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

XXI.konference
Hotel Dukla
Znojmo
29.9. – 2.10.2002

Programový výbor
Felbáb Jiří, ICZ Praha
Pavlík Roman, Trusted Network Solutions, Bílovice nad Svitavou
Rudolf Vladimír, Západočeská univerzita Plzeň

Organizační výbor
Felbáb Jiří
Lacková Edita
Opletalová Romana
Stehlíková Eva

Vážené kolegyně, vážení kolegové,

činnost sdružení se lépe hodnotí z dlouhodobější časové perspektivy, v návaznosti jednotlivých akcí a výhledu do budoucna. Proto dříve, než se budu zabývat konferencí připravovanou, se chci vrátit ke konferenci předchozí.

Jak z hodnocení konference, bleskurychle sestaveného z dotazníků kolegy ze ZČU, tak z odezvy, se kterou se každý setká, dopadla poslední konference mimořádně dobře. Po každé konferenci si říkám, „Tak tohle se nám už asi nepodaří". Říkal jsem si to v Třeboni, v Bílovicích a po jetřichovické akci opět, možná proto, že poslední dojmy jsou nejsilnější. Přitom recept na úspěšnou konferenci se zdá být poměrně prostý – zajímavá témata, kompetentní přednášející, atraktivní prostředí, při troše štěstí i počasí, a erudovaní a reagující posluchači. Poslední bod je podstatný - kolikrát jste se sami octli v situaci, kdy jste stáli před auditoriem a v duchu jste si říkali „Vědí něco nebo nevědí, je to co říkám příliš plytké nebo naopak vůbec nejsou v obraze, proč nedají nějak najevo, co si myslí?"

Každá úspěšná konference je tak svým způsobem výzvou, na kterou se díky kolektivnímu úsilí daří odpovídat. K organizaci podzimní konference měl každý možnost se vyjádřit jednak na večerním setkání v Jetřichovicích, jednak v dotazníkách a samozřejmě i individuálně. Byl jsem trochu skeptický k termínu, protože organizaci bylo třeba zajistit prakticky bezprostředně po skončení jetřichovické konference a dokončit během července. Díky kolektivnímu úsilí byl program prakticky během června připraven.

Podzimní konference má tři stránky – odbornou, organizační a společenskou. Proberu je postupně.

Velmi pozitivně byly v Jetřichovicích hodnoceny tutorialy a jsou ve Znojmě zařazeny znovu. Témata vzešla z „všelidového hlasování" – XML a IPv6. Jak témata, tak přednášející, kteří již na konferencích hovořili, jistě garantují přitažlivost obou nedělních událostí.

Témata konference lze rozdělit do čtyř skupin. Podpora vývoje bezpečného a kvalitního software, technologické novinky, bezpečnost a realizované projekty či „work-in-progress". Hodnocení kvality software, o kterém zasvěceně hovořil profesor Vaníček v Malé Úpě, je samo o sobě nelehké. Podpora vývoje takového software je jistě úkol ještě obtížnější. Příspěvky, které se na konferenci sešly, nabídnou pohled na tuto problematiku z různých stran.

Mezi technologické novinky je jistě možné zařadit Solaris 9, stejně tak ale spadají do této oblasti i příspěvky další, Jirky Novotného a kolegů z akademického prostředí. Těší mě, že se na konferenci tyto příspěvky sešly, protože informují o vlastních cestách, postupech, implementacích a získaných zkušenostech. Podíl podobných příspěvků na skladbě programu je z více důvodů stále nízký – stačí porovnat třeba s podílem obdobných příspěvků na konferencích Usenixu.

Příspěvky zaměřené na problematiku bezpečnosti nejen mapují možné implementační technologie – OpenSSL, MS CryptoAPI a Jav Cryptography Architecture, které velmi úzce navazují na konferenci předchozí, ale zabývají se i problematikou čipových karet, o které na konferencích zatím řeč nebyla.

Stránka organizační se týká přijetí nových stanov valnou hromadnou. Od jasnějšího definování organizačních struktur si osobně slibuji snížení zbytečného dohadování a neproduktivní ztráty času a odstranění překážek v další činnosti sdružení. Protože se řada věcí odvíjí od usnesení valné hromady, které musí být přijato nadpoloviční většinou členů, přičemž valná hromada dále volí radu, je klíčovým prvkem otázka, kdo je vůbec členem EurOpenu. Dosavadní stanovy určují že ten, kdo byl přijat valnou hromadou za člena a plní členské povinnosti, které lze z tohoto pohledu redukovat na úhradu symbolického ročního příspěvku 1000 Kč. Součástí pozvánky je proto u členů žádost o úhradu příspěvku na rok 2002. Při přípravě valné hromady budeme pro potřeby stanovení členství proto vycházet z úhrady tohoto příspěvku. Velmi transparentní a flexibilní přístup má v tomto směru opět Usenix.

Pokud jde o stránku společenskou, vycházeli jsme při přípravě konfernce z několika axiomů, respektujících požadavky účastníků – třeba volba atraktivní lokality při současné nepřípustnosti opakování akce na místě, kde se již konference konala. Přestože se naše akce obvykle nekonají ve

městě, myslím že Znojmo nikoho nezklame. Historický střed města s vyhlídkovou radniční věží, středověkým podzemím, románská rotunda svaté Kateřiny, údolí blízké Dyje či přímo proti hotelu ležící Loucký klášter s vinnými sklepy Znovínu a návštěvnickým centrem jsou vděčné cíle. Pro mobilní účastníky se jenom na moravské straně nabízí v okruhu třiceti kilometrů řada skvostů – od zámků či hradů v Jaroměřicích, Jevišovicích, Vranově, Cornštejnu či Bítově po Národní park Podyjí.

Návštěva sklepa, která měla v Bílovicích velký úspěch, se bude opakovat. Na pondělí je připravena ochutnávka vína s rautem ve vinném sklepě v Novém Šaldorfu, 20 minut pěšky od hotelu. Podle předběžné návštěvy, je myslím, na co se těšit.

