NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

06/2023

ČERVEN

Expertní zástupci Platformy k výzkumu a vývoji se setkali již po šesté

Setkání členů Platformy pro výzkum a vývoj v oblasti kybernetické a informační bezpečnosti se uskutečnilo 20. června v prostorách Fyzikálního ústavu Akademie věd ČR. Jednání otevřela série přednášek na téma aktuálních trendů v různých oblastech výzkumu kybernetické a informační bezpečnosti v podání expertů NÚKIB. Možnostem financování výzkumu a vývoje se ve svých příspěvcích věnovali zástupci Technologického centra Praha, Technologické agentury a Ministerstva vnitra. Online vstup měl cyber attaché NÚKIB pro Izrael, který přiblížil možnosti rozvoje českého kyberbezpečnostního výzkumu v zahraničí. V rámci odpoledního programu proběhly čtyři kulaté stoly zaměřující se na aktuální témata v oblasti výzkumu a vývoje v kybernetické bezpečnosti. Účastníci z různých sektorů si tak mohli vyměnit své zkušenosti, navázat nové kontakty a diskutovat o možnostech další spolupráce.

Z Česka se může stát centrum pro kvantové počítače

O vybudování centra pro kvantové počítače v Česku začala jednat ministryně pro vědu, výzkum a inovace Helena Langšádlová a předsedkyně Poslanecké sněmovny Markéta Pekarová Adamová během jejich cesty po USA. Česká delegace byla doprovázena zástupci univerzit a soukromého sektoru, přičemž toto téma bylo projednáváno také v Bílém domě, pro který jsou kvantové technologie bezpečnostním, vědeckým i obchodním tématem budoucnosti. Zájem o vybudování evropského kvantového centra v Česku projevila společnost IBM, jež je aktuálně jedním z největších výrobců kvantových počítačů na světě. Uplynulá jednání představují důležitý krok také pro uzavření memoranda o spolupráci v kvantových technologiích mezi ČR a USA.

V Bukurešti se uskutečnilo šesté zasedání správní rady Evropského centra kybernetické bezpečnosti

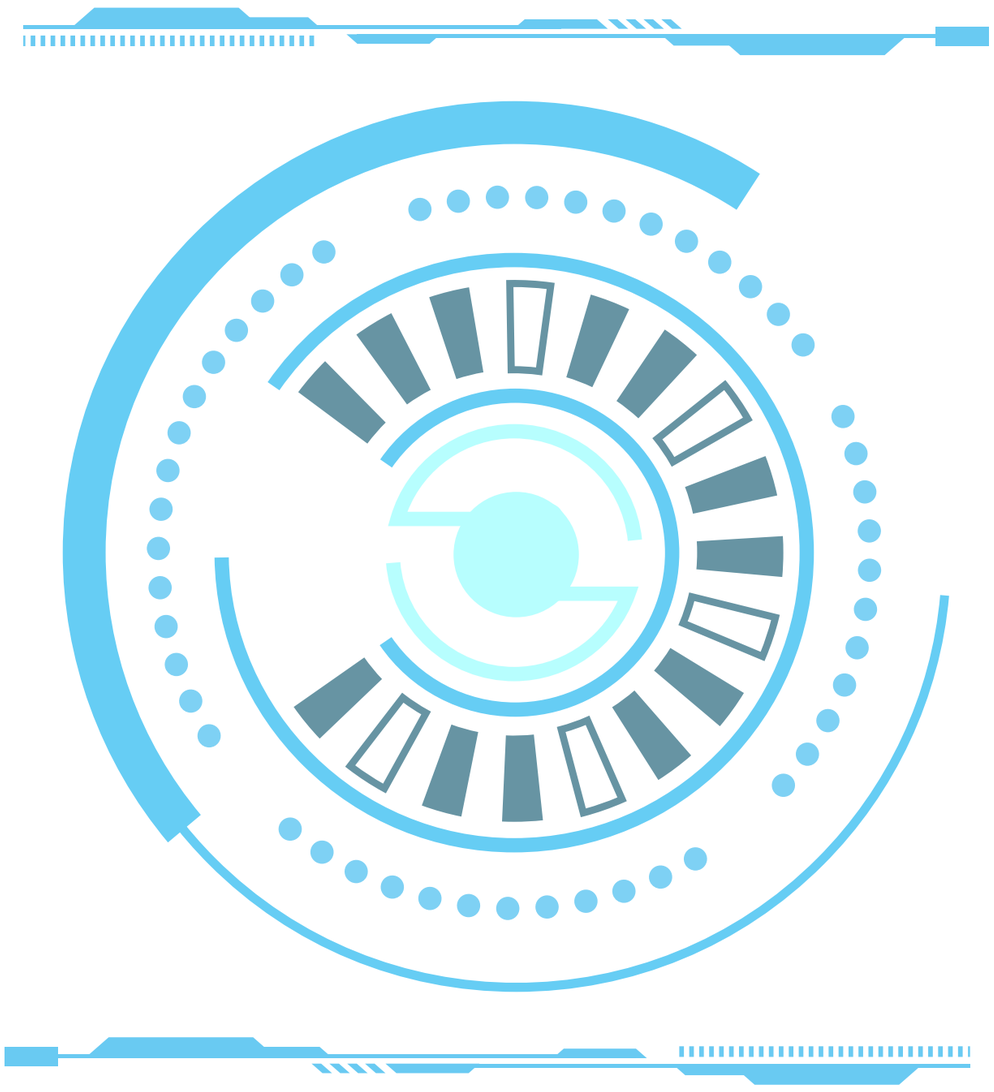
Zasedání, v rámci kterého došlo k setkání zástupců evropských Národních kompetenčních center (NKC), proběhlo ve dnech 8. až 9. června. Jednání ECCC předcházel 7. června tzv. Networking day, kde se zástupci NKC sešli také s reprezentanty Evropské komise a Evropské agentury pro kybernetickou bezpečnost (ENISA). Správní rada jednala mimo jiné o aktuálních činnostech v oblasti rozvoje spolupráce napříč NKC, formách podpory evropské kyberbezpečnostní komunity a o aktuálních možnostech financování výzkumných a vývojových projektů skrze programy Horizon Europe a Digital Europe. Správní rada se poprvé sešla v nově otevřených prostorách ECCC a premiérově byli přítomni noví členové sítě NKC z Norska a Islandu.

