Crypto-World

Informační sešit GCUCMP

Ročník 7, číslo 4/2005 **15. duben 2005**

4/2005

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

Obsah : **str.**

Příloha (PR) : sina.pdf
J.Strelec (Secunet) : SINA - BEZPEČNÁ KOMUNIKAČNÍ INFRASTRUKTURA

A. Co se stalo s hašovacími funkcemi?
aneb přehled událostí z poslední doby, část 2

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

Vlastimil Klíma:
"SHA-1 bude do roka prolomena."

Odpověď na dotaz posluchače na semináři
Cryptofest, Praha, 19.3.2005:
Kolik dáváte času SHA-1?

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.

III. Blok, týkající se iterativních hašovacích funkcí

V tomto bloku ukážeme, že základ všech moderních hašovacích funkcí - iterativní princip - je teoreticky špatný. Odhalení, která přinesly dvě hlavní práce v minulém roce, ukazují, že iterativní hašovací funkce jsou postaveny na špatném teoretickém základě, který oddaluje tyto funkce od žádoucích náhodných vlastností (od náhodného orákula). Nezbytné pojmy a fakta jsme umístili do dodatku. Jeho text vychází z přednášky [VK2005c], kde naleznete širší výklad k hašovacím funkcím. Nyní uvedeme hodnocení a závěry z obou klíčových prací.

1. Generické problémy iterativních hašovacích funkcí

Generické problémy hašovacích funkcí ukazují dvě práce. První představil Joux [Joux04] na konferenci Crypto v srpnu 2004 a druhý Kelsey-Schneier [KS2004] v listopadu 2004. Obě dvě práce ukazují, že iterativní konstrukce hašovací funkce implikuje značnou odlišnost této funkce od náhodného orákula.

[Joux04b] A. Joux: Multicollisions in iterated hash functions. Application to cascaded constructions. Proceedings of Crypto 2004, LNCS 3152, pages 306-316.
Joux ukazuje, že

1) u iterativních hašovacích funkcí lze docílit **mnohonásobné kolize** mnohem jednodušeji než ve srovnání s náhodným orákulem
2) **kaskádovitá konstrukce** F || G pomocí dvou hašovacích funkcí pozbývá smyslu, neboť očekávaná složitost nalezení kolize není součinem dílčích složitostí, ale spíše součtem

Poznamenejme, že kaskádovitou konstrukci používají někteří architekti k tomu, aby ze dvou slabších funkcí vytvořili silnější nebo aby ze dvou nezávislých hašovacích funkcí s kratším hašovým kódem vytvořili silnější hašovací funkci s dvojnásobně dlouhým hašovacím kódem, a tedy poskytující neporovnatelně vyšší bezpečnost.

Intuitivně se totiž očekávalo, že složením hašovacího kódu funkce F o délce n_f bitů a hašovacího kódu funkce G o délce kódu n_g bitů vznikne kvalitní hašovací funkce F || G o délce kódu $n_f + n_g$ a složitost nalezení kolize bude tak $2^{(nf+ng)/2}$. Joux ukázal, že místo toho je to mnohem méně, a to $n_g/2 * 2^{nf/2} + 2^{ng/2}$, tedy řádově stále číslo $2^{ng/2}$ nebo $2^{nf/2}$.
Pokud se týká mnohonásobné kolize, jedná se spíše o teoretickou záležitost, ukazující, že hašovací funkce se výrazně odlišuje od náhodného orákula.

[KS2004] John Kelsey, Bruce Schneier: Second Preimages on n-bit Hash Functions for Much Less than 2^n Work, http://eprint.iacr.org/2004/304/, November 15, 2004
Kelsey-Schneierova práce

1) obsahuje výrazně zlepšenou metodu konstrukce multikolizí oproti Jouxovi,
2) **umožňuje konstruovat druhý vzor zprávy** u iterativních hašovacích funkcí se složitostí cca $2*2^{n/2} + 2^{n-k+1}$ pro velmi dlouhé zprávy o délce 2^k blízké $2^{n/2}$.

Konkrétně pro SHA-1 lze ke zprávě o délce 2^{60} bajtů vytvořit druhý vzor se složitostí 2^{106} na rozdíl od teoretické složitosti 2^{160}.

Kelsey-Schneierova práce je velmi významná teoreticky (zejména bod 1), ale má i praktické důsledky (bod 2). Dnes je sice složitost 2^{106} možno považovat za výpočetně nedosažitelnou, ale je to první práce, která umožňuje nalézt druhý vzor zprávy. Připomeneme-li si slova NSA "tyto útoky se mohou pouze zlepšovat", můžeme v budoucnu očekávat snížení této hranice. Pokud by se snížila pod únosnou mez, byl by to největší průlom v oblasti hašovacích funkcí. Zopakujme, že nalezení druhého vzoru zprávy pro hašovací funkci s délkou kódu n bitů má mít teoretickou složitost 2^n, oproti složitosti $2^{n/2}$ pro nalezení kolize. Jsou to tedy neporovnatelně rozdílné úlohy a zde bylo předloženo řešení, které není daleko od hranice bezpečnosti.

Závěr k novým zjištěním kryptoanalýzy iterativních hašovacích funkcí

Řada předních kryptologů se shoduje v tom, že je nutno zahájit práce na veřejné mezinárodní soutěži na nový koncept hašovacích funkcí, neboť iterativní funkce nesplňují požadované bezpečnostní vlastnosti.
Uvedené odhalené vlastnosti jsou teoretického rázu, ale jednoho dne by se mohly projevit zcela prakticky. Proto je nezbytná změna konceptu.

2. NIST doporučuje přechod na SHA-2 do r. 2010

Americký standardizační úřad NIST, který za standardy hašovacích funkcí odpovídá, vydal **25. 8. 2004** prohlášení k tehdejším výsledkům na [NIST05a], z něhož vyjímáme:

- Doporučuje se používat třídu funkcí SHA-2.
- Do roku 2010 se předpokládá opuštění i SHA-1 a přechod na SHA-2.

Po oznámení možnosti nalézt kolizi SHA-1 za 2^{69} operací NIST **23. 2. 2005** svoje dřívější stanovisko ještě více podtrhl [NIST05b].

3. Třída hašovacích funkcí SHA-2 (SHA-256, 384, 512 a 224)

Z důvodu zvýšení odolnosti vůči kolizím je od 1. února 2003 k dispozici nová trojice hašovacích funkcí SHA-256, SHA-384 a SHA-512 [SHA-2] a od února 2004 SHA-224 (dodatek [SHA-2]). Tyto funkce přichází se zvýšením délky hašového kódu na 256, 384 a 512 bitů (SHA-224 má 224 bitový hašový kód), což odpovídá složitosti 2^{128}, 2^{192} a 2^{256} pro nalezení kolizí narozeninovým paradoxem. To je jednak už dost vysoká složitost a také to odpovídá složitosti útoku hrubou silou na tři délky klíčů, které nabízí standard AES.
Pokud se týká konstrukce nových funkcí, jsou velmi podobné SHA-1 a používají stejné principy, pracují však se složitějšími funkcemi a širšími vstupy. Podrobnosti lze nalézt v uvedených standardech. Jejich cílem bylo poskytnout větší odolnost proti kolizi a nabídnout odpovídající bezpečnost jako klíče pro AES.

