# Oblíbené mýty a omyly

Letos koncem května se v areálu Pražského hradu bude konat již devátý ročník konference Information Security Summit 2008. Autoři seriálu kryptologie pro praxi zde přednesou příspěvky na téma RFID a na téma řízení kryptologie. Ač se řízení kryptologie zdá odtažité pro technicky orientovaný časopis, určitě v článku najdete něco ze své firemní praxe.

## Porady podle Parkinsona

Na mnoha firemních jednáních to vypadá, že šifrám rozumí každý, zatímco antiviry a firewally po letech zevšedněly a přenechávají se specialistům. To proto, že je s nimi mnoho práce a odpovědnosti a každému je jasné, že by se mohl spálit. Naproti tomu do šifer se mnozí pašáci (tedy ti, co všemu rozumějí, a jdou hned na věc) pouštějí na všech úrovních. Parkinsonovy zákony se projevují v půlhodinových diskusích na téma jak má být dlouhé a z čeho se má skládat heslo, zatímco systémová bezpečnostní opatření jsou vyřízena za deset minut, neboť účastníci porady jsou již odborně vyčerpáni a také je tlačí čas. Takže se to přesune jako vždy na oddělení IT. Avšak na příští poradě se pro IT schválí jen seškrtané prostředky, čímž je původní problém vyřešen a vrací se jako aktuální až zase za rok.

## Chybějí kryptoinženýři

To podstatné na současné situaci je, že ve světě a v Česku obzvlášť chybí vrstva kryptoinženýrů, kteří by mohli od řídicích pracovníků a od oddělení IT převzít agendu aplikované kryptologie. Měli by být pomocníkem manažerů, kterým by připravovali odborné podklady pro jejich rozhodnutí. Naším seriálem se vlastně snažíme o to, aby zájemci o tuto oblast měli k dispozici alespoň nějaký studijní materiál pro sebevzdělávání. Doba, kdy naše vysoké školy a univerzity tuto mezeru zaplní, je ještě vzdálená, i když příslušné odborníky již mnoho let vychovávají.

## Pěstujte si svého kryptoinženýra

Jde o to, že kryptologie proniká do mnoha systémů a produktů a je potřeba se v ní začít trochu orientovat. Už jste viděli řídicího pracovníka, aby nastavoval firewall nebo posuzoval, který je lepší? Asi ne, spoléhá se na vyjádření specialisty. Ale v oblasti aplikované kryptologie je dnes na toto rozhodování sám, je na něm, jaký šifrovací prostředek vybere nebo jaké certifikáty zvolí. Proto často dochází k nepřiměřenému riskování. Dobrým rádcem není ani dodavatel (ať je jeho zástupce v jakékoliv vysoké funkci), který vyjmenuje všechny výhody a nezřídka i normy, jež jeho produkt splňuje. Je potřeba znát drobné nuance. Třeba, že bezpečnostní certifikát nemá nabízený produkt, ale jeho jiná verze, která se ovšem nedováží, nebo kterou můžete také mít, ale nutno si ještě něco dokoupit nebo doinstalovat, ... Nebo jak se vyznat v lákavých nabídkách šifrovaných disků, které používají 128bitové šifrování a ochránily by vaše firemní data (jeden příklad z několika podobných na trhu, [1]) ?


