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

XXV. konference
Hotel Klášter
Teplá u Mariánských Lázní
3.10. – 6.10.2004

Programový výbor
Pavlík Roman, Trusted Network Solutions,
Felbáb Jiří, Platina s.r.o.
Rudolf Vladimír, Západočeská univerzita Plzeň
Novotný Jiří, Masarykova univerzita Brno
Pánková Jarmila, UTIA

Organizační výbor
Rudolf Vladimír
Šlosarová Anna
Felbáb Jiří
Urbanec Jakub

Vážené kolegyně, vážení kolegové, vážení příznivci otevřených systémů,

přijměte prosím mé srdečné pozvání k účasti na XXV. konferenci EurOpen.CZ. "Dvacáté páté?", pomyslí si zřejmě náhodný čtenář, "může na dvacáté páté konferenci zaznít něco nového? Nebude hlavním jmenovatelem konference stereotyp?". Věřím, že pravidelný návštěvník bude mít již při letmé prohlídce programu zcela jiné pocity. Jako pravděpodobně první je tato konference monotematická - všechny příspěvky jsou věnované bezpečnosti informačních systémů. Inspirací pro hlavní osnovu konference se stala norma ISO/IEC 17799, která popisuje soubor postupů pro řízení informační bezpečnosti.

Důraz jsme při přípravě konference kladli na praktické využití teoreticky popsaných postupů pro zajištění bezpečnosti. To se odrazilo i při volbě tutoriálu - série příspěvků na téma čipových karet z předešlých konferencí bude zakončena tutoriálem s cílem prakticky předvést použití čipových karet v otevřených systémech (především systémech UNIX). Pro zájemce bude k dispozici čipová karta a čtečka, celý tutoriál bude prokládán řadou praktických cvičení.

Pondělní dopoledne je věnováno úvodu do problematiky bezpečnosti. První příspěvek seznámí posluchače s postupem při tvorbě a zavádění bezpečnostní politiky informačního systému podle relevantních norem, druhý se věnuje bezpečnosti z praktického hlediska. Bude zajímavé porovnat závěry obou příspěvků - první příspěvek začíná v teoretické rovině a postupu směrem k praktickým závěrům, zatímco druhý čerpá z praktických zkušeností, které se pokouší zobecnit.

V odpoledním bloku se návštěvníci konference mohou těšit na praktické zkušenosti z používání identifikačních systémů, příspěvek na téma často opomíjených útoků na klienty a v závěru pak dva "hardwarové" příspěvky - řešení problematiky akcelerace šifrování a monitorování sítí na rychlostech 10 Gbps.

Úterý ráno bude konference pokračovat řešením problematiky zálohování dat. I zde přednášející popíše konkrétní opensource software a zkušenosti s jeho používáním. Následují příspěvky věnované problematice škodlivého softwaru a firewallům - v obou těchto příspěvcích autoři rekapitulují seznam požadavků, které by měl ideální systém splňovat. Posledním příspěvkem úterního dopoledne je atraktivní příspěvek na téma útoků prostřednictvím API. Úterý odpoledne bude již tradičně věnováno práci v sekcích.

Vaší pozornosti by neměl uniknout večerní příspěvek, který je tentokrát věnován kompozici ve fotografii.

Ve středu doplní program příspěvek na téma stále populárnějšího systému pro řízení změn v IT - COBIT. Konferenci zakončí opět čipové karty - tentokráte jejich využití při zvýšení bezpečnosti softwarových aplikací.

Dovolte mi poděkovat všem, kteří se na přípravě programu podíleli. Jirkovi Felbábovi, za jeho odvahu svěřit přípravu programu mnohočlennému programovému výboru, Dolfovi za jeho skvělou organizaci a odstínění programového výboru od jakýchkoliv organizačních záležitostí, Liboru Dostálkovi, za jeho neutuchající úsilí při popularizaci čipových karet, Martinu Macháčkovi za jeho zaoceánské postřehy při hodnocení příspěvků autorů.

Přeji všem příznivcům otevřených systémů, aby XXV. konference byla úspěšná, aby i náhodný čtenář, který se se svými pochybami přeci jen konference zúčastní, dospěl v závěru konference k poznání, jak hluboce se při podobných pochybách mýlil. Jsem přesvědčen, že k tomu přispěje i příjemné prostředí Teplé a doprovodný sportovní a kulturní program.

--
Roman Pavlík
předseda programového výboru

--

Neděle:

13.00 Tutorial - OpenSC - začněte používat čipové karty (součástí bude příklad použití smartcard pro OpenSSH a přihlášení do systému UNIX)	Libor Dostálek

Pondělí:

9.00 zahájení	
9.05 Úvod do norem kolem bezpečnosti	Michal Dostál
10.30 káva, čaj	
11.00 Základní pravidla pro tvorbu bezpečných systémů	Jan Müller
12.25 Otázky a odpovědi	
12.45 oběd	
14.00 Identifikační systémy	Jan Abel
15.00 Útoky na klienta	Juraj Bednár
16.00 káva, čaj	
16.30 Hardwarová akcelerace šifrování datové komunikace	Jiří Novotný, Milan Sova
17.30 Pasivní monitorování počítačových sítí na rychlosti 10Gbps	Tomáš Kořínek, Jan Kořenek
19.00 večere	
19.30 valná hromada	
20.00 kulturní program	

