Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

XXX. konference – XXXth conference

Hotel MALEVIL, s. r. o., Jablonné v Podještědí
20.–23. května 2007

Vážené kolegyně, vážení kolegové,

uplynulo to, ani nevím jak, a máme tu třicátou jubilejní konferenci EurOpen. Kulaté výročí oslavíme úvodní přednáškou L. Lhotky o historii UNIXu. Dále je konference členěna po jednotlivých dnech na tři samostatná témata:

- Pondělí: Identity/Access management.
- Úterý: Dlouhodobá archivace elektronicky podepsaných dokumentů.
- Středa: Bezpečnost v počítačových sítích. Tedy spíše ne-bezpečnost, takže doufám, že z toho nebudeme mít nějaké nepříjemnosti s orgány státní moci.

Ještě je třeba připomenout, že se začíná už v neděli tutoriály. Ano, opravdu budou tutoriály dva: první bude věnován bezpečnosti OS Windows Vista a druhý současným standardům pro platební karty.

Vzhledem k zahraničním hostům proběhnou pondělí a úterý některé přednášky v angličtině.

Identity/Access management

Tato oblast je dnes velice aktuální, protože asi málokterá organizace/firma se nezabývá implementací (nebo alespoň o ní neuvažuje) těchto prostředků. Existuje celá řada produktů pro Identity Management. My jsme vybrali čtyři různé přístupy k této problematice. Blok zahájí Key Note Petera Sylvestera z Paříže, pak následuje Ralf Knöringer ze Siemensu v Mnichově, pak Jiří Bořík ze Západočeské university a nakonec Marta Vohnoutová se s případovou studií a svými zkušenostmi s ITIM. Blok je doplněn příkladem implementace workflow pro Idenity Management, bez kterého se žádná rozumná implementace neobejde.

V případě Access managementu jsme zvolili zcela jiný postup. Po Key Note L. Dostálka bude následovat přednáška jak na Access management s Open Source produkty.

Dlouhodobá archivace

Dlouhodobá nebo dokonce trvalá archivace elektronických dokumentů je oříšek, který dosud nebyl uspokojivě vyřešen. IETF proto vytvořila pracovní skupinu „Long-Term Archive and Notary Services“ – LTAS. Šedou eminencí této skupiny je Peter Sylvester, který udržuje i web skupiny http://ltans.edelweb.fr na svém počítači. Hnacím motorem skupiny je A. Jerman Blažič (Slovinsko). Úterní dopoledně jsme pak připravili jako workshop s těmito osobnostmi.

Bezpečnost

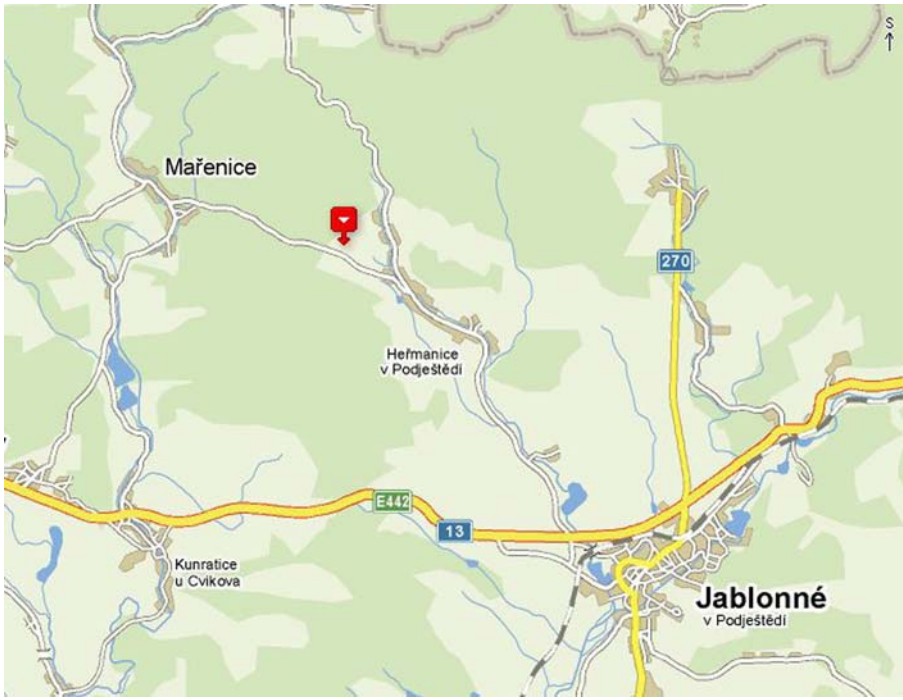
Středa je ze zcela jiného soudku. Je věnována bezpečnosti. Nejprve si vyslechneme přednášku o tom, o čem se dnes hovoří. Tj., jak je to s těmi algoritmy pro výpočet otisku (hash). Abychom se pak byli schopni sami rozhodnout, jestli algoritmy MD-5 a SHA-1 musíme hned zítra nahradit algoritmy z rodiny SHA-2 nebo stačí třeba až za rok.

Následovat bude přednáška Petra Břehovského. On nám řekne, jak to udělat, abychom byli na Internetu opravdu anonymní. Abych byl upřímný, tak si tak zcela nejsem jist, jestli se o tom může vůbec přednášet. Ale každopádně se na tu přednášku velice těším.

Nakonec přijdou dvě velice zajímavé přednášky o praktických zkušenostech, tj., jak to opravdu v praxi s bezpečností chodí.

Kde

Konference proběhne v pohádkovém prostředí ranče Malevil v Heřmanicích v Lužických horách (http://www.malevil.cz). Ubytování bude jak přímo na Ranči tak v několika přilehlých objektech maximálně vzdálených 1 200 m. Stravování bude přímo na ranči.



Ranč disponuje velkým množstvím zajímavých možností sportovního vyžití (squash, plážový volejbal, jízdní kola, golf, ...). Zamluvili jsme na neděli a pondělí večer bowling. A neprojevili jsme zájem o adrenalinovou stěnu.

Práce v sekcích

Heřmanice v Lužických horách jsou na hranici se Svobodným státem Sasko, jehož součástí je i bývalá součást českého státu – Lužice. Po prostudování mapy jsme zjistili, že na české straně se pohoří jmenuje Lužické hory a na lužické straně Žitavské hory. Nezbylo než provést podrobnou rekognoskaci terénu. A výsledek byl překvapivý. Ač jsem ze zeměpisu nikdy neexceloval (slovo nesouvisí s MS Excel), tak jsem pochopil, že to jsou opravdu asi dvojí hory. Lužická strana připomíná miniaturní Česko-Saské Švýcarsko, kdežto českou stranu tvoří kužele bývalých sopek. Uprostřed Žitavských hor je městečko Oybin s hradem na monumentální pískovcové skále. Do městečka se údolím proplétá údajně stále funkční úzkokolejka.

Největším zážitkem z rekognoskace terénu pro mne byla vcelku nenápadná Česká vyhlídka v Žitavských horách, ze které je výhled na Žitavu, megalomanskou elektrárnu Bogatyňa v Polsku, ale opravdu trochu i do Čech. A musím říci, že je to příjemný pohled do Čech.

Nevýhodou ale je, že v okolí je značné množství hraničních přechodů, ale všechny jsou jen pro pěší a cyklisty. Autem je to do Oybinu (centra Žitavských hor) hodina. Proto jsme se dohodli s majitelem ranče, že nás odveze na přechod pro pěší nad Oybinem a práce v sekcích bude spočívat ve vaší rekognoskaci obojích pohoří a návrat zpět po svých.

Libor Dostálek

Program

Neděle 20. 5. 2007

14.00	Bezpečnost OS Windows Vista	*Martin Pavlis*
16.30	Co obnáší současný standard platebních karet	*Jan Okrouhlý*

Pondělí 21. 5. 2007

9.00	Oficiální zahájení	*Jiří Felbáb*
9.05	Historie UNIXu	*Ladislav Lhotka*
10.00	KeyNote: Identity and authorisation in multi-organisation contexts	*Peter Sylvester*
10.45	Přestávka na kávu	
11.00	Identity Management – Compliance and Cost Control	*Ralf Knöringer*
11.45	Identity Management – ORION implementation	*Jiří Bořík*
12.30	Oběd	
13.30	Případová stude: Identity a access managment	*Marta Vohnoutová*
14.45	Implementace Workflow pro Identity Managment	*Jakub Balada*
15.15	Přestávka na kávu	
15.30	KeyNote: Reverzní proxy neboli Access management	*Libor Dostálek*
16.15	Implementace Access Managementu s open source produkty	*Martin Čížek*
17.30	Večeře	
18.30	(večerní přednáška) Zkušenosti s granty EÚ	*Aljosa Blažič*

Úterý 22. 5. 2007

8.30	Spisová a archivní služba v ČR z hlediska současné legislativy a praxe	*Bohumír Brom*
9.30	Trusted Archive Autority	*Aljosa Blažič*
10.30	Přestávka na kávu	
10.45	Slovenian experience with long term archiving	*Aljosa Blažič*
11.30	Electronic Signatures: The French Administration's profile for XADES	*Peter Sylvester*
12.15	Electronic notary services	*Peter Sylvester*
	Oběd	
	Práce v sekcích	
19.30	**Společenský večer** – opékání masa	

Středa 23. 5. 2007

8.30	Jak je to se sílou algoritmů pro výpočet hash	*Michal Hojsík*
9.15	Jak opravdu anonymně vystupovat na Internetu	*Petr Břehovský*
10.30	Přestávka na kávu	
10.45	Kovářova kobyla...	*Radoslav Bodó*
11.30	...už nechodí bosa	*Michal Švamberg*
	Oběd	

Konferenční poplatky

Vložné		
Platba	Tutoriály (oba)	Konference
Členové		
do 15. 5. 2007	790	1 900
po 15. 5. 2007	890	2 150
Nečlenové		
do 15. 5. 2007	890	2 200
po 15. 5. 2007	990	2 450
Ubytování a stravování		
od neděle 20. 5. 2007	3 030	od nedělní večeře do středečního oběda, 3 noclehy
od pondělí 21. 5. 2007	2 270	od pondělní snídaně do středečního oběda, 2 noclehy

Tutoriál je možné objednat i samostatně, poplatek za tutoriály je pouze jeden a nelze jej dělit. Účast na konferenci není podmínkou pro účast na tutoriálu.

Ubytování a plná penze 1 010 Kč na den (ubytování 600 Kč na den, plná penze 410 Kč, oběd 130 Kč, večeře 160 Kč a snídaně 120 Kč).

Kapacita hotelu je zhruba 100 osob.

Programový výbor

Dostálek Libor, Siemens Praha
Felbáb Jiří, Commerzbank Praha
Rudolf Vladimír, Západočeská univerzita v Plzni

Kdy	Tutoriál se uskuteční v neděli 20. 5. od 14 do 19 a více hodin
	Konference začíná v pondělí 21. 5. v 9 hodin a končí ve středu 23. 5. cca ve 14 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělní snídaně, podle zvolené varianty.
Kde	MALEVIL, s. r. o. 471 25 Jablonné v Podještědí http://www.malevil.cz
Kontaktní adresa	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, občerstvení během přestávek a ubytování
Úhrada poplatku	č. ú. 478928473 u ČSOB Praha 1, kód banky 0300, variabilní symbol v elektronické přihlášce (nutno uvést), společnost EurOpen.CZ, Univerzitní 8, Plzeň IČO: 61389081, DIČ: CZ61389081 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.
On-line přihlášky	Anotaci příspěvků a elektronickou přihlášku je možné najít na adrese: http://www.europen.cz V programu konference může dojít k drobným časovým i obsahovým změnám.
Doklad o zaplacení	Zašleme v rámci vyúčtování po skončení semináře.
Uzávěrka přihlášek	16. 5. 2007 nebo při naplnění ubytovací kapacity.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 100.
Další informace	Pořizování audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno.
Přihláška	**Pouze e-přihláška: Webový formulář viz** http://www.europen.cz

Bezpečnost OS Windows Vista

Martin Pavlis

Přednáška seznámí s novinkami v oblasti bezpečnosti na platformě OS Windows Vista. Zaměří se komplexněji na Windows Firewall, nahlédne blíže do chystaného Network Access Protection (NAP), představí novinky v samotném TCP/IP mnohé další.

Martin Pavlis – martin@pavlis.net
Microsoft
Martin Pavlis, MCT, MCSE+S+E, MCSA+S+E, MCP.
Vedení autorizovaných kurzů firmy Microsoft, účast na projektech návrhu a implementace podnikových řešení na platformě Microsoft, realizace odborných seminářů a konferencí. Se zaměřením na tyto technologie: Windows Cluster, Windows Server Systems, Echange Server, ISA Server a další.

Co obnáší současný standard platebních karet

Jan Okrouhlý

Kartu s čipem již má asi téměř každý. Co ale její výroba a používání obnáší? Lehký úvod do standardu čipových karet ISO 7816 a do EMV standardu pro platební aplikace. Bude následovat praktická ukázka komunikace s čipovou kartou, včetně předvedení platební transakce.

Hlavní důraz bude kladen na přiblížení reálného životního cyklu aplikace od přípravy prostředí, výběru a testování čipu, přes výrobu a certifikace až po reálné použití. Jaké jsou další aplikační možnosti využití čipu, bezpečnostní aspekty platebních karet v praxi a kam dále hodlá vývoj standardů kráčet.

Jan Okrouhlý – okrouhly@kp.cz
Hewlett-Packard, s. r. o.
Ing. Jan Okrouhlý (*1972) vystudoval Katedru informatiky a výpočetní techniky Fakulty aplikovaných věd Západočeské Univerzity v Plzni. Po vystudování pracoval v tamním Centru informatiky a výpočetní techniky v Laboratoři počítačových systémů na rozličných IT projektech. Od roku 2005 je zaměstnán jako technologický konzultant v Hewlett-Packard Praha, kde se podílí na vydávání čipových karet.

Historie UNIXu

Ladislav Lhotka

Unix má dnes silnější pozici než kdykoli v minulosti. Některou z jeho odnoží najdeme prakticky na všech počítačových platformách od mobilních telefonů přes laptopy a servery až po superpočítače.

Přednáška se zabývá Unixem především jako ideou a všímá si okolností vzniku a vývoje jeho hlavních principů a stavebních kamenů, které jsou přítomné ve všech jeho variantách. Unix ale pamatuje vedle úspěšných období i jednu poměrně dlouhou periodu postupného úpadku, která jen shodou okolností nevedla k jeho zániku. Přednáška proto ukazuje, že úspěch Unixu je také odvozen ze specifického modelu vývoje softwaru založeného na sdílení zdrojového kódu, relativní tvůrčí samostatnosti programátorů a potlačení marketingových priorit. Přednáška si také všímá některých zajímavých aspektů souběžného vývoje a postupného prolínání Unixu s protokoly TCP/IP.

Ladislav Lhotka – lhotka@cesnet.cz
CESNET, z. s. p. o.
Ladislav Lhotka (*1959) absolvoval v r. 1983 matematické inženýrství na FJFI ČVUT a v r. 1992 ukončil vědeckou aspiranturu v ÚTIA AV ČR v oboru Technická kybernetika. V první dekádě své profesionální kariéry se věnoval 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. Od r. 2001 pracuje ve sdružení CESNET, kde v současné době vede aktivitu Programovatelný hardware a podílí se též na spolupráci v rámci mezinárodního projektu GÉANT2. K jeho odborným zájmům patří kromě síťových technologií ještě operační systém Linux, programování v Pythonu a systémy pro zpracování textu (XML, TEX).

KeyNote: Identity and authorisation in multi-organisation contexts

Peter Sylvester

Identity and authorisation are deeply related issues with impacts on their respective management. The topic gets complicated in a context where authorisation has to be managed across boundaries of organisations. As an example, this applies in particular to public administrations or to semi-public organisations where agents/employees from one organisation want to access resources of another organisation. using a concrete use case, the topic and a solution will be explained and compared with other techniques.

Electronic Signatures: The French Administration's profile for XADES

Peter Sylvester

The European Directive for Electronic signatures requires that an electronic signature identifies the signer. ETSI has produced two texts extending the major signature formats, i. e. CADES for the Cryptographic message syntax and XADES for XML-DSIG with several features. In the context of establishing interoperability rules, the French administration has specified a profile for XADES which must be supported by all implementations. The presentation explains the profile and the reasons for the choices.

Electronic notary services

Peter Sylverster

Trusted "third" parties are used in real life situations, the services provided by them share a common framework concerning the requests and the results of such services. In the electronic world, this framework translates to common requirements and features that such services need to provide independant of the nature of the service itself using two examples of work in the IETF, details of such a common framework are presented.

Peter Sylvester – Peter.Sylvester@edelweb.fr

More than 30 years of experience in network, system and application security, studies and implementation od security solution for various environments and networks. Co-founder of EdelWeb, a French IT-security company since 1995, after work as IT engineer at INRIA France and GMD Bonn, Active participation of standardisation and open source development, specification, architecture, development et maintenance of software and proof of concept implementations Development of multinational computer networks, participation in 5 EU IST programs. Diplome in Mathematics from University Bonn.

