Současná kryptologie v praxi

Vlastimil Klíma

v.klima@volny.cz

kryptolog
http://cryptography.hyperlink.cz
Praha

Abstrakt

Přednáška přináší stručný manažerský přehled kryptografické technologie, zabývá se použitelností kryptografických nástrojů a úrovní jejich bezpečnosti. Uvádí příklady z praxe a novinky z oboru. Obsahuje doporučení pro manažery jak se v kryptologii zorientovat, co je v současné době nejdůležitější a co podstatné pro její řízení.

Klíčová slova: kryptologie, manažeři

1 Úvod

Příspěvek je určen manažerům informačních systémů a bezpečnosti. Jeho cílem je předat jim zkušenosti a doporučení pro jejich činnost, pokud se ve své práci dostanou do kontaktu s aplikovanou kryptologií.

Dnešní kryptologie už není věda o utajování, kterou byla čtyři tisíce let, nyní je to věda o matematických metodách informační bezpečnosti.

Dříve bylo jejím obsahem navrhování šifer a jejich luštění. Dnes je jejím předmětem návrh nejrozmanitějších matematických metod informační bezpečnosti (kryptografie) a na druhé straně odhalování jejich slabin (kryptoanalýza). Výstupem kryptografie nemusí být jen šifra, ale třeba algoritmus prokazující zachování integrity, nepopiratelnosti odeslání digitálního dokumentu elektronickou poštou, protokol prokázání identity nebo protokol výměny klíčů. Výsledkem kryptoanalýzy může sice být odhalený šifrovací klíč nebo rozluštěný otevřený text jako dříve, ale dnes to spíše bude digitální dokument s falšovaným elektronickým podpisem, ale i důkaz toho, že nějaká kryptografická technika má větší riziko prolomení, než bylo o ní předpokládáno v době jejího nasazení. Z různých hledisek se kryptologie může zdát výjimečná, a *proto by kryptologové rádi viděli, aby jejich dítě bylo něco zvláštního.* Z manažerského hlediska však při podrobnějším zkoumání žádné velké rozdíly od ostatních metod informační bezpečnosti nenajdeme. Například jsme si vyvrátili postupně argumenty, že:

- kryptologii se na světě věnuje velmi málo lidí (skutečným *teoretickým matematickým metodám* antivirů, antispamů apod. se věnuje možná ještě méně lidí než kryptologii),
- kryptologie je více založena na matematických základech (kryptologie používá velmi mohutně *heuristické metody*, možná ještě více než antiviry; používané metody jsou sice matematické, ale matematika až na jednu dvě výjimky stejně nezajišťuje jejich absolutní neprolomitelnost),
- důsledky nesprávného použití nebo chyby nebo výběru špatné kryptografické techniky mohou mít větší následky než u jiných metod (*těžko říci, co způsobí větší škodu*, jestli špatně nastavený antispam, který zahodí poptávkový mail, jež mohl půl roku živit firmu, nebo ztráta notebooku s nešifrovanými daty).

*Odtud činíme **první manažerský závěr**:*

Kryptologie je jedna z metod informační bezpečnosti, není nutné se jí věnovat více než ostatním metodám, jako třeba antivirům, antispamům nebo firewallům .

Jediný rozdíl, na který jsme přišli, je, že má bohatší historii a dokonce už zasáhla i do chodu dějin. To však ostatní metody informační bezpečnosti v nejbližších čtyřech tisíciletích mohou ukázat také. 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 dalších služeb.

Jsou to:

- **utajení,**
- **autentizace,**
- **integrita,**
- **nepopiratelnost.**

Tyto služby kryptografie dosahuje různými technikami, algoritmy, protokoly, nástroji. Mezi základní patří

- **Symetrické šifry - proudové, blokové,**
- **Autentizační kódy zpráv (MAC),**
- **Hašovací funkce,**
- **Klíčové hašovací autentizační kódy zpráv (HMAC),**
- **Generátory náhodných znaků a pseudonáhodné generátory,**
- **Asymetrická schémata digitálního podpisu,**
- **Asymetrická schémata pro šifrování,**
- **Asymetrická schémata dohody na klíči,**
- **Kryptografické protokoly,**
- **a další.**