Poslední velmi zajímavou událostí, na kterou bych vás rád pozval, je připravovaný seminář „Internet Security: Then and Now" s přednáškami Petera H. Saluse, na kterém účast předběžně přislíbili i další přednášející, například Petr Koubský nebo Honza Muller. Anotace přednášek dr. Saluse najdete v této pozvánce, podrobnější program pak bude vydán k vlastnímu semináři. Pokud by vás napadl zajímavý příspěvek s uvedenou tématikou, je možné kontaktovat kohokoli z programového výboru semináře – Dolfa, Romana Pavlíka, Honzu Mullera nebo mě. Akce potvrzuje, že je správné, aby EurOpen.CZ se v rámci svých možností snažil udržovat co nejširší kontakty jak s národními skupinami v Evropě, tak s Usenixem. Dík patří kolegům ze ZČU, jejichž rozhovor s Peterem Salusem na NLUUG akci inicioval.

Na závěr snad místo obvykle ne příliš čitelné mapky popis cesty k hotelu. Projedete Znojmem hlavní silnici směrem na Vídeň. Prakticky na konci města, v panelové zástavbě vlevo od silnice, na konci mírného táhlého klesání cca 2 km od centra, nelze na pravé straně přehlédnout Loucký klášter a na levé hotel Dukla. Že jste hotel minuli zjistíte snadno a jednoznačně v okamžiku, kdy jste dorazili k Dyji. Nevadí, stačí se obrátit a vrátit cca 500m.

Těším se na setkání na konferenci a přeji vám příjemný pobyt ve Znojmě.

Jiří Felbáb
předseda rady sdružení

Neděle 29.IX.		
11:00	XML	Ipv6
	Jiří Kosek	Ladislav Lhotka, Pavel Satrapa
19:00 – 21:00	večeře	

Pondělí 30.IX.		
9:00	Zahájení	Jiří Felbáb, EurOpen.CZ
9:05	Úvodní slovo	
10:00	Automatizovaná formální verifikace	Luboš Brim Fakulta informatiky MU Brno
11:05	Přestávka na kávu	
11:25	Projekt IPv6 routeru na bázi PC s hardwarovým akcelerátorem	Jiří Novotný UVT MU Brno
12:30	Oběd	
13:30	Testování bezpečnosti výpočetních systémů	Petr Břehovský
14:35	Vývoj bezpečného software	Tomáš Weinfurt
15:40	Přestávka na kávu	
16:00	SUN OpenNetworkEnvironment & OperatingEnvironment	Vladimír Müller, Jiří Dostálek, SUN Microsytems
17:05	Overview of the CORBA Performance	Adam Buble, Petr Tůma, KSI MFF UK
18:10	Dotazy, diskuse a závěr prvního dne	
18:30	Večeře	
19:15	Návštěva vinného sklepa v Novém Šaldorfu spojená s degustací	

Úterý 1.X.		
8:30	Jednotný identifikační systém na Západočeské univerzitě v Plzni	Alexandr Vituško
9:35	Bezdrátová síť v polouzavřeném prostředí	Jan Kasprzak Fakulta informatiky MU v Brně
10:40	Přestávka na kávu	
11:00	FAI (Fully Automated Instalation) na ZČU	Petr Holeček CIV ZČU Plzeň
12:05	Diskuse a závěr dopolední sekce	
12:15	Oběd	
13:00	Práce v sekcích	
18:30	Valná hromada	
19:00	Večeře	
20:00	Kontrolni mechanismy v moderni demokracii	Václav Peřich Fakulta humanitních studií UK

Středa 2.X.		
8:30	PKCS#15	Luděk Rašek, Alena Kabelová, PVT a.s
9:35	OpenSSL	Martin Szotkowski, Libor Dostálek, PVT a.s.
10:40	Přestávka na kávu	
11:00	Microsoft CryptoAPI 2.0	Petr Borsodi, ICZ.a.s.
12:05	Java Cryptography Architecture	Jiří Felbáb, ICZ a.s.
13:10	Diskuse a závěr	
13:30	Oběd	

XML
Jiří Kosek

Tutoriál posluchače seznámí s jazykem XML, který přináší mnoho revolučních změn do oblasti elektronického publikování, výměny a sdílení dat a elektronického obchodu. Kromě základních principù XML se posluchači seznámí i s dalšími navazujícími technologiemi: se stylovými jazyky (CSS, XSLT, XSL FO), s jazyky pro definici schématu dokumentu (DTD, XML schémata, Relax NG), s dotazovacími jazyky (XPath, XQuery) a s jazyky pro tvorbu odkazù (XLink, XPointer). Pozornost bude věnována i oblastem, kde použití XML přináší výhody oproti konkurenčním technologiím.

Jazyk XML (eXtensible Markup Language) je poměrně nový značkovací jazyk. Mezi jeho největší výhody patří naprostá otevřenost a velká flexibilita. Díky tomu se během krátké doby stalo XML velice populární. XML vzniklo zjednodušením jazyka SGML (Standard Generalized Markup Language), který je ISO normou 8879 z roku 1986. Kvůli své složitosti bylo SGML nasazováno jen ve větších aplikacích. XML je oproti tomu jednoduchý jazyk, který vytvořilo konsorcium W3C.

Jiří Kosek
Vystudoval informatiku na VŠE Praha. Profesně se zajímá zejména o elektronické publikování a vývoj webových aplikací. Je autorem několika knih, které se zabývají internetovými technologiemi. Kniha HTML -- tvorba dokonalých WWW stránek získala ocenění Grada '98. U nakladatelství Grada vydal rovněž knihy PHP -- tvorba interaktivních internetových aplikací a XML pro každého. Na VŠE vede kurzy věnované tvorbě webových aplikací a XML, na toto téma lektoruje i komerční školení. Je členem mezinárodního týmu, který vyvíjí XSL styly pro zpracovní dokumentù v XML formátu DocBook. Pravidelně publikuje články zaměřené zejména na XML v předních českých odborných časopisech.

