NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

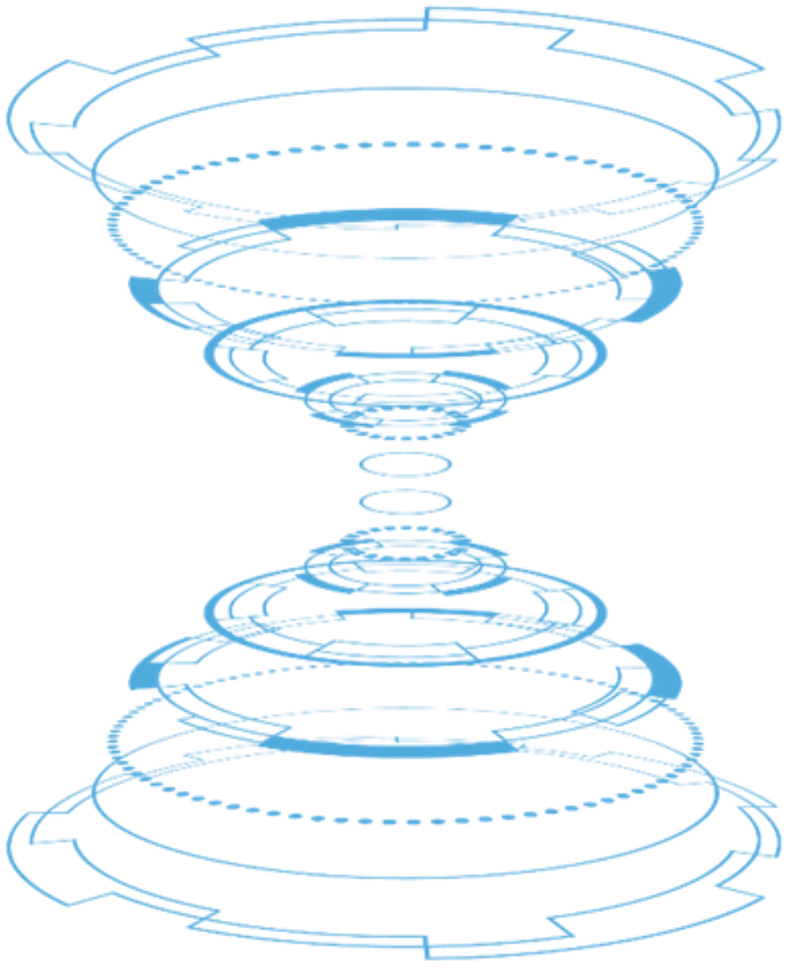
Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

02/2023

ÚNOR

Grantová agentura České republiky vyhlásila soutěže na rok 2024

Grantová agentura České republiky (GA ČR) v průběhu února oznámila vyhlášení výzvy k předkládání projektů do pravidelně realizovaných soutěží Standardní projekty, JUNIOR STAR, POSTDOC INDIVIDUAL FELLOWSHIP, Mezinárodní projekty a projekty Lead Agency. Termín pro podání projektů je stanoven na 4. dubna 2023, přičemž úspěšné projekty budou řešeny od roku 2024. Soutěže doznaly řady změn, z nichž nejvýznamnější je možnost pozastavit řešení projektu na 6-18 měsíců. Upravena byla také pravidla pro nakládání s přidělenými finančními prostředky, která by měla být v nové podobě výrazně flexibilnější. Výsledky soutěží budou vyhlášeny v listopadu.



Uskutečnil se 20. ročník konference České dny pro evropský výzkum

Konference s názvem CZEDER organizovaná Technologickým centrem Praha ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy ČR, se konala 14. února, a to jak ve fyzické tak i online podobě. Prostřednictvím tohoto hybridního formátu CZEDER 2023 představil příklady výsledků 12 projektů rámcových programů s českou účastí, shrnul úspěchy českého předsednictví v oblasti výzkumu a inovací a poskytl odborníkům prostor pro diskusi o dotačních příležitostech. Videozáznam z konference je veřejně dostupný prostřednictvím webových stránek CZEDER.

Výzva European Excellence Initiative aktualizovala své přílohy

Dne 22. února Evropská komise zveřejnila informace o nové samostatné povinné příloze o nákladech na výzkum a inovace, kterou musí žadatelé přiložit ke své dokumentaci. European Excellence Initiative je program zaměřený na prohloubení spolupráce mezi univerzitami, zejména potom z těch zemí, které v oblasti výzkumu a inovací nenaplňují svůj potenciál. Cílem programu je zvýšit globální konkurenceschopnost evropských univerzit ve všech oblastech, na které se program Horizon Europe zaměřuje.