V každé z uvedených oblastí existuje vždy mnoho *algoritmů* a většinou i několik uznávaných *mezinárodních norem a standardů*, které mají různé *parametry* a *vlastnosti*, vhodné pro různé *druhy použití*. Konkrétních *technik* (*šifer, protokolů, modů, parametrů*) stále přibývá, místo aby ubývalo. Vzniká mnoho *norem*, které říkají, jak se mají tyto algoritmy *implementovat, nastavovat, kombinovat a používat.* Tyto normy je důležité *přesně dodržovat*. Mnohokrát bylo ukázáno, že *"lidová tvořivost" ve vlastním výkladu norem je většinou fatální*. I když kryptografických norem jsou tisíce, pro daný konkrétní případ se jejich množina velmi zužuje. *Normy jsou většinou vyjádřením zkušeností řady odborníků v oboru, jejich aktuálnost a bezpečnost bývá sledována, a proto by měly být velmi dobrým pomocníkem pro aplikování kryptografických metod, pokud pro danou oblast existují.*

Dnes není nedostatek kryptografických technik, ale **chybí vrstva kryptoinženýrů a kryptoinformatiků**, kteří by je uměli správně *kombinovat a implementovat.*

Každá norma musí být konfrontována se současným stavem kryptologie, neboť jsme ukázali, že kryptologie je velmi živá a přináší nové útoky a s nimi i nová protiopatření, která se musí průběžně a co nejrychleji zapracovávat, jako v ostatních metodách informační bezpečnosti.

Příklad:

- Nejpoužívanější norma pro aplikaci nejpoužívanějšího asymetrického kryptosystému, PKCS#1, prošla zásadními změnami.

  (První útok na ni ukázal Bleichenbacher v roce 1998 [2], v roce 2003 byl útok ještě prohlouben, viz Klíma-Rosa-Pokorný [3]. V obou případech byla přijaty záplaty v nejdůležitějších aplikacích, například protokolu SSL, ihned po vydání zprávy).

- IP šifrátory.

  (Šifrují protokol IP a byly konstruovány podle platných, prověřených a vyzrálých standardů IPSec. Tato zařízení se předřadí lokálním sítím nebo jednotlivým počítačům v síti a zajišťují, že veškerý provoz mezi nimi je šifrován. Proto tato zařízení mohou být propojena prostřednictvím jakékoliv veřejné sítě, třeba internetu. Tyto drahé "železné krabice" se obvykle jednou nastaví, a pak léta pracují a spolehlivě chrání přenášená data, aniž bychom se o ně museli nějak zvlášť starat. Použití nejnovějších kryptoanalytických metod (tzv. postranních kanálů, viz dále) však ukázalo, že komunikaci lze poměrně snadno dešifrovat! Proto tato zařízení bylo nutné okamžitě překonfigurovat, jinak by se staly zbytečnými kusy železa, vhodnými jen do šrotu [1, díl 51 a 52].)

2 Novinky

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

- V celosvětové veřejné soutěži byl přijat nový šifrovací standard AES, USA jej dokonce poté schválily pro ochranu utajovaných informací stupně TOP SECRET
- Byly nalezeny slabiny v konstrukci téměř všech moderních hašovacích funkcí, včetně nejpoužívanější SHA-1, která za dva roky již nebude podporovaným standardem a měla by být do té doby nahrazena,
- připravuje se standard SHA-3 v celosvětové veřejné soutěži jako AES,
- Byly nalezeny kolize hašovací funkce MD5 a jejich generování je otázkou vteřin na notebooku,
- Byla ukázána možnost rozšifrování protokolu SSL,
- Byla ukázána možnost získání privátního podpisového klíče PGP,
- Byla objevena revoluční metoda kryptoanalýzy, tzv. postranní kanály. Jejich aplikace přinesla snové výsledky a jedná se o bezprecendentně nejúčinnější metodu kryptoanalýzy,
- 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.

