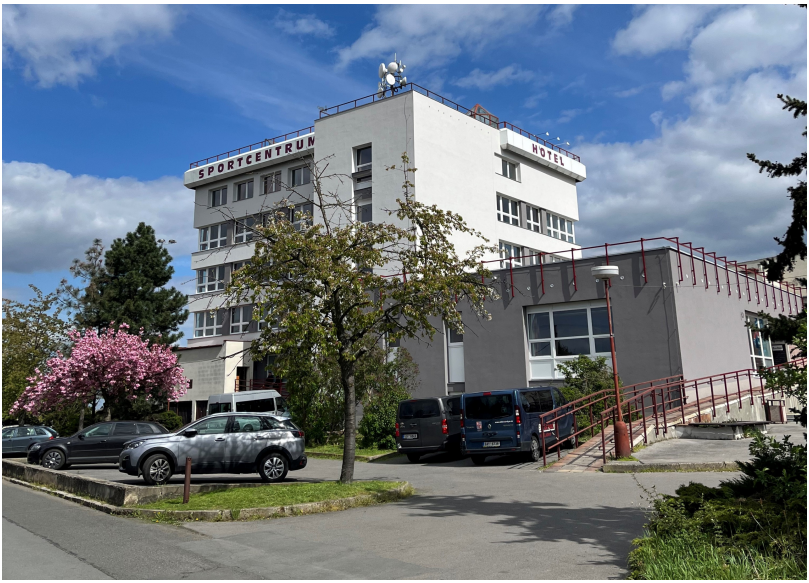
Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

57. konference



Sportcentrum, Brandýs nad Labem
25. – 28. května 2025

Milí přátelé EurOpenu!

Zaměření letošní konference jsme upekli v Hotelu Mědínek v Kutné Hoře. Už dlouho jsem chtěl uspořádat konferenci na téma programovacích jazyků, a když nikdo neprotestoval, vzal jsem si program letošní konference na hrb a začal se shánět po přednášejících, kteří by dobře zapadli jak do domluveného konceptu, tak do charakteru konference. Některé z přednášejících ostatně už znáte z let minulých.

Měl jsem představu, že se podíváme na současný stav programovacích jazyků, nástrojů a dalších souvisejících témat. Tak jedna z prvních nabídek přednášky byla na téma Cobol a Mainframe. Protože jsem už Davida slyšel na toto téma mluvit v rámci programátorských večerů, které jsme v době pandemie Covid-19 s malou skupinou lidí zavedli na platormě Clubhouse a později přesunuli na Discord, věděl jsem, že tohle na EurOpen chceme.

Pak přišly nabídky přednášek o programovacích jazycích Modula-2, Lisp a APL, a to už jsem si říkal, jestli to s tou archeologií trochu nepřeháníme. Trochu to zachránila Hanička, která věrně zastupuje naši zemi a progresivní směr při tvorbě nových verzí programovacího jazyka C++, kterému už taky pomalu táhne na půlstoleté jubileum, a Matějčík s Pythonem a Rustem.

Aby i letošní program zůstal dostatečně pestrý, proložíme to tématy z bezpečnosti, operačních systému, radarové techniky, použití informatiky ve výuce školních dětí a v pondělí večer si místo tradiční netechnické přednášky něco z těch dětských hraček a učebních pomůcek představíme a především vyzkoušíme.

Věřím, že se vám letošní program bude líbit, a že společně najdeme zajímavé nosné téma pro další běh naší tradiční konference. Ostatně jsem tu vlastně benjamínek, když jezdím s přestávkami od roku 2010, zatímco EurOpen je tu s námi už od roku 1988. Těšíme se na vás!