IP verze 6
Ladislav Lhotka, Pavel Satrapa

Nová verze protokolu IP (IPv6) se prosazuje zřejmě poněkud pomaleji, než se původně předpokládalo, jeho postupné rozšíření je však nepochybně jen otázkou času. Základním motivem IPv6 je jistě rozšíření adresy na 128 bitů, důležitá jsou však i další vylepšení stávajícího IPv4 v oblastech autokonfigurace koncových stanic, bezpečnosti, mobility aj. Příspěvek seznamuje se základními stavebními kameny IPv6 formou tutorialu s praktickými ukázkami konfigurace směrovačů a stanic. Jsou pokryty následující tematické okruhy:

- Adresace IPv6, struktura hlavičky datagramu
- Autokonfigurace a zjišťování sousedů
- Vazba na protokoly linkové vrstvy, zejm. Ethernet
- DNS
- Směrovací protokoly
- IPSec
- Mobilita
- Programování aplikací
- Technologie přechodu od IPv4 k IPv6

Ladislav Lhotka
CESNET

Ladislav Lhotka
(1959) vystudoval matematické inženýrství na FJFI ČVUT a poté se více než deset let věnoval matematickému a simulačnímu modelování ekologických systémů. Po příchodu Internetu do Československa se zapojil do budování akademických sítí a to se mu postupně stalo hlavním zaměstnáním. V současné době je výzkumným pracovníkem CESNETu a vede zde projekt IPv6, který je zařazen i do mezinárodního projektu 6NET. K jeho odborným zájmům patří kromě síťových technologií operační systém Linux, programování v Pythonu a systémy pro zpracování textu (XML, TeX).

Pavel Satrapa
(1964) vystudoval MFF UK, specializaci samočinné počítače a programování. Od roku 1989 působí na Technické univerzitě v Liberci, v současnosti jako vedoucí katedry informačních technologií. Zabývá se především počítačovými sítěmi, zejména pak Internetem. Podílel a podílí se na rozvoji akademické sítě ČR. Je autorem několika odborných publikací.

Automatizovaná formální verifikace
Luboš Brim

V posledních letech stále více narůstá význam formální verifikace komplexních hardwarových a softwarových systémů jako alternativního přístupu ke zvýšení správnosti, spolehlivosti a kvality. Formální verifikace částečně odstraňuje omezení tradičních metod jakými jsou simulace a testování.

V příspěvku se zaměříme na přehled současného stavu, charakterizujeme postavení formálních metod verifikace v procesu vývoje komplexních systémů. Podrobněji pak pojednáme o tzv. ověřování správnosti modelu (Model Checking), který je v současné době již standardně používán v průmyslové praxi.

Doc. RNDr. Luboš Brim, CSc.
Fakulta informatiky, Masarykova Univerzita Brno
Je docentem na Fakultě informatiku MU v Brně. Problematikou verifikace se systematicky zabývá již od roku 1976 a publikoval na 60 vědeckých a odborných prací z této oblasti, převážně na významných zahraničních konferencích. V současné době je i vedoucím Laboratoře paralelních a distribuovaných systémů při FI, ve které je problematika automatizované verifikace jedním ze stěžejních výzkumných témat. Je rovněž řešitelem několika výzkumných projektů z této oblasti. Mezi jeho výzkumné zájmy patří i softwarové inženýrství, teoretické základy informatiky a návrh distribuovaných algoritmů.

Projekt IPv6 routeru na bázi PC s hardwarovým akcelerátorem
Jiří Novotný

Cílem projektu je ověřit možnost hardwarové implementace routeru IPv6 založených na PC architektuře pomocí hardwarového akcelerátoru na bázi hradlových polí. Projekt vychází z dlouholetých zkušeností získaných při implementaci softwarového routeru na platformě operačního systému NetBSD. Ze získaných zkušeností a měření vyplýva, že limit rychlosti softwarového routeru je v oblasti stovek Mb/s. Na základě analýzy jsme navrhli architekturu PC routeru tak, že vlastní přepínání paketů (data plane) bude probíhat v hardwarovém akcelerátoru, zatímco řídící funkce (control plane) budou realizovány v hostitelském počítači architektury PC. Výhodou uvedeného řešení je zvýšení výkonu routeru do oblasti jednotek až desítek Gb/s. Projekt je zařazen do strategického projektu CESNETu „Implementace IPv6 v síti CESNET 2" jako dílčí úkol „Vývoj hardware pro podporu směrování IPv6".

Ing. Jiří Novotný
Ústav vypočetní techniky, Masarykova Univerzita Brno
Ing. Jiří Novotný pracuje na Masarykově univezitě v Brně od roku 1981, kde začínal jako technik sálových počítačů. Později se věnoval návrhu a vývoji hardware i software pro osobní počítače (8smibitové i PC). V roce 1992 položil společně s predčasně 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 veducím subprojektu „Vývoj hardware pro podporu směrování IPv6" v rámci strategického projektu CESNETu.

Testování bezpečnosti výpočetních systémů
Petr Břehovský

Přednáška se bude zbývat následujícími tématy: Sbírání informací o testovaném subjektu, testy černé skříňky, analýza architektury systému, auditing zdrojového kódu a reverzní inženýrství (disassembler a debuging, analýza síťového provozu). Dále budou též zmíněny následující body: Útoky brutální silou, práce s lidmi, kontrola fyzického zabezpečení a attack trees. Bude proveden zevrubný přehled volně šiřitelných a komerčních testovacích nástrojů.

Petr Břehovský
Pracuje jako správce výpočetních systémů a zabývá se testováním jejich bezpečnosti. Široké veřejnosti je znám spoluprací na překladech knih Hacking Exposed a Incident Response. Věnuje se lektorské činosti v oblasti protokolů TCP/IP a bezpečnosti výpočetních systémů.

Vývoj bezpečného software
Tomáš Weinfurt

V současné době se objevuje stále roste počet bezpečnostních incidentů. A to nejen počet publikovaných chyb, ale zejména počet zasažených systémů a způsobených škod. Je to nezbytné zlo nebo je to něco, co lze aktivně ovlivnit? Proč je vývoj bezpečného software tak složitý a kolik nás stojí (ne)bezpečnost?
Odpověď na tyto otázky se pokusí najít tato prezentace. Řeč bude zejména o příčinách chybného software a tom co je možné udělat pro to zlepšení současné situace.

