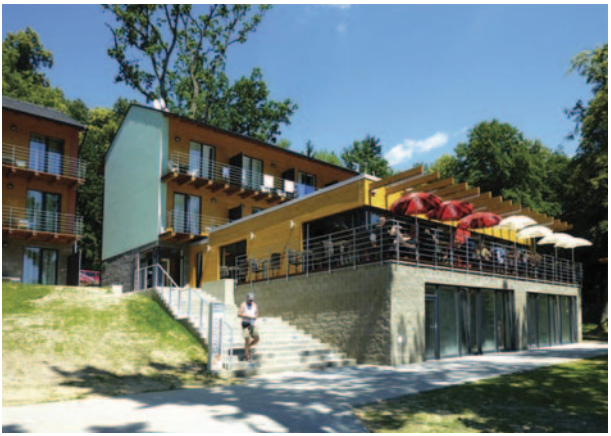
Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

43. konference



Penzion Gaudeo
29. září–2. října 2013

Slovo úvodem

Podzimní konference

Nadcházející verze konference Europen se zaměřením na praktickou bezpečnost pro vývojáře, administrátory a výzkumníky je za dveřmi – naposledy jsme se věnovali bezpečnosti v povznášejícím prostředí kláštera Želiv v roce 2011 a tentokrát se přesuneme na vranovskou pláž. Opět jsme pro vás připravili pestrou směs příspěvků, které pokryjí problematiku analýzy malwaru a jeho výskytu na mobilních zařízeních, netradičních kryptografických implementací a jejich optimalizací, využití a modifikace diskového šifrování, vyhýbání se síťové detekci a automatickém testování aplikací. Pro potěchu nejen bezpečnostních mozkových závitů pak přijde téma astrofotografie. Jako ochutnávku vám níže představíme část z nich, pro plné menu pokračujte ve čtení i po tomto úvodu.

Každý den vznikají tisíce nových variant virů díky jejich automatickým generátorům. Na chytání běžných virů máme antivirové programy a doufáme, že jejich automatické analýzy nás dostatečně ochrání. Co když ale někdo napsal virus speciálně pro naši firmu, jak se už kdysi dávno (90. léta) stalo třeba švýcarské bance UBS? Můžeme i v tomto případě spoléhat na pomoc antivirů? A řeknou nám, kam byla poslána data z našich serverů? Ne vždy je odpověď kladná a někdy nám nezbude než nažhavit disassembler a podívat se zachycenému viru na zoubek osobně. Jak na to nám ukáže Vašek Lorenc v nedělním tutoriálu s názvem „Praktický disassembling malwaru“.

Pondělní program se zaměří především na bezpečnost mobilních zařízení. Začneme zvanou přednáškou Petra FPL Odehnala o současných virových hrozbách na mobilních platformách a jak se jim bránit. Základní bezpečnostní mechanismus Androidu – oprávnění – představí Juraj Varga, včetně útoku, kterým lze současný ochranný mechanismus obejít. Zisk citlivých informací z mobilního zařízení – tentokrát z platformy Apple iOS – nám představí Eugen Antal. Po obědě nás čeká srovnání výpočetních možností různých platforem kryptografických karet (JavaCard, Multos, .NET) pro potřeby méně tradičních kryptografických operací, včetně porovnání s platformou Android, od Jana Hajného. O možnostech zabránit útočníkovi získat používaný šifrovací klíč i v případě, že během šifrování může pozorovat vykonávané instrukce i používanou paměť, nám prozradí něco více Dušan Klinec. Aleš Padrta nás zasvětí do problematiky ukládání a mazání dat na SSD discích včetně praktických výsledků. Těsně před večeří se od Marka Sýse dozvíme něco o tom, jak rychlostně optimalizovat numerické operace používané typicky v kryptografických algoritmech.

Navečer nás čeká mentální a vizuální výlet opravdu hodně daleko a hluboko – Petr Švenda v kabátě astrografa nám ukáže temná zákoutí moderní astrofotografie s digitálními zrcadlovkami, počítačovou honbu za využití každého zachyceného fotonu a boj s neklidnou atmosférou. Kromě pěkných astrofotografií se nás

ale pokusí přesvědčit, že tato oblast je přístupnější než kdykoli předtím a pokud to počasí dovolí, budeme mít možnost si popsané postupy vlastoručně vyzkoušet pod hvězdnou oblohou. (Fotoaparáty s sebou – a na kvalitě záleží!)