Pavel Šimerda

Programový výbor: Pavel Šimerda, Jiří Sitera, Pavel Růžička, Zdeněk Šustr

Titulní fotografie: Sportcentrum Brandýs

Program

Pondělí 26. 5.		
9.00	David Bečvařík	Cobol – Víc než jen historie
9.45	Jan Dušátko	Jak moc je možné důvěřovat certifikátům a certifikačním autoritám
10.30	Přestávka	
11.00	Anna Marešová	Když Linux přestal být jen pro geeky
11.45	Pavel Šafl	Micro:bit a matematika v programování – cesta od senzorů k porozumění datům
12.30	Oběd	
14.00	Martin Kolařík	Modula-2: když první řešení už je dobré
14.40	Jan Matějek	Rust a MicroPython ve společné paměti: Tenhle čip není dost velký pro nás oba!
15.20	Eduard Drusa	Výzvy pri ochrane pamäte v real-time prostredí mikrokontrollerov
16.00	Přestávka	
16.20	Hana Dusíková	Dualita C++
17.00	Tomáš Rosa Jiří Pavlů	Jemný úvod do postkvantových algoritmů na pozadí schématických modelů
17.40	Marek Petko	Zero-Trust Security Architecture
18.20	Večeře	
20.00	Pavel Šafl, Pavel Šimerda, Sára Šimerdová	Kdo si hraje, nezlobí

Úterý 27. 5.		
Čas	**Přednáška**	**Přednášející**
9.00	Jenda Hrach	Radarová technika 21. století
9.45	Nicol Daňková	Jak nebojovat se sekuriťáky během incidentu
10.30	Přestávka	
11.00	Pavel Tišnovský	Vzory v IT: význam vhodné notace a programovací jazyk APL
11.30	Lukáš Hozda	Wait, it's all LISP? Always has been
12.45	Oběd	
	Práce v sekcích ...s možností organizované vycházky a prohlídky brandýských kostelů	
19.00	Večeře	
Středa 28. 5.		
9.00	Lukáš Hozda, Pavel Šimerda	Tutorial – Bezpečné programování: Schopnosti programovacího jazyka

Konferenční poplatky

Vložné		
platba	**tutorial**	**konference**
Členové		
do 15. 5. 2025 včetně	400	2 200
po 15. 5. 2025	400	2 400
Nečlenové		
do 15. 5. 2025 včetně	400	2 450
po 15. 5. 2025	400	2 650

Ubytování a stravování		
od neděle 25. 5.	2 500	od nedělní večeře do úterního oběda, dva noclehy
od pondělí 26. 5.	1 650	od pondělního dopoledne do úterního oběda, jeden nocleh
setrvání do středy 28. 5.	+1 175	setrvání do středečního tutorialu vč. večeře v úterý a oběda ve středu.
úterní prohlídka	+ 300	prohlídka baziliky sv. Václava a Navštívení panny Marie a kostela Sv. Klimenta, platba pouze v hotovosti na místě

Ubytování a plná penze 1 325 Kč na den (ubytování 700 Kč/den se snídaní, oběd 175 Kč, večeře 150 Kč, občerstvení o přestávkách 150 Kč).

Užitečné informace

Kdy	Konference začíná v pondělí 26. 5. 2025 v 9 hodin a končí ve středu 28. 5. 2025 cca ve 12 hodin. Stravování je zajištěno od nedělní večeře nebo od pondělního oběda, podle zvolené varianty.
Kde	Sportcentrum Brandýs, Kostelecká 1776, 250 01 Brandýs nad Labem
Kontaktní adresa	Anna Šlosarová, EurOpen.CZ, Univerzitní 8, 306 14 Plzeň, e-mail: europen@europen.cz, tel.: 377 632 804
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://57.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	19. 5. 2025 nebo při naplnění ubytovací kapacity.
Kapacita	Kapacita přednáškového sálu a ubytovací kapacita hotelu limitují počet účastníků na cca 60.
Další informace	Pořizování audio či video záznamů bez svolení přednášejících a organizátorů konference není povoleno.
Přihláška	Pouze e-přihláška: webový formulář viz `http://57.europen.cz`

Cobol – Víc než jen historie

David Bečvařík

COBOL? Není to ten jazyk, co pamatuje dinosaury a děrné štítky? No... vlastně jo. Ale než ho hodíte do starého železa, pojďme se podívat, proč tenhle „dědoušek“ stále běží na pozadí spousty věcí (a ne, nejsou to jen banky!). Během prezentace prozkoumáme, co si z jeho posedlosti čitelným kódem, datovými strukturami (takový pravěk JSON schémat?) a neprůstřelnou logikou můžeme vzít. Zjistíme, že jeho parťák CICS řešil transakce podobně, jako dnes kouzlíme se serverless funkcemi nebo orchestrujeme mikroslužby. A co takové JCL? Možná předchůdce dnešních CI/CD pipeline a Ansible? Zkrátka, trocha archeologie v IT světě může být překvapivě užitečná, i když zrovna stavíte tu nejvíc cool appku na světě.

