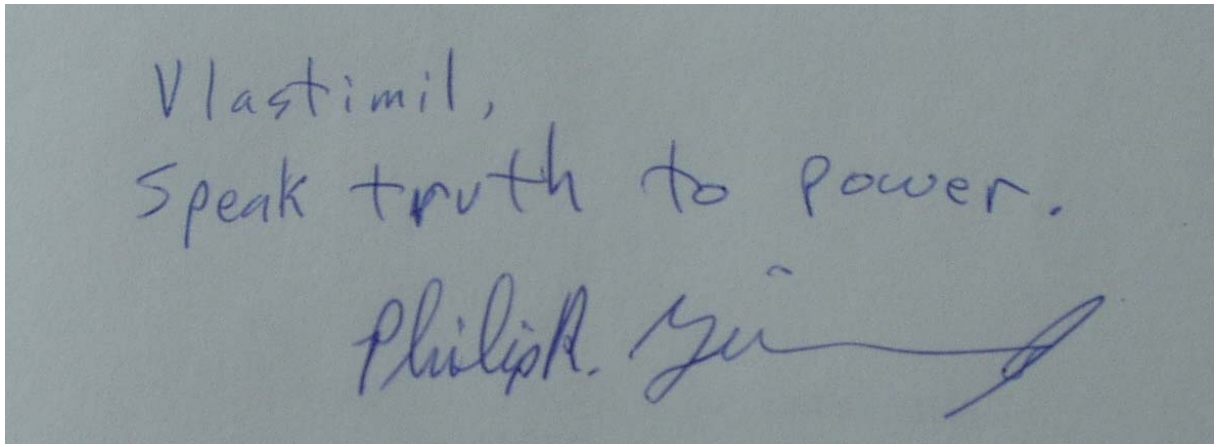
Současná kryptologie v praxi

Vlastimil Klíma
v.klima@volny.cz
nezávislý kryptolog
http://cryptography.hyperlink.cz
Praha

IS2 2008, Information Security Summit 2008, Martinický Palác, 28. – 29. května 2008, Praha.

Cíl

Manažerům informačních systémů a bezpečnosti předat zkušenosti a doporučení pro jejich činnost, pokud se ve své práci dostanou do kontaktu s aplikovanou kryptologií.



Obr.: Rada otce PGP: "říkej mocným pravdu"

Kryptologové by rádi viděli, že jejich dítě je výjimečné, ale není tomu tak.

- Co byla a nyní je kryptologie?
- Kryptologie je jedna z metod informační bezpečnosti, **není nutné se jí věnovat více než ostatním metodám**, jako třeba antivirům, antispamům nebo firewallům, fyzické nebo personální bezpečnosti.
- Přesto stále platí, že kryptologie je pro nás užitečná a někdy přímo nepostradatelná, umožňuje zajistit potřebné a důležité základní služby informační bezpečnosti, na nichž jsou sestaveny miriády ryze uživatelských služeb (bez aplikované kryptologie by nevzniklo moderní mobilní a internetové bankovnictví).

Lidová tvořivost ve vlastním výkladu kryptografických norem je většinou fatální.

- Dnes není nedostatek kryptografických technik, ale **chybí vrstva kryptoinženýrů a kryptoinformatiků**, kteří by je uměli správně kombinovat a implementovat.
- Každá kryptografická norma musí být konfrontována se současným stavem kryptologie, která přináší nové útoky a s nimi i nová protiopatření, která se musí průběžně a co nejrychleji zapracovávat, jako v ostatních metodách informační bezpečnosti.
- Lidová tvořivost ve vlastním výkladu kryptografických norem je většinou fatální (lit. *Kryptologie pro praxi*).
- Kryptologie není nic zvláštního, je to jedna z metod informační bezpečnosti, je však nutné **věnovat se jí alespoň tak jako ostatním metodám**, jako třeba antivirům, antispamům nebo firewallům.

- Závěr: **Pěstujte si svého (1/4, 1/2, 3/4) kryptoinženýra**.

Novinky od roku 2001

Na téma "poslední vývoj v kryptologii" zde na IS2 naposledy v roce 2001 hovořil známý světový kryptolog Aarjen Lenstra. **Od té doby se toho mnoho zásadního událo**. Připomeňme některé události:

- AES, SHA-1, MD5, SHA-3, SSL, PGP, faktorizace, postranní kanály, nové vzorce útoků, kryptologie a aplikovaná **kryptologie se začala vyučovat na mnoha vysokých školách a univerzitách v Česku**, na Karlově Univerzitě byl k tomu založen nový studijní obor (MMIB).

Kryptologie kulhá, ale nohu si zkracovat nebude, protože kulhá jen díky šikmé ploše IT.

- Kryptologie nám v současné době neposkytuje příliš mnoho jistoty. Často máme obavy, že je tak trochu sopkou, u níž nevíme, jestli nezačne bouřit.

- Prvním velkým rozporem v kryptologii je, že většina jejích metod je založena na nedokazatelné bezpečnosti (zmínil i A. Lenstra, IS2, 2001).
- Druhým velkým rozporem kryptologické současnosti je rozpor mezi teorií a praxí.
  - Kryptologie je ve fázi exponenciálního rozmachu do šířky, hloubky i významu nových věcí, které přináší, v kladném i záporném směru, v teorii i praxi.
  - Tlak trhu: nejprve funkčnost, pak bezpečnost. Kryptologii často "dolepují" aplikační programátoři.
  - Důsledek: Praxe nestačí vstřebávat pokrok kryptologie. Proto existuje široká škála kvality i chyb, na všech úrovních a ve *všech* typech kryptoprostředků.
- **V oblasti aplikované kryptologie se dnes neuvědoměle (z neznalosti) dost riskuje.**

Marketing

Marketingové materiály zřídkakdy odráží skutečný produkt a často obsahují seznam cílů výrobce, které by měly být obsaženy v následující verzi produktu.

Na křídovém papíru a s barevnými obrázky vypadá všechno mnohem lépe.

Pokud se Vám marketingové materiály líbí a jsou opravdu profesionálně udělané, nekupujte si příslušný (kryptografický) produkt, ale kupte si od něj ty marketingové materiály.

Komerčně zvrácená bezpečnostní koncepce kryptografie v IT a manažerská reakce

- Komerční kryptografie je dnes v zajetí maximální rychlosti a minimální ceny řešení.
- Svět nechce bezpečné funkce, ale rychlé funkce, u nichž nejsou známy slabiny (komerčně zvrácená bezpečnostní koncepce).
- Roste funkčnost, zvyšuje se paměť, rychlost procesorů, narůstá objem dat. To vyžaduje rychlejší přenosy, rychlejší a nové šifry, podpisy, haše,....

Enormní požadavky na výzkum přináší zvyšování rizika prolomení kryptografických nástrojů.

- Důsledek pro manažery: **přísně modulární** výstavbou nových systémů nebo nakupováním a užíváním nových prostředků tak, aby bylo možné jednoduchou aktualizací SW nebo FW **jednoduše vyměnit** prolomené nebo oslabené kryptografické algoritmy.

Vize

Trend zvrácené bezpečnostní koncepce bude pokračovat. Kryptologie proto ani v blízké budoucnosti nebude poskytovat informačním technologiím příliš mnoho jistoty a jednoduchých nástrojů.

- Příčina: IT nemají pro bezpečnost připravenu architekturu.
- Tam, kde je architektura připravena, kryptografie se snadno a vysoce účinně realizuje (profesionální produkty na ochranu utajovaných informací).

Až si to potřeba praxe vyžádá a vývoj půjde směrem vyžadování bezpečnosti v IT, kryptologie budoucnosti bude přímo součástí základů informačních technologií, nebude nás obtěžovat a pravděpodobně o ní téměř nebudeme ani vědět. A bude velmi kvalitní.

Manažerské shrnutí

- 1. teze: Kryptologie není žádná zvláštnost, ale jedna z metod informační bezpečnosti. Nepřeceňovat, neignorovat, delegovat její výkon na specialistu, zajistit její řízení.

- 2. teze: Pěstujte si svého kryptologa nebo kryptoinženýra, sejme z vás odbornou odpovědnost.

Literatura

- Aarjen Lenstra: Poslední vývoj v kryptografii, Information Security Summit 2001, Praha, 30.-31. května 2001.

- Vlastimil Klima, Ondrej Pokorny, Tomas Rosa: Attacking RSA-based Sessions in SSL/TLS, CHES 2003, pp. 426 - 440, Springer - Verlag, 2003, http://eprint.iacr.org/2003/052.pdf,

- Vlastimil Klíma, Tomáš Rosa: **On-line archiv** (56+...) článků ze seriálu „**Kryptologie pro praxi**“, publikovaných v časopisu Sdělovací technika, dostupné na stránkách autorů http://cryptography.hyperlink.cz/, http://crypto.hyperlink.cz/