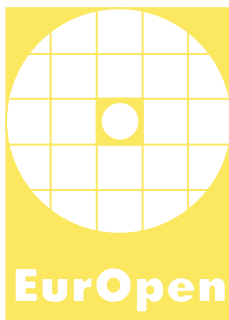


Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz



XXXII. konference



**Rožmberk nad Vltavou
18.–21. května 2008**

Úvodní slovo

Vážené kolegyně, vážení kolegové,

opět se Vám dostává do ruky pozvánka na konferenci EurOpen.CZ. V pořadí je již třicátá druhá, což už je úctyhodná řada. Neodklonili jsme se od tradice, takže časový harmonogram již většinou znáte. V neděli začínáme tutoriálem, v pondělí využíváme skutečnosti, že jste ještě čerství a je celodenní program až do pozdních hodin. V úterý a ve středu jsou přednášky již jen dopoledne a v úterý je samozřejmě odpolední práce v sekcích.

Konference v Rožmberku má tři hlavní témata, všechna určitě najdou své příznivce.

Tutoriál

Začněme nedělním tutoriálem, který se bude věnovat moderním trendům v telefonii, tj. využití IP i v této oblasti. Nosným „buzzword“ určitě bude zkratka VoIP (Voice over IP). Tutoriál povede Michal Petrovič ze Západočeské univerzity, který má bohaté zkušenosti se zaváděním VoIP technologií právě na ZČU v Plzni. Během tutoriálu si některé věci přímo osaháte, neboť není ve zvyku Michala vést své přednášky pouze v teoretickém duchu.

Kybernalita

Celé pondělí je věnováno fenoménu dnešní doby – internetové bezpečnosti. Už jsme na několika EurOpen konferencích toto téma probírali, většinou však z pohledu systémového administrátora nebo člověka, který má bezpečnost na starost. Pohled z druhé strany nám poskytl na konferenci v Devět skal pozvaný pan kapitán Dastych, byla to však svým tématem izolovaná přednáška. Nyní nabízíme ucelený a jistě zajímavý pohled na danou problematiku. Hlavní osoba pondělní sekce a její garant Václav Jirovský nám v úvodu pomůže utřídit pojmy a poté přednesou svůj pohled další řečníci. Pohledy to budou legislativní, sociální, kriminalistické, forenzní i jak se v množství informací orientovat a najít černokloboučnickou stránku či aktivitu.

Je na co se těšit.

VoIP

V úterý se dozvíme, zda VoIP je skutečně za dveřmi jako reálná možnost náhrady klasické telefonní technologie. O tématu budou hovořit lidé, kteří se tímto tématem zabývají dlouhodobě. Jejich zkušenosti nám umožní pohlédnout na problematiku pohledem nezávislých odborníků, pohledem výrobce zařízení a pohledem poskytovatele služeb. Tomuto tématu je ostatně věnován i tutoriál. I když

se to nezdá, i v tomto oboru se uplatňuje open source a mnohé aplikace dosahují v open source oblasti lepších výsledků než komerční produkty. Ostatně, to se možná dozvíte v Rožmberku od přednášejících. Sekci garantuje a zorganizoval Jarda Martan, jeden z přednášejících.

Souborové systémy

Třetí nosné téma konference je věnováno oblasti, kterou jste si vyžádali v dotaznících z minulých konferencí. Jsme Vám vděční za každé téma a jak vidno, umíme i naslouchat. S garantem sekce Honzou Kasprzakem se podařilo sestavit velmi zajímavý blok přednášek o souborových systémech. Úvodní přednáška bude přehledová, od historie po vize. Jen doufejme, že v rámci tréninku nebude přednáška v japonštině, kterou autor, jak sám říká, za účelem mentální relaxace studuje. Své praktické zkušenosti se stabilitou jednotlivých souborových systémů nám poví kolega Michal Krátký. A v další přednášce se seznámíme s nástroji na ovládání a správu souborových systémů. Ucelený blok tvoří přednášky s jedním společným jmenovatelem – SUN, které tvoří závěrečný blok konference.

Konference je letos v Jižních Čechách v Rožmberku nad Vltavou. Někteří jste si jistě otevřeli stránky školicího střediska, kde se konference bude konat. Tam stojí: *„Školící a ubytovací zařízení České pošty se nachází v malebné jihočeské obci Rožmberk nad Vltavou, ležící 25 km jižně od Českého Krumlova, v areálu bývalého zámku, v těsné blízkosti státního hradu. Výhled z oken většiny pokojů skýtá nádherný pohled na celý Rožmberk, kterým protéká řeka Vltava.“* Lépe bych to nenapsal.

Na setkání s Vámi se za všechny, kteří konferenci připravovali, těší

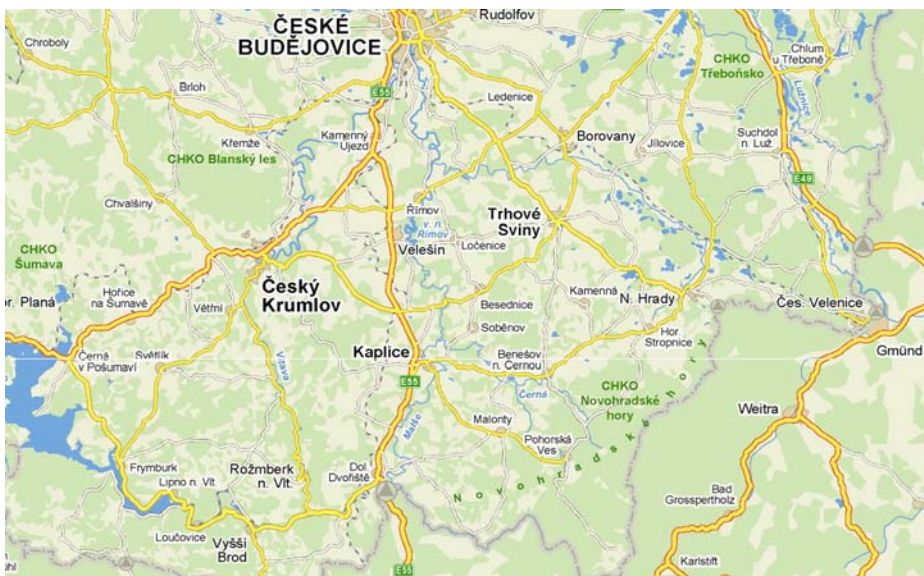
Vladimír Dolf Rudolf

Kam jedeme?

