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

XXII.konference
Ústav fyzikální biologie JČU a klášter servitů
Nové Hrady
25.5. – 28.5.2003

Dear colleague,

The topics of our 22.nd conference fall into three basic categories: time in the world of computers, software management and security. Monday's presentations will be devoted to the first of these themes. I feel that we have assembled the choisiest speakers.

The basic tools used in software development is a recurring theme; I dare say that these four papers will definitely be impressive.

The theme of security seems stir the whole IT community with natural reflection on the agenda of EurOpen.CZ conferences. With respect to this theme, three submitted papers will no doubt neatly fill the empty spaces of the security puzzle.

As most of you know however, our conference is not only centered around sessions and papers. We offer time for meeting new acquaintances and seeing old friends as well and, also, a few social events. It looks quite promising this time: I hope you'll enjoy the organ concert in the Church of St. Peter and Paul on Monday and the roast pork dinner served on the courtyard of the old castle in Nove Hrady, enhanced by a night tour of the castle.

In continuation of a tradition tha we are proud of, again this year we will welcome several speakers from abroad.

In continuation of a tradition that we are proud of, again this year we will welcome several speakers from abroad. After last year's seminars with Werner Koch and Peter. H. Salus we introduce, this time as part of the conference agenda, our colleagues from Estonia and Slovakia.

I would like to thank the program committee for such a highly attractive agenda, the speakers for accepting our invitation, and our partners in Nove Hrady for their help and cooperation.

Last but not least, I would like to mention something about our venue, the beautiful Nove Hrady. Located directly on the Czech-Austrian border in the middle of Vitorazsko – Weitra historical region, Nove Hrady promises a stunning countryside with an array of monuments and historical structures. To the surprise of many, Nove Hrady contains a distinguished academic center, tucked into its lovely hills.

I hope you will find "business as usual" in Nove Hrady: informal events, friendly people and a conference packed with new ideas and experiences.

I'm looking forward to seeing you at Nove Hrady.

Jiri Felbab
EurOpen.CZ Governing Board Chair

Programový výbor – Program Committee

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

Vážené kolegyně, vážení kolegové

letošní jarní konferenci dominují tři témata. Pondělní program je věnován sledování a měření času a jejich použití v praktických aplikacích. Bez důvěryhodného prokázání času provedení události nemá totiž řada operací požadovanou vypovídací schopnost. Jak bude z přednášek zřejmé, má zdánlivě běžná a samozřejmá věc, jakou pro většinu lidí sledování času je, hluboké a propracované kořeny.

Nástrojům pro podporu vývoje softwarových projektů je věnováno úterní dopoledne. O některých byla již řeč na předchozích konferencích, například o správě požadavků a nástroji Request Tracker. CVS je nejpoužívanější systém pro správu verzí, ant začíná dominovat jako nástroj pro řízení kompilací a definování závislostí softwarových modulů a to nejen ve světě Javy a JUnit představuje možný přístup k automatizovanému testování aplikací. Součástí úterní sekce je i příspěvek shrnující zkušenosti z vývoje softwarového projektu.

Středa je věnována bezpečnosti. Každý z příspěvků se zaměřuje na jiný aspekt a společně pak, zejména v kontextu konferencí minulých a především konference jetřichovické a podzimního semináře Internet Security: Then and Now, doplňují mapu této problematiky, které je na našich konferencích věnována systematická péče.

Do tohoto kontextu zapadá i nedělní tutorial, zabývající se typy internetových útoků, který jistě potěší nejen ty, kterým se líbil příspěvek kolegy Břehovského ve Znojmě.

Jsem rád, že po loňských samostatných seminářích s Wernerem Kochem a Peterem Salusem, se i letos podařilo zajistit účast zahraničních kolegů z Estonska a ze Slovenska.

Konferenci doplňují dvě přednášky na zaměřující se na témata, která mají na našich akcích velmi živou odezvu. Úvodní slovo ředitele Ústavu fyzikální biologie bude jistě zajímavé z mnoha aspektů mimo jiné představí Nové Hrady jako významné akademické centrum.

Téma životního prostředí a jeho ochrany by mělo být povinnou součástí každé konference, bez ohledu na její profesní zaměření. Na EurOpenu má dlouholetou tradici a kompetentního přednášejícího. Tématem bude summit v Johannesburgu.

Odborná část je jako vždy doplněna doprovodným programem, který je tentokrát, i díky kulturnímu zázemí Nových Hradů, velmi bohatý. Pondělí je obohaceno o varhanní koncert v klášterním kostele sv. Petra a Pavla, v úterý je pak na programu večerní prohlídka státního hradu v Nových Hradech a raut v Hradní šenkovně a na nádvoří hradu, při kterém nebude chybět sele na rožni.

Pro usnadnění orientace na konferenci je součástí této pozvánky kapitola „Pro snazší orientaci". Samostatnou částí je i stručný popis některých zajímavostí v Nových Hradech a blízkém okolí.

Děkuji programovému výboru za přípravu konference, přednášejícím za vstřícnost, s jakou akceptovali žádost o příspěvek, a všem partnerům v Nových Hradech – Ústavu fyzikální biologie JČU, správě kláštera servitů, správě státního hradu v Nových Hradech i provozovatelům Hradní šenkovny za ochotu, s jakou vyhověli našemu oslovení.

Doufám, že vás odborný i doprovodný program konference zaujme a těším se na shledanou v Nových Hradech.

Jiří Felbáb
předseda rady EurOpen.CZ

Neděle 25.5.	**Tutorial**	
13:00 17:00	Typy útoků v Internetu/intranetu	Petr Břehovský

Pondělí 26.5	**Čas ve světě počítačů a sítí**	
9:00	Zahájení	Jiří Felbáb, EurOpen.CZ
9:05	"Natura sensibus percepta per ideas glorificanda est" aneb biologie očima fyziků a chemiků na Ústavu fyzikální biologie Jihočeské univerzity	Dalibor Štys, ředitel Ústavu fyzikální biologie, Jihočeská univerzita v Českých Budějovicích
10:00	Realizace sekundy SI a světové časové stupnice UTC	Otokar Buzek, Ústav radiotechniky a elektroniky AV ČR, Praha
11:05	Přestávka na kávu	
11:25	Čas ve světě počítačů a sítí	Vladimír Smotlacha, CESNET z.s.p.o.
12:30	Oběd	
13:30	Časová razítka – od norem k praxi	Jaroslav Pinkava, PVT a.s Brno
14:30	Časová razítka a Autorita časových razítek	Marta Vohnoutová, František Drdák, PVT a.s. Plzeň
15:15	Od časových razítek k e-notary	Libor Dostálek, PVT a.s. České Budějovice
16:00	Přestávka na kávu	
16:30	Secure and Practical Time-Stamping	Ahto Buldas, Tallinn Technical University and Cybernetica AS, Tallin
17:15	Estonian ID-card and Digital Signature Act	Arne Ansper, Margus Freudenthal Cybernetica AS, Tallin
18:05	Dotazy, diskuse a závěr prvního dne	
18:30	Varhanní koncert v klášterním kostele sv.Petra a Pavla	
19:30	Večeře	
20:15	Summit o udržitelném rozvoji v Johannesburgu – ekologický nebo ekonomický?	Ivan Rynda Fakulta humanitních studií UK Praha

Úterý 27.5.	**Nástroje pro podporu vývoje softwarových projektů**	
9:00	Concurrent Version System	Tomáš Kraus, Dan Veselka, ICZ a.s.
9:50	ant	Tomáš Kraus, Dan Veselka, ICZ a.s.
10:50	Přestávka na kávu	
11:20	JUnit	Petr Janata, ICZ a.s.
11:50	Software Management	Petr Ferschmann, Kerio Technologies, Plzeň
12:50	Dotazy a závěr dopolední části	
13:00	Oběd	
14:00	Práce v sekcích	
18:30 – 24:00	Večeře a raut v Hradní šenkovně a na nádvoří starého hradu v Nových Hradech	
19:30	Večerní prohlídka státního hradu v Nových Hradech	

Středa 28.5.	**Bezpečnost**	
9:00	Kybernalita – kybernetická kriminalita	Václav Jirovský, Matematicko-fyzikální fakulta Univerzity Karlovy
10:00	Trustworthiness of signed data	Petr Švéda, Fakulta informatiky, MU Brno
11:00	Přestávka na kávu	
11:30	Bezpečnost na urovni jadra	Milan Pikula NAPRI a Slovenske zdruzenie pouzivatelov operacneho systemu Linux SkLUG
12:30	Zakončení konference	
13:00	Oběd	

Typy útoků v Internetu/intranetu

Petr Břehovský
breh@breh.cz

Tutorial bude věnován popisu, demonstraci a praktickému vyzkoušení nástrojů a metod používaných při útoku na server (klient) připojený do TCP/IP sítě. Účastník se seznámí s metodami získávání informací o cílovém počítači (síti), s metodami průniků do operačního systému (zneužití autentizačních mechanizmů, přebírání spojení, zneužití chyb v systémovém software, průnik v případě fyzické dostupnosti počítače atd.) a s metodami lokálního zvyšování privilegií v rámci OS. Budou demonstrovány metody odposlechu nešifrovaných i šifrovaných (ssh1) dat v lokálních sítích a to jak v běžném segmentu ethernetu, tak i v přepínaném prostředí. V neposlední řadě budou analyzovány metody průniků na klientské počítače, včetně dopadů na bezpečnost celé sítě. Posluchač bude také seznámen s některými relativně „novými" typy útoků jako je XSS (cross site scripting) a SQL injection. Během tutoriálu budou používány převážně volně šiřitelné nástroje.

Petr Břehovský
Přednášející v současné době pracuje jako správce UN*X serverů ve společnosti Český Telecom, kde se zároveň podílí na testování úrovně zabezpečení provozovaných aplikací. Mimoto se zabývá lektorskou činností v oblasti protokolů TCP/IP, os UN*X a bezpečnosti výpočetních systémů. Širší veřejnosti je znám spoluprací na překladech knih Hacking bez tajemství a Počítačový útok, detekce, obrana a okamžitá náprava.