Americká agentura CISA oznamuje vydání bíle knihy o výzkumu, vývoji a inovacích

Bíla kniha vydávaná Agenturou pro kybernetickou bezpečnost a infrastrukturní bezpečnost (CISA) se zaměřuje na zvýšení odolnosti kyberneticko-fyzické kritické infrastruktury Spojených států. Dokument definuje tři hlavní kroky, které budou muset být učiněny pro zajištění integrovanějšího přístup k výzkumu: provedení analýzy důsledků a faktorů rozhodování pro snížení rizik v kritických službách; pochopení společenských rozměrů zvyšování odolnosti bezpečnostních systémů a zapojení koncových uživatelů do výzkumu kyberneticko-fyzické infrastruktury. Dokument vypracovala pracovní skupina složená z odborníků z akademické, soukromé i státní sféry ve spolupráci se sdružením zabývajícím se kybernetickou odolností, které zastřešuje CISA. Kniha také doporučuje desítku opatření, jimiž by se měl federální výzkum řídit pro efektivnější naplnění národních priorit v oblasti zvyšování kybernetické bezpečnosti.

Aplikace pro správu hesel 1Password přibližuje budoucnost bez hesel

Správa hesel prostřednictvím aplikací patří k rozšířeným metodám pro zajištění bezpečnosti uživatelských přístupů. Aplikace 1Password ovšem výrazně zjednodušuje užívaní správce hesel a to bez ohrožení bezpečnosti uživatelů. Uživatelé 1Password se ke svým online účtům nebudou přihlašovat za využití klasických hesel, ale pomocí tzv. přístupových klíčů (passkeys). Přístupové klíče představují metodu digitální autorizace přístupu, které jsou již dnes běžně využívány například v aplikacích pro internetové bankovnictví. Přístupové klíče k jednotlivým webovým stránkám nebo aplikacím jsou uloženy v trezoru aplikace. Při pokusu o přihlášení do dané služby uživatel přihlášení pouze potvrdí např. skenem otisku prstu, nebo tváře. 1Password si sám pamatuje webové stránky a aplikace spojené s přihlášeními pomocí přihlašovacích klíčů, a tedy jejich využití pro přihlášení uživateli sám automaticky nabízí. Klíče jsou navíc synchronizovány napříč všemi zařízeními uživatele a lze je také bezpečně sdílet s dalšími uživateli prostřednictvím sdílených trezorů. V případě, že aplikace nebo webová stránka, kterou uživatel využívá, nepodporuje možnost využití klíčů, 1Password sám službu pravidelně monitoruje a upozorní uživatele, když daná služba začne přístupové klíče podporovat. Přístupové klíče jsou v souladu s autentizačními standardy aliance FIDO, díky čemuž jsou považovány za bezpečnější než tradiční hesla. Případný úspěch aplikace 1Password by mohl vést k dalšímu posunu ve snaze o opuštění potřeby využívaní tradičních hesel.



