Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

VEŘEJNÁ PODPORA

Veřejná soutěž GAMA 2

Technologická agentura České republiky (TA ČR) vyhlásila dne 2. června 2021 třetí veřejnou soutěž v Programu na podporu aplikovaného výzkumu, experimentálního vývoje a inovací GAMA 2, podprogram 2. Veřejná soutěž se zaměřuje především na komercionalizaci inovačních řešení, růstu a rozvoje malých a středních podniků a na ověřování výstupů a výsledků aplikovaného výzkumu z hlediska jejich praktického uplatnění nebo komerčního využití. Více informací o veřejné soutěži naleznete zde.

Program MSCA 2021

Evropská komise vyhlásila v rámci rámcového programu Horizon Europe nové výzvy v grantovém programu Marie Skłodowska-Curie Actions (MSCA) na podporu rozvoje dovedností a kariérního růstu výzkumníků. V letošním roce nabízí MSCA celkem 822 milionů EUR, a to v pěti podprogramech. Podpora je určena především na podporu výzkumníků nebo výzkumných institucí na jejich podporu pro doktorandy, postdoktorandy a mladé vědce. Více o jednotlivých podprogramech naleznete zde.

AKCE

Konference SCI-PO 2021

Byla zahájena registrace na již čtvrtý ročník konference SCIPO (Science Policy), která se uskuteční 30. září 2021 hybridní formou. Hlavním tématem letošního ročníku jsou dopady výzkumu, vývoje a výzkumných infrastruktur na společnost. Registrace je bezplatná. Více informací můžete nalézt zde.

PUBLIKACE

Horizon Europe Programme Guide zveřejněn na FTOP

Dne 17. 6. byl na FTOP zveřejněn Průvodce programem Horizont Evropa - Horizon Europe Programme Guide. Průvodce má přístupnou formou informovat o struktuře, rozpočtu a politických prioritách programu. Zahrnuje také detaily týkající se přípravy projektu a má napomoci zodpovědět i konkrétní praktické otázky, na které mohou uživatelé narazit. Program je ke stažení na tomto odkazu.

Poltergeist útok vůči autonomním vozidlům

(18. 06. 2021; theregister.com) Tým výzkumníků z čínské Zhejiang University a americké University of Michigan nalezl nový typ útoku, který se dá využít proti autonomním vozidlům. Tento typ útoku nazývají „Poltergeist“. Ten dokáže zmást řídící systém vozidla tak, aby některé překážky neviděl nebo naopak viděl překážky, které vůbec neexistují. Poltergeist využívá zranitelnosti způsobené tím, že digitální kamery autonomních vozidel využívají ke stabilizaci obrazu inerciální měřící jednotky. Pomocí specifických zvukových vln se podařilo výzkumnému týmu kamery zmást natolik, že dokázali zamlžit obraz z digitálních kamer. Tím dokázali donutit autonomní vozidlo ignorovat některé překážky, které se mu vyskytly v cestě. Výzkumníci sami zařadili tento typ útoku do nové větší třídy útoky nazývané „AMpLe“. Tato třída zahrnuje útoky, které využívají fyzikálních nástrojů k útoku na systémy strojového učení.

Komentář: Bezpečnost autonomních vozidel představuje jednu z hlavních výzev jejich zavádění do běžného provozu. Poukázání na tento nový typ útoku je tak důležité pro větší zabezpečení budoucnosti autonomní mobility. Poltergeist byl dokonce natolik účinný, že dokázal ve 100% pokusných případů donutit autonomní vozidlo ignorovat překážku a v 87.9% případů dokázal vozidlu vnutit do rozhodování překážku, která ve skutečnosti neexistovala. V reálném provozu by tak mohlo jít o závažný bezpečnostní problém, který by měl bezprostřední dopady na zdraví a životy lidí.

Adversarial Octopus – nový typ útoku proti systémům rozpoznávání obličeje

(25. 06. 2021; cyware.com) Nový typ útoku, který nese název „Adversarial Octopus“ se zaměřuje na několik nástrojů rozpoznávání obličejů, které využívají umělou inteligenci. Tento typ útoku byl představen skupinou výzkumníků z firmy Adversa. Adversarial Octopus útoky dokážou pozměnit fotografie tak, aby je rozpoznávací algoritmy vyhodnotily jako úplně jiné osoby. Dle tvůrců může být tento typ útoku využit nejen k získávání přístupu do různých zařízení a systémů, ale také v případě vytváření pokročilých „deep fakes“, jejichž rozlišení by mohlo být problémem pro řadu v současné době dostupných nástrojů. Tento útok dokáže překonat většinu služeb, aplikací a API pro rozpoznávání obličejů. Výzkumný tým toto demonstroval na útoku proti PimEyes, což je jeden z nejpokročilejších online nástrojů pro rozpoznávání obličejů.

Komentář: Odemykání zařízení a služeb pomocí snímku obličeje se již v minulosti stalo častým terčem nových typů útoků. Předkládaný typ útoku směřuje především na algoritmy umělé inteligence, které jsou k rozpoznávání obličeje využívány. Právě nové typy útoků, které využívají slabin v umělé inteligenci by měli stát v popředí současné pozornosti výzkumné komunity v oblasti kybernetické bezpečnosti, neboť stále více roste počet zařízení a systémů využívajících umělou inteligenci.

PETR MARTINEK; p.martinek@nukib.cz
Oddělení výzkumu a evropské spolupráce, NÚKIB