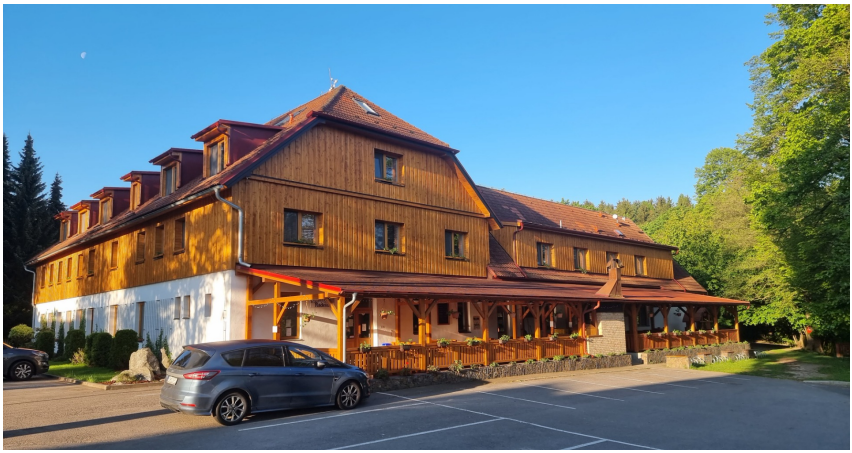
Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

54. konference



Balónový hotel a pivovar, Radešín
29. května – 1. června 2022

Milí přátelé EurOpenu!

Svět se probouzí a my s ním! Po dvou letech, kdy plánování jakékoli společenské akce bylo nanejvýš riskantním podnikem, se alespoň v tomto ohledu blýská na časy. Jsem rád, že u toho EurOpen nechybí.

Konferenci s bezpečnostním zaměřením jsme původně plánovali na jaro roku 2020 a postupně s těžkým srdcem několikrát odkládali. Při pohledu z té lepší stránky zato můžeme říci, že výsledkem dlouhých příprav je nabitý program se vším, co k vydařené konferenci patří. Těšit se můžete na tradiční nedělní tutorial, večerní „netechnickou“ přednášku, dokonce po několika letech znovu i na tištěný sborník. Na Vás tak už zbývá jen zajistit, aby stejně nabitý jako program byl i přednáškový sál.

Nechci se podrobně rozepisovat o tématech. Ostatně od stránky 8 dále najdete jako obvykle anotace jednotlivých příspěvků. Ale rád bych upozornil ještě na místo konání. EurOpen tíhne k horám a i letošní ročník je toho důkazem. Přijeďte i kvůli nim! Poloha je spravedlivá: stejně daleko od Prahy jako od Brna, případně od Plzně jako od Ostravy. Pro nikoho by vzdálenost neměla být překážkou. A v programu samozřejmě pamatujeme i na dostatek času k odpolednímu výletu. Bude nám potěšením, sejde-li se opět v hojném počtu sekce pěší i cyklistická. A kdo přijede na motorce, může na vyjížďku se mnou.

Přijeďte, těšíme se na Vás!

Zdeněk Šustr

Program

Neděle 29. 5.		
Čas	**Přednáška**	**Přednášející**
15.00	Antonín Dufka, Petr Švenda	*Tutoriál*: Praktické využití prahové kryptografie (Multisig) a anonymizačních technik (CoinJoin) v Bitcoinu i mimo něj
Pondělí 30. 5.		
9.00	Jiří Kůr	Bezpečnost mobilních sítí (téměř) všech generací
9.50	Jaroslav Řezník	Vládní certifikace a otevřený software
10.40	Přestávka	
11.00	Adam Janovský	Do certification schemes (Common Criteria, FIPS-140) improve security?
11.50	Antonín Dufka, Jakub Janků	MeeSign: Threshold Signing for Electronic Evidence Management
12.40	Oběd	
14.00	Jan Dušátko	Standardizace v oblasti kryptografie
14.40	Ondřej Hujňák	E-Banking Authentication – Dynamic Password Generators and Hardware Tokens
15.20	Tono Firc	Deepfakes as a threat to biometrics systems: a survey on creation and detection
16.00	Přestávka	
16.20	Tono Firc	The dawn of a text-dependent society: deepfakes as a threat to speech verification systems
17.00	Ivan Homoliak	The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses
17.40	Martin Perešíni	DAG-Oriented Protocols PHANTOM and GHOSTDAG under Incentive Attack via Transaction Selection Strategy
18.20	Přestávka	
18.40	Milan Brož	Lesk a bída šifrování disků
19.20	Rump Session	
19.50	Večeře	