3 Interpretace a vyhodnocování kryptologických zpráv (novinek)

Pro manažera bezpečnosti je vyhodnocování novinek z oblasti virů, záplat operačních systémů nebo programů běžnou věcí, kterou je dávno zautomatizována a přenechána pověřeným pracovníkům. Avšak vyhodnocování novinek z oblasti kryptologie je většinou ponecháno na bedrech manažerů a při absenci "podnikového kryptologa" je přenecháno lidové tvořivosti pracovníků IT. Odtud činíme ***druhý manažerský závěr***:

Kryptologie není nic zvláštního, je to jedna z metod informační bezpečnosti, je však nutné se jí věnovat alespoň tak jako ostatním metodám, jako třeba antivirům, antispamům nebo firewallům.

Interpretace kryptologických novinek je dosud nejslabší stránkou aplikované kryptologie, a to i v kryptologicky vyspělých zemích, kde je vrstva kryptoinženýrů a kryptoinformatiků vychovávána o 10 - 15 let déle než u nás.

4 Současný stav

Kryptologie nám v současné době neposkytuje příliš mnoho jistoty. Možná 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, o níž hovořil A.Lenstra zde v roce 2001 [4]. To má praktické důsledky v tom, že musíme pracovat s rizikem prolomení těchto metod. Pokud tato rizika pouze ignorujeme, může pro nás mít zásadní objev fatální důsledky. Vždyť co by znamenalo jiného objevení metody faktorizace velkých čísel pro světové internetové bankovnictví nebo pro světový internetový obchod? Co všechno pečlivě zašifrované v minulosti, by bylo odhaleno? Co by znamenalo, kdyby zásadní pokrok v použití kvantových počítačů umožnil dešifrovat všechny symetrické šifry?

Druhým velkým rozporem kryptologické současnosti je rozpor mezi teorií a praxí.

Na jedné straně existují metody šifrování, které nerozluští ani nejmocnější luštitelské služby světa, a přitom je může používat obyčejný občan. Na druhé straně jsou na exponovaných místech používány šifry nebo jiné kryptografické metody tak špatně, že jejich význam je degradován. Na jedné straně masově používaný operační systém obsahuje silné nástroje šifrování, na druhé straně je málokdo používá z důvodu složitosti, obavy o ztrátu dat nebo nedůvěry z existence zadních vrátek. Na jedné straně existují volně dostupné zdrojové kódy PGP a dalších programů, na druhé straně jsou tak složité, že za bezpečnost celého produktu dá ruku do ohně jen málokdo.

Moderní kryptoanalýza dokáže proměnit šifrovací zařízení v samotné vykonavatele útočníkových výpočtů. To je důsledek revolučního rozvoje kryptoanalýzy. Takové možnosti kryptoanalytikové nikdy předtím v historii neměli. Tímto způsobem byla v roce 2003dešifrována i komunikace, chráněná protokolem SSL [3].

Kryptologie je ve fázi exponenciálního rozmachu do šířky, hloubky i významu nových věcí, které přináší, v kladném i záporném směru. To vede k řadě problémů v praxi, která nestačí vstřebávat nové výsledky a zapracovávat existující know-how do kryptografických produktů a systémů. Kryptologie přináší nové úžasné možnosti obráncům, ale také útočníkům. A chybí odborníci, kteří by byli schopni sledovat tento vývoj a v praxi aplikovat odpovídající obranná opatření. *Setkáváme se proto s celou škálou aplikací, prostředků a systémů, které patří k absolutní špičce, i se školáckými chybami na všech úrovních*, včetně velmi citlivých z hlediska možného dopadu. I v celosvětově rozšířených bezpečnostních produktech nalezneme hrubé chyby, které tyto produkty otevírají útočníkům. Příčinou je ohromný tlak konkurence a trhu. Bezpečnost je až v druhé řadě za funkčností. U produktu se v napjatých termínech často stihne vývoj tak, že je částečně splněna funkčnost, bezpečnost se doplňuje na poslední chvíli nebo "až pak". *Místo kryptologů a kryptoinženýrů kryptologii nakonec často "dolepují" aplikační programátoři.* Jenže bezpečnost nelze dolepovat, musí být od začátku zahrnuta v architektuře a někdy bohužel znamená i uživatelský diskomfort. Odtud činíme tuto ***manažerskou poznámku***:

V oblasti aplikované kryptologie se obecně vzato neuvědoměle příliš riskuje.