"Natura sensibus percepta per ideas glorificanda est" aneb biologie očima fyziků a chemiků na Ústavu fyzikální biologie Jihočeské univerzity

Dalibor Štys
Ústav fyzikální biologie, Jihočeská univerzita v Českých Budějovicích
stys@jcu.cz

Ústav fyzikální biologie Jihočeské univerzity v Nových Hradech vznikl díky projektu výzkumného centra „Mechanismus, ekofyziologie a biotechnologie fotosyntézy". Sešli se v něm pracovníci řady laboratoří v Jihočeském regionu, které se zabývaly měřením biologických objektů fyzikálními metodami obecně a fotosyntézou zvláště. Klade si za cíl získat co nejpřesnější měření na biologických objektech nejrůznější úrovně organizovanosti, od proteinových molekul, přes membrány, organely, buňky až po celé orgány a organismy. Významných výsledků bylo dosaženo při vývoji přístrojů, měření zpětnovazebných dějů v buňce, matematickém popisu a aplikaci poznatků do praxe v biotechnologii a medicíně. Ústav též buduje vlastní výukové programy zaměřené na techniky moderního biologického výzkumu a vývoje.

RNDr. Dalibor Štys CSc.
ředitel Ústav fyzikální biologie, Jihočeská univerzita v Českých Budějovicích
1987 RNDr. ve fyzikální chemii, Univerzita Karlova, Praha, 1992 CSc. v biochemii, Ústav organické chemie a biochemie AVČR, Praha, 1992-1994 postdoktorandský pobyt, katedra biologie rostlinné buňky, Univerzita v Lundu, 1994-1995 výzkumný inženýr, postdoktorandský pobyt, katedra biologie rostlinné buňky, Univerzita v Lundu, 1995-2002 vedoucí laboratoře, Biologická fakulta Jihočeské univerzity v Českých Budějovicích, 2002 ředitel Ústav fyzikální biologie, Jihočeská univerzita v Českých Budějovicích

Realizace sekundy SI a světové časové stupnice UTC

Otokar Buzek
Ústav radiotechniky a elektroniky AV ČR, Praha
buzek@ure.cas.cz

V přednášce bude popsána spolupráce národních laboratoří přesného času a frekvence koordinované Časovou sekcí Mezinárodního úřadu pro váhy a míry (BIPM) v Sévres při

vytváření časového intervalu podle kvantové definice sekundy SI a světové koordinované časové stupnice UTC založené na sekundě SI.
Dále bude popsán systém českého státního skupinového etalonu času a frekvence a jeho parametry.

Ing. Otokar Buzek, CSc
vystudoval Leningradský elektrotechnický institut a v roce 1959 a po pětileté praxi vývojového pracovníka v Tesle Hloubětín přešel v roce 1965 na řádnou aspiranturu do Ústavu radiotechniky a elektroniky ČSAV v Praze.Po ukončení aspirantury pracoval na školicím pracovišti jako vědecký pracovník. V roce 1975 byl jmenován vedoucím vědeckého oddělení přesného času a frekvence, uchovávajícího národní a od roku 1987 státní etalon času a frekvence. Tuto funkci vykonával do roku 1997. Oblastí vědeckého zájmu Ing. Buzka je studium metod generace, distribuce a měření signálů přesného času a frekvence, teorie fázových závěsů, optické sdělováním spektrálně čistých signálů, studium dlouhodobé a krátkodobé stability signálů apod.

Čas ve světě počítačů a sítí

Vladimír Smotlacha
CESNET z.s.p.o.
vs@cesnet.cz

Příspěvek se zabývá problémem času jako fyzikální veličiny a jeho vztahu k počítačům a počítačovým sítím. V první části popisuje síťové protokoly pro přenos času, zejména protokol NTP. Implementace protokolu NTP je komplexní problém týkající se také HW počítače. Proto je stručně vysvětlena HW i SW část realizace systémových hodin na platformě PC při interní reprezentaci času v řádu mikrosekund nebo nanosekund.

S protokolem NTP úzce souvisí časové servery a jejich hierarchie. Pozornost je věnována zejména primárním časovým serverům, které odvozují svůj čas od externího zdroje času, např. atomových hodin nebo přijímače GPS. V další části příspěvku je představen projekt primárního časového serveru navázaného na státní etalon času.

Dr. Ing. Vladimír Smotlacha
absolvoval obor elektronické počítače na FEL ČVUT a teoretická kybernetika na MFF UK. Pracuje jako výzkumný pracovník ve sdružení CESNET z.s.p.o. Kromě časové synchronizace se zabývá zejména problémy vysokorychlostních sítí, jejich monitorování a QoS.

Časová razítka – od norem k praxi

Jaroslav Pinkava
PVT a.s.
jaroslav.pinkava@pvt.cz

Pojem časového razítka, jeho obsah a význam. Souvislost s problematikou elektronického podpisu.
Přehled existujících norem a normativních iniciativ pro oblast časových razítek (IETF, ETSI, ISO).
Protokoly pro přenos žádosti o časové razítko a pro vydávaná časová razítka. Autorita časových značek. Dokumentace. Formáty elektronických podpisů obsahujících časová razítka. Některé aplikace časových razítek.