Identity Management – Compliance and Cost Control

Ralf Knöringer

Identity management has evolved from the urgent need to efficiently manage heterogeious IT-enviromnments.

Furthermore security requirements and upcomming compliance issues are dominant drivers in the development of future integrated identity and access technologies. Focus areas of this presentation will be the support of service

oriented architectures and the strong integration with existing IT-infrastructure elements like business applications from SAP and Microsoft ADS.

Ralf Knöringer – ralf.knoeringer@siemens.com
Siemens AG
Mr. Knöringer has more than 15 years practical experience within the international security market place. His special focus areas are Identity & Access Management, Provisioning & Directory solutions.

With his comprehensive knowledge of the Security market place, technology trends and international customer projects Mr. Knöringer is the management contact for Siemens key customers and strategic partners interested in secure user management, entitlement and access management solutions.

Identity Management – ORION implementation

Jiří Bořík

This presentation discusses two steps crucial to the implementation of an Identity Management system – data source consolidation, and building an advanced provisioning system. As a part of an actual solution (ORION management), Sun Java System Identity Manager project implementation is presented.

Jiří Bořík – borik@civ.zcu.cz
CIV ZČU
Ing. Jiří Bořík graduated in 1992 at the University of West Bohemia specializing in Electronic computers. Since 2004, he works with the Centre for Information Technology at the University of West Bohemia. As a member of the Laboratory for Computer Science, he participates in developing the ORION Computing Environment focusing, among others, on identity management solutions.

Případová stude: Identity a access managment

Marta Vohnoutová

Implementace identity a access managementu se mohou velmi lišit. Přesto z vlastní zkušenosti vím, že pouhá teorie identity a access většinou příliš nepomůže v našem vlastním řešení. Prostě není nad praktický příklad.

Naše implementace je poměrně rozsáhlá pokrývá intranet klienta a bude se rozšiřovat i na oblast Internetu a extranetů. Zajímavá je v tom, že neřeší pouze centralizovanou správu uživatelských identit, ale také centralizovanou správu uživatelských oprávnění, žádání o jejich přidělení a schvalovací mechanismy.

Také uživatelská oprávnění jako taková nejsou převzata z nabídky access managementu, ale vytvořili jsme si vlastní systém uživatelských oprávnění „šitý na míru“ jednotlivým integrovaným aplikacím.

Marta Vohnoutová – Marta.Vohnoutova@siemens.com
Siemens IT Solutions and Services, s. r. o.
Měla na starosti projekty bezpečného připojení k Internetu a budování a monitorování bezdrátových sítí. V PVT, a. s. byla zaměstnána jako Senior konzultant. V současné době pracuje v Siemens IT Solutions and Services, s. r. o., jako Solution architekt. Je spoluautorkou nově vyšlé knihy *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Je držitelem MCSE a MCT pro W2K.

KeyNote: Reverzní proxy neboli Access management

Libor Dostálek

Přednáška bude obsahovat objasnění rozdílů mezi proxy a reverzní proxy. Bude popsán problém autentizace klientů vůči cílovým serverům. Zmíněny budou základní autentizační metody: basic, webovými formuláři, uživatelským certifikátem, protokolem Kerberos (včetně SPNEGO) atd.

Dále pak budou zmíněny uživatelské role, přístupové seznamy (ACL) a přístupová práva (POP).

Libor Dostálek – Libor.Dostalek@siemens.com
Siemens IT Services and Solutions
RNDr. Libor Dostálek (*1957) je vedoucím oddělení IT Security Consulting společnosti Siemens IT Solutions and Services. Podílel se na projektech se zaměřením na poskytování Internetu, elektronické bankovnictví, bezpečnost sítí a IT bezpečnost. Je autorem Velkých průvodců:

- *Velký průvodce protokoly TCP/IP a DNS* (anglicky vyšlo jako dvě publikace: „Understanding TCP/IP“ a „DNS in action“, rusky vyšlo jako „TCP/IP и DNS в теории и на практике. Полное руководство“.
- *Velký průvodce protokoly TCP/IP, bezpečnost* (vyšlo též polsky pod názvem „Bezpieczeństwo protokołu TCP/IP“)
- *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.*

Implementation of Workflow for Identity Management

Jakub Balada

Jedním z velkých přínosů implementace I&A managementu je automatizace organizačních postupů ve společnosti, ať už se jedná o zařazení nového zaměstnance do systému, nastavení jeho přístupových oprávnění nebo například změna pracoviště. Převedení těchto operací z papírové formy pod správu I&A systému

vyžaduje hlubokou analýzu organizace společnosti, komplikované jednání s jejími zástupci, navržení a implementace daných workflow a v neposlední řadě naučení všech zaměstnanců novým návykům. O tom všem bude tento příspěvek.

