Oblíbené mýty a omyly (3)

Stálicí mezi Obecně Oblíbenými Omyly v kryptografii je „pohádka o asymetrické kryptografii“, často vyprávěná jako „pohádka o PKI pro manažery“. Natolik se pohádka již rozšířila, že zkratka PKI (infrastruktura veřejných klíčů) se dostala do prezentací manažerů a všech, kdo chtějí vypadat in.

Mýtus o PKI

Pro čtenáře, kteří se chtějí seznámit se základy asymetrické kryptografie, doporučujeme články ve ST (3–6/2004) [1] nebo učebnici [2] (obojí on-line). V dalším už předpokládáme, že čtenář ví, co je veřejný a privátní klíč. Skoro na každé prezentaci naleznete následující již klasickou pohádku o asymetrické kryptografii. Představme si, že máme síť o N bodech (klientech) a každý chce komunikovat s každým pomocí klasické symetrické kryptografie. Takže každý musí mít svůj klíč pro komunikaci s každým *(obr. 1)*. V celé síti tak musí existovat $N(N–1)/2$ nebo $N(N–1)$ klíčů podle toho, jestli chceme, aby klíč pro spojení z bodu A do B byl stejný jako klíč pro spojení z bodu B do bodu A nebo ne. Je-li účastníků tisíc, klíčů je řádově milion, je-li účastníků milion, klíčů je řádově bilion. Takové množství klíčů je obtížné spravovat, proto pro velkou síť je nutné použít asymetrickou kryptografii, kde každý ze zúčastněných má pouze dva klíče – jeden veřejný a jeden privátní. Přitom to stačí na to, aby všichni mohli šifrovaně komunikovat se všemi! A to je konec pohádky.

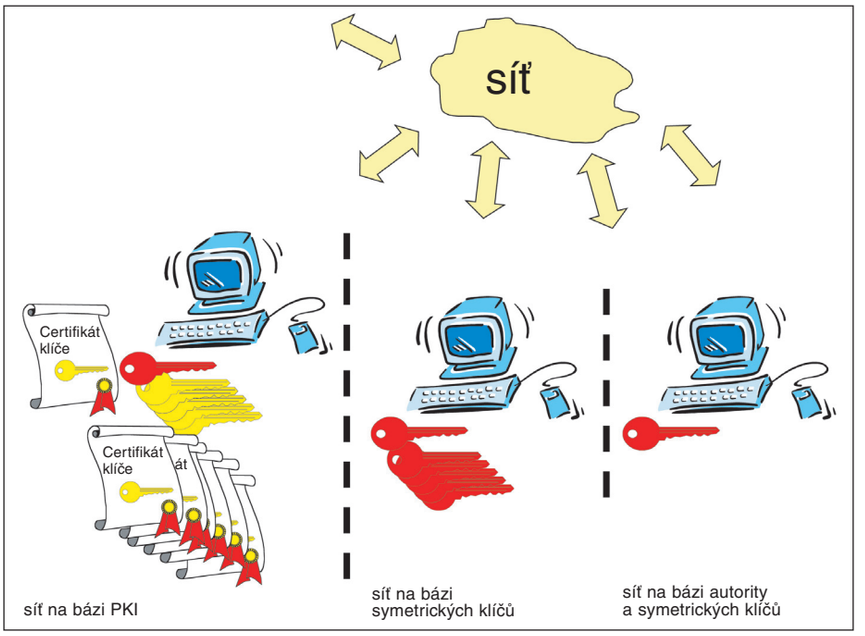
Kde je čertovo kopýtko?

Klasik praví, že čertovo kopýtko je skryto v detailech a naše pohádka je čertovými KOPYTY přímo prošpikovaná. Na úvod poznamenáváme, že přínos asymetrické kryptografie je ohromný a nezastupitelný, jen se „obouváme“ do této pohádky, která v rámci jednoduchého výkladu a zápalu pro asymetrii zcela zamlžuje její základní výhodu (a tou je nepopiratelnost, nikoli množství klíčů).