Jedeme do Rožmberku nad Vltavou, který leží jižně od Českých Budějovic a dokonce i jižně od Českého Krumlova. A tak asi budu jedním z mála, který tam pojedje jinak než přes České Budějovice.

Z Budějovic do Rožmberka vedou dvě cesty. Jedna přes Krumlov proti proudu Vltavy a druhá zemědělskou krajinou přes Dolní Dvořiště až na státní hranici a potom zpět k Vltavě. Do Rožmberku pak přijedete z jihu. Druhá cesta sice není turisticky tak zajímavá, ale je výrazně rychlejší a navíc hned na začátku Rožmberku pohodlně zahnete napravo do kopce na silničku vedoucí hradu, kde v Horním hradu bude EuroOpen. Až pojedete silničkou nahoru, tak nezapomeňte v sedle pod mostními oblouky odbočit vlevo jakoby za hrad. O tom, kam kdo odbočil se večer jistě povede plodná diskuse.

Pokud se z Českých Budějovic opravdu vydáte přes Kaplici, pak pojedete i kolem mediálně nejznámějšího jihočeského místa. Tím nejsou památky UNESCO Český Krumlov a Hološovice, ale bohužel Nažidla. Je to osada mezi Skronicemi a Dolním Dvořištěm (nemá ani ceduli na silnici). Při průjezdu roklí za Nažidly směrem na Dolní Dvořiště je na pravé straně onen nový památník.



Silnice z Českých Budějovic do Dolního Dvořiště vede podél železniční trati do Lince. Předchůdcem této trati byla koněspřežná železnice. Po koněspřežné železnici zbyla celá řada pozůstatků. Od budov až po zbytky železničních náspů. Např. pokud pojedete od Českých Budějovic, tak před Velesínem na křižovatce

se silnicí 155 (Krumlov – Římov – Třeboň) přibrzděte, protože po pravé straně u železničního přejezdu jsou zbytky přeprahací stanice. O 300 m dále za vrcholem stoupání je po pravé straně zase obnoven mostek koněspřežné železnice.

Kam na práce v sekcích?

Voda

Když se řekne Rožmberk nad Vltavou, tak se asi málokomu nevybaví vzpomínky na sjezd Vltavy. Úsek Vltavy mezi Vyším Brodem a Českým Krumlovem, na kterém Rožmberk leží, je rozhodně nejfrekventovanější „vodou“ v Česku. Je to i díky tomu, že Lipenská přehrada svým sanitárním výtokem udržuje tento úsek splavným i v těch nejsušších letech.

Ve Vyším Brodu hned pod klášterem je oblíbená půjčovna www.ingetour.cz. Jen pro orientaci: doba plavby z Vyšího Brodu do Rožmberka trvá okolo dvou hodin.

Vyšší Brod a Čertova stěna

Do Vyšího Brodu lze jet z Rožmberka údolím Vltavy, ale také jen přes kopec. Cestu přes kopec doporučuji hlavně při zpáteční cestě, protože ta poskytuje nádherné výhledy na Rožmberk z výšky.

Ve Vyším Brodě je jeden z nejkrásnějších českých klášterů. Po prohlídce kláštera nezapomeňte vyrazit po turistické značce proti proudu Menší Vltavice kolem vodopádů sv. Wolfganga až na vrchol Vyklestila s pozoruhodným vrcholovým skalním útvarem. Dále pak pokračujte na Čertovu stěnu. Tou je nejkrásnější slézt až do koryta Vltavy. Korytem Vltavy lze pak skákat z balvanu na balvan. Až vás to přestane bavit, tak se po druhém břehu podél železnice vraťte zpět do Vyšího Brodu.

Horní Dvořiště a okolí

Pro milovníky netradičních výletů bude jistě zajímavý výlet do Horního Dvořiště, kde se zastavil čas. Obyvatelé si dokonce prosadili značku zakazující vjezd větších automobilů do této obce. Je to úplně jiný svět, který je v naprostém kontrastu s turistickými středisky kolem Vltavy.

Horní Dvořiště známe jako železniční přechod do Rakouska. Dodnes v železniční stanici Horní Dvořiště krátce zastavují i mezinárodní rychlíky. Snad z pietní vzpomínky na minulé časy. Lístky na vlak tu ale už nekoupíte. Samo nádraží leží v bizarní obci Český Heršlák (připomínající kasárna) ze kterého lze dokonce i autem přejet po prašné silničce do Deutsch Hörschlag. Z rakouské strany tam ale zapomněli oddělat zákaz vjezdu.

Směrem na jihozápad z Horního Dvořiště je pak země nikoho. Silničky postavené pohraničníky jsou autem už téměř nesjízdné. Takže pokud byste chtěli navštívit nejjihnější bod Česka, pak je to turisticky náročné. Je to ale kraj průzračných bystřin a pastvin s nádhernými výhledy do okolí. Dobře dostupný ale jen z rakouské strany.

