Ochranu proti útokům kvantovými počítači řešila konference CHES 2023

24.10.2023 - Ivana Macnarová | Fakulta informačních technologií ČVUT v Praze

Odborníci očekávají v blízké budoucnosti příchod éry kvantových počítačů, a i proto byly hlavními tématy letošního ročníku konference CHES právě postkvantová kryptografie, útoky na kryptografické implementace, a jak se proti nim chránit. Některé soudobé kryptografické algoritmy jsou bohužel zranitelné vůči hackerským útokům, které jsou vedeny kvantovými počítači. Konference ukázala nová řešení ochrany, která budou odolná vůči těmto útokům.

Jeden z hlavních řečníků prof. Peter Schwabe ve své přednášce s názvem „Kryptografie s vysokou mírou jistoty v praxi – Výzvy a nejnovější výsledky“ zdůvodnil, proč je třeba změnit způsob, jakým vytváříme kryptografický software. Ukázal, že nástroje a jazyky z oblasti tzv. „kryptografie s vysokou mírou jistoty“ jsou mnohem vhodnější pro vytváření důvěryhodných implementací kryptografie a začínají být použitelné i pro uživatele, kteří nejsou vyloženě odborníky. Diskutoval o výzvách, které musíme řešit, aby se kryptografie s vysokou mírou jistoty stala de facto standardem v kryptografickém inženýrství. Schwabe je vedoucím výzkumné skupiny v institutu Maxe Plancka pro bezpečnost a soukromí a profesorem na nizozemské Radboudově univerzitě. Věnuje se postkvantové kryptografii a je spoluautorem bezpečnostních klíčů, které pomáhají zabezpečit komunikaci na internetu společnosti Google.

Druhý hlavní řečník Thomas Unterluggauer se ve své přednášce „Bezpečnost mikroarchitektur: současný stav“ zabýval tím, jak společnost Intel řeší zabezpečení procesorů Intel Core a Intel Atom. Představil celkovou strategii, která pomáhá chránit zákazníky před bezpečnostními zranitelnostmi v mikroarchitektuře Intel. Popsal také, jak mohou hardwarové a softwarové prostředky společně zmírňovat různé třídy zranitelností, aby měl software kontrolu nad konkrétními kompromisy mezi mírou zabezpečení a výkonem. Vše uvedl na konkrétních příkladech, aby pomohl vývojářům pochopit možné hrozby, a vysvětlil, jak konkrétně rizika snížit. Unterluggauer pracuje jako výzkumník v oblasti bezpečnosti v laboratořích Intel Labs (Security & Privacy Research), kde se zabývá výzkumem útoků na mikroarchitektury a obranou proti nim.

Na konferenci je tradičně udělována cena Test of Time Award. Tuto cenu získává publikace, která byla na konferenci CHES publikována před 20 lety a jejíž kvalitu a význam pro kryptologii prověřil čas. V letošním roce tuto cenu získala publikace A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD z roku 2003. Její autoři Gilles Piret a Jean-Jacques Quisquater v ní popsali útok injekcí chyb, který se následně stal standardem při testování odolnosti kryptografických implementací proti této skupině útoků. Tento útok se dodnes používá při testech jak v průmyslu, tak v certifikačních laboratořích.

Při příležitosti 25. ročníku konference pohovořili i její zakladatelé prof. Çetin Kaya Koç, prof. Christof Paar a její dlouholetý účastník prof. Jean-Jacques Quisquater o historii CHESu – jak se z malého workshopu v roce 1999 stala největší a nejvýznamnější světová konference na hardwarovou kryptografii pod záštitou IACR.

https://fit.cvut.cz/cs/zivot-na-fit/aktualne/zpravy/20168-ochranu-proti-utokum-kvantovymi-pocitaci-resila-konference-ches-2023