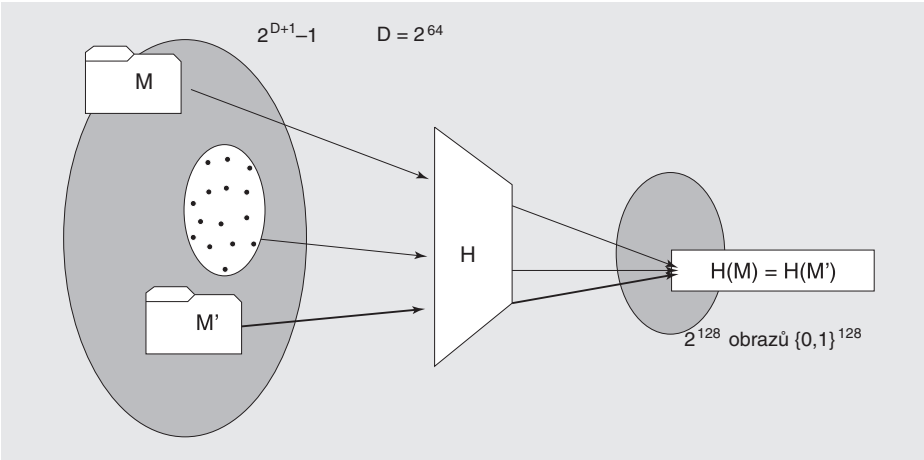
Kryptologie pro praxi – prolomení hašovací funkce MD5 aj.

Letošní srpen přinesl nové objevy v kryptoanalýze, které budou mít vliv na bezpečnostní praxi v sektoru IS/IT. V úvodu si zopakujeme některé pojmy z ST 2/2004 a zároveň si je doplníme o nové souvislosti.

Hašovací funkce h zpracovává prakticky neomezeně dlouhá vstupní data M na výstupní hašový kód $h(M)$, který má předem danou pevnou délku. Například u hašovacích funkcí MD5/SHA-1/SHA-256/SHA-512 je to 128/160/256/512 bitů.



Hašovací funkce musí být jednocestná (one-way) a bezkolizní (collission-free). Jednocestnost znamená, že z M lze jednoduše vypočítat $h(M)$, ale obráceně to není pro náhodně zadaný hašový kód $h(X)$ výpočetně zvládnutelné. Díky tomu lze například v operačních systémech používat a ukládat haše hesel. Bezkoliznost se zase využívá k digitálním podpisům. Nepodepisuje se přímo zpráva, často velmi dlouhá (u MD5/SHA-1/SHA-256 prakticky až do délky $D=2^{64}-1$ bitů), ale pouze její haš. Bezkoliznost požaduje, aby bylo výpočetně nezvládnutelné nalezení libovolných dvou různých (byť naprosto nesmyslných) zpráv M a M' tak, že $h(M)=h(M')$. Pokud se to stane, říkáme, že jsme nalezli kolizi. Protože možných zpráv je mnoho ($1 + 2^1 + ... + 2^D=2^{D+1}-1$) a hašových kódů málo (u MD5 například pouze 2^{128}), musí existovat ohromné množství zpráv, vedoucích na tentýž hašový kód – v průměru řádově 2^{D-127}. Kolize tedy teoreticky existují v hojné míře. Pointa hašovacích funkcí je ale v tom, že díky výpočetní složitosti je nejsme schopni prakticky nalézt. Jakmile proto někdo kolizi nalezne, hašovací funkce ztrácí smysl, neboť hypotéza o její bezkoliznosti byla vyvrácena. Taková funkce by zejména neměla být používána k digitálním podpisům. Tam kolize znamená, že je možné předložit dvě různé zprávy s tímtéž digitálním podpisem, platným pro obě zprávy.

Kolize v teorii a praxi

Při nalezení kolize nějaké hašovací funkce se v praxi můžeme setkat s otázkou, jak „moc" byla funkce prolomena. Jádro odpovědi je v tomto případě v matematické logice, která stojí za argumenty o bezpečnosti toho kterého systému. Tato logika je dvouhodnotová: výrok buď platí, nebo neplatí. Mravenčí matematickou prací se na jednodušších tvrzeních stavějí složitější, až nakonec na vrcholku pyramidy stojí výrok: Tento systém je pravděpodobně bezpečný. Někde v hloubi této konstrukce přitom stojí výrok: Hašovací funkce je bezkolizní. Pokud někdo ukáže, že kolizi našel, pyramida se hroutí společně s výrokem na vrcholu a po formální stránce je z celého schématu pouhá ruina. Je přitom jedno, jestli kolidující zprávy nám jako lidem připadají smysluplné nebo ne. Na druhou stranu zhroucení pyramidy s důkazem bezpečí v jednom konkrétním systému ještě neznamená, že pro jiný systém nemůže vyrůst jiná pyramida, kde nalezení kolizí vyústí v mírné zvýšení reálného rizika nebezpečnosti. Zde většinou bývá jistý časový odstup. Přísně logicky vzato tak lze nějakou chvíli používat i prolomené funkce. Praktické zkušenosti ovšem ukazují, že je to jen poslední večírek na Titaniku.