Úterní program bude věnován šifrování dat na disku a zahájí jej přednáška Dana Rosendorfa na téma novinek v programu Bitlocker s přihlédnutím ke změnám souvisejícím s OS Windows 8. S upozorněním na možné problémy open-source nástroje TrueCrypt a návrhem řešení založeného na kombinaci s dedikovaném hardwaru nám představí Martin Kákona. Detailní popis fungování nástroje TrueCrypt a možnosti jeho využití v nástroji cryptsetup nám ukáže Milan Brož. Po obědě nás čeká zajímavá a pro většinu i náročná a napínavá práce v sekcích.

Ve středeční části nás čekají dvě zvané přednášky. Juraj Michálek, všestranně nadaný komunikátor nám ukáže možnosti skriptovacího prostředí PowerShell pro MS Windows z pohledu uživatele *nixu pro automatické testování softwarových aplikací. Ve druhé přednášce nám Marián Novotný ukáže zkušenosti jak se vyhýbat síťové detekci, které načerpal v rámci vývoje nástroje pro detekci průniku.

Co se týká práce v sekcích, nejlépe Vás navedou stránky „domovského“ penzionu http://www.penzionygaudeo.cz a záložka „Tipy na výlet“. Je zde i zajímavý tip „Za vínem na Znojemsku“.

Zamyšlení na závěr...

Ve slově závěrem před dvěma lety v Želivě jsme si položili obtížné otázky – lze si uchovat alespoň nějakou bezpečnost na počítači napadeném mlawarem (čím dál více je tímto počítačem náš telefon s Androidem)? Jak vysvětlit babičce, aby neklikala na podvodné maily (výzkum ukazuje, že starší lidé jsou jednoduše více důvěřiví)? Kolik vašich kamarádů už konečně používá šifrování disku?

Zaznamenali jsme nějaký vývoj v těchto otázkách? A byl tento vývoj pozitivním směrem? A do jaké míry mohou situaci ovlivnit velmi dobře vzdělaní a zodpovědní vývojáři? A přispěje k tomu tato konference?

Opět nás čekají nejen denní, ale i noční diskuze na všemožná témata během podzimního bezpečnostního Europenu.

Za programový výbor se těší

Petr Švenda

Programový výbor

Vašek Matyáš (předseda, Masarykova univerzita v Brně)
Petr Hanáček (Vysoké učení technické v Brně)
Ondřej Krajíček (Y-Soft Corporation, a. s.)
Marek Kumpošt (Masarykova univerzita v Brně, NetSuite Czech Republic, s. r. o.)
Marián Novotný (ESET, spol. s r. o.)
Josef Pojsl (Trusted Network Solutions, a. s.)
Zdeněk Říha (Masarykova univerzita v Brně)
Roman Štěpánek (SODATSW, spol. s r. o.)
Petr Švenda (Masarykova univerzita v Brně)

Program

Neděle 29. 9. 2013

13.00	Tutoriál: Praktický disassembling malwaru	*Václav Lorenc*

Pondělí 30. 9. 2013

9.00	Oficiální zahájení	*Vashek Matyáš*
9.05	Zvaná přednáška: Virové hrozby na mobilních platformách a jak se jim bránit	*Petr Odehnal*
10.30	Přestávka	
10.55	Exploiting missing permission in Android	*Juraj Varga, Martin Gazdík*
11.40	Techniky získavania citlivých údajov z Apple iOS zariadení	*Eugen Antal, František Baranec*
12.30	Oběd	
14.00	Mobilní zařízení a jejich využití v současné kryptografii	*Jan Hajný*
14.55	Kryptografie v nedůvěryhodném prostředí	*Dušan Klinec, Petr Švenda*
15.50	Přestávka	
16.15	Uchovávání dat v SSD	*Aleš Padrta, Karel Nykles*
17.05	Optimalizace numerických operácií používaných pri šifrovaní	*Marek Sýs*
18.00	Večeře	
19.30	Zvaná přednáška: Astrofotografie	*Petr Švenda*

