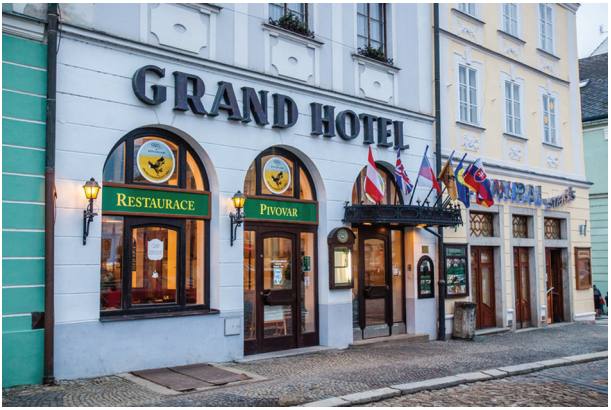
Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

48. konference



Grand hotel Černý Orel
15.–18. 5. 2016

Vážení přátelé EurOpenu!

Znovu nastal čas pozvat vás na velkou konferenci, tentokrát do Jindřichova Hradce. To je to město odkud vedou železniční koleje o dvou rozchodech a vrčí tam nejstarší vodní elektrárna u nás. Mně tedy, když se řekne Jindřichův Hradec, se vybaví hrušky. Ne že bych se tam jimi snad někdy nacpal, dost možná jsem tam nikdy nesnědl ani jedinou, ale už snad třicet let mi leží v hlavě stařičký vtip:

> Zákazník vchází do prodejny n. p. Ovoce a zelenina a ptá se:
> „Dobrý den, máte nějaký jižní ovoce?“
> A prodavač na to:
> „Ano, jsou tady hrušky z Jindřichova Hradce.“

No a ty hrušky, ty mám v paměti dodneška a když se řekne „Jindřichův Hradec“, vždycky se mi vybaví.

Teď ale rychle k programu. Jako obvykle jsme se snažili skládat dohromady větší tématické celky.

Prvním z nich je SIEM. Nechoďte to hledat, SIEM je Security Information and Event Management. Podařilo se nám sezvat přednášející ze všech koutů, jen aby nám o svých zkušenostech něco pověděli.

Dalším tématem je správa identit. Zde tentokrát zabereme širokou škálu řešení od těch „domácích“, vyrobených z nadšení, až po velké a složité produkty, neřku-li systémy, které si musíte koupit od slovutných firem.

Několik přednášek se nám sešlo i kolem tématu forenzního zkoumání výpočetní techniky, ať už klasických počítačů či malé techniky přenosné a kapesní. Potkají se nám tu zkušenosti soudních znalců s pohledy nám blízkých „bezpečáků“ – lidí jako my.

No a konečně se celou konferencí bude proplétat oblíbený motiv malé automatizační techniky, zkrátka hraček. Začne to nedělním tutorialem ESP8266, v pondělí se objeví v tématu síťování pro IoT (než se vydáte znovu googlit, vězte, že IoT je „Internet of Things“) a v úterý nás zase čeká přehled počítacího ovoce (vida, hrušky!) a možná už budou ve středu k mání i nějaké historky o jeho forenzním zkoumání. Kdyby ne, tak se sami zeptáme.

Tolik k programu. Nedopadl špatně, a to jsem ještě nezmínil největší lákadla jako májové počasí v jižních Čechách a úterní práci v sekcích – to se vždy rozumí samo sebou. A tak na závěr už přidám jenom malou výzvu, převážně k mužské části zúčastněných:

„Chlapi! Přes veškerou snahu se nám zase nepodařilo vyhnout konfliktu mezi programem konference a hokejem (v neděli odpoledne s Dánskem, v úterý kolem oběda se Švýcarskem). Přesto na ty přednášky určitě přijďte. A fanděte potichu!“

Zvu vás do Jindřichova Hradce!