Úterý:

9.00 Zálohování dat pomocí OpenSource SW	Oldřich Balák
9.45 Ochrana proti škodlivému SW	Pavel Baudis
10.30 káva, čaj	
11.00 Firewally v praxi	Josef Pojsl
11.45 Hardwarové bezpečnostní moduly – API a útoky	Jan Krhovják, Daniel Cvrček, Vašek Matyáš
12.30 Otázky a odpovědi	
13.00 Oběd	
14.00 Práce v sekcích	
18.30 Večeře	
19.30 60 minut dobrých rad pro fotoamatéry	Jarmila Pánková

Středa:

8.30 Řízení změn v IT - COBIT	Luděk Novák
9.30 Zvýšení bezpečnosti softwarových aplikací pomocí kryptografické čipové karty	Vašek Matyáš, Petr Švenda
10.30 káva, čaj	
11.00 Cobit v praxi	Ptáčková
12.00 Oběd	

Tutorial - čipové karty a OpenSC
Luděk Rašek
PVT, a.s.

Cílem tutoriálu bude objasnit možnosti čipové karty v operačním systému Linuxu i operačních systémech Windows. Prakticky demonstrováno bude využití v operačním systému Linux.

Zvláštní zřetel bude kladen na zprovoznění čipové karty jako úložiště kryptografických klíčů pro autentizaci SSH relace (OpenSSH, OpenSC, ...). Dále bude popsáno a předvedeno použití karty k přihlášení do operačního systému Linux.

Tutoriál bude tentokrát rozdělen na vlastní tutoriál a volitelná cvičení. Bezprostředně po vlastním tutoriálu budou za sebou budou připravena dvě praktická cvičení: jedno pro uživatele Linuxu a druhé pro uživatele systémů Microsoft.

Zájemci se mohou přihlásit na jedno praktické cvičení (cena cvičení je 350,- Kč -- cena karty). Podmínkou je, že si účastníci přinesou vlastní notebook. Ideální je i čtečka čipových karet (kompatibilní se standardem PC/SC), jinak čtečky budou během tutoriálu k dispozici na zapůjčení. Na cvičení pak obdrží čipovou kartu, takže na svém notebooku si ze cvičení odnesou řádně nainstalovaného klienta.

Na úvod praktického cvičení pro oblast MS Windows bude přednesena přehledná informace o využívání čipových kartách ve Windows.

--
Luděk Rašek (*1973)

vystudoval ČVUT FEL. Dnes pracuje v PVT,a.s. jako konzultant, kde se zabývá zejména problematikou PKI a využíváním čipových karet.

Úvod do norem kolem bezpečnosti
Michal Dostál
KPMG, s.r.o.

Při zavádění bezpečnostních opatření vždy usilujeme o to, aby náklady na tato opatření nepřevyšovaly jejich pozitivní efekt. První kroky ke zvýšení bezpečnosti by se tedy měly opírat o hrubé zmapování bezpečnostní situace, při kterém identifikujeme hlavní aktiva, které chceme chránit a vyhodnotíme rizika, která jim hrozí. To nám umožní určit přiměřená bezpečnostní opatření, která co nejefektivněji zmírní potenciální dopady identifikovaných rizik.

Udržování a zvyšování informační bezpečnosti v organizaci není jednorázovým krokem, ale dlouhodobým procesem. Abychom dosáhli uspokojivého stavu, kdy rizika jsou identifikována a zmírněna na přijatelnou míru, je zapotřebí promítnout řízení bezpečnosti do organizační struktury a identifikovat individuální zodpovědnost a pravomoci.

--
Michal Dostál

je původním vzděláním matematik. Několik let pracuje jako konzultant bezpečnosti informačních systémů, v současné době ve firmě KPMG Česká Republika. Zabývá se analýzami rizik, bezpečnostními prověrkami a tvorbou politik a procedur.

Základní pravidla pro tvorbu bezpečných systémů
Jan Müller
ICZ

Cílem příspěvku je popsat bezpečnost ICT systémů jako průřezový proces, který zasahuje do všech oblastí návrhu, implementace a provozu informačních a komunikačních systémů a který má proto celou řadu nesourodých aspektů. Příspěvek pokrývá širokou škálů těchto bezpečnostních aspektů, od standardů typu ISO 17799 a PP profilů z Common Criteria přes problematiku kryptografie až po technická opatření jako jsou firewally nebo IDS systémy, ale spíše než na technické aspekty jednotlivých řešení je orientován na komplexní pohled na bezpečnost ICT a na možnosti, implicitní požadavky a také na omezení těchto řešení.

