Výzkum a nové technologie v kybernetické a informační bezpečnosti

Č. 2/2020 • PRAHA • 28. SRPNA 2020

Nebezpečí sdílení screenshotů z videokonferencí

(13. 07. 2020, in.bgu.ac.il) Výzkumníci z Ben Gurionovy univerzity v Negevu představili výsledky svého výzkumu ve kterém se zaměřili na možnosti získávání osobních informací z veřejně dostupných screenshotů z různých videokonferencí. V rámci výzkumu bylo analyzováno více než 15 700 snímků. Pomocí nových algoritmů využívajících umělou inteligenci pro rozpoznávání obličejů bylo rozpoznáno až 80% obličejů na těchto snímcích a to včetně identifikace pohlaví a přibližného věku. V řadě případů bylo také ze snímků možno přímo vypozorovat nebo odvodit skutečná jména účastníků.

Komentář: Důležitost bezpečného využívání videokonferencí vzrostla především v návaznosti na opaření způsobená pandemií, kdy se k jejich využívání uchýlila celá řada organizací (dle odhadů se jednalo až o 500 milionů uživatelů). V řadě případů si však uživatelé neuvědomují všechna rizika, která mohou být s videokonferencemi spojená. Nejedná se však pouze o sdílení snímků z proběhlých videokonferencí. Více o zabezpečení videokonferencí se můžete dozvědět v Bezpečnostním standardu pro videokonference.

Nový algoritmus pro zabezpečení Single sign-on autentizace

(30. 06. 2020; helpnetsecurity.com) Mechanismus SSO (Single sign-on/jediného přihlášení) centralizuje autentizační proces uživatele do jednoho místa (tzv. poskytovatele identity). A to tak, že dává uživateli možnost přihlašovat se do různých systémů pomocí jednoho účtu (typicky MojeID; Google nebo Facebook). Rostoucí využívání tohoto mechanismu však sebou přináší i otázky jak zajistit jeho bezpečnost a minimalizovat rizika ztráty a zneužití osobních dat uživatelů. S novým řešením přišli japonští výzkumníci. Ve svém článku představili nový algoritmus, který omezuje osobní data o uživateli, která jsou dostupná poskytovatelům služeb do kterých se pomocí SSO přihlašuje.

Komentář: Přestože mechanismus SSO přináší řadu výhod pro uživatele a to i z bezpečnostního pohledu, přináší i řadu nevýhod. Jednou z nich je právě zmíněné riziko zcizení osobních údajů. Nový algoritmus a jeho případné zavedení do praxe by tak dokázalo poskytnout více bezpečí pro uživatelská data.

Možnost útoků na průmyslové řídicí systémy pomocí čárových kódů

(30. 06. 2020, securityweek.com) Výzkumníci organizace IOActive objevili nový způsob pomocí kterého je možno napadnout průmyslové řídicí systémy (Industrial control systems – ICS), a to v případě, že je průmyslový řídicí systém připojen na čtečku čárových kódů. Čárový kód může být upraven a poté využit jako vektor útoku. Výzkumníkům se pomocí čárových kódů podařilo vypnutí řídicí jednotky nebo její přenastavení. Tento vektor útoků tak využívá především toho, že proces skenování čárových kódů nevyžaduje žádnou autentizaci.

Komentář: Čtečky čárových kódů fungují jako vstupní zařízení, což si množství jejich uživatelů neovědomuje. Současné čtečky jsou připojeny pomocí USB a moderní čárové kódy (a jejich varianty) dokáží obsáhnout až 70 symbolů. To představuje dostatek místa proto, aby útočník infikoval počítač škodlivým kódem.

Nová bezpečnostní metoda pro IoT

(04. 08. 2020; helpnetsecurity.com) Tým výzkumníků z Ben Gurionovy univerzity v Negevu a Singapurské národní univerzity vyvinul novou metodu, která umožňuje poskytovatelům internetu a telekomunikačního připojení lepší přehled o zařízeních připojených do jejich sítí. Rostoucí nebezpečí spojené s internetem věcí (internet of things – IoT) totiž ohrožuje nejen potencionální oběti masivních DDoS útoků, ale taky samotnou infrastrukturu poskytovatelů připojení. Navíc není možné spoléhat na znalosti a schopnosti běžných uživatelů z hlediska zabezpečení IoT. Zmínění výzkumníci tedy vyvinuli metodu, pomocí které lze identifikovat, zda jsou v rámci domácích sítí jejich klientů připojena zařízení, která jsou náchylná ke zneužití útočníky. Poskytovatelé připojení tak dostanou možnost takovému zneužití lépe předcházet.

Komentář: Tento výzkum je jedním z prvních, které se zabývají předcházení rizik pojících se s IoT. Navíc, jak zmiňuje i výzkum, není možno v bezpečnosti IoT spoléhat na koncové uživatele. Dá se ale předpokládat, že v dohledné době se bude nebezpečí spojené s IoT významně zvyšovat. Počet připojených zařízení rychle roste a v současné době neexistuje žádný jejich monitoring, což se právě tento výzkum snaží změnit.

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