Úterý 31. 5.		
Čas	**Přednáška**	**Přednášející**
9.00	Tomáš Rosa	Kryptolog a sousedův P.E.S.
9.50	Petr Jedlicka	Hardwarově akcelerovaná kryptografie s využitím FPGA
10.30	Přestávka	
10.50	Roman Kümmel	PTWEBDISCOVER: Nástroj pro efektivní mapování webových aplikací během penetračního testování
11.30	Martin Šebela	Phishingator aneb cvičný phishing „nejen“ na ZČU
12.10	Jan Kvapil	Bug bounty hunter
12.50	Oběd	
	Práce v sekcích	
19.00	Večeře	
večer	Martin Čarnogurský	Praktické otevírání zámků s klíči i bez
Středa 1. 6.		
9.30	Adam Ruman	Detekce škodlivého kódu v programech SSH
10.10	Tomas Weinfurt	Ověřené postupy pro validaci certifikátů
10.50	Přestávka	
11.10	Roman Oravec	Obfuskácia s využitím frameworku LLVM
11.50	Martin Čarnogurský	Supply chain attacks on package managers
12.40	Oběd	

Konferenční poplatky

Vložné		
platba	**tutorial**	**konference**
Členové		
do 20. 5. 2022 včetně	750	3 000
po 20. 5. 2022	750	3 200
Nečlenové		
do 20. 5. 2022 včetně	750	3 250
po 20. 5. 2022	750	3 450

Ubytování a stravování		
od neděle 29. 5.	3 435	od nedělní večeře do středečního oběda, tři noclehy
od pondělí 30. 5.	2 485	od pondělního oběda středečního oběda, dva noclehy

Ubytování a plná penze 1145 Kč na den (ubytování 780 Kč/den se snídaní, oběd 195 Kč, večeře 170 Kč).

Užitečné informace

Kdy	Konference začíná v pondělí 29. 5. 2022 v 9 hodin a končí ve středu 1. 6. 2022 cca ve 14 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Balónový hotel, Radešín 11, 592 55 Bobrová
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, občerstvení během přestávek a ubytování
Úhrada poplatku	č.ú. 478928473 u ČSOB Praha 1, kód banky 0300, variabilní symbol v elektronické přihlášce; spolek EurOpen.CZ, Univerzitní 8, Plzeň IČO: 61389081, DIČ: CZ61389081 Spolek EurOpen.CZ není plátcem DPH.
Neúčast	Při neúčasti se účastnický poplatek nevrací. 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 konference.**
Uzávěrka přihlášek	24. 5. 2022 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: Praktické využití prahové kryptografie (Multisig) a anonymizačních technik (CoinJoin)

Antonín Dufka, Petr Švenda

Tutoriál představí různé možnosti autorizace transakce v síti Bitcoin a zaměří se na pokročilejší varianty použitelné i mimo ekosystém Bitcoinu. Účastníci si kolaborativně vytvoří Bitcoin peněženku vyžadující autorizaci transakce od více osob s vhodnou prahovou konfigurací (multisig, např. 3-z-5), provedou dlouhodobou zálohu potřebného kryptografického materiálu (BIP-39) a sestaví několik transakcí včetně studia výsledné datové struktury. Ve druhé části pak společně vytvoříme vytvoříme mixovací transakce (PayJoin, CoinJoin Whirpool) zvyšující odolnost vůči analýze blockchainu s cílem identifikovat chování uživatele a přeposílaných prostředků.

Antonín Dufka, Petr Švenda Bezpečnostní výzkumníci a učitelé na Fakultě Informatiky, Masarykovy university, fascinovaní množstvím užitečných technik, které možná byly akademicky publikovány již před dlouhou dobou, ale teprve díky kryptoměnám dochází k jejich opravdovému nasazení, optimalizaci a širokému použití – a to i mimo kryptoměny samotné.

Praktické otevírání zámků s klíči i bez (Lockpicking)

Martin Čarnogurský

Přednáška prakticky ukáže principy fungování běžných zámků, možnosti jejich obcházení a různá bezpečnostní vylepšení. Především ale nechá posluchače samotné na několika sadách vyzkoušet jejich otevírání pomocí šperháků (lockpicking) a vybaví je tak schopností provádět „penetrační testování“ zámků před jejich nákupem i těch již pořízených.