Úterý 1. 10. 2013

9.30	Šifrovací schéma BitLocker s přihlédnutím ke změnám ve Windows 8	*Dan Rosendorf*
10.25	Přestávka	
10.50	Může šifrování dat na přenosných počítačích ochránit EU proti průmyslové špionáži?	*Martin Kákona*
11.40	Šifrování disků a Truecrypt	*Milan Brož*
12.30	Oběd	
14.00	Práce v sekcích	
19.00	Večeře, diskuse, valná hromada	

Středa 2. 10. 2013

9.00	Zvaná přednáška: PowerShell z pohľadu *nix používateľa	*Juraj Michálek*
10.30	Přestávka	
10.55	Zvaná přednáška: Techniky vyhýbání se síťové detekci	*Marián Novotný*
12.25	Závěr	*Vashek Matyáš*
12.30	Oběd	

Konferenční poplatky

Vložné		
Platba	Tutoriál	Konference
Členové		
do 20. 9. 2013	690	2 300
po 20. 9. 2013	790	2 550
Nečlenové		
do 20. 9. 2013	790	2 600
po 20. 9. 2013	890	2 850
Ubytování a stravování		
od neděle 19. 9. 2013	2 250	od nedělní večeře do středečního oběda, 3 noclehy
od pondělí 30. 9. 2013	1 650	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 750 Kč na den (ubytování se snídaní 450 Kč na den, oběd 150 Kč, večeře 150 Kč).

Kapacita hotelu je zhruba 80 osob.

Kdy	Tutoriál se uskuteční v neděli 29. 9. 2013 od 13.00 hodin
	Konference začíná v pondělí 30. 9. 2013 v 9.00 hodin a končí ve středu 2. 10. 2013 cca ve 14.00 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Penzion Gaudeo http://www.penzionygaudeo.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	25. 9. 2013 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: Praktický disassembling malwaru

Václav Lorenc

V posledních letech se zlepšily možnosti i dostupnost programů pro pořízení obrazu a analýzu RAM, což vedlo ke změně zavedených postupů i usnadnění práce bezpečnostních týmů. Namísto vypínání počítačů se v některých případech pořizuje obraz paměti a provádí se jeho detailní analýza. Tutoriál bude zaměřený právě na artefakty, které se dají nalézt v paměti napadených počítačů, popis výhod, které tato metoda má proti klasické offline analýze či reverse engineeringu malware; to vše na systémech s Windows XP/7/8.

Během praktické části workshopu si účastníci na konkrétních příkladech a obrazech pamětí si vyzkouší praktickou analýzu bezpečnostních incidentů, od pořízení obrazu RAM až po sestavení závěrečného hlášení o nalezených artefaktech či zdrojích infekce. Pro účast na workshopu je třeba mít počítač schopný provozovat virtualizační program VirtualBox.

Václav Lorenc – vaclav.lorenc@honeywell.com
Pracuje ve společnosti Honeywell jako bezpečnostní analytik. Obvyklou náplní jeho práce je krom procházení Twitteru a pití kávy také reakce na počítačové bezpečnostní incidenty, s nimi spojená forenzní analýza napadených strojů a příležitostně i zkoumání zajímavých kousků malware.

Exploiting missing permission in Android

Juraj Varga, Martin Gazdík

Google Android is currently the most widespread mobile operating system. With growing number of mobile devices in daily use increases the amount of data stored on these devices. And since it is an open-source system, the number of possible exploits also grows. In this paper we focus on the main security mechanism in Android — the permission model. We present a simple way how to circumvent this security mechanism and how to get to user data stored on device. Moreover we propose a simple way to modify common antivirus applications to detect this form of attack.

Juraj Varga – juraj.varga@stuba.sk
Vyštudoval Fakultu elektrotechniky a informatiky na STU v Bratislave so zameraním na bezpečnosť informačných systémov. V súčasnosti je doktorandom na FEI STU a svoj výskum zameral na bezpečnosť mobilnej platformy Google Android. Okrem toho sa venuje aj využitiu mobilných zariadení ako zdrojov náhodnosti.

Martin Gazdík – gazdik.martin.87@gmail.com
Čerstvý absolvent Fakulty elektrotechniky a informatiky na STU v Bratislave so zameraním na bezpečnosť informačných systémov. V súčasnosti pracuje ako vývojár mobilných aplikácií na platforme Google Android.

