Výzkum a nové technologie v kybernetické a informační bezpečnosti

Co píšete při videokonferencích?

(23. 02. 2021; thehackernews.com) Výzkumný tým složený ze zástupců University of Texas a University of Oklahoma (USA) představil nový možný typ útoku, při kterém je možno pomocí videozáznamu z videokonferencí odpozorovat co uživatel píše na své klávesnici. Představený typ útoku funguje v třech základních fázích. V první fázi dojde k základním zpracování a vyčištění videozáznamu. V druhé fázi poté dochází k vysledování pohybujících se rukou uživatele, kdy je obraz rozdělen na části a v rámci nich se snaží identifikovat, kdy dochází ke stisknutí klávesy a kterou rukou tomu tak je. V poslední fázi poté pomocí speciálního algoritmu je sledován pohyb rukou uživatele (především úhel rukou pohybujících se na klávesnici), počet úhozů apod. Na základě těchto dat následně dochází k predikci slova, které uživatel napsal. Výzkumníci pomocí této metody dokázali úspěšně „odpozorovat“ 91 % zadaných uživatelských jmen a téměř 96 % emailových adres. V případě hesel se však úspěšnost pohybovala pouze okolo 20 %.

Komentář: Výzkumy zaměřené na možnosti zneužití videokonferencí jsou vzhledem k současné pandemické situaci poměrně na vzestupu. V tomto případě se však jedná o originální snahu, jak zjistit ještě více informací z videozáznamů. V realitě se však jedná o poměrně náročnou metodu útoku a není tak pravděpodobné, že by se brzy výrazně rozšířila.

Generování „pastí na kanaráky“ pomocí umělé inteligence

(01. 03. 2021; sciencedaily.com) Katedra informatiky z Dartmouth College (USA) představila nový nástroj pro ochranu dat (především v ohledu na duševní vlastnictví). Nový nástroj nese název WE-FORGE a využívá umělé inteligence při tvorbě „pastí na kanárky“ (*canary trap*). Systém využívá umělou inteligenci pro tvorbu vysoce věrohodných podvržených verzí jednotlivých souborů. Případný útočník, který získá přístup do systému je poté postaven před dilema, která z verzí je vlastně ta pravá. WE-FORGE totiž dle autorů dokáže generovat nespočet verzí, které jsou pouze složitě odlišitelné od původní verze, a přitom poskytují neplatná data a závěry. Tento nástroj je tak nejvíce vhodný pro ochranu duševního vlastnictví, různých výzkumů nebo patentů.

Komentář: Jak uvádí sami autoři, nástroj WE-FORGE nutí případného útočníka vynakládat značný čas na určení a rozhodnutí, který ze souborů obsahuje pravdivá data. A ani poté si útočník nemůže být jist, že se rozhodl správně. Takovýto nástroj je určitě vítanou možností pro kybernetickou bezpečnost v situaci, kdy roste počet útoků na instituce, které výzkum realizují jako jsou například univerzity.

Bezplatný kurzu umělé inteligence

(nedatováno; prg.ai) Neziskový spolek prg.ai společně s Českým vysokým učením technickým v Praze, Univerzitou Karlovou, Úřadem vlády České republiky a s podporou velvyslanectví Finska v Praze přináší **bezplatný online kurz Elements of AI.** Kurz vznikl již v roce 2018 a celosvětově má již více než 620 000 absolventů. Ve čtvrtek 25. 3. 2021 dojde k oficiálnímu spuštění české verze tohoto kurzu. Cílem Elements of AI je ukázat, co umělá inteligence umí, jak funguje a jaké jsou její klady ale i možná rizika, která s sebou může přinést. Tento online kurz bude bezplatný a bude vhodný pro širokou veřejnost. Na podzim 2021 bude navíc spuštěna i iniciativa **#AIchallange**, do které se budou moci přihlásit různé firmy a organizace. Cílem této výzvy bude dosáhnout co největšího procenta proškolených zaměstnanců pomocí tohoto kurzu. V rámci propagace kurzu je navíc naplánován i rozsáhlý propagační program včetně launch eventu, doprovodné grafiky a návrhů na příspěvky na sociální sítích.

Komentář: Téma umělé inteligence čím dál více rezonuje i mezi laickou veřejností. Vzhledem k tomu, že kurz nepředpokládá žádné vstupní znalosti bude vhodný pro každého, kdo má o toto téma zájem. Tento kurz může přispět k rozšíření povědomí o umělé inteligenci, a navíc může pomoci vyvrátit i některé mýty, které se k umělé inteligenci vážou.

Nová organizace pro spolupráci v oblasti umělé inteligence

(26. 02. 2021; helpnetsecurity.com) AI Infrastructure Alliance je nová organizace, která spojuje 25 globálních technologických korporací za cílem vytvořit prostředí, kde by firmy a komunity mohli spolupracovat a diskutovat nástroje a vývoj umělé inteligence a strojového učení. Tato organizace si dává za cíl vytvoření a propagaci standardů a *best practices* pro zavádění umělé inteligence a strojového učení. Dále se snaží o posilování otevřeného přístupu k algoritmům, nástrojům, knihovnám a *data setům* umělé inteligence a strojového učení. Z hlediska kybernetické bezpečnosti jsou důležité především cíle jako je podpora diferenciálního soukromí nebo homomorfického šifrování, které mohou pomoci anonymizovat osobní data v datasetech a více tak chránit osobní údaje.

Komentář: Oblast umělé inteligence je v současné době jedním z nejvýrazněji rostoucích odvětvích informatiky. Z hlediska kybernetické bezpečnosti je takováto iniciativa určitě vítána. Tvorba standardů a norem pro umělou inteligenci může snížit případné možnosti zneužití nových algoritmů.

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