Martin Čarnogurský Profesionálny Python developer a výskumník v oblasti bezpečnosti zo zameraním na OSINT, zber dát a ich analýza. Zakladateľ SourceCode.AI s cieľom vytvoriť nástroje a edukovať programátorov a spoločnosti v oblasti bezpečného vývoja softwaru.

Kryptolog a sousedův P.E.S.

Tomáš Rosa

Lze ukázat, že každá infekční nemoc má svůj vnitřní epidemický kód, který na pozadí náhodných fluktuací neúprosně řídí mechanizmus jejího šíření. Přiblížíme si typický epidemický program zapsaný jednoduchou soustavou diferenciálních rovnic, který se dobře hodí pro účely strategické bezpečnostní analýzy. Kromě vysvětlení hlavních kvalitativních aspektů šíření infekcí (základní a efektivní reprodukční číslo, lockdown, vakcinace, kolektivní imunita, endemie) nám zde poslouží i k připomenutí významu matematického modelování v bezpečnostních analýzách obecně. Budeme se ovšem věnovat nejen modelování bezpečnosti, ale i bezpečnosti modelování samotného, aneb například: „Jak těžké je vytvořit zadní vrátka pro psa?“ Tím přineseme alespoň malé zrnko kryptografické etiky, která tento obor právem činí vzorem matematické bezpečnosti, do míst, kam světlo úvah páně Kerckhoffsových dosud zjevně nedopadá.

Tomáš Rosa získal doktorát v oboru matematické kryptologie s Cenou rektora ČVUT za rok 2004, studoval na FEL ČVUT a MFF UK v Praze. Rozvíjí matematické modelování coby klíč k informacím uloženým v datových záznamech pozorovatelných veličin mnoha druhů. Přirozenou aplikací je kryptoanalýza pomocí postranních a skrytých kanálů, kde dosáhl uznávaných výsledků. Jeho práce pomohla zlepšit řadu standardů: PGP, TLS, platební schéma EMV, Bluetooth a GNSS. Tomáš je hlavním architektem matematické bezpečnosti v Kompetenčním centru pro kryptologii a biometrii skupiny Raiffeisen Bank International a přednáší modelování bezpečnosti na MFF UK.

Bezpečnost mobilních sítí (téměř) všech generací

Jiří Kůr

Přednáška se věnuje problematice bezpečnosti mobilních sítí od GSM po 5G. V úvodu posluchače stručně seznámí s jejich bezpečnostní architekturou. V hlavní části pak představí zásadní zranitelnosti, které byly v průběhu let odhaleny. Prezentovány budou primárně zranitelnosti, které vychází ze samotného standardu, nikoliv chybné implmenetace. Představené problémy nejsou teoretického rázu, ale byly a stále jsou využívány/zneužívány v reálném životě.

Jiří Kůr Vystudoval doktorské studium na Masarykově Univerzitě, kde se zaměřoval na ochranu soukromí a bezpečnost internetu věcí. Poté se zaměřoval na bezpečnostní výzkum komunkačních nástrojů, od mobilních sítí, přes satelitní telefony až po moderní chatovací aplikace. V současné době působí jako CTO ve společnosti Invasys, která se věnuje bezpečnosti mobilních telefonů a vyvíjí nástroje pro boj s organizovaným zločinem a terorismem.

Supply chain attacks on package managers

Martin Čarnogurský

V tejto prednáške sa budeme zaoberať problémami z hľadiska bezpečnosti, ktoré vyplývajú z iniciálneho návrhu celého ekosystému balíčkov. Ten vznikol ešte v dobe kedy bol kladený dôraz primárne na flexibilitu aby bolo čo najjednoduchšie možné publikovať nový kód. Tieto „nedostatky“ sa začali v poslednej dobe výrazne zneužívať útočníkmi, zvyčajne na podvrhnutie škodlivého kódu a na iné nekalé úmysly. Napriek tomu že máme už znalosti ako vytvoriť takýto systém aby bol bezpečný, nemôžeme si dovoliť len tak zahodiť ten existujúci pretože na ňom zavisia milióny užívateľov a spoločností. Namiesto toho sme nútený vytvoriť nástroje na monitorovanie a audit balíčkov, ktoré preskúmame počas prednášky. Dôležité je samozrejme aj zavedenie nových štandardov, ktoré za cenu užívateľského komfortu výrazne zvýšia zabezpečenie balíčkovacieho ekosystému. Tieto nástroje a štandardy si samozrejme aj prakticky ku koncu prednášky ukážeme na príkladoch.

