Whitfield Diffie

Působí ve společnosti Sun Microsystems a to od roku 1991, v současnosti jako Chief Security Officer, Vice President a Sun Fellow. Je vedoucím činitelem pro formování i realizaci bezpečnostních vizí ve společnosti Sun. Veřejnosti je znám především jako objevitel konceptu asymetrické kryptografie, od 90. let pak působí v oblasti veřejné politiky se vztahem ke kryptografii, jako oponent omezení použití kryptografie a mj. opakovaně jako expert v obou komorách amerického Kongresu.

Je členem Marconi Foundation a International Association for Cryptologic Research a dále také držitelem ocenění od řady organizací, včetně IEEE, Electronic Frontiers Foundation, NIST, NSA, Franklin Institute a ACM. Absolvoval bakalářské studium na Massachusetts Institute of Technology v roce 1965 a od roku 1992 je nositelem čestného doktorátu v technických vědách od Swiss Federal Institute of Technology.

Během konference IS2, která proběhla v Míčovně Pražského Hradu ve dnech 24.–25. května, diskutovali šéfredaktor DSM Jaroslav Dočkal a známý český kryptolog Tomáš Rosa s jednou z legend v oblasti kryptografie – Whitfieldem Diffiem.

Vítáme Vás v Praze; Vy zde ale nejste poprvé?
Vlastně je to podruhé, co jsem zde. Poprvé jsem tu byl v roce 1996 na konferenci Pragocrypt, kdy jsem u vás strávil několik dnů, které jsem si báječně užil. Ze všeho nejraději vzpomínám na dvě věci. První z nich byl výstup do kopce na Pražský hrad, při kterém jsem intenzivně cítil atmosféru Kafkových románů a způsob, jakým on zobrazil byrokratický aparát pomocí fyzické struktury. Byla to paráda, takhle si vyšlápnout nahoru. Dalším velkým potěšením pro mě bylo posezení v jedné z těch kaváren, ve které sedával Albert Einstein, když během pobytu v Praze v letech 1911 až 1912 pracoval na své takzvané pražské teorii, která v jistém smyslu předcházela obecné teorii relativity vydané v roce 1916.

Přejděme tedy na otázky z oblasti kryptografie. Jak na Vás, coby spoluzakladatele asymetrické kryptografie působí všechny ty zkratky a pojmy, jako jsou PKI, Identity Management, elektronický podpis atd.? Jste spokojen, když vidíte výsledný obraz svého snažení?
Myslím, že krátká odpověď zní: „ano". Zhruba před deseti lety jsem si uvědomil jednu zásadní věc. Bylo to na konferenci RSA zrovna v tom roce, kdy se původní setkání pro pár stovek lidí změnilo na podnik pro několik tisíc návštěvníků. Najednou přede mnou byla čtvercová plocha 100 x 100 metrů, plná lidí nabízejících své bezpečnostní produkty. Tam jsem si uvědomil, že ačkoliv jsem věděl, jak je kryptografie důležitá, a ve svých představách jsem viděl miliony bezpečnostních zařízení, už jsem netušil, kolik lidí se tomu celému kolosu bude věnovat. Prostě jsem dříve nechápal, jak bude vypadat komerční stránka kryptografie.

Co říkáte na současné problémy PKI a podobných technologií?
Takže PKI... Problémy PKI mě překvapují a nechávají klidným zároveň. Určitě jsem je všechny nepředvídal, ostatně jsem v mnoha směrech neočekával ani PKI samotné. Myslím, že jsme s Martinem Hellmanem příliš neuvažovali o rozsahu nasazení asymetrických schémat, což je jeden z hlavních problémů v PKI. Později se z PKI stala těžkopádná, standardy svázaná oblast, ve které bylo těžké přijít s nějakým zásadním objevem. Proto jsem se jí také nikdy nevěnoval tolik, jako samotné kryptografii.