Zdeněk Šustr

Program

Neděle 15. 5. 2016

13.00	Tutoriál: Postavme si bezdrátovou meteostanici	*Jiří Bořík*

Pondělí 16. 5. 2016

8.55	Oficiální zahájení	*Jakub Urbanec*
9.00	Úvod do problematiky SIEM	*Jakub Urbanec*
9.25	ArcSight	*Ondřej Krabec*
10.15	Přestávka	
10.45	Qradar	*Slávek Heřman*
11.35	Mentat, systém pro zpracování informací z bezpečnostních nástrojů	*Jan Mach*
12.25	Oběd	
14.00	Celoplošná síť pro IoT	*Štěpán Bechynský*
14.50	Informační systém KrIStýnka	*Tomáš Kukrál*
15.40	Přestávka	
16.10	CzechIdM – první Identity Management, který umí česky	*Lukáš Cirkva, Marcel Poul*
17.00	Nasazení jednotné správy identit a řízení přístupu na Masarykově univerzitě s využitím systému Perun	*Slávek Licehammer*
18.00	Večeře	
20.00	Co se připravuje v kuchyni Evropské kosmické agentury? Aneb mírná ochutnávka z připravovaných evropských kosmických programů s mírnou preferencí v pozorování Země	*Ondřej Šváb*

Úterý 17. 5. 2016

9.00	Použití identit ve federativním prostředí, příklady z elektronických zdrojů knihoven	*Jiří Pavlík*
9.50	Národní identita a projekt STORK	*Michal Procházka*
10.40	Přestávka	
10.55	Networking Academy Games – nová kategorie IoE	*Michal Petrovič*
11.45	Na co se hodí křemíkové ovoce?	*Pavel Jindra, Martin Lávička*
12.35	Oběd	
14.00	Práce v sekcích	
19.00	Večeře	

Středa 18. 5. 2016

9.00	Forenzní zkoumání výpočetní techniky	*Jaroslav Kothánek, Jakub Kothánek*
9.50	Forenzní zkoumání malé digitální a telekomunikační techniky	*Jaroslav Kothánek, Jakub Kothánek*
10.40	Přestávka	
10.55	Malware Houdiny – spolupráce CSIRT a forenzní laboratoře (případová studie)	*Aleš Padrta*
11.45	KYPO	*Dan Kouřil*
12.30	Závěr	
12.35	Oběd	

Konferenční poplatky

Vložné		
Platba	Tutoriál	Konference
Členové		
do 10. 5. 2016	1 190	2 350
po 10. 5. 2016	1 290	2 550
Nečlenové		
do 10. 5. 2016	1 290	2 600
po 10. 5. 2016	1 390	2 850
Ubytování a stravování		
od neděle 15. 5. 2016	1 950	od nedělní večeře do středečního oběda, 3 noclehy
od pondělí 16. 5. 2016	1 400	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 650 Kč na den (ubytování 450 Kč na den se snídaní, oběd 100 Kč, večeře 100 Kč).

Vyhrazená kapacita hotelu je zhruba 70 osob.

Programový výbor

Zdeněk Šustr
Jiří Bořík
Jan Kynčl
Jakub Urbanec

Kdy	Tutoriál se uskuteční v neděli 15. 5. 2016 od 13.00 hodin
	Konference začíná v pondělí 16. 5. 2016 v 9.00 hodin a končí ve středu 18. 5. 2016 cca ve 14.00 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Grand hotel Černý Orel http://www.grandhotelcernyorel.cz
Kontaktní adresa	Anna Šlosarová EurOpen.CZ, Univerzitní 8, 306 14 Plzeň e-mail: europen@europen.cz, tel.: 377 632 701
Co zahrnuje účastnický poplatek	vložné, sborník, stravné, občerstvení během přestávek a ubytování
Úhrada poplatku	č. ú. 478928473 u ČSOB Praha 1, kód banky 0300, variabilní symbol v elektronické přihlášce (nutno uvést), společnost EurOpen.CZ, Univerzitní 8, Plzeň IČO: 61389081, DIČ: CZ61389081 Společnost EurOpen.CZ není plátcem DPH.
Neúčast	Při neúčasti se účastnický poplatek nevrací, ale sborník bude zaslán. Při částečné účasti se platí plný účastnický poplatek.
On-line přihlášky	Anotaci příspěvků a elektronickou přihlášku je možné najít na adrese: http://www.europen.cz V programu konference může dojít k drobným časovým i obsahovým změnám.
Doklad o zaplacení	**Zašleme v rámci vyúčtování po skončení semináře.**
Uzávěrka přihlášek	13. 5. 2016 nebo při naplnění ubytovací kapacity.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 70.
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: Postavme si bezdrátovou meteostanici