--
Jan Müller

v současné době pracuje jako strategický konzultant ve společnosti ICZ a.s., kde se zabývá především problematikou rozsáhlých sítí a jejich bezpečností. Po studiu matematiky na SGWU v Montrealu a MFF UK v Praze a po externí aspirantuře na ČVUT pracoval jako systémový programátor veVÚMS a aplikační programátor v ČSAD. V dalším období se věnoval návrhu a správě sítí a Unixových systémů v ČNR. V té době se stal také spoluzakladatelem CSUUG (nyní EurOpen) a účastnil se na práci Komise pro státní IS jako předseda síťové pracovní skupiny. Po období budování prvních TCP/IP sítí u nás a posléze prvního komerčního poskytovatele Internetu se věnoval návrhu a implementaci síťových a bezpečnostních projektů rozsáhlých zákaznických sítí.

Kombinované identifikační systémy v reálném životě
Jan ABEL
Řízení letového provozu ČR, s.p.

Přednáška bude zaměřena na praktické aspekty procesů zavádění identifikačních systémů na bázi PKI, resp. čipových karet a jejich integraci do heterogenních počítačových systémů.

Na základě dnes již úspěšně realizovaného projektu ukazuje jednotlivé nutné předpoklady a postupné kroky, vedoucí k úspěšnému nasazení takovéhoto systému do reálného života.

Na závěr přednášky budou shrnuta jednotlivá doporučení. A to jak z technického hlediska, tak i z hlediska administrativních resp. byrokratických překážek, na které je nutno se předem připravit, aby celá práce nakonec neskončila vniveč z důvodu neprůstřelné byrokratické hradby i možného odporu uživatelů k takto chráněným systémům.

--
Jan ABEL (*28.6.1964 v Praze)

vystudoval ČVUT, fakultu elektrotechnická, obor Elektronické počítače. Od r. 1991 pracuje v podniku Řízení letového provozu ČR, s.p. jako IT specialista na různých pracovištích v provozu i administrativě. Od ledna 2002 je vedoucí IT oddělení pro oblast manažerských informačních systémů (MIS)

Útoky na klienta
Juraj Bednár

Prednáška sa zaoberá doteraz nie veľmi prebádanou časťou bezpečnosti. Väčšina bezpečnostných produktov sa príliš zameriava na servery ako zdroje najväčších bezpečnostných rizík. Zabúda sa pritom na potenciálne najnebezpečnejšiu časť sieťovej infraštruktúry: ľudia za svojimi počítačmi.

Prednáška zhrnie doterajšie poznatky a prinesie niektoré nové techniky a pozorovania. Bude sa zaoberať:

- Riadenie vnemov (resp. sociálne inžinierstvo), skôr okrajovo
- Útoky na bežné protokoly pomocou man in the middle s ukážkami.
- Interaktívna zmena WWW stránok za chodu, zmeny dôveryhodných zdrojov informácii, nakazenie sťahovaného softvéru (a dôležitosť podpisovania softvéru)
- Okrajovo: obchádzanie osobných softvérových firewallov, možnosti súčasných backdoorov
- Nabúranie PKI klienta: Praktický útok na certifikačnú autoritu (zrealizovaný), iné útoky na PKI
- Man in the middle prakticky: techniky, spôsoby menenia a možnosti odhalenia a ochrany.

Prednáška bude vysoko praktická, k väčšine tém budú praktické ukážky realizácie (pokiaľ to dovolia technické možnosti a neuškodí to názornosti prednášky). Počas konferencie bude možnosť osobného predvádzania zložitejších techník v menších skupinkách.

--
http://juraj.bednar.sk/cv

Hardwarová akcelerace šifrovaného spojení
Jiří Novotný, Milan Sova
Masarykova univerzita Brno, CESNET

Přenos citlivých informací po internetu vyžaduje kryptografické zabezpečení. V příspěvku provedeme základní zhodnocení (klasifikaci) použití kryptografie na různých vrstvách síťového modelu s ohledem na využití hardwarové akcelerace. Pro vybrané aplikace popíšeme problematikou vzniku, řízení a správy akcelerovaného šifrovaného kanálu.

Zaměříme se na implementaci šifer v hardwaru a pokusíme se specifikovat požadavky na kooperaci hardwaru a softwaru při provozu kryptograficky zabezpečeného spojení.

--
Jiří Novotný

pracuje na Masarykově univerzitě od roku 1981, kde začínal jako technik sálových počítačů. Později se věnoval návrhu a vývoji hardware i software pro osobní počítače (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 zástupcem vedoucího aktivity "Programovatelný hardware" CESNETu.

Milan Sova

vystudoval telekomunikační techniku na ČVUT. V letech 1990 až 2000 působil na elektrotechnické fakultě ČVUT jako správce počítačové sítě. 0d roku 2000 pracuje v CESNETu jako koordinátor aktivit v oblasti autentizačního a autorizačního middlewaru.

Pasivní monitorování počítačových sítí na rychlosti 10Gbps
Tomáš Martínek, Jan Kořenek
CESNET

Monitorování síťového provozu je jednou z typických aplikací správy systémů založených na počítačových sítích. S příchodem vysokorychlostních technologií vzniká stále větší tlak na výkon aplikací, které musí celý datový tok analyzovat a zpracovávat. Kritické funkční celky jsou proto přesouvány na úroveň aplikačně specifických obvodů nebo programovatelných hradlových polí.

