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

39. konference

klášter Želiv
2.–5. října 2011

Slovo úvodem

Podzimní konference

Bezpečnostně laděné přednášky se objevují na konferenci Europen natolik často, že jsme jim letos (po dohodě s Dolfem z loňska a se vzpomínkami vždy na další rok $n - 1$) vyhradili celou vlastní podzimní část. Připravili jsme pro vás pestrou směs příspěvků, které pokryjí problematiku počínaje síťovou bezpečností v rozsáhlých infrastrukturách přes aktuální stav dospívajícího puberťáka jménem PKI až po webovou bezpečnost a využití pokročilých kryptografických aplikací. Jako ochutnávku vám zde představíme část z nich, pro plné menu pokračujte ve čtení i po úvodníku.

Čipové karty jsou na konferenci Europen probírány často, dokonce byl už i tutoriál na jejich používání, tuším v roce 2004. Vývoj v oblasti ale přinesl rozšíření snadno programovatelných karet a tak lze dnes psát vlastní aplikace běžící přímo v bezpečném prostředí čipové karty ve vysokoúrovňových jazycích jako Java nebo C#. Pro nedělní tutoriál jsme zajistili pro každého účastníka moderní programovatelnou čipovou kartu (kterou si pak každý odnese) s platformou JavaCard a pokusíme se ukázat, že psaní webových aplikací se od čipovek zase tolik neliší. Navíc od roku 2004 přibylo i užitečných aplikací, které umí čipovky používat. I v případě, že nejste zrovna fanda do programování, tak vás může potěšit praktická část, po které si odnesete kartu s vašimi privátními klíči použitelnou třeba pro program PGP/GPG nebo TrueCrypt.

Pondělní program bude naplněn příspěvky týkajícími se rozsáhlých počítačových sítí. Začneme přednáškou o praktické realizaci formátů pro digitální podpis od Libora Dostálka. Zkušenosti při dohledování rozsáhlých infrastruktur Masarykovy univerzity s více než tisícem stanic, desítkami serverů a desítkami tisíc účtů představí Pavel Tuček. Často opomíjenou problematiku útoku dočasných vnitřních uživatelů ve firemní síti ve zvané přednášce probere Ondra Ševeček se zaměřením na nástroje firmy Microsoft. Aktuální stav IPsecu představí Pavel Šimerda se zaměřením na jeho proměny od původně zamýšleného prostředí IPv6. Těsně před večeří se dozvíme zákulisní informace o principech i aktuálním stavu nástrojů pro diskového šifrování od Milan Brože, hlavního vývojáře dm-cryptu.

Navečer nás čeká mírně sžíravý vhled od Luďka Smolíka do budoucnosti někdy oslavované, někdy proklínané infrastruktury pro správu a distribuci veřejnými klíči asymetrické kryptografie – už délka názvu napovídá, že situace není jednoduchá, přestože se anglická zkratka PKI tváří, že všechny problémy jsou již překonány.

Úterní program zahájí zvaná přednáška o slibech a realitě elektronických pasů od Zdenka Říhy, který pro Evropskou komisi dlouhodobě pracoval na jejich testování a uvádění do praxe na evropské úrovni. Úzce souvisejícím tématem je správa revokovaných certifikátů, byť nahlížena z pohledu elektronického plateb-

ního systému Vítkem Bukačem. Před prací v sekcích nás čeká zvaná přednáška na téma návrhu decentralizovaných a těžko odhalitelných červů od Norberta Szetei, který se proslavil mimo jiné implementací nástroje pro cracking karet Mifare Classic.

Středeční část uvede Jaromír Dobiáš představením práce týkající se možnosti deanonymizace uživatelů při používání webových technologií, která úzce souvisí s jeho působením na technické universitě v Drážďanech. Svým neopakovatelným stylem zpracuje častý účastník Europenu Radoslav „Bodík“ Bodó zkušenosti z hrátek na bezpečnostní mobilizaci při obraně evropské gridové architektury EGI. A o závěr se postará zvaná přednáška na téma bezpečnosti a vývoje RIA aplikací od Juraje Michálka, všestranně nadaného komunikátora a „rozjížděče“ softwarových firem.