Jakub Balada – Jakub.Balada@siemens.com
Siemens IT Solutions and Services
Jakub Balada je studentem 5. ročníku MFF UK, oboru softwarového inženýrství. Ve společnosti Siemens patří do skupiny IT bezpečnosti, kde se v současné době věnuje Identity managementu. Dále se zabývá problematikou PKI čipových karet, hlavně jejich využitím v elektronickém bankovnictví.

Implementace Access Managenetu s open source produkty

Martin Čížek

Access management je možné implementovat různými způsoby. Některá řešení jsou založena na komplexních komerčních produktech, jiná jsou kombinací menších projektů, kde každý plní jen svoji funkci. Rozhodneme-li se vydat cestou vlastní integrace menších balíků software, vezmeme tím na sebe určitou odpovědnost, ale získáme mnoho možností a velkou flexibilitu. Některými možnostmi implementace access managementu s využitím open source software se zabývá tato přednáška.

Martin Čízek – martin@cizek.com

Autor se zabývá problematikou integrace a návrhu heterogenních systémů, vývojem lightweight J2EE aplikací, školením technologií a open source produktů. V současné době pracuje jako team leader ve společnosti Itonis, s. r. o., vyvíjející platformu pro multimediální služby dodávané prostřednictvím IP sítí.

Spisová a archivní služba v ČR z hlediska současné legislativy a praxe

Bohumil Brom

Zaměření:

- nová legislativa o archivní a spisové službě v ČR platná od 1. 1. 2005 (zákon č. 499/2004 Sb. a jeho prováděcí vyhlášky), organizace a kompetence příslušných institucí v oblasti spisové služby a archivnictví v ČR,
- tzv. spisová služba – správa dokumentů v instituci (u původce): nová legislativní pravidla a povinnosti pro příslušné subjekty, správa „specializovaných“ dokumentů (účetní, utajované apod.), dokumenty v klasické i v elektronické podobě,

- tzv. předarchivní péče u veřejnoprávních i soukromoprávních institucí, výběr archiválií, povinnosti subjektů a jejich komunikace s příslušnými veřejnými archivy,
- ukládání archiválií a jejich správa v archivech.

PaedDr. Bohumír Brom – BOHUMIR.BROM@NACR.CZ

Absolvent VŠ studia historie se zaměřením na učitelství. V letech 1980–1990 působil jako pedagog. Od roku 1990 pracuje v Národním archivu (dříve Státním ústředním archivu) jako archivář, a to v oblasti předarchivní péče. Dlouhodobě se specializuje na obory průmysl, obchod a finance, zejména pokud jde o ústřední instituce státní správy a jejich podřízené organizace.

Trusted Archive Autority

Aljoša Jerman Blažič

Contemporary business platforms and active legislation are getting in line to deliver foundation for overall business process dematerialization. Business processes heavily rely on documents where more than 80 % of information is kept. Shifting to electronic form and preserving such electronic heritage is a challenging task. Beside management and readability issues of archived electronic records on the long term basis technology solutions now address preservation of electronic documents' integrity and authenticity.

Trusted Archive Authorities is the final building block of business process dematerialization, providing a stable and secure environment for electronic records on a long term basis. In technology context, Trusted Archive Authorities present a combination of sophisticated record keeping solutions, which efficiently manage preserved records and demonstrate their integrity at any point in the future. Using Trusted Archive Solutions authenticity of business documents is assured during the complete preservation period. Authorities providing preservation capabilities may come in different scenarios. Being a part of internal network or outsourced service they tightly integrate with business information systems. In the recent years a series of technology standardization steps and legislation attempts have been made internationally to fill the gap of missing technological concepts and solutions for long term and formally recognized trusted archiving.

