Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Horizon Cluster 3 - Cybersecurity

V současné době jsou vypsány výzvy Horizon Europe Clusteru 3 pro oblast kybernetické bezpečnosti. Výzvy jsou otevřeny do 21. 10. 2021. Mezi tématy výzev můžete nalézt například využití umělé inteligence pro kybernetickou bezpečnost nebo zabezpečení open source technologií. Více informací o tématech a možnostech zapojení se naleznete zde.

Grant TEAMING v programu HORIZONT

Ministerstvo školství, mládeže a tělovýchovy zveřejnilo informaci určenou budoucím žadatelům, kteří plánují podávat návrh projektu do výzvy TEAMING for Excellence s uzávěrkou prvního kola dne 5. 10. 2021. Vzhledem k souladu aktivit nástroje TEAMING s cíli operačního programu Jan Amos Komenský předpokládá MŠMT, že po schválení OP JAK budou s největší pravděpodobností prostředky na komplementární financování investičních výdajů úspěšných projektů zajištěny v tomto programu. Financování bude určeno na podporu projektů českých žadatelů, které uspějí v obou kolech a získají grant. Více informací naleznete zde.

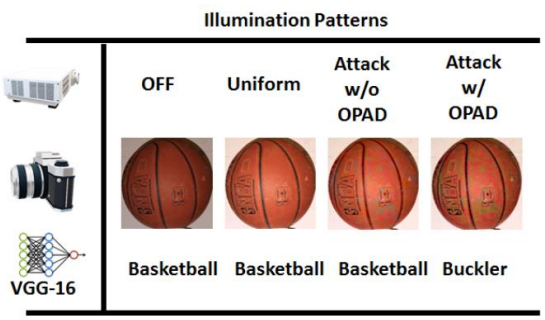
The EIT Digital Flagship Conference 2021

Dne 14. září 2021 proběhne konference The EIT Digital Flagship Conference 2021. V rámci konference proběhnou tři hlavní příspěvky věnované technologickým inovacím. Konference proběhne plně online. Více o programu a možnostech registrace naleznete zde.

OPAD útok a umělá inteligence

(17. 08. 2021; hackread.com) Výzkumný tým z Purdueovy univerzity (USA) objevil nový typ útoků zneužívající slabin umělé inteligence. Nový útok byl pojmenována OPAD (OPtical ADversarial attack) a pro jeho realizaci je třeba využít projektor, kameru a počítač. Útok potom funguje tak, že pomocí světla projektoru namířeného proti reálnému objektu dochází k pozměnění toho, jak tento objekt umělá inteligence interpretuje. Výzkumníci toto demonstrovali například na případu, kdy dokázali zmást algoritmus umělé inteligence tak, aby místo dopravní značky „STOP“ přečetl pouze značku s omezením rychlosti „SPEED 30“.

Komentář: Podobné výzkumy ukazují nové zranitelnosti, které je třeba brát v potaz především v oblasti zavádění autonomní automobilové dopravy. Tento typ útoku sice nejspíše nebude fungovat v každé situaci (např. je ovlivněn denní dobou, množstvím světla apod.), ale přesto poukazuje na potencionální bezpečnostní problém, se kterým by měly organizace vyvíjející algoritmy umělé inteligence počítat. Výzkum byl financován armádou Spojených států což může předznamenávat možné vojenské využití této technologie.

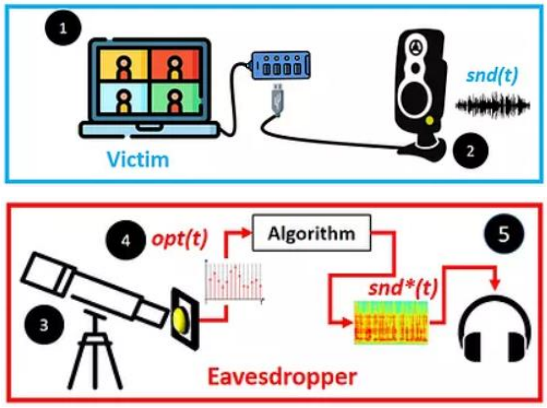


Zdroj: Optical Adversarial Attack

Nový způsob odposlechu GLOWWORM

(18. 06. 2021; cyware.com) Tým akademiků z Ben-Gurion University of Negev (Izrael) představil nový typ útoků, označován jako nový optický TEMPEST útok. Jádro útoku spočívá v tom, že útočník může sledovat vyzařování LED diod ze zvukových zařízení (typicky reproduktorů). Takto zaznamenané chování LED diody je poté možno reprodukovat do zvuku, který z daného zařízení vychází. Výzkumníkům se podařilo tímto útokem získat data přibližně z poloviny analyzovaných zařízení. Demonstrace tohoto útoku proběhla například na sledování chování světla LED diody běžných reproduktorů ze vzdálenosti 35 metrů, kdy zvuk vycházející z reproduktorů nebyl vůbec slyšet. Rekonstrukce zvukové stopy je poté s menšími obtížemi poměrně dobře srozumitelná. Demonstrace je dostupná jako video na youtube.

Komentář: Předkládaný výzkum přímo navazuje na výzkum, o kterém jsme reportovali přibližně před rokem, kdy k odposlechu byla využita změna chování světla v odposlouchávané místnosti (více zde). V reálné situaci je možné tento typ útoků využít především pro odposlech virtuálních schůzek. Výzkumníci však sami uvádějí, že základní ochrana proti tomuto útoku může být poměrně jednoduchá, a to zatemnění LED diody.



Zdroj: nassiben.com

DESOLATOR a autonomní vozidla

(27. 07. 2021; sciencedaily.com) Výzkumné laboratoře armády Spojených států představili nový koncept obrany digitálních systémů autonomních vozidel. Především se zaměřili na zvýšení bezpečnosti autonomních vojenských vozidel. Vycházeli přitom z klasické myšlenky, že je pro protivníka mnohem složitější trefit pohybující se cíl. V oblasti kybernetické bezpečnosti tak jde především o IP adresy jednotlivých zařízení, které pokud jsou statické tak dávají protivníkovi mnohem více prostoru a času pro útok. Výzkumníci přišli s přístupem nazvaným DESOLATOR. Jedná se o nový algoritmus využívající strojové učení, který má za úkol ve vozidlech identifkovat optimální frekvenci změn IP adres. Tento přístup tak ztěžuje zaměření dané IP adresy případným útočníkem. Systém se poté sám dále „učí“ aby poskytl co největší bezpečnostní záruky a zároveň co nejméně zasahoval do výkonu informačních a komunikačních systémů vozidel.

Komentář: Autonomní vozidla se stávají nepostradatelnou součást armádního vybavení většina armád světa. Předkládaný přístup tak umožnuje výrazně zvýšit kybernetické zabezpečení těchto vozidel, a to bez toho, že by výrazně narušoval jejich výkonnost (v některých oblastech ji dokáže dokonce ještě zlepšit). Navíc DESOLATOR není přístup limitovaný pouze na vojenské technologie nebo na oblast autonomních vozidel. Schopnost dynamicky měnit IP adresu a její rozsah lze využívat i v celé řadě dalších oblastí, kde je třeba podpořit kybernetickou bezpečnost.

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