Ing. Jaroslav Pinkava, CSc.
Jaroslav Pinkava, kandidát matematicko-fyzikálních věd. začínal na katedře statistiky VŠE. Od roku 1978 se profesionálně věnuje kryptografii. V létech 1998-2002 pracoval jako kryptolog brněnské firmy AEC s r.o., od podzimu 2002 pracuje v PVT a.s. Je místopředsedou kryptologické skupiny JČMF, byl členem organizačního výboru významných kryptologických

konferncí Pragocrypt ´96 a Eurocrypt ´99. Podílel se na přípravě zákona o elektronickém podpisu. Publikoval řadu odborných článků.

Časová razítka a Autorita časových razítek

Marta Vohnoutová, PVT a.s.
František Drdák, PVT a.s.
marta.vohnoutova@pvt.cz
frantisek.drdak@pvt.cz

V přednášce bude vysvětlena teorie a význam časových razítek a Autority časových razítek a jejich napojení na důvěryhodné zdroje času. Dále seznámíme posluchače s našimi zkušenostmi s výstavbou Autority časových razítek, předpokládáme také praktickou ukázku.

Ing. Marta Vohnoutová
vystudovala VŠSE v Plzni. Měla na starosti projekty bezpečného připojení k Internetu a budování a monitorování bezdrátových sítí. Nyní pracuje jako konzultant v PVT a.s. Je držitelem MCSE a MCT pro Windows2000.

Ing. František Drdák, CSc
vystudoval na elektrotechnické fakultě ČVUT v Praze. Na témže pracovišti obhájil vědeckou aspiraturu v oboru počítačových sítí. V posledních letech se zabýval vývojem aplikací, které využívají prostředky veřejné kryptografie (Homebanking, Internetbanking). Nyní vede projekt 1. časová autorita.

Od časových razítek k e-notary

Libor Dostálek
PVT a.s.
Libor.Dostalek@pvt.cz

V přednášce bude vysvětleno co vše schází dnešnímu pojetí elektronického podpisu, aby zcela nahradil rukou psaný dopis. Budou zmíněny elektronické podpisy podle normy ETSI TS 101733. Bude zmíněn problém ověřování elektronického podpisu po vypršení certifikátu určeného k verifikaci elektronického podpisu.

Dále se přednáška bude zabývat normami pro ověřování elektronického podpisu a ověřování elektronicky podepsaných dokumentů.

Závěrem budou zmíněny systémy pro dlouhodobou archivaci elektronicky podepsaných dokumentů.

RNDr. 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

Secure and Practical Time-Stamping

Ahto Buldas
Cybernetica AS

ahtbu@cyber.ee

Time stamp provides reliable confirmation (or proof) that data existed at certain time. Time stamp is one of the main security attributes in legal-grade electronic documents. Its main role is to prevent back-dating and unauthorised modification of data. Hence, both the security and technical feasibility of time-stamping solutions are very important issues. We discuss the basic availability and security requirements to time-stamping systems.
We describe a solution that meets those requirements.

Ahto Buldas
(*1967), Professor, chair of Information Security,education: Tallinn Technical University, Computer Engineering

Research and professional experience, institutional affiliation:

1989--1992	Tallinn Technical university, research engineer
1992--1994	Tallinn Technical University, lecturer
1996--1997	Tallinn Technical University, assistant professor
1993--1994	Institute of Cybernetics, junior researcher
1995--1997	Institute of Cybernetics, researcher
1998--	Cybernetica, Chief researcher
2000--	Tartu University, assistant professor
2001--	Tallinn Technical University, professor

Academic degrees:

1993	Master of Sciences (MSc) in Computer Engineering
1999	Doctor of Philosophy (PhD) in Exact Sciences, Thesis: "An algebraic approach to the structure of graphs"

Recognitions:

1993	Arnold Humal price in mathematics
2002	"Young scientist of the year" price (Issued by Estonian President's cultural foundation)

Main research activities:
Applied and theoretical cryptography: digital time-stamping schemes, public-key cryptography, database security, computational graph theory.
Dissertations advised:

2002	Jan Willemson. Size-efficient interval time stamps. PhD Thesis. Tartu University.

Estonian ID-card and Digital Signature Act

Arne Ansper, Cybernetica AS, Tallinn, Estonia
Margus Freudenthal, Cybernetica AS, Tallinn, Estonia
arne@cyber.ee
margus@cyber.ee

We provide an overview of the Estonian Digital Signature Act and describe the requirements placed upon legally valid signatures and the Estonian Digital siganture standardisation. We describe current status of the Estonian ID-card project, the process of issuing ID-cards and the technologies used.

Arne Ansper
(*1970) Cybernetica AS, Development Manager, education: Tallinn Technical Univesity, systems engineering, MSc
Arne Ansper has long experience in designing and building security critical distributed systems and three-year experience in designing and building security critical governmental information systems. His Master studies were related to securing governmental information systems and Master Thesis about e-government from security viewpoint

Margus Freudenthal
(*1976), Cybernetica AS, researcher, education: Tallinn Technical University, computer science, MSc
Margus Freudenthal is experienced software architect and project manager, working also as a research engineer. His master's thesis "Personal Security Environments" analyses security properties needed for secure communication over untrusted data link.