Tyto funkce jsou iterativního charakteru, takže mají teoretické nedostatky, zmíněné výše. Proto by bylo vhodné přejít na jiný koncept konstrukce.

4. Hodnotící práce

[HOSCH05] P. Hoffman, B. Schneier: **Attacks on Cryptographic Hashes in Internet Protocols**, Internet-Draft, March 25, 2005, http://www.ietf.org/internet-drafts/draft-hoffman-hash-attacks-00.txt
Dokument *sumarizuje vše, co je známo o útocích* na hašovací funkce a týká se internetových protokolů, takže jeho platnost je ve skutečnosti všeobecná. Zároveň konstatuje, že existuje všeobecná neshoda v tom, co z toho vyplývá a jak reagovat. Dokonce se konstatuje, že i autoři tohoto internetového dokumentu mají odlišný názor na to, jak reagovat na současné útoky. Nicméně se shodují v tom, že migrace na SHA-256 není rozhodně na škodu plus že aplikace by měly být připraveny na použití hašovacích funkcí s delším kódem. Pokud tyto vlastnosti nemají, měly by být brzo opraveny. Bruce Schneier k tomu dodává úsloví, které se traduje v NSA: *Útoky se pouze vylepšují, nikdy nezhoršují.* A dále říká: *současné kolize MD5 se dají najít na jednom počítači, útoky proti SHA-1 jsou zatím za horizontem, ale budou se pouze zlepšovat. Délka 256 bitů SHA-256 nám dá mnohem větší bezpečnostní polštář v případě objevení eventuelních dalších útoků. Během několika dalších let by pak kryptografická komunita měla dát zlepšené návrhy konstrukce hašovacích funkcí.*

Poznámka. Schneier zde cituje práci [VK2005a], která má však už aktualizaci i s popisem metody hledání kolizí [VK2005b].

[EU05] Katholieke Universiteit Leuven: **Recent Collision Attacks on Hash Functions**, ECRYPT Position Paper, kontraktor (autor dokumentu): Katholieke Universiteit Leuven, 17. February 2005, Revision 1.1
http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf
Stručný závěr: Kde je to možné, přejít na SHA-2 nebo Whirlpool, funkce MD5 a SHA-1 používat pouze tam, kde nevadí narušení vlastnosti bezkoliznosti, tedy nepoužívat v digitálních podpisech. V kódech HMAC je možné MD5 a SHA-1 používat. Jedná se o shrnující práci projektu EU ECRYPT.

[LE05] Arjen K. Lenstra: **Further progress in hashing cryptanalysis**,
February 26, 2005, http://cm.bell-labs.com/who/akl/hash.pdf
Stručný závěr: Nepoužívat MD5 pro potřeby certifikátů. Nové produkty by měly používat SHA-2. Existující systémy používající MD5 nebo SHA-1 jsou ohroženy, pokud se spoléhají na vlastnost bezkoliznosti. Nejsou zatím ohroženy ty systémy, kde by jejich narušení požadovalo konstrukci druhého vzoru.

[VK2005c] Vlastimil Klíma: **Hašovací funkce, principy, příklady a kolize**, přednáška na semináři Cryptofest, http://www.cryptofest.cz/, Praha, 19. 3. 2005, http://cryptography.hyperlink.cz/2005/cryptofest_2005.htm.
Stručný závěr a doporučení z této práce jsou uvedeny dále.

5. Které techniky jsou a které nejsou bezpečné

- Prolomené hašovací funkce by se neměly používat tam, kde se jedná o nepopiratelnost, tedy u digitálních podpisů. Neměly by se používat tam, kde je důležitá vlastnost bezkoliznosti, kde útočník může využít náhodné kolize.
- **Klíčované hašové autentizační kódy zpráv HMAC ani pseudonáhodné funkce PRF a pseudonáhodné generátory PRNG, které používají hašovací funkce jako nástroje, zatím nejsou současnou kryptoanalýzou dotčeny**. (Pojmy PRNG, PRF a HMAC viz například kapitoly 9 - 11 [VK2005c]).
- Je tu ale možné riziko pramenící z toho, že máme jen velmi málo informací o technikách prolomení současných hašovacích funkcí a že lze v této oblasti očekávat pokrok. To je hrozba, kterou si každý musí ohodnotit.
- Dále víme, že iterativní konstrukce hašovací funkce vede k rozporu s vlastnostmi náhodného orákula. To může časem také přinést nová odhalení vlivu této konstrukce na kvalitu PRNG s těmito hašovacími funkcemi.

6. Doporučení

- Je vhodné provést revizi všech aplikací, kde jsou použity hašovací funkce MD4, MD5, SHA-0, RIPEMD a HAVAL-128.
- Je-li některá z těchto funkcí použita pro účely digitálních podpisů (s klasickým účelem zajištění nepopiratelnosti), je nutno tuto funkci nahradit.
- U funkce SHA-1 je nutné ji nahradit nebo zvážit riziko jejího ponechání v každé aplikaci. Jde zejména o možnost vzniku škody "zpětně", tj. argumentací v budoucnu, kdy by byla SHA-1 prolomena, že mohla být prolomena již teď, tj. v minulosti.
- Podle okolností provést náhradu za některou z funkcí SHA-2, které jsou zatím považovány za bezpečné (SHA-256, SHA-384 nebo SHA-512, nejlépe SHA-512 [SHA-1,2]).
- Je-li některá z prolomených hašovacích funkcí použita pro účely HMAC, PRF nebo PRNG, individuálně posoudit, zda je toto užití bezpečné nebo ne.

7. Dodatek

Tento dodatek obsahuje některé pojmy a informace tvořící základ pro závěry uvedené v předchozí části. Text vychází z přednášky [VK2005c], kde naleznete širší výklad k hašovacím funkcím. Na stránce věnované kolizím hašovacích funkcí http://cryptography.hyperlink.cz/2004/kolize_hash.htm naleznete také další literaturu v češtině i v angličtině vztahující se ke konkrétním hašovacím funkcím a technikám.

Orákulum a náhodné orákulum

Orákulum nazýváme libovolný stroj (stroj "podivuhodných vlastností"), který na základě vstupu odpovídá nějakým výstupem. Má pouze vlastnost, že na tentýž vstup odpovídá tímtéž výstupem. Náhodné orákulum je orákulum, které na nový vstup odpovídá náhodným výběrem výstupu z množiny možných výstupů.

Hašovací funkce jako náhodné orákulum

Z hlediska bezpečnosti bychom byli rádi, kdyby se hašovací funkce chovala jako náhodné orákulum. Odtud se odvozují bezpečnostní vlastnosti.

Bezpečnost z hlediska nalezení vzoru, prolomení hašovací funkce poprvé

Pokud se bude hašovací funkce $f: \{0,1\}^D \rightarrow \{0,1\}^n$ chovat jako náhodné orákulum, bude složitost nalezení vzoru k danému hašovacímu kódu rovna 2^n.
Pokud je nalezena cesta, jak vzory nalézat jednodušeji, hovoříme o prolomení hašovací funkce.

