Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

PUBLIKACE

Threat Landscape for Supply Chain Attacks

ENISA vydala 29. 07. 2021 mapování a studii útoků na dodavatelský řetězec. V publikaci můžete nalézt jak definici a základní charakteristiky útoků na dodavatelský řetězec tak i některé typy útoků, u kterých se dá očekávat, že budou v budoucnu důležité. Součástí publikace je i analýza pěti incidentů, které jsou spojeny s útoky na dodavatelský řetězec. Publikace je dostupná zde.

Záznamy z informačních dnů Horizon Europe

Na konci června a v první polovině července proběhla série informačních dnů k programu Horizon Europe. V tento moment jsou záznamy z Klastrů 1, 2, 3 a 5 dostupné ke shlédnutí online. Více informací a odkazy naleznete zde.

Kvantový přenos šifrovacích klíčů

(21. 07. 2021; itsec-nn.com) Konsorcium e-INFRA CZ realizovalo kvantový přenos klíčů skrze kvantový kanál o délce 75 kilometrů mezi Ostravou a polským Těšínem. Kanál měl průměrnou kvantovou chybovost pouze 2,19 %. Realizace proběhla v rámci evropského projektu OpenQKD na který Evropská komise poskytla 15 milionů EUR. V rámci probíhajícího upgradu své sítě je CESNET připraven realizovat kvantové kanály na vláknové infrastruktuře, a to včetně napojení na mezinárodní infrastruktury. Tvoří tak základ první kvantové sítě v České republice. Budoucnost bezpečné komunikace odolné proti dešifrování na kvantových počítačích je v technologiích založených na Quantum Key Distribution (QKD). V zásadě jde o generování náhodných klíčů mezi dvěma stranami, kdy klíč je kódován do kvantových stavů fotonů přenášených kvantovým kanálem. Ten je vysoce odolný proti odposlechům, jednak v něm platí relace neurčitosti umožňující takovýto odposlech odhalit a zároveň není možné duplikovat neznámý kvantový stav. Tyto fyzikální vlastnosti kvantové mechaniky jsou využity v QKD a činí z ní technologii umožňující zabezpečení nejvyšší známé úrovně.

Komentář: Bezpečnost kvantového přenosu dat je jednou z hlavních výzev, které s sebou přináší nastupují kvantová éra. Na předloženém experimentu lze demonstrovat, že ČR má v této oblasti značný potenciál.

Šifrovaní fotografií na cloudových službách

(21. 07. 2021; helpnetsecurity.com) Tým vědců z *Columbia Engineering* představil první nástroj pro šifrování fotografií, které jsou ukládány na cloudových službách od Google, Apple, Flickr a ostatní. V minulosti jsme mohli zaznamenat řadu incidentů, kdy došlo k únikům často osobních fotografií z těchto služeb. Výzkumníci představili nový nástroj s názvem *Easy Secure Photos (ESP).* Pokud si uživatel nainstaluje na své zařízení tuto aplikaci, může poté na cloudové služby ukládat zašifrované fotografie tak, aby nebylo možné je zobrazit případnému útočníkovi nebo dokonce ani provozovateli dané služby. K rozšifrování je poté využíván klíč uložený na jiném digitálním zařízení. Tímto způsobem se výzkumníci snaží předejít nutnosti, aby si uživatelé museli pamatovat nebo ukládat další bezpečnostní klíče a hesla. Nový způsob navíc šifruje fotografie již v zařízení uživatele a nevyžaduje tak žádné změny v současných populárních cloudových službách.

Komentář: Ukládání fotografií do cloudových služeb se často děje automaticky pro pohodlí uživatelů. Ti si přitom nemusí uvědomovat, že ukládání svých fotografií na cloudovou službu jim může přinést značné problémy v případě úniku těchto fotografií. Nástroj, který fotografie šifruje již v zařízení uživatele je tedy vhodným nástrojem, především s ohledem na to, že se výzkumníkům již podařilo jej implementovat do aplikací jakou jsou Google Photos nebo Flickr.

Malware skrytý v neuronových sítích

(22. 07. 2021; vice.com) Čínská akademie věd představila článek, podle kterého se jim podařilo infikovat neuronové sítě umělé inteligence malwarem. Svůj postup výzkumníci demonstrovali na případu, kdy dokázali nahradit až téměř polovinu neuronů AlexNet modelu umělé inteligence neurony malwaru. I při takového změně v daném modelu však stále zůstávala úspěšnost modelu více než 93 %, což ztěžuje případnou detekci takovéhoto malwaru. Výzkumníci tvrdí, že téměř čtvrtina objemu kódu tohoto modelu může být bez problémů nahrazena malwarem bez toho, aniž by bylo možno jej jednoduše detekovat. Některé z pokusných modelů infikování neuronových sítí malwarem byly dokonce podrobeny testu na rozpoznání v 58 antivirových programech. Žádný z těchto antivirových programů je přitom nebyl schopný detekovat.

Komentář: Jedná se o další vektor útoků, se kterým se můžeme v budoucnosti stále více setkávat. V blízké budoucnosti lze totiž očekávat masové nasazování umělé inteligence do téměř všech sektorů lidské činnosti. Výzkumníci navíc ve svém článku popisují i případné scénáře, jak by k podobným útokům mohlo v budoucnu docházet. Navíc se nejedná o první výzkum, který poukazuje na nové hrozby, které mohou vyvstat se zaváděním umělé inteligence. V jednom z dřívějších newsletterů jsme informovali například i o výzkumu, který se zabýval možností zneužití umělé inteligence pomocí obrazových materiálů. Jedná se tak do značné míry o nový trend v oblasti VaV v KB.

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