Horizon Europe zahájil projekt hodnocení naslepo

Evropská komise zahájila pilotní projekt, který umožní předkladatelům projektů zůstat v plné anonymitě. Absence informací o totožnosti žadatele by měla přispět v maximální možné míře k zajištění objektivity hodnotitelů. Evaluační proces by tak v případě slepého hodnocení (blind evaluation) neměl být ovlivněn žádnou formou zaujatosti či nedůvěry vůči předkladatelům. Všechny předběžné návrhy z klastrů 1, 4 a 6 ve výzvách 2023/2024 musí být podány anonymně. Pro jasnější specifikaci fungování tohoto systému hodnocení uspořádala Evropská komise také zpětně dostupný online seminář.

Umělá inteligence se stává významným prostředkem posílení kybernetické bezpečnosti

Výzkumníci z Pacific Northwest National Laboratory (PNNL) ve Spojených státech vytvořili schéma autonomní kybernetické obrany využívající umělou inteligenci. Konkrétně se jedná o formu umělé inteligence (UI) známou jako deep reinforcement learning (DRL), která dokáže detekovat změny v prostředí počítačové sítě a přijmout preventivní opatření k odvrácení potenciálních útoků. Základem pro vytvoření celé autonomní obranné architektury byl návrh simulačního prostředí pro testování různých scénářů útoků pocházejících od širokého spektra protivníků. Toto dynamické prostředí umožňuje výzkumníkům porovnávat účinnost různých obranných mechanismů, včetně těch postavených na UI. Začlenění umělé inteligence založené na hlubokém učení (deep learning) do bezpečnostních nástrojů umožňuje nepřetržitě monitorovat síťový provoz a v případě zjištění rizika okamžitě přijmout řešení k jeho eliminaci. DLR však kromě detekce potenciálních rizik a narušení bezpečnosti dokáže také vyhodnotit, zda rozhodnutí, které přijme, bude mít pozitivní, nebo negativní dopad na celkový stav bezpečnosti sítě. Součástí procesu učení u DLR je totiž nejen analýza databáze předchozích útoků, jako je tomu v případě hlubokého učení, ale také zpětná vazba, tedy zda mělo konkrétní rozhodnutí pozitivní, nebo negativní dopad. To vede ke vzniku komplexních rozhodovacích plánů, které jsou v případě útoku autonomně aplikovány. Použití DLR UI v nástrojích pro zajištění kybernetické bezpečnosti se jeví jako vysoce efektivní, jelikož v simulačním prostředí dokázala čelit 95 % útoků.

