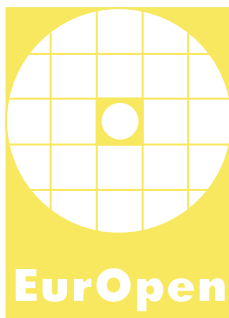


Česká společnost uživatelů otevřených systémů EurOpen.CZ  
Czech Open System Users' Group  
[www.europen.cz](http://www.europen.cz)



**45. konference**



**Hotel Šumava, Kašperské Hory  
5.–8. 10. 2014**



## Slovo úvodem

Vážení přátelé EurOpenu!

Letošní podzimní konference se kvapem blíží. Po letních prázdninách nám zbude jen chvilka na rozkoukání a pak zamíříme – letos už podruhé – na Šumavu, tentokrát do Kašperských Hor.

Jistě si vzpomenete, že jsme na jaře začali téma programovatelných hraček pro výuku dětí i pro zábavu dospělých. Tentokrát v něm budeme pokračovat. Kdo si v neděli 5. října přivstane, stihne tutoriál Raspberry PI. Tam se s tímto miniaturním počítačem v poklusu seznámíme a pak se zaměříme především na programování I/O portů a interakci s jednoduchými, tj. také levnými, perifériemi. Jako bonus si každý účastník svou „malinu“ s příslušenstvím odnese domů. Proto je také cena tutoriálu vyšší než obvykle. Ale nemyslete si, že získané zkušenosti přijdou vniveč. Podobným hračkám a jejich použití v seriózních i zábavných aplikacích se budeme i v příštím roce věnovat na dalších konferencích.

Po nedělní rozcvičce s malinou se vrhneme do hlavních témat. „Když nejde o peníze, nejde o nic“, říkávalo se u nás. V pondělí půjde o peníze především. Jsou banky, které si kupují komplexní systémy od věhlasných firem. Podíváme se jim trochu pod pokličku, a to zejména na moderní metody placení. Na druhé straně jsou banky, které si vše staví skoro od základu samy. U těch nás zas bude zajímat, co vytvoření takového bankovního systému obnáší.

Až uzavřeme téma bank, bude nás čekat druhá velká sekce o testování a monitoringu, která se protáhne až do úterka. Sešly se nám příspěvky jak o testování zátěžovém, tak funkčním, dojde na funkční i výkonnostní srovnání filesystémů a seznámíme se s několika řešeními pro dohled nad IT infrastrukturou.

V úterý večer se nezapomeňte včas vrátit z práce v sekcích! Jestli se někdo pokusí zorganizovat druhé Lipno, upadne v nemilost! Po večeri se totiž uskuteční tradiční netechnická přednáška, tentokrát astronomicko-historicko-detektivní. Jménem vás všech jsem slíbil přednášejícímu obecenstvo početné, inteligentní a vnímavé, a tímto na vás odpovědnost za svůj slib přenáším!

Poslední den 45. konference, středu, začneme také okénkem do netradičního oboru, i když o netechnickou přednášku už rozhodně nepůjde. Jen nahlédněte do programu! Pak se rychle vrátíme do světa PC, do světa, v němž řada z nás žije každý den, do světa Webu a databází. A po doznění tohoto bloku bude konference u konce.

Doufáme, že jsme vás programem zaujali. Jestli o své účasti nerozhodujete sami, pak doufáme, že jsme zaujali i vaše vedoucí. A věříme, že se za námi rozjedete, nebo se necháte vyslat, a těšíme se s vámi na shledanou v Amálině údolí!

# Program

**Neděle 5. 10. 2014**

13.00	Tutoriál: Raspberry PI	<i>Jakub Urbanec, Jiří Bořík</i>
-------	------------------------	--------------------------------------

**Pondělí 6. 10. 2014**

9.00	Oficiální zahájení	<i>Zdeněk Šustr</i>
9.05	Platby mobilním telefonem	<i>Martin Chlumský</i>
9.55	Přestávka	
10.15	Bezkontaktní platební karty – radost nebo starost?	<i>Jan Okrouhlý</i>
11.05	Zabezpečení 3D-Secure při platbě na Internetu	<i>Martin Zich</i>
12.00	Oběd	
14.00	Jak udělat banku	<i>Václav Votíпка</i>
14.55	Interní vývoj bankovního systému	<i>Adrian Kantor</i>
15.50	Přestávka	
16.15	Služba sledování infrastruktury a IP provozu sítě pro uživatele e-infrastruktury CESNET	<i>Tomáš Košnar</i>
17.05	Zpracování logů a netflow	<i>Radoslav Bodó</i>
18.00	Večeře	
19.30	valná hromada EurOpen.CZ	

**Úterý 7. 10. 2014**

9.00	Výkonnostní a funkční testy souborových systémů pro cloud	<i>Filip Hubík</i>
9.50	ZFS a BTRFS v praxi	<i>Jan Krčmář</i>
10.40	Přestávka	
10.55	Dohled nad (nejen) IT prostředím pomocí PRTG	<i>Martin Couf</i>
11.45	Zátěžové testování aneb „Sakra, kdo to bude platit“	<i>Ján Hrabik</i>
12.35	Oběd	
14.00	Práce v sekcích	
19.00	Večeře	
20.00	Jak byla (ne)objevena poslední planeta	<i>Pavel Najser</i>

**Středa 8. 10. 2014**

9.00	Programovací techniky a úskalí při vývoji SW v automobilovém průmyslu	<i>Martin Butníkošarovski</i>
9.50	SQL včera a dnes	<i>Petr Jiroušek</i>
10.40	Přestávka	
10.55	Vizualizace dat a framework D3.js	<i>Karel Minařík</i>
11.45	Databázový kyberzločin je na vzestupu! Jak se mu bránit?	<i>Jan Musil</i>
12.35	Závěr	
12.40	Oběd	

## Konferenční poplatky

Vložené		
Platba	Tutoriál	Konference
Členové		
do 29. 9. 2014	2 190	2 300
po 29. 9. 2014	2 290	2 550
Nečlenové		
do 29. 9. 2014	2 290	2 600
po 29. 9. 2014	2 390	2 850
Ubytování a stravování		
od neděle 5. 10. 2014	2 820	od nedělní večeře do středečního oběda, 3 noci
od pondělí 6. 10. 2014	2 060	od pondělního oběda do středečního oběda, 2 noci

Tutoriál je možné objednat i samostatně, účast na konferenci není podmínkou pro účast na tutoriálu. Kapacita tutoriálu je 20 osob.

Ubytování a plná penze 940 Kč na den (ubytování se snídaní 580 Kč na den, oběd 180 Kč, večeře 180 Kč).

Kapacita hotelu je zhruba 80 osob.

## Programový výbor

Zdeněk Šustr  
 Jiří Šitera  
 Jan Kynčl

Kdy	Tutoriál se uskuteční v neděli 5. 10. 2014 od 13.00 hodin
	Konference začíná v pondělí 6. 10. 2014 v 9.00 hodin a končí ve středu 8. 10. 2014 cca ve 14.00 hodin. Stravování je zajištěno od nedělní večere nebo od pondělního oběda, podle zvolené varianty.
Kde	Hotel Šumava, Kašperské Hory <a href="http://www.sumavanet.cz/zsmv">http://www.sumavanet.cz/zsmv</a>
Kontaktní adresa	Anna Šlosarová EurOpen.CZ, Univerzitní 8, 306 14 Plzeň e-mail: <a href="mailto:europen@europen.cz">europen@europen.cz</a> , 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: <a href="http://www.europen.cz">http://www.europen.cz</a> V programu konference může dojít k drobným časovým i obsahovým změnám.
Doklad o zaplacení	<b>Zašleme v rámci vyúčtování po skončení semináře.</b>
Uzávěrka přihlášek	1. 10. 2014 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	<b>Pouze e-přihláška: Webový formulář viz <a href="http://www.europen.cz">http://www.europen.cz</a></b>

Tutoriál: RASPBERRY PI  
**Jakub Čuba++ Urbanec, Jirka Bořík**

**Kdo by nechtěl mít doma server s odběrem pod 3 W, který měří, mailuje a ukazuje?**

*(Kdo nechce, ať nejede na tutoriál!)*

Tutoriál se tentokrát bude zabývat fenoménem Raspberry Pi, malého počítače s velkým potenciálem. Provede Vás základy použití, dětského i dospělého programování, ukáže Vám, jak sbírat informace z čidel a jak je publikovat na serveru nebo posílat výstražné e-maily: „Teplota na půdě je nyní 78 stupňů a stále stoupá. Mám zavolat hasiče?“

**Co si z tutoriálu odnesete?**

Především si odnesete Raspberry Pi B+, které je v ceně tutoriálu. K tomu dostanete čidla, součástky a vývojové nástroje. To je důvod, proč bude tutoriál tentokrát dražší než obvykle – mimo zážitky si odnesete domů také samotný počítač.

**Co s sebou na tutoriál?**

Notebook s funkčním ethernetovým portem (který umíte nastavit). Může se také hodit reproduktorek nebo sluchátka s 3.5 mm jackem a stará USB kamera.

**Co musíte znát?**

Hodí se znalost nastavení sítě na vašem počítači, základy programování a základy OS Linux (nebojte, my to taky moc neumíme)

**Jakub Čuba++ Urbanec** – URBANEC@T1.CZ  
<http://www.linkedin.com/in/urbanec>

**Jirka Bořík** – BORIK@CIV.ZCU.CZ  
<http://www.linkedin.com/in/jborik>

PLATBY MOBILNÍM TELEFONEM

**Martin Chlumský**

Čipové platební karty zaujaly místo v našich peněženkách již před řadou let. Po poněkud váhavém přijetí bezkontaktní technologie začínáme vídat další platební nástroje – bezkontaktní nálepky, hodinky nebo mobilní telefony. A právě



mobilní telefony se od ostatních forem liší, neboť nejde o jednorázová zařízení, ale o systémy umožňující instalaci řady aplikací a komunikaci s uživatelem. Příspěvek je věnován dvěma rozdílným světům – mobilním platbám na běžných bezkontaktních terminálech prostřednictvím technologie NFC a Internetovým platbám mobilním telefonem zapojeným do programu MasterCard Mobile.