Martin Čarnogurský Profesionálny Python developer a výskumník v oblasti bezpečnosti zo zameraním na OSINT, zber dát a ich analýza. Zakladateľ SourceCode.AI s cieľom vytvoriť nástroje a edukovať programátorov a spoločnosti v oblasti bezpečného vývoja softwaru.

PTWEBDISCOVER: Nástroj pro efektivní mapování webových aplikací během penetračního testování

Roman Kümmel

Článek popisuje nástroj ptwebdiscover, který je určen k mapování webových aplikací během bezpečnostního penetračního testování. Hlavní rozdíl od současných nástrojů představuje běh ve více vláknech a poskytování unikátních možností testerovi. Příkladem těchto možností je aplikování metody hrubé síly v situacích, kdy je nutné hledat kratší názvy souborů nebo možnost označit v testovaném URL konkrétní místo, na které bude program vkládat ověřované řetězce. Článek popisuje vlastní vícevláknovou implementaci nástroje a porovnání s konkurenčními nástroji během penetračního testování webové aplikace.

Roman Kümmel Penetrační tester, bezpečnostní konzultant a lektor počítačové školy Gopas zaměřující se převážně na bezpečnost a etický hacking webových aplikací. Je provozovatelem známého webového serveru SOOM.cz, který se věnuje hackingu a IT bezpečnosti. Je autorem knihy XSS: Cross-Site Scripting v praxi a mnoha článků v odborných časopisech. V současnosti patří mezi jeho největší projekty vývoj unikátního nástroje pro realizaci bezpečnostních testů Penterep.com, na kterém spolupracuje s VUT v Brně.

Bug bounty hunter

Jan Kvapil

Hledání zranitelností v softwaru – dříve činnost často za hranicí legálních aktivit, nyní (ne)obyčejné zaměstnání. Jak hledat chyby legálně a pomáhat tak zabezpečit software pro ostatní? Kde a jak napsat vulnerability disclosure report a odpovídající proof of concept? Kromě odpovědí se podíváme na zajímavé publikované reporty. Dále na nástroje, které lze k hledání využít, ale i na to, jak hledání chyb zapadá do OSS světa a zda byste měli mít vlastní bounty program.

Jan Kvapil Na MUNI vystudoval bakaláře obecné matematiky a magistra získal z bezpečnosti informačních technologií. Po bakaláři pomáhal

v korporátu navrhnout model využívající strojového učení na rozpoznávání úspěšnosti projektů. Následně odjel na roční stáž do Holandska, kde se věnoval vývoji softwaru na zakázku. Studium bezpečnosti doplnil o další stáž v oblasti počítačové bezpečnosti a o spolupráci pod Fakultou informatiky zaměřenou na forenzní analýzu. Nyní vypomáhá s výukou na fakultě a věnuje se etickému hackingu. Jako hacker se rád ponoří do každé technologie, ale doma se cítí v terminálu nebo na horách.

Do certification schemes (Common Criteria, FIPS-140) improve security?

Adam Janovský

Adam will present a tool for fully automated large-scale analysis of artifacts that accompany security certifications (Common Criteria, FIPS-140). Worldwide, the devices in many areas of governance and public services are regulated to products that underwent this certification. This makes the certified products ubiquitous in areas where information security is of utmost importance. Yet, these documents are difficult to process automatically, and it is challenging to step back and take a bird's eye view of the landscape of certified devices. This is addressed by our Python framework that daily parses all publicly available artifacts to all certified devices (in CC, FIPS-140), to gain both overall and detailed insights into how these devices are deployed. Among other notable extracted features, we link the existing certified devices to the National Database of Vulnerabilities, and we show the graph of dependencies between certified devices. The tool is accessible from seccerts.org.

Adam Janovský Adam is a Ph.D. candidate at the Masaryk University (MUNI) in Brno, CZ. He received his Master's degree from MUNI in 2018. His research concentrates on data mining of cryptographic API records from large datasets and their subsequent analysis. This work is limited to three particular domains: bias in RSA private keys, cryptographic API in Android malware, and cryptographic API in certification schemes (Common Criteria, FIPS-140). Along with his research, Adam is (or has been) a teaching assistant in several courses on cryptography and information security at the faculty of informatics, Masaryk University. Adam's PhD programme is financially supported by Invasys company where he also works as a security researcher.

Vládní certifikace a otevřený software

Jaroslav Řezník

Jsou vládní standardy, certifikace, bezpečnost a open source navzájem kompatibilní, nebo ne? Odpověď je ano. Ale jako vždy s nějakým ale. V téhle přednášce se seznámíte s tím, co jsou vládní certifikace a jaké certifikace máme. Odpovíme si na otázku kompatibility a na jaké problémy můžete narazit při certifikaci otevřeného software (a to i v případě, kdy je distribuován jako enterprise produkt). Hlavní téma přednášky budou Common Criteria certifikace (a Commercial Solutions for Classified), FIPS 140-2 a FIPS 140-3. Zběžně se podíváme i na další, nejen bezpečnostní, certifikace jako je FedRAMP, USGv6, SCAP a Section 508/VPAT.

Přednášku bude především z praktického pohledu. Přednášející má za sebou nejeden certifikační projekt a získal několik desítek Common Criteria a FIPS certifikátů pro známé enterprise produkty založené na otevřeném software. K tomu si povíme více detailů o procesu jak takové certifikace probíhají – od úplného začátku až k vydání certifikátů.

Jaroslav Řezník Jaroslav Řezník pracuje jako Engineering Program Manager v brněnském Red Hatu a je zodpovědný program vládních certifikací v týmu Product Security Compliance and Risk. Jaroslav vede nejen bezpečnostní certifikace jako FIPS 140-2 a FIPS 140-3, Common Criteria, USGv6 a SCAP – od prvotní analýzy projektu až po koordinaci vydání tiskové zprávy. Jaroslav je nadšenec do otevřených technologií. V minulosti byl člen Fedora Board a Fedora Council, přispíval do projektů jako je Fedora a KDE a je jeden z lidí za konferencí OpenAlt.

Standardizace v oblasti kryptografie

Jan Dušátko

Příspěvek představí problémy související se standardizací kryptografie v oblasti IT na základě několika let systematické analýzy kryptografických schémat se zaměřením na vývoj v čase a porovnáním jednotlivých variant. O standardizaci v oblasti kryptografie patrně každý slyšel. Ale jaký účel plní? Jakou má historii, jak se vyvíjela a vyvíjí? Jaký vliv na ni mají zákony a normy? Jak se tyto standardy vyvíjely? Jaká je blízká budoucnost a co to znamená z pohledu IT? Uvedené otázky mohou být zajímavým

pohledem na současné snahy o zajištění bezpečnosti. Stejně tak je potřeba si uvědomit, k čemu kryptografie slouží a s jakými hrozbami se potkává.

Jan Dušátko, 50 let. Vyučený soustružník, později si dodělal průmyslovku. Nadšenec do informačních technologií, ke kterým se dostal přes opravy rádií. Začínal na osmibitech, ale měl možnost si odzkoušet i sálové počítače. Pracoval většinou v soukromé sféře. O kryptografii se zajímá od roku 1996 díky článkům Vlastimila Klímy. Až příliš pozdě zjistil, že se jedná o velice návykovou oblast. V poslední době se snaží o misionářské aktivity a tuto krásnou oblast přiblížit správcům sítí (které to ale bohužel většinou nezajímá).

Lesk a bída šifrování disků

Milan Brož

Šifrování dat na úrovní disku je jedna z nejstarších, a zdánlivé triviálních, cest k dosažení důvěrnosti dat (nebo alespoň cesty pro splnění položky „osobní data jsou šifrována“ v IT auditní zprávě). Zkusme si projít historii různých implementací, včetně dobrých nápadů, ale i omylů, počínaje TrueCryptem (respektive VeraCryptem), BitLockerem, LUKS a FileVault a jejich přístupem. Když dva dělají totéž, není to vždy totéž.

Přednáška je postavena na autorově snaze (a nezměrnému úsilí jeho studentů ji realizovat) o nativní a otevřenou open-source (re)implementaci všech výše uvedených systémů pro Linux. Ukážeme si, jak jednotlivé implementace přistupují k ukládání klíčů, integraci (či ignoranci) hardwarových prostředků a různých poznatků, které jsme na této cestě potkali.