Složitost nalezení kolize

Jestliže kolize zákonitě existují, položme si otázku, jak velká musí být množina náhodných zpráv, aby v ní s nezanedbatelnou pravděpodobností existovaly dvě různé zprávy se stejnou haší. Narozeninový paradox říká, že pro n-bitovou hašovací funkci nastává kolize s cca 50% pravděpodobností v množině $2^{n/2}$ zpráv, namísto očekávaných $1/2 * 2^n$. Například pro 160bitový hašový kód bychom očekávali $1/2 * 2^{160}$ zpráv, paradoxně je to pouhých 2^{80} zpráv.

Tvrzení (narozeninový paradox)

Mějme množinu M m různých koulí a proveďme výběr k koulí po jedné s vracením do množiny M. Potom pravděpodobnost, že vybereme některou kouli dvakrát nebo vícekrát je $P(m, k) = 1 - m(m-1)...(m - k + 1)/m^k$. Pro $k = O(m^{1/2})$ a m velké je $P(m, k) \approx 1 - \exp(-k^2/2m)$.

Důsledek

Pro m velké se ve výběru $k = (2m * \ln_e 2)^{1/2} \approx m^{1/2}$ prvků z M s cca 50% pravděpodobností naleznou dva prvky shodné.

Paradoxnost.

Běžně by člověk uvažoval následovně. Máme množinu m prvků, vezmeme si jeden prvek a hledáme k němu druhý. Abychom dostali pravděpodobnost 1/2, musíme vytahat asi polovinu množiny M, tj. m/2 prvků. Místo toho ale postačí odmocnina z m prvků.

Máme P(365, 23) = 0.507. Pro čísla m = 365 a k = 23 interpretujeme tvrzení tak, že skupina 23 náhodně vybraných lidí postačí k tomu, aby se mezi nimi s cca 50%

pravděpodobností našla dvojice, slavící narozeniny tentýž den. U skupiny 30 lidí je pravděpodobnost už P(365, 30)= 0.706.

Tvrzení se zdá paradoxní protože, ač je vyřčeno jinak, obvykle ho vnímáme ve smyslu "kolik lidí je potřeba, aby se k danému člověku našel jiný, slavící narozeniny ve stejný den". V této podbízející se interpretaci hledáme jedny konkrétní narozeniny, nikoli "jakékoliv shodné" narozeniny. Oba přístupy odráží přesně rozdíl mezi kolizí prvního řádu (libovolní dva lidé) a druhého řádu (nalezení druhého člověka k danému).

Multikolize

Multikolizí (r-násobnou kolizí, r-cestnou kolizí) nazýváme r-tici různých zpráv vedoucích na stejnou haš.

r-násobná kolize u náhodného orákula

K tomu, abychom mezi odpověďmi náhodného orákula na N různých dotazů nalezli jednu odpověď r-krát (r-násobnou kolizi), postačí s dostatečnou nenulovou pravděpodobností $N = 2^{n*(r - 1)/r}$ dotazů, což je pro větší r přibližně 2^n. Pro r = 2 dostáváme známý narozeninový paradox a složitost $2^{n/2}$. Pojmem r-násobné kolize se poprvé zabýval Merkle na konferenci Crypto 1989.

Bezpečnost z hlediska nalezení kolize, prolomení hašovací funkce podruhé

Pokud se hašovací funkce $f: \{0,1\}^D \rightarrow \{0,1\}^n$ bude chovat jako náhodné orákulum, bude složitost nalezení kolize rovna přibližně $2^{n/2}$ a složitost nalezení r-násobné multikolize přibližně $2^{n*(r - 1)/r}$.

Pokud je nalezena cesta, jak kolize nalézat jednodušeji, hovoříme o prolomení hašovací funkce.

Prakticky používané hašovací funkce nejsou prokazatelně bezpečné

I když uvidíme, že vytváření hašovacích kódů je opravdu neskutečně složité, nalezení kolizí je přesto pouze otázkou intelektuální výzvy, neboť u prakticky používaných hašovacích funkcí není prokázána výpočetní složitost nalezení kolize nebo druhého vzoru. Jejich bezpečnost tak u obou vlastností (jednosměrnost, bezkoliznost) závisí pouze na stavu vědy v oblasti kryptografie a kryptoanalýzy.

Prolomení některých kryptografických technik je proto přirozeným a průvodním jevem rozvoje poznání v této oblasti.

Když je nalezena kolize

Hašovací funkce, u níž byla nalezena kolize, ztrácí generálně smysl, neboť hypotéza o tom, že se chová jako náhodné orákulum byla vyvrácena. Zejména by neměla být používána k digitálním podpisům, neboť tam kolize znamená, že je možné předložit dvě různé zprávy s tímtéž platným digitálním podpisem, platným pro obě zprávy. Existují ale techniky, kde nejsou využity všechny vlastnosti hašovací funkce a kde porušení bezkoliznosti (nebo částečné porušení bezkoliznosti) nevadí (PRNG, PRF, HMAC).

Generické problémy iterativních hašovacích funkcí

Generické problémy hašovacích funkcí ukazují dvě práce. První představil Joux [Joux04] na konferenci Crypto v srpnu 2004 a druhý Kelsey-Schneier [KS2004] v listopadu 2004. Obě dvě práce ukazují, že iterativní konstrukce hašovací funkce implikuje značnou odlišnost této funkce od náhodného orákula.

[Joux04b] A. Joux: Multicollisions in iterated hash functions. Application to cascaded constructions. Proceedings of Crypto 2004, LNCS 3152, pages 306-316.
[KS2004] John Kelsey, Bruce Schneier: Second Preimages on n-bit Hash Functions for Much Less than 2^n Work, http://eprint.iacr.org/2004/304/, November 15, 2004
Joux ukazuje, že

1) u iterativních hašovacích funkcí lze docílit **mnohonásobné kolize** mnohem jednodušeji, než ve srovnání s náhodným orákulem
2) **kaskádovitá konstrukce** F || G pomocí dvou hašovacích funkcí pozbývá smyslu, neboť očekávaná složitost nalezení kolize není součinem dílčích složitostí, ale spíše součtem

Kelsey-Schneierova práce

1) obsahuje výrazně zlepšenou metodu konstrukce multikolizí oproti Jouxovi,
2) **umožňuje konstruovat druhý vzor zprávy** u iterativních hašovacích funkcí se složitostí cca $2*2^{n/2} + 2^{n-k+1}$ pro velmi dlouhé zprávy o délce 2^k blízké $2^{n/2}$.