Nová technologie umožní používat chytré telefony jako RFID čtečky

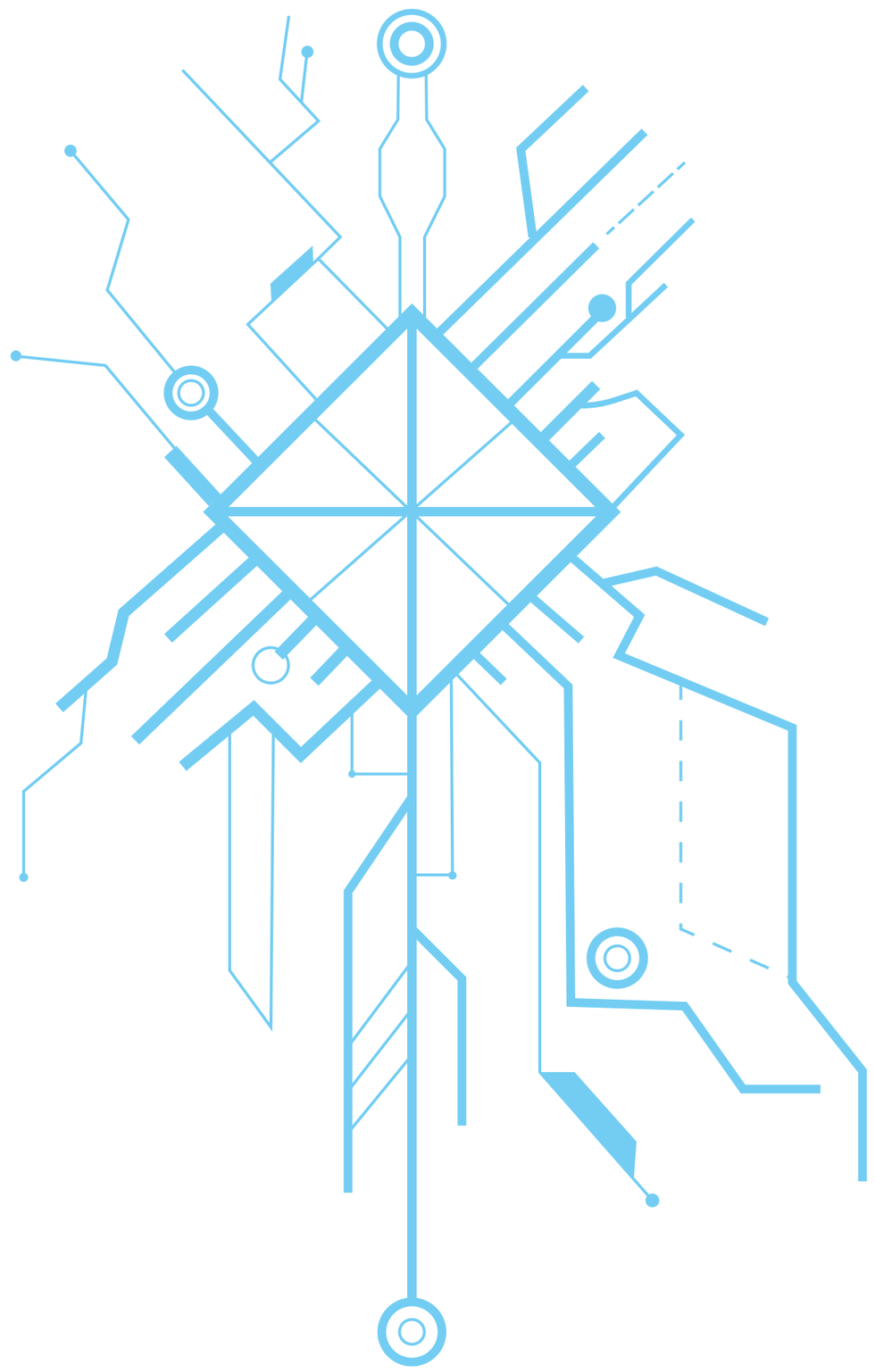
Technologie vyvinutá na Kalifornské univerzitě v San Diegu je dalším využitím schopnosti chytrých telefonů číst bezdrátové signály. Univerzitou vyvinuté čipy vysílají signály na specifických frekvencích, jež za použití vhodného softwaru mohou být identifikovány chytrými telefony prostřednictvím připojení Bluetooth nebo WiFi. Chytrý telefon se tak může stát „RFID čtečkou“, kterou lze použít v celé řadě různých oblastí a situací. Mikročip se například muže stát součástí balení jakéhokoliv produktu, což by chytrým telefonům umožnilo okamžitý přístup ke všem informacím o něm. Tento technologický průlom využívá poznatků z oblasti zpětné komunikace, která je založena na využití pouze těch typů signálů, jenž jsou již generovány chytrými telefony a jsou pak pouze přesměrovány zpět ve formátu zpracovatelném pro telefony. Klíčovou výhodou této technologie je skutečnost, že tato forma komunikace vyžaduje pouze velmi nízkou spotřebu energie. Čipy o velikosti zrnka písku potřebují tak málo energie, že mohou být napájeny přímo signály LTE. Vývoj zařízení, která nepotřebují baterie a místo toho získávají energii formou tzv. radiofrekvenčního sběru energie (RF energy harvesting), by výrazně snížil nejen jejich výrobní náklady, ale také zátěž pro životní prostředí, která je s výrobou čipů spojena.

„Elektronický odpad, zejména baterie, je po změně klimatu jedním z největších problémů, kterým planeta čelí.“

**profesor Dinesh Bharadia,
Kalifornská univerzita San Diego**

Malware ChromeLoader cílí na hráče pirátských verzí videoher

Jednou z metod, jak se malware může účinně šířit, je jeho ukrytí v softwaru, který se stává cílem pirátského šíření. Tímto způsobem se začal šířit také malware ChromeLoader, jenž se poprvé objevil v lednu 2022. Malware původně zaměřený na krádež přihlašovacích údajů z webového prohlížeče je však nyní mnohem silnější a kromě krádeže citlivých dat dokáže na hostitelská zařízení nasadit i ransomware. ChromeLoader byl původně distribuován prostřednictvím formátu ISO, nyní však využívá soubory virtuálního pevného disku (VHD). Tento typ souborů se často používá pro programy videoher, které jsou pak distribuovány v pirátské podobě. Soubory VHD se svými názvy maskují jako hacky (získávání neférové výhody ve hře manipulací s programovým kódem videohry) nebo cracky (software určený k prolomení ochrany videohry před pirátským šířením) pro videohry Nintendo a Steam. Uživatel tak stahuje škodlivý soubor VHD domnění, že stahuje program související s hrou. Po spuštění má malware za cíl kompromitovat webové prohlížeče, například Google Chrome, a upravit jejich nastavení tak, aby uživatele přesměroval na pochybné reklamní stránky schopné dalšího poškození. Některé verze tohoto malwaru jsou také schopny infiltrovat systémové soubory operačních systémů Windows a macOS. Mezi oblíbené videohry a software, na které se tento malware zaměřuje, patří Red Dead Redemption 2, Need for Speed, Call of Duty, Microsoft Office nebo Adobe Photoshop.



