Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Nová technologie pro odemykání rozpoznáváním obličeje

(22. 03. 2021; indiatimes.com) Odemykání mobilních zařízení pomocí obličeje se v poslední době stalo velmi populárním. Algoritmy rozpoznávání obličeje však bylo možné ošálit například fotografií získanou ze sociálních sítí. Profesor z Brigham Young University D. J. Lee přišel s inovací pro tuto technologii. Vedle rozpoznávaného obličeje potřebuje jeho rozpoznávací algoritmus i speciální gesto ve tváři – může se jednat o mrknutí nebo třeba specifický úsměv. Teprve poté je uživateli povolen přístup k zařízení. K rozpoznávání gest bylo využito strojového učení pomocí neuronových sítí, které pracovalo s více než 8 000 videozáznamů od 50 účastníků výzkumu. Pomocí tohoto data setu se algoritmus „naučil“ rozpoznávat různá gesta v obličej.

Komentář: Představená technologie přidává další ověřovací vrstvu do rozpoznávání pomocí obličeje. To bylo v nedávné době často zneužíváno, a i na sociálních sítích byly často sdíleny jednoduché možnosti, jak rozpoznávací algoritmy obejít. Dle autora je tato technika „natolik bezpečná“, že by se dokonce mohla využívat i pro přístup k internetovému bankovnictví, bankomatům nebo různým úložným prostorům. Nová technologie určitě zvyšuje bezpečnost rozpoznávání obličeje, je však otázkou, zda se skutečně ujme v praxi a dostane se v dohledné době i na běžné mobilní zařízení.

Nový vektor útoku zneužívající strojového učení

(14. 04. 2021; portswigger.net) Výzkumníci z několika australských univerzit představili článek, ve kterém varují o možném novém vektoru kybernetických útoků. ten využívá zranitelnosti spojené se strojovým učením (ML), a především s tím, že nástroje a principy ML jsou stále více zavádění do různých programů a systémů. Nový typ útoků tzv. „Inference attacks“ zneužívá toho, že ML systémy se často učí na reálných datech uživatelů – jménech, datech narození, adresách apod. Zjednodušeně je takovýto systém plněn podvratnými daty tak, aby se dalo zpětně odvodit jaká data byla využita k jeho učení. Výzkumníci mluví o dvou typech *inference* útoků. První z nich je *membership inference*. Ten funguje na principu, že do systému ML jsou vložena reálná data a poté může útočník vysledovat, zda tato data byla využita v rámci datasetu ML. Druhým typem je *attribute inference* u kterého je třeba, aby útočník znal alespoň část dat, která systém využil pro učení. Pomocí postupného vkládání dalších dat se mu může podařit určit, jaké další atributy byly pro ML využity.

Komentář: Představený typ útoků je poměrně složitý na výkon počítače, a proto se v současné době jedná spíše o akademickou záležitost. Vzhledem k rozvoji kvantových počítačů se však může riziko podobných hrozeb v dohledné době zvyšovat.

VEŘEJNÁ PODPORA

Program DOPRAVA 2020+

Technologická agentura České republiky (TA ČR) vyhlásila dne 14. dubna 2021 třetí veřejnou soutěž v Programu na podporu aplikovaného výzkumu, experimentálního vývoje a inovací v oblasti dopravy DOPRAVA 2020+. Program se zaměřuje i na témata jako jsou Digitální technologie (především na umělou inteligenci) a Kybernetické technologie (zabezpečení a konektivita). Více informací o programu je dostupných na stránkách TAČR.

PUBLIKACE

ENISA: Advancing Software Security in the EU

Evropská agentura pro bezpečnost sítí a informací (ENISA) představila novou studii ve které jsou diskutovány některé klíčové elementy softwarové bezpečnosti. Studie se snaží poskytnout i přehled nejrelevantnějších přístupů a standardů v oblasti bezpečného vývoje SW. Studie také reflektuje požadavky na vývoj SW v souvislosti s EU certifikacemi kybernetické bezpečnosti a přidruženými schématy. Publikace je dostupná na stránkách ENISA.

AKCE

SMI2G Event 2021

31. května až 1. června proběhne akce SMI2G Event 2021. Dvoudenní konference bude

zaměřena především na diskuzi ohledně tématu Civilní bezpečnost pro společnost v rámci výzev programu Horizon Europe pro rok 2021. Více informací je bude dostupných zde.

Informační den Klastru 3 - Civilní bezpečnost pro společnost

18. – 19. května 2021 proběhne oficiální evropský informační den k tématům první výzvy bezpečnostního výzkumu v HE. Akce se bude zaměřovat na představení prvních výzev, podmínky a pravidla účasti a výhledové aspekty tohoto clusteru. Více informací a možnost registrace bude dostupná zde.

CzeduCon 2021

Byla spuštěna registrace na Fórum mezinárodního vysokoškolského vzdělávání - CzeduCon 2021. Akce se uskuteční ve dnech 15.–17. 6. 2021. Tematicky se bude letošní ročník zaměřovat na Krizový managment, nové rozpočtové období programu Erasmus+, Nové priority internacionalizace vzdělávání a Strategické řízení a budování kapacit vysokých škol. Akce proběhne zcela online a registrace je bezplatná. Více informací je dostupných zde.

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