Jak moc je možné důvěřovat certifikátům a certifikačním autoritám

Jan Dušátko

V současnosti dochází ke generační obměně algoritmů. Zároveň také probíhá zkracování životnosti používaných certifikátů, změnám pravidel pro jejich definici a užití. Tato prezentace zmiňuje pouze nejkřiklavější excesy a upozorňuje, proč se jedná o problémy. Díky technologiím a procesům je naštěstí alespoň část z těchto problémů řešit.

Jan Dušátko – počítačům a počítačové bezpečnosti se věnuje více než 30 let. S kryptografií ho seznámi Vlastimil Klíma, Tomáš Rosa a další osobnosti. V tuto chvíli pracuje jako bezpečnostní konzultant, jeho hlavní náplní jsou témata související s kryptografií, e-mailovou komunikací a linuxovými systémy. Mimo to se aktivně snaží propagovat kryptografii u veřejnosti a též v této oblasti vzdělávat i správce IT systémů.

Když Linux přestal být jen pro geeky

Anna Marešová

Linux je dnes všude – v telefonech, autech, nemocnicích, superpočítačích i na oběžné dráze. Ale jak se z „toho systému, co si lidi kompilovali doma v garáži“ stal základ moderní digitální infrastruktury? V přednášce se společně podíváme na vývoj Linuxu od dob `/etc/init.d/` až po dnešní svět neměnných systémů, transakčních aktualizací a zabezpečeného startu, kde počítač sám ověřuje, jestli mu může věřit. Ukážeme si, co všechno si můžete s Linuxem snadno postavit doma – a co naopak musí být extrémně stabilní, aby to mohlo běžet v datacentrech, na vědeckých misích nebo v nemocnicích.

Dozvíte se, jak funguje komerční podpora něčeho, co je zdarma, proč open source není jen kód, ale i způsob myšlení, a proč i malý příspěvek může mít velký dopad. A chybět nebude ani příběh o tom, jak přestupná sekunda způsobila zmatek v jádře systému a na chvíli ochromila servery po celém světě.

Micro:bit a matematika v programování – cesta od senzorů k porozumění datům

Pavel Šafl

Matematika v programování není jen o číslech – je to klíč k tomu, abychom dokázali smysluplně pracovat s daty ze světa kolem nás. Na této přednášce si ukážeme, jak propojit základy matematiky a práci se senzory pomocí Micro:bitu, dostupné vzdělávací platformy, která otevírá dveře k reálným projektům i kreativnímu učení.

Představíme si konkrétní příklady, kde matematika hraje hlavní roli – například při měření pH vody v bazénu, analýze údajů z meteostanice nebo při výpočtu průměrné rychlosti pohybu. Naučíme se, jak ze surových dat ze snímačů vytvořit užitečné informace, jak správně pracovat s průměry, maximy, minimy, jednotkami i přepočty, a jak studentům ukázat, že za každým číslem se skrývá příběh a reálný jev.

Přednáška je určena pro odborné publikum, které se zajímá o využití Micro:bitu v technickém vzdělávání a praktických aplikacích. Zaměříme se na využití jednoduchých i pokročilejších výpočtů, ukážeme si možnosti

rozšíření projektů o další senzory a dotkneme se i témat jako je validace dat a chyby měření.

Přijďte zjistit, jak pomocí Micro:bitu, trochy matematiky a spousty nápadů otevřít studentům cestu k modernímu a smysluplnému vzdělávání!