Především, chce-li někdo v naší pohádce komunikovat s každým, musí mít pro každého příjemce k dispozici jeho veřejný klíč. Čili původní optimistický obrázek pro asymetrický systém, že u každého účastníka jsou jen dva klíče, se mění na obrázek, kdy je u něj jeden (jeho) privátní klíč (na obrázku červený) a N–1 klíčů veřejných pro spojení s ostatními účastníky (na obrázku žluté). Celkem zde tedy máme N klíčů u každého z N účastníků, což dává $N.N$ klíčů v celé síti. Kdybychom chtěli používat stejnou mystifikaci, jako byla použita v pohádce, řekli bychom, že asymetrická síť potřebuje klíčů více než původní síť symetrická, neboť evidentně $N.N > N(N–1) > N(N–1)/2$.

Náš pohotový „pašák“ (tedy ten, co všechno ví nejlíp a „jde hned na věc“) namítne, že to není pravda, neboť veřejné klíče nemusí účastník mít u sebe, že je v případě potřeby může stáhnout z nějaké autority. Pašáci automaticky mluví o autoritě certifikační, ale, budete se divit, ony jsou i jiné [2]. V tom případě ovšem plně spoléhá na tuto autoritu, že mu místo požadovaného veřejného klíče příjemce nepodstrčí veřejný klíč svůj a tím elegantně nepřesměruje tajnou korespondenci na sebe. Pohádka o snadnosti a lehkosti PKI je ta tam. Vše je něčím zaplaceno, a tak, chceme-li mít svoji jistotu, musíme si pro vlastní síť udělat svoji autoritu, u níž máme neporovnatelně větší jistotu, že nás nepodvádí. Místo ní však můžeme mít jinou centrální autoritu (centrum), například server, který nedistribuuje asymetrické, ale symetrické klíče. Každému účastníkovi sítě pak stačí mít pouze jediný tajný (symetrický) klíč pro spojení s tímto centrem (například na čipové kartě, USB klíčence apod.). Při naší registraci do této sítě můžeme ale kromě tohoto klíče dostat přímo i celou sadu symetrických klíčů třeba pro milion účastníků sítě. Nebo můžeme klíč pro libovolného účastníka dostávat ad hoc od centra, když ho právě potřebujeme.

Dobře informovaný pašák zde okamžitě namítne, že to vyžaduje, abychom byli stále on-line ve spojení s centrem, zatímco u PKI to nepotřebujeme. Tam můžeme posílat třeba zašifrované e-maily bez on-line spojení s autoritou, protože certifikáty častých adresátů máme již uloženy na počítači. První omyl je, že nemusíme být on-line. Musíme, abychom si u (certifikační) autority on-line ověřili, že veřejný klíč našeho obvyklého adresáta ještě platí. Mohlo se totiž stát, že zamýšlený příjemce klíč ztratil a poté ho u autority zneplatnil (zablokoval). Pokud si neověříme, že daný klíč (nebo certifikát) stále platí, můžeme naše cenné informace poslat přímo do náručí nepovolané osoby.



Obr. 1 Pohádka o PKI v praxi – PKI potřebuje klíčů více než symetrický systém

Pohádka o PKI tedy není ani o počtu klíčů ani o on-line nebo off-line spojení, ale o charakteru klíčů a o službě nepopiratelnosti.

Jestli se tedy někdo ohání on-line spojením a možností on-line komunikace s milionem účastníků, musí důvěřovat nějaké autoritě, která tyto účastníky autentizuje – a to třeba veřejným certifikátem nebo firemním certifikátem, nebo firemním e-mailem nebo čímkoliv jiným, pochopitelně na dané úrovni bezpečnosti a jistoty. V každém případě, pokud chceme komunikovat šifrovaně s někým neznámým, potřebujeme od někoho jistotu, že ten neznámý na dané e-mailové adrese, na daném telefonním čísle nebo kdekoliv jinde v počítačové síti je opravdu ten, se kterým chceme hovořit, e-mailovat, nebo na dané místo posílat soubory nebo transakce. Identitu tohoto člověka, počítače, serveru nebo automatu si musíme nechat vlastně

zajistit někým jiným, a tím je to naše centrum, obecně „třetí důvěryhodná strana“.

Centrální autorita nemusí vědět všechno

Pokud takovou stranu máme, můžeme pomocí ní distribuovat buď certifikáty, nebo rovnou symetrické klíče. U symetrických klíčů odpadá pochopitelně celá mašinerie asymetrické kryptografie (se všemi jejími nevýhodami, ale bohužel i výhodami!). Podívejme se, jak systém funguje v případě symetrických klíčů. Stejně jako u PKI i zde můžeme mít v zásobě klíče pro všechny obvyklé adresáty, ale i zde stejně jako u PKI by bylo vhodné mít možnost si ověřit, že potřebný klíč není odvolán (zneplatněn). V zásadě je tedy malý rozdíl mezi on-line symetrickým centrem a on-line PKI. Avšak uvědomujeme si, že použité slovní spojení „v zásadě“ je ošidné spojení, a že rozdíl, který je někde nepatrný, může být v jiném systému nepřekročitelný. Proto se tak obtížně vyslovují soudy o symetrické a asymetrické kryptografii.

Pašák ještě nekončí a argumentuje, že v případě symetrického centra toto zná všechny klíče v systému a může dešifrovat veškerou komunikaci. První omyl je, že je to vždy nevýhoda, někdy je to naopak významná výhoda oproti asymetrii. Druhý omyl je, že centrum je všemocné. Konkrétní systém může být postaven tak, že centrum na požádání vygeneruje klíč pro spojení účastníka *A* s účastníkem *B* a zašle jim je (pochopitelně šifrovaně a každému pod jeho klíčem pro spojení s centrem). Poté tito účastníci (příslušná aplikace) vytvoří mezi sebou spojení šifrované tímto klíčem, ale pro komunikaci využijí jiný komunikační kanál, který není monitorován centrální autoritou (a vygenerují si a předají tímto kanálem klíč nový). Účastníci *A* a *B* v tomto případě pouze využijí toho, že je centrum vzájemně identifikovalo (autentizovalo, seznámilo) a utajení si zajistí jinak. Pokud je centrum „naše“ (například server nadnárodní firmy) a nemáme zájem na dešifrování komunikace, je systém dostačující. Pokud nechceme důvěřovat centru, lze využít jen jeho identifikující úlohu a pro ochranu spojení přijmout jiné metody.

Existují pouze konkrétní systémy

Je zřejmé, že na každý uvedený příklad a argument bude existovat protiargument nebo protipříklad, kdy je výhodnější ta či ona metoda. Těžko se dobereme v podobných diskusích konce, dokud si neuvědomíme skutečný rozdíl mezi symetrickou a asymetrickou kryptografií. A ten je v charakteru klíčů a ve službě nepopiratelnosti. U asymetrické kryptografie charakter klíčů umožňuje, aby jeden klíč mohl být veřejně znám. Služba nepopiratelnosti umožňuje (ve spojení s existencí veřejného klíče), aby nezávislá třetí strana mohla ověřit (a to bez znalosti jakéhokoliv privátního tajemství), že se nějaká událost stala či nikoli (například soudní znalec je schopen ověřit elektronický podpis, aniž by měl podpisový klíč, postačí mu jeho certifikát). Aby tato služba a možnost byla naplněna, je nutno splnit určité podmínky. A v těchto podmínkách, které pro různé systémy jsou více či méně splnitelné a smysluplné, je ono čertovo kopýtko a odpovídající riziko. A proto také nelze paušálně říci, že symetrické systémy jsou horší než asymetrické nebo naopak. Mohli bychom zkusit říci, že tam, kde není potřeba služba nepopiratelnosti, je pravděpodobně symetrický systém jednodušeji zaveditelný nebo levnější. Avšak umíme nadefinovat systém s takovými konkrétními podmínkami, kde ani toto platit nebude. Jinými slovy, bez posouzení potřeb konkrétního systému nelze o symetrickém a asymetrickém schématu říci ve skutečnosti vůbec nic, kromě vyprávění pohádek.

Popelka aplikované kryptografie

Tím, kdo nakonec rozhodne, jestli se někdo dostane k dešifrované zprávě, může být nenápadná postavička Popelky kryptografie, kterou je generátor náhodných čísel (RNG). Jak vidíte, v původní pohádce o PKI se o ní nic nedozvíme, a přesto ona bude mít nakonec poslední slovo. Například můžeme mít kvalitní vlastní autoritu, moderní podpisový elektronický systém využívající *asymetrické podpisové schéma* (třeba DSA nebo ECDSA) a na generátor náhodných znaků nám už nezbude energie nebo peníze, takže budeme využívat třeba systémový generátor odvozující náhodná čísla od aktuálního času v milisekundách. Teď si stačí připomenout, že systém (EC)DSA (viz ST 4/2004 [1]) používá tzv. dočasný, náhodně vygenerovaný klíč *k*, pomocí něhož vytváří elektronický podpis. Kvalita podpisu je dána kvalitou náhodného čísla *k*. Pokud víme, kdy byl podpis vytvořen s přesností na hodinu, máme pouze 3600.1000 možností hodnot počtu milisekund, a tím i hodnot klíče *k*. Všechny tyto hodnoty můžeme hrubou silou během velmi krátké doby vyzkoušet, zjistit hodnotu *k* a poté i privátní klíč (!) podepisujícího. Pak můžeme padělat podpis jakéhokoliv dokumentu.

Podobný význam má RNG u *asymetrických systémů pro šifrování*, kdy se ve skutečnosti asymetrickým systémem protistraně předává náhodně vygenerovaný symetrický klíč. Útočník tedy nemusí útočit na asymetrický systém (třeba RSA), ale přímo na RNG odesílatele. Třeba z jeho dokonalé znalosti ví, že po určité době degeneruje téměř do konstanty nebo vydává sice náhodně vyhlížející, ale stejné klíče, nebo na něj může aktivně útočit apod. Přitom pokud na RNG skutečně leží břemeno odpovědnosti (třeba při ochraně velmi drahých nebo velmi privátních informací), je získání kvalitních RNG v praxi velmi složité. Prakticky dostupných pohodlných řešení je velmi málo (kompromisem může být třeba čipová karta s certifikovaným RNG, pokud mu věříte), což dokládá to, že tato oblast je zanedbávaná.

U symetrických systémů (pokud přímo nepotřebujeme RNG pro generování klíčů) se teoreticky můžeme bez RNG obejít, ale není to ani obvyklé, ani příliš dobré. Pravděpodobně budeme potřebovat RNG pro tvorbu tzv. inicializačních hodnot, a to třeba pro proudové šifry, pro protokoly typu výzva-odpověď se symetrickými schématy, pro šifrování blokovými šiframi v modu CBC apod. I zde je význam RNG velký a závislý na místě použití, stejně jako u asymetrických systémů.

Tím to ale nekončí, protože jsme ani nevyjmenovali všechna použití RNG, ani nezmínili *další prvky kryptografické stavebnice*, pouze jsme ukázali na často opomíjenou roli RNG. Ďábel ovšem může být skryt ve VŠECH detailech kryptografického systému.

Synergie symetrie a asymetrie

Když to tak člověk čte, získává asi pocit, že nic není dost bezpečné. A to je také jediná pravda, ke které se diskusí skutečně dobereme. Vždy děláme kompromisy a vždy počítáme rizika. Kvalitní systém je proto vystavěn na definování a znalosti těchto rizik. Běžným řešením a výsledkem studií proveditelnosti se stává synergie symetrických a asymetrických systémů a aplikování přiměřených kryptografických prvků. Někde postačí generátory na bázi kvalifikovaného sběru entropie v systému, někde se musí zakoupit zásuvný HW modul do serveru. Někde je nejbezpečnější symetrický klíč domluvený při osobní schůzce, jindy kvalifikované certifikáty od veřejné certifikační autority, někdy obyčejné certifikáty, ale od důvěryhodné firemní autority nebo soubor (a/symetrických) klíčů uložených na flash disku na osobní klíčence. Ostatně technologie posouvají naše možnosti – na klíčence můžeme mít už klíče pro miliardu lidí (miliarda 128bitových symetrických klíčů zabere pouhých 16 GB) nebo ostatně kompletně všechna naše důležitá data.

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

LITERATURA

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

[2] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.: Handbook of Applied Cryptography, CRC Press, 2001, http://www.cacr.math.uwaterloo.ca/hac/