V článku prezentujeme návrh architektury síťového monitorovacího systému pro technologii 10Gbps. Systém umožňuje vytvářet statistiky vstupních datových toků, vzorkovat pakety s požadovanými vlastnostmi a prohledávat v jejich tělech zadané řetězce. Architektura monitorovacího systému je navržena pro cílovou platformu FPGA a její základní prvky tvoří několik aplikačně specifických nano-procesorů a jednotek, které spolu kooperují. Jako základní prvek, který slouží pro klasifikaci vstupních datových toků, je použita rychlá asociativní paměť CAM.

Návrh a implementace monitorovacího adaptoru je součástí řešení páteho rámcového programu SCAMPI IST-2001-32404.

--
Tomáš Martínek

vystudoval Fakultu informačních technologií VUT v Brně v roce 2003. Nyní je postgraduálním studentem v oblasti aplikačně specifických systémů na čipu a mapování algoritmů na takovéto systémy. Současně pracuje ve funkci zástupce vedoucího skupiny VHDL designu v aktivitě "Programovatelný hardware" sdružení CESNET a podílí se na řešení projektu Liberouter.

Jan Kořenek

vystudoval Fakultu informačních technologií VUT v Brně v roce 2003. Nyní je postgraduálním studentem v oblasti aplikačně specifických systémů na čipu složených z rekonfigurovatelných obvodů a rekonfigurovatelného propojení.
Současně pracuje ve funkci vedoucího skupiny VHDL designu v aktivitě "Programovatelný hardware" sdružení CESNET a je řešitelem EU projektu SCAMPI IST-2001-32404.

Zálohování dat pomocí Open Source software
Oldřich Balák
ZČU Plzeň

Cílem příspěvku je podělit se o zkušenosti získané při hledání Open Source varianty komplexního zálohovacího systému. Jádrem příspěvku je tak popis Open Source zálohovacího software Bacula a jeho srovnání s komerčním protějškem Legato Networker. Kromě popisu použití tohoto software v rámci výpočetního prostředí ZČU Plzeň (zálohování strojů několika platforem a centrálního souborového systému AFS) si tak může posluchač odnést i řadu praktických argumentů pro a proti možnosti náhrady nákladného komerčního software řešením vytvořeným v rámci Open Source.

--
Oldřich Balák

vystudoval Vysokou školu strojní a elektrotechnickou v Plzni. Od roku 2003 pracuje v Centru informatizace a výpočetní techniky ZČU v oblasti zálohování dat a správy tiskových služeb.

V předchozích zaměstnáních pracoval jako programátor a správce počítačové sítě. V současné době se také podílí na vývoji softwarového vybavení Českého národního registru dárců kostní dřeně.

Ochrana proti škodlivému SW
Pavel Baudis
ALWIL software, s.r.o.

Počítačové viry a škodlivé programy jsou bezesporu jedním z velkých nebezpečí dnešních dnů, navíc v poslední době vykazují opravdu bouřlivý vývoj. Příspěvek nejprve shrne možná rizika a nebezpečí, která uživatelům počítačů a Internetu hrozí, a poté ukáže, jakým způsobem je možné se proti těmto nepříjemným programům uspěšně bránit.

Příspěvek se zaměří na jednotlivé viry, které se v posledním roce objevily, a shrne důvody, které k jejich velkému rozšíření vedly. Poté se zmíní o možnostech antivirové ochrany jak pro domací uživatele tak pro velké firmy.

--
Pavel Baudiš

Pracuje jako vedoucí virové laboratoře ve firmě ALWIL Software. Navštěvoval gymnázium v Radotíně a pak VŠCHT, obor ASŘ. Po ukončení školy pracoval ve Výzkumném ústavu matematických strojů v oblasti počítačové grafiky. V roce 1988 se poprvé setkal s počítačovým virem a hned poté se začal věnovat vývoji antivirového systému avast! Již sedmnáctým rokem se zabývá bojem proti virům a vývojem antivirových programů. V roce 1991 spoluzakládal firmu ALWIL Software, často publikuje a přednáší na různých konferencích, které se zabývají bezpečností počítačů.

Firewally v praxi
Josef Pojsl
TNS, a.s.

Pro zařízení oddělující sítě s různou úrovní důvěryhodnosti se vžil termín firewall. Pod tímto názvem se skrývá několik technologií, které se mohou různě kombinovat. Jejich základní povaha a principy jsou všeobecně známy.

V praxi se setkáváme s velmi různou znalostí problematiky. Zásluhou propagace v 90. letech se rozšířil názor, že síť každé organizace má být chráněna firewallem. Představy o tom, co to vlastně znamená, se však diametrálně rozcházejí.

Příspěvek se zaměřuje na praktické zkušenosti s instalací a konfigurací firewallů ve státním i soukromém sektoru v ČR. Shrnuje poptávku a očekávání zákazníků (IT managementu) od firewallu a mapuje rozdíl mezi těmito očekáváními a funkcemi, které může moderní firewall skutečně nabídnout.

--
Josef Pojsl (32)

je technickým ředitelem společnosti Trusted Network Solutions, a.s. Z této pozice řídí vývoj firewallu Kernun a pracuje na projektech týkajících se bezpečnosti sítí a bezpečnostních politik. Bezpečností informačních technologií se zabývá od roku 1996, předtím pracoval jako analytik databázových systémů.

Hardwarové bezpečnostní moduly - API a útoky

Jan Krhovják, Daniel Cvrček, Vašek Matyáš
Fakulta informatiky Masarykovy univerzity v Brně

Příspěvek pojednává o vybraných aspektech hardwarových bezpečnostních modulů a zaměřuje se na útoky na a přes aplikační programovací rozhraní (API). Zajištění bezpečné komunikace u distribuovaných systémů a aplikací vyžaduje, aby byla nějakým způsobem zaručena integrita použitých kryptografických funkcí a důvěrnost jejich šifrovacích klíčů. U běžně používaných výpočetních systémů toho nelze dosáhnout, protože jejich hardware je obvykle fyzicky nezabezpečen a software obsahuje velké množství chyb. To bylo hlavním dovodem návrhu a vytvoření hardwarových bezpečnostních modulů, do jejich fyzicky zabezpečeného prostředí se přesunulo provádění veškerých kryptografických operací. Hlavní oblastí využití hardwarových bezpečnostních modulů je zabezpečení stále se zvyšujícího počtu elektronických transakcí, které probíhají především v bankovních sítích (např. VISA, MasterCard, American Express) při vzájemné komunikaci jednotlivých bank a při komunikaci s jejich peněžními bankomaty.

V první části příspěvku se krom architektury kryptografických modulů seznámíme se základními požadavky na jejich bezpečnost a s americkými normami FIPS 140-1 a FIPS 140-2, jimiž jsou tyto požadavky specifikovány.

Typickou úlohou hardwarových bezpečnostních modulo používaných ve finančním sektoru je, kromě zabezpečení přenosu dat, také bezpečná správa kryptografických klíčů a jiných citlivých dat (např. PINů). Tím se obvykle předchází podvodům ze strany klientů i zaměstnanců bank, a právě
proto musí tyto moduly splňovat ty nejpřísnější možné bezpečnostní požadavky. V druhé části se pak budeme věnovat samotné problematice bezpečnosti API a také popisu útoků, které jsou chybným návrhem mnohých běžně používaných aplikačních programovacích rozhraní umožněny. Funkce API tvoří většinou jediné komunikační rozhraní mezi kryptografickým koprocesorem a vnější aplikací. Jejich pomocí je realizován přístup k veškerým operacím, které umožňuje koprocesor provádět, a jsou tedy nezbytné jak pro správu samotného zařízení, tak také pro komunikaci s jinými zařízeními. API by mělo být navrženo tak, aby nemohlo dojít k jakémukoliv zneužití i kompromitování chráněných dat. Na základ funkcí API jsou budovány protokoly, které bývají typicky tvořeny množinou tří a pěti zpráv, které si předávají jednotliví účastníci. Návrh protokolo je již sám o sobě velmi obtížnou záležitostí, a to i přes malý počet vyměňovaných zpráv, které mohou být útočníkem zmanipulovány. API kryptografického koprocesoru však navíc obsahuje typicky 30-500 funkcí s mnoha nastavitelnými parametry, čímž poskytuje mnohem větší prostor ke zneužití. Představíme si útoky na API starších i současných hardwarových bezpečnostních modulů, přičemž zvláštní pozornost bude věnována útokům vedoucím k získání PINů. Mnoho z objevených útoko na API hardwarových bezpečnostních zařízení spočívá v korektním zadávání příkazů koprocesoru, avšak v neočekávaném pořadí a s neočekávanými parametry. Snaha o co nejflexibilnější návrh těchto (ale i mnohých dalších) zařízení, a tudíž i podpora mnoha standardů i norem, může vyústit v až příli rozsáhlé API, jehož správnou funkčnost lze jen stěží zaručit. V příspěvku ukážeme, že bezpečnost současné generace API není dostačující. I přesto, že cílem tohoto článku není stanovit, jak by měl bezpečný návrh kryptografických API vypadat, je porozumění chybám ve stávajících API prvním krokem jak toho dosáhnout.

--
Jan Krhovják

je postgraduálním studentem Fakulty informatiky Masarykovy univerzity v Brně. Zabývá se bezpečností v IT a mezi jeho hlavní oblasti zájmu během magisterského studia patřil bezpečný hardware. V současné době se zabývá také generováním kryptografického materiálu z hesel a náhodných či pseudonáhodných sekvencí.

Daniel Cvrček

vystudoval (dvakrát) Vysoké učení technické v Brně. Během doktorského studia se věnoval oblasti kontroly přístupu v distribuovaných informačních systémech. Dalšími oblastmi, kterými se zabýval v rámci různých projektů, jsou např. PKI nebo fyzické útoky na čipové karty. V současné době se věnuje projektu SECURE na University of Cambridge.

Vašek Matyáš

přednáší na Fakultě informatiky Masarykovy univerzity a v současné době je Visiting Researcher v Microsoft Research Cambridge, UK. Věnuje se aplikované kryptografii a bezpečnosti IT. Působil na University College Dublin; výzkumném ústavu Ubilab švýcarské banky UBS; jako Royal Society Postdoctoral Fellow na University of Cambridge a u certifikační autority Uptime Commerce. Podílel se i na vývoji Common Criteria, práci v ISO/IEC JTC1 SC27 a je členem redakční rady časopisu Data Security Management.