Tomáš Weinfurt
promoval v roce 1995 na ZČU v oboru informatiky a od té doby se věnuje počítačovým sítím a bezpečnosti výpočetních systémů. Nejprve ve společnosti Conet a později v jejích reirkarnacích Internet CZ a EUnet. Jako součást provozního a později projekčního oddělení byl odpovědný za návrhy, implementaci a údržbu rozsáhlých datových sítí včetně aktivního zabezpečení. Později, ve společnosti ICZ, se podílel na rozvoji PKI v Čechách a na vývoji crypto aplikací. V současné době pracuje pro společnost Terabeam, kde je odpovědný za vývoj embedded systémů pro řízení síťových prvků.

SUN OpenNetworkEnvironment a OperatingEnvironment (ONE & OE)
Vladimír Müller, Jiří Dostálek

SUN ONE a co to je, z čeho se skládá. Solaris9 – operační prostředí. Nové vlastnosti v operačním systému, integrované produkty ze SUN ONE do operačního systému – adresářový server, web server, firewall a další. Samostatné produkty SUN ONE dodávané jako součást operačního prostředí. Přibalené testovací verze produktů SUN ONE.

Ing.Vladimír Müller
Sun Microsystems
41 let, absolvent VŠE – ASŘ. UNIXu se věnuje od roku 1988, nejprve v Kancelářských strojích – instalace, školení, systémové práce a technická podpora pro UNIXové systémy, později v soukromých firmách X/Konzult, BITS s tímtéž zaměřením. Od roku 1994 vedoucí systémového oddělení a útvaru informačních technologií v PRE, nyní skoro dva roky jako konzultant v Professional services SUN Microsystems.

Mgr. Jiří Dostálek
Sun Microsystems
27 let, absolvent MFF UK. Od roku 1997 pracuje ve firmě SUN Microsystems, nejprve jako systémový inženýr a v současné době jako konzultant v Professional services.

Overview of the CORBA Performance

Adam Buble, Petr Tůma

CORBA has been established as one of the most common middleware today. Its language transparency and strong industrial background makes it promising middleware for the future. However, choosing the right implementation is not easy. The implementations vary in features and performance and user should carefully choose the one to use. We present a benchmarking suite, which is simple and yields results that are easy to understand. The results can be combined to assess the performance of more complicated application. Finally, we present an overview of performance of today's C++ CORBA brokers.

Adam Buble
je postgraduální student na Katedře softwarového inženýrství MFF UK, kde se zabývá výkonností middleware. Spolu s Petrem Tůmou (inženýrské studium na ČVUT, doktorské studium na MFF UK, dnes odborný asistent na KSI MFF UK) se zúčastnil několika výzkumných projektů na toto téma. Od roku 1998 se oba intezivně zabývají benchmarkováním a vyhodnocováním výkonnosti middleware.

Jednotný identifikační systém na Západočeské univerzitě v Plzni

Alexandr Vituško

Příspěvek popisuje problematiku vývoje, výstavby a provozu Jednotného identifikačního systému (JIS) v prostředí Západočeské univerzity. Sjednocení různých druhů identifikačních médií do vhodně vybraného typu a správa uživatelů, jsou významnými prvky nejen pro zajištění dobré úrovně obsluhy a servisu, ale i pro udržení otevřenosti systému z hlediska jeho dalšího rozvoje. Příspěvek stručně popisuje architekturu systému, otázku administrace a organizačních návazností, které zajišťují jeho operativní správu a provoz.

Startovní podmínkou výstavby takového systému je nejen jeho schopnost implementovat se do již stávajících systémů, ale zejména volba moderního a bezpečného identifikačního média s ohledem na agresivní prostředí technicky zdatných uživatelů. Systém JIS je založen na bezkontaktních identifikačních kartách s kryptočipem, které umožňují bezpečné ověřování jejich pravosti snímačem. Tyto karty zároveň v souladu se zákonem plní funkci průkazu studenta.

Služby, které systém poskytuje nebo zprostředkuje, jsou dnes používány tisíci uživateli. Počet služeb se soustavně zvyšuje, a proto je od systému vyžadována rychlá odezva, spolehlivá a bezpečná identifikace a autentizace uživatelů. Důležitou schopností je proto také rychlý vývoj a výroba požadovaných HW a SW modulů.

Bc. Alexandr Vituško

ekoTIP Plzeň

Autor se narodil v Chebu dne 21. ledna roku 1950. V roce 1969 absolvoval Střední průmyslovou školu elektrotechnickou v Plzni, obor konstrukce elektrických strojů a přístrojů. Bakalářské studium oboru marketing a management ukončil na katedře ekonomiky Západočeské univerzity v Plzni v roce 1995.

Do zaměstnání nastoupil v roce 1971 jako operátor pro řízení energetického bloku v Severočeském kraji. Od roku 1975 na Plzeňsku jako investiční pracovník a dále jako technik sálového počítače. Od roku 1981 do roku 1991 jako radiodůstojník čsl. námořní plavby. Od roku 1991 jako podnikatel v oblasti zdravotnické a výpočetní techniky. Od roku 1997 pracuje dosud pro Západočeskou univerzitu na projektu Jednotného identifikačního systému.

Bezdrátová síť v polouzavřeném prostředí
Jan Kasprzak

Bezdrátové technologie podle IEEE 802.11b se stávají levnou alternativou lokálních sítí na bázi strukturované kabeláže. Jak ale nakonfigurovat takovouto síť, aby byla aspoň trochu zabezpečena před odposlechem dat a před zneužitím ze strany neoprávněných osob? Přednáška se bude zabývat architekturou takovéto sítě v budově Fakulty informatiky Masarykovy univerzity.