Slovenian experience with long term archiving

Aljoša Jerman Blažič

Long term trusted archiving presents the final obstacle in dematerialization of business processes. With the aim to overcome actual problems, technology and formal answers related to long term preservation need to be provided. This is why international and national initiatives are focusing on the final goal of harmonizing recognition of electronic archiving on technology and on formal level.

First attempts to support electronic archiving have already been done in the past with Law on electronic business and electronic signature (year 2001), whereas Law on document material preservation and archiving (year 2006) provides the general legislative foundation for recognition of electronic document preservation. In the line with legislation attempts, the final and missing technology blocks have been defined and standardized to support trusted archiving in business and governmental environments.

Moving to electronic form is a delicate process for company and organization of any size. Slovenian industry is ready and supported by technology solutions and by legislation. Implementing long term electronic archiving systems is formal and technology based process defined by national legislation in terms of law decree and Common technology requirements (EZT). Learning the steps of national experiences is valuable information for European wide and cross border recognition of electronic records and electronic archiving in both business and governmental environments.

Aljoša Jerman Blažič, M.Sc. – aljosa@setcce.si
SETCCE

Aljoša Jerman Blažič is the head of SETCCE, a research and development company in the field of electronic business and information security. He has graduated of Telecommunication science at the Faculty of Electrical Engineering, University of Ljubljana and obtained his Masters degree at the Faculty of Economics, University of Ljubljana. He is a Ph.D. candidate at the same educational institution, preparing a thesis on the topic of Trusted Archiving Services.

His past work was performed as a researcher for Laboratory for Open Systems and Networks at Jozef Stefan Institute on security systems, broadband and mobile communications mainly for European research projects. He moved to applied research and development projects. His current work is performed in the field of research, design and development of advanced electronic business platforms, formal electronic documents, preservation systems for electronic records, security and privacy mechanisms and ambiental intelligence. He is an active contributor to standardization bodies (IETF, ETSI, GZS, ...) and author of technology standards with special focus on formal electronic documents and preservation mechanisms.

Jak je to se sílou algoritmů pro výpočet hash

Michal Hojsík

Od augusta roku 2004, keď tím čínskych vedcov objavil kolízie pre série hašovacích funkcií MD4, MD5, HAVAL-128 a RIPEMD, získala táto oblasť veľkú pozornosť. Boli objavené nové algoritmy na generovanie kolízií, popísané kolízie pre certifikáty X509, navrhnuté a následne zlomené veľké množstvá vylepšení týchto funkcií. Pozornosti vedcov ale neušla ani dnes najrozšírenejšia funkcia SHA1. Veľké úsilie sa taktiež venuje vývoju nových hašovacích funkcií.

Príspevok obsahuje popis súčastnej situácie v oblasti hašovacích funkcií a detailnejšie popisuje praktické následky známych objavov. V skratke sa taktiež venuje budúcnosti hašovacích funkcií.

Michal Hojsík – Michal.Hojsik@siemens.com
Siemens IT Solutions and Services
Mgr. Michal Hojsík (*1982) vyštudoval obor matematické metódy informačnej bezpečnosti na matematicko-fyzikálnej fakulte Univerzity Karlovej v Prahe, kde taktiež pokračuje na doktorskom štúdiu.

V súčasnosti pracuje ako konzultant na bezpečnostnom oddelení firmy Siemens.

Zaujíma sa predovšetkým o symetrickú kryptografiu a kryptoanalýzu.

Jak opravdu anonymně vystupovat na Internetu

Petr Břehovský

Každé připojení do Internetu, každá odeslaná zpráva a každý kontakt s protějškem zanechá v infrastruktuře sítě nesmazatelnou stopu, kterou nemáme jako uživatelé pod kontrolou, a už vůbec nevíme kdo, kdy a k čemu ji může použít.

Příspěvek obsahuje přehled informací, které v Internetu zanecháváme a přehled metod, které umožňují jejich množství a informační hodnotu redukovat. Podrobněji jsou zmíněny praktické realizace těchto metod: proxy servery, remailery I., II., a III. typu, Nym servery a systém TOR.

Petr Břehovský – breh@breh.cz

Ing. Petr Břehovský (*1965) Vystudoval obor Operační systémy a sítě na katedře výpočetní techniky Petrohradského institutu jemné mechaniky a optiky. Pracoval jako správce operačních systémů UN*X a TCP/IP sítí. Zabývá se 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. V současné době pracuje v oddělení bezpečnosti informačních technologií firmy Telefónica O2 Czech Republic.

Kovářova kobyla...