NFC (Near Field Communication) je bezkontaktní technologie určená k snadné výměně informací na krátkou vzdálenost. Tato technologie zahrnuje rovněž emulaci karet komunikujících protokolem ISO 14443, který je základem bezkontaktních plateb. Mobilní telefony s rozhraním NFC tedy mohou obsahovat obraz platební čipové karty a provádět platby na bezkontaktních terminálech. U platebních čipových karet je kladen důraz na bezpečnost, proto data a samotná aplikace představující platební kartu musí být i v případě mobilního telefonu uložena v bezpečné oblasti. Tou není paměť telefonu, nýbrž Secure Element (SE), který vyhovuje všem potřebným kritériím a certifikacím. SE může být implementován jako dodatečný čip v telefonu, speciální microSD, SIM (dnes UICC) nebo jako čip v ochranném obalu na telefon. V závislosti na zvoleném řešení se pak může lišit i ekosystém spojený s vydáváním a správou karet, a tedy i způsob, jakým se např. aplikace a data reprezentující kartu dostanou k uživateli. Mobilní telefon neobsahuje ale pouze SE s aplikací platební karty, nýbrž i grafické rozhraní, které umožňuje držiteli výběr z více karet, prohlížet historii transakcí, měnit platební preference nebo verifikovat držitele během platby (PassCode). Zásadní rozdíly lze najít i v oblasti risk managementu offline plateb nebo správou PassCode. Běžné karty jsou občas zasunuty do kontaktního rozhraní, a banka má tedy prostor k provedení nezbytného resetování interních offline čítačů, změny parametrů karty, aktualizaci PINu nebo zablokování karty. Mobilní telefon ale do kontaktního terminálu vkládat nelze, proto musí aplikace umožňovat bezpečnou komunikaci s bankou prostřednictvím sítě MNO nebo WiFi.

MasterCard Mobile představuje zcela odlišný pohled na použití mobilního telefonu při placení. V současnosti je již možné na některých Internetových platebních branách vidět loga MCM a QR kódy, které jsou pak skenovány z obrazovky počítače telefonem vybaveným vhodnou platební aplikací. Držitel karty pak nemusí přepisovat údaje své karty do platebního formuláře, ale po spárování telefonu s danou transakcí prostřednictvím QR kódu vybere jednoduše kartu ze své mobilní peněženky. Po verifikaci PINu na telefonu předá poskytovatel služby MasterCard Mobile bezpečnou formou informaci o zvolené kartě platební bráně, kde je následně provedena běžná e-Commerce transakce. Aplikace v mobilním telefonu neobsahuje citlivé údaje karty, ty jsou při registraci karty do mobilní peněženky uloženy do systému poskytovatele, který splňuje veškeré bezpečnostní požadavky asociací. Kromě placení v Internetových obchodech je služba připravena i na přímé platby z aplikací mobilního telefonu, dobíjení kreditu telefonů, dárcovské platby apod.

**Martin Chlumský** – MARTIN.CHLUMSKY@HP.COM

(\*1971) Je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni. Po ukončení studia působil řadu let v Centru Informatizace a výpočetní techniky (CIV) ZČU. V současnosti pracuje jako konzultant společnosti Hewlett-Packard se zaměřením na bezpečnost. Většinu času tráví na projektech z oblasti bankovního sektoru.

## BEZKONTAKTNÍ PLATEBNÍ KARTY – RADOST NEBO STAROST?

**Jan Okrouhlý**

V roce 2008 jste se mohli na ranči Malevil při workshopu detailně obeznámit s tím, co obnáší současný standard platebních karet a kam míří technologie platebních karet. Trendům v oblasti platebních karet se ostatně věnovala v roce 2010 též přednáška v Maxičkách. Dnes jsou tehdy avizované bezkontaktní platby již všudypřítomnou realitou. Každý výrobce telefonů, tabů či padů již podporuje NFC a na trhu jsou tak k dispozici desítky přístrojů s touto technologií. V mnoha klientech bank však dosud přetrvává jistá nedůvěra v bezkontaktní technologii. Často mají obavy, jak ze ztráty prostředků na svých účtech, tak ze skimmingu či scanningu (nevyžádaného čtení informací o držiteli karty). Proto bychom rádi navázali na předchozí přednášky a uvedli aktuální informace a více detailů o současných technologiích plateb u obchodníků samozřejmě s primárním zaměřením na bezkontaktní platby a bezpečnost. V roce 2008 jste se mohli na ranči Malevil při workshopu detailně obeznámit s tím, co obnáší současný standard platebních karet a kam míří technologie platebních karet. Trendům v oblasti platebních karet se ostatně věnovala v roce 2010 též přednáška v Maxičkách. Dnes jsou tehdy avizované bezkontaktní platby již všudypřítomnou realitou. Každý výrobce telefonů, tabů či padů již podporuje NFC a na trhu jsou tak k dispozici desítky přístrojů s touto technologií. V mnoha klientech bank však dosud přetrvává jistá nedůvěra v bezkontaktní technologii. Často mají obavy, jak ze ztráty prostředků na svých účtech, tak ze skimmingu či scanningu (nevyžádaného čtení informací o držiteli karty). Proto bychom rádi uvedli aktuální informace a více detailů o současných technologiích plateb u obchodníků. V roce 2008 jste se mohli na ranči Malevil při workshopu detailně obeznámit s tím, co obnáší současný standard platebních karet a kam míří technologie platebních karet. Trendům v oblasti platebních karet se ostatně věnovala v roce 2010 též přednáška v Maxičkách. Dnes jsou tehdy avizované bezkontaktní platby již všudypřítomnou realitou. Každý výrobce telefonů, tabů či padů již podporuje NFC a na trhu jsou tak k dispozici desítky přístrojů s touto technologií. V mnoha klientech bank však

dosud přetrvává jistá nedůvěra v bezkontaktní technologii. Často mají obavy, jak ze ztráty prostředků na svých účtech, tak ze skimmingu či scanningu (nevyžádaného čtení informací o držiteli karty). Proto bychom rádi navázali na předchozí přednášky a uvedli aktuální informace a více detailů o současných technologiích plateb u obchodníků samozřejmě s primárním zaměřením na bezkontaktní platby a bezpečnostní přednáška v Maxičkách. Dnes jsou tehdy avizované bezkontaktní platby již všudypřítomnou realitou. Každý výrobce telefonů, tabů či padů již podporuje NFC a na trhu jsou tak k dispozici desítky přístrojů s touto technologií. V mnoha klientech bank však dosud přetrvává jistá nedůvěra v bezkontaktní technologii. Často mají obavy, jak ze ztráty prostředků na svých účtech, tak ze skimmingu či scanningu (nevyžádaného čtení informací o držiteli karty). Proto bychom rádi navázali na předchozí přednášky a uvedli aktuální informace a více detailů o současných technologiích plateb u obchodníků samozřejmě s primárním zaměřením na bezkontaktní platby a bezpečnostní samozřejmě s primárním zaměřením na bezkontaktní platby a bezpečnostní aspekty.