Jan Kasprzak, , Masarykova Univerzita Brno
(*1974) vystudoval Fakultu informatiky MU v Brně, kde nyní i působí. Zabývá se správou UNIXových systémů a počítačových sítí, tvorbou firewallů a aplikačních clusterů založených na operačním systému Linux. Je předsedou Českého sdružení uživatelů OS Linux.

FAI (Fully Automatic Installation) na ZČU
Petr Holeček

FAI je neinteraktivní systém pro instalaci Debian GNU/Linuxu na cluster PC. FAI používá pro instalační proces Debian GNU/Linux a kolekci shell a perl scriptů. Změny v konfiguračních souborech instalovaného systému mohou být prováděny pomocí cfengine, shell, perl a expect scriptů. Systém FAI byl primárně vyvinut pro instalaci uzlů výpočetních clusterů, ale lze jej použít všude tam, kde je třeba udržovat v větší množství instalací Debian GNU/Linuxu.
Příspěvek se zabývá praktickými zkušennostni s použitím systému FAI pro instalaci stanic ve veřejných učebnách ZČU. Autorem FAI je Thomas Lange.

Ing. Petr Holeček
CIV Západočeská univerzita Plzeň
Petr Holeček absolvoval Vysokou školu strojní a elektrotechnickou v Plzni, fakultu strojní. Poté pracoval jako systémový programátor v ČKD-Polovodiče a ve výpočetním středisku VŠSE Plzeň, později jako člen systémové a technické podpory v CCA a.s. V současnosti pracuje jako správce databáze Oracle na CIV ZČU. Kromě správy databázového systému Oracle a OS UNIX se příležitostně zabývá tvorbou databázových aplikací a v poslední době zejména nasazením OS Debian GNU/Linux.

Kontrolni mechanismy v moderni demokracii
PhDr. Václav Peřich
Fakulta humanitních studií UK

1962 - vyučen zahradníkem
do 1975 - různá zaměstnání převážně v dělnických profesích
1975 - Agroprojekt Praha (VTEI, průmyslově právní ochrana)
1981 - PhDr FF UK (Pragmatická adresnost informace)
1987 - Ústav stavebních informací
1990 - 1993 PedF UK (katedra výchovy k občanství); v roce 1992 poslanec FS ČSFR
1993 - 2002 Nejvyšší kontrolní úřad
nyní Fakulta humanitních studií UK

PKCS#15
Luděk Rašek, Alena Kabelová

Po krátkém přehledu norem PKCS se přejde k normě PKCS#15. Jedná se o normu standardizující souborový systém a specifikaci souborů na čipových kartách určených pro PKI. Bude diskutováno i využití těchto karet jak v prostředí PKCS#11, tak i v prostředí PC/SC. Dále bude probrána návaznost PKCS#15 na normy řady ISO7816 a možnosti praktického využití těchto standardů v praxi. Součástí přednášky bude i demonstrace čipové karty pro PKI.

Ing. Luděk Rašek (*1973)
vystudoval ČVUT FEL. Zabývá se problematikou využití čipových karet v PKI, technologiemi na bázi Javy a XML v prosředí Internetu a bezpečnostními aspekty těchto technologií. Nyní je zaměstnán jako konzultant v PVT.

Ing. Alena Kabelová
(*1964); vystudovala VŠE. Pracovala jako hostmaster i jako vývojář. Je spoluautorem publikace "Velký průvodce protokoly TCP/IP a systémem DNS". Zabývá se problematikou využívání

čipových karet pro PKI. V současné době vede vývojový tým řešící využití PKI karet v aplikacích elektronického bankovnictví.

.

OpenSSL
Martin Szotkowski, Libor Dostálek

Úvod bude věnován protokolům SSL a TLS. Poté se přejde k praktickému využití protokolů SSL/TLS - systému OpenSSL. Bude zmíněna filosofie práce s OpenSSL volaného z aplikací. Dále bude popsáno volání OpenSSL z příkazového řádku. Jako praktická demonstrace bude ukázka jednoduché certifikační autority postavené na volání příkazového řádku OpenSSL.

Ing. Martin Szotkowski
PVT a.s.
(*1972), vystudoval VUT v Brně. Pracoval jako vývojář, nyní vede v PVT vývojový tým projektu I. Certifikační autorita.

RNDr. Libor Dostálek
PVT a.s.
(*1957); vystudoval MFF UK. Zabýval se zejména IT architekturou v oblasti e-commerce, e-banking i m-banking. Je zaměstnán v PVT jako vedouc konzultačního oddělní. Je autorem dvou populárně naučných publikací: "Velký průvodce protokoly TCP/IP a systémem DNS" a "Velký průvodce protokoly TCP/IP - Bezpečnost".

Microsoft CryptoAPI 2.0
Petr Borsodi

Jedním z kryptografických rozhraní, která jsou v moderních informačních systémech používána, je rozhraní CryptoAPI. Toto rozhraní je implementováno v operačních systémech Windows firmy Microsoft a je používáno aplikacemi jako je Internet Explorer, Outlook, Outlook Express, Internet Information Services a dalšími.
Služby, nabízené rozhraním CryptoAPI, tvoří nedílnou součást PKI infrastruktury tak, jak je zejména implementována v produktech Microsoft Windows 2000 a Windows XP. Cílem příspěvku je úvodní seznámení s tímto rozhraním – koncepce, začlenění do systému, kryptografické objekty a nabízené služby, certifikáty a jejich úložiště atd.

Ing. Petr Borsodi
ICZ a.s.
Autor je pracuje jako samostatný vývojový pracovník ve firmě ICZ a.s. (dříve DECROS, s.r.o.) a zabývá se vývojem systémového software, kryptografických aplikací a implementací bezpečnostních předmětů (Smart Card, USB tokens, apod.) na platformě Windows.