Práce v sekcích je na konferencích EurOpen oblíbená a málokdy dostane nějakou horší známku v hodnocení. Její náplň je ponechána především na Vás, účastníky. Abyste však moc netápali, připravujeme alespoň jednu organizovanou akci a tou bude podvečerní prohlídka kláštera Želiv.

Zamyšlení na závěr...

Bezpečnostních aplikací máme k dispozici téměř nepřeberné množství, často se ale zapomíná na jejich použitelnost pro méně technicky zdatné až nezdatné osoby. Kdy jste naposledy zkoušeli rozjet a vysvětlit šifrování poznámek (s PINy) na mobilu pro někoho z rodiny? Kolik vašich kamarádů používá šifrování disku? Lze si uchovat aspoň nějakou bezpečnost na počítači, který byl napaden určitým malwarem? Máte již splněno políčko „Dobrý čin: Zvýším počítačovou bezpečnost náhodného kolemjdoucího“ ve svém Modrém životě pro tento den? Nejen tyhle, ale i další otázky na vás čekají během denních, večerních i nočních přestávek podzimního bezpečnostního Europenu.

Za programový výbor se těší

Petr Švenda.

Programový výbor

Vašek Matyáš (předseda, Masarykova univerzita)
Marek Kumpošt (Masarykova univerzita, Trusted Network Solutions, a. s.)
Marián Novotný (ESET, spol. s r. o.)
Josef Pojsl (Trusted Network Solutions, a. s.)
Zdeněk Říha (Masarykova univerzita) Roman Štěpánek (SODATSW, spol. s r. o.)
Petr Švenda (Masarykova univerzita)

Program

Neděle 2. 10. 2011

13.00	Tutoriál: Programování kryptografických čipových karet na platformě JavaCard a jejich praktické použití v aplikacích	*Petr Švenda*

Pondělí 3. 10. 2011

9.00	Oficiální zahájení	*Vashek Matyáš*
9.05	Formáty pro zaručený elektronický podpis	*Libor Dostálek*
9.55	Sledování rozsáhlé počítačové infrastruktury	*Pavel Tuček*
10.45	Přestávka	
11.05	Zvaná přednáška: Uzamčená firemní síť	*Ondřej Ševeček*
12.40	Oběd	
14.00	Zabezpečení bezdrátových sítí založených na protokolu IEEE 802.11 v aplikaci rozsáhlých distribučních sítí	*Jan Nagy*
14.50	IPsec na Linuxu	*Pavel Šimerda*
15.40	Přestávka	
16.10	Šifrování disků (nejen) v Linuxu	*Milan Brož*
18.00	Večeře	
19.30	Zvaná přednáška: PKI, sen nebo noční můra?	*Luděk Smolík*

Úterý 4. 10. 2011

9.00	Zvaná přednáška: Elektronické pasy v praxi	*Zdeněk Říha*
10.40	Přestávka	
11.00	Správa revokovaných certifikátů v elektronickém platebním systému	*Vít Bukač*
11.50	Zvaná přednáška: Moderné spôsoby návrhu kompletne distribuovaných, decentralizovaných a ťažko odhaliteľných červov	*Norbert Szetei*
13.00	Oběd	
14.00	Práce v sekcích	
19.00	Večeře, diskuse, chat, jabber, práce v sektech, valná hromada	

Středa 5. 10. 2011

9.00	Sledování uživatelů prostřednictvím webových technologií	*Jaromír Dobiáš*
9.50	SSC5 EGI Security challenge: Lehce na cvičišti...	*Radoslav Bodó*
10.40	Přestávka	
11.00	Zvaná přednáška: Bezpečnosť a vývoj RIA (Rich Internet Application)	*Juraj Michálek*
12.40	Závěr	*Vashek Matyáš*
13.00	Oběd	

Konferenční poplatky

Vložné		
Platba	Tutoriál	Konference
Členové		
do 18. 9. 2011	890	2 200
po 18. 9. 2011	990	2 450
Nečlenové		
do 18. 9. 2011	990	2 500
po 18. 9. 2011	1 090	2 750
Ubytování a stravování		
od neděle 2. 10. 2011	1 350	od nedělní večeře do středečního oběda, 3 noclehy
od pondělí 3. 10. 2011	970	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 se snídaní 310 Kč na den, oběd 70 Kč, večeře 70 Kč).

