Digitální otisk SHA-4 přeskočil SHA-3

Vlastimil Klíma

Digitální otisk má dnes stejný právní význam pro data jako otisky prstů pro člověka. Bez nich by nebylo elektronické bankovnictví ani elektronický obchod. Letos skončí pět let trvající soutěž na nový standard digitálního otisku SHA-3, navzdory tomu byl ale právě nyní vydán standard SHA-4.

Využití digitálních otisků

Hašovací funkce mají velké využití ve výpočetní technice i v aplikované kryptografii. Používají se zejména v oblasti certifikátů a elektronických podpisů. Jsou to algoritmicky složité funkce, které libovolným vstupním datům přiřazují jejich jedinečný digitální otisk, nazývaný též hash nebo hašový kód. Každá hašovací funkce má definovánu pevnou délku digitálního otisku, což také odráží její bezpečnost – čím delší, tím větší bezpečnost.

Nejznámější hašovací funkce

O první standardy se postarala společnost RSA, která před 20 lety zavedla první slavné hašovací funkce MD4 a poté MD5. Obě byly sice prolomeny, ale udělaly velkou službu. Jejich štafetu převzaly již oficiální standardy amerického úřadu NIST, který nejprve vydal funkci SHA-1 se 160bitovým digitálním otiskem, a poté rodinu funkcí označovanou SHA-2, která zahrnuje funkce SHA-224, SHA-256, SHA-384 a SHA-512 s 224-, 256-, 384- a 512bitovými otisky.

Bezpečnost

S prolomením nejrozšířenější hašovací funkce MD-5 (k čemuž si autor dovolil také přispět nejrychlejší metodou hledání kolizí na světě [1]) vznikla nedůvěra v bezpečnost jejího následníka SHA-1 i celé třídy funkcí SHA-2. Všechny tyto funkce tříd MD i SHA vycházely z podobného způsobu míchání dat uvnitř těchto funkcí, tzv. Merkle-Damgardova principu konstrukce. Prolomení těchto funkcí, jak bylo naznačeno v úvodu, by mělo velké následky pro bezpečnost ve výpočetní technice, komunikacích, elektronickém bankovnictví a obchodu atd. Proto po nalezení praktických kolizí u MD5 a víceméně teoretických slabin u SHA-1 byla v roce 2007 vypsána soutěž na nový standard SHA-3. Ano, SHA-3, neboť v době nalezení kolizí u MD5 a slabin u SHA-1 už totiž existovala celá třída nových bezpečnějších funkcí SHA-2. Soutěž na SHA-3 byla vypsána v roce 2007 a letos skončí, byla vypsána proto, aby právě bylo zase v záloze něco pro případ, že by se našly problémy i u SHA-2. Ovšem průmysl nerad zavádí nové standardy, když nemusí, a tak byla situace dost tristní, neboť nebyl ani zdaleka ještě dokončen přechod od MD5 k SHA-1, když se „začalo strašit“ kolem bezpečnosti SHA-2, která se zaváděla do praxe pomaleji než hlemýždím tempem. Počítačový průmysl je šetřivý a v době, kdy už skončila platnost SHA-1 (od 1. ledna 2010 by neměla být používána v nových aplikacích), byla někde stále používána prolomená MD5 (a ještě dosud je!). Průmysl IT na rozdíl od teoretiků velmi dobře rozlišuje, co je „teoretické“ prolomení a co je praktické ohrožení nějaké funkčnosti. A tam, kde nic nehrozí nebo je riziko přijatelné, se prostě toto riziko přijme, i když si bezpečnostní technici ťukají na čelo.