Modula-2: když první řešení už je dobré

Martin Kolařík

Modula-2 je historický programovací jazyk Niklause Wirtha, tvůrce Pascalu, Moduly a Oberonu. Má moderní vychytávky a nemá složené závorky. Příspěvek vypíchne důležité vlastnosti Moduly, odlišnosti a souvislosti vůči současným jazykům. Protože duch modulárního programování je už dávno zpět.

Rust a MicroPython ve společné paměti: Tenhle čip není dost velký pro nás oba!

Jan Matějek

V této přednášce si ukážeme dva možné přístupy ke správě paměti: garbage collection v podání (Micro)Pythonu na straně jedné, a Rustovské sledování vlastnictví (ownership) na straně druhé. Předvedeme si jejich vlastnosti, výhody a nevýhody. V případě Rustu si také ukážeme, jaké nároky jeho metoda klade na programátora i na ostatní části kódu.

Dozvíte se, čím jsou tyto dva přístupy neslučitelné, a jak je lze přes to sloučit a úspěšně používat ve společné paměti na stejném mikrokontroléru – a taky proč by se do toho vůbec někdo chtěl pouštět.

Výzvy pri ochrane pamäte v real-time prostredí mikrokontrollerov

Eduard Drusa

Ochrana pamäte sa v počítačových systémoch berie za samozrejmosť nejake tri desaťročia. Je na nej postavená spoľahlivosť bežných počítačov, serverov aj mobilných telefónov. Hardware potrebný na jej implementáciu

existuje v procesoroch používaných v IoT a embedded zariadeniach vyše dve desaťročia. Avšak jeho využitie je minimálne.

Vo svojom projekte realtime operačného systému som sa snažil prísť s prístupom k ochrane pamäte, ktorý by umožnil túto technológiu využívať bez nutnosti čeliť obštrukciam zo strany hardware-u.

Temou tejto prednášky bude prečo je vlastne ochrana pamäte v prostredí embedded systémov problém, akým výzvam musí funkčné riešenie v tomto odvetví čeliť a aké sú doterajšie prístupy k tomuto problému. Pozrieme sa aj na prístupy, ktoré su technicky možné ale nespĺňaju základne požiadavky. Vzhľadom k povahe témy si čo-to povieme aj o tom, čo to vlastne taky real-time systém je a prečo na tom záleží.

Dualita C++

Hana Dusíková

Jaký je rozdíl mezi kompilovaným a interpretovaným C++? Je k tomu nějaký důvod? Proč by mě to mělo zajímat když má práce je dodat aplikaci mým uživatelům. V této přednášce ukáži, jak se měnilo metaprogramování v C++ od vzniku jazyka až po blížící se standard C++26. Prodiskutujeme také jak se tyto změny dostávají do standardu a co je pro to zapotřebí.

Hana Dusíková je zástupce České Republiky v ISO C++ komisi, kde předsedá studijní skupině pro compile-time programování a je místopředsedkyně pracovní skupiny pro design a evoluci jazyka. Pracuje ve firmě Woven by Toyota, kde je součástí týmu pro vnitřní standardizaci a technologie. Předtím pracovala 13 let v AVG a Avastu na vývoji interních high-performance systémů.

Jemný úvod do postkvantových algoritmů na pozadí schematických modelů

Jiří Pavlů, Tomáš Rosa

Ukážeme si, jaké matematické konstrukce dovolují nastupujícím kryptografickým algoritmům odolat síle klasických i kvantových počítačů. Uvedeme si k tomu snadno uchopitelný, nicméně stále dostatečně přesný, model standardů ML-KEM a ML-DSA, založený na konceptu brány LWE.