Rozšíření pro virtuální realitu umožňuje vnímat čichové vjemy

Výzkumníci ze City University of Hong Kong a Beihang University vyvinuli bezdrátový systém čichové zpětné vazby, který integruje pachy do virtuální reality (VR) a rozšířené reality (augumented reality – AR). Systém využívá miniaturní generátory pachů, které uvolňují různé vůně a poskytují tak jejich nositeli vjemový zážitek. Generátory pachů jsou vyrobeny z pružných a lehkých materiálů a lze je nosit jako náplast na horním rtu, nebo jako pružnou obličejovou masku s několika typy pachů. Zahřátím a roztavením vonného parafínu na generátorech se uvolňují různé vůně. Parafín je umístěný na vyhřívací podložce a v závislosti od intenzity jejich zahřátí je možno regulovat také koncentraci pachu. Generátor pachů je možno využívat bezdrátově, takže běžné využití VR či AR nijak neomezují. Potenciál pro využití této technologie nespočívá jen v zaměření na zábavu, jako například sledování 4D filmů, ale také v praktických oblastech života, jako je třeba oblast vzdělávání nebo v rámci medicínských účelů. Praktickým příkladem využití této technologie je léčba pacientů s amnézií, kteří by si za pomoci uvolňování různých vůní mohli být schopni vybavit ztracené vzpomínky. Výzkumníci, jež generátor pachů vyvinuli, již pracují na jeho aktualizaci se zaměřením na rychlejší dobu odezvy a na zmenšení velikosti.

Věděli jste, že...

...v červnu proběhla ve švédském Stockholmu a Uppsale konference zaměřená na udržitelnost akademického prostředí? Akce je pořádaná evropskou radou Eurodoc, která zastupuje vědce po celé Evropě. Mezi klíčová témata se dlouhodobě řadí například hodnocení akademických výstupů a připravovaná reforma systému jejich hodnocení. Současný systém založený na značně subjektivním hodnocení recenzentů pro odborné časopisy totiž nezřídka upřednostňuje kvantitu publikací konkrétního autora před skutečnou kvalitou publikovaných výstupů.

Byla zveřejněna druhá zpráva o pokroku ve zvyšování bezpečnosti evropské 5G sítě

Členské státy Evropské unie (EU) s podporou Evropské komise (EK) a ENISA zveřejnily druhou zprávu o pokroku ve věci implementace nástrojů pro zajištění bezpečnosti evropské 5G sítě (The EU Toolbox on 5G cybersecurity). Tento dokument obsahuje strategická a technická opatření soustředěná na zmírnění rizik souvisejících s 5G sítěmi. Zpráva zdůrazňuje pokrok ve věci přípravy legislativních opatření členských států pro posuzování dodavatelů a omezovaní rizik spojených s dodavatelským řetězcem. EK vyjádřila znepokojení nad riziky spojenými s některými dodavateli jako například Huawei nebo ZTE a zvažuje vydání rozhodnutí o jejich omezení nebo úplném zakázaní jejich nasazování v rámci evropské 5G sítě. Kromě toho EK přistoupila k posouzení a vyhodnocení zranitelností ve svých vlastních komunikačních systémech a zavázala se nepoužívat jakékoli produkty výše uvedených společností. Zpráva o pokroku rovněž obsahuje doporučení členským státům, aby posílily vlastní bezpečnostní opatření, posoudily rizikovost svých dodavatelů, přestaly používat zařízení od těch, kteří vykazují vysokou rizikovost, a rozšiřovaly evidenci kapacit mobilních operátorů pro přechod na 5G. V nadcházejícím období se EK bude zabývat zkoumáním dalších možných opatření ke zvýšení odolnosti vnitřního trhu EU, včetně rozšíření aktuálních legislativních rámců jak na evropské, tak na národní úrovni. Bezpečnost 5G sítí představuje pro EK klíčovou prioritu z hlediska celé bezpečnostní strategie evropských komunikačních sítí.

