Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 11/2006 **15. listopad 2006**

11/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1188 registrovaných odběratelů)

Obsah : str.

A. Soutěž v luštění 2006 skončila

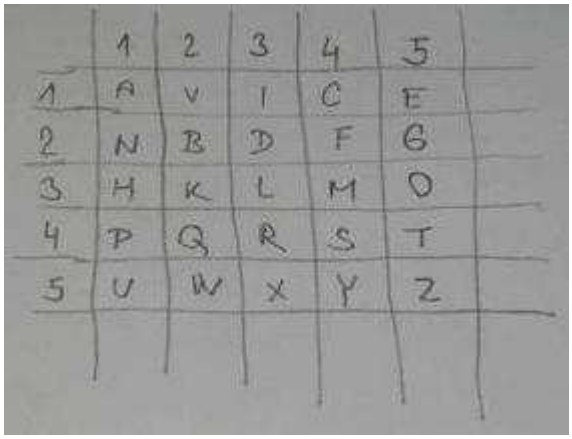
Pavel Vondruška, (pavel.vondruska@crypto-world.info)

Soutěž v luštění 2006 (http://soutez2006.crypto-world.info/) skončila. Možnost vkládat správné výsledky řešení jednotlivých úloh byla uzavřena 2.11.2006 ve 20.30 hod.

Důvodem bylo, že toho dne vyšla v nakladatelství Albatros moje kniha **Kryptologie, šifrování a tajná písma** (http://crypto-world.info/oko/), ve které jsou všechny soutěžní úlohy uvedeny. V kapitole šest (Vyzkoušejte si…) jsou dále otištěny i všechny otevřené texty a to včetně stručného návodu na jejich získání. V souladu s pravidly musela být proto soutěž ukončena.

Pořadí na prvých deseti místech:

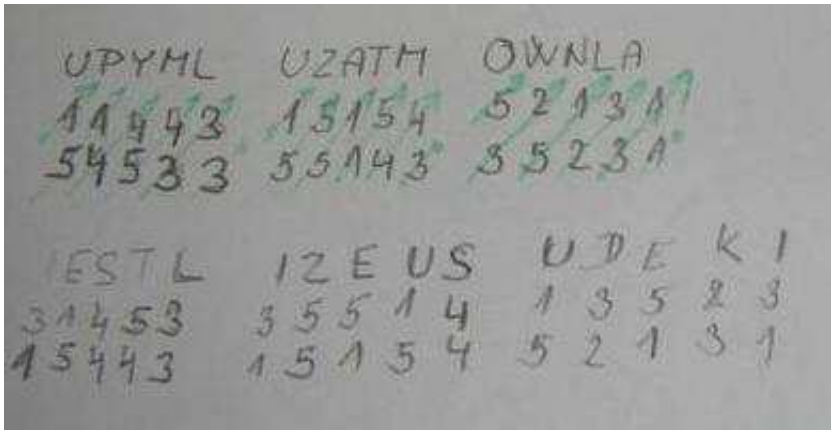
1 room132	**80**	**23.09 (14:16)**
2 peta007	**80**	**24.09 (20:10)**
3 MD5Mir	**80**	**29.09 (10:14)**
4 crcker	80	28.10 (23:41)
5 stanislaw	74	26.09 (01:32)
6 hodiny	68	19.10 (21:19)
7 tvrz	67	23.09 (19:43)
8 gimli2	66	30.09 (20:52)
9 smash	63	24.09 (14:42)
10 jmkollar	63	25.09 (10:59)



Ceny (http://soutez2006.crypto-world.info/index.php?crypto=ceny) získali první tři řešitelé a dále tři řešitelé, kteří byli vylosování z 83 soutěžících, kteří dosáhli více než 15 bodů (limit pro zařazení do losování).

Vylosovaní řešitelé:

15. jahoda (55 bodu)
31. Michalko (40 bodu)
65. skalibu (20 bodu)



Doprovodné fotografie : Room132, luštění šifry BIFID (úloha č. 29)

Řešení všech úloh, včetně postupů a návodů na jejich získání, budou uvedeny v prosincovém čísle 15/2006, které vyjde 15.12.2006.

Všem úspěšným řešitelům blahopřeji a věřím, že se zúčastníte opět příštího ročníku.

Pavel Vondruška

B. Nový koncept hašovacích funkcí SNMAC s využitím speciální blokové šifry a konstrukcí NMAC/HMAC

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

V tomto příspěvku prezentujeme část projektu NBÚ Bezpečná hašovací funkce (ST20052005017). Část tohoto příspěvku byla zaslána do mezinárodní kryptologické konference EUROCRYPT 2007. Rozšířená verze byla zveřejněna v archívu IACR jako eprint 2006/376 a v češtině na domácí stránce SNMAC [Kli06b]. Populární výklad, základních myšlenek tohoto článku, byl autorem zveřejněn 13.11.2006 na root.cz [Kli06d].

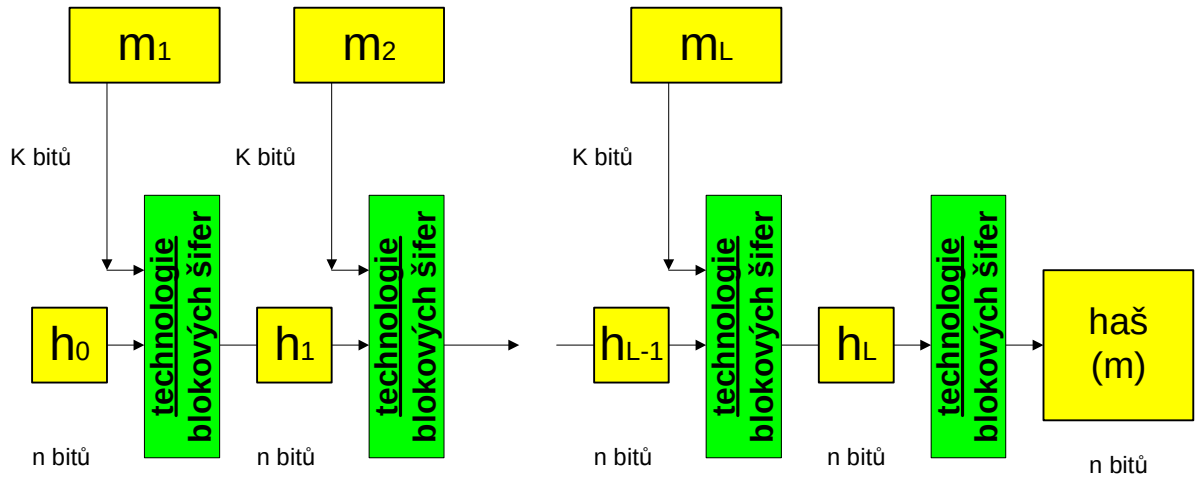
Abstrakt. V příspěvku prezentujeme nové důkazy bezpečnosti velmi dobře známých hašovacích konstrukcí NMAC/HMAC, navržené Bellare a kol. v roce 1996. Ukazujeme, že blokové šifry by měly být v hašovacích funkcích používány jiným způsobem než dosud. Zavádíme nové kryptografické primitivum, speciální blokovou šifru (SBŠ). SBŠ je odolná proti útokům, specifickým pro blokové šifry v hašovacích funkcích. Navrhujeme nový koncept hašovacích funkcí (SNMAC, Special NMAC), který vzniká použitím SBŠ v konstrukcích NMAC/HMAC. Z nových důkazů bezpečnosti NMAC/HMAC vyplývá, že hašovací funkce SNMAC jsou výpočetně odolné proti nalezení vzoru a kolize. Navíc Coron a kol. na CRYPTO 2005 ukázali, že SNMAC se limitně blíží náhodnému orákulu. Konstrukce SNMAC je obecná a umožňuje různorodé návrhy pomocí různých instancí SBŠ. Navrhujeme speciální blokovou šifru DN (Double Net) a na základě ní konstruujeme hašovací funkci HDN (Hash Double Net) jako konstrukci typu SNMAC.

Obsah

1. Úvod

Je známo, že většina používaných iterativních hašovacích funkcí podléhá tzv. útoku prodloužením zprávy [Tsu92], tj. z hodnoty h(M) lze vypočítat h(M || N) pro vhodné N. I když se tím odlišují od náhodného orákula, tato vlastnost byla mnoha hašovacím funkcím dlouho tolerována. V roce 2004 a 2005 byly zjištěny další generické problémy hašovacích funkcí, multikolizní útok Jouxe [Jou04] a Kelsey-Schneierův multikolizní útok a útok na druhý vzor [KS05]. Poznamenejme, že všechny moderní hašovací funkce podléhají těmto třem generickým útokům ([Tsu92], [Jou04], [KS05]), a proto se silně odlišují od chování náhodného orákula.
Jako možná náhrada funkcí MD5 a SHA-1 byla dříve uvažována třída SHA-2 [SHA-2]. Hašovací funkce této třídy však také mají všechny generické slabiny a navíc jejich návrhová kritéria nebyla nikdy publikována. Avšak i u této třídy hašovacích funkcí se začínají objevovat

útoky. Využívají slabých nelinearit v expanzi klíče a v použité blokové šifře ([HPR04], [SKH04], [YB05], [YBP05], [MPRR06a], [MPRR06b]).
Také praktická kryptoanalýza hašovacích funkcí v posledních letech velmi pokročila. Byly odhaleny závažné slabiny v řadě hašovacích funkcí ([WY05], [WYY05a], [WYY05b], [YWYP06], [BCJ05], [Kli06a]), zejména u MD5, SHA-0 a SHA-1 ([MD5], [SHA-0], [SHA-1]). Generické útoky na současné nejsilnější hašovací funkce ([Tsu92], [Jou04], [KS05]) a praktické útoky na funkce třídy MD a SHA ukázaly, že je potřeba navrhnout novou filozofii hašovacích funkcí ([Sch04]).
Konstrukce NMAC/HMAC navrhli v roce 1996 Bellare a kol. na CRYPTO 1996 [BCK96]. Coron a kol. [CDMP05] na CRYPTO 2005 zkoumali konstrukci typu NMAC se dvěma náhodnými orákuly a konstrukci typu HMAC s ideální blokovou šifrou v Davies-Meyerově úpravě. Dokázali, že se zvyšováním délky bloku se tyto konstrukce stávají neodlišitelné od náhodných orákul. V tomto příspěvku poprvé dokazujeme kvantitativní odhady odolnosti uvedených konstrukcí proti nalezení vzoru a kolize. Z Věty 1 až 4 vyplývá, že pro nalezení kolize NMAC/HMAC je útočník nucen vykonat řádově $2^{n/2}$ operací a pro nalezení vzoru NMAC/HMAC řádově 2^n operací, tedy stejně jako u náhodných orákul. Konstrukce NMAC/HMAC, které navrhli v roce 1996 Bellare a kol. [BCK96], se tak stávají prakticky i teoreticky podloženými kandidáty na hašovací funkce nové generace.
V současné době Bellare [Bel06] ukázal, že v konstrukci HMAC je dokonce možné zeslabit tradiční požadavky na kompresní funkci. Například k tomu, aby HMAC byla PRF postačuje, aby kompresní funkce byla PRF.
Protože funkce NMAC/HMAC jsou výpočetně odolné proti nalezení vzoru a kolize, nemusíme se obávat generických útoků, které objevili Joux a Kelsey-Schneier ([Jou04], [KS05]). Zbývajícím generickým útokem je útok rozšířením zprávy. V současné práci Gauravarama a kol. [GHA06] se takový útok ukazuje pro NMAC na základě pouze velmi vyumělkovaného tvaru jeho vnitřních funkcí.
Druhá část příspěvku se zabývá praktickou konstrukcí funkcí NMAC/HMAC a návrhem hašovací funkce SNMAC. Příčinou současných útoků na hašovací funkce tříd MD a SHA, včetně SHA-2, jsou slabé nelinearity v použité blokové šifře a její expanzi klíče. Aby se nové hašovací funkce vyhnuly moderním útokům ([KML02], [BDK03], [HKK03], [KKH04], [SKH04], [KKL04], [BDK05], [HKL05], [KBP05], [MPRR06a], [MPRR06b], [YWYP06], [BDK07]), měly by odstranit tyto slabě nelineární funkce ze svých návrhů a nahradit je současnou *technologií* blokových šifer [Bih05]. Technologií máme na mysli osvědčené principy a stavební bloky blokových šifer. Pokud tuto technologii použijeme, dostáváme hašovací funkci na obr. 1.



Obr. 1: Hašovací funkce na bázi technologie blokových šifer

Ukazujeme, že blokové šifry by měly být použity v hašovacích funkcích jiným způsobem než dosud. Nazýváme je speciální blokové šifry (SBŠ) a formulujeme jejich vlastnosti. Toto nové kryptografické primitivum se vymyká klasické představě blokových šifer. Základní vlastností SBŠ je, že útočník má plnou kontrolu nad jejím klíčem. S takovým požadavkem nebyly dosud blokové šifry konstruovány, a proto žádné současné blokové šifry nejsou příliš vhodné pro použití v hašovacích funkcích. Konstrukci blokové šifry, která bude použita v hašovacích funkcích, je nutné podřídit požadavku, že útočník má plnou kontrolu nejen nad otevřeným a šifrovým textem, ale i nad klíčem. Není to pouze teoretický koncept, praktický příklad SBŠ uvádíme v [Kli06b].