Neboli nakonec jste se současným stavem spokojený?
Nevím, co by se na všech těch věcech dalo udělat zásadně lépe. Jasně, je tu řada nepříjemných problémů, pokud budeme mluvit například o elektronické identitě. Lidé jako David Chaum se tomuto tématu věnovali velmi intenzivně. Zdá se však, že žádné jednoduché, elegantní řešení tu neexistuje. Práce v této oblasti je něco jako tlačení balvanu do kopce. Dře-

te se a nakonec máte jen malý úspěch, a to nemluvím o penězích. Je to frustrující. Co k tomu říct víc?

Litujete, že jste nemysleli na patentování Vašich nápadů?

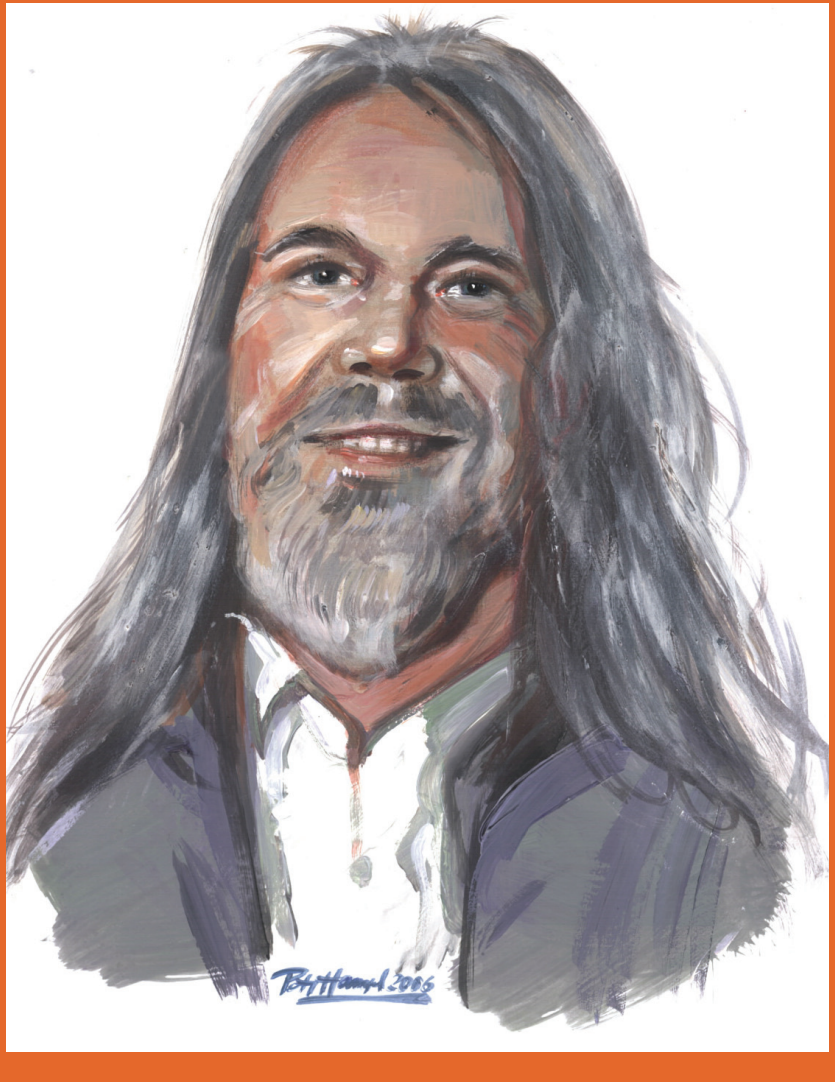
Ale my jsme je patentovali! Ovšem nebyl jsem to já, kdo za tím stál, to měl na starosti Martin Hellman. V konkrétních krocích jsme byli snad jen trochu pozadu. Čeho ale lituji je, že jsem si neuvědomil, jak důležitý Diffie-Hellman byl. Trochu odbočím. Podobně jako Diffie-Hellman řeší problém, který formuloval Ralph Merkle, RSA řeší problém, jehož znění jsem definoval já. RSA přišlo jako velmi přirozený způsob realizace digitálního podpisu. Bylo to něco, co jsem si sám představoval, takže jsem měl RSA rád a podporoval jsem ho. Dost úspěšně, podle mě. Trvalo mi několik let, než jsem pochopil, že RSA má v sobě hluboký a neřešitelný problém. Na základě předloženého veřejného klíče totiž nelze spolehlivě otestovat, zda se v klíčovém páru skrývají zadní vrátka. Ve schématech Diffie-Hellman naproti tomu existuje snadný způsob, jak pouze na základě znalosti veřejných údajů snadno ověřit, že klíč je v pořádku. Tak si teď říkám, že jsem měl včas rozpoznat, že máme s Martinem lepší sadu kryptografických primitiv, i když jsou snad někdy trochu komplikovanější. Kdybych to byl býval udělal, tak jsme na tom mohli vydělat víc. Zároveň jsme se mohli dřív dostat k využití eliptických křivek v kryptografii, neboť to jsou právě schémata z rodiny Diffie-Hellman, která se zde používají. RSA je tu mimo hru.