Techniky získavania citlivých údajov z Apple iOS zariadení

Eugen Antal, František Baranec

Dnešné mobilné zariadenia, či už tablety alebo smartfóny, fungujú na moderných mobilných operačných systémoch. Počet takýchto zariadení neustále narastá a stávajú sa pre ľudí súčasťou ich každodenného života. S narastajúcim počtom narastá aj ich využiteľnosť a tým pádom aj ukladanie a spracovanie citlivých údajov.

Apple iOS zariadenia patria medzi najvýznamnejších predstaviteľov moderných mobilných zariadení.

Veľké množstvo citlivých údajov indikuje nutnosť ochrany týchto údajov. Operačný systém iOS sa prezentuje ako jedna z najbezpečnejších mobilných platforiem. V tomto príspevku sa venujeme možnostiam získavania citlivých informácií na mobilných zariadeniach od spoločnosti Apple Inc. bežiacich na mobilnom operačnom systéme iOS.

Eugen Antal – eugen.antal@stuba.sk
Tri roky pracoval ako vývojár mobilných aplikácií. V súčasnosti je doktorandom v odbore Aplikovaná informatika na Slovenskej technickej univerzite v Bratislave, kde sa špecializoval na bezpečnosť informačných systémov. Zaoberá sa lúštením nezlomených klasických šifier. Vo voľnom čase sa zaoberá bezpečnosťou mobilných platforiem a vývojom mobilných aplikácií.

František Baranec – baranecfrantisek@gmail.com
Čerstvý absolvent Aplikovanej informatiky na Slovenskej technickej univerzite v Bratislave. Zaujíma sa o bezpečnosť mobilných platforiem. Túto problematiku spracoval a popísal aj vo svojej diplomovej práci. Aktuálne pracuje ako iOS developer na voľnej nohe.

Mobilní zařízení a jejich využití v současné kryptografii

Jan Hajný

S nárůstem výkonu mobilních zařízení stoupá také jejich využitelnost v náročných kryptografických výpočtech. Zařízení jako jsou programovatelné čipové karty a smart-phony se stávají častou platformou pro implementaci kryptografických algoritmů a protokolů. Stále však existuje mnoho kryptografických aplikací, kde je výkon mobilních zařízení limitujícím faktorem. V příspěvku jsou

porovnány možnosti a analyzovány výsledky výkonových testů všech hlavních platforem programovatelných čipových karet (JavaCard, .NET, MultOS). Výsledky jsou srovnány s testy na zařízeních s OS Android. Výkon čipových karet a mobilních zařízení je pak analyzován s ohledem na aplikace v tzv. Privacy-Enhancing Technologies (PETs), tedy aplikace na ochranu soukromí a digitální identity. PETs aplikace jsou v příspěvku dále představeny především v souvislosti s výzkumem a vývojem schémat atributové autentizace vedeným na VUT v Brně.

Jan Hajný – HAJNY@FEEC.VUTBR.CZ, CRYPTO.UTKO.FEEC.VUTBR.CZ
Jan Hajný je absolventem magisterského a doktorského programu na Fakultě elektrotechniky a komunikačních technologií Vysokého učení technického v Brně. Jeho hlavním zaměřením je oblast návrhu kryptografických protokolů, které se dále věnoval na University of Aarhus v Dánsku a v rámci Fulbrightova programu na University of Minnesota v USA. Je členem IACR (International Association for Cryptologic Research) a je zakládajícím členem Cryptology Research Group na VUT v Brně. V současné době se věnuje mimo návrhu protokolů i jejich implementaci na čipových kartách a smart-phonech (iOS a Android).

Kryptografie v nedůvěryhodném prostředí

Dušan Klinec, Petr Švenda

Přednáška představí současný stav aplikovaného výzkumu v oblasti počítání v nedůvěryhodném prostředí (White-box Cryptography) – způsob, jak mohou být algoritmy jako např. AES být implementovány a vykonány v prostředí, které je plně pod kontrolou útočníka, ale úto. Díky speciální implementaci útočník ale nemůže získat hodnotu použitého kryptografického klíče. Budou probrány oblasti využití těchto speciálních implementací (DRM systémy, simulace asymetrické kryptografie, ...), existující návrhy publikované ve výzkumné literatuře a jejich praktické implementace včetně možných útoků vůči těmto schématům.