Jiří Bořík

Už vás nebaví Arduino? Na Raspberry se práší v šuplíku? Chcete něco novějšího, menšího a bezdrátového? Zkuste s námi vývojový kit osazený ESP8266. Naučíte se základům jazyka Lua, zkusíte si napsat a rozchodit pár technických ukázek a domů si odnesete funkční základ bezdrátové meteostanice.

Jiří Bořík – borik@civ.zcu.cz
Odrostlý bastlíř fascinovaný možnostmi IoT zkouší dohonit, co v dětství nestihl.
https://cz.linkedin.com/in/jborik

ArcSight

Ondřej Krabec

Seznámení se SIEM řešením HPE ArcSight a popis zpracování události, která vznikla na zdroji a je třeba jí parsovat, normalizovat, uložit, korelovat a následně vyhledávat. Posluchači budou seznámeni s koncepcí a přístupem k řešení této problematiky, kterou je možné tímto řešením realizovat.

Ondřej Krabec – ondrej.krabec@hpe.com
Technický konzultant se specializací na SIEM od HP ArcSight. Dříve působil ve společnosti S&T, kde ArcSight implementoval především pro finanční instituce, nyní pokračuje na pozici konzultanta a spolupracuje se společností Hewlett Packard Enterprise.

QRadar

Slávek Heřman

Přehled technologického řešení SIEM QRadar od přijetí eventu přes parsing a korelaci, po jeho uložení a následné vyhledávání. Příspěvek je koncipován jednak jako ucelený pohled na daný produktu, aby měl posluchač možnost sám si porovnat technologii QRadaru s ostatními řešeními, ale především jako příležitost sdílet praktické poznatky ze správy globálního systému, který se sestává z destítek serverů a sbírá logy z tisíců zdrojů.

Slávek Heřman – slavek.herman@seznam.cz
Zabývá se SIEM řešeními a security monitoringem obecně již 6 let. Nejdříve na pozici konzultanta v Hewlett-Packard, nyní v roli interního administrátora pro společnost Novartis.

Mentat, systém pro zpracování informací z bezpečnostních nástrojů

Jan Mach

Bezpečnostních nástrojů, které monitorují síťový provoz a detekují útoky na infrastrukturu, služby a uživatele, neustále přibývá a s tím přibývá i dat, které bezpečnostní týmy a správci musí zpracovat, analyzovat a distribuovat. Sdružení CESNET za účelem zpracování velkého množství dat vyvíjí a provozuje systém Mentat, který postupně dotváří do podoby SIEM systému.

Jan Mach – jan.mach@cesnet.cz
Pracuje již téměř 7 let pro sdružení CESNET, kde působí jako člen bezpečnostního týmu CESNET-CERTS. Kromě správy několika produkčních serverů a systémů se zabývá zejména otázkami síťové bezpečnosti, monitoringem a zpracováním dat. Je také hlavním vývojářem systému Mentat.

Celoplošná síť pro IoT

Štěpán Bechynský

Jedním z problémů IoT je bezpečná komunikace, která bude dostupná optimálně všude a bude potřebovat minimum energie. Jedna z možností je použití technologie označované jako Ultra Narrow Band. V přednášce udivíte praktickou ukázku sítě SIGFOX, která UNB technologii používá a je dostupná, skoro, celoplošně. Během přednášky si postavíme zařízení, které bude data posílat přes síť SIGFOX do Microsoft Azure pro visualizaci.