Takže jste se měli do RSA pustit dřív.

Ano, mohl jsem zkusit protlačit algoritmy Diffie-Hellman tímto způsobem, a bohužel jsem to neudělal.

Vaším příspěvkem „New Directions in Cryptography“ z roku 1976 jste položili základy asymetrické kryptografie. Udělal byste dnes něco jinak?

Odpověď musí být: „Samozřejmě,“ ale neberu to teď tak vážně. Pokud si dobře vzpomínám na obsah našeho příspěvku, měl v podstatě dvě části. První z nich si už ani moc nepamatuji, zabývala se nějakými odhady složitosti konkrétních úloh a podobnými věcmi, které byly velmi poplatné době svého vzniku. Druhá část se věnovala protokolům pro dohodu na klíči. Můžete se mě třeba ptát, jestli bych se dnes soustředil jen na druhou část našeho příspěvku, tedy na tu, co přežila roky a je stále aktuální. Odpověď by ale byla pravděpodobně: „Ne“, neboť nelze nikdy přesně určit, co má jaký vliv na pokrok v nějakém oboru. Jediné, co mě snad trochu trápí, je, že jsem se nezaměřil na souvislosti mezi teorií signálů a nástroji známými jako diferenciální a lineární kryptoanalýza. Mám dojem, že jsem tam mohl přijít dřív na pár pěkných výsledků.



Whitfield Diffie

Když už jsme u kryptoanalýzy, zastavme se u obávané techniky zvané postranní kanály. Jak na Vás jejich objev v roce 1996 zapůsobil? Překvapil Vás?

Popravdě řečeno si nevzpomínám. Nebyl jsem překvapený v tom smyslu, že bych si předtím myslel, že něco takového není možné. Zaujala mě spíš elegance konkrétních metod, když jsem je poprvé uviděl. Mívali jsme v té době pravidelné semináře na Stanfordově univerzitě, kam nás Paul Kocher přišel se svými výsledky seznámit. Vlastně jsem byl překvapen. Překvapený tím, jak snadno se dá takový útok provést. Nicméně v principu jsem něco takového očekával. Navíc podobné téma, tedy implementační slabiny, bylo diskutováno už dříve v roce 1984 na Eurocryptu v Paříži. Tenkrát se probíraly čipové karty a byla ukázána řada útoků fungujících za podmínky, že útočník může řídit hodinový signál karty. Takže o tomto druhu útoků se už alespoň částečně vědělo.

Věděla o něm NSA ještě o něco dřív než ostatní?

Odhaduji, že odpověď je: „Ano“. Kryptografické předměty byly pro NSA vždy důležité, proto lze předpokládat, že se o problémy spojené s jejich bezpečností aktivně zajímala.

Když už mluvíme o náskoku NSA před veřejností, jaký má podle Vás charakter?

Podle vlastní zkušenosti mohu říct, že teoretický kryptologický výzkum můžete dělat na veřejné půdě stejně dobře jako v NSA. Naproti tomu se nikdy nemůžete vyrovnat špionážním možnostem takové agentury. Jak byste chtěl třeba jako soukromý výzkumník provádět odposlechy datových kabelů a analýzu získaných dat? To prostě nejde, potřeboval byste ohromné množství prostředků na techniku, a pak je tu ještě zákon. Vaše snažení by brzo skončilo. Z pohledu agentury je to však jiné, ta si s těmito všemi problémy dokáže poradit. Špionáž je totiž její hlavní deviza.