Kompoziční principy ve fotografii
Karel Ježek, Jarmila Pánková

Velice důležitým aspektem kteréhokoli díla je vhodné spojení jeho obsahové roviny s rovinou formální. To platí pro tvorbu literární, hudební i výtvarnou, včetně fotografické - a to od fotografie reportážní až po uměleckou. Správně zvolené umístění objektu, členění ploch, jejich rytmizace, proporce celku - to vše tvoří zásadní část vyjadřovací formy nazývanou kompozice obrazu.
Obsahem sdělení bude přehled podstatných aspektů kompozice ve fotografii. Bude se vycházet z psychologického a kulturního základu, který popisovaná pravidla určuje a jehož respektování vede k účinnému podání roviny obsahové, jež je (na rozdíl od formy) již zcela v rukou autora.

Sdělení bude vedeno interaktivní formou a část vyhrazené doby bude dle zájmu věnována diskuzi nad vlastními fotografiemi účastníků.

--
Karel Ježek

pracuje v Oddělení neurofyziologie paměti Fyziologického ústavu Akademie věd ČR. Mimo svojí profesi se zabývá výtvarnou fotografií. Pracuje se středo- a velkoformátovou snímací technikou a vychází z postupů klasické černobílé fotografie.

Jarmila Pánková

pracuje jako správce unixové sítě ve výpočetním středisku Ústavu teorie informace a automatizace Akademie věd ČR. Asi deset let se věnuje amatérské fotografii. Pracuje v redakci fotografického e-zinu Paladix. Fotí s manuální kinofilmovou zrcadlovkou a jako zápisník používá jednoduchý digitální přístroj. Nejvíce si cení otištění svých snímků v časopisu Královského autoklubu Tasmánie (RACT).

CobiT - metodika pro řízení a správu procesů ICT
Luděk Novák

CobiT (Control Objectives for Inrormation and releated Technology) je uznávanou metodikou, která napomáhá ve zvládání managementu informačních a komunikačních technologií, které jsou používány pro naplnění hlavních cílů a záměrů organizace. Využívání ICT je v CobiT řízeno souborem všeobecně akceptovaných nejlepších praktik tak, aby využití informací a nasazení informačních a komunikačních technologií přispívalo k dlouhodobému rozvoji organizace, prohlubovalo strategické cíle a snižovalo existující rizika použití ICT. Pro tyto potřeby CobiT definuje 4 základní domény, které odráží základní řídící mechanismy ICT: (1) Plánování & Organizace, (2) Akvizice & Implementace, (3) Dodávka & Podpora a (4) Monitorování.

--
Luděk Novák

v roce 1991 dokončil Vojenskou Akademii v Brně, kde do roku 1994 působil jako odborný asistent. Poté pracoval na Generálním štábu Armády České republiky jako odborník na informační bezpečnost. Od poloviny roku 1999 se věnuje informační bezpečnosti a projektování bezpečnosti informačních systémů v komerčním sektoru. Nyní pracuje ve společnosti BDO IT a.s. jako vedoucí konzultant. Autor je držitelem certifikátu CISA a členem odborných sdružení AFCEA a ISACA.

Zvýšení bezpečnosti softwarových aplikací pomocí kryptografické čipové karty
Vašek Matyáš, Petr Švenda

Digitální zpracování dat poskytuje mimo jiné možnost snadné tvorby identických kopií a rychlou distribuci bez ohledu na geografickou vzdálenost. Přináší s sebou však také problém kontroly jejich použití tak, aby byly zachovány zájmy všech zúčastněných stran. Efektivní správa práv k digitálním objektům (Digital Rights Managment, dále DRM) by měla tento cíl plnit. DRM prováděná ve výpočetním prostředí koncového uživatele bývá typicky zajištěna pomocí autonomní softwarové aplikace (dále softwarový agent) odpovědné za kontrolu využití digitálních dat v souladu s definovanými právy. Problémem běžných výpočetních prostředí typu PC je možnost útočníka plně kontrolovat běh tohoto softwarového agenta, především možnost čtení kódu a zpracovávaných dat a jejich následná modifikace. Útočník tak může docílit nežádoucí změny chování softwarového agenta úpravou jeho kódu nebo využít získaných dat k přímému přístupu k chráněným objektům.

