Eurocrypt 99, Praha 2.-5. května 1999, hotel Hilton

Pokud hledáte spíše oficiální informace o konferenci, odkazuji Vás na můj článek v DSM 3/99. Na tomto místě bych se čtenáři chtěl podělit s dojmy spíše subjektivními.

Při pohledu zpět začal pro mě letošní Eurocrypt již vlastně na konferenci Pragocrypt 96, kterou rovněž uspořádala naše kryptologická skupina při JČMF. Tato konference, která proběhla mimo standartní kalendář konferencí IACR, byla vyhodnocena jako úspěšná a Jarda Hrubý (který se stal členem představenstva IACR) byl pověřen přípravou konference Eurocrypt 99 (tyto probíhají každý rok vždy v jiném místě Evropy). Určitě je nezbytné zdůraznit organizátorskou roli Jardy. Nebýt jeho, jeho obětavosti a ochoty podstoupit desítky různých jednání, konference by se v Praze nekonala.

Samotnou konferenci jsme připravovali téměř dva roky – první schůze organizačního výboru se konala již v září 1997. Pro takto velkou konfenci již nebylo možné, abychom kompletně zvládli všechny potřebné úkoly (jako tomu bylo na na Pragocryptu – ale tam bylo 126 účastníků, počet účastníků Eurocryptu překročil čtyři stovky). Obrátili jsme se proto na pražskou firmu ITC (Incentive travel&Conference). Základním problémem při pořádání takovýchto akcí je kromě vyřešení spousty organizačních otázek samozřejmě i jejich financování. Těmto problémům také byla věnována převážná část obsahu jednotlivých jednání výboru. Z hlediska sponzoringu byl hlavní úspěch zaznamenán v momentu, kdy se podařilo získat za generálního sponzora českou pobočku firmy Hewlett Packard.

Pro mě (jakožto jediného mimopražského člena výboru – kromě tedy "zahraničního" Vaška Matyáše, který obstarával součinnost s vedením IACR a oficiální webovskou stránku konference) vyplynulo více úkolů až na samotné konferenci, kde jsem fungoval jako "oficiální tiskový mluvčí konference". Role nezáviděníhodná, ale nějaké informace se podařilo do tisku dostat. I když musím podotknout, že asi ne vše se podařilo. Z novin mělo zájem především Právo, nějaké informace publikovala ČTK, televize pouze sondovala terén, rozhlas sice uveřejnil jeden rozhovor, ale ten byl poněkud "mimo", reportérku zajímal pouze obsah pondělního večerního koncertu v Karolinu, nikoliv však problematika konference. Kdesi v tisku jsem pak dokonce zahlédl noticku o "přísně utajené konferenci jakýchsi špiónů", která probíhá v Praze. Oficiálním mediálním partnerem bylo DSM, zde již před konferencí bylo zveřejněno několik informací. A to by snad bylo všechno, kdyby nebylo touhy reportéra z Práva po nějaké senzaci.

Začalo to nevinně. Adi Shamir při svém prvním vystoupení v pondělí zamával jakýmsi černým válečkem a dával jen reklamu svému vystoupení v "rump session". Asi většina účastníků (tedy včetně mě) nepochopila co tím Adi vlastně mínil. Pak ale přišly najednou dotazy (rozhlas, Právo) na Shamirovo vystoupení a ukázalo se, že souběžně s tímto vystoupením byly v USA publikovány některá fakta, která se tohoto zařízení týkají. A že to má rozbít RSA (tedy 512-bitové) atd. No nic, nezbývalo než čekat na úterý večer, kdy Shamir vystoupil s popisem svého válečku.

Nebudu se zde zabývat technickými podrobnostmi Shamirova řešení, lze je nalézt např. na webu (webovské stránky RSA) nebo u mne. Po konferencí se objevila řada hodnocení , která již jaksi objektivizovala skutečný stav věcí. 512-bitové RSA odborníci již delší dobu nedoporučují používat (raději alespoň 768 či lépe 1024 bitů) a na šifru s delším klíčem si toto řešení zatím netroufá. Zajímavé a podstatné na "válečku" je zejména zcela nový přístup k problematice faktorizace a teprve budoucnost může ukázat všechny možnosti tohoto přístupu.

Redaktor Práva, který senzaci potřeboval, interpretoval Shamirovo vystoupení samozřejmě v těch "nej-nej" barvách. Senzace se však nekonala a když, tak v poněkud jiném duchu.

Obsah konference však byl podstatně bohatší než toto jedno vystoupení. Mě zaujalo např. mnohem více vystoupení francouzského kryptologa Pointchevala k novým variantám RSA. A určitě každý z účastníků tam našel svůj předmět zájmu, snad až na toho nejmladšího, kterému bylo tak půl roku a kterého sem vzali jeho rodiče. Ale kdoví, třeba za čtvrt století budeme poslouchat jeho přednášky.

Účastníkům se konference i samotná Praha líbily, myslím, že je pobavil i středeční gala-večer v Obecním domě, kdy "konferenciér" Vašek Matyáš losoval pomocí klasických mariášových karet lahve becherovky (také dar sponzora). Eurocrypt 99 skončil, ať žije Pragocrypt 200x (?)!