Kolize ohrožují budoucí digitální podpisy

Nalezení kolizí v létě t. r. ohrožuje zprávy, které teprve „budou podepsány". Například sekretářka předloží řediteli k podpisu nevinně vyhlížející objednávku kancelářských potřeb, která má stejný hašový kód jako nějaká nevýhodná smlouva, datovaná do budoucnosti. Situace se může ještě zhoršit, pokud je prolomena i odolnost proti nalezení druhého vzoru (tzv. second preimage resistance): Pro „dané" M nalézt jiné M' tak, aby $h(M)=h(M')$. Takové oslabení by ohrožovalo i zprávy podepsané v minulosti. Naštěstí je toto ale mnohem silnější druh útoku, ve který se útoky na bezkoliznost nemusí rozvinout. Nicméně i tento aspekt se u napadených funkcí musí sledovat.

Moderní kryptologie chápe hašovací funkce jako pseudonáhodná zobrazení, která se používají zejména v kódech HMAC (viz ST 2/2004), v generátorech pseudonáhodných čísel PRF (ST 12/2003) a při odvozování klíčů. Oslabením pro tyto konstrukce je předložení důkazu, že funkce se nechová podle postulátu pseudonáhodného zobrazení. Svým způsobem se jedná o alternativní model využití hašovací funkce, přičemž prolomení v jednom modelu (jednosměrnost a bezkoliznost) se určitým způsobem může dotýkat i modelu druhého (pseudonáhodné zobrazení) a obráceně. Konkrétní popis vzájemných vazeb je však obvykle velmi komplikovaný, takže zejména v praxi se dopady jednotlivých útoků uvádějí obvykle pro první a druhý model zvlášť.

Nalezeny techniky hledání slabin

Srpen tohoto roku byl velmi špatným měsícem pro hašovací fukce a mimořádným pro kryptoanalytiky, kteří dosáhli minimálně dvou významných vědeckých úspěchů. Za prvé byly definitivně prolomeny hašovací funkce MD4, MD5, RIPEMD a HAVAL-128 [1], neboť byly předloženy jejich kolize. Dále byly nalezeny nové obecnější techniky hledání slabin iterativních hašovacích funkcí [1] až [4], což se dotýká všech důležitých současných hašovacích funkcí. Výsledkem je trochu mrazení v zádech, zda tyto moderní hašovací funkce a zejména převládající SHA-1 ustojí nové techniky a na nich založené útoky. Dobrou zprávou je, že zatím je vše v pořádku, tj. SHA-1 a novější třída funkcí SHA-256, SHA-512, SHA-384 a SHA-224 (souhrnně jsou označovány jako třída SHA-2) zůstávají bezpečné. Další dobrou zprávou je, že funkce HMAC, používající MD5, tj. HMAC-MD5, nemusí být v některých případech vyměňovány a že HMAC v kombinaci s funk-

cemi SHA-1 nebo třídou SHA-2 zůstávají také bezpečné.

HMAC a PRF

Hašovací funkce se používají i ve spojení s tajným klíčem, kde mají v zásadě dva typy použití. První je ve smyslu PRF (pseudonáhodná funkce) a druhé ve smyslu HMAC (hašový autentizační kód zprávy). V prvním případě se pomocí hašovací funkce a klíče generuje větší množství (pseudonáhodných) dat a zde by se prolomené funkce neměly používat (i když není ukázán žádný devastující útok, pouze jsou mírně oslabeny bezpečnostní vlastnosti). U použití typu HMAC se hašovací funkce použije dvakrát, ale s tajným klíčem a produkuje krátký výstup. Zde není známo žádné devastující oslabení funkce autentizačního kódu. Toto vysvětlení je vágní, ale jeho cílem je prvotní zpráva a orientace, nikoli přesnost. O přesné interpretaci výsledků [1] až [4] kryptologové diskutují, protože čínský tým, který kolize předložil [1] nepublikoval svůj postup, ale pouze výsledky. Je to velmi neobvyklé a lze to přičíst tomu, že výsledky chtěli prezentovat v neformálním fóru (jedná se o tzv. rump session) na nejprestižnější kryptologické konferenci Crypto 2004, nestihli plný příspěvek sepsat nebo postup precizují nebo ho nechtějí odhalit z jiného důvodu. Díky chybě, kterou udělali při první publikaci výsledků, však vyplynulo, že jsou schopni nalézat kolize pro různé počáteční hodnoty, s nimiž začíná pracovat hašovací funkce. Odtud pak plyne mírné oslabení vlastností HMAC jako PRF.