Důkazy bezpečnosti konstrukcí NMAC/HMAC jsou založeny na faktu, že f a g jsou nezávislá náhodná orákula v NMAC a E je ideální bloková šifra v HMAC. Pokud máme k dispozici speciální blokovou šifru, můžeme ji přímo použít jako náhodné orákulum v modelu NMAC (viz. obr. 3), který je obecnější než HMAC (viz obr. 4). Tuto konstrukci nazýváme SNMAC (Special NMAC) podle toho, že používá speciální blokovou šifru (SBC) v modelu NMAC. Poznamenejme, že model HMAC využívá klasickou blokovou šifru. Pokud bychom ji smysluplně přeměnili na speciální blokovou šifru, obdrželi bychom SNMAC také. Konstrukce SNMAC je tedy jakýmsi kompromisem mezi HMAC a NMAC. Dostaneme se k ní zdola "zesílením" HMAC (použitím speciální blokové šifry namísto klasické) nebo shora "zeslabením" NMAC (použitím speciální blokové šifry namísto náhodných orákul).

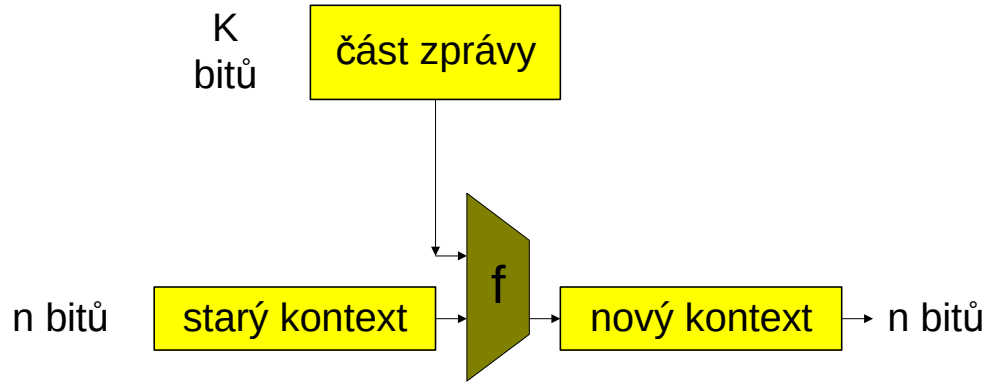
Navrhujeme koncept SNMAC jako kandidáta na hašovací funkci nové generace. Je výpočetně odolný proti nalezení vzoru a kolize, limitně se blíží náhodnému orákulu a umožňuje návrh různých instancí pomocí různých SBŠ.

SNMAC využívá speciální blokovou šifru zvláštním způsobem v kompresní funkci, a to podle vztahu $h_i = SBŠ_{hi-1 \parallel mi}(Const_0)$.Využívá faktu, že dlouhá desetiletí byly blokové šifry konstruovány tak, aby ze znalosti libovolného množství otevřeného a šifrového textu nebylo možné určit klíč. Tím se konstrukce SNMAC brání proti určení vzoru, neboť ten vstupuje do klíče SBŠ. Dále využívá vlastnosti, že při pevném otevřeném textu a proměnném klíči jsou šifrové texty náhodné a příslušné zobrazení je náhodné orákulum. Kompresní funkce je pak tímto náhodným orákulem.
Příspěvek má následující obsah. V kapitole 2 je uvedena definice NMAC a HMAC, v kapitole 3 hlavní věty o odolnosti NMAC a HMAC vůči nalezení vzoru a kolize. V kapitole 4 uvádíme koncept SBŠ a SNMAC. Konkrétní instance SBŠ a SNMAC je popsána v kapitole 5 a příspěvek uzavíráme v kapitole 6. Důkazy hlavních vět z kapitoly 3 lze nalézt v anglické verzi tohoto příspěvku [Kli06c] a definice funkcí DN a HDN v rozšířené verzi [Kli06b].

2. Definice NMAC a HMAC

Základní konstrukce. V praxi se setkáváme s nutností hašovat zprávy po částech. Například když z komunikačního kanálu dostáváme zprávu jako posloupnost a nemáme dostatek paměti na uložení celého proudu. Představme si hašovací funkci jako konečný automat. Po zpracování určité části zprávy dostáváme jako výsledek vnitřní stav tohoto automatu, který u hašovací funkce nazýváme kontext. Vstupem do dalšího kroku konečného automatu je tento kontext a další část zprávy. První kontext konečného automatu označujeme jako inicializační hodnota. Dostáváme tak základní model, využívající kompresní funkci f, viz obr. 2. Z přirozeného požadavku, aby kompresní funkce f byla definována pro konstantní šířku vstupu, dostáváme nutnost zarovnání zprávy a její dělení na stejné bloky. Tím obdržíme klasický Merkle-

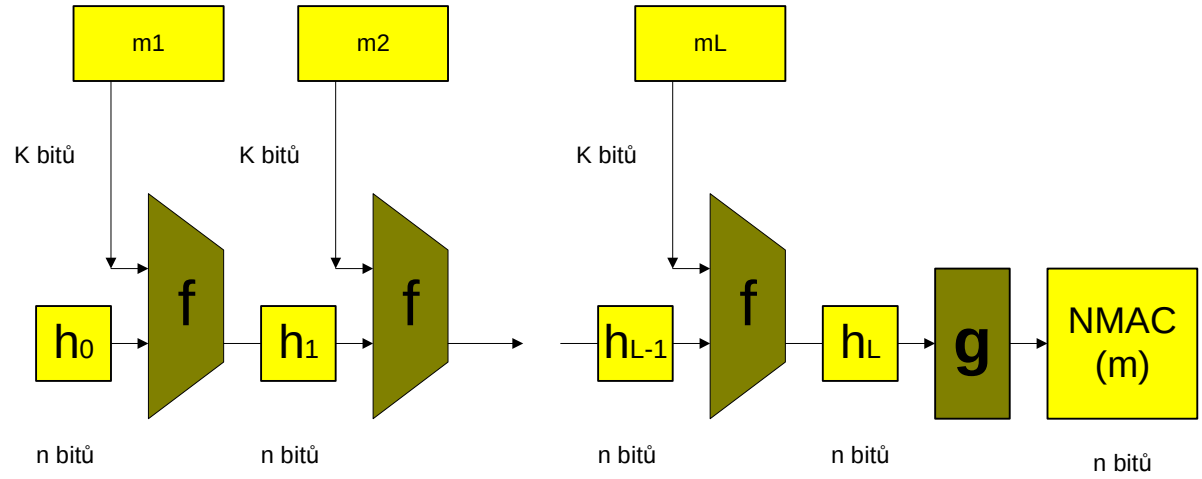
Damgardův model iterativní hašovací funkce, který je základem všech moderních hašovacích funkcí [Mer89][Dam89].



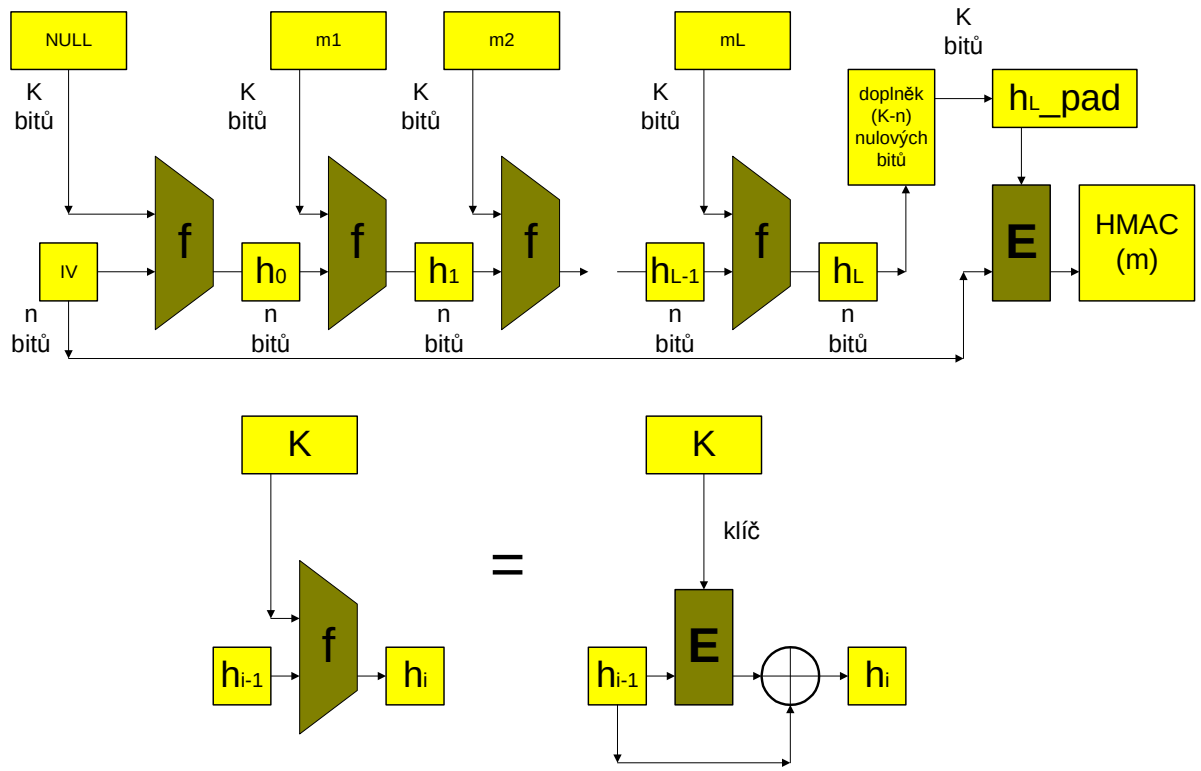
Obr.2: Iterativní hašovací funkce

Bohužel právě tento model má tři uvedené generické slabiny, a to nezávisle na tom, jaký je obsah kompresní funkce f. Zejména umožňuje nalézat multikolize a multivzory s menším úsilím než u náhodného orákula ([Jou04], [KS05]). Opustit velmi přirozenou konstrukci na bázi iterativního principu ([Mer89], [Dam89], [BCK96]) však nemůžeme. Proto se musíme smířit s tím, že hašovací funkce nové generace bude z teoretického hlediska náchylná k multikolizním útokům. Vhodnou obranou může být výpočetní složitost. Funkce musíme konstruovat tak, aby tyto útoky vyžadovaly příliš mnoho operací. V konstrukci na obr. 3 a 4 je použita závěrečná operace g. To je obrana proti třetímu generickému útoku - útoku prodloužením zprávy. Nezabrání mu teoreticky ale učiní jej velmi nepravděpodobným v praxi.

Protože funkce f a g jsou různé, nepůjde k tvorbě h(M || N) použít h(M) jednoduše. Výpočet h(M) končí operací g, zatímco při výpočtu h(M || N) je v příslušném místě použita operace f. Pokud použijeme dvě náhodná orákula f a g, dostáváme konstrukci NMAC (viz obr. 3) podle [BCK96], [CDMP05]. Pokud tato orákula konstruujeme pomocí blokové šifry například v Davies-Meyerově formě [MMO85], dostáváme konstrukci, kterou označujeme HMAC (viz obr. 4) podle [BCK96], [CDMP05]. Poznamenáváme, že se jedná formálně o mírně odlišnou definici HMAC, než která je standardizovaná například v [RFC2104].



Obr.3: Definice hašovací funkce NMAC (viz [BCK96], [CDMP05])



Obr.4: Definice hašovací funkce HMAC (viz [BCK96], [CDMP05])

U obou modelů HMAC a NMAC uvažujeme, že zpráva se standardně doplňuje (bitem 1, bity 0 a délkou původní zprávy) a zarovnává se na bloky stejné délky (K bitů) podobně jako u SHA-2.

3. Bezpečnost hašovacích funkcí HMAC a MAC

V této kapitole dokážeme věty o odolnosti HMAC a NMAC proti nalezení kolize a vzoru. Věty 1 až 4 obsahují kvantitativní odhady pravděpodobnosti nalezení kolize nebo vzoru v závislosti na počtu operací, které má útočník k dispozici. Obdržené odhady jsou velmi těsné, neboť dolní a horní meze jsou řádově stejné.

Z Věty 1 až 4 vyplývá, že pro nalezení kolize je jakýkoliv útočník nucen vykonat řádově $2^{n/2}$ operací a pro nalezení vzoru řádově 2^{n} operací, tedy hašovací funkce HMAC a NMAC se vůči němu v těchto případech chovají podobně jako náhodná orákula.

V dalším použijeme obvyklou definici black-box modelu blokové šifry podle [BRS02].

3.1 Věty o bezpečnosti HMAC

Označme BC(K, n) množinu všech blokových šifer E, které mají K bitový klíč a n bitový blok. Nechť E je náhodně vybraná bloková šifra z množiny BC(K, n), tj. $E \xleftarrow{\$} BC(K, n)$, kde symbol $\xleftarrow{\$}$ M označuje náhodný výběr objektu z množiny M.

Model black-boxu ([BRS02], str. 322). Tento model se připisuje Shannonovi a byl použit v pracích jako [W84], [KR96], [EM91]. Nechť K je pevná délka klíče a n délka bloku blokové šifry E. Útočník A má přístup k orákulům E a E^{-1}, kde E je náhodná bloková šifra E: $\{0, 1\}^{K}$ x

$\{0, 1\}^n \rightarrow \{0, 1\}^n$ a E^{-1} její inverze. To znamená, že pro každý klíč $k \in \{0, 1\}^K$ je $E_k = E(k, *)$ náhodně vybraná permutace na množině $\{0, 1\}^n$ a útočník má přístup k orákulům E a E^{-1}. Tohoto útočníka, tj. jakýkoliv algoritmus útoku, který má přístup k orákulům E nebo E^{-1}, označujeme $A\_E\_E^{-1}$. Poznamenejme, že pro vstup (k, y) orákulum E^{-1} vrací hodnotu x takovou, že $y = E_k(x)$. $A\_E\_E^{-1}(\sigma)$ označuje algoritmus, zvolený na základě parametru σ.

I když HMAC bude použita s $K \geq n$, některé důkazy níže platí i pro $K < n$. Při závěrečné úpravě u HMAC je proto potřeba vzniklou n-bitovou proměnnou h_L doplnit na K bitovou hodnotu. Tuto operaci značíme h_L_pad a označuje doplnění h_L o K - n nulových bitů.
Označme $HMAC^E$ hašovací funkci HMAC, založenou na blokové šifře E, viz obr. 4.