Teď zase jiný bubák – máme se bát kvantových počítačů?

Bohužel nemám patřičnou kvalifikaci, ale fyzici se zdají být optimističtí, tedy co se příchodu kvantových počítačů týče – pro nás je to naopak špatná zpráva. Na druhou stranu oni jsou optimističtí celých posledních deset let. Nechci tvrdit, že by zatím vůbec nepostoupili, ale přeci jen... Slíbili, že do dvaceti let budou schopni faktorizovat celá čísla v délce 2 000 bitů. Pokud jedou podle plánu, tak to zatím není moc vidět. Můj osobní pocit z kvantových počítačů je ten, že pokud se skutečně stane všechno to, co fyzici slibují, že se stane, budou kryptografické problémy poněkud nepodstatné. Takže abych to shrnul, na kvantové počítače se těším, ale nečekám, že skutečně přijdou.

Vraťme se k Vašemu stěžejnímu příspěvku na IS2, který sliboval nové směry v kryptografii. Můžete je konkretizovat?

Geniální řešení problému bezpečné dohody klíčů: algoritmus Diffie-Hellman (D-H)

Úloha vznikla v prostředí algoritmů založených na sdíleném tajném klíči; problémem je jeho distribuce. Dříve rychlá elektronická forma předání vyžadovala šifrování jedněch klíčů jinými, což původní problém jen kaskádovitě posunovalo. Klíče na vrcholu celé pyramidy museli transportovat agenti na příslušných fyzických médiích (například děrných páskách). To ovšem ve větším měřítku představovalo náročný logistický problém.

Autory vynalezený kryptografický algoritmus umožňuje spolehlivou výměnu klíče k symetrické šifře a to přes nezabezpečený kanál.

Stručný popis je následující:
Algoritmus má dva veřejné systémové parametry p a g.
Parametr p je prvočíslo a parametr g (obvykle zvaný generátor) je kladné celé číslo menší než p s následující vlastností: pro každé celé číslo n mezi 1 a p-1 včetně, existuje kladný celočíselný exponent e takový, že platí $n = g^e \bmod p$.

Strany A a B získají pomocí D-H algoritmu sdílený klíč tímto postupem: Obě strany zvolí svá tajná čísla: strana A číslo a a strana B číslo b. Pomocí neutajovaných čísel p a g pak odvodí své veřejné klíče, A číslo $\alpha = g^a \bmod p$ a B číslo $\beta = g^b \bmod p$, a vymění si je po nechráněném kanálu. Na straně A pak proběhne výpočet $\beta^a \bmod p = (g^b)^a \bmod p = g^{ba} \bmod p$ a na straně B $\alpha^b \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$. Protože platí $g^{ab} \bmod p = g^{ba} \bmod p = K$, strany A i B získávají stejný klíč K.

Síla protokolu se skrývá ve složitosti problému diskrétního algoritmu; pokud je prvočíslo p dostatečně veliké (a nejsou v něm algebraická zadní vrátka), není v rozumném čase výpočetně schůdné z hodnot veřejných klíčů α a β přenášených po nezabezpečeném kanálu získat hodnotu klíče $K = g^{ab} \bmod p$.
Algoritmus byl publikován v W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* 22 (1976), 644-654.

Foto: Zleva Tomáš Rosa, Whitfield Diffie a Jaroslav Dočkal.

Jedním z hlavních směrů je nový pohled na návrh kryptografických algoritmů. Tím myslím jednak veřejné soutěže jako tomu bylo u AES a nyní nově u hašovacích funkcí, jednak také posun v přístupu samotném. Dříve nejprve vznikl inženýrský popis algoritmu a poté se k němu hledal matematický model. Algoritmy nové generace vycházejí rovnou z matematického modelu. V tomto směru je velmi důležitý rozvoj kryptoanalýzy. Budeme-li navrhovat nový algoritmus bez detailní znalosti analytických metod, je to práce naslepo, kdy se opíráme jen o náš subjektivní pocit. Solidní kryptoanalytická teorie nám pomůže objektivně určit, na co se máme soustředit především. Fandím také práci ve stylu Paula Kochera, zabývající se bezpečností konkrétních implementací. Byl jsem rovněž nadšeným příznivcem takzvané kvantové kryptografie. V širším pojetí je to rozhodně nový směr informační bezpečnosti, který je postaven na úplně jiných základech než náš současný přístup.