Konkrétně pro SHA1 lze ke zprávě o délce 2^{60} bajtů vytvořit druhý vzor se složitostí 2^{106} na rozdíl od teoretické složitosti 2^{160}.

r-násobné kolize pro iterativní hašovací funkce lze docílit s nižší složitostí

Joux [Joux04b] ukázal, že u iterativních hašovacích funkcí lze r-násobnou kolizi najít se složitostí $\ln_2 r * 2^{n/2}$ namísto $2^{n*(r-1)/r}$.
Postup. Vyjdeme ze standardní hodnoty IV, H_0 = IV, se složitostí S(F) najdeme kolizi hašovací funkce F s inicializační hodnotou H_0 (zprávy $M_{1,1}$ a $M_{1,2}$). Výslednou haš označme H_1. Se složitostí S(F) nalezneme kolizi F s inicializační hodnotou H_1 (zprávy $M_{2,1}$ a $M_{2,2}$), výslednou haš označíme H_2. Takto uděláme N kroků pro N = $\ln_2 r$. Nyní můžeme sestavit 2^N = r zpráv majících tutéž haš H_N a to tak, že z každé dvojice bloků $M_{i,1}$ a $M_{i,2}$ vybereme vždy jednu z nich. Dostaneme tak 2^N zpráv, které prochází stejnými hašovacími mezivýsledky a končí stejným hašovacím kódem H_N.

Kaskádovitá konstrukce pozbývá smyslu

Druhou vlastností, kterou Joux [Joux04b] odhalil, je, že složení hašovacích funkcí F a G (kaskáda), F||G (|| označuje zřetězení) neposkytuje intuitivně předpokládanou bezpečnost, ale mnohem nižší. Předpokládalo se, že složitost S(F||G) nalezení kolize hašovacího kódu F(x)||G(x) bude rovna součinu složitostí nalezení kolizí dílčích hašovacích kódů, tj. S(F||G) = S(F) * S(G). Joux ukázal, že je to jen o něco více než S(F) + S(G), přičemž postačí, aby pouze F byla iterativní hašovací funkce, zatímco G může být i náhodné orákulum. Stručně řečeno kaskádovitá konstrukce pozbývá smyslu, protože výsledný kód je přibližně pouze tak složitý jako silnější z dílčích hašovacích funkcí. Tyto dvě vlastnosti přímo neohrožují žádné prakticky používané schéma, ale ukazují, že iterativní konstrukce není ideální, neboť oddaluje takové hašovací funkce od náhodného orákula.
Postup.

- Nechť F je iterativní hašovací funkce s délkou hašovacího kódu $n_f \leq n_g$.
- Potom se složitostí $n_g/2 * S(F)$ vytvoříme $n_g/2$ návazných kolizí funkce F (postup stejný jako použil Joux), které dávají $2^{ng/2}$ - násobnou multikolizi vzhledem k F.
- Mezi těmito $2^{ng/2}$ zprávami nalezneme jednu kolizi vzhledem ke G.
- Máme tedy dvě zprávy, které mají stejný hašový kód vzhledem k F i G, tj. k F||G.

Složitost je $n_g/2 * S(F) + 2^{ng/2}$ (druhý sčítanec je počet hašování G), tedy $n_g/2 * S(F) + S(G) \approx S(F) + S(G)$.

Intuitivně se očekávalo, že složením kvalitní hašovací funkce F o délce kódu n_f a funkce G o délce kódu n_g vznikne kvalitní hašovací funkce o délce kódu $n_f + n_g$ a složitosti nalezení kolize bude $2^{(nf+ng)/2}$. Místo toho je to mnohem méně, $n_g/2 * 2^{nf/2} + 2^{ng/2}$.

Nalezení druhého vzoru u dlouhých zpráv snadněji než se složitostí 2^n

V práci [KS2004] se tato vlastnost ukazuje pro dlouhé zprávy, o délce blízké $2^{n/2}$ bloků. Postup (zkrácený postup s využitím pevných bodů).

- Nechť zpráva M má délku 2^k bloků.
- Vytvoříme seznam průběžných kontextů K_t při hašování zprávy $M = m_1, m_2, ..., m_t, ...$ Je jich 2^k.
- Volíme náhodně $2^{n/2}$ bloků M_i , které dávají seznam $2^{n/2}$ haší $h_i = h(H_0, M_i)$.
- Volíme náhodně $2^{n/2}$ bloků N_j a z N_j určíme pevný bod $H_j = f(H_j , N_j)$, využijeme k tomu Davies-Meyerovy konstrukce.
- Nalezneme kolizi mezi seznamy $\{H_j\}$ a $\{h_i\}$, tj. i* a j* tak, že $h_{i*} = H_{j*}$.
- Volíme náhodně $2^{n - k}$ bloků $Mlink_l$, l = 1, 2, ..., $2^{n - k}$, které dávají seznam $2^{n - k}$ haší $hlink_l = h(H_{j*}, Mlink_l)$.
- Nalezneme kolizi mezi seznamy $\{hlink_l\}$ a $\{K_t\}$, tj. l* a t* tak, že $hlink_{l*} = K_{t*}$.
- Zpráva (M_{i*}, N_{j*}, $Mlink_{l*}$) a prvních *i* bloků zprávy M dávají stejný hašovací kontext K_{t*} .
- Tyto zprávy mají různou délku, ale zprávu (M_{i*}, N_{j*}, $Mlink_{l*}$) doplníme o potřebný počet bloků na i bloků pomocí pevného bodu, jako (M_{i*}, N_{j*}, N_{j*},..., N_{j*}, $Mlink_{l*}$). Za obě zprávy pak připojíme zbytek zprávy M a dostaneme druhý vzor zprávy M.

Složitost je $2^{n/2}$ (seznam M_i) + $2^{n/2}$ (seznam N_j) + 2^{n-k} (seznam $Mlink_l$) + 2^k (seznam K_t) = $2^{n/2+1} + 2^{n-k} + 2^k \approx 2^{n/2+1} + 2^{n-k+1}$. To je mnohem méně než 2^n.

8. Literatura

[ARCHIV] Archiv autora obsahující články o kryptologii a bezpečnosti, http://cryptography.hyperlink.cz/

[BC04a] Biham, Eli, Chen, Rafi: Near Collisions of SHA-0, CRYPTO 2004 http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2004/CS/CS-2004-09.ps.gz

[BC04b] Eli Biham, Rafi Chen: New results on SHA-0 and SHA-1, CRYPTO 2004 Rump Session

[BoBo93] B. den Boer and A. Bosselaers. Collisions for the compression function of MD5. In Advances in Cryptology, Eurocrypt '93, pages 293-304, Springer-Verlag, 1994.

[D96a] H. Dobbertin, Cryptanalysis of MD4, Fast Software Encryption 1996, LNCS, Vol. 1039, Springer-Verlag, 1996, pp. 53 - 69

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

[DO96eu] H. Dobbertin. Cryptanalysis of MD5 Compress. Presented at the rump session of Eurocrypt ‘96, May 14, 1996.

[DO96cb] H. Dobbertin. The Status of MD5 after a Recent Attack. CryptoBytes, 2(2): 1-6, 1996.

[HAVAL] Y. Zheng, J. Pieprzyk, J. Seberry, HAVAL - A One-way Hashing Algorithm with Variable Length of Output, Auscrypt 92

[HMAC] FIPS PUB 198, The Keyed-Hash Message Authentication Code (HMAC), NIST, US Department of Commerce, Washington D. C., March 6, 2002, http://csrc.nist.gov/CryptoToolkit/tkhash.html, resp. RFC 2104, http://www.rfc-editor.org/

[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

[Joux04a] Antoine Joux: Collisions in SHA-0, CRYPTO 2004 Rump Session

[Joux04b] A. Joux: Multicollisions in iterated hash functions. Application to cascaded constructions. Proceedings of Crypto 2004, LNCS 3152, pages 306-316.