Konvence ([BRS02], str. 328). V dalším budeme uvažovat následující významné předpoklady. Za prvé, útočník se neptá orákula na žádnou otázku, na kterou již zná odpověď. Zejména když se A ptá na Ek(x) a obdrží odpověď y, pak se už neptá na $E_k(x)$ ani na $E^{-1}_k(y)$. Jestliže se A ptal na E^{-1}_k (y) a obdržel odpověď x, pak se už neptá na $E^{-1}_k(y)$ ani na $E_k(x)$.
Za druhé, když útočník hledající kolizi pro HMAC jako výstup předkládá M a M´, pak se předpokládá, že musel projít výpočtem HMAC(M) a HMAC(M´) v tom smyslu, že se musel zeptat na všechny hodnoty E (nebo E^{-1}), které jsou použité ve všech iteracích během výpočtu HMAC(M) a HMAC(M´). Podobně, když útočník hledající vzor HMAC jako výstup předkládá zprávu M, předpokládáme, že musel projít výpočtem HMAC(M), tj. musel zjistit všechny hodnoty E (nebo E^{-1}), které jsou použité ve všech iteracích během výpočtu HMAC(M).
Důkazy Vět 1 až 4 jsou uvedeny v Dodatku 1.

3.2 Odolnost HMAC proti nalezení vzoru

Věta 1: Odolnost HMAC proti nalezení vzoru.

Nechť $Pr\_E\_\sigma = Pr[E \xleftarrow{\$} BC(K, n); \sigma \xleftarrow{\$} \{0, 1\}^n; M \longleftarrow A\_E\_E^{-1}(\sigma): HMAC^E(M) = \sigma]$ je pravděpodobnost jevu, že pro nějakou náhodně vybranou hodnotu haše σ a náhodně vybranou blokovou šifru E útočník $A\_E\_E^{-1}$ pomocí algoritmu $A\_E\_E^{-1}(\sigma)$ získá hodnotu zprávy M, pro níž je $HMAC^E(M) = \sigma$, tj. nalezne vzor k dané haši. Označme $Adv\_inv\_HMAC[n](q) = Max \{Pr\_E\_\sigma\}$, kde maximum se bere přes všechny možné útočníky $A\_E\_E^{-1}(\sigma)$, používající dohromady nejvýše q volání orákula E nebo E^{-1}. Zvolme $n \in N$ a $K \geq n$. Potom pro libovolné $1 \leq q < 2^n$ platí

$$0.3 * q / 2^n \leq Adv\_inv\_HMAC[n](q) \leq 1.0 * q / 2^n.$$

3.3 Odolnost HMAC proti nalezení kolize

Věta 2: Odolnost HMAC proti nalezení kolize

Označme výhodu pro nalezení kolize jako reálné číslo

$Adv\_coll\_HMAC[n](A) = Pr[E \xleftarrow{\$} BC(K, n); (M, M') \xleftarrow{\$} A: M' \neq M \& HMAC^E(M) = HMAC^E(M')]$. Pro $1 \leq q$ definujeme $Adv\_coll\_HMAC[n](q) = Max \{Adv\_coll\_HMAC[n](A)\}$, kde maximum se bere přes všechny možné útočníky $A\_E\_E^{-1}$, používající dohromady nejvýše q volání orákula E nebo E^{-1}. Zvolme $n \in N$. Nechť $K \geq n \geq 3$. Potom pro libovolné $1 < q \leq 2^{n/2}$ platí

$$0.158 * q(q-2) / 2^n \leq Adv\_coll\_HMAC[n](q) \leq 1.5 * q(q-1) / 2^n.$$

3.4 Věty o bezpečnosti NMAC

Množinu všech náhodných orákul s p bitovým vstupem a q bitovým výstupem označujeme NO(p, q). NMAC definovanou výše pomocí orákul $f \in NO(K + n, n)$ a $g \in NO(n, n)$ označujeme jako $NMAC^{f,g}$, resp. krátce NMAC. Označením A_f_g značíme útočníka (jakýkoliv

algoritmus útoku), který má přístup k orákulům f a g. A_f_g(σ) označuje algoritmus, zvolený na základě parametru σ.

Konvence ([BRS02], str. 328). V případě NMAC budeme v dalším uvažovat následující významné předpoklady podobně jako u HMAC. Když útočník hledající kolizi NMAC jako výstup předkládá M a M´, pak se předpokládá, že musel projít výpočtem NMAC(M) a NMAC(M´) v tom smyslu, že se musel zeptat na všechny hodnoty f a g, které jsou použité ve všech iteracích během výpočtu NMAC(M) a NMAC(M´). Podobně, když útočník hledající vzor NMAC jako výstup předkládá zprávu M, předpokládáme, že musel projít výpočtem NMAC(M), tj. musel zjistit všechny hodnoty f a g, které jsou použité ve všech iteracích během výpočtu NMAC(M).

3.5 Odolnost NMAC proti nalezení vzoru

Věta 3: Odolnost NMAC proti nalezení vzoru

Nechť Pr_f_g_σ = Pr[f $\xleftarrow{\$}$ NO(K + n, n); g $\xleftarrow{\$}$ NO(n, n); σ $\xleftarrow{\$}$ {0,1}^{n}; M $\longleftarrow$ A_f_g(σ): NMAC(M) = σ] je pravděpodobnost jevu, že pro nějakou náhodně vybranou hodnotu haše σ a náhodně vybraná orákula f, g útočník A_f_g(σ) získá hodnotu zprávy M, pro níž je NMAC(M) = σ, tj. nalezne vzor k dané haši. Označme Adv_inv_NMAC[n](q) = Max {Pr_f_g_σ}, kde maximum se bere přes všechny možné algoritmy (útočníky) A_f_g, používající dohromady nejvýše q volání orákula f nebo g. Zvolme n ∈ N. Potom pro libovolné $1 \le q < 2^n$ platí

$$0.3 * q/2^n \le \text{Adv\_inv\_NMAC}[n](q) \le 1.0 * q/2^n.$$

3.6 Odolnost NMAC proti nalezení kolize

Věta 4. Odolnost NMAC proti nalezení kolize

Označme výhodu pro nalezení kolize jako reálné číslo Adv_coll_NMAC[n](A) = Pr[f $\xleftarrow{\$}$ NO(K + n, n); g $\xleftarrow{\$}$ NO(n, n); (M, M´) $\xleftarrow{\$}$ A: M´ ≠ M & NMAC(M) = NMAC(M´)]. Pro 1 ≤ q definujeme Adv_coll_NMAC[n](q) = Max { Adv_coll_NMAC[n](A) }, kde maximum se bere přes všechny možné algoritmy (útočníky) A_f_g, používající dohromady nejvýše q volání orákula f nebo g. Zvolme n ∈ N. Potom pro libovolné $1 < q \le 2^{n/2}$ platí

$$0.158 * q(q-2)/2^n \le \text{Adv\_coll\_NMAC}[n](q) \le 0.5 * q(q-1)/2^n.$$

4. Nový koncept SBŠ a SNMAC

V této kapitole zavedeme pojem speciální blokové šifry a na její bázi definujeme hašovací funkci (SNMAC).

Připomeňme, co způsobilo problémy současných hašovacích funkcí třídy MD a SHA:

- blokové šifry, použité v kompresních funkcích, zpracovávají klíč a otevřený text zásadně odlišně, umožňují vzájemné řízení změn jednoho vstupu pomocí druhého,
- dílčí funkce umožňují propagaci diferencí ze vstupů na výstupy,
- dílčí funkce jsou slabě nelineární, existují vysoce pravděpodobné lineární vztahy mezi jejich vstupy a výstupy.

Biham [Bih05] navrhl, aby se v hašovacích funkcích začala používat technologie blokových šifer. Máme na mysli takové stavební bloky, které jsou silně nelineární a odolné proti lineární a diferenciální kryptoanalýze.

Uvažujme tedy, že v kompresní funkci f, $h_i = f(h_{i-1}, m_i)$ jakýmkoliv způsobem, třeba i několikrát, použijeme blokovou šifru.

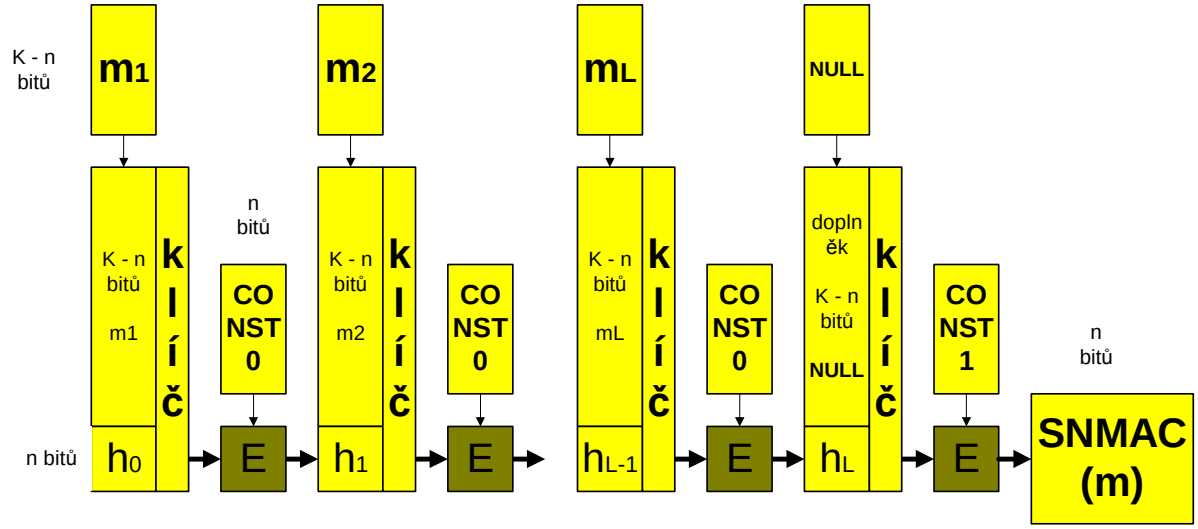
U současných útoků na hašovací funkce se v předpisu $h_i = f(h_{i-1}, m_i)$ vhodně mění současně h_{i-1} i m_i tak, aby vznikaly odpovídající diference v h_i. Protože funkci f realizuje nějaká bloková šifra a útočník může manipulovat všemi proměnnými, které do ní vstupují, může také manipulovat všemi proměnnými té blokové šifry. **U hašovacích funkcí tedy vzniká zvláštní situace, že útočník má možnost libovolně manipulovat otevřeným textem i klíčem použité blokové šifry**, a to nezávisle na tom, jakým způsobem je bloková šifra v hašovací funkci využita.

Způsobů použití blokových šifer pro konstrukce hašovacích funkcí byla studována celá řada. **Nikdy však nebyla klasická bloková šifra navrhována s předpokladem, že útočník bude mít možnost libovolně manipulovat s jejím klíčem.** Naopak, u většiny moderních šifer je klíč zpracováván slabšími funkcemi než datový vstup. Například u TripleDES je to lineární funkce, u AES slabě nelineární.

Homogenita. Aby nebylo možné využít ani slabin ve zpracování datového vstupu, ani ve zpracování klíče, požadujeme, aby u použité blokové šifry byly všechny proměnné bity zpracovány stejně kvalitně a podobným způsobem. Tuto vlastnost nazýváme homogenitou. Homogenitu požadujeme také u výstupních bitů použité blokové šifry. Příkladem homogenně zpracovaných vstupních i výstupních bitů může být náhodný substituční box (permutace), i když bity výstupu jsou značně odlišné funkce vstupních bitů. Klasické blokové šifry téměř nikdy nesplňují požadavek homogenity. U většiny moderních šifer je klíčový vstup zpracováván slabšími funkcemi než datový vstup. Na druhé straně jsou téměř vždy homogenně zpracovávána množina bitů klíče a množina bitů otevřeného textu každá zvlášť. Proto požadovanou homogenitu můžeme docílit tak, že buď klíč nebo otevřený text volíme konstantní, zbylý vstup bude zpracován homogenně.

Speciální bloková šifra (SBŠ) a speciální NMAC (SNMAC). Uvažujme, že vlastnost homogenity u blokové šifry (E), použité v kompresní funkci (f), splníme tím, že všechny proměnné vstupy kompresní funkce (tj. datový blok m_i a kontext h_{i-1}) vedeme jako proměnnou $X = h_{i-1} \| m_i$ do otevřeného textu a klíč volíme konstantní: $f(X) = E_{Const0}(X)$. Kompresní funkce f by měla být jednocestná, aby bránila nalézání vzoru hašovací funkce, což tato konstrukce nesplňuje. Na druhou stranu blokové šifry byly vyvíjeny desítky let tak, aby ze znalosti šifrového a otevřeného textu nešel určit klíč, tj. zajišťují jednocestnost vzhledem ke klíči. Využijeme-li tohoto faktu, dostáváme konstrukci kompresní funkce přirozeně jako $f(X) = E_X(Const_0)$, tedy všechny proměnné bity vedou do klíče blokové šifry, a ta je použita pouze s konstantním otevřeným textem. Proto se dále budeme zabývat jen konstrukcí $f(X) = E_X(Const_0)$. V tomto případě E nazýváme speciální blokovou šifrou. Tento název si E určitě zaslouží, protože je použita pouze se dvěma různými konstantními otevřenými texty - $Const_0$ pro orákulum f a $Const_1$ pro orákulum g. Nyní můžeme definovat hašovací funkci SNMAC na bázi NMAC a SBŠ tak, jak ilustruje obr. 5.