Co říkáte na tzv. důvěryhodné moduly?

Na jedné straně umožňují provádět řadu nešťastných aktivit souvisejících s našim soukromím, ale pokud jsou používány korektně, jsou to úžasné věci. Uvažujete-li například elektrickou rozvodnou síť, za jejímž řízením stojí spousta počítačů, tak potom pochopitelně musíte zajistit, že se vám do nich nedostane škodlivý kód. Ideální je v tomto případě začít od důvěryhodných modulů. Musíte však mít k dispozici jejich přesný popis, pak je to celé super. Dost mě znervózňují tajemné moduly, které se snaží monitorovat činnost svých uživatelů. Bohužel to jde ruku v ruce – jak se u nás někdy říká, je těžké mít koláč celý a jíst ho zároveň. Očekávám, že se do celé hry vloží politika, ale nevím přesně, jak to dopadne.

Existuje jednoduché pravidlo pro správný poměr mezi soukromím a bezpečím?

Jednoduchá pravidla většinou pocházejí od lidí, kteří se vás snaží přesvědčit, že se musíte vzdát jednoho ve prospěch druhého, neboť nelze mít obojí zároveň. Praktické situace však vyžadují, aby bylo zajištěno obojí a to kvalitně a prakticky nezávislým způsobem. Nemůžete si nikdy být úplně jistí, že organizace, které svěřujete svá data, bude vždy jednat ve vašem zájmu. Jednoduché pravidlo vám ale nepovím.

Jaké druhy bezpečnostních mechanizmů preferujete?

Kryptografie je podle mě důležitá, a to nejen proto, že jsem jí zasvětil velkou část svého života. Sama o sobě ale vše nezvládne. Velmi záleží na konkrétních platformách a způsobu implementace bezpečnostních mechanizmů. Proto jsem se ve své přednášce na IS2 2006 věnoval právě problematice bezpečné výpočetní základny.

Co soudíte o regulacích kryptografie?

V devadesátých letech minulého století se objevily dva přístupy k regulaci kryptografie. Charakterističtější byla snaha o zavedení systémů, provádějících povinnou zálohu použitých šifrovacích klíčů (tzv. key escrow). Záměrem bylo prosadit model, ve kterém občané nemají právo komunikovat spolu způsobem, který by státní orgány nebyly schopny úspěšně odposlouchávat. Kryptografii nakonec ovlivnil víceméně jen druhý přístup, který vycházel ze zákonem daných exportních omezení. Historie zákonů pro kontrolu exportu kryptografických nástrojů je v USA úzce spojena s obdobím studené války. Nicméně v praxi jsme jejich dopad pocítili s jistým zpožděním až v době, kdy o kryptografii projevila zájem širší veřejnost. Koncem devadesátých let však celý program z mnoha důvodů zkolaboval. I stát nakonec pochopil, že pokud chce mít sám pro sebe za přijatelnou cenu dostupnou bezpečnostní techniku, musí do této oblasti pustit běžné komerční subjekty, aby pravidla trhu mohla fungovat.

Jak hodnotíte úroveň výuky v oblasti kryptologie?

Mám kryptologii rád a chápu ji jako pěknou cestu k diskrétní matematice. Její místo tak vidím zejména na matematicky orientovaných katedrách. Pokud mi ovšem řeknete o seznam oborů, ve kterých je nutné cíleně zlepšovat výuku, řazený podle priorit, potom se asi kryptologie moc vysoko nedostane. Myslím, že informační inženýrství momentálně potřebuje hlavně cílenou výchovu expertů v oblasti bezpečných programovacích technik, které jsou klíčovým prvkem pro dosažení důvěryhodných výpočetních prostředí. S existencí takových prostředí stojí a padá celá informační bezpečnost.

Děkujeme Vám za čas, který jste nám věnoval.

Rád jsem ho s Vámi strávil.