Příspěvek se zabývá možnostmi zvýšení bezpečnosti běhu softwarového agenta využitím programovatelné kryptografické čipové karty s podporou JavaCard, kombinované s metodami mobilní kryptografie. Popisuje ochranné rozhraní umožnující zvýšit úroveň ochrany softwarového agenta v prostředí MS Windows před vybranými útoky. Části softwarového agenta obsahující citlivý kód a data jsou přesunuty do bezpečnějšího prostředí kryptografické čipové karty. Přesunutý kód (dále chráněný algoritmus) je využíván na principu klient-server, kde serverem je čipová karta a klientem zbylá část softwarového agenta ponechaná v nechráněném prostředí PC. Chráněný algoritmus může být využíván pouze definovanou množinou autentizovaných softwarových agentů. Je navržena speciální implementace autentizačního a transportního protokolu pro ochranu hodnot autentizačních klíčů, odolnost proti manipulaci kódu provádějícího kroky protokolu, robustní zajištění důvěrnosti a čerstvosti vyměňovaných dat. Důležitým rozdílem oproti standardním autentizačním protokolům je zohlednění faktu, že klient může být manipulován útočníkem. Je využita alternativní implementace šifrovacího algoritmu AES umožnující ukrýt hodnotu šifrovacího klíče a zároveň ponechat možnost tímto klíčem šifrovat. Prostředí čipové karty lze sdílet více chráněnými algoritmy, u každého chráněného algoritmu lze definovat množinu softwarových agentů oprávněných k jeho využití.

Pro možnost vzdálené a rozšiřitelné správy celého prostředí je přímo na čipové kartě implementována podpora zpracování XML licencí. Pomocí těchto licencí lze mimo jiné vzdáleně aktualizovat interní hodnoty chráněných algoritmů a měnit množiny oprávněných softwarových agentů. Výsledek lze použít pro implementaci DRM architektur, pro možnost kontroly přístupu k uživatelovým privátním informacím (podpisové klíče apod.), nebo utajení implementace algoritmu (podmínky pro spuštění reakčního mechanismu u IDS systému).

Využití programovatelných čipových karet s podporou JavaCard přináší oproti jiným hardwarovým klíčům (dongles) větší výpočetní výkon, možnost bezpečné vzdálené aktualizace umístěných programových balíků a bezpečné sdílení výpočetního prostředí více stranami. Navržené ochranné rozhraní využívá těchto vlastností, přidává možnost správy dat pomocí XML licencí a popisuje rešení problému provedení autentizace mezi stranami, z nichž jedna je vykonávána v prostředí pod kontrolou útočníka.

--
Petr Švenda

vystudoval Fakultu informatiky Masarykovy univerzity v Brně, kde je v současné době PhD studentem v oblasti aplikované kryptografie a bezpečnosti IT. Věnuje se již několik let problematice správy práv k digitálním objektům, bezpečnosti a využití kryptografických čipových karet, kryptografickým protokolům, a to jak v oblasti akademického výzkumu, tak i průmyslového vývoje.

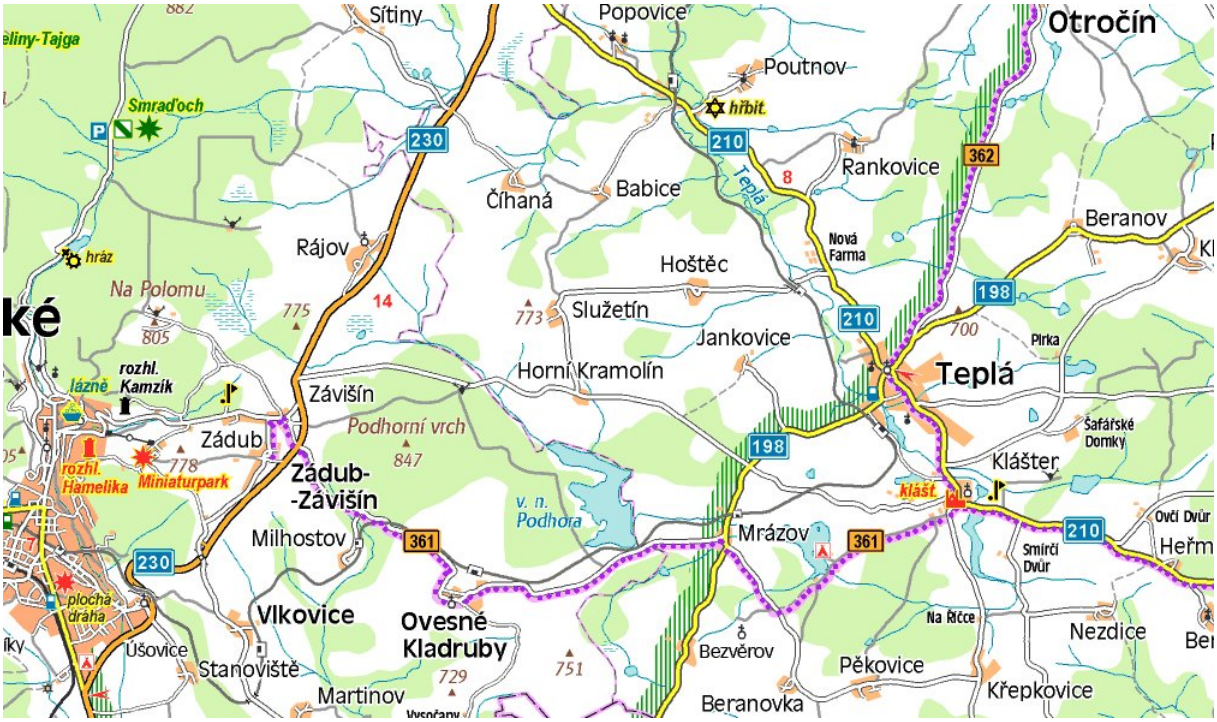
Vašek Matyáš

přednáší na Fakultě informatiky Masarykovy univerzity a v současné době je Visiting Researcher v Microsoft Research Cambridge, UK. Věnuje se aplikované kryptografii a bezpečnosti IT. Působil na University College Dublin; výzkumném ústavu Ubilab švýcarské banky UBS; jako Royal Society Postdoctoral Fellow na University of Cambridge a u certifikační autority Uptime Commerce. Podílel se i na vývoji Common Criteria, práci v ISO/IEC JTC1 SC27 a je členem redakční rady časopisu Data Security Management.