Přednáška nejprve osvěží informace o kontaktním rozhraní (EMV), aby bylo možné názorně ukázat rozdílný způsob zpracování a komunikace při použití bezkontaktního rozhraní definovaného asociacemi VISA PayWave a MasterCard PayPass. Zjistíte tak za jakou cenu dosahuje jedna z asociací dvojnásobnou rychlost odbavení komunikace s kartou a jakým způsobem se tak technologie těchto asociací vzájemně odklání. Aby bylo možné platit i v jiných částech světa, kde čipové technologie nejsou používány, vznikly též obchodně nezbytné technologické odbočky v podobě MasterCard PayPass Mag Stripe a VISA MSD, bez kterých se naše karty neobejdou. Přítomnost těchto technologií vnáší další dimenzi a proto bude následovat sumarizace, v níž se dozvíte např. jak se liší tradiční platební karty od stickerů/samolepek a NFC a také jak záleží na tom, v které geografické lokalitě, resp. jakým terminálem je platba uskutečněna. Pro jednotlivé varianty se dále budeme soustředit na bezpečnostní aspekty každé s nich a ukážeme si, jakým způsobem asociace a banky chrání své klienty, resp. nás koncové zákazníky, při bezkontaktních platbách. Vysvětlíme si, jak je to s ověřováním držitele karty s PIN, bez PIN, limity plateb a jejich offline či online vyhodnocování, rychlostech odbavení atp. Na závěr se zaměříme na časté otázky a mýty, které kolem bezkontaktních plateb kolují. Ukážeme dosud možná nepřiliš známé způsoby zneužití a způsobech ochrany. Technologicky zajímavým doplňkem pak může být případová studie o použití bezkontaktních karet v Londýnském dopravním systému.

**Jan Okrouhlý** – JAN.OKROUHLY@HP.COM

Ing. Jan Okrouhlý (\*1972) vystudoval Katedru informatiky a výpočetní techniky Fakulty aplikovaných věd Západočeské Univerzity v Plzni. Po vystudování pracoval v tamním Centru informatiky a výpočetní techniky na rozličných IT projektech. Od roku 2005 je zaměstnán jako technologický konzultant v Hewlett-

Packard Praha. Jan se specializuje na projekty vydávání a akceptace čipových platebních karet, dále se věnuje infrastrukturní bezpečnosti, programování ve skriptovacích jazycích a kromě ženy s dětmi má nejraději Unix.

## ZABEZPEČENÍ 3D-SECURE PŘI PLATBĚ NA INTERNETU

**Martin Zich**

V dnešní době je placení kartami mnoha českých bank při eCommerce transakcích na Internetu zabezpečeno jen do určité míry. Držitelé karty stačí k provedení platby pouze tři údaje a to číslo karty (PAN), datum expirace a CVV2/CVC2 kód, který je k dispozici na zadní straně každého z „plastů“. To s sebou přináší rizika ve 2 rovinách:

- Držitel karty nemá žádnou jistotu, že v případě ztráty nebo zcizení karty nedojde k jejímu zneužití na Internetu. Všechny potřebné údaje jsou totiž dostupné přímo na kartě samotné a to komukoliv, kdo ji zrovna drží v ruce nebo se mu podařilo nějakým způsobem tištěné údaje uchovat.
- V případě mezibankovních vypořádání reklamovaných transakcí (tzv. „chargeback“), prohrává spor o jejich hrazení vždy vydavatel, jehož platební karty nejsou zabezpečeny např. pomocí 3D-Secure nebo jiné adekvátní služby. Náklady reklamovaných transakcí jdou pak vždy na vrub finančního ústavu a co hůře, nyní se jednotlivými roky stále rapidně zvyšují.

Řešit popsaný problém je možné zavedením mezinárodně uznávané služby 3D-Secure podporované hlavními hráči na tomto trhu (VISA, MasterCard). 3D-Secure na straně vydavatele karet spočívá v implementaci autentizační vrstvy před v současnosti provozované řešení. Držitelova identita je tak spolehlivě ověřena jedním z vybraných způsobů a při následném zadání karetních údajů tak existuje mnohem větší jistota, že platební brána komunikuje přímo s osobou, která je vlastníkem použité karty.

Bankovní ústavy v České republice se rozhodly v posledních letech na toto řešení přejít. Způsobů zavedení je však několik a celý projekt integrace podobné služby dovnitř rozlehlelé banky neznamená zdaleka jen zapnutí jednoho boxu, který ověřuje klienty při provádění plateb. To, jak rozsáhlý takový projekt může být a co všechno skýtá za úskalí, se též pokusí osvětlit tato přednáška.