[KS2004] John Kelsey, Bruce Schneier: Second Preimages on n-bit Hash Functions for Much Less than 2^n Work, http://eprint.iacr.org/2004/304/, November 15, 2004

[LWW05a] Arjen Lenstra, Xiaoyun Wang and Benne de Weger: Colliding X.509 Certificates, *Cryptology ePrint Archive*, Report 2005/067, http://eprint.iacr.org/2005/067

[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

[MD245] MD2, MD4, MD5 - RFC 1319, 1320, 1321, http://www.rfc-editor.org/

[NIST05b] NIST Brief Comments on Recent Cryptanalytic Attacks on SHA-1 http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf

[NIST05a] NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1, http://csrc.ncsl.nist.gov/hash_standards_comments.pdf,

[OOW94] P. van Oorschot and M. Wiener. Parallel collision search with application to hash functions and discrete logarithms. In Proceedings of 2nd ACM Conference on Computer and Communication Security, pages 210-218, ACM Press, 1994.

[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

[PKCS2] *PKCS#5 v2.0: Password-Based Cryptography Standard*, RSA Labs, March 25, 1999

[RIPEMD-160] H. Dobbertin, A. Bosselaers, B. Preneel, "RIPEMD-160: A Strengthened Version of RIPEMD," Fast Software Encryption, LNCS 1039, D.Gollmann, Ed., Springer-Verlag, 1996, pp. 71-82

[SHA-0] FIPS 180 (superseded by FIPS 180-1 and FIPS 180-2), Secure hash standard (SHS), NIST, US Department of Commerce, Washington D. C., May 1993

[SHA-1] FIPS 180-1 (superseded by FIPS 180-2), Secure hash standard (SHS), NIST, US Department of Commerce, Washington D. C., April 1995

[SHA-2] FIPS 180-2, Secure Hash Standard (SHS), NIST, US Department of Commerce, Washington D. C., August 2002 (change notice: February 2004), http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, platný standard, obsahuje definice SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512

[VK2005a] Vlastimil Klima: Finding MD5 Collisions – a Toy For a Notebook, *Cryptology ePrint Archive*, Report 2005/075, March 5, 2005, http://eprint.iacr.org/2005/075, v češtině "Nalézání kolizí MD5 - hračka pro notebook", http://cryptography.hyperlink.cz/md5/MD5_kolize.pdf.

[VK2005b] Vlastimil Klima: Finding MD5 Collisions on a Notebook PC Using Multi-message Modifications, March 31, 2005, *Cryptology ePrint Archive*, Report 2005/112, http://eprint.iacr.org/2005/102, v češtině "Nalézání kolizí MD5 na notebooku pomocí mnohonásobných modifikací zprávy", http://cryptography.hyperlink.cz/md5/Vlastimil_Klima_MD5_kolize.pdf .

[VK2005c] Vlastimil Klíma: Hašovací funkce, principy, příklady a kolize, přednáška na semináři Cryptofest, http://www.cryptofest.cz/, Praha, 19.3. 2005, on line na http://cryptography.hyperlink.cz/2005/cryptofest_2005.htm.

[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

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

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

B. Neviditelné (sympatetické) inkousty

Pavel Vondruška, ČESKÝ TELECOM, a.s.,
(pavel.vondruska@crypto-world.info)

Stručná historie

Mezi známé steganografické metody, tedy metody, kdy se odesílatel a příjemce snaží utajit před nepovolanou osobou samotné předávání senzitivních informací, patřilo již odedávna použití neviditelných neboli sympatetických inkoustů. Tedy inkoustů, kdy zapsaný text není při běžném pohledu viditelný. Příjemce předaný neviditelný text zobrazí jemu známým způsobem, což může být např. zahřátím, působením nějakých jiných chemikálií, případně osvícením ultrafialovým nebo infračerveným světlem.

Je to velmi stará metoda. O jejím použití píše již v 1. století n.l. Plinius ve svém známém díle *Naturalis historia*. Zmiňuje se zde o tom, že rostlinné mléko (z rostliny tithymallus) může být využito jako neviditelný inkoust. O neviditelném inkoustu se zmiňuje i básník Ovidius ve svém díle Umění lásky. Řecký vědec Filio byzantský popisuje neviditelný inkoust vyrobený z duběnek, který se dá vyvolat roztokem modré skalice. V arabském světě je popsáno hned několik typů neviditelných inkoustů založených na různých chemických reakcích a to v knize Subh-al-á-šá od Qalqashadiho. V Evropě byly neviditelné inkousty oblíbené zejména ve středověku pro využití v diplomatické poště. Zmiňují se o nich oba „klasikové“ evropské kryptografie Alberti a Porta. Druhý zmiňovaný zasvětil neviditelným inkoustům XVI. knihu svého rozsáhlého díla Magia Naturalis.

Obliba tohoto jednoduchého a relativně bezpečného způsobu (zejména tehdy, kdy nepovolaná osoba neočekává předávání tajných informací mezi odesílatelem a příjemcem) přetrvala až dodnes. Jako zajímavost si uvedeme, že např. neviditelný inkoust využíval i Lenin, kdy do dopisů z vězení připisoval poznámky psané mlékem. Za I. světové války byl neviditelný inkoust velmi rozšířen a byl používán špióny na všech frontách. České země nebyly v tomto ohledu výjimkou, neviditelný inkoust byl např. používán ke spojení mezi domácím (Jan Frič) a zahraničním odbojem. Za druhé světové války používali němečtí špióni různé druhy neviditelných inkoustů a to od velice sofistikovaných až po ty triviální (mléko, moč). Za všechny jmenujme alespoň George Dasche, vůdce osmi německých špiónů, kteří se pod jeho vedením vylodili z ponorky na Long Islandu v roce 1942 s úkolem ničit americká obranná zařízení a železniční mosty. Po namočení jeho kapesníku do čpavku se objevil červeně psaný text, který prozradil kontaktní adresy špiónů ve Španělsku a USA. Známé je používání neviditelných inkoustů i v době studené války, kdy špióni v padesátých až sedmdesátých letech používali neviditelný inkoust k předávání svých hlášení přes „železnou“ oponu pomocí běžných dopisů zasílaných na smluvené adresy.

Obliba tohoto spojení spočívá v mnoha faktorech. Především je to velice jednoduchý způsob, který nevyžaduje složité zaškolení. Dále je možné jej použít i v situacích, kdy by jiné metody nebyly možné. Typickým příkladem je zasílání pokynů z vězení. Pokud by v dopise vězně byla nalezena šifra, nebyl by doručen. Tedy použití této metody zajišťuje samotné utajení senzitivní komunikace, což v některých situacích je rozhodující pro výběr zabezpečeného spojení. Další obrovskou výhodou je operativnost, tím myslím, že lze použít k vytvoření neviditelného písma zdroje, které jsou lehce dostupné (močovina, mléko, ocet …).

