Crypto-World

Informační sešit GCUCMP

Ročník 7, číslo 3/2005 **15. březen 2005**

3/2005

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(820 registrovaných odběratelů)

Obsah :

Co se stalo s hašovacími funkcemi?

aneb přehled událostí z poslední doby, část 1

Vlastimil Klíma , http://cryptography.hyperlink.cz , v.klima@volny.cz

Abstrakt

Z praktického hlediska se loučíme s hašovací funkcí MD5. Z teoretického, a pro mnohé i z praktického hlediska, se loučíme s hašovací funkcí SHA-1. Jako poslední prakticky bezpečné hašovací funkce zůstávají ty ve třídě SHA-2 (funkce SHA-256/384/512/224). Hledá se nový koncept hašovacích funkcí, neboť ani třída SHA-2 nemá ty teoretické vlastnosti, které bychom si u kvalitní hašovací funkce představovali.

I. Blok, týkající se zejména MD5

Od srpna 2004 do března 2005 se toho v oblasti hašovacích funkcí událo tolik, že stanovisko k jejich bezpečnosti musela řada lidí dvakrát přehodnotit. Události si stručně připomeneme a okomentujeme. Pro hlubší studium uvádíme odkazy na literaturu. Uvádíme pouze práce stěžejní, neboť se zaměřujeme na praktické dopady.

[WFLY04] X. Wang, D. Feng, X. Lai, H. Yu, "**Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD**", rump session, CRYPTO 2004, *Cryptology ePrint Archive*, Report 2004/199, http://eprint.iacr.org/2004/199

Tým profesorky Wangové prezentoval 16. 8. a 17. 8. 2004 na rump session konference Crypto 2004 datové kolize pro hašovací funkce MD4, MD5, HAVAL-128 a RIPEMD. Oznámil také schopnost generovat kolize pro libovolný inicializační vektor MD5 a kolizi MD5 během hodiny a čtvrt na velkém počítači IBM p690. Kolize pro MD4 dokázali najít se složitostí odpovídající ručnímu výpočtu. To bylo obzvláště frustrující, neboť kolize MD4, získaná Dobbertinem v roce 1996 byla jediná známá "opravdová" kolize, a bylo k ní nábožně vzhlíženo.

Čínský tým ovšem nepublikoval myšlenky, jak kolize získávat, pouze strohá data. Pozn.: Protože funkce MD5 je z uvedených nejdůležitější, budeme práci dále zmiňovat pouze v souvislosti s MD5.

[HPR04] Philip Hawkes, Michael Paddon, Gregory G. Rose: **Musings on the Wang et al. MD5 Collision**, *Cryptology ePrint Archive*, Report 2004/264, 13 October 2004, http://eprint.iacr.org/2004/264.pdf

V této práci se v říjnu 2004 australský tým pokusil čínskou metodu zrekonstruovat pouze na základě zveřejněných kolizí. Nejdůležitější "čínský trik" se nepodařilo objevit, ale na základě dat z [WFLY04] bylo dobře popsáno diferenční schéma, kterým uveřejněné čínské kolize vyhovují. Naplnění podmínek tohoto schématu bylo však ještě příliš náročné a výpočetně složitější, než ukazovaly výsledky z [WFLY04], a tak práce nepřinesla čistě praktické výsledky.

[OM2004] Ondrej Mikle: **Practical Attacks on Digital Signatures Using MD5 Message Digest**, *Cryptology ePrint Archive*, Report 2004/356, http://eprint.iacr.org/2004/356, 2nd December 2004, http://cryptography.hyperlink.cz/2004/collisions.htm

[DK2004] Dan Kaminsky: **MD5 To Be Considered Harmful Someday**, *Cryptology ePrint Archive*, Report 2004/357, http://eprint.iacr.org/2004/357, 6 December 2004

V těchto dvou pracích z prosince 2004 bylo ukázáno, jak lze využít nikoli schopnost generovat kolize, ale pouhou jednu jedinou datovou kolizi MD5, publikovanou výše, ke konstrukci sofistikovaných útoků. Zejména v práci [OM2004] jsou ukázány velké možnosti. Podle ní lze v konečném důsledku určitým postupem docílit toho, že libovolné dva různé, útočníkem volené soubory, se uživatelům jeví jako naprosto shodné, a to prostřednictvím kontroly haše a digitálního podpisu.

[LWW05] Arjen Lenstra, Xiaoyun Wang and Benne de Weger: **Colliding X.509 Certificates**, *Cryptology ePrint Archive*, Report 2005/067, http://eprint.iacr.org/2005/067

Prvního března 2005 bylo uveřejněno další sofistikované využití kolize MD5, tentokrát pro zvolenou inicializační hodnotu. Prof. Wangové stačilo k účasti na tomto projektu jenom jediné. Do svého programu zadat inicializační hodnotu, poskytnutou zbývajícími dvěma autory. Výsledkem jsou dva různé moduly n kryptosystému RSA, které vedou na stejný otisk a tedy po vložení do příslušného pole certifikátu má celý certifikát stejný digitální podpis příslušné certifikační autority. Byla tím ukázána možnost vytvořit k vydanému certifikátu jiný, který příslušná certifikační autorita ve skutečnosti nevydala….