Některé banky tvrdí a propagují, že mají ověření pomocí 3D-Secure kompletně zavedeno, ale pokud dojde k vlastní platbě na jejich platební bráně, k žádnému ověření přesto ve Vašem případě nedojde. Jak je to možné? Je totiž nutné rozlišovat zavedení 3D-Secure pro tzv. Issuing a tzv. Acquiring. Pro plnou funkčnost musí být k dispozici obě části této služby.

Zavedení 3D-Secure znamená postupný nárůst počtu klientů využívajících tuto službu. Způsoby, jak dosáhnout pokrytí všech klientů té které banky je několik. Pro velký finanční ústav disponující desítkami i stovkami tisíc klientů není tento „náběh“ nic triviálního. Pro tento účel se kromě jiných opatření využívají definované stavy, které jsou mnohdy ve „front-end“ systémech viditelné i klientům („Not Enrolled“, „Semi-Enrolled“, „Enrolled“ atd.). Jde pak o to, definovat scénáře a způsoby, jak klienty mezi těmito stavy vhodně přesouvat a zajistit jim tak plně funkční službu s potřebnými parametry. Velmi vhodným způsobem se jeví tzv. aktivace během nákupu („Activation During Shopping“), kdy je klient přidán do systému během provádění první ověřované platby. Je však možné ho nutit ihned službu využívat? Mnohdy k ní bude potřebovat další nástroje (viz následující odstavec) a nebylo by příliš vhodné blokovat mu v takovém případě provádění elektronických plateb. I k tomuto problému existují vhodné způsoby řešení, které byly v rámci 3D-Secure projektů nasazeny.

Klient provádějící platbu může být v zásadě ověřován několika způsoby. První z nich je ten nejjednodušší a to pomocí statického hesla. S tím je spojeno množství problémů jeho správy, a proto se dnes volí daleko hladší způsob ověření pomocí SMS kódů přes síť GSM. To však nejsou jediné způsoby, které se při zavedení 3D-Secure služeb zvažovaly. Ty méně známé, ale velmi zajímavé, např. pro budoucí použití ve spojení s dalšími službami, mohou být systémy CAP-DPA, které využívají speciální kapesní čtečky karet nebo které jsou přímo integrovány do samotné platební karty („Display Cards“ / „Code Secure“).

Při použití CAP/DPA jsou generována „jednorázová hesla“ (tzv. tokeny). Jedná se o vícefaktorovou autentizaci, při které musí mít uživatel k vygenerování jednorázového hesla k dispozici platební kartu a její PIN. Karty většinou generují tokeny o délce 9, když na sobě mají kromě platebních aplikací např. pro VISA, MasterCard, JCB apod. personalizovanou i separátní aplikaci právě pro CAP/DPA. Je však vhodné dát klientům tento kapesní způsob použití platební karty? Pokud Vás někdo přepadne, vezme Vám platební kartu a bude chtít vědět její PIN, bude mít i možnost přímo si ověřit jeho správnost i bez nutnosti složitě shánění čtečky podobného typu. V tomto nastavení jí totiž bude vlastnit téměř každý, kdo u sebe bude mít i související kartu. Ověřit správnost PIN lze dnes především u bankomatů, kde jsou však ve všech případech instalovány kamerové systémy. Není také příliš vhodné ztratit kartu s čtečkou, na které jsou vmačkána pouze 4 tlačítka. Pravděpodobnost uhodnutí kódu PIN se pak přeci jen značně zvyšuje. Je otázkou, zda se také v případě GSM jedná o ideální řešení, které je velmi závislé právě na dostupnosti mobilního telefonu a také schopnosti jeho ochrany před případnou manipulací prohlížeče i SMS kódu, pokud obojí provozujete na dnešních „chytrých“ telefonech. Takové i další problémy jsou v podobném projektu intenzivně řešeny a hodnocena případná rizika.

České banky dnes službu 3D-Secure nabízí a to v různých verzích a nastaveních. Přednáška si klade za cíl i zmapování současného stavu včetně dosud zná-

mých plánů do blízké budoucnosti. Jde také o zhodnocení skutečné „bezpečnosti“ a použitelnosti 3D-Secure a také potřebné použitelnosti řešení pro eCommerce platby, které jsou dnes využívány skutečně velkou masou současných držitelů platebních karet vydaných těmi největšími finančními ústavy v ČR.

**Martin Zich** – MARTIN.ZICH@HP.COM

Martin Zich nyní pracuje ve společnosti Hewlett-Packard Česká republika, do které nastoupil v září 2008 jako technologický konzultant. Jeho rolí je práce na množství různorodých projektů týkajících se bezpečnosti a proměn infrastruktury. Jeho rolemi jsou především konkrétní technické dodávky jednotlivých projektů, jejich management nebo celková koordinace. Pro příklad lze uvést práci na rozsáhlých projektech týkajících se problematiky Contactless, eCommerce, DLP nebo PCI-DSS. Před nástupem do HP studoval na Českém vysokém učení technickém v Praze, které dokončil v roce 2009. Studoval také na technické univerzitě DTU v dánské Kodani a to zejména kryptologii, kryptografii a datovou bezpečnost. Během svých studií pracoval pro malé a středně velké firmy, kde poskytoval outsourcingové služby a dále publikoval do několika technických magazínů.

## JAK UDĚLAT BANKU

### Václav Votípka

Internetové bankovníctví zná dnes téměř každý. Jsou lidé, kteří si podle něj vybírají svoji banku. I když je Internetové bankovníctví z IT pohledu jistě zajímavá aplikace, uvnitř banky najdeme spoustu dalších (běžnému klientovi skrytých) aplikací. Během přednášky si ukážeme, co vše (z pohledu IT) banka pro svoje fungování potřebuje. Budeme se zabývat nejen systémy pro samotné zpracování transakcí ale i aplikacemi pro různé komunikační kanály, získávání a obsluhu klientů, podporu manažerského rozhodování atd.