Pojem SBŠ je nový a jeho definice se určitě bude ještě vyvíjet. Pro důkazy bezpečnosti konstrukce SNMAC budeme potřebujeme vlastnost, aby při pevném otevřeném textu ($Const_0$ a $Const_1$) byly $E: \{0, 1\}^K \times Const_0 \rightarrow \{0, 1\}^n : (k, Const_0) \rightarrow y = E_k(Const_0) = f(k)$ a $E: \{0, 1\}^K \times Const_1 \rightarrow \{0, 1\}^n : (k, Const_1) \rightarrow y = E_k(Const_1) = g(k)$ náhodná orákula vzhledem k proměnnému klíči. Aby f, g byly kvalitní funkce při libovolné volbě konstant $Const_0$ a $Const_1$, budeme požadovat, aby $E: \{0, 1\}^K \times \{0, 1\}^n \rightarrow \{0, 1\}^n : (k, x) \rightarrow y = E_k(x)$ byla kvalitní bloková šifra jakožto celé zobrazení s proměnným klíčem i proměnným otevřeným textem.



Obr. 5: Definice SNMAC, založená na SBŠ a NMAC

Všechny diferenční a lineární útoky, které jsou úspěšné u hašovacích funkcí, se u SBŠ převádí na diferenční a lineární útoky s využitím klíče. Proto na rozdíl od běžných blokových šifer bude od speciální blokové šifry požadováno, aby byla odolná proti různým diferenčním a lineárním útokům, vedeným zejména z klíčového vstupu. Požadavek můžeme rozšířit i na datový vstup (jako by byl proměnný) a na kombinaci datového a klíčového vstupu.

Požadujeme tedy, aby mezi proměnnými (k, x) a $y = E_k(x)$ neexistovaly žádné diferenční a lineární vztahy s využitelnou pravděpodobností. Jinými slovy, požadavky na SBŠ jsou stejné jako na klasickou blokovou šifru a navíc se požaduje silnější zpracování klíče. Klíč by měl být u SBC zpracováván se stejnou kryptografickou kvalitou Zpracování klíče by mělo být na stejné úrovni, jako je zpracováván otevřený text u klasických blokových šifer. Co tedy víme o SBŠ:
Speciální bloková šifra E:

- zpracovává klíč na stejné úrovni kvality jako datový vstup,
- zpracovává všechny bity klíče stejně kvalitně (homogenně),
- na rozdíl od klasických blokových šifer bude přirozené použít délku klíče obvykle mnohonásobně delší než délku bloku, například K = 4096, resp. 8192 a n = 256, resp. 512,
- je konstruována pomocí technologie blokových šifer,
- není primárně určena k šifrování dat,
- je použita v hašovací funkci s konstantním otevřeným textem, veškerá proměnná vstupuje do E prostřednictvím klíče,
- když uvažujeme, že má také proměnný otevřený text, měla by to být kryptograficky silná klasická bloková šifra,
- útočník může libovolně manipulovat s klíčem.

Definice SBŠ není uzavřena a musí se ještě dále zkoumat.

Definice. Hašovací funkce SNMAC. Hašovací funkce SNMAC je iterativní hašovací funkce typu NMAC ([BCK96], [CDMP05]), která využívá speciální blokovou šifru E s n bitovým blokem a K-bitovým klíčem. Má kompresní funkci f a závěrečnou úpravu g, kde
$f: \{0, 1\}^K \rightarrow \{0, 1\}^n : X \rightarrow E_X(Const_0)$,
$g: \{0, 1\}^n \rightarrow \{0, 1\}^n : X \rightarrow E_{X \,\|\, NULL}(Const_1)$,
$K \geq n$, $Const_0$ a $Const_1$ jsou různé konstanty a NULL je řetězec K - n nulových bitů.

Hašování zprávy m má tři kroky.

Krok 1. Doplnění
Zprávu m, kterou hašujeme, nejprve doplníme bitem 1, nejmenším (i nulovým) počtem bitů 0 a 128bitovým číslem (které vyjadřuje délku m v bitech) tak, aby její délka byla L násobkem čísla K - n, kde L je přirozené číslo. Tuto doplněnou zprávu rozdělíme na L bloků o délce K - n bitů, $m = m_1 \| ... \| m_{L-1} \| m_L$.
Definujeme (viz obr. 5) h_0 jako konstantu (inicializační hodnota)

Krok 2. Iterace
$h_i = f(h_{i-1} \| m_i)$, i = 1, ..., L,

Krok 3. Závěrečná úprava
$SNMAC(m) = g(h_L)$.

Cíl útočníka. U klasických blokových šifer byl hlavním cílem útočníka klíč. U speciální blokové šifry může útočník s klíčem dokonce libovolně manipulovat. Vzniká otázka, co je nyní jeho cílem. Protože hašovací funkce SNMAC je založena na SBŠ, jeho cílem bude zejména nalézt vzor nebo kolizi SBŠ. Obecněji bude jeho cílem možnost jakýmkoliv způsobem řídit vztah mezi vstupem a výstupem SBŠ, což by mohlo vést k nalezení vlastností odlišujících hašovací funkci od náhodného orákula.
Blokovou šifru tak, jak ji dnes známe, budeme muset upravit. Libovolná manipulovatelnost s klíčem je pro současné blokové šifry naprosto nepřirozený požadavek, na který nejsou připraveny, a nemají proto k tomu vystavěna obranná opatření. Příprava klíče je většinou slabá, neporovnatelná se zpracováním otevřeného textu. Proto zpracování klíče musí být u SBŠ zesíleno na úroveň zpracování otevřeného textu v současných blokových šifrách.

Proč není vhodné použít kvalitní klasickou blokovou šifru pro konstrukci hašovací funkce?
Z práce Corona a kol. [CDMP05] a důkazů z kapitoly 2 vyplývá, že konstrukce NMAC a HMAC jsou výpočetně bezpečné proti excesům typu kolize a nalezení vzoru. Nestačilo by proto například použít kvalitní klasickou blokovou šifru v konstrukci HMAC? Odpověď je záporná. Nevýhodou všech současných blokových šifer je, že zpracovávají klíč a datový vstup různým způsobem, nehomogenně a s různou kryptografickou silou. Tato nehomogenita byla využita k útokům na blokové šifry i k útokům na hašovací funkce (viz například [BDK03], [BDK05], [HKL05], [KBP05], [KHL04], [KKH04], [KLS04], [KML02], [SKH04], [Kli06a], [YWYP06] a nejnověji [BDK07]). Ze současných útoků na hašovací funkce vyplývá, že hodnoty vstupních dat a kontextu jsou stejně kryptograficky cenné, a proto by měly být zpracovány homogenně (stejně kvalitně). Tuto vlastnost nemá žádná současná bloková šifra. Stejně tak žádná současná bloková šifra nebyla konstruována s předpokladem, že útočník bude mít plnou kontrolu nad klíčem. Konstrukce SBŠ bude proto odlišná od klasických blokových šifer, i když může využívat jejich osvědčené stavební prvky.

5. Konkrétní instance SBŠ a SNMAC

Konstrukce SNMAC na bázi SBŠ je obecná a umožňuje využívat různé instance SBŠ. Jako konkrétní instanci SBŠ jsme navrhli algoritmus DN (Double Net) a s jeho využitím jsme obdrželi hašovací funkci HDN (Hash Double Net). Popisy DN a HDN jsou uvedeny v dodatcích 2 a 3. Jejich zdrojové kódy, testovací příklady apod. budou k dispozici po schválení jejich publikace na [Kli06b].

DN má délku klíče 8192 bitů a délku bloku 512 bitů. HDN má 512bitový kód a dosahuje rychlosti hašování 3 - 4x nižší než SHA-512.
Nižší rychlost hašování HDN oproti SHA-512 je pochopitelná po porovnání obou funkcí. SHA-512 používá slabší vnitřní nelineární funkce, zatímco HDN používá technologii blokových šifer a je bezpečnostně naddimenzovaná.

6. Závěr

Generické problémy hašovacích funkcí vyvolaly potřebu nového návrhu konceptu hašovacích funkcí. Nové důkazy bezpečnosti však umožňují využít konstrukci NMAC/HMAC, navrženou Bellare a kol. v roce 1996 [BCK96]. V tomto příspěvku poprvé dokazujeme kvantitativní odhady odolnosti těchto konstrukcí proti nalezení vzoru a kolize. Odtud vyplývá, že jsou výpočetně odolné i proti nalezení multivzorů a multikolizí. Coron a kol. [CDMP05] na CRYPTO 2005 ukázali, že NMAC/HMAC se limitně blíží k náhodnému orákulu. To spolu se zde předloženými kvantitativními důkazy dává velmi dobré záruky bezpečnosti těchto konstrukcí.

Druhá část příspěvku se zabývá praktickou konstrukcí funkcí NMAC/HMAC a návrhem hašovací funkce SNMAC na bázi blokové šifry. Ukazujeme, že blokové šifry by měly být použity v hašovacích funkcích jiným způsobem než dosud. Nazýváme je speciální blokové šifry (SBŠ) a formulujeme jejich vlastnosti. Toto nové kryptografické primitivum se vymyká klasické představě blokových šifer. Základní vlastností SBŠ je, že útočník má plnou kontrolu nad jejím klíčem. Proti takovému požadavku nebyly dosud blokové šifry konstruovány, a proto žádné současné blokové šifry nejsou příliš vhodné pro použití v hašovacích funkcích. Konkrétní příklad SBŠ je uveden v [Kli06b].

Navrhujeme novou třídu hašovacích funkcí SNMAC jako konstrukci typu NMAC s využitím speciální blokové šifry. Tento koncept může být kandidátem na hašovací funkce nové generace. Má dokazatelnou výpočetní odolnost proti nalezení vzoru a kolize, limitně se blíží náhodnému orákulu a umožňuje návrh různých instancí pomocí různých SBŠ.

Jako příklad také navrhujeme speciální blokovou šifru DN (Double Net) a definujeme hašovací funkci HDN (Hash Double Net) jako konstrukci SNMAC na bázi DN.

Poděkování.
Autor děkuje Tomáši Rosovi za mnoho užitečných připomínek k předchozím verzím příspěvku.

7. Literatura

[BCK96] M. Bellare, R. Canetti and H. Krawczyk. Keying hash functions for message authentication. Advances in Cryptology – CRYPTO ’96, Lecture Notes in Computer Science Vol. 1109, pp. 1-15, Springer-Verlag, 1996.

[Bel06] M. Bellare. New Proofs for NMAC and HMAC: Security without Collision-Resistance. To be published, Advances in Cryptology – CRYPTO ’06, Lecture Notes in Computer Science Vol. 4117, Springer-Verlag, 2006, Cryptology ePrint Archive, Report 2006/043.

[BCJ05] E. Biham, R. Chen, A. Joux, P. Carribault, Ch. Lemuet and W. Jalby. Collisions of SHA-0 and Reduced SHA-1. Advances in Cryptology –EUROCRYPT 2005, Lecture Notes in Computer Science Vol. 3494, pp. 36–57, Springer-Verlag, 2005.

[BDK03] E. Biham, O. Dunkelman, and N. Keller. Rectangle Attacks on 49-Round SHACAL-1, FSE 2003, Lecture Notes in Computer Science Vol. 2887, pp. 22-35, Springer-Verlag, 2003.

[BDK05] E. Biham, O. Dunkelman, and N. Keller. Related-Key Boomerang and Rectangle Attacks, Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science Vol. 3494, pp. 507–525, Springer-Verlag, 2005.

[BDK07] E. Biham, O. Dunkelman, and N. Keller. A Simple Related-Key Attack on the Full SHACAL-1, to be published, CT-RSA 2007, RSA Conference 2007, Cryptographers' Track, February 5-9, 2007, Moscone Center, San Francisco, USA.

[Bih05] E. Biham: Recent advances in hash functions and the way to go, Conference on Hash Functions (Ecrypt Network of Excellence in Cryptology), June 23-24, 2005, Przegorzaly (Krakow), Poland, http://www.ecrypt.eu.org/stvl/hfw/Biham.ps.

[BRS02] J. Black, P. Rogaway, T. Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science Vol. 2442, pp. 320-335, Springer-Verlag, 2002. Extended version: Cryptology ePrint Archive, Report 2002/066, http://eprint.iacr.org/2002/066.

[CDMP05] J. S. Coron, Y. Dodis, C. Malinaud and P. Puniya. Merkle-Damgard Revisited: how to construct a hash-function. Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science Vol. 3621, pp. 430 - 448, Springer-Verlag, 2005.

[Dam89] I. Damgard. A Design Principle for Hash Functions. Advances in Cryptology - CRYPTO 1989, Lecture Notes in Computer Science Vol. 435, pp. 416–427, Springer-Verlag, 1990.

[EM91] S. Even and Y. Mansour. A construction of a cipher from a single pseudorandom permutation. In Advances in Cryptology – ASIACRYPT '91, Lecture Notes in Computer Science Vol. 739, pp. 210–224. Springer-Verlag, 1992.

[GHA06] P. Gauravaram, S. Hirose and S. Annadurai. An Update on the analysis and design of NMAC and HMAC functions. To be published in International Journal of Network Security

[HPR04] P. Hawkes, M. Paddon, and G. G. Rose. On Corrective Patterns for the SHA-2 Family. Cryptology ePrint Archive, Report 2004/207, 2004.

[HKK03] S. Hong, J. Kim, G. Kim, J. Sung, C. Lee and S. Lee. Impossible Differential Attack on 30-Round SHACAL-2, INDOCRYT 2003, Lecture Notes in Computer Science Vol. 2904, pp. 97-106, Springer-Verlag, 2003.

[HKL05] S. Hong, J. Kim, S. Lee and B. Preneel. Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192, FSE 2005, Lecture Notes in Computer Science Vol. 3557, pp. 368–383, Springer-Verlag, 2005.

[Jou04] A. Joux. Multicollisions in Iterated Hash Functions. Advances in Cryptology - CRYPTO 2004, Lecture Notes in Computer Science Vol. 3152, pp. 306–316, Springer-Verlag, 2004.

[KML02] J. Kim, D. Moon, W. Lee, S. Hong, S. Lee, and S. Jung. Amplified Boomerang Attack against Reduced-Round SHACAL, Advances in Cryptology - ASIACRYPT 2002, Lecture Notes in Computer Science Vol. 2501, pp. 243 - 253, Springer-Verlag, 2002.

[KBP05] J. Kim, A. Biryukov, B. Preneel, and S. Lee. On the Security of Encryption Modes of MD4, MD5 and HAVAL, ICICS 2005, Lecture Notes in Computer Science Vol. 3783, pp. 147-158, Springer-Verlag, 2005.

[KK05] J. Kelsey and T. Kohno.Herding Hash Functions and the Nostradamus Attack, Cryptographic Hash Workshop, held in NIST, Gaithersburg, Maryland, 2005, IACR Cryptology ePrint Archive, Report 2005/281, 2005.

[KKH04] J. Kim, G. Kim, S. Hong, S. Lee and D. Hong.The Related-Key Rectangle Attack-Application to SHACAL-1, ACISP 2004, Lecture Notes in Computer Science Vol. 3108, pp. 123-136, Springer-Verlag, 2004.

[KKL04] J. Kim, G. Kim, S. Lee, J. Lim and J. Song. Related-Key Attacks on Reduced Rounds of SHACAL-2, INDOCRYPT 2004, Lecture Notes in Computer Science Vol. 3348, pp. 36 - 44, Springer-Verlag, 2004.

[Kli06a] V. Klima. Tunnels in Hash Functions: MD5 Collisions Within a Minute, Cryptology ePrint Archive, Report 2006/105, 18 March, 2006.

[Kli06b] SNMAC homepage http://cryptography.hyperlink.cz/SNMAC/SNMAC.html

[Kli06c] V. Klima. A New Concept of Hash Functions SNMAC Using a Special Block Cipher and NMAC/HMAC Constructions, Cryptology ePrint Archive, Report 2006/376, October 2006., http://eprint.iacr.org/2006/376.pdf

[Kli06d] Vlastimil Klíma: Zcela nový koncept hašovacích funkcí, root.cz, 13.11.2006, http://www.root.cz/clanky/vlastimil-klima-zcela-novy-koncept-hasovacich-funkci/

[KLS04] J. Kim, G. Kim, S. Lee, J. Lim and J. Song. Related-Key Attacks on Reduced Rounds of SHACAL-2, INDOCRYPT 2004, Lecture Notes in Computer Science Vol. 3348, pp. 36 - 44, Springer-Verlag, 2004.

[KML02] J. Kim, D. Moon, W. Lee, S. Hong, S. Lee, and S. Jung. Amplified Boomerang Attack against Reduced-Round SHACAL, Advances in Cryptology - ASIACRYPT 2002, Lecture Notes in Computer Science Vol. 2501, pp. 243 - 253, Springer-Verlag, 2002.

[KR96] J. Kilian and P. Rogaway. How to protect DES against exhaustive key search. Journal of Cryptology, 14(1):17–35, 2001. Earlier version in CRYPTO ’96.

[KS05] J. Kelsey and B. Schneier. Second Preimages on n-Bit Hash Functions for Much Less than 2^n. Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science Vol. 3494, pp. 474–490, Springer-Verlag, 2005.

[MD5] R. Rivest. The MD5 message-digest algorithm, Internet RFC 1321, April 1992.

[Mer89] R. C. Merkle. One Way Hash Functions and DES. Advances in Cryptology - CRYPTO 1989, Lecture Notes in Computer Science Vol. 435, pp. 428–446, Springer-Verlag, 1990.

[MMO85] S. M. Matyas, C. H. Meyer and J. Oseas. Generating strong one-way functions with cryptographic algorithm. IBM Techn. Disclosure Bull., Vol. 27, No. 10A, 1985, pp. 5658 - 5659.

[MPRR06a] F. Mendel, N.Pramstaller, C.Rechberger, and V.Rijmen. Analysis of Step-Reduced SHA-256, to be published, FSE 2006

[MPRR06b] F.Mendel, N.Pramstaller, C.Rechberger, and V.Rijmen. The Impact of Carries on the Complexity of Collision Attacks on SHA-1, to be published, FSE 2006

[S49] C. Shannon. Communication theory of secrecy systems. Bell Systems Technical Journal, 28(4):656–715, 1949.

[Sch04] B. Schneier. Cryptanalysis of MD5 and SHA. Crypto-Gram Newsletter, September 2004, http://www.schneier.com/crypto-gram-0409.html#3

[SHA-0] National Institute of Standards and Technology. Secure hash standard. Federal Information Processing Standard, FIPS PUB 180, May 1993.

[SHA-1] National Institute of Standards and Technology. Secure hash standard. Federal Information Processing Standard, FIPS PUB 180-1, April 1995.

[SHA-2] National Institute of Standards and Technology. Secure hash standard. Federal Information Processing Standard, FIPS PUB 180-2, August 2000.

[SKH04] Y. Shin, J. Kim, G. Kim, S. Hong and S. Lee. Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2, ACISP 2004, Lecture Notes in Computer Science Vol. 3108, pp. 110–122. , Springer-Verlag, 2004.

[Tsu92] G. Tsudik. Message authentication with one-way hash functions. ACM Computer Communications Review, 22(5):29-38, 1992.

[W84] R. Winternitz. A secure one-way hash function built from DES. In Proceedings of the IEEE Symposium on Information Security and Privacy, pp. 88–90. IEEE Press, 1984.

[WY05] X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science Vol. 3494, pp. 19–35, Springer-Verlag, 2005.

[WYY05a] X. Wang, H. Yu and Y. L. Yin. Efficient Collision Search Attacks on SHA-0. Advances in Cryptology - CRYPTO ’05, Lecture Notes in Computer Science Vol. 3621, pp. 1–16, Springer-Verlag, 2005.

[WYY05b] X. Wang, Y. L. Yin and H. Yu. Finding collisions in the full SHA-1. Advances in Cryptology - CRYPTO ’05, Lecture Notes in Computer Science Vol. 3621, pp. 17–36, Springer-Verlag, 2005.

[YB05] H. Yoshida and A. Biryukov. Analysis of a SHA-256 Variant, SAC 2005, Lecture Notes in Computer Science Vol. 3897, pp. 245 – 260, Springer-Verlag, 2005.

[YBP05] H. Yoshida, A. Biryukov, and B. Preneel. Some applications of the Biham-Chen attack to SHA-like hash functions, CRYPTOGRAPHIC HASH WORKSHOP, NIST, Gaithersburg, Maryland, USA, October 31 - November 1, 2005, http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Yoshida_cameraNistHash.pdf

[YWYP06] H.Yu, X.Wang, A.Yun and S. Park. Cryptanalysis of the Full HAVAL with 4 and 5 Passes. To be published, FSE 2006.

C. Elektronické cestovní doklady, část 2

Ing. Luděk Rašek, Logica CMG, (ludek.rasek@logicacmg.com)

3. Testy interoperability

Pro úspěšné nasazení e-pasů v celosvětovém měřítku je zásadní schopnost plné interoperability e-pasů nejrůznějších výrobců HW i SW se čtecími zařízeními a inspekčními systémy. Z tohoto důvodu se v Berlíně uskutečnil celosvětový test interoperability. Zde uvedeme stručnou sumarizaci některých výsledků:

- bylo testováno 47 typů čteček od 37 výrobců
- celkem bylo zkoumáno 443 e-pasů, z toho 423 s BAC a 161 s AA
- algoritmus podpisu je u 37 pasů založen na EC a u 404 pasů na RSA
- algoritmus otisku je 289 x SHA1, 142 x SHA256, 10 x SHA512
- formát fotografií byl 302 x JPEG a 132 x JPEG2000
- doba čtení pasu byla průměrně 5.8s; u pasů s BAC 5.7s; u pasů s AA 6.3s

Podrobné výsledky testů lze najít na webových stránkách věnovaných této události [Berlin Interop].

4. Budoucnost - otisky prstů v roce 2009

Dle rozhodnutí komise EU [EU Otisky] se od 28.6.2009 musí země EU vydávat pasy vybavené otisky prstů. Vložení otisků prstů vnáší do pasu daleko citlivější osobní údaj, než jakým je obličej. Úspěšnost rozpoznávání obličeje a jednoznačnost sejmuté fotografie je v porovnání s otisky prstů nižší. Otisky prstů identifikují jednoznačně jejich nositele, nelze je vyměnit a proto je jejich utajení velice citlivé. Před uvedením otisků prstů nejsou v e-pasu v podstatě žádné nové údaje proti dosavadním zvyklostem (obraz obličeje je v pasech od jejich samého počátku).

Zavedení otisků prstů proto vyžaduje zvýšení ochrany dat v pasu uložených. Mechanismu vyššího zabezpečení se ve specifikacích ICAO nazývá Extended Access Control (EAC) a není v těchto specifikacích popsán. Velkou aktivitu na tomto poli vyvíjí německý BSI a jejím výsledkem je návrh pro realizaci EAC v dokumentu [EAC TR]

4.1. Bezpečnost

Pro zavádění otisků prstů bylo vytyčeno několik požadavků:

- lepší ochrana soukromí držitelů pasů než BAC (bezpečný kanál pro přenos dat mezi čtečkou a pasem),
- vylepšení ochrany před kopírováním a odstranění challenge semantic
- ochrana soukromí držitelů pasů nastavením přístupových oprávnění pro čtení daktyloskopických údajů

Ochrana proti kopírování pasu se nazývá Chip authentication (CA). Pro zjištění, zda terminál může či nemůže číst (či dokonce zapisovat) citlivá data se využívá Terminal authentication (TA). Kombinace těchto metod se nazývá Extended Access Control (EAC) a je specifikována v [EAC TR].

4.1.1. Chip authentication (CA)

Mechanismus CA je založený na algoritmu Diffie-Hellman (dále DH). DH čísla jsou do čipu staticky vložena při jeho personalizaci. Naopak terminál používá dočasná DH čísla. Na základě výměny DH čísel dojde k ustanovení sdíleného tajemství, z něhož se odvodí klíče pro kryptografickou ochranu následující komunikace.

Soukromé DH číslo čipu je uloženo v neadresovatelné části čipu. Veřejné DH číslo čipu je uloženo v souboru DG14 a je tedy i podepsáno v rámci struktury LDSSecurityObject. Pokud veřejné DH číslo je shodné s obsahem souboru DG14 a zároveň čip rozumí komunikaci chráněné na základě sdíleného tajemství, prokazuje tak držení soukromého DH čísla příslušného k veřejnému DH číslu uloženém v souboru DG14 a tedy prokazuje, že čip nebyl zkopírován.

Důkaz původu čipu (pasu) je v podstatě vedlejším efektem vytvoření bezpečného komunikačního kanálu. Po CA již čip a čtečka komunikují s využitím secure messagingu s využitím kryptograficky silného klíče (v porovnání s BAC).

4.1.2. Terminal authentication (TA)

Vydávající státy v rámci ochrany osobních údajů svých občanů (držitelů pasu) musí mít možnost řídit, která organizace či stát má právo citlivá biometrická data číst a která ne. Za tímto účelem umožní čip v pasu přečtení citlivých dat pouze zařízením, která prokáží, že jsou k tomu oprávněna (obdobný postup je využit u platebních karet, kdy karta umožní transakci pouze autorizovaným platebním terminálům). Zařízení prokazuje svá oprávnění opět s využitím asymetrické kryptografie. Každé zařízení, které chce číst citlivá data z čipu, je vybaveno asymetrickým klíčovým párem a v rámci komunikace prokáže, že vlastní privátní klíč odpovídající klíči veřejnému, který byl zaslán do čipu. Jakmile jednou terminál prokáže, že vlastní odpovídající privátní klíč k předloženému veřejnému, musí čip nějak poznat, že zařízení vybavené tímto klíčovým párem je oprávněno číst citlivá data. Ve světě "velkých" počítačů se k přiřazení konkrétní identity k subjektu reprezentovanému párem klíčů využívá X.509 certifikátů. Někdy jsou v těchto certifikátech umístěny rovněž informace o přístupových oprávněních (např. certifikáty vydávané Microsoft CA mohou obsahovat seznam rolí uživatele v doméně).

X.509 certifikáty jsou pro využití v omezeném výpočetním prostředí čipu příliš komplikované. Pro potřeby čipových karet byla proto definována zjednodušená specifikace tzv. card verifiable certificate. V podstatě se jedná o datovou strukturu nesoucí podobné informace, které nese X.509 certifikát:

- CV Certificate
  - Certificate body
    - Certificate profile identifier - verze (=0)
    - Certificate authority reference - max. 16znakový (ISO 8859-1) identifikátor autority sestavený z kódu země, jména autority a ID klíče (např. CZ-CVCA-01)
    - Public key - hodnota veřejného klíče dle algoritmu
    - Certificate holder reference - max. 16znakový (ISO 8859-1) identifikátor držitele sestavený z kódu země, jména držitele a ID klíče (např. CZ-CPP-01)

- Certificate holder authorization - zakódovaná role (oprávnění) držitele certifikátu (viz níže)
- Certificate effective date - začátek platnosti certifikátu ve formátu YYMMDD kódované v BCD v zóně GMT
- Certificate expiration date - konec platnosti certifikátu ve formátu YYMMDD kódované v BCD v zóně GMT

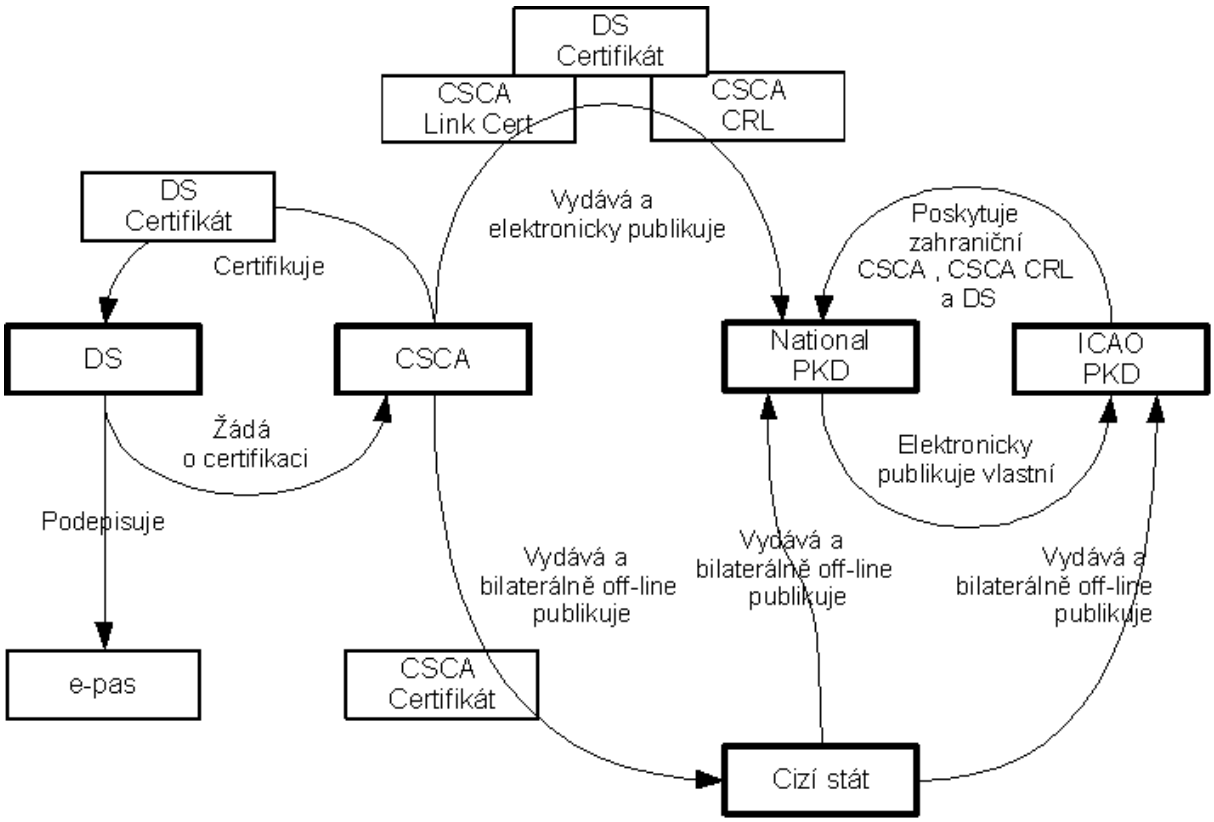
o Signature - vypočtena z Certificate body

Takto zjednodušený certifikát odešle inspekční terminál do čipu a ten ho ověří vůči klíčům, které má uloženy. Pokud ověření uspěje, jsou terminálu přidělena oprávnění dle nastavení čipu a hodnoty v položce holder authorization (viz níže).

Pro vysvětlení autorizací je nejprve potřeba zmínit, jak vypadají hierarchie certifikátů.

4.2. PKI pro kontrolu e-pasů

Celé PKI pro ověřování dokladů je postaveno na tzv. card verifiable certifikátech (nikoli na X.509 certifikátech). Hierarchie certifikátů je navržena tak, aby byla co nejvíce flexibilní (pro úkoly, které má plnit). Celá hierarchie vychází z toho, že čip v pasu důvěřuje pouze zařízením, která prokáží, že jejich klíč (nepřímo s využitím DV) certifikovala CVCA, jejíž certifikát (klíč) má čip uložen uvnitř své bezpečné paměti.



4.2.1. Country Verification Certifiation Authority (CVCA)

Každý stát provozuje (přímo či prostřednictvím pověřené organizace) alespoň jeden subjekt ověřující pravost dokladů (CVCA), který spravuje množinu povolených kontrolních systému (document verifier - DV). Certifikát CVCA se vydává na dobu 6 měsíců (minimum) až 3 roků (maximum). CVCA je povinno zpracovat žádost o vydání certifikátu pro DV do 72 hodin (ověří správnost žádosti) a následně vydat certifikát do 24 hodin. CVCA vypracuje a zveřejní pravidla vydávání certifikátů DV, aby cizí státy požadující certifikaci svých inspekčních systému věděli, jak postupovat.

Jak je vidět, maximální platnost CVCA certifikátu je kratší, než typická doba platnosti e-pasu (10 let). Z tohoto důvodu je při obnově klíče CVCA nutno vygenerovat tzv. link certifikát. Tento certifikát je pak distribuován všude tam, kde je třeba používat TA a do čipu se pak při autentizaci terminálu posílá celý řetěz: CVCA Link1 - CVCA Link2 - ... CVCALinkN - DVCert - ISCert. V čipu je uložen prvotní CVCA klíč a klíče link certifikátů a je možno celý řetěz ověřit přímo v čipu. Certifikát DV a IS se posílá do čipu při každé autentizaci, klíče certifikátů CVCA by měly být v čipu uloženy.

Doba překryvu platnosti starého a nového certifikátu by měla být minimalizována. Délka doby překryvu vychází z času potřebného pro distribuci nového certifikátu na všechna inspekční místa.

Primárním komunikačním kanálem pro komunikaci s CVCA je e-mail (mohou být i jiné). Pro výměnu dat v e-mail rámci zpráv musí být použito formátu MIME. Odesílatel by měl ve zprávě formulovat požadavek na doručenku (dle odpovídajících standardů). Pokud doručenka nedorazí v předpokládané době, může odesílatel komunikaci opakovat.

Ve standardu není explicitně uvedeno, zda a jak má být komunikace chráněna, ale vzhledem k její citlivosti by autor doporučoval ochranu S/MIME s využitím elektronického podpisu (kritická je integrita a původ zpráv, nikoli utajení jejich obsahu) zejména pro zprávy Register a DV certification request pro prvotní certifikát DV.

4.2.2. Document Verifier (DV)

Každý stát určí alespoň jeden subjekt pověřený ověřováním dokladů (DV), který bude spravovat množinu povolených inspekčních systémů (IS). DV žádá o certifikaci svého klíče u CVCA. Formátem žádosti je tzv. self-signed certifikát. CVCA vydává card verifiable certifikát a naplní jeho položku Certificate holder authorization podle toho, kdo o certifikát žádá. CVCA tedy musí mít implementován systém, kde bude definováno jak se prokazuje skutečnost, že daná žádost pochází od konkrétního subjektu, který je oprávněn číst citlivá data z pasu. Dále CVCA rozhoduje o hodnotách položky validity.

DV je certifikační autoritou, která certifikuje klíče konkrétních inspekčních systémů. V České republice by v roli DV mohla vystupovat Cizinecká a pohraniční policie, která bude spravovat inspekční systémy pro elektronické pasy, kterými budou vybavení příslušníci na letištích a dalších místech, kde se pasy prověřují.

Pokud organizace provozující DV potřebuje verifikovat pasy té které země, musí zažádat u příslušné CSCA provozované zvolenou zemí (např. v případě, že CPP ČR bude chtít číst otisky

prstů z pasů vydaných občanům Polska, musí se obrátit s žádostí o certifikaci k CVCA provozované Polskem).

Délka platnosti certifikátu DV je od 2 týdnů do 2 měsíců a je určena vydávajícím CVCA. DV je povinen zpracovat žádost o vydání certifikátu do 24 hodina a vydat pak certifikát do 48 hodin.

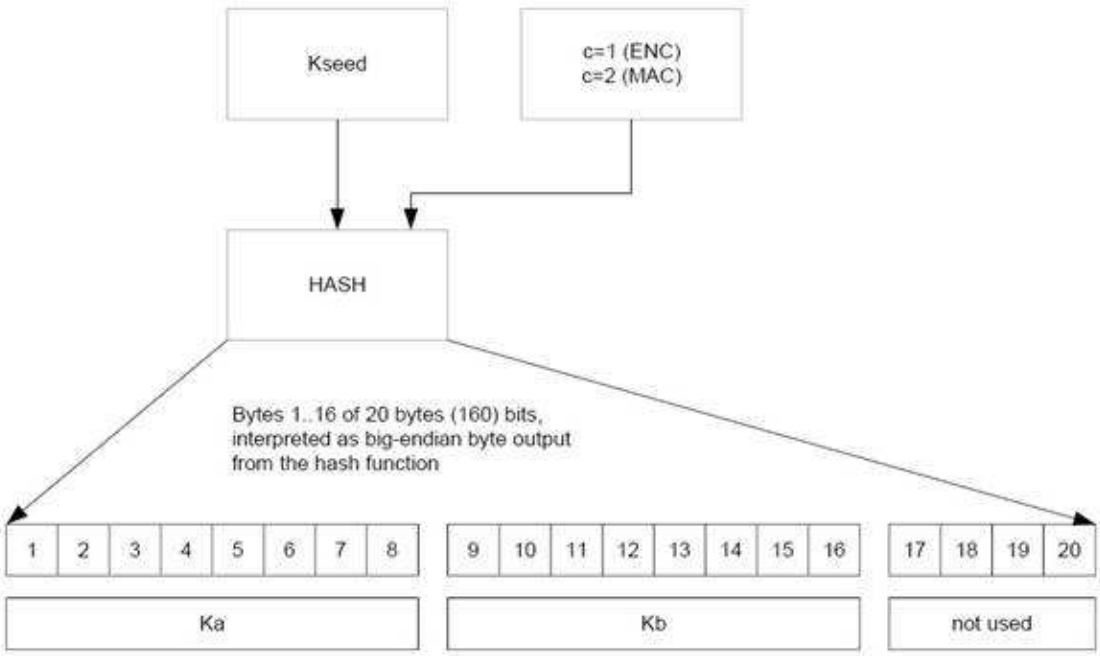
4.2.3. Inspection system (IS)

Inspekční systém je technologická jednotka, která již přichází do kontaktu s e-pasem a která pro čtení z pasu používá svůj klíč. Typicky je IS např. příruční počítač vybavený čtečkou pasů a snímačem otisku prstů a vybavený modulem pro uchování klíče pro autentizaci vůči pasu (tzv. SAM). SAM může mít např. formu čtečky kontaktních čipových karet a klíče jsou pak uloženy na čipové kartě. Inspekční systém rovněž může být implementován s centrálním úložištěm klíčů pro autentizace terminálu s tím, že koncové zařízení tyto klíče využívá v online režimu.

Délka platnosti certifikátu IS je od 1 dne do 1 měsíce. Délka platnosti musí být vždy nejdéle stejná jako platnost odpovídajícího DV, typicky však kratší. Autorizace uvedené v certifikátu IS jsou podmnožinou autorizací, které má přiděleny vydávající DV.

4.3. Autorizace

Ve všech certifikátech je naplněna položka Certificate holder authorization, která obsahuje informace, jaká je role toho kterého systému a jaké operace jsou mu povoleny. Autorizace jsou uložena podle následující tabulky a je nazvána *relativní autorizací* :



Pro určení výsledných oprávnění držitele konkrétního certifikátu je potřeba cestu od certifikátu až ke kořenové autoritě a posbírané hodnoty pole autorizace bitově logicky vynásobit (AND). Výsledná hodnota je tzv. *efektivní autorizací,* a podle ní čip řídí přidělené oprávnění.

4.4. Správa klíčů

Po vyrobení pasu (a personalizaci) obsahuje čip aktuálně platný klíč CVCA a využívá ho jako důvěryhodnou kotvu pro autentizaci terminálu. Postupem času je klíč CVCA vyměněn (za život pasu i několikrát) a aby čip mohl i nadále ověřovat klíče IS, potřebuje celý řetězec vedoucí až ke klíči CVCA, se kterým byl personalizován. Čip umožňuje autorizovaným terminálům importovat následné klíče CVCA, provede jejich ověření a uloží si je do úložiště důvěryhodných klíčů. Díky tomu, že si čip klíče po ověření uloží, postačuje při běžných autentizacích zasílat do čipu pouze certifikáty DV a IS.

4.5 Čas v čipu

Při ověřování platnosti předložených certifikátů je kromě kryptografického ověření také nutno zjistit, zda je certifikát ještě platný. Čip nemá k dispozici zdroj času (když je mimo elektromagnetické pole, je zcela vypnutý). Proto je v čipu implementován tzv. aktuální čas čipu. Jde o hodnotu, která reprezentuje poslední časový údaj, který je prokazatelně již minulostí. Při personalizaci je tato hodnota inicializována na čas personalizace. Během doby života čipu je pak aproximována na základě certifikátů, které čip zpracovává v rámci importu a autentizací. Aktuální čas čipu je nastaven po úspěšné autentizaci na největší hodnotu atributu Effective date ze zpracovaných CVCALink certifikátů, DV certifikátů a "domácích" IS certifikátů. Pokud navíc při importu a nastavení interního času čip identifikuje, že jsou v oblasti důvěryhodných klíčů vypršené certifikáty, musí je označit jako neaktivní a je možno je vymazat pro ušetření paměti.

Díky doporučenému způsobu překrývání platnosti při obnově CVCA by oblast důvěryhodných klíčů neměla nikdy obsahovat více jak 2 certifikáty CVCA.

5. Reference

[ICAO BioMRTD] *Biometrics deployment of Machine Readable Travel Documents 2004*.
http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf

[ICAO Bio Annex A] *Annex A - Photograph Guidelines*.
http://www.icao.int/mrtd/download/documents/Annex%20A%20-%20Photograph%20Guidelines.pdf

[ICAO Bio Annex B] *Annex B - Facial Image Size Study #1*.
http://www.icao.int/mrtd/download/documents/Annex%20B%20-%20Facial%20Image%20Size%20Study_1.pdf

[ICAO Bio Annex C] *Annex C - Facial Image Size Study #2*.
http://www.icao.int/mrtd/download/documents/Annex%20C%20-%20Facial%20Image%20Size%20Study_2.pdf

[ICAO Bio Annex D] *Annex D - Biometric Data Interchange Formats – Part 5: Face Image Data (ISO. /IEC JTC 1/SC 37 N 506)*.
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2300191/JTC001-SC37-N-506.pdf?nodeid=3924597&vernum=0

[ICAO Bio Annex E] *Annex E - Biometric Data Interchange Formats – Part 6: Iris Image Data (ISO. /IEC JTC 1/SC 37 N 504).*
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2300191/JTC001-SC37-N-504.pdf?nodeid=3924512&vernum=0

[ICAO Bio Annex F] *Annex F - Biometric Data Interchange Formats – Part 4: Finger Image Data (ISO/. IEC JTC 1/SC 37 N 466).*
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2300191/JTC001-SC37-N-466.pdf?nodeid=3924168&vernum=0

[ICAO Bio Annex G] *Annex G - Biometrics - Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (ISO/IEC JTC 1/SC 37 N 464).*
http://www.icao.int/mrtd/download/documents/Annex%20G%20-%20Fingerprint%20Minutiae.pdf

[ICAO Bio Annex H] *Annex H - Biometrics Data Interchange Formats – Part 3: Finger Pattern Spectral Data (ISO. /IEC JTC 1/SC 37 N470).*
http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2300191/JTC001-SC37-N-470.pdf?nodeid=3924237&vernum=0

[ICAO Bio Annex I] *Annex I - Use of Contactless Integrated Circuits.*
http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf

[ICAO Bio Annex J] *Annex J - ICAO. May 2003 Press Release*.
http://www.icao.int/mrtd/download/documents/Annex%20J%20-%20ICAO%20May%202003%20Press%20Release.pdf

[ICAO Bio Annex K] *Annex K - ICAO. Supplementary Requirements to ISO14443 -v2. .*
http://www.icao.int/mrtd/download/documents/Annex%20K%20-%20ICAO%20Supplementary%20Requirements%20to%20ISO14443%20-v2.pdf

[ICAO Bio Annex L] *Annex L - ePassports Data Retrieval Test Protocol*.
http://www.icao.int/mrtd/download/documents/Annex%20L%20-%20ePassports%20Data%20Retrieval%20Test%20Protocol.pdf

[ICAO Bio PKD] *Issues of the ICAO. Public Key Directory (PKD).*
http://www.icao.int/mrtd/download/documents/Issues%20of%20the%20ICAO%20Public%20Key%20Directory%20PKD.pdf

[ICAO Bio LDS] *Logical Data Structure(LDS) version 1.7.*
http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf

[ICAO Bio PKI] *PKI for Machine Readable Travel Documents offering ICC read-only access v1.1.*
http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf

[ICAO Bio 9303 Sup] *Supplement to Doc 9303 - ePassports*.
http://www.icao.int/mrtd/download/documents/9303%20Supplement%20-%20December%202005.pdf

[CDBP MV] *Cestovní doklad s biometrickými prvky - stránky Ministerstva vnitra*.
http://www.mvcr.cz/sprava/informat/biometrika/

[Obsah Datapge] *Popis obsahu datové strany*. http://www.highprogrammer.com/alan/numbers/mrp.html

[Datapage Example] *Příklad datové strany*. http://travel.state.gov/visa/temp/without/without_1990.html

[MRZ Calc] *Kalkulátor obsahu MRZ.*
http://www.highprogrammer.com/cgi-bin/uniqueid/mrzp

[EAC TR] *Extended Access Control TR 03110*. http://www.befreite-dokumente.de/eingereichte-akten/tr-03110-eac-1.0/

[EU Bio] *Nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy (publikováno dne 29. prosince 2004 v Official Journal of the European Union číslo L385/1).* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:CS:HTML

[EU Bio Tech] *Rozhodnutí Komise ze dne 28. února 2005, kterým se stanoví technické specifikace norem pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy - K(2005) 409.*
http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2005_409_cs.pdf

[EU Otisky] *Rozhodnutí komise ze dne 28.6.2006 kterým se stanoví technické specifikace norem pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy*. http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_cs.pdf

[329/1999 Sb] *Zákon č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), ve znění zákona č. 217/2002 Sb., zákona č. 320/2002 Sb., zákona č. 539/2004 Sb., zákona č. 559/2004 Sb. a zákona č. 136/2006 Sb.*.
http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=329/1999&PC_8411_l=329/1999&PC_8411_ps=10#10821

[326/1999 Sb] *Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, ve znění zákona č. 140/2001 Sb., zákona č. 151/2002 Sb., zákona č. 217/2002 Sb., zákona č. 222/2003 Sb., zákona č. 436/2004 Sb., zákona č. 501/2004 Sb., zákona č. 539/2004 Sb., zákona č. 559/2004 Sb. a zákona č. 136/2006 Sb.*.
http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=326/1999&PC_8411_l=326/1999&PC_8411_ps=10#10821

[325/1999 Sb] *Zákon č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o azylu), ve znění zákona č. 2/2002 Sb., zákona č. 217/2002 Sb., zákona č. 320/2002 Sb., zákona č. 519/2002 Sb., zákona č. 222/2003 Sb., zákona č. 539/2004 Sb., zákona č. 57/2005 Sb.a zákona č. 501/2004 Sb.*.
http://portal.gov.cz/wps/portal/_s.155/701?number1=325%2F1999&number2=&name=&text=

[642/2004 Sb] *Vyhláška č. 642/2004 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech.*
http://portal.gov.cz/wps/portal/_s.155/701?number1=642%2F2004&number2=&name=&text=

[ISO 1073-2:1976] *ISO norma o alfanumerickém fontu pro OCR část 2.*
http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=5568

[Berlin Interop] *Testování interoperability v Berlíně*. http://www.interoptest-berlin.de/

D. Počítačová (ne)bezpečnost

Ing. Jaroslav Pinkava, CSc., GeaCert s.r.o., (jaroslav.pinkava@zoner.cz)

(článek je rozšířenou verzí stejnojmenného článku, který vyšel v časopise Egovernment 3/2006 a je zpracován na základě informací, které se průběžně objevují v seriálu Bezpečnostní střípky)

Úvodem

Počítače – tento nástroj se stal již po nějakou dobu součástí našeho života a pro mnohé z nás její každodenní součástí. Jeho řada vynikajících vlastností (namátkou – práce s množstvím dat, komunikační schopnosti,…) z něj dělají nenahraditelného pomocníka v celé řadě lidských činností. Jeho schopnosti se rok od roku umocňují, ať už je to způsobeno vývojem HW nebo nových prostředků SW.
Na druhou stranu právě rostoucí složitost tohoto nástroje vede i k existenci složitějších problémů souvisejících s jeho bezpečným využíváním. Počítačová bezpečnost se jednak stává náročnou odbornou disciplinou, ale jednak je to fenomén, který ovlivňuje každého, kdo s počítači pracuje. A jestliže se hovoří o počítačové gramotnosti, pak mezi její součásti patří i základní prvky počítačové bezpečnosti. Některé aktuální skutečnosti:

- Evropská komise v tomto roce zveřejnila první informace týkající se její nové informační kampaně, kterou nazvala "IT Security for Europe". Firmy, jednotlivci i veřejné instituce se nedostatečně věnují zabezpečení svých počítačů a sítí, říká se v prohlášení. Mnoho dnešních hrozeb vychází z kriminálních aktivit motivovaných ziskem. S rostoucí složitostí systémů rostou i počty bezpečnostních faktorů, které souvisí s fungováním těchto systémů. Agentuře ENISA (European Network and Information Security Agency in Heraklion, Greece) byl svěřen úkol sebrat informace o bezpečnostních incidentech v 25 členských zemích a připravit tak systém "nejlepších odpovědí". Jsou připravována další opatření, včetně legislativních.
- Chystaný nový operační systém Windows Vista přinese řadu nových bezpečnostních prvků (vestavěné bezpečnostní aplikace – Windows Firewall, Windows Defender, UAC – User Account Control, nová práva běžných uživatelů, zvýšená bezpečnost prohlížeče IE7 a další bezpečnostní prvky – podrobněji to popisuje Deb Shinder ve Will Vista make you more secure?) – budeme se s ním cítit bezpečněji?
- Evropa je méně postižena bezpečnostními průniky než USA. Alespoň podle některých výsledků z přehledu Ponemon Institute LLC a právní firmy White & Case LLP (komentář k tomuto přehledu obsahuje článek Why isn't Europe suffering a wave of security breaches?). Z výsledků vyplývá, že USA jsou na tom sice lépe z hlediska používání bezpečnostních prostředků (šifrování, detekce průniků, ale i školení personálu atd.), avšak podle počtu zveřejněných incidentů je na tom zase podstatně lépe Evropa. 52 procent amerických firem má například ustaveného šéfa bezpečnosti, u evropských firem to platí jen pro 35 procent. V USA také šéfové bezpečnosti jsou na vyšších pozicích než jejich evropské protějšky. Pokud se týká školení zaměstnanců ve vztahu k bezpečnosti IT, platí zde obdobný poměr : 54 procent amerických firem školí své zaměstnance (v tomto směru), zatímco z evropských firem toto naplňuje jen 32 procent. Příčiny mohou být několikeré. Jednou z nich může být to, že evropské incidenty nejsou vždy zveřejňovány (v USA je k tomu zákonná povinnost), evropské společnosti jsou na tom v některých ohledech (identifikace, ID) přece jen lépe a za třetí americké společnosti jsou lepším cílem pro potenciální útočníky. Pokud však evropské firmy nepůjdou na minimálně stejnou úroveň používání bezpečnostních prostředků (jako dnešní Amerika), pak budou v budoucnu muset čelit dokonce horším útokům, než kterým čelí dnešní

americké firmy. Na druhou stranu by americké firmy měly převzít některé typy kontrol, které používá Evropa. Týká se to především důvěry v elektronický obchod, kde u amerických zákazníků v současnosti svým způsobem prochází tato důvěra krizí.

- Electronic signatures struggling in Europe, aneb jak to bude s uznáváním elektronického podpisu v jiné členské zemi EU? Autor článku konstatuje, že je třeba vytvořit takový systém elektronického podpisu, který by fungoval i přes hranice jednotlivých zemí. Je to důležité pro bezpečný elektronický obchod a efektivní využívání dalších veřejných služeb (v elektronické formě).
- Pozornost médií přitahuje probíhající debata Microsoft versus EU na téma bezpečnost (Microsoft Debates Vista Security with EU). Microsoft chce ovládnout i ty trhy s bezpečností pro IT, kde dříve dominovali jiní hráči. Nebudí to samozřejmě kladné reakce. Navíc pro EU je to jen jeden z antitrustových problémů, které chce s Microsoftem řešit.

A co na to vše průměrný uživatel počítače? Nemá to již dnes lehké a bohužel ani není (alespoň pro nejbližší budoucnost) možné předpovědět ulehčení jeho pozice. Jeden příklad – firewally na domácích počítačích jsou tak komplikované, že nastavit jejich správnou konfiguraci je pro běžného uživatele nereálné (Dirk Averesch v Why home firewall software is a leaky dike).

Některá fakta

Existuje velké množství různých přehledů (řadu z nich najdeme na internetu), které dokumentují aktuální vývoj ve vztahu k různým aspektům počítačové bezpečnosti (spam, počítačové viry a červi, spyware resp. jiný malware, phishing,….). Závěry těchto přehledů rozhodně nesrší optimismem.

Například:

- četnost spamu zůstává na zhruba stejné úrovni jako před rokem (polovina uživatelů konstatuje vysokou úroveň spamu)
- četnost virových infekcí také zůstává na stejné úrovni, jedna čtvrtina uživatelů hlásí velký problém a často finančně nákladný
- spyware, zde nastal pokles hlášených incidentů, přesto situace stále odpovídá epidemii, jedna osmina uživatelů měla velký problém a zase často finančně nákladný
- rhybářské útoky, zde je zhruba stejná úroveň jako před rokem, roste ale velikost průměrné ztráty jedné oběti. Alarmující je vzrůst počtu rhybářských webů.
- úhrnem lze konstatovat, že pravděpodobnost, že se uživatel stane obětí kybernetické kriminality, je rovna jedné třetině, tj. zhruba stejná úroveň jako před rokem.
- mezi nejrychleji rostoucí kybernetické hrozby patří množství počítačů infikovaných prostřednictvím malware, který z nich činí součást armád botů.