Štěpán Bechynský – stepan@bechynsky.cz
Po skoro devíti letech opustil Štěpán Bechynsky společnost Microsoft, kde pracoval jako Technical Evangelist se zaměřením na Microsoft Azure a zakotvil v klidnějších vodách farmaceutické společnosti MSD, kde měl na starost infrastrukturu v Amazon Web Services. V klidných vodách získal titul MVP a vrátil se do společnosti Microsoft, kde se stará o IoT řešení v regionu CEE jako technický konzultant. Ve volných chvílích se věnuje mikrokontrolérům a 3D tisku a víkendy tráví nejraději u plotny nebo přednášením o Arduino.

Informační systém KrISTýnka

Tomáš Kukrál

Kristýnka je hubený informační systém, který slouží ke správě uživatelů v některých klubech Studentské Unie ČVUT. Nesnaží se poskytovat mnoho funkcí, ale přistupuje k řešení problému velmi minimalisticky a bez zbytečných komplikací. V přednášce představím jakým způsobem Kristýnka pracuje, proč jsme

se rozhodli pro vlastní řešení a v neposlední řadě zmíním i několik technických detailů – např. spojení s routerem Turris.

Tomáš Kukrál – tomas.kukral@fit.cvut.cz
Působím jako správce virtualizace, kontejnerů a kompostování na ČVUT FIT. Věnuji se zde především modernizaci infrastruktury a jejím zjednodušení, takže mám na starosti virtualizační řešení postavené na softwaru OpenNebula, distribuované Ceph úložiště a Kubernetes/OpenShift platformu pro správu kontejnerů.

CzechIdM – první Identity Management, který umí česky

Lukáš Cirkva, Marcel Poul

Představení původního českého IDM systému vhodného pro velké organizace všech kategorií (zdravotnictví, školství, samospráva i komerčních firmy) – od prvního konceptu produktu při založení firmy až po komplexní systém dnes. Představíme plány dalšího rozvoje, nové technologie i přesahy do souvisejících oblastí.

Lukáš Cirkva – lukas.cirkva@bcvsolutions.eu
Od roku 2004 se věnuje Identity Managementu na plný úvazek. V roce 2008 založil vlastní firmu s primárním zaměřením na projekty IDM. Firma aktuálně zaměstnává 25 osob, většinu vývojářů a konzultantů. Pro zákazníky implementovali a provozují řešení IDM, které spravuje více než 2 milióny identit.

Marcel Poul – marcel.poul@bcvsolutions.eu
Vede tým vývojářů a konzultantů zodpovědný za implementaci a podporu řešení Identity Managementu CzechIDM například pro zákazníky CETIN, Bohemia Energy, Magistrát města Ostravy a Pojišťovnu České spořitelny.

Nasazení jednotné správy identit a řízení přístupu na Masarykově univerzitě s využitím systému Perun

Slávek Licehammer

Správa identit na Masarykově univerzitě je rozdělena mezi několik různých, vzájemně kooperujících systémů. Identity vznikají ve studijní agendě a také v personální agendě. Obě tyto agendy jsou spravovány různými systémy, které jsou mezi sebou vzájemně synchronizovány. Nad těmito systémy byla vybudována další infrastruktura nabízející rozhraní pro další systémy a služby. Mimo to vznikala další řešení pro správu identit a řízení přístupu na jednotlivých fakultách, která jsou více či méně propojená s centrálním řešením.

Naší snahou je vytvoření, jednotné koncepce pro správu identit a řízení přístupu na Masarykově univerzitě, která by měla obsáhnout jak organizační, tak technické aspekty. Základem je jednotná korporátní identita na MU, která půjde využít ve všech systémech Masarykovy univerzity nezávisle na tom, která organizační jednotka univerzity daný systém spravuje. Korporátní identita bude zahrnovat i účty externích osob a servisní účty. Pro řízení přístupu bude k dispozici jednotné rozhraní, které bude poskytovat informace o členství osob ve skupinách.