To nám dovolí nakreslit schematický diagram těchto algoritmů, který pozoruhodně zviditelňuje jejich ideovou příbuznost s protokolem Diffie-Hellman a podpisy na bázi konstrukce Fiat-Shamir, jako je zejména rodina (EC)DSA. Této afinity si všimneme podrobněji. Pozornost bude věnována i připravovanému FN-DSA. Průběžně budeme komentovat také úskalí, která velmi pravděpodobně budou tato schémata sužovat v prvních letech ostrého provozu. Připomeňme, že nám trvalo několik desetiletí, než jsme se do určité míry zbavili implementačních chyb, věrně provázejících současné algoritmy. Přesto se stále tu a tam objevují. Bylo by poněkud naivní očekávat, že tyto komplikace se novým algoritmům zázračně vyhnou. Naopak, velmi racionální by bylo učinit jejich nástup do praxe spíš pozvolným. Proti tomu však stojí paradigma retroaktivní kryptoanalýzy, což stručně řečeno znamená zachyť dnes – lušti později. To nás naopak nabádá zavést PQC (Post-Quantum Cryptography) co nejdříve a příliš s ním neotálet. Než se tak stane, je naše běžná šifrovaná komunikace v podstatě jen zasíláním otevřených zpráv do budoucnosti. To vše dohromady nám signalizuje, že stojíme patrně před největší změnou, jaká se má v oblasti počítačové bezpečnosti v tak ohromném rozsahu a zároveň tak krátkém čase odehrát.

Jiří Pavlů je absolventem magisterského studia v oboru Matematika pro informační technologie na Matematicko-fyzikální fakultě Univerzity Karlovy. Věnuje se teoretické kryptografii, zejména pak bezpečnosti a použitelnosti symetrických šifer, a teorii kódů. Je kryptologem a expertem v oblasti matematické bezpečnosti v Kompetenčním centru pro kryptologii a biometrii Raiffeisen Bank International a přednáší modelování bezpečnosti na MFF UK.

Tomáš Rosa je doktorem v oboru kryptologie s Cenou rektora ČVUT, studoval kombinovaně na FEL ČVUT a MFF UK v Praze. Věnuje se matematické a systémové bezpečnosti počítačů, jeho práce pomohla zlepšit řadu celosvětových standardů. Tomáš je vedoucím architektem v Kompetenčním centru pro kryptologii a biometrii Raiffeisen Bank International a přednáší modelování bezpečnosti na MFF UK.

Zero-Trust Security Architecture

Marek Petko

Today, it is entirely natural to expect that we can order goods, communicate with family, stream live content, and work — anytime, anywhere, and instantly via the Internet. Since the Internet's inception over thirty years ago, the physical location of a service has been irrelevant to users, and with the advancement of mobile broadband, the user's location has become equally insignificant. Services reside somewhere; users are everywhere. Despite this, for decades, commercial and non-commercial organizations alike have tried to resist this reality by creating isolated network enclaves governed by their own, often softer, security rules. Meanwhile, technological progress, in the form of cloud or BYOD, continues to erode these boundaries, working against our efforts. Cybercriminals have seized this opportunity, breaching our secured perimeters and exploiting misplaced trust to achieve their malicious goals. The Zero Trust paradigm offers a possible answer: a way to enable secure use of organizational resources based not on implicit trust, but on uncompromising authentication, least privilege authorization, and other dynamic attributes.

Kdo si hraje, nezlobí – Večerní workshop (pondělí)

Pavel Šafl, Pavel Šimerda, Sára Šimerdová

Pondělní večer využijeme netradičně. Místo večerní přednášky si popovídáme o hračkách a pomůckách, co se dají využít nejen v informatice na školách. Přivezeme nějaké hračky na ukázku a budeme si hrát. Když jsme se tomuto tématu věnovali na OpenAltu, někteří se na večerní párty tak zabrali do zkoumání Computer Engineering for Babies, že se třeba na hodinu vyřadili z diskuzí u piva a limonády. Tak uvidíme, co se stane na EurOpen.

Radarová technika pro 21. století

Jenda Hrach

Přehled aktuálního stavu a vývoje radarové techniky. Ukážeme si různé druhy radarů: pasivní zaměřování vysílačů, bistatický radar, klasický primární radar (na počasí i na letadla), budoucnost s fázovým polem (a jak

vlastně funguje Starlink terminál). U každé kategorie si ukážeme historický vývoj a současný state-of-the-art, ale také „co se s tím dá dělat za vylomeniny“, například když to neukazuje jenom „že tam něco je“, ale i „co to je“ – dostáváme různá další data, která na první pohled nejsou laikovi úplně zřejmá, a která umožní identifikaci cíle.