Soutěž o SHA-3

Nový standard SHA-3 mohl tuto situaci elegantně vyřešit, pokud by byl zároveň rychlejší a zároveň bezpečnější než SHA-2. Pak by se překlenulo období laxnosti průmyslu a ten by mohl z SHA-1 přejít rovnou na SHA-3. To se také stalo a NIST kladl tyto dvě podmínky za základ soutěže. V prvním sítu soutěže ze 64 algoritmů neprošlo 50, neboť měly zejména nějaké bezpečnostní nevýhody. Problém byl, že do druhého kola prošlo 14 kandidátů, z nichž však pouze 2 algoritmy splňovaly kritérium rychlosti a 2 byly na jeho hraně. V situaci, kterou jsme popsali, bylo však naprosto jasné, že průmysl by jako standard ignoroval funkci, která by byla pomalejší než SHA-2, neboť SHA-2 ignoruje právě proto, že je pomalejší než SHA-1. A teď to hlavní, co zatím nikdo nepochopil. NIST do finále soutěže vybral nikoli ony dva nejrychlejší, ale pět kandidátů, z nichž tři jsou naprostí outsideři a dva jsou oni dva kandidáti „na hraně“. Tímto těžko pochopitelným (asi politicky motivovaným) krokem je bohužel výsledek soutěže již předem určen, nemluvě o porušení pravidel soutěže. Až bude soutěž letos ukončena, bude na stole nějaký algoritmus SHA-3, který bude horší nebo neznatelně lepší než stávající SHA-2. V těch nejvyspělejších technologiích, kde se bude bojovat o každou nanosekundu, ho tedy nebude nikdo používat. Co se zde tedy použije? Jak napovídá název článku, bude to již platný americký federální standard SHA-4 [2].

SHA-4 jako upravená SHA-2

Průmysl nelze ošidit, takže vývojáři brzo zjistili, že stávající funkce z platného standardu SHA-2 lze trochu upravit a vznikne použitelná, rychlá a stále bezpečná hašovací funkce. Jak je to možné? Během čtyř a půl roku soutěže o SHA-3 se totiž zjistilo, že bezpečnostní slabinu SHA-1 za prvé nikdo nedotáhl do konce a za druhé, že potenciální slabiny SHA-2 jsou asi tak nevýznamné jako výhody budoucího vítěze SHA-3. Čili pokud budeme pracovat s fakty a nikoli s pocity, SHA-2 je stejně tak bezpečnostně dobrá, jako bude vítěz SHA-3. Ovšem co udělat s rychlostí SHA-2? Řešení přinesl čas, během kterého se (v důležité části počítačového průmyslu) přešlo z 32bitových procesorů na 64bitové. To přesunulo dříve zcela opomíjenou funkci SHA-512 z rodiny SHA-2 do popředí. Trik spočívá v tom, že tato funkce pracuje s 64bitovými slovy na 64bitových procesorech stejně rychle jako užívaná funkce SHA-256 s 32bitovými slovy na 32bitových procesorech. A pointa je v tom, že díky dvojnásobné šíři slova se za stejný čas, zpracuje dvakrát více dat. Jinými slovy, SHA-512 je pro 64bitové procesory dnes nejrychlejší existující standard, který je přijatelný i pro průmysl. Ovšem je potřeba celá třída funkcí, které dávají otisky o délce t bitů, kde t = 224, 256, 384 a 512 bitů. Proto NIST přišel s jednoduchým řešením. Výstup z SHA-512 se prostě zkrátí z 512 na t bitů! Tím vznikne funkce SHA-512/t pro potřebnou hodnotu t. Vznikla tedy „nová“ třída funkcí, kterou jsme si troufli označit jako SHA-4 podle normy FIPS PUB 180-4 [2], kterou je definována. Nabízí se analogie, že SHA-1 byla definována normou FIPS PUB 180-1, SHA-2 normou FIPS PUB 180-2... nicméně název SHA-4 se asi příliš neujme pro komplikované značení konkrétních funkcí, které se oficiálně označují jako SHA-512/224, SHA-512/256, SHA-512/384 a SHA-512/512.

NIST potvrzuje...

V době psaní článku se konala třetí pracovní konference NIST [3], kde pět kandidátů na SHA-3 mělo poslední příležitost vyzdvihnout své kvality, než NIST za několik měsíců vyhlásí vítěze. Ve stejnou dobu se významní hráči počítačového průmyslu v IETF na druhém konci USA shodli, že SHA-3, ať už zvítězí kdokoliv, nebude mít dvě hlavní zamýšlené vlastnosti a potvrdil to i zástupce NIST tamtéž.

LITERATURA

[1] Klima, V.: Tunnels in Hash Functions: MD5 Collisions Within a Minute, IACR ePrint archive, http://eprint.iacr.org/2006/105.pdf.

[2] FIPS PUB 180-4: Secure Hash Standard (SHS), NIST, March 2012, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

[3] http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/March2012/Program_SHA3_March2012.html.