Dušan Klinec – XKLINEC@FI.MUNI.CZ
Je postgraduálním studentem na Masarykově univerzitě se zaměřením na praktickou i teoretickou bezpečnost širokého spektra aplikací počínaje bezdrátovými sensorovými sítěmi přes kryptografické čipové karty po speciální implementace šifrovacích algoritmů v nedůvěryhodném prostředí.

Petr Švenda – SVENDA@FI.MUNI.CZ
Pracuje jako výzkumník a učitel v oblasti počítačové bezpečnosti a aplikované kryptografie na Masarykově universitě. Zabývá se návrhem kryptografických protokolů pro prostředí s částečnou kompromitací (bezdrátové sensorové sítě), testováním i implementací bezpečnostních aplikací pro kryptografické čipové karty na

platformě JavaCard, vývojem nástrojů pro ochranu běhu softwarových aplikací a ve volném čase pak studiem EEG křivek z vlastního i cizího mozku.

Uchovávání dat v SSD

Aleš Padrta, Karel Nykles

Moderní paměťová média typu Solid State Drive (SSD) mohly dosáhnout svých skvělých vlastností pouze přechodem na jinou technologii než klasické pevné disky (HDD). Jiná technologie pochopitelně vykazuje jiné chování k ukládaným a mazaným datům, což má přímý vliv na objem smazaných dat dohledatelných v obrazu média. Přednáška mapuje interní mechanismy SSD, které ovlivňují zacházení s daty, od tranzistoru s plovoucím hradlem až po softwarové vlastnosti řadiče jako FTL, garbage collector a deduplikace/komprese dat. Také je rozebrána komunikace s OS pomocí protokolu TRIM a ovladače zařízení. Na závěr budou ukázány výsledky praktických experimentů.

Aleš Padrta – apadrta@civ.zcu.cz
Po magisterském a doktorském studiu 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., kde se zabývá vzděláváním uživatelů v oblasti bezpečnosti a od roku 2011 také pracuje na projektu forenzní laboratoře FLAB.

Karel Nykles – knykles@civ.zcu.cz
Po studiu na Fakultě aplikovaných věd Západočeské univerzity v Plzni začal v roce 2007 pracovat pro zdejší Centrum informatizace a výpočetní techniky jako systémový administrátor. Od roku 2011 pak pracuje také pro sdružení CESNET, z.s.p.o., v rámci projektu forenzní laboratoře FLAB.

Optimalizace numerických operácií používaných pri šifrovaní

Marek Sýs

Rýchle algoritmy sa aj v dnešnej dobe výkonných počítacov stále tešia eminentnému záujmu vo fakticky všetkých oblastiach informatiky. Obvzlášť je to patrné v oblasti kryptografie, kde sa spravidla vyžaduje využitie rýchlych numerických operácií používaných pri šifrovaní.

Prednáška si kladie za cieľ predstaviť základný prehľad vybraných a najčastejšie využívaných rýchlych algoritmov používaných v kryptografii. V prednáške bude kladený dôraz na jednoduchý a najmä vstrebateľný popis aj „zložitých algoritmov“ formou praktických ukážok.

Na záver prednášky je plánovaná voľná diskusia spojená s optimalizáciou vybraného algoritmu s využitím rýchlych algoritmov. Záujemci môžu zaslať návrh optimalizačného problému na nižšie uvedenú adresu.

Marek Sýs – SYSO@FI.MUNI.CZ
Pracuje ako výskumník v oblasti aplikovanej kryptografie na Masarykovej univerzite a ako učiteľ na Technickej univerzite v Bratislave. V súčasnosti sa venuje najmä klasickým homofónnym šifrám (Zodiac 340), mriežkam,LLL algoritmu a testovaniu náhodných postupností. V oblasti počítačovej grafiky sa venuje spracovaniu obrazu a jednoduchým fyzikálnym animáciam.

Astrofotografie

Petr Švenda

Poslední dekáda se nesla ve znamení výrazného zlepšení sensitivity snímacích čipů v digitálních fotoaparátech a zároveň jejich velkého rozšíření mezi běžné uživatele díky příjemné ceně. Obyčejný uživatel tak dostal možnost pořizovat snímky nočních astronomických objektů v takové kvalitě, která byla před 20 lety možná jen s velmi nákladnými zařízeními v profesionálních observatořích.