Koupání

Pro ty, kteří budou chtít strávit prázdniny v plavkách, pak vzhledem k ročnímu období, je asi nejbližším řešením nový Aquaworld Lipno. Pokud vás voda omrzí, pak si můžete zpestřit den bobovou dráhou na Lipně.

Já osobně ale preferuji Svět bazénů a zejména Svět saun v Gmündu, ale ten je o 40 km dál.

Cyklisté

Cyklistům doporučuji strávit prázdniny v sekci okruhem vedoucím z Rožmberku na sever přes Rožmitál na Šumavě a zpět kolem Dolního Dvořiště ke státní hranici. Dále pak přes Horní Dvořiště a Studánky do Vyššího Brodu. Z něj pak přes kopec do Rožmberku.

Program

Neděle 18. 5. 2008

| | | |
|-------|-------------------------------|------------------------|
| 13.00 | Tutorial: Jak na IP telefonii | <i>Michal Petrovič</i> |
|-------|-------------------------------|------------------------|

Pondělí 19. 5. 2008

| | | |
|-------|---|---|
| 9.00 | Oficiální zahájení | <i>Vladimír Rudolf</i> |
| 9.05 | Taxonomie kybernetických hrozeb | <i>Václav Jirovský</i> |
| 9.50 | Češi, Internet, bezpečnost | <i>Petr Soukup</i> |
| 10.35 | Přestávka | |
| 10.55 | Soulad české právní úpravy s Úmluvou o kybernetické kriminalitě | <i>Tomáš Gřivna</i> |
| 11.40 | Úloha a možnosti policie připotírání počítačové kriminality | <i>Karel Kuchařík</i> |
| 12.15 | Oběd | |
| 13.45 | Hiearchická struktura pracovišť CERT a její funkce | <i>Andrea Kropáčová Robert Malý</i> |
| 14.25 | Forenzní analyzátor pro operativní analýzu | <i>Róbert Lórenz Tomáš Zahradnický Jiří Buček</i> |
| 15.10 | Přestávka | |
| 15.25 | Skenování otevřených zdrojů | <i>Leo Galamboš</i> |
| 16.10 | Analýza dat otevřených zdrojů | <i>Iveta Mrázová</i> |
| 16.55 | Některé méně tradiční metody detekce škodlivých aktivit v IP sítích | <i>Petr Břehovský</i> |
| 18.00 | Večeře | |
| 19.30 | Astronomická fotografie | <i>Libor Šmíd</i> |

Úterý 20. 5. 2008

| | | |
|-------|---|------------------------|
| 8.30 | Unified Communications | <i>Jaroslav Martan</i> |
| 9.15 | MRoIP, praktické zkušenosti s implementací VoIP | <i>Jiří Novák</i> |
| 10.00 | Přestávka | |
| 10.20 | SIP Express Router – Use Cases for VoIP | <i>Jiří Kuthan</i> |
| 11.05 | Praktické zkušenosti s implementací VoIP v síti O2 | <i>Petr Poupě</i> |
| 11.50 | Implementace IP telefonie na Západočeské univerzitě v Plzni | <i>Michal Petrovič</i> |
| 12.40 | Oběd | |
| 13.00 | Práce v sekcích | |
| 19.00 | Večere s případným rozněním | |
| 20.00 | Večerní prohlídka hradu | |

Středa 21. 5. 2008

| | | |
|-------|--|-----------------------|
| 8.30 | Co umí souborové systémy | <i>Jan Kasprzak</i> |
| 9.10 | Stabilita souborových systémů | <i>Michal Krátký</i> |
| 9.50 | Volume management a Linux | <i>Milan Brož</i> |
| 10.30 | Přestávka | |
| 10.45 | ZFS – The last word in Filesystems | <i>Vineeth Pillai</i> |
| 11.25 | SAM-QFS | <i>Jan Kopřiva</i> |
| 12.05 | Implementation of the file system layer in HelenOS | <i>Jakub Jermář</i> |
| 12.45 | Závěr | |
| 13.00 | Oběd | |

Konferenční poplatky

| Vložné | | |
|-------------------------------|----------|---|
| Platba | Tutoriál | Konference |
| Členové | | |
| do 9. 5. 2008 | 690 | 2 100 |
| po 9. 5. 2008 | 790 | 2 350 |
| Nečlenové | | |
| do 9. 5. 2008 | 790 | 2 400 |
| po 9. 5. 2008 | 890 | 2 650 |
| Ubytování a stravování | | |
| od neděle 18. 5. 2008 | 1 350 | od nedělní večere do středečního oběda, 3 noclehy |
| od pondělí 19. 5. 2008 | 980 | od pondělního oběda do středečního oběda, 2 noclehy |

Tutoriál je možné objednat i samostatně, účast na konferenci není podmínkou pro účast na tutoriálu.

Ubytování a plná penze 450 Kč na den (ubytování 250 Kč na den, plná penze 200 Kč, oběd 80 Kč, večere 80 Kč a snídaně 40 Kč).

Kapacita hotelu je zhruba 100 osob.