Milan Brož Vývojář Linuxových nástrojů pro transparentní šifrování disků (cryptsetup a dm-crypt), výzkumník v oblasti bezpečnosti storage a open-source technologií a doktorský absolvent na Fakultě informatiky Masarykovy Univerzity.

Ověřené postupy pro validaci certifikátů (Best practices for certificate validation)

Tomas Weinfurt

Validace certifikátu se zabývá problémy spojenými s práci s digitálními certifikáty. PKI je poměrně složité a kromě základní kryptografického zajištění také nabízí možnosti hierarchie a volitelných rozšíření. Certifikát platný pro konkrétní operaci může byt nevhodný pro jiné použití. Situaci ani nezjednodušují ani možnosti ověřovat stav platnosti online. Příspěvek je založen na poznatcích a zkušenostech získaných při vývoji bezpečnostních funkci pro .NET na všech podporovaných operačních systémech.

Tomas Weinfurt je absolventem ZCU a v devadesátých letech stál u počátku českého internetu ve firmách Conet a InternetCZ. Od roku 2000 bydlí v Seattle, USA a podílel se na vývoji různých síťových zařízení – laserových pojítek, firewallů a vyvažovačů zátěže. V současné době je zaměstnán firmou Microsot a pracuje na vývoji open-source prostředí .NET Core které umožňuje vývoj aplikaci C#, F# and VB na operační systémech Linux, macOS a Windows. Hlavním zaměřením jsou síťové funkce a bezpečnost. Je přispěvatelem a udržovatelem .NET funkci v System.Net a System.Net.Security a vývoj open-source je jeho hlavní pracovní náplní. https://github.com/wfurt

MeeSign: Threshold Signing for Electronic Evidence Management

Antonín Dufka, Jakub Janků

Electronic evidence handling often requires confirmation by multiple people to ensure liability. The confirmation can be expressed as a digital signature; however, many standard tools cannot process more than one digital signature of the same document. Threshold cryptography solves this problem by enabling the construction of a digital signature by multiple parties, indistinguishable from a standard digital signature and thus compatible with standard tools. We use this technique in the design of MeeSign, an open-source platform for multi-party document signing. The talk will have a practical part demonstrating the tools developed and will

let conference participants collaboratively create a signed PDF file using a group of signers.

Antonín Dufka vystudoval obor bezpečnost informačních technologií na Fakultě informatiky Masarykovy univezity. Aktuálně pokračuje na téže fakultě v Ph.D. studiu. Ve svém výzkumu se zabývá protokoly bezpečného počítání více stran (secure multi-party computation) implementovaných na bezpečném hardware, například čipových kartách.

Jakub Janků Student at Faculty of Informatics, Masaryk University. Former intern at Red Hat SPICE team. Currently building an open-source app showcasing multi-party signature protocols with members of the CRoCS laboratory.

Obfuskácia s využitím frameworku LLVM

Roman Oravec

Obfuskácia predstavuje spôsob úpravy programu s cieľom ukryť špecifiká jeho implementácie. Rôzne obfuskačné techniky sa používajú ako prostriedok na ochranu duševného vlastníctva a prevenciu neoprávnenej manipulácie s programom, ako aj na škodlivé účely, akým je napríklad tvorba malvéru ktorý sa dokáže vyhnúť detekcii. Popíšeme si bežne používané obfuskačné transformácie a vybrané voľne dostupné obfuskátory. Bližšie sa zameriame na implementácie založené na projekte LLVM, spôsob ich využitia na obfuskáciu počas kompilácie programu a porovnanie s ďalšími alternatívnymi metódami. V neposlednom rade sa budeme venovať otázke, aký prínos môže mať znalosť obfuskácie v kontexte otvorených systémov.

Roman Oravec je absolventom Fakulty informatiky Masarykovej univerzity a v súčasnosti sa venuje výskumu a vývoju v oblasti bezpečnosti v spoločnosti Invasys. Vo svojej diplomovej práci sa venoval možnostiam obfuskácie s pomocou LLVM, v čom momentálne pokračuje aj v rámci svojho profesného života.

Detekce škodlivého kódu v programech SSH

Ádám Ruman, Daniel Kouřil

V příspěvku představíme techniku pro automatizovanou analýzu programů, která se zaměřuje na identifikaci částí aplikace potenciálně obsahující škodlivý kód. Technika využívá porovnávání grafů systémových a knihovních volání, která aplikace provádí během svého běhu. Cílovou aplikací jsou implementace protokolu SSH a jejich automatizovaná analýza.