Summit o udržitelném rozvoji v Johannesburgu – ekologický nebo ekonomický?

Ivan Rynda
Fakulta humanitních studií UK Praha
ivan.rynda@czp.cuni.cz

Trvale udržitelný rozvoj se definitivně stal jedinou všeobecně přijatou strategií a nadějí pro budoucnost Země. Johannesburg na jedné straně zpochybnil principy ochrany životního prostředí, na druhé straně nemohl nereagovat na bídu geopolitického Jihu a také na nebezpečí střetu kultur nebo dokonce na terorismus. Znamená něco pro Českou republiku? Znamená něco pro nás, její obyvatele?

PhDr. Ivan Rynda
Studoval filosofii a češtinu na filosofické fakultě UK v Praze (doktorát 1985). Od roku 1975 se živil jako sanitář, montér, myč oken a knihovník, poté jako programátor a systémový analytik. Filosofie, literární věda, zájem o politiku a věci veřejné a o globální problémy lidské civilizace jej dovedly k problematice životního prostředí. Od listopadu 1989 se rovněž živí: nejprve jako pracovník Občanského fóra, pak jako politik od Federálního shromáždění až po místní zastupitelstvo a posléze vysokoškolský učitel. Po sedmiletém úsilí v roli zástupce ředitele Centra pro otázky životního prostředí University Karlovy se mu podařilo spoluzaložit novou Fakultu humanitních studií UK, kde vytvořil obor sociální a kulturní ekologie, jehož katedru vede.

ANT – nástroj pro sestavení aplikace

Tomáš Kraus
ICZ, a. s.
tomas.kraus@i.cz

Úkolem přednášky je seznámit posluchače s jedním z řady nástrojů určených k sestavení aplikace ze zdrojových kódů a nabídnout srovnání s obdobným nástrojem make.
Součástí prezentace bude příklad použití antu pro překlad kódu, sestavení komponenty a deployment J2EE aplikace.

Ing. Tomáš Kraus
vystudoval ČVUT, fakultu elektrotechnickou, obor Výpočetní technika v Praze.
Od roku 1996 působil jako analytik, programátor a správce serverů u firem Eunet Czechia, Internet Servis a ICZ. Dlouhodobě se věnuje zejména návrhu a realizaci webových aplikací na J2EE aplikačních serverech. Od roku 1995 spravuje české servery v komunikační síti IRCnet.

Concurent Version System (CVS)

Daniel Veselka
ICZ, a. s.
daniel.veselka@i.cz

V přednášce vysvětlíme základní principy práce s verzovacími systémy pro správu zdrojového kódu ve větších projektech, kde je nutná spolupráce více programátorů. V druhé části ukážeme příklad vložení existujícího projektu do CVS.

Základní pojmy – CVS repository, verze souboru v CVS,starší systémy - Revision Control System(RCS), Source Code Control System(SCCS)
Základní příkazy CVS – *checkout,commit,diff,export,import,log,tag*
Příklad založení projektu v CVS – vložení existujícího zdrového kódu,uložení změn, logování, zobrazení změn v jednotlivých verzích,příklad konfliktu při uložení

Ing. Daniel Veselka
vystudoval ZČU v Plzni, Fakulta aplikovaných věd, obor Informatika, zakončeno v roce 1992. Dlouhodobě se věnuje vývoji velkých projektů v oblasti Web Services. Nyní pracuje jako vývojář aplikací na J2EE platformě ve firmě ICZ, kde se podílel např. na vývoji projektu Registrované elektronické pošty pro Českou poštu.

JUnit - eXtrémní Testování

Petr Janata
ICZ a.s.
petr.janata@i.cz

Moderní vývojové metodiky jako např. eXtreme Programming kladou velký důraz na testování jak v průběhu vývoje, tak po jeho dokončení. Jedním z nejrozšířenějších nástrojů pro testování v jazyce Java je Junit Testing Framework, poskytovaná bezplatně jako open source software. Junit dovoluje vytvářet soubory základních softwarových jednotkových testů a s řadou rozšiřujících knihoven také soubory testů aplikačních, např. pro webové a J2EE aplikace. Junit je také součástí složitějších testovacích nástrojů jako jsou Apache Cactus nebo Parasoft JTest, navíc je integrována v oblíbeném vývojovém prostředí Borland JBuilder. Na populárních www serverech jako je Java World lze najít řadu tipů a návodů pro implementaci Junit testů, objevují se také nástroje pro menší či větší automatizaci testovacího procesu.

Ing. Petr Janata
je absolventem ČVUT-FEL v Praze. Ve společnosti ICZ působí v oddělení projektů a analýz především jako specialista na komponentní a XML aplikační technologie, zejména J2EE a MS .NET. Podílí se na některých významných projektech pro státní správu (především resorty financí a vnitra) i podnikový sektor (např. Škoda Auto,VZP, Česká pošta)

Software Management

Petr Ferschmann
Kerio Technologies
pferschmann@kerio.com

Každá větší vývojová firma narazí na problém údržby software. Řešením je kombinace systému pro správu verzí, buildovacích systémů, automatických testovacích nástrojů, automatických kompilací.