Programový výbor

Vladimír Rudolf
Václav Jirovský
Jaroslav Martan
Jan Kasprzak

| | |
|---------------------------------|--|
| Kdy | Tutoriál se uskuteční v neděli 18. 5. 2008 od 13 do 17 a více hodin |
| | Konference začíná v pondělí 19. 5. 2008 v 9 hodin a končí ve středu 21. 5. 2008 cca ve 14 hodin. Stravování je zajištěno od nedělní večere nebo od pondělního oběda, podle zvolené varianty. |
| Kde | Rožmberk nad Vltavou školicí a ubytovací zařízení České pošty http://www.ubytovanicp-rozmbek.w1.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 | vložené, 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. 2008 nebo při naplnění ubytovací kapacity. |
| Kapacita | Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 100. |
| Další informace | Požízení audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno. |
| Přihláška | Pouze e-přihláška: Webový formulář viz http://www.europen.cz |

JAK NA IP TELEFONII

Michal Petrovič

Jedním z aktuálně diskutovaných témat v mnoha organizacích i v široké veřejnosti je IP telefonie. Jedná se o přenos hlasového hovoru prostřednictvím lokální počítačové sítě nebo sítě Internet. Tímto způsobem přenosu lze dosáhnout výrazného snížení nákladů na volání mezi jednotlivými pobočkami organizace nebo mezi ostatními organizacemi. Stejně tak může být telefonní síť organizace tímto způsobem dosažitelná s co nejnižšími náklady ze sítě Internet, případně ze sítí ostatních operátorů podporujících IP telefonii. Tutoriál se bude zabývat praktickou ukázkou zprovoznění IP ústředny a otestování pomocí hardwarových i softwarových IP telefonů včetně poslední dobou hojně diskutovanou konvergencí do bezdrátové sítě.

Ing. Michal Petrovič – PETROVIC@CIV.ZCU.CZ*Centrum informatizace výpočetní techniky, Západočeská univerzita v Plzni, CESNET z. s. p. o.*

Absolvent fakulty aplikovaných věd, ZČU, obor Informatika a výpočetní technika, zaměření Distribuované systémy. Pracuje v oddělení Komunikací a počítačových sítí Laboratoře počítačových systémů při CIV, ZČU jako síťový specialista. Dále se podílí na provozu a rozvoji národní sítě pro výzkum a vzdělávání České republiky – CESNET2 a je specialista na IP telefonii ve skupině multimediální přenosy a kolaborativní prostředí sdružení CESNET z. s. p. o.

TAXONOMIE KYBERNETICKÝCH HROZEB

Václav Jirovský

Přednáška se zabývá rozdělením kybernetických hrozeb do skupin podle znaků hrozby. Jsou odděleně posuzovány znaky z hlediska právního popisu hrozby, z hlediska sociologické příslušnosti útočnicka i z hlediska technologického vrstevového modelu. Cílem taxonomie je kategorizovat hrozby, umožnit jejich standardní identifikaci i tím i standardizaci ochrany a reakce na útok.

Doc. Ing. Václav Jirovský, CSc. – JIROVSKY@DKM.CZ*MFF UK v Praze*

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 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.

ČEŠI, INTERNET, BEZPEČNOST

Petr Soukup

Cílem příspěvku je nabídnout bližší pohled na užívání Internetu v ČR a srovnat užívání Internetu u nás se zahraničím. Na základě výsledků sociologických kvantitativních šetření české populace (osob starších 11 let) World Internet Project 2005–2007 (Fakulta sociálních studií MU) bude provedena typologie uživatelů a poukázáno na specifické rysy užívání Internetu u jednotlivých skupin. Pozornost bude věnována též bezpečnostním aspektům užívání Internetu a vnímání bezpečnosti na Internetu samotnými uživateli. Pro doplnění obrazu nejmladších uživatelů Internetu bude využito šetření Pocit bezpečí provedeného Institutem sociologických studií Fakulty sociálních věd UK v lednu 2008. V tomto šetření byla u 14–16 letých žáků a studentů v ČR zjišťována míra obav z kriminality, dále míra viktimizace a podílu na této trestné činnosti.

Petr Soukup – SOUKUP@FSV.CUNI.CZ

Institut sociologických studií, Fakulta sociálních věd, Univerzita Karlova v Praze
Absolvent Fakulty informatiky a statistiky VŠE Praha, v oboru Statisticko-pojistné inženýrství a Fakulty sociálních věd UK, v oboru Sociologie. Od roku 2000 pracoval jako výzkumník v akademické sféře (Sociologický ústav AV ČR) i komerční (TNS AISA, s. r. o.) V současnosti (od roku 2005) vyučuje statistiku a aplikovaný sociologický výzkum na FSV UK v Praze.

SOULAD ČESKÉ PRÁVNÍ ÚPRAVY S ÚMLUVOU O KYBERNETICKÉ KRIMINALITĚ

Tomáš Gřivna

Úmluva Rady Evropy o kybernetické kriminalitě (CETS No.: 185, 23. 11. 2001) je jako jediná komplexně zaměřena na společensky nebezpečné jevy v kybernetickém prostoru a související otázky. Úmluva požaduje po členských státech, aby trestně postihovaly jednání, které sama definuje (např. neoprávněný přístup do počítačového systému; zásah do dat, „odposlech dat“, trestné činy související s dětskou pornografií). V Úmluvě nalezneme i požadavky na přijetí opatření procesního charakteru, jakož i zásady mezinárodní spolupráce. Česká republika je signatářem Úmluvy od 9. 2. 2005. Cílem přednášky je seznámit účastníky s vybranými ustanoveními Úmluvy a s tím, nakolik je česká právní úprava s nimi

souladná. Pozornost bude věnována zejména jednáním, která mají být kriminalizována, a pravomocem orgánů činných v trestním řízení především ve vztahu k třetím osobám (např. poskytovatelům služeb).

JUDr. Bc. Tomáš Gřivna, Ph.D. – TOMAS.GRIVNA@SEZNAM.CZ

PF UK v Praze

Aabsolvoval Policejní akademii České republiky a Právnickou fakultu Univerzity Karlovy v Praze. V roce 2003 dokončil rigorózní řízení (JUDr.), v roce 2005 doktorské studium (Ph.D.). V současnosti je odborným asistentem a tajemníkem katedry trestního práva Právnické fakulty Univerzity Karlovy v Praze. Vykonává též advokátní praxi se zaměřením na obhajobu v trestních věcech. Pravidelně publikuje v odborných právnických časopisech. Je spoluautorem učebnic trestního práva hmotného a procesního. Za monografii „Soukromá žaloba v trestním řízení“ byl oceněn Bolzanovou cenou. V roce 2007 byl ministrem spravedlnosti jmenován členem rekodifikační komise pro trestní právo procesní.