Oddychová přednáška představí postupy pro focení vesmírných objektů (planety, galaxie, emisní a reflexní mlhoviny, hvězdokupy, meteory, komety, rotace hvězd, Sluneční skvrny, ...) s využitím možností moderních digitálních zrcadlovek a pokročilého, přesto snadného počítačového zpracování pro dosažení nádherných snímků i velmi vzdálených a slabých objektů.

Zájemci jsou zváni také k přinesení vlastního fotografického vybavení – libovolný foťák, volitelně pak různé objektivy, stativ a automatická spoušť, pokud je vlastníte. Pokud počasí dovolí, můžeme vyzkoušet některé z popsaných technik po přednášce přímo v terénu.

Petr Švenda – SVENDA@FI.MUNI.CZ
Pracuje jako výzkumník a učitel v oblasti počítačové bezpečnosti a aplikované kryptografie na Masarykově univerzitě. Jediným volným časem na koníčky se stala noc a tak při focení usínající vesnice jednou nastavil závěrku na půl minuty a nejvyšší možné ISO, obrátil objektiv přímo vzhůru a následně nevěřícně přemýšlel o původu mlhavých obláčků mezi miliony hvězd, které zůstaly na tomto jediném snímku zachyceny. Od té doby tráví každou jasnou noc ve spacáku s pořád tou stejnou zrcadlovkou Canon 400D a fotí galaxie, mlhoviny, komety, hvězdokupy či planety a výsledky vystavuje na Astrolight.cz. Největším překvapením je pro něj fakt, že v dnešní době může každý s běžným vybavením a trochou trpělivosti pořídit snímky doposud těžko přístupné krásy vesmíru.

Šifrovací schéma BitLocker s přihlédnutím ke změnám ve Windows 8

Dan Rosendorf

Podáme krátký přehled fungování šifrovacího systému BitLocker, který je součástí vyšších edic Microsoft Windows od verze Vista.

Následně stručně rozebereme šifrovací schéma a změříme se na některé méně známé informace o implementaci algoritmu ve Windows Vista a Windows 7, včetně informací získaných z různých zdrojů o způsobu interní správy klíčů a hlaviček šifrovaných disků.

Nakonec se zaměříme na jednu málo dokumentovanou změnu v BitLockeru ve Windows 8, kterou je odebrání možnosti použít Elephant Diffuser a rozebereme některé dopady tohoto kroku.

Dan Rosendorf – dan.rosendorf@i.cz
Pracuje jako Specialista bezpečnosti informací ve firmě S.ICZ poslední tři čtvrtě roku. Předtím studoval na University of Wisconsin-Madison, kde získal Masters of Arts in Mathematics se specializací na matematickou logiku a má přerušené PhD. studium ve stejném oboru. Magisterský titul získal v roce 2004 na MFF-UK v praze v oboru Algebra, specializace Matematické struktury.

Může šifrování dat na přenosných počítačích ochránit EU proti průmyslové špionáži?

Martin Kákona

Datová úložiště přenosných počítačů se mohou stát snadným cílem průmyslové špionáže. Zaměříme se na hrozby nastávající při odcizení počítače a hrozby plynoucí z modifikace počítače ve vypnutém stavu. Ukážeme si některé útoky proti kryptografii, která je použita na ochranu lokálních dat a slabiny obecně rozšířených kryptoschémat pro šifrování velkých bloků. Jako jeden z možných způsobů ochrany notebooků si ukážeme směr založený na modifikaci open source software TrueCrypt a proprietárním hardware vyrobeném v rámci možností EU. Výhled do budoucna není příliš optimistický. Zřejmě se nevyhneme některým filozofickým úvahám.

Martin Kákona – martin.kakona@i.cz
Pracuje jako šéfkonstruktér firmy S.ICZ (nástupnické firmy společnosti DEC-ROS), která se specializuje na ochranu počítačových dat. Pod jeho vedením byl v roce 1994 vyvinut první český kryptografický mikroprocesor. Vedl vývoj několika certifikovaných kryptografických prostředků určených pro ochranu informací do stupně utajení Tajné. Je odborníkem na nosiče klíčů a je znám svými pracemi kompromitujícími biometrické metody autentizace.

Šifrování disků a Truecrypt

Milan Brož

Multiplatformní program Truecrypt pro transparentní šifrování disků se za poslední roky stal jedním z nejpoužívanějších nástrojů tohoto typu.

