujte pole člen, pokud jste členy EurOpenu.CZ.
Zakřížkujte pole do 20.9., pokud je platba provedena do 20.9.
Zakřížkujte pole od 28.9., pokud si přejete ubytování od neděle.

V opačných případech (nečlen, platba po 20.9. a ubytování a strava od pondělí ponechte příslušná pole nezaškrtnutá.

Vypište do pole tutorial, konference a ubytování částky, odpovídající členství a datu uskutečnění platby a ve sloupci celkem sečtěte.

Příklad člena platícího po 20.9., chce tutorial a ubytování od neděle.

člen ano	platba do 20.9. ano	tutorial Kč	konference Kč	ubytování od neděle	 Kč	celkem Kč
X		790	2 150	X	1 980	4 920

Přihláška na XXIII. konferenci EurOpen.CZ			
Příjmení, jméno, titul			
Název firmy, adresa včetně PSČ			
Adresa, na kterou má být zaslána faktura, včetně IČO a DIČ			
telefon			
e-mail			
Souhlasím s uvedením jména na seznamu účastníků. Není-li vyplněno, předpokládáme, že s uvedením jména souhlasíte.		**A/N**	
Podpis			

Potvrzení o zaplacení	
Potvrzujeme, že účastnický poplatek byl zaplacen dne	
Tuto částku jsme převedli z našeho účtu č.	
u banky	
ve prospěch účtu sdružení EurOpen.CZ u ČSOB Praha, číslo účtu 478928473, kód banky 0300, variabilní symbol 0290903	
Razítko a podpis účtárny	

Konferenční poplatky
(vzor vyplnění viz předchozí strana)

člen ano	**platba do 20.9. .ano**	**tutorial**	**konference Kč**	**ubytování**		**celkem Kč**
		Kč		**od neděle**	**Kč**	