Java Cryptography Architecture
Jiří Felbáb

Příspěvek se zabývá architekturou, kterou disponuje platforma Java 2, edice 1.4 pro podporu šifrování. Nejprve podá velmi stručný výčet rysů podporujících bezpečnost v Javě 2 – od verifikace bytecodu přes class loadery, security managery a policy files, k stručné charakteristice vývoje bezpečnostních modelů pro běh apletů a aplikací. Těžiště příspěvku spočívá v popisu základních rysů návrhu JCA: nezávislosti na algoritmech a poskytovatelích šifrovacích služeb. Stručně budou popsány základní stavební kameny JCA (provider, engine class a factory method) a dále core classes pro práci s šifrovacím a datovým materiálem (algoritmy, klíče, certifikáty, úložiště a další). Na JCA a s ní související JCE (Java Cryptography Extension) navazuje dále řada dalších API, například JSSE (Java Secure Socket Extension) či JAAS (Java Authentication and Authorization Service), o kterých bude stručná zmínka, ale nejsou předmětem příspěvku.

Ing. Jiří Felbáb
ICZ a.s.
Pracuje jako vývojář v ICZ a.s. Během více než dvacetileté praxe se podílel na řadě rozsáhlých projektů jak u současného, tak předchozího zaměstnavatele (ČSAD ZVT Praha), například na řízení skladového hospodářství, účetnictví či provozního řízení autobusové dopravy. Jeden y posledních projektů souvisel právě s bezpečností v Javě. Překládal z angličtiny (mimo jiné Bachovy Principy operačního systému Unix či Stonebrakerovy Objektově-relační databáze), publikoval ve sborníku Jednoty tlumočníků a překladatelů. Podílí se na práci sdružení, v současné době jako předseda rady.

Internet Security: Then and Now

Další akcí sdružení EurOpen.CZ je jednodenní seminář 'Internet Security: Then and Now', který se uskuteční ve čtvrtek 21.11. od 9:00 v Malém sále Městské knihovny na Mariánském náměstí v Praze. Kromě Petera H. Saluse, anotace jehož přednášek jsou přiloženy, přislíbili předběžně účast i další přednášející, mimo jiné Petr Koubský a Jan Muller. K semináři bude vydána samostatná pozvánka s programem akce.

Internet Security: Then and now

Peter H. Salus
<peter@matrix.net>
Matrix NetSystems, Inc.

Nearly 30 years ago, Bob Metcalfe wrote the first RFC on network security. Since then, we have lived through a variety of events, but have not yet solved the basic problems. If you are safely dug in behind your firewall and everyone in your company employs password security and cryptography, are you secure? No.

Your data may be safe from corruption or theft; your Intellectual Property may be inviolate; but businesses require transactions. Without orders, deliveries and other communications, your enterprise will starve. In other words, you're as safe as the inhabitants of a mediaeval city under siege. DDoS attacks and SYN floods render you just as helpless as those besieged without food or water. Businesses require constant traffic.

Using graphs and numbers from past attacks, This presentation will discuss both the nature of such attacks and suggest ways in which their effects can be reduced.

The Types of Internet Trauma: 1994-2002

Peter H. Salus
<peter@matrix.net>
Matrix NetSystems, Inc.

Packet switching networks are hard to destroy. This is implicit in their very design. A network of packet switching networks—the Internet—is even less fragile. However, a number of events have disrupted Internet service over the decades. Some disruptions have been large, some small.

The Northridge Earthquake

On 17 January 1994 at 4:31 AM PST (12:31 MT), a magnitude 6.7 earthquake struck the suburb of Northridge, 20 miles (30 km.) northwest of Los Angeles. In 15 seconds it led to the deaths of 15 people and injuries to more than 9,000. This was certainly a major disaster. What effect did it have on the Internet.

We ran scans at 2 AM and 4 AM PST, thus taking before and after snapshots. At that time, we noted: Comparing the two series of scans, effects of the earthquake can be seen as far north as Lawrence Livermore Laboratories southeast of San Francisco (which shows higher latencies immediately after the earthquake) and as far south as San Diego (which shows more traffic several hours later). Ensenada in Baja California, Mexico, disappears just after the quake, but that is probably coincidence, as the host we are pinging in Ensenada sometimes doesn't respond.

Figure 1 shows the reachability of 4872 destinations for the month of January 1994. The earthquake's effect is clearly visible. It is also quite shortlived: many computers crashed, but most were soon back up.

The quake did tens of billions of dollars in property damage and took most of the San Fernando Valley off the internet for more than a day. But nearly all affected areas were up and running within a week. The Internet as a whole (which consisted of about 750,000 hosts at that time) was not affected beyond the immediate vicinity.

The main reason that the local Internet took a hit was simple: computers don't run without power. The only long term damage was a router bank that fell over (that's why they should be anchored). When power was restored, all the other computers came back up.

Hurricane Floyd

Hurricane Floyd threatened the Caribbean islands and the eastern coast of the US for the first two weeks of September 1999. It achieved Category 4 status before it made landfall. It missed Hispaniola and Cuba completely, passed over the Bahamas, missed Florida, and Georgia, grazed South Carolina, and went ashore in North Carolina. By then it had tapered off to tropical storm classification, still generating high winds and much rain, but instigating far less damage than anticipated.

The expected overall effects on the Internet should be negligible. And in fact that's what we see in the MIDS Internet Average, (Figure 2) The graphs represent average Internet performance. The darker line represents the Internet as a whole. The lighter one represents the WWW, a subset of the Internet.

The MIDS Internet Average is a high-level summary of performance data measured from hosts all around the world. It provides one baseline against which more specialized Internet performance data might be compared, serving a similar role as the Dow Jones Industrial Average does in the financial world. However, negligible isn't the same as indetectible. We do in fact show a surge in both latency and packet loss on Monday 13 September 1999, starting around 8AM EDT and continuing the entire working day.

The Internet pinglist shows a pointed latency spike about noon EDT. The peak of that spike is at 186.4 milliseconds, which is about 16% higher than the usual 160 ms for a Monday afternoon. The www pinglist shows a smaller increase, to about 169 ms over the usual 158 ms of a Monday afternoon, or about 7%. There's a smaller spike on both pinglists about 5PM Monday. Latency is round trip time, or lag there and back again. It is a direct measure of Internet slowness.
For the MIDS Internet Average we measure latency from several beacons (data collection computers) and use a composite median across the data from all of them. Every 15 minutes we make measurement scans of destinations representing many different Internet services, including routers, DNS servers, and servers specializing in mail, WWW, ftp, news, games, and search engines. These scans are made from some of our beacons, each located on a different network and distributed around the world. Both pinglists show a small packet loss increase on Monday.