Přestože je zástupcem programů s otevřeným zdrojovým kódem, jeho licence vylučuje zařazení do některých Linuxových distribucí.

Tento problém (mimo jiné) vedl k zapracování podpory Truecrypt formátu do nativního nástroje pro správu šifrovaných disků pod Linuxem – cryptsetupu.

Na základě zkušeností s touto implementací si popíšeme, jak se vyvíjel formát Truecryptu, jak fungují zřetězené šifry, jak se v čase měnily používané šifrovací módy (včetně různých nestandardních „vylepšení“ na které autor při ověřování této nezávislé implementace narazil).

Řekneme si, co ve skutečnosti znamená používání skrytého disku a skrytého operačního systému. To vše z pohledu pokročilého uživatele, kterému nestačí jen obecný popis, ale který chce vědět, jak systém funguje zevnitř.

Na závěr si prakticky ukážeme, jak lze libcryptsetup (což je knihovna implementující funkce cryptsetupu) použít například k napsání jednoduchému programu k hledání „zapomenutého“ hesla pomocí slovníku hesel.

Milan Brož – milan.broz@mail.muni.cz
Absolvent FEI VUT v Brně, nyní postgraduální student Fakulty informatiky Masarykovy univerzity. Posledních několik let je mimo jiné vývojářem Linuxových nástrojů pro transparentní šifrování disků (cryptsetup a dm-crypt).

PowerShell z pohľadu *nix používateľa

Juraj Michálek

Administrátori a používatelia Windows často ani netušia, aký silný nástroj majú inštalovaný v systéme Windows. Namiesto využitia plného výkonu PowerShellu používajú pomerne neohrabané cmd a batch skripty. PowerShell je plne integrovaný so systémom a v niektorých aspektoch prekonáva možnosti *nix shellov. Open source komunita vytvára rôzne rozšírenia. Ako napríklad UIAutomation na automatizáciu GUI operácií a testovania. Pozrieme sa na PowerShell pohľadom používateľa *nixu. Nezabudneme ani na bezpečnostné aspekty ako je podpisovanie skriptov a ExecutionPolicy.

Juraj Michálek – juraj.michalek@ysoft.com
Vyštudoval FI MUNI. Pôsobil ako predseda Slovak Linux User Group, podieľal sa na tvorbe edukačných materiálov a tréningoch projektu Infovek. Pracoval pre Siemens na implementáciach SIP stacku. Pôsobil ako tréner pre Linux a Adobe

Flex v nadnárodných spoločnostiach. Optimalizoval deployment a vývojové procesy HRM a CRM systémov firmy Atollon, primárne postavených na OS Centos a Debian. Je členom skupiny Adobe Community Professionals. V súčasnosti pracuje pre Y Soft v Brne na pozícii systémového integrátora. Má na starosti tím venujúci sa výskumu a tvorbe nástrojov pre plynulý deployment produktov v heterogénnych prostrediach a vývoju pre platformu Mac OS.

Systémy detekcie sieťových útokov obvykle vytvárajú model sieťovej komunikácie za účelom identifikácie „zlých“ dát. Komplexnosť protokolov, nedodržiavanie špecifikácií výrobcami softvéru, prípadne rôznorodosť implementácií protokolov robia návrh sieťového IDS systému výzvou. Prednáška bude vychádzať z praktických skúseností získaných počas vývoja IDS systému na detekciu zneužitia zraniteľnosti MS WINDOWS sieťových protokolov (SMB, RPC). Prednáška poskytne príklady útokov, prediskutuje viaceré spôsoby detekcie, príklady techník a nástrojov pre vyhýbanie sa sieťovej detekcii v MS WINDOWS sieťových protokolov.

Marián Novotný – novotny@eset.sk
Pracuje ako dizajnér sieťových algoritmov v spoločnosti ESET, spol. s r.o., kde sa venuje výskumu, návrhu a realizácií detekčných algoritmov sieťových útokov v produktoch spoločnosti ESET. Externe spolupracuje s Laboratóriom Bezpečnosti a Aplikovanej Kryptografie FI MUNI, kde vedie záverečné práce v oblasti sieťovej bezpečnosti. Absolvoval doktorandské štúdium na Prírodovedeckej Fakulte UPJŠ v Košiciach, pričom v dizertačnej práci sa venoval problematike návrhu a analýzy bezpečnostných protokolov.