Nový systém využívající umělou inteligenci zvýší bezpečnost vůči phishingu

Společnost IRONSCALES oznámila spuštění beta verze Themis Co-pilot pro Microsoft Outlook. Jedná se asistenční rozšíření pro Outlook, jež využívá umělou inteligenci pro autonomní hlášení bezpečnostních hrozeb. Themis Co-pilot může kontinuálně monitorovat bezpečnost elektronické komunikace, získávat data o nejnovějších typech hrozeb v reálném čase a automaticky označovat podezřelé e-maily. Díky neustálému zpracovávání těchto dat je umělá inteligence schopna označovat hrozby s výrazně nižší pravděpodobností falešně pozitivních hlášení. Zároveň je schopna reagovat na nově vznikající hrozby tzv. nultého dne (zero-day threats, tedy zranitelnosti, které ještě nejsou obecně známé). Themis Co-pilot navíc generativní umělou inteligenci kombinuje s lidskými poznatky. Do svých monitorovacích procesů totiž nekomponuje jenom dostupná data, ale učí se také na základě zpětné vazby od uživatelů, kteří mohou relevantnost zranitelnosti potvrdit, nebo vyvrátit. Vzájemná integrace umělé a lidské inteligence představuje komplexní přístup k zabezpečení e-mailů již na úrovni koncových uživatelů bez ohledu na úroveň jejich znalosti kybernetické bezpečnosti, což představuje potenciál pro účinný boj proti phishingovým útokům.

„Česko musí začít jednat. Máme velice dobré teoretické a experimentální schopnosti a musíme se dostat do technologické fáze."

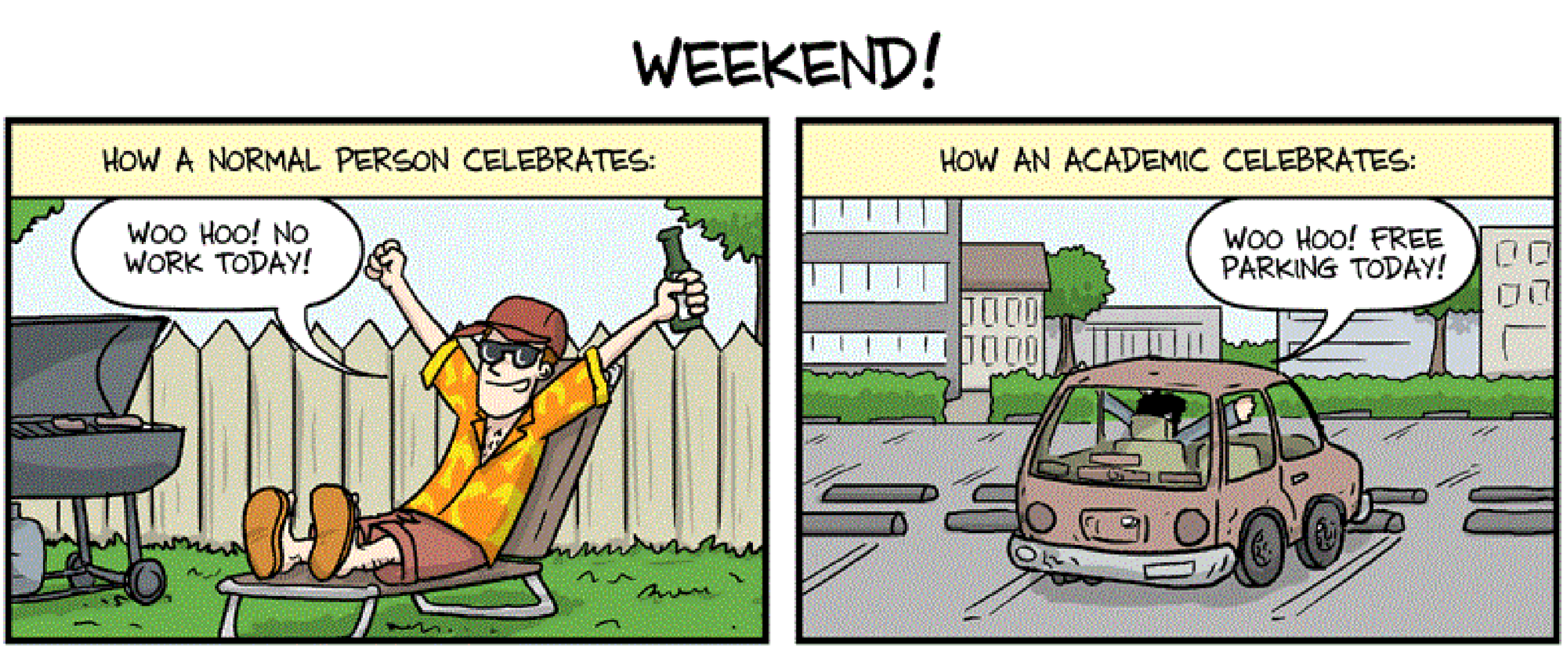
Radek Holý
prorektor ČVUT

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

06/2023



Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno

Tel.: +420 541 110 777

P.O. BOX 17, Brno 16, CZ 616 00

Oddělení vědy, výzkumu a inovací

Olšanská 36/9

130 00 Praha

Tel.: +420 607 032 806

e-mail: vyzkum@nukib.cz