Kapacita hotelu je zhruba 80 osob.

Kdy	Tutoriál se uskuteční v neděli 2. 10. 2011 od 13.00 hodin
	Konference začíná v pondělí 3. 10. 2011 v 9.00 hodin a končí ve středu 5. 10. 2011 cca ve 13.00 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	klášter Želiv http://zeliv.eu
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	29. 9. 2011 nebo při naplnění ubytovací kapacity.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 80.
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

Tutoriál: Programování kryptografických čipových karet na platformě JavaCard a jejich praktické použití v aplikacích

Petr Švenda

V rámci tutoriálu každý účastník obdrží moderní programovatelnou multiaplikační kryptografickou čipovou kartu (Gemalto TOP IM GX4 + Mifare Classic 1k) s platformou JavaCard (podporované algoritmy 3DES, AES, RSA 2 048bit, ...) a s pomocí předchystaného vývojového prostředí zvládne proces vývoje elementárního appletu, jeho nahrání na kartu a tvorbu jednoduché aplikace, která s kartou na straně PC bude komunikovat. Ve druhé části si na kartu nahrajeme několik existujících appletů využitelných pro uložení privátního podepisovacího klíče na čipovou kartu pro program PGP/GPG, vytvoření karty nabízející úložiště dle standardu PKCS#11 nebo PKCS#15 (použitelné pro širokou řadu aplikací) nebo aplikaci umožňující tvorbu klonu elektronického pasu. Probrány budou jak vývojové, tak i bezpečnostní aspekty používání programovatelných čipových karet.

Petr Švenda – svenda@fi.muni.cz
Fakulta informatiky, Masarykova Univerzita v Brně
http://www.fi.muni.cz/∼xsvenda/
Petr Švenda získal titul Ph.D. na Fakultě Informatiky Masarykovy Univerzity a nyní se zde věnuje se výzkumu v oblasti návrhu protokolů pro bezdrátové senzorové sítě, ochraně informačního soukromí a se speciálním zájmem a nadšením vývoji bezpečnostních aplikací pro kryptografické čipové karty včetně testování jejich odolnosti vůči útokům postraními kanály. Podílel se na konzultacích, vývoji i auditech pro akademické, státní i průmyslové organizace v ČR i zahraničí.

Formáty pro zaručený elektronický podpis

Libor Dostálek

Již více než deset platí evropská směrnice o elektronickém podpisu i český zákon o elektronickém podpisu. ETSI vytvořilo sadu standardů pro formáty elektronických podpisů (CAdES, XAdES a PAdES). Vznikají nám elektronické dokumenty opatřené elektronickými podpisy. Situace se zdá jasná a jednoduchá. Realita je ale jiná. Formáty ETSI se příliš nepoužívají a konec konců samotný elektronický podpis je pro drtivou většinu populace nepřátelský. Je tedy na čase si po deseti letech nalít čistého vína a vrátit se na počátek.

Přednáška se mj. bude zabývat:

- Otázkou archivace dokumentů opatřených dnešními elektronickými podpisy.

- Otázkou proč banky a jiné instituce stále hledají jednodušší alternativy k dnešním elektronickým podpisům.
- Jaké alternativy se objevují (biometrický podpis, SMS podpis,?).
- Otázkou zda-li tyto alternativy mohou nahradit elektronický podpis.

Libor Dostálek – dostalek@prf.jcu.cz
Přírodovědecká fakulta Jihočeské univerzity
Pracuje ve společnosti Atos. Je vedoucím Ústavu aplikované informatiky na Přírodovědecké fakultě Jihočeské univerzity. Je autorem Velkého průvodce PKI a technologii elektronického podpisu. Na MFF UK přednáší kurz Členění kryptografických standardů.

