Výzkum a nové technologie v kybernetické a informační bezpečnosti

Nový způsob využití umělé inteligence k ochraně zdravotnických technologií

(27. 08. 2020, helnetsecurity.com) Komplexní a složitá zdravotnická zařízení jako tomograf, magnetická rezonance nebo ultrazvuk jsou ovládána instrukcemi z počítače. Chybné vstupy mohou ohrozit jak osobní data pacientů tak je v nejzazších případech i zdravotně ohrozit. Tým výzkumníků z Ben Gurionovy univerzity (Izrael) představil novou techniku, která využívá umělou inteligenci pro detekci anomální (v tomto případě anomálních požadavků ze strany počítače). Technika je založena na identifikaci dvou základních typů anomálií – bezkontextové (zamezuje „očividně“ závadnému vstupu) a kontextové, která bere v potaz charakteristiky pacienta.

Komentář: Přestože je technologie vyvinuta především jako zábrana proti anomální instrukci z počítače může sloužit i jako ochrana případným snahám o zneužití těchto zdravotnických technologií v případných kybernetických útocích. Prostředí zdravotnických zařízení totiž představují jeden z častých cílů kybernetických útoků. V této souvislosti vydal NÚKIB na jaře Doporučení pro chování v případě spear-phishingu pro nemocnice.

Nové možnosti jak oklamat systémy pro rozpoznání obličeje

(11. 08. 2020, darkreading.com) Výzkumníci ze společnosti McAfee představili možnosti, jak lze zneužít současné technologie rozpoznávání obličeje pro rozpoznání osoby jako úplně někoho jiného. Jako příklad použili situaci, kdy by člověk byl schopen na letišti obelstít systém rozpoznání obličeje, který je využíván při ověřování pasu, tak aby jej identifikoval jako jinou osobu. Vedoucí výzkumného týmu uvedl, že jejich cílem bylo pomocí strojového učení vytvořit takovou umělou fotografii, která by sice okem odpovídala fyzickému vzhledu dané osoby, ale zároveň by ji algoritmy využívání pro rozpoznávání obličejů vyhodnotili jako osobu jinou.

Komentář: V současné době, kdy roste míra využívání systémů pro rozpoznávání obličejů (a to nejen v oblasti bezpečnosti), je důležité, aby bylo prováděno více takto proaktivních výzkumů. Možnosti zneužívání technologií rozpoznávání obličejů jsou v současné době jednou z hlavních z rostoucích výzev v oblasti kybernetické bezpečnosti. Odhalení podobných slabin současných algoritmů tak ukazuje, že lze v dohledné době očekávat rostoucí nebezpečí, které může z této technologie pramenit.

Nový algoritmus proti nechtěné těžbě kryptoměn

(26. 08. 2020; helpnetsecurity.com)

Superpočítače a jiná vysoce výkonná počítačová zařízení se stávají terčem hackerů, kteří se snaží využít jejich výkon k těžbě kryptoměn a tím ke svému obohacení. Výzkumníci z národní laboratoře v Los Alamos (USA) vytvořili způsob jak tyto počítače před snahou hackerů o vytěžování jejich výkonu ochránit. Nový algoritmus je založen na tom, že každý počítačový program může být reprezentován pomocí grafu složeného z různě propojených uzlů. Každý program může být potom reprezentován grafem, který je pro něj jedinečný. Nový algoritmus tak porovnává databázi grafů povolených programů se skutečně běžícími programy. Nefunguje tedy jako většina stávajících podobných algoritmů, které se snaží identifikovat přítomnost známého malwaru ale naopak zakazuje programy, jejichž graf neodpovídá databázi povolených programů, a tudíž u nich hrozí, že jsou malwarem infikované.

Komentář: Kryptomining má často větší účinnost než jiné typy útoků a také s sebou často nese nižší riziko pro útočníka. Přestože tento navrhovaný algoritmus nepředstavuje neprůstřelnou obranu pro všechny situace tak představuje důležitou součást repertoáru nástrojů, které mohou sloužit k ochraně vysoce výkonných počítačů.

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