Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

NÚKIB hledá odborníky na certifikace kybernetické bezpečnosti

Odbor vzdělávání, výzkumu a projektů vypsal výběrové řízení na pozici Specialista EU certifikací kybernetické bezpečnosti. Pokud Vás zajímá tvorba systému evropských certifikací, dohledová činnost a nové technologie a zajímala by Vás práce na NÚKIB tak se neváhejte ozvat! Oceníme také pokud víte o vhodném kandidátovi na tuto pozici a možnost práce na NÚKIB mu zprostředkujete. Celý inzerát na pracovní pozici je dostupný na stránkách NÚKIB.

Konference: Patent Knowledge Week (online)

Ve dnech od 2. do 5. listopadu 2021 pořádá Evropský patentový úřad (EPO) online informační konferenci Patent Knowledge Week věnovanou patentovým informacím a dalším tématům z oblasti duševního vlastnictví. Více informací a možnosti registrace najdete zde.

15th CSIRTs Network meeting

Slovinsko bude v letošním roce místem 15. ročníku síťovací akce pro CSIRT/CERT týmy z celé Evropy. Letošní akce proběhne fyzicky v Ljubljaně ale bude možno zapojit se i online. Akce slouží pro zvyšování spolupráce a kontaktů mezi jednotlivými CSIRT a CERT týmy členských států EU. Více informací o akci naleznete zde.

Bankomaty a strojové učení

(18. 10. 2021; bleepingcomputer.com) Lidé se při výběrech z bankomatů snaží chránit celou řadou způsobů. Jedním z nich je i to, že si při zadávání PIN kódu překryjí ruku vyťukávající číslice druhou rukou. Právě na tuto metody „ochrany“ se zaměřili tým výzkumníků z *University of Padua* (Itálie) a *Delft University of Technology* (Nizozemí). Ve svém článku představují nový útoků zaměřený na rekonstrukci PINů zadaných oběťmi. Vychází ze situace, kdy má útočník přístup ke klávesnici pro zadávání PIN kódu bankomatu a může odpozorovat pohyb rukou oběti. Útok staví architektuře hlubokého učení, která dokáže odvodit PIN z polohy a pohybů ruky při psaní. Výzkumníci tak dokázali správně odhadnout 4-místný PIN až ve 41% případů a 5-místný PIN ve 30% případů. Model umožňuje vyloučit klávesy na základě zakrytí rukou, která nepíše a odvozuje stisknuté číslice z pohybů druhé ruky vyhodnocením topologické vzdálenosti mezi dvěma klávesami.

Komentář: Výzkumníci představili další typ útoků, který využívá nové možnosti, které poskytuje strojové učení a umělá inteligence. Tento útok využívá velmi specifického stavu, kdy si člověk částečně zakrývá ruku píšící PIN kód na klávesnici. Úspěšnost dosledování PIN kódu poté dramaticky klesá čím více / lépe je píší ruka překrytá. Výzkum tak spíše ukazuje potenciál možného zneužití strojového učení spíše než typ útok, který by ve skutečnosti našel nějakého širšího rozšíření.

Parrondův paradox a kvantové šiforvání

(15. 10. 2021; sciencedaily.com) Výzkumníci ze Singapurské *University of Technology and Design* se rozhodli aplikovat koncepty z kvantového Parrondova paradoxu při hledání nové metody pro šifrování. Parrondův paradox je koncept z teorie her, při kterém můžeme pomocí prohození dvou prohraných her dojít k vítěznému výsledku. Ve hře na oboustranné házení kvantovými mincemi, autoři ukázali, že náhodné a určité periodické házení dvou kvantových mincí může změnit očekávanou pozici kvantového chodce z pozice prohrávající na pozici vyrovnanou, respektive na pozici vítěznou. Tým zjistil, že chaotické přepínání pro Parrondy hry s „kvantovými mincemi“ má podobné základní myšlenky a pracovní dynamiku jako šifrování. Navíc může být dobře využito jako nástroj pro kvantové šifrování.

Komentář:

Koncept chaotického přepínání v kombinaci s Parrondovým paradoxem rozšiřuje aplikaci Parrondova paradoxu z pouhého matematického nástroje používaného v kvantové informatice pro klasifikaci nebo identifikaci počátečního stavu a konečného výsledku na nástroj, který má reálné technologické aplikace. Vývoj plně implementovatelné kvantově chaotické Parrondovy hry může vést k překlenutí některých problémů, kterým stále čelíme v kvantovém šifrování.

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