Sledování rozsáhlé počítačové infrastruktury

Pavel Tuček

S rostoucím počtem počítačů v síti rostou i možnosti a rozsah útoků. Ať už se jedná o útok v rámci lokální sítě nebo o útok do sítě cizí, důsledky jsou vždy nepříjemné. Zde je třeba si uvědomit, že sledování počítačů není spásné samo o sobě. Abychom získali komplexní informaci o stavu sítě, či jinak řečeno infrastruktury, je třeba sledovat i související prvky jako jsou routery, síťové přepínače, servery a služby, které s chodem celé infrastruktury souvisí. Všechny zaznamenané události je potřeba analyzovat a dát do správných souvislostí. Teprve tehdy získáme informaci o stavu infrastruktury. Tento příspěvek pojednává o motivaci pro vývoj nového monitorovacího systému, jeho komponentách a vytyčených cílech. Vývoj probíhá v rámci na Ústavu výpočetní techniky MU v rámci Oddělení pro vývoj systémových služeb, které má aktuálně ve správě více než 1 200 počítačů a 50 serverů.

Pavel Tuček – tucek@ics.muni.cz
Masarykova univerzita
Je absolventem a v současnosti i PhD studentem na Fakultě informatiky Masarykovy univerzity, kde se věnuje bezpečnosti IT v laboratoři Bezpečnosti a aplikované kryptografie LaBAK. Od roku 2005 také pracuje na Ústavu výpočetní techniky MU v Oddělení vývoje systémových služeb.

Uzamčená firemní síť

Ondřej Ševeček

Podnikovým sítím hrozí mnoho nebezpečí od vnějších útočníků a všichni jsou si těchto hrozeb jako jsou viry, spam a hackerské útoky, velmi dobře vědomi. To, co si uvědomuje jen málo firemních prostředí je hrozba zevnitř. Mnohem větší riziko představují zaměstnanci, nebo externisté, dodavatelé, brigádníci, nebo různí servisní pracovníci a údržbáři. Mají fyzický přístup k počítačovému a síťovému vybavení a mohou mnohem snáze získat přístup k datům společnosti. Přednáška se snaží přiblížit nejpalčivější problémy stávajících sítí na platformě Microsoft a nabídnout jejich řešení za pomoci bezpečnostních technologií, které jsou od výrobce k dispozici.

Ing. Ondřej Ševeček – ondrej@sevecek.com
nezávislý konzultant
Je nezávislým konzultantem specializujícím se na identity management a bezpečnost na platformě Active Directory společnosti Microsoft. Pravidelně přednáší a je autorem mnoha článků na témata bezpečnosti a správy sítí postavených na operačních systémech Windows.

Zabezpečení bezdrátových sítí založených na protokolu IEEE 802.11 v aplikaci rozsáhlých distribučních sítí

Martin Zadina, Jan Nagy, Petr Hanáček

Bezdrátové sítě jsou dnes čím dál oblíbenější forma přístupu k Internetu. Jelikož je k přenosu dat použito rádiových vln, které se šíří s nižší intenzitou signálu i mimo požadovanou oblast pokrytí, neměla by být opomíjena otázka zabezpečení těchto sítí. V naší práci se zaměříme na několik existujících technologií určených pro bezdrátové lokální sítě, které mohou tvořit prvky sítí většího rozsahu (MAN, WAN). Zmíníme standardizované (IEEE 802.11, 802.16, HiperLAN/MAN), plně proprietární (Motorola Canopy) i kombinované technologie (Ubiquity Networks AirMAX, Mikrotik NStreme, Nv2) určené pro tento účel, jejich bezpečnostní mechanizmy a problematiku nasazení bezpečnostních protokolů sítí 802.11 v aplikaci sítí pevného bezdrátového přístupu.

Martin Zadina – izadina@fit.vutbr.cz
Fakulta informačních technologií, Vysoké učení technické v Brně
Vystudoval obor Počítačové systémy a sítě na FIT VUT Brno. V současné době je studentem doktorského studijního programu na Ústavu inteligentních systému tamtéž. Zabývá se především bezpečností, zejména v bezdrátových datových sítích.

Jan Nagy – inagy@fit.vutbr.cz
Fakulta informačních technologií, Vysoké učení technické v Brně
Vystudoval obor Počítačové systémy a sítě na FIT VUT Brno. V současné době je studentem doktorského studijního programu na Ústavu inteligentních systému tamtéž. Zabývá se především bezpečností, zejména v senzorových, bezdrátových a sociálních sítích.

Petr Hanáček – hanacek@fit.vutbr.cz
Fakulta informačních technologií, Vysoké učení technické v Brně
Docent na Fakultě informačních technologií VUT v Brně. Ve svém profesním životě se více jak deset let zajímá především o bezpečnost informačních systémů, analýzu rizik, aplikovanou kryptografie a elektronické platební systémy. Je také nezávislým poradcem v této oblasti.

IPsec na Linuxu

Pavel Šimerda

Většina návštěvníků EurOpen už přinejmenším slyšela, mnozí s ním mají i praktické zkušenosti. IPsec přišel do světa TCP/IP společně s IPv6, ale za dobu své existence se dokázal přizpůsobit i stávajícím podmínkám s IPv4 a různými NATy. IPsec se tak stal součástí síťových prvků a operačních systémů, kde konkuruje virtuálním privátním sítím i transportnímu zabezpečení.

Pavel Šimerda – pavlix@pavlix.net
nezávislý konzultant
Jeho specializací jsou počítačové sítě na bázi TCP/IP a umírněný propagátor nových technologií, otevřeného software i otevřeného hardware. Aktivně se věnuje inovaci sítí menších poskytovatelů připojení včetně nasazování IPv6, dynamického směrování a dalších věcí, které drží tyto ISP v technologickém předstihu. Mimo to programuje linuxová embedded zařízení a pořádá školení z oblasti TCP/IP, serverů a programování.

Šifrování disků (nejen) v Linuxu

Milan Brož

Představení systémů softwarového šifrování na úrovni disku (FDE – Full Disk encryption) a jejich srovnání, včetně speciálních vlastností a rozšíření (se zaměřením na dm-crypt/LUKS v Linuxu, ale neopomíjí ani loop-AES, Truecrypt a zástupce proprietárního systému z Windows – Bitlocker). Popíšeme si oblíbené útoky na tyto systémy (např. Cold Boot či použití hw keyloggeru) a specifické problémy, které mohou způsobit vlastnosti moderních disků (např. TRIM používaný v SSD). Nevyhneme se ani konceptu „skrytého disku“ (hidden volume),

využití TPM (Trusted Platform Module) a podobných rozšíření, které jsou často vnímány velmi kontroverzně.

Ing. Milan Brož – mbroz@redhat.com
Red Hat Czech, s. r. o.
Absolvent Fakulty elektrotechniky a informatiky VUT v Brně. Pracuje jako vývojář linuxového kernelu a nástrojů pro správu diskových oddílů (LVM). Posledních několik let je hlavním vývojářem dm-cryptu a cryptsetupu, včetně LUKS a ostatních rozšíření.

Elektronické pasy v praxi

Zdeněk Říha

Elektronické pasy byly zavedeny před přibližně 5 lety. Umožňují automatizaci přechodu hranic, přinášejí vyšší bezpečnost cestovního dokladu a některé problémy ochrany soukromí držitelů. Jak je to s reálným využíváním pasu dnes? Příspěvek nastíní očekávání spojená se zavedením elektronických pasů a jejich naplnění v praxi.

Zdeněk Říha – zriha@fi.muni.cz
Fakulta informatiky Masarykovy univerzity v Brně
Získal titul Ph.D na FI MU v Brně a titul Ing. na ESF MUv Brně. V letech 2005 až 2008 působil jako národní expert v Evropské komisi. V současné době pracuje jako odborný asistent na Fakultě informatiky Masarykovy univerzity.

Správa revokovaných certifikátů v elektronickém platebním systému

Roman Žilka, Vít Bukač

Příspěvek představí nejběžnější metody revokace certifikátů používaných v infrastruktuře PKI. Budou uvedeny základní charakteristiky každé metody a provedeme srovnání metod z hlediska funkčnosti a výkonu. Porovnání parametrů bude demonstrováno na několika základních scénářích použití, vypracovaných na základě požadavků a poznatků, které vzešly ze spolupráce mezi Laboratoří bezpečnosti a aplikované kryptografie a společností Y Soft na vývoji elektronického platebního systému.

Roman Žilka – zilka@fi.muni.cz
Fakulta informatiky, Masarykova univerzita, Brno
Ph.D. student při Laboratoři bezpečnosti a aplikované kryptografie na Fakultě informatiky MU. Studijními zájmy jsou elektronická platební schémata, bezpečnost v bezdrátových senzorových sítích, linuxové rootkity a operační systémy. Bývalý linuxový administrátor na fakultě a fanda do všeho otevřeného.

Vít Bukač – bukac@ics.muni.cz
Fakulta informatiky, Masarykova univerzita, Brno
Absolvent a postgraduální student Fakulty informatiky Masarykovy univerzity. Jeho hlavními výzkumnými zámy jsou síťová bezpečnost, IDS systémy a bezpečnostní protokoly. Od roku 2007 pracuje na Ústavu výpočetní techniky MU jako Active Directory doménový administrátor na Oddělení vývoje systémových služeb.

Moderné sposoby dizajnu distribuovaných, decentralizovaných a polymorfných červov

Norbert Szetei

Počítačový červ (ďalej červ) je program, ktorý rekurzívnym spôsobom replikuje potenciálne evolvovanú kópiu samého seba. Okrem škodlivého správania červy dokážu aplikovať opravy pre kritické zranitelnosti v systémoch alebo odstrániť iné nebezpečné vírusy a červy. Cieľom prednášky je analyzovať historicky zaujímavé typy samoreplikujúcich červov a botnet sietí a predstaviť najmodernejšie prístupy a technológie, ktorými by mohol nami navrhnutý červ disponovať. Dozvieme sa, ako pomocou nich vyriešiť jeho replikáciu, polymorfnosť alebo napríklad nedetekovateľné ovládanie.

Norbert Szetei – norbert.szetei@nethemba.com
Nethemba, s. r. o.
Vyštudoval informatiku na MFF UK v Bratislave a momentálne študuje umelú inteligenciu na Karlovej Univerzite v Prahe. Začínal ako linuxový low-level programátor kernelových modulov a ovládačov, neskôr získal množstvo skúsenosti s administráciou unixových systémov, dizajnom a implementáciu LB/HA clustrov. Je hlavný autor implementácie „Mifare Classic Offline Cracker“, ktorá umožňuje prelomiť viac ako miliardu čipových kariet na celom svete. Tiež je držiteľom CEH (Certified Ethical Hacker) certifikácie a pracuje už niekoľko rokov ako penetračný tester pre firmu Nethemba.

Sledování uživatelů prostřednictvím webových technologií

Jaromír Dobiáš

Webové technologie pronikají do čím dál tím širšího spektra aplikací využívaných v našem každodenním životě. Přináší však také mnohé hrozby, které mohou mít zásadní vliv na soukromí uživatelů. Programátoři využívající webové technologie si častokrát neuvědomují, jaké potenciální následky může mít např. zpřístupnění možnosti vkládání (embedding) externích objektů do webové stránky uživatelům. Ani mnozí uživatelé si častokrát neuvědomují, co vše o nich může

server vyčíst z jejich prohlížeče při brouzdání Internetem. Spousta uživatelů se také mylně domnívá, že pokud vymažou ze svého prohlížeče veškeré cookies či změní svou IP adresu, server není schopen rozpoznat, že v minulosti komunikoval již s danou entitou. Prezentace představí co a jak je možné o uživatelích zjistit v konkrétních případech prostřednictvím webových technologií.

