Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

VUT otevřelo unikátní laboratoř kvantové bezpečnosti

Odborníci z Fakulty elektrotechniky a komunikačních technologií Vysokého učení technického v Brně mají nově k dispozici laboratoř s takzvanou kvantovou komunikační infrastrukturou. Otevření laboratoře reaguje na aktuální trendy v zahraničí, zejména v EU, USA a Číně, kde už podobné infrastruktury budují a propojují v nadnárodní sítě. Celou zprávu si můžete přečíst zde.

Měsíc kybernetické bezpečnosti

Říjen je již tradičně měsícem kybernetické bezpečnosti. Letos se jedná již o 9. ročník této inciativy, která si dává za cíl propagaci potřeby online bezpečnosti mezi občany Evropské unie. V rámci tohoto měsíce proběhne řada konferenci a akcí spojených s tématy kybernetické bezpečnosti. Více o evropském měsíci kybernetické bezpečnosti se můžete dočíst zde.

Transfera Technology Day 2021

Dne 21. října 2021 proběhne v Praze druhý ročník akce *Transfera Technology Day*, jejímž cílem je propojit českou vědu a zdroje technologií s byznysovou komunitou a vytvářet vhodné podmínky pro vzájemnou spolupráci. Akce bude možné se účastnit osobně anebo ji sledovat online. Více informací je dostupných zde.

Webinář Evropská partnerství a mezinárodní výzvy 2021

Dne 18. října 2021 proběhne webinář Evropská partnerství a mezinárodní výzvy 2021. Webinář se bude věnovat tématům Evropská partnerství (nový nástroj programu Horizont Evropa), Partnerství pro biodiverzitu Call 2021 a dalším možnostem podpory. Registrace a více informací je dostupných zde.

Výzva pro zájemce o volná místa ve správní radě EIT

Evropský inovační a technologický institut (*European Institute of Innovation and Technology*) zveřejnil dne 1. 9. 2021 výzvu k vyjádření zájmu na obsazení až 7 míst ve své Správní radě (*Governing Board*). Zájemci se mohou hlásit až do 29. 10. 2021. Více informací o možnostech zapojení naleznete zde.

Methodology for a Sectoral Cybersecurity Assessment

Agentura ENISA publikovala dokument *Methodology for a Sectoral Cybersecurity Assessment.* Metodkická příručka je směřovaná především sektorovému bezpečnosti ICT produktů. Dokument je dostupný zde.

SSID Stripping útoky

(20. 09. 2021; cyware.com) Tým výzkumníků z fakulty informatiky na *Technion - Israel Institute of Technology*, ve spolupráci s výzkumným týmem společnosti AirEye, vyvinul novou metodu útoku s názvem SSID Stripping. Ta může být použita ke zfalšování názvu sítě jiným názvem v seznamu sítí zařízení k oklamání uživatelů. *SSID Stripping* funguje tak umožňuje útočníkovi přesvědčit oběť, aby se připojila k falešným bezdrátovým přístupovým bodům (WAPs). Vědci ukázali, jak může útočník zfalšovat název bezdrátové sítě. Například falešný název SSID sítě se uživateli zobrazí jako legitimní síť. Při tomto útoku uživatel vidí síťové připojení se stejným názvem připojení, kterému důvěřuje, ačkoli se musí k této síti připojit ručně, aby útok fungoval. Útok obchází ovládací prvky zabezpečení, protože zařízení zpracovává skutečný název SSID. Další řetězec přidaný útočníkem se však oběti na jejich obrazovce nezobrazí. Tento typ útoku může být dobře využitelný například ke krádežím dat ze zařízení obětí nebo k sledování a odposlechu jejich komunikace.

Komentář: Představená metoda útoku využívá slabin přenosných zařízení, která uživatelé často připojují na více či méně známé wifi sítě. Zároveň využívají i slabinu ve formě lidského faktoru, kdy k podvržené síti se musí uživatel sám aktivně přihlásit. Firma AirEye, která se na tomto výzkumu podílela již představila zdarma šiřitelný nástroj, který umožňuje organizacím a lidem lépe monitorovat, zda nejsou jejich zařízení cílem této metody útoku.

Spook.js útoky

(10. 09. 2021; portswigget.net) Spook.js je nový typ útoků, který se řadí do kategorie tzv. *spectre attacks* („přízračné útoky“). Ty se prosazovaly především v roce 2018 a zneužívají optimalizační nástroje moderních procesorů. Spectre útoky dokážou na úrovni procesů v procesoru zasahovat do paměti určené pro jiné procesy. Tímto způsobem mohou útočníci získat různé druhy dat, útočit na různé aplikace nebo spouštět aplikace dle vlastního uvážení. Spook.js je novým typem útoků v této rodině a zaměřuje se na především na prohlížeč Google Chrome. Ten má již implementovánu ochranu proti *spectre* útokům ale Spook.js ji dokáže obejít. Bylo dokázáno, že tento útok může poměrně jednoduše například krást přihlašovací údaje ze správce hesel nebo dokáže získat data zobrazovaná uživatelem v tomto prohlížeči.

Komentář: Google Chrome ale i ostatní prohlížeče již nějakou dobu implementují ochranu proti *spectre* útokům. Spook.js však ukazuje, že tato ochrana nemusí být vždy dostatečná. Představená metoda útoku funguje totiž víceméně stejně jako všechny útoky z této rodiny, ale vyžívá jiného přístupu do procesů počítače. Google již vydal bezpečnostní záplatu proti Spook.js. Tento incident nám však ukazuje, že není vhodné opomíjet „již překonané“ metody útoků, protože se mohou projevit znovu jen v jiné formě.

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