Typy inkoustů

První skupinu tvoří organické kapaliny jako moč, mléko, citrónové šťávy, ocet a ovocné šťávy (např. cibule) a mohou být vyvolány lehkým zahřátím. Důvodem je tepelný rozklad organických látek (cukrů, popř. bílkovin), na hnědě zbarvené produkty. Podobně je tomu u roztoku cukru (sacharózy) okyseleném kyselinou sírovou.

Druhou skupinou jsou chemické látky, které sice nejsou organického původu, ale vyvolávají se také zahřátím. Sem patří např. nasycený roztok dusičnanu draselného, který zanechá na papíru po odpaření malé bezbarvé krystalky. Tato sloučenina je silným oxidačním činidlem a po zahřátí papíru dojde k procesu podobnému spalování – papír v místech s inkoustem zuhelnatí. Jiným případem může být chlorid kobaltnatý, který se vyskytuje buď v podobě hydrátu nebo bezvodé soli. Hydrát je jen slabě růžový, takže na papíru není téměř vidět, avšak po zahřátí se rozloží za uvolnění hydrátové vody a spatříme jasně modrou.

Třetí skupinou je využití chemických reakcí k zviditelnění písma. Využití je založeno na tvorbě barevných produktů po reakci s jinou chemickou látkou. Takových inkoustů lze vytvořit celou řadu, stačí, když výchozí látka bude bezbarvá nebo jen slabě zbarvená a produkt po chemické reakci bude mít naopak výraznou barvu. Např. píše-li špion síranem železnatým, nebude nic vidět, dokud text nepotřeme kyanidem sodným. Obě sloučeniny spolu začnou reagovat a vytvoří ferrokyanid neboli pruskou modř.

Poslední skupinu tvoří neviditelné inkousty, kde se ke zviditelnění zapsaných zpráv nevyužívá ani teplo ani jiné chemikálie, ale ultrafialové (UV) nebo infračerveného záření. Kupříkladu text napsaný kyselinou salicylovou je viditelný pouze po dopadu ultrafialového záření. Toto záření snadno příjemce získá např. z lampiček, které se prodávají na ověřování pravosti bankovek nebo z horského sluníčka, případně ze speciálních k tomuto účelu prodávaných zařízení (viz obrázek UV lampy v podobě propisky). Obyčejné papíry pod UV zářením "svítí", proto je nutné používat neklížený speciální papír (lze však nahradit i pijákem nebo filtračním papírem). Jev, který v tomto případě umožňuje zviditelnění písma, se nazývá fluorescence. Látka, která fluoreskuje, pohltí záření o vyšší energii (v tomto případě neviditelné UV záření) a vyzáří světlo o energii nižší (zde fialové světlo).

Závěrem tohoto odstavce poznamenejme, že umění výroby dokonalého neviditelného inkoustu spočívá v nalezení sloučeniny, která bude reagovat s co nejmenším počtem chemikálií – ideální by bylo, aby to bylo pouze s jedinou. Při testech na neviditelný inkoust se dopis postupně na různých částech potíral vybranými chemikáliemi, které byly známé jako běžné „vývojky“ pro neviditelná písma. Používané vývojky měly tak široké spektrum, že vyvolávaly i takové sloučeniny jako mastné skvrny, otisky prstů a kapky potu. Dopisy byly dále zkoumány infračerveným a ultrafialovým světlem. D. Kahn v knize The Codebreakers uvádí, že za druhé světové války bylo v USA při systematických i náhodných prohlídkách pošty zachyceno a FBI předáno 4600 podezřelých dopisů a z nich 400 skutečně obsahovalo informace psané neviditelným písmem.

Přehled neviditelných inkoustů

Inkousty, které se vyvolávají teplem

- Hnědě zbarvené písmo
  - mléko
  - kostka cukru rozpuštěná ve lžíci vody
  - šťáva z cibule, citronu nebo třešní
  - močovina
  - ocet
  - roztok jedlé sody
- Modré písmo
  - 1 g chloridu kobaltnatého a 2 g glycerinu se rozpustí v 90 ml vody. Písmo po zahřátí zmodrá.
- Zelené písmo
  - 8 g chloridu nikelnatého a 2 g chloridu kobaltnatého se rozpustí v 90 ml vody. Zahřátím písmo zezelená a po ochlazení opět zmizí.
- Žluté písmo
  - Připraví se 20% roztok chloridu měďnatého ve vodě. Nápis provedený tímto inkoustem není za běžných okolností viditelný. Zahříváním nad tepelným zdrojem vystoupí žluté zabarvení písma. Po vychladnutí zabarvení zmizí.
- Černé písmo
  - 1 g kyseliny sírové a 2 g cukru se rozpustí ve 100 ml vody. Písmo zahřátím zčerná.

Inkousty, které se vyvolávají chemickou reakcí

- Černé písmo
  - 1 g síranu železnatého se rozpustí v 25 ml vody. Písmo zčerná potřením roztokem taninu nebo kyseliny galové ve vodě.
  - 1 g octanu olovnatého se rozpustí v 25 ml vody. Písmo se vyvolá sirovodíkem nebo sirovodíkovou vodou.
  - 3 g octanu olovnatého se rozpustí ve 100 ml vody. Písmo se vyvolá potíráním roztokem sirníku draselného.
  - 5 g dusičnanu nebo octanu olovnatého se rozpustí ve 100 ml vody. Písmo se vyvolá roztokem 10 g sirníku sodného ve 100 ml vody.
- Modré písmo
  - 1 g ferokyanidu draselného se rozpustí v 25 ml vody. Písmo se vyvolá roztokem chloridu železitého.
  - 1 g chloridu kobaltnatého se rozpustí v 25 ml vody. Písmo se vyvolá roztokem chloridu železitého ve vodě.
  - 10 - 15 g bramborového škrobu ve 100 ml vody. K vyvolání se používá roztok jódu. Modré zbarvení vznikající působením jódu na škrob je způsobeno vznikem zvláštního, tzv. inkluzního komplexu. Molekuly škrobu obsahují místa, kam se může jód výhodně navázat, avšak nejedná se o běžnou

chemickou reakci, protože molekuly jódu jsou pouze uzavřeny uvnitř řetězců škrobu.
    - K psaní lze použít síran železnatý, který se dá vyvolat kyanidem sodným. Barevnou viditelnou sloučeninu tvoří vzniklý ferrokyanid (pruská modř).
- Červené písmo
    - 0,5-1 g fenolftaleinu rozpustíme ve 25 ml etylalkoholu. Písmo je neviditelné a vyvolává se roztokem uhličitanu sodného (sody) nebo uhličitanu draselného (potaše).
    - 5 g chloridu železitého se rozpustí v 25 ml vody. Vyvolá se slabým okyseleným roztokem rhodanidu draselného.
    - K psaní se dá využít i síran měďnatý, který lze vyvolat parami čpavku.
- Hnědé písmo
    - Jako inkoust se dá využít octan olovnatý. Vyvolává se siřičitanem sodným.