Pro realizaci využijeme systém Perun, který je vyvíjen Masarykovou univerzitou společně se sdružením CESNET. Perun je komplexní nástroj pro správu identit a řízení přístupu. Z pohledu správy identit pokrývá celý životní cyklus uživatele, dále je možné ho napojit na existující systémy a tím zajistit dostupnost všech dat o identitách a skupinách na jednom místě, kde lze následně nastavovat přístupová práva a ta exportovat do řízených systémů. Perun podporuje delegaci správy jak uživatelů, tak skupin, díky čemu lze správcům koncových služeb a systémů minimalizovat práci věnovanou podpoře uživatelů.

V prezentaci bude představeno nové řešení včetně jednotlivých komponent a způsobu napojení na existující infrastrukturu. Dále zmíníme problémy se kterými jsme se potýkali při návrhu nového řešení a také ty, které se objevily v průběhu implementace.

Slávek Licehammer – slavek@ics.muni.cz
Student doktorského programu na Masarykově univerzitě. Zaměstnaný na Ústavu výpočetní techniky Masarykovy univerzity a také ve sdružení CESNET, kde se věnuje výzkumu a vývoji v oblasti správy identity a řízení přístupu. V rámci této činnosti se podílel na vzniku systému Perun, na jehož vývoji se i nadále podílí. Je zapojen do mezinárodních projektů EGI, GÉANT a INDIGO, kde pracuje v oblasti autentizačních a autorizačních infrastruktur a elektronických identit.

Co se připravuje v kuchyni Evropské kosmické agentury? Aneb mírná ochutnávka z připravovaných evropských kosmických programů s mírnou preferencí v pozorování Země

Ondřej Šváb

Již osmým rokem je ČR členem klubu států, které v rámci Evropské kosmické agentury (ESA) nejen drží krok se světovou špičkou v oblasti kosmických technologií a aplikací, ale do jisté míry také udává trendy, které stále častěji směřují spíše do businessu a využití dole na zemi, než do čisté vědy. ESA pracuje na systémech družicové navigace EGNOS a Galileo, má jeden z nejmohutnějších systémů programů pro pozorování Země na světě, jehož výsledkem jsou družice s fantastickými výsledky, které často mění pohled na planetu, na které žijeme.

Telekomunikační programy patřící k absolutní světové špičce se nově pouštění do dříve nemyslitelných programů pro přípravu konstelací stovek až tisíců (!) družic, megakonstelací, které budou klíčové v připojení dalších 3 miliard lidí k internetu. Výnos takového množství družic by nebyl možný bez efektivních nosných raket, avšak to je oblast, kde je potřeba výrazně přidat a dotáhnout se na léty prověřenou konkurenci z Ruska a miliardáři hnanou konkurenci z USA. Dostat se do vesmíru je (ve většině případů (!)) základem pro experimenty v mikrogravitaci. Věda tak rozhodně nepřichází zkrátka! Konec konců Vědecký program, ve kterém ESA chystá nové kosmické observatoře i sondy mířící do sluneční soustavy, je základním programem této agentury.

Slovy klasika se ESA často pouští tam, kam se dosud nikdo nevydal... Podívejme se tedy do kuchyně, v níž ESA připravuje svoje nové programy, které nás v budoucnosti snad překvapí, snad inspirují, ale rozhodně před nás postaví nové otázky! A v pozorování Země, jehož nové éra s příchodem bezplatně a hlavně doposud nebývale často dostupných dat právě začíná je jich k řešení více než dost! Těžba informací z družicových snímků. Velkoobjeové zpracování. Distribuce dat. Nové služby. Nové algoritmy. Archivace.

