EUROCRYPT 2004

Jan Janečko, Komerční banka

Ve dnech 2.-6. května se ve švýcarském alpském středisku Interlaken uskutečnila 23. mezinárodní kryptologická konference EUROCRYPT 2004. Jejím pořadatelem byla Mezinárodní asociace pro kryptologický výzkum (IACR) ve spolupráci s Výzkumnými laboratoři IBM v Curychu. Zúčastnilo se jí na 370 účastníků ze 40 zemí, a to doslova ze všech světadílů. O stále se zvyšujícím dosahu kryptologie svědčí například účast odborníků z Bangladéše, Egypta, Íránu, Jihoafrické republiky či z Nigérie. Z České republiky se letošní konference zúčastnilo osm zástupců.

Konference EUROCRYPT si programově udržuje průřezový charakter, a tak skladba příspěvků postihovala nejrůznější směry moderní kryptologie. Programový výbor zařadil do programu konference jen jednu šestinu z celkového počtu podaných prací. I když tentokrát asi nebyl na EUROCRYPTu prezentován žádný převratný výsledek, byla zde přednesena řada zajímavých příspěvků. Mezi nejčastější témata patřily různé aspekty kryptografických protokolů - podpisových schémat, distribuované kryptografie, vícestranných výpočetních schémat, anonymní identifikace, šifrování odvozené od identity a šifrování databází apod. Kryptoanalytickými metodami se tentokrát přímo zabývala jen dvě vystoupení. Z prakticky orientovaných prací vzbudil pozornost příspěvek Phuon Q. Nguyena "Můžeme důvěřovat kryptografickému softwaru? Kryptografické díry v GNU Proivacy Guard v1.2.3" ukazující závažné bezpečnostní nedostatky tohoto známého "open source" produktu a upozorňující na obecná rizika kryptografického softwaru. Se dvěma zvanými přednáškami na konferenci vystoupili Whitfield Diffie ("Informační bezpečnost - ohlédnutí zpět a pohled vpřed") a Ivan Damgaard ("Pradigmata vícestranných výpočetních schémat").

Jednou z tradičně nejzajímavějších části konference je tzv. rump session - večerní program složený z krátkých příspěvků a oznámení. K nejzajímavějším z 20 vystoupení patřil příspěvek Erana Tromera a Adi Shamira "O všetečných lidech a hlučných strojích". Po vzoru metod používaných již v 50. letech některými profesionálními kryptoanalytickými službami se jim analýzou zvuků vydávaných počítačem podařilo zjistit určité informace o prováděných kryptografických operacích. Jejich výsledky lze nalézt na http://www.wisdom.weizmann.ac.il/~tromer/acoustic/ . Účastníci odměnili cenou (velkým kravským zvoncem) jako nejlepší příspěvek Davida Naccache a Claire Whelan "11.9.: Kdo upozornil CIA? (a další tajná tajemství)", kdy se jim na základě analýzy vzdáleností mezi slovy a dalších geometrických vlastností použitých tiskových fontů podařilo doplnit začerněná místa v nedávno zveřejněné zprávě CIA pro prezidenta Bushe ze srpna 2001, obsahující zpravodajské informace k chystaných teroristickým útokům Al-Kajdá na USA (http://cryptome.org/cia-decrypt.htm).

Novinkou letošního EUROCRYPTu bylo rozhodnutí výkonného výboru Mezinárodní asociace pro kryptologický výzkum (IACR) jmenovat zasloužilé členy IACR. Prvními šesti se stali Thomas Berson (bývalý předseda IACR, propagátor kryptologie), Don Coppersmith (DES, teoreticko-číselné algoritmy, ...), Whitfield Diffie (objev kryptografie veřejného klíče, protokol DH, ...), David Chaum (podpisové, platební a jiné protokoly, elektronické peníze, ...), Ronald Rivest (např. RSA, MD-5, RC-4, ...) a Adi Shamir (RSA, sdílení tajemství, identifikační schéma, diferenční kryptoanalýza, Twinkle, ...). S výjimkou Chauma a Rivesta si na místě ocenění osobně převzali.

V pořádání EUROCRYPTu jakožto největší evropské kryptologické konference (poprvé se konala už v roce 1982) se tradičně střídají jednotlivé evropské země. Řada účastníků stále ráda vzpomíná na EUROCRYPT 1999, který se konal v Praze. Příští rok se bude konference konat v dánském Aarhusu, další pak v ruském Petrohradu.