Inkousty viditelné v UV záření

- acylpyrin nebo aspirin se rozpustí ve 2 ml vody a přidá se trochu hydroxidu sodného. Směs se zahřeje a za stálého protřepávání se udržuje ve varu nejméně jednu minutu. Po ochlazení se přidá 2 ml octa a inkoust je hotový. Účinnou složkou inkoustu je kyselina salicylová, která vznikla rozkladem kyseliny acetylsalicylové z acylpyrinu (aspirinu).
- Kvalitní inkousty viditelné pomocí UV záření lze v současné době také poměrně levně zakoupit. Konkrétní nabídku různých balení inkoustů, vyvolávacích typů UV diod a třeba i fix pro neviditelné psaní (viz. obrázek) naleznete např. zde http://www.vltava2000.cz/uv-svet/default.asp?lngDepartmentID=1

Poznámka

Jako papír je nejvýhodnější pro většinu neviditelných písem využívat papír neklížený nebo dokonce přímo filtrační. Běžný kancelářský papír obsahuje pojiva, která někdy ruší příslušné chemické reakce.

Literatura

[1] David Kahn: The Codebreakers
[2] Neviditelné písmo: http://www.iabc.cz/Clanek6264.htm
[3] Za tajemstvím molekul 2: http://www.abicko.cz/Clanek6203.htm
[4] Kučera, Martin: ZPRÁVY TAJNÝM INKOUSTEM, Masarykův ústav AV ČR, Praha 2003
[5] Sympatetické inkousty: http://www.zoubek.cz/homepage/sifry/index.html#INKOUSTY
[6] Nabídka UV inkoustů: http://www.vltava2000.cz/uv-svet/default.asp?lngDepartmentID=1

C. Kryptografie a normy
Formáty elektronických podpisů - část 3.
(dokument ETSI TS 101 7733 - Electronic Signature Formats)

Jaroslav Pinkava, PVT a.s. (jaroslav.pinkava@pvt.cz)

1. Úvod

V prvních dvou částech tohoto článku (Crypto-World 11/2004 a Crypto-World 1/2005) byly popsány jednotlivé formáty elektronického podpisu dle dokumentu ETSI [1] TS 101 733. Jednalo se postupně o formáty - základní (BES, EPES), s časovým razítkem (ES-T), tzv. rozšířené formáty (ES-X) atd. Posledním formátem byl archivační formát elektronického podpisu ES-A.

Toto pokračování je věnováno definicím souvisejících atributů (kapitola 5. a 6. dokumentu ETSI TS 101 733).

2. Atributy elektronického podpisu

Struktura elektronického podpisu je definována v CMS. Atributy, které jsou v dokumentu využívány, vychází z CMS (RFC 3369) a ESS (Enhanced Security Services - RFC 2634). Další atributy definuje samotný popisovaný dokument.

K obecné syntaxi podpisu:

`Data content type` (CMS - RFC 3369).
`Signed-data content type` (CMS - RFC 3369).
`Signed Data type` (CMS - RFC 3369).
- výjimka - zde musí však číslo verze pro syntaxi být rovno 3.

`EncapsulatedContentInfo type` (CMS - RFC 3369).
`SignerInfo type` (CMS - RFC 3369).
- pole `signedAttrs` musí obsahovat atributy: `content-type`, `message-digest`, `signing-certificate`;

Výpočty otisku, generování podpisu a proces ověření podpisu probíhají dle popisu v CMS.

Přehled již dříve popsaných atributů (v jiných dokumentech):

`content-type` (CMS - RFC 3369).
`message-digest` (CMS - RFC 3369).
`signing-certificate attribute`:
`ESS signing-certificate attribute`
(je-li použit hashovací algoritmus SHA-1, dle RFC 2634);
`other-signing-certificate attribute` (je-li použit jiný hashovací algoritmus). Tento atribut (other signing certificate attribute) je definován následovně (ASN.1):

```
id-aa-ets-otherSigCert OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
smime(16) id-aa(2) 19 }
```

Jeho hodnota pak má následující syntaxi:

```
OtherSigningCertificate ::= SEQUENCE {
certs SEQUENCE OF OtherCertID,
policies SEQUENCE OF PolicyInformation OPTIONAL
-- NOT USED IN THE PRESENT DOCUMENT
}
OtherCertID ::= SEQUENCE {
otherCertHash OtherHash,
issuerSerial IssuerSerial OPTIONAL }
OtherHash ::= CHOICE {
sha1Hash OtherHashValue, -- This contains a SHA-1 hash
otherHash OtherHashAlgAndValue}
OtherHashValue ::= OCTET STRING
OtherHashAlgAndValue ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
hashValue OtherHashValue }
```

Daný dokument stanoví, že formát EPES zahrnuje odkaz na podpisovou politiku (tento odkaz je obsažen v signedData). Atribut `signature-policy-identifier` musí být podepsaným atributem. Syntaktické definice (identifikace a hodnota):

```
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
smime(16) id-aa(2) 15 }

SignaturePolicyIdentifier ::=CHOICE{
SignaturePolicyId SignaturePolicyId,
SignaturePolicyImplied SignaturePolicyImplied -- not used in this
version}
SignaturePolicyId ::= SEQUENCE {
sigPolicyId SigPolicyId,
sigPolicyHash SigPolicyHash,
sigPolicyQualifiers SEQUENCE SIZE (1..MAX) OF
SigPolicyQualifierInfo OPTIONAL}
SignaturePolicyImplied ::= NULL
```

Dalšími (nepovinnými) atributy mohou být:

`Signing` time (CMS - RFC 3369).
`Countersignature` (CMS - RFC 3369)
- to je nepodepisovaný atribut.
`Content-reference` (ESS - RFC 2634).
`Content identifier` (ESS - RFC 2634).
`Content-hints` (ESS - RFC 2634).

Specifickými (v tomto dokumentu definovanými) atributy jsou:

`Commitment-type-indication`

- podpisující strana sděluje ověřující straně význam svého podpisu, sémantika tohoto sdělení může být součástí podpisové politiky či může být zaregistrována dle pravidel registrační autority. V dokumentu jsou definovány následující typy generických sdělení:

Proof of origin indikuje, že podepisující strana vytvořila, schválila a odeslala zprávu.
Proof of receipt indikuje, že podepisující strana obdržela obsah zprávy.
Proof of delivery indikuje, že příslušný poskytovatel doručil zprávu do lokálního umístění, které je dostupné příjemci zprávy.
Proof of sender indikuje, že příslušná entita odeslala zprávu (nemusela ji vytvořit).
Proof of approval indikuje, že podepisující strana schválila obsah zprávy.
Proof of creation indikuje, že podepisující strana vytvořila zprávu (nemusela ji však schválit ani odeslat).

`Signer-location` attribute
- tento atribut specifikuje adresu, která je asociována k podepisující straně (geografické umístění) - podle ITU-T doporučení F.1. Je to podepisovaný atribut.

`Signer-attributes`
- takto mohou být specifikovány další atributy podepisující strany (např. role). Tyto atributy mohou vzniknout buď na základě prohlášení podepisující strany či jako certifikované atributy.