In fact, they both show spikes at noon and 5PM Monday. These spikes are small, but they coincide exactly with the latency spikes, so they probably indicate a real event in the Internet. Packet loss is a percentage of probe packets we send out that do not elicit responses. It is an indirect measure of Internet slowness, because when TCP (Transmission Control Protocol) encounters packet loss, it slows down its sending speed. In other words, TCP interprets packet loss as a sign of Internet congestion, and sends packets slower to avoid contributing to that congestion.

For the MIDS Internet Average we measure packet loss from several beacons and use a composite median across the data from all of them. Each scan provides us with information on 3 performance metrics most important to the user's experience: latency, packet loss, and reachability. All of the resulting data for each metric and (internet or www in this case) is collapsed into a single line. Packet loss on the internet pinglist is markedly higher than on the www pinglist for Tuesday morning, and then becomes normal.

What we don't see is much effect on Wednesday or Thursday, when Floyd actually made landfall. If anything, there may be a decrease in latency on Wednesday. Looking more closely at the underlying Matrix IQ data, and looking only at nodes in Florida as an example, here at MIDS we can see that there was a drop in reachability at noon EDT Monday, and another at 5PM EDT.

Reachability rachets back up by the same amounts at 7 and 9AM Wednesday. That looks like a couple of folks turning off their machines as they were being evacuated, and turning them back on as they returned. What might have been expected would be brief spikes in ISP performance either when Floyd passed over an area or later when batteries were drained. Most ISPs these days have pretty good backup power, so this would seem the most likely scenario.

For big ISPs, the battery would only be on for about five minutes, and then emergency generators would take over. Then it's just availability of fuel for the generators. Smaller ISPs might have bigger problems, since they have fewer resources for USPses and generators. Or, if damage was sufficiently severe and direct to actually take routers off the net, we might see an outage of a day or more, with a sharp beginning and a gradual end as ISPs dug out and replaced broken equipment. This would be like the effects of the Northridge Earthquake, except probably more severe because the earthquake effect was caused more by power outages than by direct damage.

What we see instead is a lot of small latency and packet loss events on Monday, before Floyd hit anything, and negligible effects afterwards. The only big ISP that seems to have significant later effects is Global-one. Looking very specifically at ISPs by region, we finally notice one router going offline on PSINet in the southeast region around noon EDT Thursday. That's not much of an effect, and it's not even clear it's related.

This hurricane's bark was worse than its bite, where the Internet was concerned. Evacuation and fear of the hurricane caused much more effect on the Internet on Monday than the hurricane itself. However, there was finally a brief but noticeable event on Friday.

ISPs are quite hardened against problems with electricity and telephone service, and even flooding. Certain kinds of problems still affect the Internet, however, such as hysteria, seen here; cable cuts, which are likely the cause of the Friday event; and configuration problems inside the ISPs themselves, which were not observed in this particular week.

Fiber Cut of 29 September 1999

About noon EDT on 29 September 1999 there was a massive fiber cut in Ohio, which took more than four hours to fix. This infrastructure outage was noticeable for the entire Internet, as illustrated by our Internet Average. (Figure 3)

Not much damage is visible in latency, although interestingly enough most of what is visible is in the curve for Top Level Domain (TLD) Domain Name System (DNS) servers. Packet loss clearly shows the event in all three curves. But Reachability shows the most dramatic effects. We also examined the top 30 ISPs one by one, and found that only a few of them (AboveNet, GTE Internet, and PSINet) were noticeably affected. AboveNet got it worst, and took a day to completely recover. All the other ISPs were essentially unaffected.

Outage of 7 October 1999

About 8AM GMT (3AM EDT) on 7 October 1999 there was a massive Internet outage, bigger than the one caused by the fibercut of 29 September 1999. This infrastructure outage was noticeable for the entire Internet.

Denial of Service Attacks

On Monday and Tuesday, February 7 and 8, a large number of major sites across the US were assaulted by „Denial of Service" (DoS) attacks (e.g., eBay, Charles Schwab, Amazon.com, and Microsoft.com). These attacks are the result of millions of messages flooding a particular host or gateway, overwhelming the resources and backing up traffic in a domino fashion.

Soon afterward, Attorney General Janet Reno said that the FBI would track and punish the miscreants. The President called another meeting. All the „usual suspects" were rounded up. There were security warnings, as well. In general, the newspapers and the TV reporters appear to be clueless on the differences between cracking a site and blocking a site.

Since smurf attacks originate from a variety of sources at unpredictable times, an Internet-wide system analysis is necessary [said John Quarterman] There is only one such analyst, MIDS. Just look at the „Internet Average" for 8 February. It's completely clear that the entire Internet had higher packet loss and far lower reachability for several hours. It's like a shark took a bite out of the net. (Figure 4)

Other ‚Minor' Events

There have been other interesting events: the Victoria's Secret lingerie show slowed down AOL, but had no real effect on the Internet; the release of the Starr Report caused several spikes in latency; on 25 September 2000, the ISP Applied Theory showed wild fluctuation in reachability. This was caused by a „router flap" at Sprint. Rather than the absolute drop shown in case of the DoS attacks, or the massive outages shown by fiber cuts, the up-down seesaw here reflects the router trying to come up and succumbing again. When it was swapped out, everything returned to normal.

Under-Sea Cables

Over the past 18 months, there have been three incidents in which a cable in the China Sea has been severed by a trawler. Rather than elaborate on each of these, I'll just talk about one: the cable from Shanghai to Yokohama.