[VK2005] Vlastimil Klima: **Finding MD5 Collisions – a Toy For a Notebook**, *Cryptology ePrint Archive*, Report 2005/075, http://eprint.iacr.org/2005/075, (v češtině "Nalézání kolizí MD5 - hračka pro notebook", http://cryptography.hyperlink.cz/md5/MD5_kolize.pdf.)

Pátého března jsem oznámil, že dokážu generovat kolize MD5 na domácím počítači, a to stejně jako [WFLY04] pro libovolnou inicializační hodnotu. Od této doby je možné nikoli na velkém počítači s 32 procesory, ale i na notebooku generovat libovolné kolize. Metoda, kterou jsem použil (před publikací čínského postupu), se ukazovala jiná v obou fázích postupu, než u [WFLY04]. V první fázi byla 1000 - 2000 krát rychlejší, v druhé 2 - 80 krát pomalejší a celkově 3 - 6 krát rychlejší. Průměrná doba nalezení kolize na notebooku (Pentium 1.6 GHz) je tak 8 hodin. Čínská metoda ještě nebyla v té době publikována. Proto jsem se k podobnému kroku nechystal ani já.

[WY2005] Xiaoyun Wang and Hongbo Yu: **How to Break MD5 and Other Hash Functions**, http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf.

Profesorka Wangová umístila tento příspěvek na svůj web jak se ukázalo (po mírně detektivním zkoumání, které jsme vedli s Pavlem Vondruškou, viz http://www.crypto-world.info/news/index.php?prispevek=1245) velmi v tichosti někdy v období prvního týdne března. Tato událost, na kterou kryptografická komunita čekala půl roku, tak získala další tajemný přídech. Proběhlo to v tichosti a nenápadně. Bylo to zřejmě tak, že jakmile se prof. Wangová dozvěděla, že její příspěvek byl přijat na konferenci Eurocrypt 2005, dala ho k ostatním pracem na své internetové stránky a nechala to osudu. První to našel nějaký člověk, který si přečetl můj článek [VK2005], pak dal vyhledávat "Wang" a to ho dovedlo až k jejímu článku. Byl schován v čínských znacích, ale anglický název prominoval. Tak jsem se to dozvěděl i já (záznam viz newsgroup sci.crypt). Pak jsme se tomu s Pavlem Vondruškou chvíli věnovali, kdy to tam asi dala a výsledek je výše. Informace o tom je také například na http://www.root.cz/zpravicky/cinsti-vedci-promluvili/ s mým komentářem.

Konečně bylo možné vidět onen čínský trik. Ukázalo se, že jsou dva, a to diferenční schéma a tzv. metoda modifikace zpráv. Jak diferenční schéma funguje, bylo v zásadě prozkoumáno Australany (Číňané se liší v několika překvapivých detailech), ale jak bylo vytvořeno, zůstává stále v čínském šuplíčku. Pouze je poznamenáno, že vzniklo tak, aby bylo výhodné pro pozdější fáze schématu. U metody modifikace zpráv dává tento příspěvek jeden příklad. Dále se uvádí, že k hledání jsou použity i jiné modifikace zpráv. Jinými slovy, metoda zůstala velice zahalena do technických detailů, neboť uvedený příklad nelze nijak obecně využít.

Pokračování výzkumu z [VK2005]
V současné době pracujeme na využití některých myšlenek z [WY2005] pro ještě větší urychlení, dosažené v [VK2005]. Potvrdilo se také, že oba přístupy jsou nikoli diametrálně, ale přesto odlišné.

Tento proud novinek týkajících se hašovací funkce MD5 zatím uzavíráme s tím, že nikdo už nepochybuje o zastaralosti této funkce. Bude ale velmi těžké ji nahradit v existujících aplikacích. Pokračujeme v přehledu s SHA-1.

II. Blok, týkající se zejména SHA-1

[WYY05] Wang X., Yin L., Yu H.: **Collision Search Attacks on SHA1**, February 13, 2005, http://theory.lcs.mit.edu/~yiqun/shanote.pdf

V této práci ukazují plnou kolizi SHA-0 a kolizi SHA-1 pro 58 kroků (z 80). Oznamují též, že jsou schopni nalézt kolizi plnohodnotné SHA-1 se složitostí 2^{69} hašovacích operací. SHA-0 by pokořili se složitostí 2^{33} hašovacích operací. Pokud si uvědomíme, že SHA-0 byla určitou dobu standardem, a že se liší od SHA-1 pouze v jedné operaci v základní smyčce, je to ohromný výsledek.

[LWW05b] Arjen Lenstra, Xiaoyun Wang and Benne de Weger: **Colliding X.509 Certificates based on SHA1-collisions**,
http://www.win.tue.nl/~bdeweger/CollidingCertificates/index.html

Tým Lenstra-Wang-Weger připravuje v těchto dnech spuštění experimentu na nalezení kolize certifikátu, podobně jako v [LWW05], tentokrát ale pro hašovací funkci SHA-1 v certifikátu. To už je velmi závažné, protože většina certifikačních autorit tuto funkci používá, a to jako silnější alternativu k MD5. Scénář je stejný jako předtím. Připraví se dva klíče, vypočte se inicializační hodnota pro kolizi SHA-1, Wangová poskytne kolizi a zbytek je stejný jako předtím. Zbývá generovat kolizi SHA-1. Před měsícem oznámená složitost 2^{69} se ale pravděpodobně podaří snížit na 2^{66}. Pracuje se již jen na získání výpočetního výkonu.

Tím přehled pro tentokrát uzavíráme.