Student z FIT ČVUT vyhrál v soutěži IT SPY 2025 s prací o fyzických útocích v kryptografii

26.11.2025 - Viktorie Dittrichová | Fakulta informačních technologií ČVUT v Praze

Ing. Vít Mašek z Fakulty informačních technologií ČVUT v Praze (FIT ČVUT) uspěl se svou diplomovou prací na soutěži IT SPY 2025, kde získal 3. místo mezi stovkami IT závěrečných prací z českých a slovenských univerzit. Jeho práce se zabývá jednou z nejzajímavějších a zároveň nejnebezpečnějších oblastí moderní kryptografie – útoky, které neútočí na matematiku, ale na fyzické chování zařízení. Zároveň za svou práci obdržel Cenu děkana za letní semestr 2024/2025.

Vítova diplomová práce se zaměřuje na tzv. útoky postranními kanály. Tyto útoky neprolamují kryptografické algoritmy pomocí složitých výpočtů, ale využívají nenápadné fyzické projevy zařízení při šifrování – například drobné změny ve spotřebě energie nebo elektromagnetickém vyzařování. I takové signály mohou útočníkovi pomoci odhalit tajný klíč. Jde o oblast, která je stále důležitější, protože kryptografie je součástí téměř každého moderního zařízení – od chytrých karet přes mobilní telefony až po průmyslové systémy.

Vít Mašek se ve své práci zaměřil na bezpečnost algoritmu SipHash, který se používá pro zabezpečení integrity a autenticity dat. V praxi se například využívá v dopravních prostředcích, kde je důležité zabezpečit, že data, která si jednotlivé řídící jednotky předávají, nejsou nijak změněna a pocházejí od autorizovaného zdroje. SipHash je známý jako kryptografická funkce založená na tzv. ARX struktuře (Addition-Rotation-XOR). Tyto struktury jsou často považovány za typy konstrukcí, které by měly být vůči útokům přes postranní kanály odolné samy o sobě, ale současný výzkum ukazuje, že to nemusí vždy být pravda.

Vít proto vytvořil kompletní implementaci algoritmu SipHash na FPGA platformě, která umožňuje přesné měření spotřeby a je určena právě pro analýzu fyzických útoků. Po důkladném měření a statistickém vyhodnocení se ukázalo, že implementace skutečně vykazuje měřitelné úniky informací. Tyto úniky pak dokázal využít v praktickém postranním útoku, jehož cílem bylo získat tajný klíč pouze na základě analýzy spotřeby energie během výpočtu.

Ačkoli útok nebyl na reálném zařízení plně dokončen, výsledky jasně prokázaly, že ani SipHash není automaticky chráněn proti fyzickým útokům.

> „Výsledky ukazují, že i moderní, výpočetně jednoduché kryptografické algoritmy mohou být v praxi zranitelné. Je důležité myslet nejen na matematickou stránku kryptografie, ale i na fyzické úniky, které mohou ohrozit i jinak bezpečné systémy," uvádí Vít Mašek.

> „3. místo v soutěži IT SPY pro mne znamená, že i přes záplavu témat věnujících se AI a strojovému učení, se nezapomíná na IT bezpečnost jako důležitou oblast výzkumu. Aktuálně uvažuji nad doktorským studiem, kde bych se rád věnoval zabezpečení postkvantové kryptografie proti fyzickým útokům," dodává Vít.

Soutěž IT SPY (IT Student Project of the Year) každoročně vybírá nejlepší a nejinovativnější diplomové práce v oblasti informačních technologií z univerzit v České republice a na Slovensku. Hodnotí se technická úroveň, originalita i potenciál pro reálné využití.

http://fit.cvut.cz/cs/zivot-na-fit/aktualne/zpravy/23885-student-z-fit-cvut-vyhral-v-soutezi-it-spy-2025-s-praci-o-fyzickych-utocich-v-kryptografii