HIERARCHICKÁ STRUKTURA PRACOVIŠŤ CSIRT A JEJÍ FUNKCE

Andrea Kropáčová, Robert Malý

Součástí preventivní a aktivní ochrany počítačů a počítačových sítí je důsledné a efektivní řešení bezpečnostních incidentů včetně odstraňování jejich příčin a následků. Proto je nutné, aby na možnost narušení bezpečnosti sítě a počítačů byli jejich správci a uživatelé připraveni a měli k dispozici funkční struktury, efektivní postupy, pravidla a technické prostředky vedoucí k co nejrychlejšímu odstranění problémů při minimalizaci škod.

Problematiku řešení bezpečnostních incidentů řeší obecně tzv. CSIRT týmy – Computer Security Incident Response Team (případně CERT – Computer Emergency Response Team). Existence alespoň jednoho oficiálního CSIRT týmu je žádoucí v každé provozované síti, obzvláště pak v těch velkých (univerzitních, v sítích bank, v sítích ISP). CSIRT dané sítě obecně představuje záchytný bod, na který je možné se obrátit se zjištěným bezpečnostním problémem. Dohromady tvoří CSIRT týmy funkční infrastrukturu, která v prostředí Internetu umožňuje rychle a efektivně zasáhnout v případě závažného bezpečnostního incidentu, případně varovat ostatní potenciální oběti útoku.

Andrea Kropáčová – ANDREA.KROPACOVA@CESNET.CZ

CESNET, z. s. p. o.

Pracovala v letech 1997–1999 pro VC ČVUT, kde zodpovídala za administraci webových serverů a vývoj webových aplikací. Od roku 1998 je zaměstnancem sdružení CESNET, z. s. p. o. Ve sdružení začínala na pozici administrátora síťových služeb a aplikací, v posledních letech se specializuje na problematiku

bezpečnosti sítí a služeb a to především v oblasti formování a řízení CSIRT týmů.

FOREZNÍ ANALYZÁTOR PRO OPERATIVNÍ ANALÝZU
Róbert Lórencz, Tomáš Zahradnický, Jiří Buček

V rámci projektu „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“ je na Katedře počítačů FEL ČVUT v Praze vyvíjen forenzní analyzátor osobních počítačů. Vyvíjený forenzní analyzátor je určen zejména pro nejnižší úroveň nasazení – operativní analýzu – při odhalování počítačové kriminality vyškolenými vyšetřovateli. Při vývoji forenzního analyzátoru je kladen důraz na jeho jednoduchost, přenositelnost a otevřenost kódu. Cílem tohoto příspěvku je ve zkratce představit východiska, požadavky plynoucí z praxe a navržené technické řešení forenzního kitu.

Róbert Lórencz – LORENCZ@FEL.CVUT.CZ

Katedra počítačů, FEL ČVUT v Praze

Autor je přednášejícím předmětů zabývajících se bezpečností počítačových systémů, architektur počítačových systémů a aplikované numerické matematiky. Zabývá se výzkumem v oblasti hardwarových akcelerátorů pro kryptografické systémy a bezchybovými numerickými algoritmy. Další oblast jeho výzkumu se týká vývoje forenzních analyzátorů pro počítačové systémy. Vystudoval Elektrotechnickou fakultu na ČVUT v Praze, doktorát získal na Fyzikálním ústavu SAV v Bratislavě a habilitován byl na FEL ČVUT v Praze.

SKENOVÁNÍ OTEVŘENÝCH ZDROJŮ

Leo Galamboš

V rámci příspěvku bude věnována pozornost několika oblastem s přímým vztahem ke skenování otevřených zdrojů. Mezi ně patří základní architektura skeneru, reakce na různé anomálie (např. na chybové stavy serverů a sítě), správa báze URL adres, techniky pro vyhýbání se „pastem na roboty“ a jednoduché heuristiky pro eliminaci duplicitního skenování.

Leo Galamboš – LEO.GALAMBOS@MFF.CUNI.CZ

MFF UK v Praze

Je autorem vyhledávacího systému EGOTHOR, který je vyvíjen od roku 1999. V současnosti působí jako odborný asistent na Matematicko-fyzikální fakultě UK v Praze.

ANALÝZA DAT Z OTEVŘENÝCH ZDROJŮ

Iveta Mrázová

Podstata úspěšné analýzy dat z otevřených zdrojů spočívá v efektivním zpracování velkého množství údajů, a to pokud možno bez výraznějších zásahů uživatele. Cílem takové analýzy je najít vzájemné vztahy mezi zpracovávanými daty a tuto informaci smysluplně interpretovat. Výsledky získané během analýzy ovšem může být poměrně obtížné vhodně vizualizovat. Významným požadavkem bývá také snadná použitelnost vyvinutých metod i pro pozměněné požadavky, např. nová data.

Data běžně dostupná z otevřených zdrojů mají typicky různé vlastnosti a různý formát. Velká část informací je uložena v textové podobě. S rozvojem výpočetní kapacity běžně dostupných informačních technologií však dochází i k masivnímu rozšiřování netextových informací, např. sdílení obrázků, akustických záznamů, videí apod. K úlohám řešeným v rámci analýzy dat z otevřených zdrojů tedy patří zejména klasifikace, shlukování, analýza (sociálních) vazeb a vyhledávání (např. v textech).