Cílem přednášky bude přednesení požadavků na tyto systémy a možné problémy. Součástí bude i popsání způsobu jakým se tento problém řeší v Kerio Technologies. Zmíněné budou i některá Open
Source řešení.

Petr Ferschmann
7 let se zabývá Linuxem a programováním pro něj. Má zkušenosti s jazyky C++, Java a PHP. V minulosti se účastnil na takových projektech jako je Effata.net (jabber like instant messanger), kde
působil jako analytik a hlavní programátor. Později působil jako nezávislý programátor zabývající se tvorbou internetových aplikací a webových informačních systémů (postcard.cz, webový autorizační systém core (core.ferschmann.cz), informační systém společnosti Disk). Od roku 2002 je zaměstnancem Kerio Technologies, kde působí jako programátor a release engineer. Je studentem Fakulty Aplikovaných Věd Západočeské Univerzity od roku 1998.

Kybernalita – kybernetická kriminalita.

Václav Jirovský
Matematicko-fyzikální fakulta Univerzity Karlovy
jirovský@dkm.cz

Kybernalita, kriminalita zaměřená na informatické prostředky nebo jich využívající k protiprávním cílům je novým společenským fenoménem. Situace je o to těžší, že technologie se prudce rozvíjejí, a filosofie kybernetického zločinu se vymyká stávajícímu legislativnímu uspořádání. Přesto však protiprávní jednání v této oblasti můžeme poměrně snadno zařadit do stávajících ustanovení trestního zákona, i když mnohdy důkazní prostředky budou tím nejslabším článkem.
Protiprávní chování na síti můžeme v zásadě zařadit do několika základních kategorií

- klasickou kriminalitu
- kriminalitu využívající informatické prostředky nebo metody
- průmyslová a jiná špionáž
- terorismus

Přednáška se zabývá ve své úvodní části základními charakteristikami kybernetického zločinu a jeho zařazením do stávající legislativy. Podrobně se věnuje kyberterorismu a ukazuje odezvy informatických útoků s teroristickým pozadím.

Doc. Ing. Václav Jirovský, CSc
Vystudoval elektrotechnickou fakultu Českého vysokého učení technického v Praze, kde rovněž v roce 1975 obhájil kandidátskou disertační práci. V letech 1975 a 1986 pracoval v Oblastním výpočetním centru vysokých škol, kde vedl úkoly základního plánu výzkumu. V roce 1987 byl pod jeho vedením dokončen pilotní projekt řízení MHD pro hlavní město Prahu a od tentýž rok přešel na Matematicko-fyzikální fakultu Univerzity Karlovy, kde působí dosud. Tuto svoji činnost přerušil v letech 1991 až 1998, kdy pracoval jako ředitel útvaru výzkumu a vývoje firmy Advanced Computer Applications Inc., Newtown, USA. V současné době je docentem na katedře softwarového inženýrství, kde přednáší základy architektury počítačů a věnuje se otázkám počítačové kriminality a protiprávního jednání na sítích. V těchto oblastech rovněž působí jako soudní znalec jmenovaný ministrem spravedlnosti.

Trustworthiness of signed data

Petr Švéda
Fakulta informatiky, MU Brno
xsveda@fi.muni.cz

Use of digital signatures is not as straightforward as one would like to see it. We have to be aware of the fact that computers sign all electronic documents on behalf of humans and only few computers can be considered as fully trustworthy. Visual representation of file formats can

be dramatically changed by settings of a viewer or a text processor. Users cannot be absolutely sure that they sign only the data visible on their computer screen. Proprietary signature solutions are not fully compatible as there are no standards.

This paper reviews the problem of the document content interpretation. Introductory section reviews problems related to the use of digital signatures in practice. The second section briefly summarizes necessary cryptographic assumptions and gives an overview of signature functional properties. The third section discusses questions and possible ways of an interpretation of documents content. The fourth section suggests design principles for trustworthy electronic document structure.

Petr Švéda
Graduated at Faculty of Informatics, Masaryk University Brno, in June 2000. His research is performed as PhD candidate at Masaryk University Brno. His research topics include secure hardware, smart cards, trust and secure issues of data and digital signature.

Since 1996 he publishes articles and papers in national technical magazines and on conferences and workshops. He developed and tested security and protection extensions for operating systems during years 1998-2000.

Bezpečnost na urovni jadra

Milan Pikula
NAPRI a Slovenske zdruzenie pouzivatelov operacneho systemu Linux SkLUG
milan.pikula@napri.sk

Rozne pristupy k aplikacnej bezpecnosti, zvysovanie bezpecnosti na urovni jadra OS, prehlad projektov na zvysenie bezpecnosti unixovych OS, moznosti vyhody a nevyhody jednotlivych rieseni, podrobny pohlad na projekt Medusa DS9, "prakticka" vs. "teoreticka" bezpecnost.

Ing. Milan Pikula
Narodeny r. 1977, vystudoval informatiku na FEI STU v Bratislave. Hlavne zamestnania: 1997-2003 NAPRI ISP - spravca siete, programator, riaditel pobocky, 2002 Terminus - programator, od roku 2003 pracuje vramci vlastnej spolocnosti ako konzultant v oblasti IT. Je zakladajucim clenom Slovenskeho zdruzenia pouzivatelov operacneho systemu Linux - SkLUG, kde je od zalozenia v roku 1999 clenom spravnej rady. Venuje sa pocitacovej bezpecnosti a systemovemu programovaniu. Je autorom viacerych open-source projektov, vratane projektu Medusa DS9 zameraneho na zvysenie bezpecnosti, ktory vznikol v roku 1997.