Radoslav Bodó

V dnešní době rychlého a hojně rozšířeného internetu jsou hackerské útoky na denním pořádku. Díky kvalitním vyhledávačům je navíc velmi snadné najít si různé informace o zdokumentovaných technikách, hotových nástrojích a nezřídka i potenciálních obětech útoku. V tomto příspěvku ukážeme případovou studii forenzní analýzy napadeného počítače s OS Linux.

Radoslav Bodó – bodik@civ.zcu.cz
CIV ZČU
Absolvent Fakulty Aplikovaných Věd Západočeské univerzity v Plzni v oboru Distribuované systémy. Od roku 2005 pracuje v oddělení Laboratoře počítačových systémů, Centra informatizace a výpočetní techniky jako správce operačních systémů Linux a distribuovaného výpočetního prostředí Orion, se specializací na oblast bezpečnosti IS a služeb na platformě Java.

...už nechodí bosa

Michal Švamberg

Žádný operační systém není bezpečný. Je pouze otázkou času, peněz a pohnutek, kdy bude prolomen. Nejčastěji jsou dnes napadány koncové stanice, které mají často nízkou nebo žádnou ochranu. Jako jeden z důsledků „kovářovy kobyly“ bylo zlepšení situace a tím nutnost projít dostupné programy. Jejich průřez s poznámkami z praktického užití naleznete v příspěvku o kování kobyly.

Michal Švamberg – svamberg@civ.zcu.cz
CIV ZČU
Vystudoval obor Distribuované systémy na Západočeské univerzitě v Plzni. Dlouhodobě se věnuje správě operačního systému Linux a jeho nasazení v distribuovaném prostředí Západočeské univerzity v Plzni. Mezi další oblasti patří správa virtuálních serverů Xen, diskového subsystému či distribuovaného souborového systému AFS.

Předběžné oznámení o konání konference a žádost o příspěvky

XXXI. konference Českého sdružení uživatelů otevřených systémů EurOpen.CZ

se bude konat od neděle 21. 10. 2007 do středy 24. 10. 2007 v komplexu Jiřičná u Petrovic na Šumavě http://www.hoteljiricna.cz/

Konference se soustředí na problematiku vývoje aplikací a operačních systémů na bázi Open source. Základní tematické okruhy příspěvků jsou zaměřeny, ale nikoliv omezeny, na následující témata

- Linux a jeho pronikání do podnikové sféry
- vývoj Java aplikací, portálové technologie, portlety, ucelená řešení v portálech

Přijaty budou pouze příspěvky referující o aplikaci uvedených postupů či nástrojů v úspěšně realizovaných projektech.

Výběr příspěvků provede programový výbor konference. Stručnou anotaci příspěvku společně se stručným profesním životopisem autora zašlete nejpozději do 15. 8. 2007 buď emailem na adresu `europen@europen.cz` nebo poštou na adresu

České sdružení uživatelů otevřených systémů EurOpen.CZ
Univerzitní 8
306 14 Plzeň

O přijetí příspěvku budou autoři informováni nejpozději do 10. 9. 2007.

Na webové stránce http://www.europen.cz je možné najít anotace a profily autorů z předchozích konferencí.

Příspěvky do sborníku je třeba zaslat na některou z výše uvedených adres nejpozději do 5. 10. 2007. Příspěvky neprocházejí redakční ani jazykovou úpravou. Sborník je zařazen do nomenklatury ISBN. Autorům příspěvků náleží autorský honorář obvyklý na konferencích sdružení EurOpen.CZ.

Program konference s pozvánkou bude k dispozici do 15. 9. 2007 v papírové a elektronické formě. Dotazy či žádosti o podrobnější informace je možné zaslat emailem na adresu `europen@europen.cz`

Programový výbor konference

Jiří Sitera, Západočeská univerzita Plzeň
Dostálek Libor, Siemens Praha
Felbáb Jiří, Commerzbank Praha
Rudolf Vladimír Západočeská univerzita Plzeň

Pozvánka na XXX. konferenci EurOpen.CZ, 20.–23. května 2007

Editor: Vladimír Rudolf

Sazba a grafická úprava: Ing. Miloš Brejcha – Vydavatelský servis, Plzeň
e-mail: servis@vydavatelskyservis.cz

Tisk: TYPOS – Digital printing, spol. s. r. o.
Podnikatelská 1 160/14, Plzeň