5 Interpretace marketingových materiálů

Z výše uvedeného vyplývá, že je nutné velmi pečlivě ověřovat pravdivost informací, uváděných o kryptografických produktech.

Typické chyby marketingových materiálů: nedostatečná specifikace technik, použití nekvalitního RNG, aplikace staré normy, použití nevhodného modu šifrování nebo nevhodné techniky, nedokonalá autentizace, nedomyšlené zálohování a obnova klíčů, nekvalitní generování klíčů, nezajištěná ochrana klíčů po celou dobu jejich životnosti (včetně dokonalého mazání), nedomyšlená obnova dat, nemožnost kryptografické konfigurace a aktualizace.

Mezi základní rady jak hodnotit marketingový materiál patří také:

- ověření a ochota dodavatele umožnit ověření, že produkt realizuje danou techniku tak, jak tvrdí,
- vyzkoušení praktického chování produktu ve zkušebním provozu,
- posouzení vlastností nezávislým subjektem,
- ověření, že výrobek má certifikáty, které deklaruje (často tento certifikát mají jiné verze daného produktu).

6 Základní teze

Základní teze tohoto příspěvku je:

Kryptologie není nic zvláštního, je to jedna z metod informační bezpečnosti, chovejte se k ní úplně stejně jako k ostatním metodám, třeba jako k antivirům, antispamům, bezpečnostním záplatám operačních systémů a aplikací nebo personální, procesní či fyzické bezpečnosti.

Pravděpodobně nenajdeme manažera, který by v rámci své funkce zkoumal logické algoritmy antivirů, antispamů nebo nastavoval firewall. Proč by se tedy manažeři měli orientovat v kryptologických metodách? A přesto po nich často někdo chce rozhodnout, jak dlouhý klíč mají mít certifikáty nebo jestli k šifrování firemní sítě zakoupit ten či onen šifrovací prostředek nebo co pro firmu znamená zpráva z médií, že elektronický podpis je ohrožen. Příčinou je, že v průmyslu IT chybí vrstva kryptoinženýrů a kryptoinformatiků, kteří by manažerům měli připravit podklady k rozhodnutí. Rozhodování bez dostatečných informací dnes v oblasti kryptologie na svých bedrech odnáší manažeři. A proto další rada je:

Pěstujte si svého kryptologa

Pěstujte si svého odborníka, který bude mít kryptologii na starosti a bude sledovat novinky, vzdělávat se, informovat vás a připravovat podklady pro vaše rozhodnutí. Protože samostatného kryptologa si většina firem a institucí nebude chtít nebo moci dovolit, je možné zadat tuto problematiku někomu třeba jako poloviční pracovní náplň. Ideální, pokud to nebude člověk z IT, abyste měli dva úhly pohledu. Současný stav, kdy manažeři musí na různých školeních také vstřebávat technické problémy kryptologie (často podávané tak populárně, že je to stejně málo efektivní) je dlouhodobě špatný.

7 Honba za rychlostí

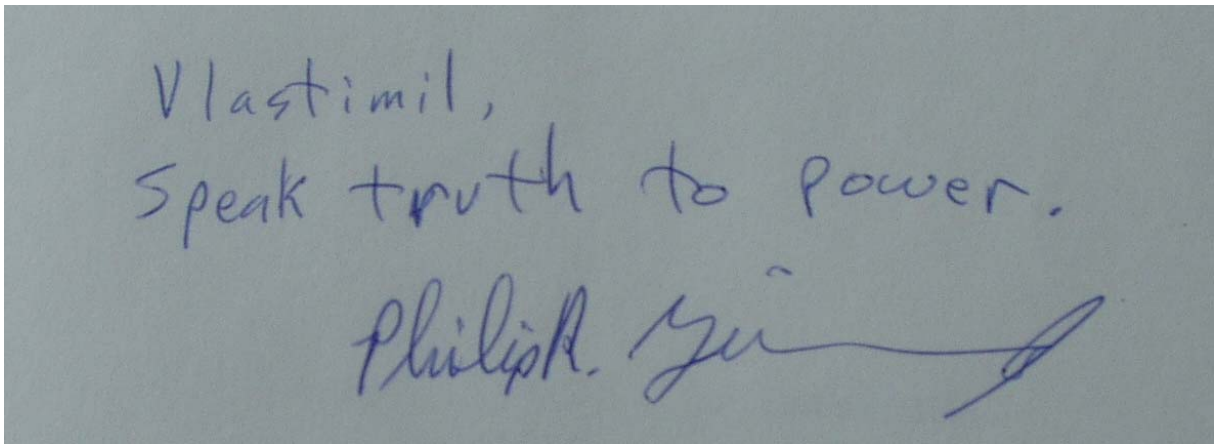
Komerční kryptografie je dnes v zajetí maximální rychlosti a minimální ceny řešení.