Pro lepší orientaci

Konference se koná na zámku Ústavu fyzikální biologie JČU a v klášteře servitů sv. Petra a Pavla. Jde o běžné schéma odborných konferencí pořádaných v Nových Hradech. Oba objekty jsou vzdáleny zhruba dvěstě metrů (podrobněji viz dále).

Přednášky budou probíhat v Divadelním sále zámku, stravování je v refektáři kláštera.

Ubytování je zajištěno jak v klášteře, tak na zámku. V obou případech se jedná o vícelůžkové pokoje se společným sociálním zařízením na patře. Prostředí je velmi příjemné, pokoje jsou velmi prostorné. Pokoje budou brány jako dvoulůžkové, pokud bude chtít bydlet více kolegů společně, není to problém.

Recepce bude fungovat na zámku. Zde je třeba se přihlásit a vyzvednout si klíče, bez ohledu na to, zda budete bydlet na zámku nebo v klášteře. Zde je také třeba klíče při odjezdu odevzdat.

V přihlášce je možné si zaškrtnout požadované ubytování. Požadavku se budeme snažit v rámci možností vyhovět.

Pokud přijedete v neděli, večeře bude zajištěna od 19 do 21 hodin, snídaně budou denně od 7:30
a obědy podle programu.

Pro lepší orientaci uvádíme polohu obou objektů, jak ji zaměřil Dolf při návštěvě Nových Hradů:

souřadnice Nové Hrady, klášter

N 48° 47,385
E 14° 46,800

souřadnice Nové Hrady, zámek

N 48° 47,411
E 14° 46,922

Nové Hrady a okolí

Nové Hrady

připomínány již roku 1279 jako osada s hradem střežícím Vitorazskou stezku. Hrad postavili Vítkovci, na počátku 14. století patřil pánům z Landštejna. R. 1359b jej získali Rožmberkové. R. 1425 dobyt a vypálen husity. R. 1611 přechází dědictvím na Švamberky. R. 1619 dobyl Nové Hrady císařský generál Karel Bonaventura Buquoy a 6.2.1620 je pak získal darem od císaře s celým panstvím, které zůstalo v majetku rodu až do roku 1945.

Nový zámek : trojkřídlá jednopatrová empírová budova, vybudován v letech 1801 - 1810.

Klášter servitů: barokní, z let 1679 – 1685, zrušen císařem Josefem II roku 1789.

Starý hrad: ze 2. pol. 13 století, původně gotický, časté přestavby a opravy po požárech, největší r. 1605 a 1792 – 1798.

okolí (do 15 km)

Nové Hrady jsou vstupní branou do **Novohradských hor**. v Rakousku nazývané Freiwald, tvoří horskou skupinu mezi Dolním Dvořištěm a Českými Velenicemi. Nejvyšším vrcholem je Viehberg (1112m) na území Rakouska. Pohořím probíhá hlavní evropské rozvodí mezi Černým a Severním mořem.
Cílem výletů bývá Kuní hora (925m) s výhledy na Alpy, Kraví hora (962m) se starou vojenskou rozhlednou a Vysoká (1034m). K dispozici je množství značených turistických cest i lesních silnic pro cyklisty a cyklistických okruhů (příhraniční 25km, Žumberk 22km, Blata 20km, Nakolice-Hranice 24km, minulostí Novohradska 26km). Pro pěší výlety do Novohradských hor je lepší se autem přiblížit na Dobou Vodu.

Vitorazsko je historické území v oblast horného povodí řeky Lužnice, původně řídce osídlené slovanským obyvatelstvem, od 12. stol. postupně kolonizováno německým obyvatelstvem. Roku 1185 udělil český kníže Bedřich Vitorazsko Hadmarovi II. z německého rodu Kuenringů, který pak vybudoval rodové sídlo Weitra. Po bitvě na Moravském poli byla Vitoraz dobyta a Kuenringům odňata za pomoc Přemyslovi Otakarovi II a připojena k Dolnorakouskému arcivévodství. Roku 1339 byla stanovena přesná hranice mezi panstvím Novohradským a Vitorazským. Po 1. světové válce byla na základě Saint Germainské mírové smlouvy část Vitorazska připojena k Československu.

Cuknštejn tvrz původně pozdně gotická (1488 – 1491), později upravena renesančně.

Červené blato státní přírodní rezervace (331 ha) uprostřed rozsáhlých lesů zvaných odedávna Dolní Hvozd v CHKO Třeboňsko, 8 km od Nových Hradů. Naučná stezka v Jiříkově Údolí.

Dobrá Voda v 16. a 17. století lázeňské městečko na úpatí Kraví Hory, později letovisko a známé mariánské poutní místo. Barokní farní kostel Nanebevzetí Panny Marie z let 1708 – 1715. Od kostela nádherný výhled do podhůří Novohradských hor a Třeboňské pánve.