Nalezeny velké množiny kolizí

Číňané [1] předvedli, že umí najít velkou třídu kolizí u hašovacích funkcí MD4, MD5, RIPEMD a HAVAL-128 s časovou náročností od sekund po 1–2 hodiny. Joux [3] na tomtéž fóru prezentoval kolize u SHA-0. Tým Biham-Chen [2], [4] a Hawkes-Paddon-Rose představili úvahy a techniky zkoumání moderních hašovacích funkcí typu SHA-1,2. Poznamenejme ještě, že (jedna) kolize MD4 (a to ještě poměrně pracně) byla nalezena Dobbertinem v roce 1996. Tehdy to vzbudilo velký rozruch a od MD4 se rychle upustilo. Dnes to Číňanům trvá u MD4 a MD5 pár sekund až hodin a nalezenou kolizí celou řadu. Co tedy s tím? V současné době jsou nejpoužívanějšími SHA-1 a MD5. U MD5 byla v roce 1996 nalezena slabina (kolize v kompresní funkci) a společností RSA bylo doporučeno ji přestat používat. Bohužel MD5 zakořenila do mnoha systémů, takže díky tomu, že nebyla nalezena úplná kolize, bezpečnostní architekti ji v mnoha systémech ponechali, aniž by si nechali zadní vrátka k výměně. V některých systémech tak bude těžké ji nahradit. Prodlužování klinické smrti MD5 se nyní tedy vymstilo.

SHA-0 byla krátkou dobu oficiálním standardem, ale byla rychle nahrazena SHA-1, proto by její odpis neměl být problémem. RIPEMD a HAVAL se příliš neujaly (RIPEMD byl nahrazen bezpečnějším RIPEMD-160), takže předvedení kolizí je pouze demonstrací síly čínského útoku. U SHA-1 byly předvedeny některé techniky, které ji více prozkoumávají, ale nesnižují její bezpečnost [2], [3], [4].

Umí Číňané prolomit i SHA-1?

Z publikovaných příspěvků vyplynula určitá nervozita, zda tato odhalení nějak nenarušují bezpečnost systémů, používajících SHA-1. Dobrá zpráva je, že nikoli, ale to mrazení v zádech by mělo všechny dostatečně poučit. Co kdyby to vliv mělo? Hašovací funkce nové třídy SHA-2 jsou použity zatím jen minimálně, protože jsou poměrně nové, spoléhá se na bezpečnost SHA-1 a není ochota příliš věci měnit.

Nový vzor chování při používání kryptografických technik

Poučení tedy je, že je nutné se na průšvihy tohoto typu připravit jako na reálné jevy, tak jako se reálně u složitých programů vydávají záplaty. Nové paradigma by mělo být nedůvěřovat slepě jen jedné funkci, ale systémy budovat tak, aby se kryptografické nástroje v nich mohly pružně měnit. Bezpečnost není konstantní, je to komplikovaná veličina, která se postupem času vyvíjí. Proto ji ošetřujeme procesem řízení rizika, který bezpečnost monitoruje a včas provádí příslušné korekce. Tuhle poučku sice každý zná a v některých oblastech se už i rutinně uplatňuje, v oblasti používání kryptografických nástrojů ale jako by všichni ztuhli.

Přejděte na SHA-2

Americký standardizační úřad NIST, který za standardy hašovacích funkcí odpovídá, vydal prohlášení k současným výsledkům na http://csrc.ncsl.nist.gov/hash_standards_comments.pdf, z něhož vyjímáme:

- SHA-1 zůstává bezpečná,
- doporučuje se používat třídu funkcí SHA-2,
- do roku 2010 se předpokládá opuštění i SHA-1 a přechod na SHA-2.

MD5CRACK zastaven

Možná nevíte, že o nalezení kolizí se hrubou silou pokoušel i projekt MD5CRACK na http://www.md5crk.com/, kde Češi patřili k významným přispěvatelům strojového času. Cílem bylo najít kolizi MD5 hrubou silou a přesvědčit tak bezpečnostní architekty, aby od ní konečně ustoupili. Jakmile byl publikován čínský výsledek, projekt byl pochopitelně zastaven. Číňani ukázali, že geniální nápad skály proráží.

Další informace, definice funkcí, příklady kolidujících zpráv, literaturu apod. naleznete na [5] a na domácí stránce, věnované kolizím hašovacích funkcí http://cryptography.hyperlink.cz/kolize_hash.htm.

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

LITERATURA

[1] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu: Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Crypto 2004 Rump Session, http://eprint.iacr.org/2004/199.pdf

[2] Eli Biham, Rafi Chen: Near Collisions of SHA-0, Crypto 2004

[3] Antoine Joux: Collisions in SHA-0, Crypto 2004 Rump Session

[4] Eli Biham, Rafi Chen: New results on SHA-0 and SHA-1, Crypto 2004 Rump Session

[5] V. Klíma: Symetrická kryptografie I a III., MFF UK, http://adela.karlin.mff.cuni.cz/~tuma/nciphers.html

[6] HYPERLINKHYPERLINK el. archivy článků autorů: http://cryptography.hyperlink.cz/ a http://crypto.hyperlink.cz/