Vývoj kvantových počítačů zaznamenal významný posun

Odborníci působící na univerzitě v Sussexu prokázali schopnost kvantových bitů (qubitů) přenášet se mezi mikročipy v kvantových počítačích. Nová technologie nazvaná "UQ Connect" využívá propojení elektrickým polem, které umožňuje přesouvat qubity z jednoho kvantového mikročipu do druhého s obrovskou rychlostí a přesností. Díky tomu je možné tyto čipy spojovat do větších modulů a vytvářet tak výkonnější kvantové počítače. Navíc bylo ověřeno, že po spojení čipů do modulů zůstala kvantová povaha qubitů, spočívající v jejich schopnosti být současně 0 i 1, zachována. Rychlost a přesnost, s jakou došlo k přenosu qubitů, jsou nejen světovými rekordy, ale také řádově lepšími výsledky, než jaké byly naměřeny u předchozích řešení. Současné hodnoty tak představují klíčový objev pro další vývoj, neboť otevírají cestu ke vzniku dostatečně výkonných kvantových počítačů schopných efektivně a stabilně řešit složité problémy. Kvantové počítače by tak mohly pomoci řešit mnoho důležitých společenských problémů téměř ve všech odvětvích, od leteckého průmyslu až po finanční sektor.

Věděli jste, že?

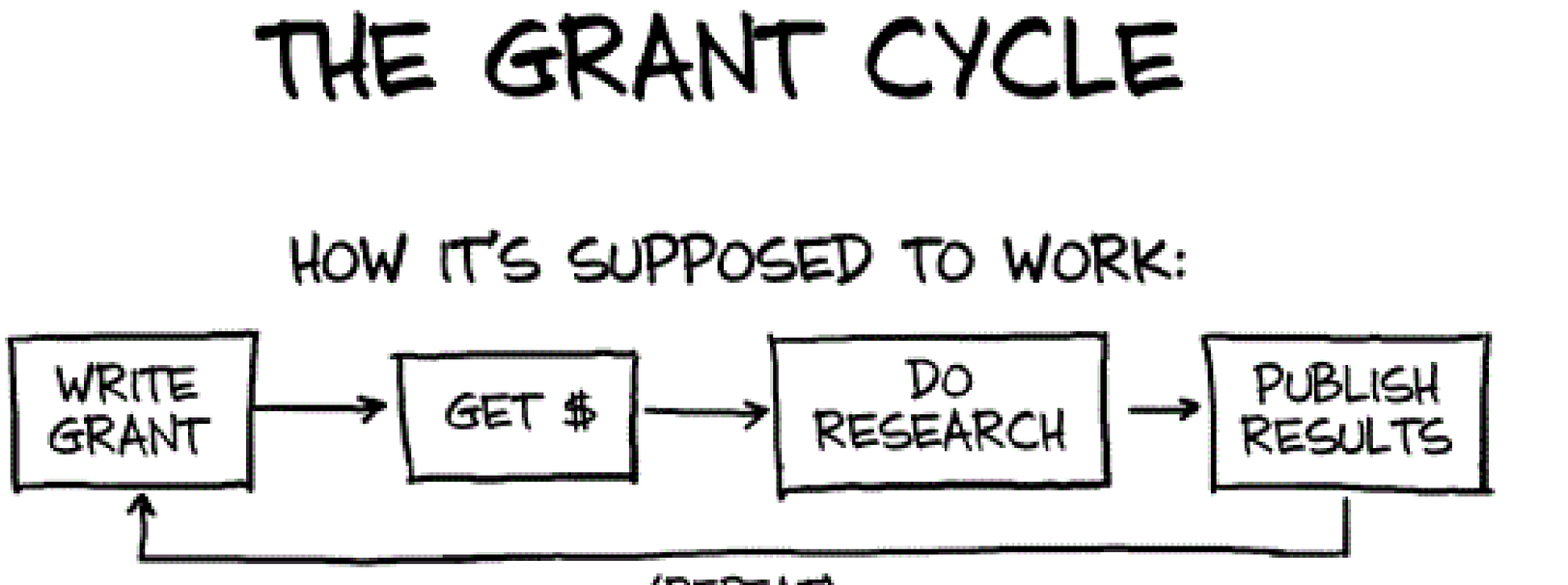
Ministerstvo obrany Spojených států amerických každoročně pořádá výzvu nazvanou Hackněte Pentagon (Hack The Pentagon). Letos se konal již třetí ročník této výzvy, která zaznamenala svou premiéru v roce 2016. V rámci této výzvy se mohou odborníci na kybernetickou bezpečnost výměnou za finanční odměnu pokusit odhalit zranitelná místa v kybernetické struktuře Pentagonu. Za dobu své existence se soutěže zúčastnilo 600 etických hackerů, kteří společně odhalili více než 700 zranitelností.

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

02/2023



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: a.janovec@nukib.cz