U každého systému probereme specifické nároky, které jsou na něj kladené a způsoby jeho integrace s okolními systémy.

**Václav Votípka** – VACLAV.VOTIPKA@ARBES.COM

Pracuje ve společnosti ARBES Technologies jako SW architekt v divizi bankovních systémů. Účastnil se nasazení bankovního systému ARBES OBS do 14 bankovních i nebankovních institucí v sedmi různých zemích. Vystudoval SW inženýrství na Fakultě Aplikovaných Věd ZČU.

## INTERNÍ VÝVOJ BANKOVNÍHO SYSTÉMU

**Adrian Kantor**

V protikladu outsourcingu, externím dodavatelům a integrátorům stojí dnes trochu opomíjený interní vývoj. V případě velkého systému se, kromě zřejmých rozdílů ve vývoji, projeví v provozu systému důsledky, které nejsou na první pohled patrné.

Příspěvek na jednom konkrétním příkladu ukazuje postupy, které osvědčily. Není zaměřen na konkrétní technologie, ale spíše se zamýšlí nad otevřeností systémů z pohledu skutečných koncových uživatelů, kteří rozhodně nejsou IT odborníky. Filozofii UNIXu lze totiž aplikovat i na celou firmu.

**Adrian Kantor** – ADR@FIO.CZ

Ve Fio začal pracovat v roce 1997 jako vývojář, nyní je ve Fio bance zástupcem vedoucího IT a vedoucím pražského vývojového týmu. V bance se věnuje vývoji backendu, jeho napojením na třetí strany a vývojem interního frontendu.

SLUŽBA SLEDOVÁNÍ INFRASTRUKTURY A IP PROVOZU SÍTĚ PRO UŽIVATELE  
E-INFRASTRUKTURY CESNET**Tomáš Košnar**

V rámci budování a rozvoje e-infrastruktury CESNET vyvíjíme nástroje pro souvislé a plošné sledování její technologické infrastruktury (systém G3) i jejího IP provozu (systém FTAS). Tyto nástroje jsou schopny poskytnout v interaktivním nebo semi-interaktivním režimu detailní i přehledové informace o stavu, chování a trendech v e- nfrastruktuře, ale i detekovat, aktivně oznamovat a vizualizovat neočekávané dynamické jevy, překročení nastavených mezních hodnot a některé typy síťových útoků. Architektura obou monitorovacích systémů umožňuje jejich využití v lokálním, metropolitním i jakkoli jinak vymezeném specifickém prostředí – tedy i v sítích koncových uživatelů. Přednáška bude zaměřena na možnosti a příklady poskytnutí monitorovacích a analytických služeb uživatelům prostřednictvím těchto systémů.

**Tomáš Košnar** – KOSNAR@CESNET.CZ

Absolvent Elektrotechnické fakulty ČVUT v oboru telekomunikační technika. Od roku 1988 pracoval jako vývojový pracovník v TESLA VÚT. Od roku 1990 jako správce fakultní sítě na Elektrotechnické fakultě ČVUT v Praze Dejvicích. Od roku 1996 pracuje částečně, od roku 2000 plně pracuje ve sdružení CESNET, z.s.p.o. Specializuje se na návrh, vývoj a provozování systémů pro sledování infrastruktury a IP provozu sítí.

## VÝKONNOSTNÍ A FUNKČNÍ TESTY SOUBOROVÝCH SYSTÉMŮ PRO CLOUD

**Filip Hubík**

Distribuované či sdílené souborové systémy jsou v dnešní době nedílnou součástí moderních datacenter. Jedná se o systémy, které jsou svou strukturou odolné, rychlé, škálovatelné, propustné a často vysoce dostupné. Mají řadu výhod. Při výpadku určité části clusteru nemusí dojít přímo k pádu celého úložiště („No Single-Point-of-Failure“), systém může také zavádět redundanci dat, automatické vyvažování zátěže všech dostupných serverů, objektové úložiště, umožňovat paralelní práci s daty apod.

Pro optimální provoz cloudových služeb je třeba důsledně volit veškeré součásti infrastruktury, souborový systém nevyjímaje. V prostředí open source můžeme dnes vybírat z několika desítek kandidátů, které vyhodnocujeme dle provozovaných služeb a potřeb datacentra. Z širokého spektra vybereme současné lídry v oboru – souborové systémy Ceph a GlusterFS. Za oběma stojí jak silná komunita, tak velké IT společnosti, které se snaží prosadit v konkurenci právě svůj projekt.

Cílem přednášky je představit vlastnosti a srovnat souborové systémy nejen po stránce výkonnostní, ale také po stránce vhodnosti použití v cloudovém datacentru. Je třeba také zhodnotit kompatibilitu se současnými virtualizačními technologiemi či vhodnost použití s určitými typy cloudových služeb či middlewaru (OpenNebula, OpenStack).

**Filip Hubík** – HUBIK@ICS.MUNI.CZ

V roce 2013 dokončil magisterské studium na fakultě informatiky VUT v Brně. Od roku 2011 pracuje jako systémový admin při CESNETu a Masarykově univerzitě se zaměřením na cloud computing. Zajímá se o distribuované počítání, linuxové distribuce, programování a umělou inteligenci. Žije v Brně. Ve volném čase běhá, baví ho zimní sporty, americké seriály, hra na violu a folklor.

## ZFS A BTRFS V PRAXI

**Jan Krčmář**

Už Vás unavuje řešit nafukování úložišť přes archaické nástroje a následné rozšiřování souborového systému, při kterém se musíte vždy pokřivořit? Pojdte to zkusit s moderními COW filesystemy. Jejich nasazením můžete získat stabilitu, škálovatelnost, redundanci a v neposlední řadě jednoduchou správu. Představíme si základní principy, pokročilé vlastnosti a některé výhody těchto souborových systémů, které mají oproti svým starším kolegům. Nakonec se zkusíme podívat, jestli jsou tyto moderní přístupy opravdu v praxi použitelné a jak daleko je to s jejich implementací a vývojem.



**Jan Krčmář** – HONZA801@GMAIL.COM

Vystudoval na Západočeské Univerzitě v Plzni obory Informatika a Kybernetika. Jeden z jeho hlavních koníčků je počítačová virtualizace. S tím je úzce spojen i jeho zájem o souborové systémy. Ve svém současném zaměstnání, ČD Informační systémy, nasadil a již několik let úspěšně používá ZFS na operačním systému FreeBSD.

## DOHLED NAD (NEJEN) IT PROSTŘEDÍM POMOCÍ PRTG

**Martin Couf**

Potřebujete nepřetržitě něco měřit? Přejete si kdykoliv vidět aktuální i historická data? Chcete být okamžitě informováni o výpadku či kritickém stavu? PRTG Network Monitor od společnosti Paessler je špičkovým řešením pro monitorování nejen IT systémů, ale ve spojení s vhodnými senzory je skvělým nástrojem i pro sledování jiných veličin, potažmo řízení souvisejících systémů. Na skutečných příkladech ukážeme, jak lze PRTG profesionálně využít v IT i ve vědě, a podělíme se o naše několikaleté zkušenosti s tímto produktem.

**Martin Couf** – MARTIN.COUF@WHITESOFT.EU

Přednášející vystudoval PřF UK v Praze se specializací na molekulární genetiku člověka, kde poté pracoval 5 let jako asistent na katedře vývojové biologie a imunologie. V roce 2001 nastoupil jako třetí zaměstnanec do česko-belgické IT společnosti Whitesoft, ve které v současnosti pracuje jako technický ředitel a šéf pražské pobočky zaměřené na IBM software. Mezi jeho záliby patří hraní si na písku a sběratelství historických sad LEGO.

## ZÁTĚŽOVÉ TESTOVÁNÍ ANEB „SAKRA, KDO TO BUDE PLATIT“

**Ján Hrabik**

Přednáška pojednává o finančních aspektech zátěžového testování a možnostech návratnosti provádění ZT v závislosti na zvolené technologii a SW. Hlavní část přednášky je o poukázání na skutečnosti, které vedou k volbě efektivního řešení pro vykonání ZT, tedy nejen volba SW, ale i vhodnost infrastruktury pro testování a různá rizika, která se zde mohou skrývat.

**Ján Hrabik** – JHRABIK@TRASK.CZ

Absolvent oboru aplikovaná informatika na Univerzitě Hradec Králové. IT specialista od roku 1998, specializace na zátěžové a automatizované testování s nástroji IBM a HP. V současnosti pracující na volné noze pro společnost Trask Solutions. Mezi zajímavé projekty v oblasti ZT bych rád uvedl ZT pro Škoda Auto nebo Český statistický úřad.

## JAK BYLA (NE)OBJEVENA POSLEDNÍ PLANETA

**Pavel Najser**

Příběh takřka detektivní o objevu poslední planety Sluneční soustavy, s přihlédnutím k tomu, že každá ze vzdálenějších planet byla někdy tou poslední.

**Pavel Najser**

Vystudoval sociologii kultury na FSV UK. Od roku 1970 působí jako odborný pracovník Štefánikovy hvězdárny v Praze. Zabývá se dějinami vědy, především historií astronomie.

## PROGRAMOVACÍ TECHNIKY A ÚSKALÍ PŘI VÝVOJI SW V AUTOMOBILOVÉM PRŮMYSLU

**Martin Butnikošarovski**

Tématem tohoto příspěvku je nástin postupů a programovacích technik používaných při vývoji SW v automobilovém průmyslu prezentovaný na příkladu vývoje SW automatických převodovek ve firmě ZF Engineering Plzeň, s. r. o.

V úvodu představíme firmu ZF, její zaměření, produkty a zákazníky, pro které dodáváme automatické převodovky. V rámci úvodu bude taky předveden historický vývoj SW do automatických převodovek.

Hlavní obsah příspěvku se zabývá jednotlivými aspekty vývoje. V prvé řadě se zaměříme na důvody vzniku kvalitativních procesů při vývoji, včetně vysvětlení tzv. „V“ modelu. Dále se zaměříme na vliv finančně dostupného a kvalitního hardwaru na vývoj SW. Hlavní součástí příspěvku však bude volba programovacích jazyků (assembler, C/C++, Java), SW technik (design jednotlivých komponent, omezení v možnostech zvoleného jazyka) a pravidel pro psaní kódu (externí nástroje na statickou, dynamickou kontrolu kódu), který je bezpečný a dostatečně robustní.

Cílem příspěvku je seznámit posluchače s problematikou vývoje softwaru v tzv. uzavřených (embedded) systémech, které se vyskytují v automobilovém průmyslu. A také ukázat odlišnosti od „běžného“ vývoje SW s důrazem na omezení, rychlost a bezpečnost SW, jenž musí být dodán.