Ádám Ruman je studentem Masarykovy univerzity, v oboru informatická bezpečnost. Při studiu je zapojen v bezpečnostním týmu CSIRT-MU, kde se zaměřuje na automatizaci ofenzivní bezpečnosti. Analýzou škodlivého kódu se zabývá ve volném čase a v rámci své diplomové práce.

Daniel Kouřil působí na Masarykově univerzitě a ve sdružení CESNET, kde se zabývá návrhem, vývojem a provozem bezpečnostních řešení pro rozsáhlé IT infrastruktury. Má bohaté zkušenosti s řešením bezpečnostních incidentů a detailní analýzou artefaktů, které se při vyšetřování objevují.

Deepfakes as a threat to biometrics systems: a survey on creation and detection

Tono Firc

Příspěvek pojednává o metodách tvorby a detekce deepfakes se zaměřením na biometrické systémy. Dozvíte se, jaké typy deepfakes existují, jak je možné je zneužit pro oklamaní biometrických systémů a kde najít nástroje s kterými si můžete sami pohrát. Hlavním jádrem přednášky budou praktické ukázky jednotlivých metod pro tvorbu deepfakes a návody, jak je zprovoznit.

Tono Firc je studentem doktorského studia na FIT VUT a členem výzkumné skupiny Security@FIT. Momentálně se věnuje výzkumu využitelnosti deepfakes v počítačové bezpečnosti. Zaměřuje se jak na zabezpečení systémů (např. biometrické systémy) proti deepfakes, tak na lidské aspekty bezpečnosti při potýkání se s deepfakes.

Hardwarově akcelerovaná kryptografie s využitím FPGA

Petr Jedlicka

Obvody FPGA (Field Programmable Gate Array) hrají nezastupitelnou roli při vývoji systémů vyžadujících vysokorychlostní zpracování dat v digitální podobě, přičemž míra produkce těchto systémů není slučitelná s vývojem zákaznických digitálních integrovaných obvodů typu ASIC (Application Specific Integrated Circuit). Jednou z oblastí takových systémů je hardwarově akcelerovaná kryptografie, na kterou je v kontextu FPGA tato přednáška zaměřena. Hlavními tématy jsou specifika vývoje na FPGA, rozdíly oproti klasickému programování procesorových systémů a způsoby optimalizace. V rámci kryptografie jsou prezentovány výsledky implementace a konkrétní příklady optimalizace postkvantových kryptosystémů CRYSTALS-Dilithium a CRYSTALS-Kyber.

Petr Jedlicka Petr Jedlicka je Ph.D. student Vysokého Učení Technického v Brně. Svůj inženýrský titul získal na fakultě elektrotechniky a komunikačních technologií v oblasti zpracování digitálního signálu a FPGA implementacím komunikačních systémů, především globálním navigačním satelitním systémům (GNSS). Jako Ph.D. student se výzkumně věnuje optimalizacím a implementacím post-kvantových kryptosystémů v FPGA.

Phishingator aneb cvičný phishing „nejen“ na ZČU

Martin Šebela

Příspěvek se zabývá vzdělávací aplikací Phishingator, která původně vznikla jako bakalářská práce autora s cílem upozornit na stále se zvyšující hrozbu phishingu. Aplikace umožňuje jednoduše vytvářet cvičné phishingové kampaně, které se skládají z vlastních podvodných webových stránek (například falešného přihlášení do univerzitních systémů) a z vlastních podvodných e-mailů, které jsou následně rozeslány konkrétním příjemcům. Phishingator poté průběžně sleduje, jakým způsobem příjemci na podvodný e-mail a stránku reagují a především, zdali se do ní nepokusili zadat platné přihlašovací údaje. Každému příjemci je zároveň poskytnuta zpětná vazba s vyznačenými indiciemi, na základě kterých bylo možné phishing rozpoznat. Na ZČU bylo díky aplikaci Phishingator provedeno již

několik cvičných phishingových kampaní na různá témata. Jak na cvičné phishingové kampaně reagují uživatelé v akademickém prostředí, jak vypadá typický průběh kampaně ve Phishingatoru a je riziko phishingu na základě výsledků z Phishingatoru opravdu aktuální?

