Konference EurOpen.CZ - klášter Želiv 2.–5. října 2011

Vložil/a EurOpen [1], 11 Září, 2011 - 19:33

- Konference [2]
- Security [3]

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

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

Pondělní program bude naplněn příspěvky týkajícími se rozsáhlých počítačových sítí. Začneme přednáškou o praktické realizaci formátů pro digitální podpis od Libora Dostálka. Zkušenosti při dohledování rozsáhlých infrastruktur Masarykovy univerzity s více než tisícem stanic, desítkami serverů a desítkami tisíc účtů představí Pavel Tuček. Často opomíjenou problematiku útoku dočasných vnitřních uživatelů ve firemní síti ve zvané přednášce probere Ondra Ševeček se zaměřením na nástroje firmy Microsoft. Aktuální stav IPsecu představí Pavel Šimerda se zaměřením na jeho proměny od původně zamýšleného prostředí IPv6. Těsně před večeří se dozvíme zákulisní informace o principech i aktuálním stavu nástrojů pro diskového šifrování od Milan Brože, hlavního vývojáře dm-cryptu. Navečer nás čeká mírně sžíravý vhled od Luďka Smolíka do budoucnosti někdy oslavované, někdy proklínané infrastruktury pro správu a distribuci veřejnými klíči asymetrické kryptografie – už délka názvu napovídá, že situace není jednoduchá, přestože se anglická zkratka PKI tváří, že všechny problémy jsou již překonány.

Úterní programzahájí zvaná přednáška o slibech a realitě elektronických pasů od Zdenka Říhy, který pro Evropskou komisi dlouhodobě pracoval na jejich testování a uvádění do praxe na evropské úrovni. Úzce souvisejícím tématem je správa revokovaných certifikátů, byť nahlížena z pohledu elektronického plateb4 ního systému Vítkem Bukačem. Před prací v sekcích nás čeká zvaná přednáška na téma návrhu decentralizovaných a těžko odhalitelných červů od Norberta Szetei, který se proslavil mimo jiné implementací nástroje pro cracking karet Mifare Classic.

Středeční část uvede Jaromír Dobiáš představením práce týkající se možnosti deanonymizace uživatelů při používání webových technologií, která úzce souvisí s jeho působením na technické universitě v Drážďanech. Svým neopakovatelným

stylem zpracuje častý účastník Europenu Radoslav „Bodík Bodó zkušenosti z hrátek na bezpečnostní mobilizaci při obraně evropské gridové architektury EGI. A o závěr se postará zvaná přednáška na téma bezpečnosti a vývoje RIA aplikací od Juraje Michálka, všestranně nadaného komunikátora a „rozjížděče softwarových firem.

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

Zamyšlení na závěr

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

Za programový výbor se těší
Petr Švenda.
www.europen.cz [4]

URL článku:
https://security-portal.cz/clanky/konference-europencz-kl%C3%A1%C5%A1ter-%C5%BEeliv-2%E2%80%935-%C5%99%C3%ADjna-2011

Odkazy:
[1] https://security-portal.cz/users/europen
[2] https://security-portal.cz/category/tagy/konference
[3] https://security-portal.cz/category/tagy/security
[4] http://www.europen.cz