**Obr. 1 Data jsou takzvaně šifrována 128bitovou šifrou, přesto je přečte každý [1]**

Přitom kryptoinženýr by manažerovi řekl, že v materiálech je sice napsáno, že je tam silné 128bitové šifrování, ale nikdo tam přímo netvrdí, že data na disku jsou šifrována (ani jak a čím). A skutečnost je taková, že data z mnoha tzv. šifrovaných disků může získat každý, kdo ho umí fyzicky přečíst. Stoosmadvacetibitová šifra je zde skutečně použita, ale nikoli k šifrování dat, nýbrž k vytvoření jednoho řetězce, který je uložen na disku a který překrývá (operací xor) všechny jeho sektory. Aplikační kryptolog by po přečtení marketingového materiálu, kde stojí „používá se 128bitové šifrování“, ihned pojal silné podezření. Především tam chybí konkrétní šifra a její modus (způsob použití). Z našeho seriálu ve ST je poučen, že šifrování disků je vážný problém, který řeší mezinárodní normy a uhnutí od nich znamená značné riziko. V uvedeném případě chybějí nejen tyto normy, ale i konkrétní šifra. Zatímco manažer by byl spokojen, protože slyšel, že 128bitové šifrování se považuje za kvalitní, kryptoinženýr by ho z omylu vyvedl. Z našeho seriálu by také věděl, že i 256bitová šifra, a to i kvalitní standard, je k ničemu, když se použije špatně.

## I půlkryptolog je velký náskok

V Česku je nedostatek kryptoinženýrů nejen mezi dodavateli (nejodbornější odpověď je, že je tam šifra AES, a proto je to bezpečné), ale i mezi odběrateli. Obvykle není nutné zaměstnávat kryptologa na plný úvazek, ovšem doporučujeme svěřit tuto problematiku firemnímu specialistovi na půl nebo čtvrt úvazku, ale oficiálně. Tento člověk se vám bude starat o novinky, podklady, bude se vzdělávat a bude také odpovědný za přípravu podkladů pro vaše rozhodnutí. Bude trápit dodavatele svými dotazy a zkoumat výhody či nevýhody nabízeného řešení, stejně jako to dělá oddělení IT při výběru antispamu, firewallu nebo antiviru. Je nutné, aby o kryptografické bezpečnosti a aplikacích rozhodovali alespoň samoukové. Ti, kdo nemají svého čtvrtkrypptologa nebo půlkryptologa, nejsou schopni často ani formulovat své požadavky a očekávání od bezpečnostního produktu. A protože dodavatel také o kryptologii mnoho neví, vzniká kuriózní situace.

## Dezinterpretace

Často se setkáváme s tím, že novinky v oboru jsou dezinterpretovány. Například nedávno (květen 2007) bylo faktorizováno 1039bitové číslo. Manažeři se mohli vyděsit, neboť schopnost faktorizace takto velkých čísel by mohla prolomit řadu komunikací chráněných 1024bitovým RSA. Ve skutečnosti toto číslo mělo speciální tvar, mělo známý 22bitový faktor, a tak se jednalo o faktorizaci 1017bitového speciálního čísla. Ani to však nic neznamená pro bezpečnost RSA, neboť na speciální číslo byla použita jiná metoda, než je nutné použít na faktorizaci používaných nespeciálních modulů RSA. Jinými slovy, kryptolog by manažera uklidnil a ukázal mu tabulku: v roce 1994 bylo faktorizováno 426bitové číslo, v roce 1999 512bitové, v roce 2005 663bitové, zatím nejvyšší. Manažer si pak může interpolovat: pokud vše půjde stejným tempem, lze očekávat v roce 2010 800bitové a v roce 2015 až 2020 1024bitové. Podobně byla dezinterpetována řada výsledků v oblasti hašovacích funkcí a dělány nepodložené závěry o bezpečnosti elektronického podpisu. To, že u MD5 lze generovat kolize, neznamená, že z tabulky zhašovaných přístupových hesel je lze získat v otevřené podobě apod. Také to neznamená, že MD5 je špatná a nelze ji použít vůbec k ničemu. Lze přimhouřit oči, když se říká autentifikace (správně autentizace), nebo „podepíšeme to certifikátem“ (privátním klíčem) nebo „koupíme si elektronický podpis“ (koupíme si certifikát), ale pokud ponecháme interpretaci kryptologických a bezpečnostních novinek laikům (nebo přímo pašákům), vystavujeme se zbytečně rizikům.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

*LITERATURA*

*[1] http://www.easy-nova.com/index. php?siteID=18&productID=28*

*[2] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz*