

Éra krátkých klíčů končí

Jedno známé bezpečnostní pravidlo praví, že útoky se nikdy nezhoršují, jen zlepšují. Roste také výpočetní síla a paměťová kapacita běžně dostupné techniky. Útočníci mají větší možnosti útoku hrubou silou a zvyšuje se velikost různých předem vypočítaných hodnot a tabulek, neboť je možné je rychleji vypočítat i uložit do velkých a levnějších pamětí. Na rostoucí možnosti potenciálních útočníků je pamatováno bezpečnostními rezervami i kontinuálním přizpůsobováním bezpečnostních opatření. Platí to i o kryptografii. Americký úřad pro standardizaci, který se stará o ochranu citlivých neutajovaných dat, v tomto směru vydal metodiky k délce klíčů a síle kryptografických mechanismů a tyto metodiky nyní aktualizuje. V ČR jsme přistoupili pouze k opatřením v oblasti síly hašovací funkcí, a to z důvodu zákona o elektronickém podpisu, protože nemáme ekvivalent americkému NIST. Metodiky NIST de iure nemají žádnou platnost mimo USA, ale v komerční oblasti jsou to ve skutečnosti mezinárodně respektované (a vyžadované) standardy. Seznámíme se tedy s názorem NIST k síle kryptografických algoritmů a časovému plánu jejich přechodu k silnějším. Jde o plánovitý a dlouho dopředu známý bezpečnostní proces, nic nového a nahodilého, co by odráželo nějaký konkrétní pokrok v kryptoanalýze. Ba právě naopak – toto je právě proces, který je výsledkem spojitého uvažování o pokroku v kryptoanalýze a výpočetní technice.

Měřítko bezpečnosti

Bezpečnost budeme vyjadřovat počtem bitů (n), odpovídající složitosti 2^n . Složitost je vždy počtem operací řešení příslušného matematického problému. Takže například pro AES-128 máme bezpečnost danou číslem 128, což znamená, že neznáme jinou metodu nalezení 128bitového klíče než útok hrubou silou se složitostí 2^{128} . Naproti tomu například u RSA-2048 s 2048bitovým modulem máme bezpečnost danou číslem 112, což znamená NISTem odhadovanou složitost řešení problému faktORIZACE takového modulu 2^{112} . Tou hlavní zprávou článku je, že doba bezpečnosti

80 bitů končí v roce 2010 a od roku 2011 je požadována bezpečnost alespoň 112 bitů. To například ze známých technik splňuje pouze 3DES se třemi různými klíči (DES se dvěma různými klíči je ohodnocena

80 bitů). Rozlišuje se také způsob využití digitálního podpisu na autentizaci dat (požaduje se 112 bitů), entit nebo pouze kontrolu integrity softwaru (80 bitů). U algoritmů digitálních podpisů se zpřísňuje

všechno: generátory náhodných znaků, délky klíčů, testy prvočíselnosti, kvalita generování parametrů apod. U algoritmů na bázi eliptických křivek se umožňují nové křivky, specifikované v normě ANS X9.62. Všem, kteří mají co do činění s digitálními podpisy, se doporučuje seznámit se s FIPS 186-3 a zvláštními příručkami NIST (Special Publication) SP 800-57 a SP 800-90.

Algoritmy dohody na klíči

K dohodě na klíčích, které mohou poté sloužit k šifrování, autentizaci nebo pro generování dalších klíčů, slouží algoritmy (protokoly) DH a MQV. V nich se ale používá i funkce pro derivování klíčů (KDF), která také musí v budoucnu splňovat silnější požadavky (definované v SP 800-56A). Implementace IKEv2, IKEv1, X9.42, X9.63, SSH a TLS (používající DH nebo MQV) budou muset pro ochranu citlivých dat po roce 2013 splňovat požadavky SP 800-56A.

Algoritmy pro předávání klíčů

RSA je klasicky používána pro šifrování symetrických klíčů. Požadavky na RSA pro přenos klíčů specifikují příručky SP 800-56B a SP 800-57. Změny se budou týkat přenosu klíčů ve velice rozšířených protokolech SSL a TLS aj., které budou posuzovány podle SP 800-56B (finální verze se dokončuje).

Algoritmy pro generování klíčů

Zpřísňují se také algoritmy pro generování nebo derivování klíčů. Těm se věnuje příručka SP 800-108.

Hašovací funkce

Konečně po roce 2010 nelze používat SHA-1 pro účely digitálních otisků, zatímco třída SHA-2 nemá stanoveno žádné časové ani aplikační omezení.

Generátory náhodných znaků

Generátory jsou použity pro různé aplikace – generování klíčů, soli, v protokolech

Tabulka 1 Posilování symetrických šifer

Šifrovací algoritmus	Nové produkty	Již certifikované produkty
Triple DES se 2 různými klíči	do 2010	Zákaz po 2010
Triple DES se 3 různými klíči	OK	OK
SKIPJACK	do 2010	Zákaz po 2010
AES-128, 192, 256	OK	OK

Tabulka 2 Posilování hašovacích funkcí

Hašovací funkce	Nové produkty	Již certifikované produkty
SHA-1	do 2010	V digitálních podpisech: viz tab.3 Pouze hašování: zákaz po 2010 Jiné aplikace: povoleno
SHA-224, 256, 384, 512	Povoleno pro všechny aplikace	Povoleno pro všechny aplikace

Tabulka 3 Posilování digitálních podpisů

Účel	Operace	Nové produkty	Již certifikované produkty
Autentizace dat	Vytváření podpisu	≥ 80 bitů do 2010 ≥ 112 bitů po 2010	< 112 bitů zákaz po 2010 ≥ 112 bitů po 2010
	Ověřování podpisu	≥ 80 bitů	Již certifikované produkty budou nadále platit
Autentizace entit	Ověřování i verifikace podpisu	≥ 80 bitů do 2013 ≥ 112 bitů po 2013	< 112 bitů zákaz po 2013 ≥ 112 bitů po 2013
Zajištění integrity SW a FW	Vytváření podpisu	≥ 80 bitů do 2010 ≥ 112 bitů po 2010	Již certifikované produkty budou nadále
	Ověřování podpisu	≥ 80 bitů	

pouze 80 bity!), RSA-2048 místo všudypřítomného RSA-1024, AES – 128 a další, viz dále. Přejít algoritmy na silnější verze ukazují přehledně tabulky. Algoritmy SKIPJACK (vyvinuté NSA s délkou klíče 80 bitů) a dvouklíčová DES se tedy v USA nemohou po roce 2010 používat k ochraně citlivých informací a všechny certifikované produkty je musí nahradit nebo budou vyřazeny ze seznamu certifikovaných prostředků.

Značný vliv na digitální podpisy

V rámci přechodu na bezpečnější klíče dochází také k přechodu od algoritmů digitálních podpisů podle normy FIPS 186-2 k tvrdší normě FIPS 186-3, a tím k velmi závažným změnám. Po roce 2010 nebude možné použít žádný podpisový prostředek, který vytváří digitální podpisy s SHA-1, RSA-1024 nebo DSA-1024. Rozlišuje se přitom prostředek, který podpis vytváří (požaduje se bezpečnost 112 bitů) a prostředek verifikační, který podpis pouze ověřuje (požaduje se bezpečnost min.

typu výzva-odpověď, ve výplni různých formátů apod. V podstatě se používají tři typy. Jsou to generátory, založené na SHA-1, na blokových šifrách a na standardu ANS X9.31 (dříve ANS X9.17). V roce 2007 byla schválena nová množina generátorů podle SP 800-90, která garantuje vyšší úroveň bezpečnosti. Proto se bude přecházet na tuto úroveň i u RNG. Staré generátory nebudou schvalovány po roce 2010 a od roku 2015 budou zakázány.

Závěr

Změny, které nepřinášejí žádný viditelný výsledek, jako je posilování bezpečnosti, jsou a budou vždy nepopulární. Jednou však taková situace nastat musí, jinak bychom asi dodnes používali Cézarovu šifru. Pokud budete plánovat nějaké změny, pamatujte na to, že kryptografie by měla být modulárně používaná (viz např. Současná kryptologie v praxi, Information Security Summit 2008, [2])

aby příští výměna nebyla tak drahá a náročná.

Vlastimil Klíma, nezávislý kryptolog,
v.klima@volny.cz

LITERATURA

- [1] NIST cryptographic toolkit: <http://csrc.nist.gov/groups/ST/toolkit/index.html>
- [2] Archivy autora a archiv článků kryptologie pro praxi: <http://cryptography.hyperlink.cz>