Práce v sekcích.

Práce v sekcích je důležitou součástí konference, kde je možné se seznámit s historií místa konání konference, udělat něco pro své tělo a i prodiskutovat s kolegy(němi) mnohé problémy, které by vás v sevřené místnosti ani nenapadly.
Po zkušenostech z minulé konference poblíž Králického Sněžníku jsme raději situovali konferenci více do vnitrozemí a tak, věříme, znesnadnili během vášnivých diskusí nepovšimnutý přechod státní hranice a s tím související komplikace.
Konference se koná v v komplexu Kláštera premonstrátů v Teplé u Mariánských Lázní a myslím, že nebude třeba tak podrobný popis cesty, jaký předložil Libor Dostálek v minulé pozvánce. Ostatně organizační výbor zjistil, že popis cesty z Johanesburgu stejně nikdo nevyužil. Přesto podstatná informace alespoň pro cyklisty – klášter Teplá je důležitou křižovatkou cyklistických stezek. Končí zde (nebo začínají?) cyklistické stezky č. 352, 361 a 362.

K alespoň základní orientaci malá mapka:



Po Nových Hradech se konference EurOpen.CZ opět koná místě s bohatou historií, tentokrát se jedná o klášter premonstrátský, založený již v roce 1193. Konference bude probíhat v přilehlém hotelu „Klášter Teplá“, který je nedílnou součástí komplexu budov Kláštera. Milovníci historie najdou další informace na stránkách http//:www.klastertepla.cz, které ale určitě nenahradí osobní zážitky přímo v místě.

Na shledání na XXV. konferenci EurOpen.CZ se těší organizační výbor.

Kdy	Tutorial se uskuteční v neděli 3.10. od 13 hodin
	Konference začíná v pondělí 4.10. v 9 hodin a končí ve středu 6.10. cca ve 13 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Hotel Klášter Teplá u Mariánských Lázní tel./fax: 353392264/353392312 http://www.pmgastro.cz
Kam zaslat přihlášku	Vyplněnou přihlášku společně s oznámením o platbě zašlete na adresu: Anna Šlosarová EurOpen.CZ Univerzitní 8, 306 14 Plzeň tel: 377632701 fax: 377632702 e-mail:europen@europen.cz
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 041004 (nutno uvést), společnost EurOpen.CZ, Univerzitní 8, Plzeň IČO: 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	27.9.2004 nebo při naplnění ubytovací kapacity.
On-line přihlášky	Anotaci příspěvků i formulář přihlášky je možné najít na adrese: http://www.europen.cz V programu konference mùže dojít k drobným časovým i obsahovým změnám.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 100.
Další informace	Pořizování audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno.

Konferenční poplatky

Vložné		
platba	tutorial	konference
členové		
do 17.9.	600+350	1 900
po 17.9.	700+350	2 100
ostatní		
po 17.9.	700+350	2 150
po 21.9.	800+350	2 350

Ubytování a stravné	
od neděle 3.10.	2 850
od pondělí 4.10.	2 050

Ubytování 650 Kč/den ve dvoulůžkovém pokoji
Plná penze 300 Kč/den.
Ubytovací kapacita: 100 osob.

Pouze vzor, vyplňte až v přihlášce na další straně.

člen ano	platba do 17.9.ano	tutorial Kč	Cvičení Kč	Konference Kč	ubytování od neděle	Kč	celkem Kč

Zakřížkujte pole člen, pokud jste členy EurOpenu.CZ.
Zakřížkujte pole do 17.9., pokud je platba provedena do 17.9.
Zakřížkujte pole od nedele, pokud si přejete ubytování od neděle.

V opačných případech (nečlen, platba po 17.9. 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 17.9., chce tutorial s praktickým cvičením a ubytování od neděle.

člen ano	platba do 17.9. ano	tutorial Kč	Cvičení Kč	konference Kč	ubytování od neděle	Kč	celkem Kč
X		700	350	2100	X	2 850	6000

Přihláška na XXV. 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 zaškrtnuto, předpokládáme, že s uvedením jména souhlasíte.		A	N
Podpis			
Potvrzení o zaplacení			
Potvrzujeme, že účastnický poplatek ve výši 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 041004			
Razítko a podpis účtárny			

Konferenční poplatky
(vzor vyplnění viz předchozí strana)

člen ano	**platba do 17.9. ano**	**tutorial Kč**	**Cvičení Kč**	**konference Kč**	**ubytování**		**celkem Kč**
					od neděle	**Kč**	