Svět nechce bezpečné funkce, ale rychlé funkce, u nichž nejsou známy slabiny.

Toto je důsledek tržní ekonomiky, která na první místo staví funkčnost. Elektronika se zrychluje, zvyšuje se paměť, rychlost procesorů, narůstá objem dat. To vyžaduje rychlé přenosy. Důsledkem jsou nové požadavky na rychlé proudové šifry, rychlé blokové šifry, rychlé hašovací funkce, rychlé asymetrické kryptosystémy. Například nový světový hašovací standard SHA-3 bude muset být pravděpodobně nejen bezpečnější než starý, ale také rychlejší. Tyto požadavky jsou však klasicky v přímém rozporu, nicméně praxe je taková. To klade na výzkum enormní požadavky a vede to ke *zvyšování* rizika prolomení takových kryptografických nástrojů (podtrhujeme slovo zvyšování, protože uvedené riziko existuje i tak, vzhledem k nedokazatelnosti bezpečnosti většiny kryptografických nástrojů). Protože uvedený trend bude pokračovat, manažeři na to musí reagovat *přísně modulární výstavbou nových systémů nebo nakupováním a užíváním nových prostředků tak, aby bylo možné jednoduchou aktualizací SW nebo FW jednoduše nahradit prolomené nebo oslabené kryptografické algoritmy.*

8 Jak budeme šifrovat v roce 2100 ?

Kryptologie obecně neposkytuje v současné době informačním technologiím příliš mnoho jistoty a jednoduchých nástrojů. Příčinou je, že matematické metody informační bezpečnosti se v současných informačních technologiích nedají jednoduše a účinně použít, protože současné informační technologie nejsou pro účel bezpečnosti konstruovány, nemají pro to připravenu vhodnou architekturu. Až budou informační technologie od základu navrhovány tak, aby mohly být bezpečné nebo bezpečnost u nich bezpečně doplňována, kryptologie jistě přijde s jednoduchými a bezpečnými nástroji. To dokazují profesionální produkty například na ochranu utajovaných informací, kde bezpečnost je od jejich počátku základem jejich architektury. Tam kryptologie již nabízí vysoce účinná řešení. Pokud vývoj půjde směrem vyžadování bezpečnosti, kryptologie budoucnosti bude přímo součástí základů informačních technologií, nebude nás obtěžovat a pravděpodobně o ní téměř nebudeme ani vědět.



Obr. 1: Rada otce PGP: "říkej mocným pravdu"

9 Manažerské shrnutí

V příspěvku jsme se snažili popsat současný stav, provést jeho analýzu a vyvodit závěry. Z manažerského hlediska jsme učinili tento závěr: kryptologie není žádná zvláštnost, ale jedna z metod informační bezpečnosti. Z toho také plyne jak se k ní chovat: neignorovat, nepřeceňovat, delegovat její výkon na specialistu a zajistit pouze její řízení.

10 Poděkování

Rádi bychom poděkovali za velice cenné připomínky zejména Mgr. Pavlu Vondruškovi a doc. Vašku Matyášovi, Ph.D. Druhému jmenovanému patří též velký dík za skvělý překlad článku do angličtiny.

Literatura

[1] Vlastimil Klíma, Tomáš Rosa: 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/

[2] Daniel Bleichenbacher: Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, CRYPTO '98, pp. 1 - 12, Springer - Verlag, 1998,

[3] 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,

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