Martin Šebela je absolventem magisterského studia v oboru Softwarové inženýrství na Fakultě aplikovaných věd Západočeské univerzity v Plzni. Během studia pracoval na částečný úvazek v uniherzitním bezpečnostním týmu WIRT v Centru informatizace a výpočetní techniky ZČU, kam po dokončení magisterského studia nastoupil na plný úvazek. V roce 2021 obdržel stipendium primátora města Plzně. Od roku 2022 začal také pracovat ve Forenzní laboratoři (FLAB) CESNET.

The dawn of a text-dependent society: deepfakes as a threat to speech verification systems

Tono Firc

Tento příspěvek pojednává o útocích na systémy hlasové biometrie za pomoci deepfakes. Postupně odhalíme, jak náročné je syntetizovat hlas vybrané osoby za pomoci open-source nástrojů a také komerčních nástrojů, jak je možné takto vytvořený syntetický hlas zneužít pro oklamání hlasové biometrie a nakonec to nejdůležitější, jaké jsou možnosti obrany proti takovému útoku.

Tono Firc je studentem doktorského studia na FIT VUT a členem výzkumné skupiny Security@FIT. Momentálně se věnuje výzkumu využitelnosti deepfakes v počítačové bezpečnosti. Zaměřuje se jak na zabezpečení systémů (např. biometrické systémy) proti deepfakes, tak na lidské aspekty bezpečnosti při potýkání se s deepfakes.

DAG-Oriented Protocols PHANTOM and GHOSTDAG under Incentive Attack via Transaction Selection Strategy

Martin Perešíni

This work explores the performance/scalability issues of blockchain protocols. Some existing solutions present a new concept of DAG-oriented blockchain protocols to address this problem. In contrast, in this work, we investigate two unique DAG-oriented blockchain protocols – PHANTOM and GHOSTDAG and make a security analysis of their designs. To this end, we develop a custom simulator that extends the open-source simulation tool to support multiple chains within the protocol. We have empirically shown that these protocols cannot work in realistic scenarios and need to be redesigned.

Martin Perešíni received his M.S. degree in Information Technology Security from the Brno University of Technology in 2020, where he is currently pursuing his Ph.D. degree in Computer Science and Engineering. From 2015 to 2020, he worked as a researcher and kernel developer in the Liberouter team within the CESNET group. He is currently a member of a research group focusing on Security in the Faculty of Information Technology, where his interests are in blockchain technology security, consensus protocols in blockchains, privacy-enhancing technologies, and cyber-security in general.

The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses

Ivan Homoliak

The paper proposes security reference architecture (SRA) for blockchains, which adopts a stacked model (similar to the ISO/OSI) describing the nature and hierarchy of various security and privacy aspects. The SRA contains four layers, and at each of these layers, we identify known security threats, their origin, and countermeasures. Next, we analyze several cross-layer dependencies for which we discuss their costs and impact on blockchain features. Next, to enable better reasoning about security

aspects of blockchains by the practitioners, we propose a blockchain-specific version of the threat-risk assessment standard ISO/IEC 15408 by embedding the stacked model into this standard. Finally, we provide designers of blockchain platforms and applications with a design methodology following the model of SRA and its hierarchy.

Ivan Homoliak is a research scientist at BUT FIT and his research interests include cryptocurrency wallets, distributed ledgers, e-voting, consensus protocols. Prior to joining FIT BUT, Ivan worked at SUTD on various projects focusing on the security of blockchains and insider threat detection. Ivan holds a Ph.D. in the area of adversarial intrusion detection in network traffic from BUT FIT.

E-Banking Authentication – Dynamic Password Generators and Hardware Tokens

Ondřej Hujňák

The e-banking has undergone a rapid development fueled recently by new legislation, such as PSD2. In our work we present an overview of possible authentication schemes suitable for e-banking and their security properties. We especially focus on concurrent technical solutions, which usually revolve around dynamic password generators or dedicated hardware tokens, and novel web standard for strong authentication – FIDO2.

Ondřej Hujňák received the M.S. degree in information technology security from the Brno University of Technology in 2016. He is currently pursuing the PhD degree in computer science and engineering at the Brno University of Technology and is a member of the research group Security@FIT focusing on computer and network security. His research interests include the security of IoT networks and devices, privacy-enhancing technologies and cyber-physical systems.