Třeba právě v kosmických technologiích a aplikacích najdete inspiraci ve své další práci. Pojďte zjistit, co se chystá a jak se můžete zapojit i Vy!

Ondřej Šváb – ondrej.svab@mdcr.cz
Ondřej Šváb vystudoval krajinné a pozemkové úpravy na Fakultě životního prostředí ČZU v Praze. Od roku 1999 je demonstrátorem pražské Štefánikovi hvězdárny a od roku 2009 pracuje na Ministerstvu dopravy, kde je vedoucím Oddělení kosmických technologií a aplikací, které je odpovědné za zastoupení ČR v ESA a za kosmickou politiku ČR. Kromě zájmu o vesmír se věnuje turistice, fotografii a četbě historických, špionážních a sci-fi románů – a to vše za podpory a lásky své budoucí ženy Lenky.

Použití identit ve federativním prostředí, příklady z elektronických zdrojů knihoven

Jiří Pavlík

Federativní autentizace zjednodušuje přístup k elektronickým informačním zdrojům, které akademické i veřejné knihovny zajišťují pro své čtenáře. Díky federativní autentizaci čtenáři využívají jednotné přihlášení ke katalogu knihovny i při přístupu k elektronickým knihám, elektronickým časopisům i databázím. Federativní autentizace je dostupná u EBSCOhost, Proquest, ebrary, Web of Sciences, Elsevier Science Direct a Scopus, SpringerLink, Cambridge Journals, Brill, Sage Journals, Emerald, eReading.cz a u řady dalších platforem. V přednášce si představíme federativní autentizaci na příkladu Univerzity Karlovy a Moravské zemské knihovny.

Jiří Pavlík – jpavlik@cesnet.cz
Absolvoval v roce 2000 České vysoké učení technické, Fakultu elektrotechnickou. Od roku 1995 je zaměstnancem Univerzity Karlovy. Do konce roku 2014 působil na Ústavu výpočetní techniky, kde se věnoval podpoře knihovních systémů, federativní autentizaci, plnotextovým technologiím, multimédiím. O začátku roku 2015 působí v Ústřední knihovně Univerzity Karlovy. Od roku 2006 pracuje v CESNET jako administrátor České akademické federace identit eduID.cz.

Networking Academy Games – nová kategorie IoE

Michal Petrovič

Tento rok proběhl již 11. ročník soutěže Networking Academy Games. Novinkou tohoto roku byla nová kategorie zaměřená na nejnovější trend v počítačovém světě a to Internet všeho. Jedná se o podporu a zatraktivnění výuky pro studenty zaměřené nejen na počítačové sítě ale i obecněji na základy elektroniky a operační systém Linux. Soutěž začala vyškolením lektorů pro přípravu studentů a pokračovala čtyřmi on-line koly a pátým finálovým on-site kolem. Do soutěže se přihlásilo 42 týmů z celé ČR, kde jeden tým se skládal ze tří studentů a jednoho lektora. V rámci přednášky bude představen způsob organizace, technické aspekty soutěže a výsledky jednotlivých soutěžních kol s ukázkami, co celá soutež přinesla.

Michal Petrovič – petrovic@civ.zcu.cz
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 sí?ťový a IP telefonní architekt. Dále se podílí na provozu a rozvoji národní sítě pro výzkum a vzdělávání České republiky – CESNET. V neposlední řadě je zakladatelem a členem představenstva spolku i-com-unity z. s., který provozuje v ČR podporu síťových akademií, lektorský terénink, organizaci konferencí a soutež Networking Academy Games.

Na co se hodí křemíkové ovoce?

Pavel Jindra, Martin Lávička

Raspberry, Banana, Orange, ... Byl by jednodeskový minipočítač s ARMem schopen odvést stejnou práci jako běžný server a to za 10× menší cenu? Možná ano! Pořídili jsme si několik výkonných minipočítačů a zkusili to. Podle parametrů se mezi modely jako Krait, ODROID, CUBIEBOARD jeví Raspberry Pi2 jako chudý bratříček. Jakmile došlo na plnění reálných úloh byla situace

překvapivá. Výběr vhodného typu pro konkrétní aplikaci je vždy komplikovaný a komplexní proces, my bychom se rádi podělili o své postřehy a zkušenosti.