Algoritmy vhodné pro automatickou analýzu dat z otevřených zdrojů obvykle patří k výpočetně náročnějším a volba odpovídající techniky závisí mj. i na charakteru řešené úlohy a použitých dat, která navíc mohou být zatížena vysokou mírou šumu. V příspěvku představíme některé z technik použitelných pro analýzu dat z otevřených zdrojů – mezi jinými klastrovací metody, klasifikační techniky založené na principu k-NNR, Bayesovské klasifikátory, rozhodovací stromy a umělé neuronové sítě.

Iveta Mrázová – IVETA.MRAZOVA@MFF.CUNI.CZ*MFF UK v Praze*

Je absolventkou oboru Informatika na Univerzitě Friedricha Schillera v Jeně, Německo (1989). Disertační práci v oboru Výpočetní technika obhájila v roce 1997 v Ústavu informatiky Akademie věd České republiky. Habilitační práci v oboru Teoretická informatika obhájila v roce 2007 na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze. Na MFF UK začala působit v roce 1992, od roku 2008 zde pracuje jako docentka na Katedře teoretické informatiky a matematické logiky. V současné době se zabývá problematikou umělých neuronových sítí a dobývání znalostí.

Iveta Mrázová je autorkou nebo spoluautorkou více než 40 odborných publikací. Příspěvky Ivety Mrázové byly dvakrát oceněny cenou za nejlepší článek na konferenci ANNIE, St. Louis, USA (2000, 2007). V roce 1996 získala Výroční cenu Bolzanovy nadace, v roce 2001 jí byla Jednotou českých matematiků a fyziků a Českou společností pro mechaniku udělena Cena Profesora Babušky. V letech 2002–2003 byla stipendistkou Fulbrightovy komise.

NĚKTERÉ MÉNĚ TRADIČNÍ METODY DETEKCE
ŠKODLIVÝCH AKTIVIT V IP SÍTÍCH

Petr Břehovský

Spolehlivá detekce útoků a škodlivých aktivit v sítích, se stává stále komplexnějším problémem. Vyladění IDS tak, aby poskytovaly smysluplné (oproštěné od falešných poplachů) informace je jednou z nejpracnějších činností při nasazování těchto systémů.

Existují však mnohem jednodušší metody detekce útoků, které sice nemohou IDS zcela nahradit, ale mohou výrazně pomoci jak při identifikaci skutečných útoků, tak i při analýze falešných poplachů.

Příspěvek bude věnován popisu levných a snadno dostupných technologií detekce útoků založených na vizuálních metodách analýzy paketů (The Spinning Cube of Potential Doom), dedikovaných detekčních sítích (Darknet, HoneyNet) a specializovaných filtrech paketů.

Ing. Petr Břehovský – PETR.BREHOVSKY@O2.COM

Telefónica O2 Czech Republic, a. s.

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.

ASTRONOMICKÁ FOTOGRAFIE

Libor Šmíd

Rychlý rozvoj techniky umožnil v posledních letech pořizovat i v amatérských podmínkách kvalitní fotografie hvězdné oblohy. Současně je však stále větší problém najít opravdu kvalitní oblohu, která by nebyla přесvícena umělým osvětlením. Přednáška přibližuje některé specifické postupy astronomické fotografie, požadavky na techniku a nejčastější problémy. Zmíněny budou zejména možnosti současných digitálních fotoaparátů a problematika zpracování astronomických fotografií. Cílem přednášky je ukázat, že i snadno dostupnou technikou lze pořídit hezké snímky hvězdné oblohy.

Libor Šmíd – SMID@CIV.ZCU.CZ

Centrum informatizace výpočetní techniky, Západočeská univerzita v Plzni

Absolvent Vysoké školy strojní a elektrotechnické v Plzni, obor technická kybernetika. Nyní pracuje jako technik počítače na Západočeské univerzitě v Plzni. Ve

volném čase se věnuje astronomii, zejména astronomické fotografii, pozorování zákrytů hvězd planetkami a stavbě přístrojů.

UNIFIED COMMUNICATIONS

Jaroslav Martan

V přednášce se krátce podíváme na historii VoIP a pak na některé nové technologie, které mohou vést k zajímavým změnám a funkcím. Jmenovitě to bude ENUM, integrace s mobilními telefony nebo vývoj aplikací.

Ing. Jaroslav Martan – JMARTAN@CISCO.COM

Cisco Systems

Od roku 1999 pracuje v českém zastoupení společnosti Cisco Systems, momentálně na pozici Consulting Systems Engineer. Věnuje se především Unified Communications technologiím. Předchozí zaměstnáni: ICZ a.s., Alef Nula, EUnet B.V., Expert & Partner engineering. Absolvent ČVUT FEL (1992).

LMR – LAND MOBILE RADIO

Jiří Novák

LMR je způsob, jak efektivně spojit několik běžných radiostanic pomocí VoIP sítě.

Spojování více rádií do jednoho systému je obecně problematika velkých areálů (letišť, nádraží) nebo problematika pokrytí velkých území (záchranné složky, řízení letového provozu).

V LMR se hlas přenáší multicastem. Tento přenos je efektivní, ale má i svá úskalí. Proto bude část přednášky věnována vysvětlení šíření multicastu v lokálních a WAN sítích.

Díky tomu, že jsou rádia připojena do VoIP sítě, je možné s rádií komunikovat z běžných telefonů i IP telefonů a naopak. Také je možné do radiové sítě přidat aplikace vyvinuté pro VoIP technologie a prostředí.

Jiří Novák – J.NOVAK@NETSYSTEM.CZ

NET-SYSTEM, Liberec

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

SIP EXPRESS ROUTER – USE CASES FOR VOIP

Jiří Kuthan

Technologie VoIP dosahuje masového rozšíření po celém světě. Jednou z klíčových komponent je signalizační server, tzv. SIP proxy server. V tomto příspěvku se zabýváme populárním server „SIP Express Router“, způsoby použití a obtížemi, které nasazení VoIP provázejí: propojování se sítěmi PSTN, QoS, NATs, atd.

Jiří Kuthan – JIRI@IPTEL.ORG*iptelorg GmbH*

Je šéfem vývoje firmy iptelorg GmbH v Berlíně a v Praze, která je známá především svým open-source SIP proxy serverem známým jako „SIP Express Router“. Před založením firmy iptelorg se Jiří Kuthan věnoval u výzkumného ústavu Fraunhofer Fokus v Berlíně protokolům pro VoIP, bezpečnosti Internetových služeb a standardizaci v IETF. Softwarové inženýrství vystudoval na univerzitě v Salcburku, Rakousko.

PRAKTICKÉ ZKUŠENOSTI S IMPLEMENTACÍ VOIP V SÍTI O2

Petr Poupě

Příspěvek se bude zabývat nasazováním VoIP/IMS (IP Multimedia Subsystem) řešení v síti Telefónica O2 Czech Republic, a. s., se zaměřením na nesnáze a problémy s tím související.

Petr Poupě – PETR.POUPE@O2.COM*Telefónica O2 Czech Republic, a. s.*

Ing. Petr Poupě (*1968) vystudoval katedru Telekomunikační techniky fakulty elektrotechnické ČVUT v Praze. Po studiu nastoupil jako technický pracovník v oblasti provozu veřejných ústředěn E10, po třech letech přestoupil do odboru rozvoje a testování digitálních telefonních ústředěn EWSD. Od roku 2001 se zabývá rozvojem, implementací a testy platform NGN/IMS (Siemens Surpass, IMS Ericsson).

IMPLEMENTACE IP TELEFONIE NA ZÁPADOČESKÉ UNIVERZITĚ V PLZNI

Michal Petrovič

Přednáška se bude zabývat implementací SIP IP telefonie na Západočeské univerzitě v Plzni pomocí svobodného software. Obsahem bude i konvergence IP telefonie do bezdrátového připojení (telefonování pomocí tzv. hybridního IP telefonu). Další tematickou částí bude zvýšení dostupnosti poskytované služby IP telefonie při případném výpadku a autoregistrační systém pro snadnější nasazení většího množství IP telefonů.

CO UMÍ SOUBOROVÉ SYSTÉMY

Jan Kasprzak

Souborový systém je jednou ze základních komponent UNIXového počítače. V této přednášce shrneme historii souborových systémů v UNIXu i Linuxu, představíme si souborové systémy, které se reálně používají v současnosti (ext3, XFS, JFS a ReiserFS), popíšeme pokročilé a nestandardní vlastnosti některých souborových systémů, a ukážeme, kam směřuje vývoj, včetně představení projektů, které se vize budoucnosti snaží realizovat: Reiser4, ext4, CRFS/BTRFS, POHMELFS a některé další.

Jan Kasprzak – KAS@FI.MUNI.CZ*Fakulta informatiky Masarykovy univerzity v Brně*

Je absolventem Fakulty informatiky Masarykovy univerzity. V současné době pracuje na Fakultě informatiky MU, kde se podílí na vývoji a správě Informačního systému MU a na správě fakultní sítě. Mezi jeho odborné zájmy patří nasazování Linuxu a spotřebního hardware namísto drahých proprietárních systémů. Linux na svých pracovních stanicích používá přibližně od verze 0.99.11. Za účelem mentální relaxace studuje ve volných chvílích Japonštinu.

STABILITA SOUBOROVÝCH SYSTÉMŮ

Michal Krátký

Jakým způsobem vznikají v souborovém systému nekonzistence? Jak na ně operační systém zareaguje a co v téhle věci může podniknout systémový administrátor? Před čím nás ochrání žurnálovaný filesystém a před čím ne? Tyto otázky si autor položil poté, co k tomu byl okolnostmi dotlačen. Odpovědi jsou předmětem tohoto příspěvku. Konkrétnější informace se budou týkat filesystémů ext2/ext3, xfs a VxFS.

Michal Krátký – KRATKY@FZU.CZ*Fyzikální ústav AV ČR, v. v. i.*

Autor obhájil kandidátskou dizertaci z chemického inženýrství a potom se od roku 1983 živil jako programátor a administrátor unixových a linuxových serverů. V současné době je vedoucím úseku IT Fyzikálního ústavu AV ČR.

VOLUME MANAGEMENT A LINUX

Milan Brož

Nasazení Linuxu v obrovské škále systémů přináší různorodé požadavky na správu diskového prostoru. V této části si popíšeme jaké nástroje poskytuje Linux pro práci s blokovými zařízeními, tedy vrstvy pod vlastním filesystémem. Co je to kernel device-mapper, jak se liší od MD (multiple device). Jaké aplikace a nástroje jej využívají přímo a jaká je výhoda takovéto vrstvené architektury (použití od desktopu až po správu diskového prostoru pro virtuální servery). Krátce se zastavíme u dm-cryptu/LUKS a rozdílů od šifrovaného filesystému. Další část je o LVM2 – co poskytuje z uživatelského pohledu (správa oddílů, redundance, online snímky a realokace prostoru, změna velikosti). Popis logiky ovládání, řešení problémů například při výpadku části diskového prostoru a také kde jsou slabá místa současné implementace. Krátce se také zmíníme o použití LVM2 v clusterovém prostředí.

Milan Brož – MBROZ@REDHAT.COM

Red Hat Czech, s. r. o.

Absolvent Fakulty elektrotechniky a informatiky VUT v Brně, obor výpočetní technika a informatika. Pracuje jako vývojář linuxového kernelu (zejména core device mapperu a v poslední době vývoji dm-cryptu) a LVM2 nástrojů.

ZFS – THE LAST WORD IN FILESYSTEMS

Vineeth Pillai

Zetabyte Filesystem, A new object based 128 bit filesystem from Open Solaris and ported to many well known Operating Systems. Designed from scratch, it is a fundamentally new approach to data management blowing away all the obsolete assumptions of conventional Filesystem. ZFS provides simple administration, transactional semantics, end-to-end data integrity and immense scalability all bundled with heights of usability. This presentation aims to dwell deep into ZFS and let the audience feel the power of this innovation.

Vineeth Pillai – VINEETH.PILLAI@SUN.COM

Sun Microsystems

Author is a Sustaining Engineer at SUN Microsystems Prague. Mainly working on the filesystems space in Solaris and an Open Source enthusiast. Author is Indian and educational background is from India, where he did a bachelors on Information technology. Author has done many presentations across the globe regarding Open Solaris and related Technologies.

SAM-QFS

Jan Kopřiva

SAM-QFS je produkt firmy Sun Microsystems s nedávno otevřeným zdrojovým kódem. Jedná se o kombinované řešení distribuovaného souborového systému QFS a unikátního archivovačního systému SAM – Storage Archive Manager.

QFS, díky svým vlastnostem jako je spojování diskových oddílů do větších logických celků, oddělení metadat a dat, variabilní délky datových bloků a rychlostí přístupu na disk, kdy dosahuje tzv. „raw disk speed“, má široké použití v praxi. Mimo jiné se hojně používá pro streamovací aplikace, ale můžeme je nalézt i v HPC segmentu, kde slouží jako úložiště pro petabyty dat.

SAM představuje transparentní rozšíření pro QFS, které minimalizuje nechtěně známé zálohovací a obnovovací okno (backup and recovery window). Jeho nasazením lze postavit celou hierarchii datových úložišť s použitím dalších disků, pásek a optických médií. Zálohovat lze také po síti do vzdálených míst (remote storage sites). Samotné zálohování pak probíhá naprosto transparentně, kdy soubory jsou archivovány na pozadí a zpětně získávány při nejbližším dalším přístupu.

Jan Kopřiva – JAN.KOPRIVA@SUN.COM

Sun Microsystems

Jan Kopřiva vystudoval FEL CVUT, obor Vypočetní technika. V současnosti pracuje v Sun Microsystems jako SAM-QFS Sustaining Engineer.

IMPLEMENTATION OF THE FILE SYSTEM LAYER IN HELENOS

Jakub Jermář

HelenOS is an open source microkernel based operating system originally developed by students and staff of the Faculty of Mathematics and Physics, Charles University in Prague. As part of its on-going development, a new file system layer has been added to HelenOS recently. This talk will introduce HelenOS itself and focus on the new file system layer and its implementation in the context of a microkernel.

Jakub Jermář – JAKUB@JERMAR.EU

Received a master's degree in computer science from the Faculty of Mathematics and Physics, Charles University in Prague. Jakub is the founding member of the HelenOS project, in which he has been involved since 2001, and since 2006 works for Sun Microsystems in Solaris kernel sustaining.

Předběžné oznámení o konání konference a žádost o příspěvky

XXXIII. konference Českého sdružení uživatelů otevřených systémů EurOpen.CZ

se bude konat od neděle 5. října 2008 do středy 8. října 2008, Lesní chata Kořenov v Jizerských horách (<http://www.hotel-lesnichata.cz>)



Zaměření

Konference se soustředí tři tematické okruhy: nové webové technologie, zpracování textů, skriptovací jazyky a praktické zkušenosti z vývoje aplikací. Každému z tematických okruhů bude věnován jedna celodenní či polodenní sekce. Sekce či přednášky s jiným tematickým zaměřením lze zařadit, pokud budou nabídnuty programovému výboru konference a jím schváleny.

Nabídka a výběr příspěvků a oznámení o přijetí

Stručné anotace příspěvků společně s názvem příspěvku a stručným profesním životopisem autora lze zasílat průběžně, nejpozději do 17. 8. 2008 e-mailem na adresu europen@europen.cz nebo přímo členům programového výboru. Na webové

stránce <http://www.euopen.cz> je možné najít anotace a profily autorů z předchozích konferencí. Výběr příspěvků provede programový výbor konference. O přijetí příspěvku budou autoři informováni po projednání programovým výborem obratem, nejpozději do 22. 8. 2008.

Příspěvek do sborníku

Příspěvky do sborníku je třeba zaslat e-mailem nejpozději do 15. 9. 2008. Příspěvky neprocházejí redakční ani jazykovou úpravou. Sborník je zařazen do nomenklatury ISBN. Autorům příspěvků náleží autorský honorář obvyklý na konferencích sdružení EurOpen.CZ.

Program a registrační formulář

Program konference s pozvánkou bude k dispozici do 31. 8. 2008 v papírové a elektronické formě. Dotazy či žádosti o podrobnější informace je možné zaslat emailem na adresu euopen@euopen.cz. Na tuto adresu je možné zaslat i žádost o zařazení do seznamu adresátů tištěných pozvánek.

Práce v sekcích

Je nedílnou součástí konference. Umožňuje neformální sblížení zájemců o společnou problematiku. Je plánována na úterní odpoledne, náměty budou zařazeny do pozvánky.

Tutoriály

Pro zajištění co nejzajímavější nabídky tutoriálů hledá EurOpen.CZ neustále nové náměty. S námětem či nabídkou je možné se obrátit na programový výbor nebo e-mailem na adresu euopen@euopen.cz.

Pozvánka na XXXII. konferenci EurOpen.CZ, 19.–22. května 2008

© EurOpen.CZ, Univerzitní 8, 306 14 Plzeň

Editor: Vladimír Rudolf

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

Tisk: TYPOS, Tiskařské závody, a. s.
Podnikatelská 1 160/14, Plzeň