Myslím si, že dnes je v možnostech motivovaného jednotlivce nebo malé skupiny postavit si funkční modely prezentovaných zařízení, a osobně jsem to tak s některými z nich už udělal, proto představím i vyloženě hands-on zkušenosti.

Jak nebojovat se sekuriťáky během incidentu

Nicol Daňková

Kyberbezpečnostní incident je boj sám o sobě. O něco horším se stává, když proti sobě stojí více stran než pouze útočníci a firma. Nezřídka kdy se stává, že Incident Respondeři musí čelit různým nástrahám, které přicházejí z vnitřku organizace. Tato přednáška se zaměřuje na to, jak vypadá průběh bezpečnostního incidentu a jak můžeme zajistit co nejsnadnější průběh pro všechny zúčastněné. Projdeme si možnosti přípravy, jaké věci je fajn mít po ruce, třeba pro případ ověření aktivit, nebo naopak si projdeme i reálné příklady toho, jak to opravdu nedělat.

Vzory v IT: význam vhodné notace a programovací jazyk APL

Pavel Tišnovský

Lidé jsou vynikající v rozpoznávání vzorů a navíc je relativně snadné se vycvičit k rozpoznávání nových typů vzorů. Mj. i z tohoto důvodu se v minulosti i současnosti objevuje poměrně velké množství notací zápisu, které nejsou „lineární“, ale spíše dvourozměrné. Patří sem například notový zápis, matematické vzorce, notace používaná v kvantové fyzice, strukturální vzorce v chemii atd. Vhodně zvolená notace může ovlivnit způsob myšlení. To je základní myšlenka některých programovacích jazyků, zejména APL a do jisté míry i Fortress a Mathematica. V této prezentaci budeme hovořit o myšlenkách začleněných do všech jazyků podobných APL. Zápis programů v těchto jazycích připomíná hieroglyfy, ovšem po zaučení se

zcela změní způsob myšlení programátora. Na přednášce si dále popíšeme operátory v APL, takzvané kombinátory, vlaky a v neposlední řadě i tzv. point-free programming.

Wait, it's all LISP? Always has been

Lukáš Hozda

Lisp je zajímavý programovací jazyk, který si většina v dnešní době představí jen jako neskutečnou změť závorek (je to ale pravda?). Přitom je to jeden z nejstarších programovacích jazyků, který jako první přišel s koncepty, které dnes považujeme jako naprosto všední, jako například if statement.

Jeho vliv se promítnul do řady jazyků a technologií, které vizuálně mají k Lispu daleko. Shodou okolností se dostal i na místa, kde bychom ho vůbec nečekali. Jak je možné, že Lisp může za moderní web?

Pokud sami máte něco zajímavého, co byste rádi zařadili do programu, přivezte a dejte nám vědět. Zároveň můžeme ten čas využít ke sdílení inspirace a nápadů na podzimní dětskou konferenci v Nečtinách.

Tutorial – Bezpečné programování: Schopnosti programovacího jazyka

Lukáš Hozda, Pavel Šimerda

Budeme programovat v Rustu. Na něm si ukážeme, jaké vlastnosti má mít programovací jazyk, aby zároveň pomohl zajistit bezpečnost a spolehlivost kódu, nenutil nás zaplatit výkonovým propadem a zároveň nám tvorbu a úpravu software zásadním způsobem neztížil. Je pravda, že spolehlivost, výkon a snadnost se navzájem tak trochu vylučují, na druhou stranu tvorba výkonného a spolehlivého kódu nemusí být úplné peklo.

Tutoriál je pro všechny, kteří se o bezpečné programování zajímají. Vůbec nemusíte programovat v Rustu. Všechno, co budeme dělat, můžete v nějaké míře přenést do jiných jazyků a prostředí. Borrow checker je fajn a mnozí by ho měli rádi i v C++, ale spousta kritického software je v jazycích, které nic takového nemají. Můžeme se o tom ještě pobavit před odjezdem z konference.