Jaromír Dobiáš – JAROMIR.DOBIAS@MAIL.MUNI.CZ
Fakulta informatiky Masarykovy univerzity, Brno
Je studentem doktorského studijního programu na Fakultě informatiky MU. V minulosti působil jako tester průniků specializující se na bezpečnost webových aplikací. Po dobu téměř dvou let byl zapojen do vývoje technologií zvyšujících ochranu soukromí (PETs) na Technické univerzitě v Drážďanech. V roce 2007 obdržel ocenění Career Recognition Award od společnosti Cisco Systems za profesní úspěch v boji s kybernetickým zločinem.

SSC5 EGI Security challenge: Lehce na cvičišti...

Radoslav Bodó, Daniel Kouřil

Evropská gridová infrastruktura EGI, která sdružuje národní gridové infrastruktury a zajišťuje koordinaci poskytování služeb nad touto infrastrukturou rozsáhlé uživatelské základně přesahující sto tisíc aktivních uživatelů. V takto rozsáhlé infrastruktuře je přirozené, že zajištění bezpečnosti celého prostředí je nesnadná úloha. Ve snaze o zlepšování komunikace a ověření použitelnosti procedur v relativně klidném provozu pořádá EGI CSIRT cvičení, která simulují napadení infrastruktury rozsáhlým útokem. V tomto článku bychom se chtěli podělit o zkušenosti získané cvičením EEGI SSC5 a ukázat základní body postupu použitých pro analýzu zachyceného malware.

Radoslav Bodó – BODIK@CIV.ZCU.CZ
CIV ZCU
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.

Daniel Kouřil – KOURIL@ICS.MUNI.CZ
Centrum CERIT-SC, Masarykova univerzita v Brně
Daniel Kouřil vystudoval Fakultu informatiky Masarykovy univerzity. Zabývá se bezpečnostními otázkami v Gridech, zejména oblastí autentizace a autorizace. Účastní se několika národních i mezinárodních projektů, zaměřených na vybudování a použití Gridové infrastrukury.

Bezpečnosť a vývoj RIA (Rich Internet Application)

Juraj Michálek

RIA technológie posunuli možnosti internetu a webu výrazne ďalej, za hranice statického HTML. Firma Adobe vytvorila Flash platformu, ktorá umožňuje vytvárať aplikácie pre web, desktop, mobily, tablety a televízie. Flash Platform pozostáva z množstva otvorených technológii ako je napríklad framework Flex, middleware BlazeDS, či Open Source Media Framework. Aplikácie postavené na Flash Platform prinášajú so sebou bezpečnostné špecifiká ako napríklad Cross Domain Policy a Security Sandbox. Naviac aplikácie vytvorené pre Flash Platform je možné priamo vložiť do PDF dokumentu a celú aplikáciu distribuovať ako dokument. V takomto prípade vstupujú do hry ďalšie bezpečnostné prvky. V prednáške si predstavíme bezpečnostné mechanizmy Flash Platformy a dáme ich do kontextu web technológii ako je HTML5 a JavaScript. Ukážeme si aj možnosti prepojenia HTML5 a Flash platformy. Povieme si o výhodách, ktoré takéto prepojenie môže priniesť.

Juraj Michálek – juraj.michalek@sinusgear.com
softwarový integrátor
Je priaznivcom otvoreného softvéru a inovácii. Je členom Spoločnosti pre Otvorené Informačné Technológie (soit.sk) Venuje sa vývoju a konzultáciam v oblasti digitálnych technológií. Niekoľko rokov sa intenzívne venuje vývoju okolo Rich Internet Application (RIA) technológii súvisiacimi s firmou Adobe. Primárne sa jedná o otvorené technológie ako Adobe Flex a messaging middleware BlazeDS. Podieľal sa na tvorbe a návrhu architektúry enterprise systémov a ich napojenia na najnovšie technológie postavené na platforme Adobe AIR a HTML5.

Pozvánka na 39. konferenci EurOpen.CZ, 2.–5. října 2011

Editor: Vladimír Rudolf

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

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