Hojná Voda na úpatí Kraví hory zhruba 1 km nad Dobrou Vodou. Zmínka o léčivém prameni již z roku 1564, malé lázně zde založil již Vilém z Rožmberka.

Horní Stropnice podhůří Novohradských hor, připomínaná již roku 1185 jako hranice panství Vítkovců a Kuenringů.

Terezino údolí anglický park v přímém sousedství Nových Hradů s řadou romantických staveb a umělým vodopádem; jméno dostalo po buqoyské hraběnce, která je začala r 1756 budovat. Okružní naučná stezka z náměstí (6 km) vede až k Cuknštejnu.

Weitra (Vitoraz) hrad i město založil v letech 1201 Hadmar II. z Kuenringů. Renesanční zámek Furstenbergů z let 1590 – 1606, na náměstí zachována řada renesančních měšťanských domů, částečně zachované středověké městské opevnění.

Žumberk tvrz doložena již v polovině 13.století, v l.1602 – 1610 letní sídlo Viléma z Rožmberka, později přestavěna renesančně a opevněna hradbou se 6 baštami. Dnes expozice lidového malovaného nábytku Jihočeského muzea.

Podrobnější informace se dají získat na adrese www.novehrady.cz

V Informačním centru na náměstí v Nových Hradech je možné získat materiály popisující zajímavosti Nových Hradů, okolí a to včetně popisu cykloturistických tras.

Zdroje:
Novohradské hory, soubor turistických map 1 : 50 000, Edice Klubu českých turistů, č. 74, 1. vydání, vydal KČT Praha, 1992
Informační materiály Kulturního a informačního střediska v Nových Hradech

Předběžné oznámení o konání konference a žádost o příspěvky

XXIII. konference Českého sdružení uživatelů otevřených systémů EurOpen.CZ (www.europen.cz) se koná od neděle 28.9. do středy 1.10.2003 v hotelu Flag 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
- digitální TV a Multimedia Home Platform
- vyhledávací stroje
- XML a ASN.1

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 10.8.2003 buď e-mailem na adresu europen@europen.cz

nebo poštou na adresu.

Česká společnost uživatelů otevřených systémů
EurOpen.CZ
V Olšinách 75/2300
100 00 Praha 10

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 17.8.2003.

Příspěvky ve tvaru publikovatelném ve sborníku je třeba zaslat do 14.9.2003. 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 24.8.2003 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 25.5. od 13 do 17 hodin
	Konference začíná v pondělí 26.5. v 9 hodin a končí ve středu 28.5. cca ve 14 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Ústav fyzikální biologie Nový Zámek 136 , 373 33 Nové Hrady www.greentech.cz Klášter sv. Petra a Pavla řádu servitů Husova 2 373 33 Nové Hrady http://www.novehrady.cz/turista/klaster/klaster.htm
Kam zaslat přihlášku	Vyplněnou přihlášku společně s oznámením o platbě zašlete na adresu: EurOpen.CZ V Olšinách 75/2300, 100 00 Praha 10 tel: 281 002 222, fax: 281 002 244 e-mail:europen@europen.cz
Co zahrnuje účastnický poplatek	vložné, sborník, stravné, raut, občerstvení během přestávek, prohlídku hradu, varhanní koncert a ubytování
Úhrada poplatku	č.ú. 478928473 u ČSOB Praha 1, kód banky 0300 variabilní symbol 0250503 (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	23.5.2002 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 90. Tutorial se uskuteční v učebně ÚFB JČU vybavené 10 počítači. Maximální počet účastníků tutorialu je 20.
Další informace	Pořizování audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno.

Konferenční poplatky

Vložné		
platba	tutorial	konference
členové		
do 17.5.	790	1 800
po 17.5.	890	2 050
ostatní		
do 17.5.	890	2 100
po 17.5.	990	2 350

Ubytování a stravné	
od neděle 25.5.	1 350
od pondělí 26.5.	975

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

Ubytování 250 Kč/den ve dvoulůžkovém pokoji
Plná penze 200 Kč/den, oběd a večeře 75 Kč, snídaně 50 Kč
Ubytovací kapacita je zhruba 90 osob.

člen ano	platba do 17.5..ano	tutorial	konference Kč	ubytování od neděle	Kč	celkem Kč

Zakřížkujte pole člen, pokud jste členy EurOpenu.CZ.
Zakřížkujte pole do 17.5., pokud je platba provedena do 17.5.
Zakřížkujte pole od 25.5., pokud si přejete ubytování od neděle.

V opačných případech (nečlen, platba po 17.5. 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 17.5., chce tutorial a ubytování od neděle.

člen ano	platba do 17.5. ano	tutorial Kč	konference Kč	ubytování od neděle	Kč	celkem Kč
X		890	2 050	X	1.350	4 290

Přihláška na XXII. 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					
Ubytování v rámci možností jednu možnost označit x	klášter		zámek		

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 0250503	
Razítko a podpis účtárny	

Konferenční poplatky
(vzor vyplnění viz předchozí strana)

člen ano	**platba do 17.5. .ano**	**tutorial**	**konference Kč**	**ubytování**		**celkem Kč**
		Kč		**od neděle**	**Kč**	