This is the first segment of the transpacific cable connecting China to the United States. From midnight on 9 February 2001 till 20 Fenruary, millions of users in China and others in Southeast Asia suffered a severe delay or a total disruption of service. The cause was transparent: a trawler captain was trawling too deeply in a clearly marked zone. China Telecom officials reported that the cut had occurred near Yokohama and that repairs were already underway. Duncan Clark of BDA, a Beijing-based Internet consultancy stated that the cable was cut near Shanghai. NANOG also reported the cut as near Shanghai. Wherever the cut occurred, a new cable was laid and in service 11 days later. Contrast this with the three hours for the Ohio cable cut: under-sea cables are harder to repair than surface cables.

9/11

This brings me to 11 September 2001. As you all know, just before 9AM EDT an airplane plowed into World Trade Center 2. Twenty minutes later, a second plane struck WTC 1. As a major commercial center, this was a malicious act that was immediately noticeable on the Internet. Damage to the surrounding area made the effect even more dramatic. Three transatlantic fiber cables came ashore in WTC 7, which was leveled by debris. Verizon had a major switching station on West Street. There were colocation hotels on Broadway and on Broad Street.

The Internet was made up of about three-quarters of a million hosts at the time of the Northridge earthquake; reachability dropped by over 25% for nearly 24 hours. Last September, there were about 160 million hosts on the net. At the time of greatest disruption, reachability dropped about 9%. And it returned to within 2% of „normal" within 90 minutes. (Figures 5 and 6).

It was a major disaster, but packet switching really demonstrated that even with a massive rent in its fabric, re-routing could compensate in real time.

The transatlantic rerouting pattern was the most dramatic: with three cables to lower Manhattan truncated, the latency to Boston doubled and that to Washington nearly tripled within 20 minutes. Over the next four hours, this waned to merely 10-15% above normal. It was clear that as London, Amsterdam and Frankfurt became backed-up, the routers found other paths.

Peter H. Salus

is Chief Knowledge Officer at Matrix NetSystems in Austin, TX.

Dr. Salus has extensive experience in large organizations, having been Executive Director of the USENIX Association and the Sun User Group and Vice President of the Free Software Foundation, following 20 years' experience in academia and a stint at IBM's T.J. Watson Research Center. He has also been Director of The Tcl/Tk Consortium.

He is a frequent speaker at European and North American computer events, including the Atlanta Linux Showcase, USENIX, CompCon, Comdex, UniForum Canada, the UKUUG, the NLUUG, the Open Technology Association (Brussels), OpenForum (Moscow), NORDU, SANE, and several other European conferences, as well as the Open Software Forum in Brazil.

He has appeared on the BBC, the Discovery Channel, PBS, PCTV, Voice of America and the Dr. Dobbs webcast as computing and networking historian.
Dr. Salus has written or edited over a dozen books, including A Quarter Century of UNIX, Casting the Net, the four-volume Handbook of Programming Languages, and the Big Book of IPv6 Addressing RFCs.

Kdy	Tutorialy se uskuteční v neděli 29.9. od 11 do 18 hodin
	Konference začíná v pondělí 30.9. v 9 hodin a končí ve středu 2.10. cca ve 14 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Hotel Dukla Holandská 5 669 02 Znojmo tel./fax: 0624/227332 http://www.hotel.cz/dukla
Kam zaslat přihlášku	Vyplněnou přihlášku společně s oznámením o platbě zašlete na adresu: EurOpen.CZ V Olšinách 75/2300, 100 00 Praha 10 tel: (02) 8100 2300, fax: (02) 8100 2301 e-mail:europen@europen.cz
Co zahrnuje účastnický poplatek	vložné, sborník, stravné, degustaci a raut v pondělí 30.9.,občerstvení během přestávek a ubytování
Úhrada poplatku	č.ú. 478928473 u ČSOB Praha 1, kód banky 0300 variabilní symbol 0290902 (nutno uvést), společnost EurOpen.CZ, V Olšinách 75/2300, 100 00 Praha 10 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	27.9.2002 nebo při naplnění kapacity hotelu.
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. Tutorialy se uskuteční při účasti minimálně 8 účastníků.
Další informace	Pořizování audio či video záznamů není bez svolení přednášejících a organizátorů povoleno.

Konferenční poplatky

Vložné			
platba	tutorial		konference
	XML	IPv6	
členové			
do 21.9.	590	790	1 800
po 21.9.	690	890	2 050
ostatní			
do 21.9.	690	890	2 100
po 21.9.	790	990	2 350

Ubytování a stravné	
od neděle 29.9.	1 650
od pondělí 30.9.	1 200

Cena za tutorial zahrnuje oběd v neděli 29.9.
Cena tutorialu IPv6 zahrnuje knihu Pavla Satrapy IPv6
Tutorial je možné objednat i samostatně, účast na konferenci není podmínkou pro účast na tutorialu.

Ubytování 280 Kč/den ve dvoulůžkovém pokoji
Plná penze 270 Kč/den, oběd a večeře 100 Kč, snídaně 70 Kč
Kapacita hotelu je zhruba 100 osob.

člen ano	platba do 21.9..ano	tutorial jaký	 Kč	konference Kč	ubytování od neděle	 Kč	celkem Kč

Zakřížkujte pole člen, pokud jste členy EurOpenu.CZ.
Zakřížkujte pole do 21.9., pokud je platba provedena do 21.9.
Zakřížkujte pole od 29.9., pokud si přejete ubytování od neděle.
Pokud si přejete tutorial, uveďte do pole tutorial jaký – označením 'XML' nebo 'IP').

V opačných případech (nečlen, platba po 21.9. 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 21.9., chce tutorial IPv6 a ubytování od neděle.

člen ano	platba do 21.9. ano	tutorial jaký	 Kč	konference Kč	ubytování od neděle	 Kč	celkem Kč
X		IP	890	2 050	X	1 650	4 590

Přihláška na XXI. 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 0290902	
Razítko a podpis účtárny	

Konferenční poplatky
(vzor vyplnění viz předchozí strana)

člen ano	**platba do 21.9.ano**	**tutorial**		**konference Kč**	**ubytování**		**celkem Kč**
		jaký	**Kč**		**od neděle**	**Kč**	