`Content-time stamp`
- časová razítko, které vzniklo k podepisovaným datům před vlastním podpisem.

Nezávislé vícenásobné podpisy jsou podporovány nezávislými `SignerInfo` každé podepisující strany. Každý `SignerInfo` musí obsahovat všechny atributy, které požaduje daný dokument a každý `SignerInfo` musí být zpracováván ověřující stranou nezávisle jeden na druhém.

Včleněné podpisy jsou podporovány užitím atributu `countersignature`.

3. Další atributy pro validaci elektronického podpisu

V kapitole 6. dokumentu jsou specifikovány atributy, které obsahují různé typy ověřovaných (validovaných) dat. Patří mezi ně

`Signature-time-stamp`
- definován pro ES-T;

a také úplné odkazy na ověřovaná data, které se sestávají z časového razítka pro hodnotu podpisu a dále se sestávají z:

```
Complete-certificate-references;
Complete-revocation-references.
```

Tyto informace musí být použity pro úplné ověření elektronického podpisu (ES-C).

Nepovinně jsou definovány rozšířené formáty (eXtended forms) ověřovaných dat - dva typy formátu ES-X, dále ES-X Long, resp. ES-X Long Type 1 a 2.
Jsou zde rovněž tak specifikovány struktury dat pro ES-A.

3.1. ES-T

Elektronický podpis s časovým razítkem je typ podpisu, kde jsou dostupná jen některá ověřovaná dat (například některé certifikáty či revokační informace), nejsou však dostupná všechna ověřovaná data. Minimální strukturu ověřovaných dat tvoří atribut Signature-time-stamp s následující definicí pro identifikací a hodnotu:

```
id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= { iso(1) member-
body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}

SignatureTimeStampToken ::= TimeStampToken
```

(definice TimeStampToken je dána dle RFC 3161 a dokumentu ETSI TS 101 861 - Time Stamping Profile). Pro vícenásobné podpisy může být TimeStampToken (TST) počítán odděleně pro každý z nich, nebo jen pro jeden z nich a žádný další. Mohou být také přítomny TST vydané různými TSA - pro stejnou signerInfo.

3.2. ES-C

Toto je typ podpisu s úplnými odkazy na ověřovaná data, tj. přítomna je veškerá informace o certifikátech a revokacích. Minimální struktura úplných ověřovaných dat musí obsahovat:

- čas (buď jako atribut signature-timestamp nebo jako časovou značku, kterou vydává Time-Marking Authority);
- complete-certificate-references;
- complete-revocation-references.

Atribut complete-certificate-references je nepodepisovaný atribut. Odkazuje se na úplnou množinu certifikátů, které byly použity pro ověření el. podpisu s úplnými ověřovanými daty až po certifikát (ale ne včetně) podepisující strany. Identifikace a hodnota atributu:

```
id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 21}

CompleteCertificateRefs ::= SEQUENCE OF OtherCertID
```

Obdobně atribut complete-revocation-references je nepodepisovaný. Odkazuje se na úplnou množinu CRL (resp. ACRL či odpovědi OCSP), které byly použity pro ověření certifikátů podepisující strany a certifikátů certifikační autority v elektronickém podpisu s úplnými ověřovanými daty. Identifikace a hodnota atributu:

```
id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= { iso(1) member-
body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 22}

CompleteRevocationRefs ::= SEQUENCE OF CrlOcspRef
CrlOcspRef ::= SEQUENCE {
crlids [0] CRLListID OPTIONAL,
ocspids [1] OcspListID OPTIONAL,
otherRev [2] OtherRevRefs OPTIONAL
}
```

Přítomen musí být alespoň jeden CRL pro každou CA na certifikační cestě. Kopie CRL a odpovědí OCSP mou být uchovávány prostřednictvím atributu revocation-values.
V případě, že je přítomen v podpisu atributový certifikát, pak jsou použity atributy `Attribute-certificate-references` a `Attribute-revocation-references` pro informace nezbytné k ověření tohoto atributového certifikátu.

3.3. ES-X

Existuje celá řada nepovinných atributů pro rozšířený formát elektronického podpisu:

`Certificate-values`
- obsahuje hodnoty certifikátů, na které je odkazováno atributem `complete-certificate-references`.

`Revocation-values`
- obdobně obsahuje hodnoty CRL a odpovědí OCSP odkazované atributem `complete-revocation-references`.

`ES-C-timestamp`
- tento atribut má za cíl ochranu před kompromitací klíče CA. Je to časové razítko hashe elektronického podpisu spolu s úplnými ověřovanými daty (ES-C).

`Time-stamped-certs-crls-references`
- atribut je používán k časovému razítku nad odkazy k certifikátům a revokačním informacím. Je to tedy časové razítko přes seznam odkazovaných certifikátů a CRL (resp. odpovědí OCSP) a slouží jako ochrana před kompromitacemi CA.

3.4. ES-A

Pokud je platnost elektronického podpisu žádoucí ve velmi dlouhém časovém období, je třeba z důvodů možných nebezpečí plynoucích z potenciálního oslabení použitých algoritmů či z omezení dob platnosti certifikátu TSA, aplikovat znova časová razítka a to i vícekrát.

V tomto případě je používán atribut `archive-time-stamp` (pro formát ES-A). Tento atribut je časovým razítkem přes celou řadu prvků `signedData` elektronického podpisu.

Pokud nejsou přítomny atributy `certificate-values` a `revocation-values` (ve formátech BES a EPES), pak tyto atributy musí být přidány ještě před výpočtem archivního časového razítka.

Atribut `archive-time-stamp` je nepodepisovaný a v elektronickém podpisu se může vyskytovat vícekrát (i od různých zdrojů časových razítek). Identifikace a hodnota:

```
id-aa-ets-archiveTimestamp OBJECT IDENTIFIER ::= { iso(1) member-
body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 27}

ArchiveTimeStampToken ::= TimeStampToken
```

Algoritmus, o který se opírá použité časové razítko, by měl být "silnější" či by měl používat větší délku klíče, než měly použité algoritmy původního elektronického podpisu a původní časové značky. Takto tento formát poskytuje i ochranu proti kompromitaci klíče TSA.

Poznámka: Pro vyslovení shody s tímto normativním dokumentem:

- musí být implementován jeden ze základních dvou formátů elektronického podpisu (BES či EPES);
- shoda musí vést až k ES s úplnými ověřovanými daty - ES-C (nemusí být tedy implementovány rozšířené a archivní formáty, samozřejmě pak vznikají omezení možného využití - dlouhodobá archivace).

5. Literatura

[1] ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
[2] RFC 3126, Electronic Signature Formats for long term electronic signatures
Mezi známé steganografické metody, tedy metody kdy se odesílatel a příjemce snaží utajit před nepovolanou osobou samotné předávání senzitivních informací, patřilo již

D. O čem jsme psali v dubnu 2000 – 2004

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

Crypto-World 4/2003

Crypto-World 4/2004

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze **jméno a příjmení, titul**, pracoviště (není podmínkou) a **e-mail adresu** určenou k zasílání kódů ke stažení sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a **e-mail adresu**, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf

NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška

Webmaster Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@pvt.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/