Pavel Jindra – PAJA@CIV.ZCU.CZ
Je absolventem Fakulty elektrotechnické na ZČU v Plzni. Od roku 2003 pracuje na Západočeské univerzitě v Centru informatizace a výpočetní techniky. Jeho pracovní náplní je především správa autentizační a PKI infrastruktury. Ve volných chvílích se věnuje jednodeskovým počítačům a elektrotechnice.

Martin Lávička – MLAVICKA@CIV.ZCU.CZ
Vystudoval fakultu elektrotechnickou na Západočeské univerzitě v Plzni. V současné době pracuje jako správce OS Windows na Západočeské univerzitě. Dlouhodobě sleduje trendy v oblasti IoT, jednodeskových počítačů a možnosti jejich nasazení.

Forenzní zkoumání výpočetní techniky

Jakub Kothánek, Jaroslav Kothánek

Pro potřeby trestního řízení je čím dál častěji nutné vytěžovat důkazní materiál z výpočetní techniky. Pro orgány činné v trestním řízení představuje výpočetní technika takřka bezednou studnu tohoto důkazního materiálu, kdy drtivá většina lidí dnes výpočetní techniku využívá, ať již k práci, či k zábavě nebo vyhledávání informací.

Z těchto důvodů je nutné tomuto relativně novému oboru věnovat řádnou pozornost, aby nedocházelo ke ztrátám důkazního materiálu a také k procesním chybám, které by znamenaly nevyužitelnost vytěžených důkazů v trestním řízení.

Cílem této přednášky bude informovat širší veřejnost o možnostech forenzního zkoumání výpočetní techniky, o různých problémech ať již technických, či právních tak, aby se rozšířilo povědomí o tomto fenoménu, kdy v České republice toto povědomí je obecně velmi malé a to i v rámci orgánů činných v trestním řízení.

Jaroslav Kothánek – KOTHANEK@IT-ZNALEC.CZ
23 let pracoval na Krajském ředitelství policie Jihočeského kraje, kde většinu času zastával funkci soudního znalce v oborech počítačové kriminality následně 2 roky působil na Policejním prezidiu, ČR odboru Informační kriminality jako vyšetřovatel a metodik. Po odchodu od Policie ČR v roce 2010 založil znaleckou kancelář v oblasti Kybernetiky, výpočetní techniky a elektroniky. Od roku 2011 začal vytvářet nové studijní programy na Jihočeské univerzitě, nejprve na Pedagogické fakultě a následně dodnes na Přírodovědecké fakultě, Ústavu aplikované informatiky, kde založil nové oddělení forenzních věd a kriminalistiky a stal se

jejím vedoucím. Dále v současné době problematiku přednáší taktéž na Západočeské univerzitě, Fakultě elektrotechnické. Za svojí kariéru předložil několik tisíc znaleckých posudků pro orgány činné v trestním řízení.

Jakub Kothánek – jakub.kothanek@it-znalec.cz
Vystudoval Právnickou fakultu Masarykovy univerzity v Brně, kde v průběhu studia se zejména zajímal o informační kriminalitu a dále spolupracoval na založení znalecké kanceláře v oblasti Kybernetika, výpočetní technika a elektronika, kde působí jako asistent znalce a dále se zaobírá právem v IT. V současné době se podílí na vzdělávání orgánů činných v trestním řízení v oblasti forenzního zkoumání mobilních telefonů a výpočetní techniky. Od roku 2015 se podílí na výuce a přednáší jako externí vyučující na Jihočeské univerzitě, Přírodovědecké fakultě, Ústavu aplikované informatiky, oddělení forenzních věd a kriminalistiky, zejména problematiku forenzního zkoumání a právních věd v oblasti IT. V rámci své činnosti se podílel na tvorbě stovek znaleckých posudků v oblasti zkoumání digitální techniky.