**Martin Butnikošarovski** – MARTIN.BUTNIKOSAROVSKI@ZF.COM

Je absolventem Přírodovědecké fakulty Univerzity Palackého v Olomouci obor Matematika a její aplikace. Pracuje ve firmě ZF Engineering Plzeň, s. r. o., kde začínal jako SW developer, v současnosti působí na pozici SW Safety Engineer for embedded systems.

## SQL VČERA A DNES

**Petr Jiroušek**

Asi každý už někdy tuto zkratku slyšel. Když se v sedmdesátých letech začaly objevovat první relační databáze, vznikla potřeba nějakého mechanismu, který by uměl s uloženými daty nějakým jednoduchým způsobem manipulovat. A tak vzniká první tzv. dotazovací jazyk SEQUEL. Postupně se tato zkratka poněkud smrškla na pouhé SQL. Asi nejnámějším standardem v této oblasti je standard ANSI SQL-92, který obsahuje základní sadu příkazů typu select, update, insert, delete atd., které asi většina z nás dá bez mrknutí oka dohromady. Ale od té doby již vyšlo několik dalších standardů a jazyka SQL a mnohé dnes může i překvapit, co všechno se pod touto třípísmennou zkratkou skrývá.

**Petr Jiroušek** – PETR@CIV.ZCU.CZ

Vystudoval Fakultu aplikovaných věd Západočeské univerzity v Plzni (ZČU), obor Kybernetika a řídicí technika. Od roku 1993 pracuje na ZČU, Centrum informatizace a výpočetní techniky, Středisko informačního systému (CIV-SIS). V současné době je vedoucím skupiny projektující informační systémy. Zabývá se administrací databází a vývojem databázových aplikací, je projektovým managemerem informačního systému studijní agentury vysokých škol IS/STAG.

## VIZUALIZACE DAT A FRAMEWORK D3.JS

**Karel Minařík**

Vizualizace dat je čím dál důležitější disciplína, vzhledem k rostoucímu množství množství dat, které zpracováváme, a zvyšující se sofistikovanosti a přístupnosti softwarových nástrojů.

V přednášce si krátce představíme historii a kontext vizualizace dat, a budeme se věnovat v současnosti dominantnímu frameworku D3.js (<http://d3js.org>) pro tvorbu sofistikovaných a interaktivních vizualizací. Projdeme si významné příklady vizualizací a aplikací ze světa i České republiky zpracovaných jeho pomocí, a na praktických ukázkách si demonstrujeme jeho základní princip: tzv. „data join“, vazbu mezi daty a grafickými elementy.

Posluchači by si měli odnést pochopení toho, proč se framework D3.js stal dominantním, proč se vyplatí vytvářet vizualizace „na zelené louce“, místo slepého využívání předpřipravených komponent, a odkazy na zdroje k dalšímu studiu.

**Karel Minařík** – KARMI@KARMI.CZ

Je návrhář a vývojář webových aplikací a Ruby programátor. Od roku 2012 pracuje ve společnosti Elasticsearch B.V. na Ruby, Rails a Chef integracích a interních nástrojích. Žije v Praze.

## DATABÁZOVÝ KYBERZLOČIN JE NA VZESTUPU! JAK SE MU BRÁNIT?

**Jan Musil**

Na úvod přednášky bude technicky představeno řešení InfoSphere Guardium, které poskytuje neinvazivní architekturu pro monitorování a audit práce uživatelů s databázemi a jinými zdroji dat v reálném čase. Řešení je v souladu s důležitými standardy databázové bezpečnosti (SOX, PCI, NIST, STIG a další) a podporuje všechny hlavní databázové platformy včetně nestrukturovaných úložišť dat, jako jsou například NoSQL databáze. Pro všechny tyto zdroje dat má řešení předpřipravené testy pro vyhodnocení zranitelnosti systému, což je nedílná součást plné ochrany dat.

V praktické ukázce budeme demonstrovat, jak se monitoruje přístup uživatelů k systému a datům a prostřednictvím databázového firewallu nastavíme aktivní prostředky, které zabrání přístup a manipulaci s citlivými daty jak ze strany privilegovaných, tak ze strany vybraných „normálních“ uživatelů. Dále budeme simulovat některé typy útoků a řešení použijeme pro demonstraci toho, jak tyto útoky včas odhalit a případně jim preventivně zabránit. Kromě jiného také prokážeme, že řešení je nezávislé na zranitelném nativním databázovém auditu a ani privilegovaní uživatelé nemají možnost manipulovat s auditními záznamy.

**Jan Musil** – MUSIL@CZ.IBM.COM

Přednášející vystudoval Fakultu jadernou a fyzikálně inženýrskou na ČVUT v Praze. Po ukončení studia v roce 1989 začal pracovat jako administrátor a programátor databázové technologie Informix nejprve ve státní správě a pak v soukromém sektoru. V roce 1996 nastoupil do zastoupení firmy Informix Software, kde pracoval jako team leader technické podpory pro Českou a Slovenskou republiku. V souladu s akvizicí společnosti se stal v roce 2002 zaměstnancem IBM Česká republika, kde pracuje doposud jako technická podpora prodeje produktové řady Informix, Guardium a Optim. Na starosti má region Střední a Východní Evropy a Ruska. Je ženatý a má tři děti.

Pozvánka na 45. konferenci EurOpen.CZ, 5.–8. 10. 2014

© 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](mailto:servis@vydavatelskyservis.cz)

Tisk: TYPOS, Tiskařské závody, s. r. o.  
Podnikatelská 1160/14, Plzeň