Světoví experti na hardwarovou kryptografii se setkají na prestižní konferenci CHES

21.8.2023 - Pavla Bradáčová | Fakulta informačních technologií ČVUT v Praze

Konference se bude týkat zásadních témat z oblasti kryptologie, kterými jsou především Kryptografické implementace, Útoky na implementace a protiopatření nebo Interakce mezi kryptografickou teorií a otázkami implementace. Ročník 2023 přinese také zcela nová témata, kterými jsou Systematizace znalostí, Izolační a monitorovací hardware pro kybernetickou odolnost, Inženýrství systémů důkazů s nulovou znalostí a Výpočetní technika zachovávající soukromí v praxi.

Součástí programu jsou i dvě zvané přednášky. Prof. Peter Schwabe, který působí na Institutu Maxe Plancka pro bezpečnost a soukromí a na Radboudově univerzitě, pohovoří o tom, jak vytvářet vysoce zabezpečený kryptografický software a jaké výzvy je třeba překonat. Thomas Unterluggauer z firmy Intel seznámí účastníky se současným stavem zabezpečení mikroarchitektur procesorů Intel Core a Intel Atom a popíše, jak mohou hardwarové a softwarové prostředky společně předcházet zneužitelným zranitelnostem a rizikům. Program konference je velmi pestrý a nabitý, kromě prezentací přijatých příspěvků nabídne také tutoriály odborníků z Německa, Kanady a Taiwanu.

Kromě ceny za nejlepší příspěvek je v rámci konference CHES udělována i 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 loňském roce tuto cenu získala publikace z roku 2002, ve které autoři představili Šablonové útoky (Template Attacks), což je dodnes vysoce účinná metoda prolomení bezpečnosti kybernetických systémů.

Při příležitosti 25. ročníku konference pohovoří její zakladatelé prof. Çetin Kaya Koç, prof. Christof Paar a její dlouholetý účastník prof. Jean-Jacques Quisquater o historii CHESu od malého workshopu v roce 1999 po současnou konferenci pod záštitou IACR.

Konference CHES, která se pravidelně koná od roku 1999, propojuje výzkumnou a inženýrskou komunitu v oblasti kryptologie a sdružuje účastníky z akademické sféry, průmyslu, státní správy i dalších oblastí. CHES je jednou z osmi stěžejních konferencí pořádaných prestižní světovou kryptologickou asociací IACR.

https://fit.cvut.cz/cs/zivot-na-fit/aktualne/zpravy/19573-svetovi-experti-na-hardwarovou-kryptografii-se-setkaji-na-prestizni-konferenci-ches