Forenzní zkoumání malé digitální a telekomunikační techniky

Jakub Kothánek, Jaroslav Kothánek

Snad každý člověk dnes využívá mobilní telefon či tablet, a to i pro připojení k internetu, komunikaci nejen mobilní, ale i chatové, apod. Pro orgány činné v trestním řízení se tak naskýtá další možnost, jak získat důležitý důkazní materiál. Mnoho lidí totiž využívá tzv. chytré mobilní telefony s operačními systémy Android, iOS či Windows Mobile, kdy v těchto systémech lze využívat nepřeberné množství aplikací a tak je možno z mobilních telefonů vytěžit nepřeberné množství informací, které by se orgány činné v trestním řízení nedozvěděly ani od nejlepšího kamaráda či partnera vlastníka daného telefonu.

Z tohoto důvodu je nutno se tomuto forenznímu zkoumání pečlivě věnovat, aby nedošlo k poškození či ztrátě tohoto důkazního materiálu, kdy by toto mohlo mít fatální důsledky pro celé trestní řízení.

Cílem přednášky bude informovat veřejnost o možnostech forenzního zkoumání přenosné digitální techniky, hlavně mobilních telefonů a tabletů, o různých omezeních tohoto zkoumání a dalších problémech s tímto spjatých. Budeme se věnovat různým mobilním platformám spolu s jejich specifiky a požadavky na forenzní zkoumání.

Malware Houdiny – spolupráce CSIRT a forenzní laboratoře (případová studie)

Aleš Padrta

Pro rychlé a efektivní řešení bezpečnostních incidentů potřebují bezpečnostní týmy informace, hodně informací. V případě reakce na výskyt malware jsou to typicky odpovědi na otázky „Kde se vzal?“, „Jak se šíří?“, „Jaké má schopnosti?“, „Jak poznat už napadené stanice?“ a „Jak se jej zbavit?“. V tomto příspěvku je ukázána spolupráce bezpečnostního týmu Západočeské univerzity v Plzni (WIRT) a forenzní laboratoře CESNET (FLAB) při reakci na výskyt malware Houdiny na pracovních stanicích uživatelů. Jsou zde popsány jednotlivé kroky bezpečnostního týmu, způsob komunikace, předávání informací a spolupráce s forenzní laboratoří, postupy použité při analýze malware a na závěr pak také využití získaných informací při řešení bezpečnostního incidentu.

Aleš Padrta – apadrta@cesnet.cz
Po absolvování magisterského a doktorského studia na Fakultě aplikovaných věd Západočeské univerzity (ZČU) začal v roce 2005 pracovat pro Centrum informatizace a výpočetní techniky jako administrátor počítačových systémů se zaměřením na bezpečnost. Od roku 2006 je zakládajícím členem bezpečnostního týmu typu CSIRT pro ZČU. Dále, od roku 2007 pracuje pro sdružení CESNET, z. s. p. o., se zaměřením na vzdělávání uživatelů v oblasti bezpečnosti a od roku 2011 přibývá také práce na projektu forenzní laboratoře FLAB a analytická činnost. V roce 2014 mu bylo svěřeno vedení této laboratoře.

KYPO

Daniel Kouřil

Projekt bezpečnostního výzkumu Kybernetický polygon má za cíl vytvořit unikátní prostředí pro výzkum a vývoj metod na ochranu proti útokům na kritické infrastruktury. Ve virtualizovaném prostředí umožňuje provádět komplexní scénáře útoků vedených proti kritickým infrastrukturám a analyzovat jejich průběh. Prostředí slouží pro aplikovaný výzkum a ověřování nových bezpečnostních metod, nástrojů a školení členů bezpečnostních týmů.

Daniel Kouřil – kouril@ics.muni.cz
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.