Americká společnost Websense opublikovala přehled Security Trends Report, který časově pokrývá události v druhém pololetí roku 2005. Z obsahu:

- Nové cíle rhybářů
- Změny v typech rhybaření
- Podvodné webovské stránky
- Malware (keyloggery, boty, spyware)

K některým faktům, které jsou ve zprávě uvedeny:

- Množství malware i počty podvodných webovských stránek rostou.
- Rhybaření, tento typ útoků se stává sofistikovanějším. Často byl třeba použit motiv pomoci obětem živelných pohrom (tsunami, hurikán Katrina,...). Cílem útoků se stávají i nefinanční organizace (jako Microsoft, Volkswagen, Symantec a McAfee). Například jeden typ podvodného e-mailu vyžadoval kliknutí na odkaz, který jakoby vedl ke stažení a instalaci záplaty od společnosti McAfee. Nic netušící oběť se dostala na podvodnou webovskou stránku, která imitovala stránku McAfee Security. Záplata byla ve skutečnosti trojským stahovačem (downloader).
- Ale i v druhém pololetí roku 2005 byly nejlákavějšími cíly rhybářů finanční služby (banky, úvěrové společnosti) a základním prostředkem tedy sociální inženýrství. Aktuálně lze zmínit velice nedávný rhybářský útok na Českou spořitelnu.
- Cílené rhybaření (spear phishing) jako technika podvodu se v pololetí 2005 dále vyvíjelo k větší rafinovanosti. Tyto postupy si vybírají jako cílovou skupinu specifickou podmnožinu lidí (například členy jedné organizace, pracovníky jedné firmy). K přesvědčení obětí, že se jedná o legální postupy, jsou často využívány ukradené interní informace. Cílem útoků také není již jen krádež osobních (např. bankovních) údajů, ale také např. informace, které bývají předmětem průmyslové špionáže (plány, pracovní postupy, atd.).
- Pomocí trojanů jsou počítače obětí infikovány keyloggery nebo programy stahujícími části obrazovky (screen-scraping). Objevuje se také software (zde je použit termín crimeware), který přesměrovává uživatele jinam než tento zamýšlel (je měněna informace vztahující se k DNS a existují další podobné triky). Jiným útokem analogického typu jsou tzv. homografické útoky. Útočník ovládá stránku s názvem blízkým nějakému známému odkazu a počítá s tím, že se řada lidí při zadávaní adresy splete (překlep, častým trikem je například záměna písmena O za číslici 0). Oběť si pak nevšimne, že není na správném odkazu atd.
- Většina rhybářských stránek sídlí v USA, Číně a Jižní Koreji. Stránky s crimeware mají poměrně obdobné rozložení, jen mezi nejčetnějšími Brazilie nahradila Jižní Koreu.
- V budoucnosti autoři studie předpovídají využití RSS jako efektivního prostředku pro šíření obdobných podvodů a infekcí. Kromě bezprostředního finančního zájmu se budou organizátoři takové kriminality orientovat na informace typu průmyslová špionáž. Zranitelnosti typu XSS (cross site scripting) budou používány k útokům na stránky finančních institucí a elektronického obchodu. Mezi předpověďmi se objevuje také využití VoIP.
- Jak byly rhybářské útoky v druhé polovině roku rozděleny? Finančních služeb se týkalo 89,3 % útoků, poskytovatelů internetových služeb 5 % útoků a maloobchodu 2,5 %.
- Problém rychlosti záplatování u zranitelností a publikací jejich exploitů je stále vážnější. Některé webovské stránky využily tři publikované zranitelnosti prohlížečů k infekci nikoho nepodezřívajících návštěvníků. Obdobná situace byla s WMF zranitelnosti Windows koncem roku.
- Objevují se tzv. "toxické" blogy. Autoři popisují situaci, kdy jeden rodinný blog byl použit k infekci, která oběť přivede až k stáhnutí trojana se zadními vrátky.
- Nejrychleji rostoucím spyware v sledovaném období byly tzv. bankovní trojské koně. Pokud si je oběť (na základě nějakého triku) nainstaluje, hlídají znaky vkládané klávesnicí (keyloggery). Existují i postupy pro oklamání ochran proti keyloggerům (anti-key logging programs), jsou stahovány části obrazovky.
- Roste počet útoků DoS (denial of service), které se opírají o využití botnetů. Dokonce jsou nabízeny tyto sítě jako obchodní artikl. Potřebujete potrápit konkurenci?
- S tím souvisí i jiná rozšiřující se metoda, je jí kybernetické vyděračství. Zaplať a my ti odstraníme tvůj problém anebo v jiné verzi – zaplať a my ti problém neuděláme. Objevují se dokonce společnosti, které se vydávají za ochránce proti spyware a pod tímto pláštíkem

vám budou tzv. pomáhat. U vás se objeví podvodná hláška typu "váš počítač je ohrožen" no a firma vám pomůže, ale od peněz. Tento typ kriminality se objevuje v Rusku, na Ukrajině a také v Mexiku.

- Rok 2005 je také rokem rostoucí spolupráce hackerů. Nové skupiny mladých hackerů pochází z východní Evropy a Brazilie. Výstupem činnosti hackerů nejsou již pouze vlastní kriminální aktivity, ale objevují se i publikované sady nástrojů (kits). Jejich jednoduchá úprava pak umožňuje konkrétní provedení útoku.

Noam Eppel v rozsáhlém článku Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security vyjadřuje skepsi nad současným stavem IT bezpečnosti. Svoje názory dokumentuje celou řadou dalších odkazů. Říká třeba: z nedávných přehledů vyplývá, že dospělý Američan věří, že pravděpodobněji se stane obětí kriminality na internetu než obětí fyzického kriminálního činu. Z jednoho letošního přehledu společnosti Gartner vyplývá, že 14 procent těch, kteří provozovali bankovnictví online, opustilo tento způsob bankovnictví a 30 procent změnilo své postupy. Důvodem jsou bezpečnostní obavy. Přitom o otázkách bezpečnosti se v souvislosti s informačními technologiemi dnes hovoří neustále. Bezpečnost sama je posilována dlouhou škálou technologických prostředků (firewally, antimalware, systémy pro detekci průniků, autentizační a autorizační prostředky, ...). Jsou však jsou tyto prostředky schopny ji zajistit? Rok 2005 měl být podle dostupných informací ve vztahu k bezpečnostním průlomům nejhorším rokem historie vůbec. Asi něco není opravdu v pořádku. A jiný příklad, který autor uvádí. Pokud si uživatel je vědom hrozících rizik a doporučení typu Surviving the First Day of Windows XP a bude nový systém XP doplňovat posledními záplatami Microsoftu, bude nucen stáhnout a nainstalovat data v objemu 70-260 MB. A toto mu zabere nepochybně podstatně delší dobu, než je třeba k tomu, aby nezáplatovaný počítač byl infikován. Je přitom známo, že v některých situacích stačí 30 vteřin k tomu, aby byla získána plná kontrola nad počítačem.

K dokonalému zabezpečení (a o 100 procentech se hovořit nedá) i jednotlivého počítače jsou zapotřebí už poměrně hluboké znalosti informačních technologií a pokud se týká složitějších infrastruktur... Zkrátka složitost používaných technologií je jednou z hlavních překážek pro dosažení kýžené bezpečnosti. Budoucností (ale spíše z pohledu ochrany soukromí) se zabývá také Bruce Schneier v Your vanishing privacy. Komentáře k tomuto článku najdete na Schneierově blogu. Důsledky počítačové éry se v této oblasti projevují velice silně. Systémy sledování se zdokonalily, ať jsou to průmyslové kamery, odposlechy telefonů či monitoringy samotných počítačových aktivit (e-maily, e-obchod, ...). Nastupují čipy RFID, mobilní telefon lze lokalizovat s přesností na desítky metrů, obdobně nás prozradí používání bluetooth a bezdrátových zařízení. Autor na závěr říká, že jedinou možnou cestou boje proti zneužívání takto získaných informací jsou vhodná nastavení legislativy.

Existující nebezpečí

Hackeři jsou stále vynalézavější. A vše se posouvá do roviny peněz. Typickým cílem útoků není již zdaleka jen snaha poukázat na slabinu softwaru, systému, ale cílem je finanční zisk a snaha dostat se k datům, které umožní přístup k penězům obětí:

- Hackeři se učí, jak obcházet (silná) autentizační schémata. Již se objevil trojan, který nekrade heslo, ale čeká, až se oběť spojí s bankou a potom tiše vysaje peníze z konta.

- Keyloggery, aneb malí špioni ve Vašem počítači. Ať již se tam dostali např. neopatrným otevřením přílohy e-mailu (SW verze) či dnes již existují i HW verze, kdy stačí malý

fyzický zásah do vaší klávesnice či kabelu. Veškerá data, která pak vkládáte do počítače, putují k podvodníkovi. Zatím nejsnadnějším způsobem detekce takového zařízení je kontrola cest, kudy jsou následně přenášeny kradené informace. Je otázkou, jakým směrem další vývoj půjde a jakou potom volit obranu, až tyto informace budou šifrovány. Pokud se obáváte špionáže, tak je snad nejlépe zamykat do trezoru celý počítač (i před uklízečkou). Paranoia? Ano, ale každý musí zvážit svá existující rizika.

- Jiným dnes často zmiňovaným HW rizikem jsou mobilní USB zařízení. Robert Lemos v komentáři na Security Focus (USB drives pose insider threat) rozebírá možná nebezpečí, která souvisí s jejich používáním. Autor informuje o zajímavém pokusu. Konzultanti auditorské firmy nechali různě položené USB flash disky (20 kusů) uvnitř budovy jedné finanční skupiny. V paměti každého disku byl umístěn program (maskovaný jako obrázkový soubor), který měl za cíl sběr hesel, jmen uživatelů a dalších informací o systému uživatelů. Patnáct z těchto zařízení zaměstnanci zvedli a postupně vložili do počítačů kreditní společnosti.

- Útoky na bázi sociálního inženýrství (opírá se o vytvoření vztahu důvěry s podváděnou stranou a tak slouží k získání citlivých informací či neoprávněnému přístupu). Např. v Social Engineering defence for Small Businesses autor článku Russell Morgan popisuje prostředky obrany proti útokům tohoto typu v malých firmách, podává přehled možných nebezpečí i doporučovaných strategií.

- Příkladem předešlého typu útoků je phishing. To je zejména v poslední době velice se rozšiřující postup, kterým se podvodní hackeři snaží získat citlivá data obětí. Další podrobnosti lze nalézt např. v článku Phishing aneb rhybaření .

Ekonomický pohled při hodnocení bezpečnostních incidentů bývá diskutován méně (ve srovnání s diskusemi k podstatám bezpečnostních průniků), přesto ekonomika, ať chceme či ne, je vždy přítomna.

Bezpečnostní rizika počítačů se netýkají jen jednotlivců, ale je to také problém společností, institucí. V odpovědi na otázku, zda dnes společnosti vynakládají dostatečně peněz na ochranu svého počítačového prostředí, říká známý bezpečnostní odborník Bruce Schneier, že je to otázka správy rizik. Ne vždy jsou vynaložené peníze správně rozloženy. Je mnoho organizací, které vynakládají na bezpečnost adekvátní sumy peněz, ale utratí je nevhodně, nepokryjí ta správná místa.

Andrew Brandt v rozsáhlém článku (The 10 Biggest Security Risks You Don't Know About) se věnuje cestám minimalizace rizik uživatele PC. Uvádí následující seznam vážných bezpečnostních problémů, kterých by si uživatel měl být vědom:

- Armády PC Zombií
- Vaše ukradená data dostupná volně na webu
- Rhybáři kooptují legitimní stránky
- Bezpečnostní dírou je člověk
- Triky k přesměrování vašeho prohlížeče na podvodné stránky
- Rootkity a viry
- Viry volají vaším telefonem
- Malware ve vašem pasu
- Vaše data jsou zadržována za výkupné
- Neexistuje bezpečné útočiště, nebezpečí číhají na všech platformách

Google hacking, Google Earth (satelitní snímky), Google Deskop, nyní Google Notebook a co nás ještě čeká? V článku Ways Google is shaking the security world se Sarah D. Scalet zamýšlí nad tím, jak s využíváním těchto prostředků, které nám Google nabízí, jsou ovlivňovány různé aspekty bezpečnosti. Google nám nastavuje zrcadlo, říká v závěru autorka, co vše dáváme napospas online. A v budoucnu lze předpokládat pouze ještě větší agresivitu vyhledávacích technologií. Nestojí to za zamyšlení nad postupy nás samotných? Jak si chráníme svá data, své informace, které se mohou stát v určitých situacích zranitelnými?

Co s tím

Samozřejmě existuje mnoho cest, jak popisovaná rizika snížit či eliminovat. Otázkou ale zůstává, zda dnešní běžný uživatel se dokáže v množství souvisejících informací orientovat, resp. zda k nim vůbec najde cestu. Alespoň některé:

Pokud si chcete pohled na bezpečnost maximálně zjednodušit, lze začít následujícími třemi prioritami (Your Top Three Security Priorities):

- 1. Zajistěte, aby zaměstnanci byli dobře proškoleni. A to s ohledem na cesty k rozpoznání hrozeb i s ohledem na vhodné reakce na tyto hrozby.
- 2. Používání hesel. V současné době je velkým problémem používání triviálních hesel, a to v širokém měřítku. Pokud jsou používána složitější hesla, nejsou dobře chráněna. Autor doporučuje dvoufaktorovou autentizaci, speciálně tu, která využívá kombinaci biometrie a čipových karet.
- 3. Bezpečnost by se měla pokud možno opírat o princip maximální jednoduchosti. Bohužel dnes je využíván za tímto účelem software, který pochází od celé řady dodavatelů a vzniklý systém je svou složitostí vzdálen tomuto principu.

Chraňte své soukromí při vyhledávání online (Six Tips to Protect Your Online Search Privacy) , v tomto článku najdete těchto šest doporučení:

- 1. Do vyhledávače nevkládejte informace, které mohou sloužit k vaší identifikaci
- 2. Nepoužívejte vyhledávač poskytovatele vašeho internetového připojení
- 3. Nepřihlašujte se do vámi používaného vyhledávače, resp. do souvisejících nástrojů
- 4. Zablokujte cookies vašeho vyhledávače (autor doporučuje používání Firefoxu a v článku informuje, jak je ho třeba nastavit), obdobná informace je tam obsažena i pro Internet Explorer.
- 5+6. Lze-li to, měňte svou IP adresu, v opačném případě používejte anonymizující software.

Několik jednoduchých doporučení pro každého, jak zabezpečit svá data, najdete v článku Computer Security: How to Safeguard Your Data:

- Používejte a spravujte antivirový software a firewall (včasné aktualizace)
- Pravidelně skenujte svůj počítač s ohledem na výskyt spyware
- Aktualizujte svůj software (záplaty instalujte pokud možno ihned po jejich vydání)
- Vyhodnoťte si nastavení svého softwaru (defaultní nastavení umožňují sice vždy správnou funkcionalitu, nemusí však poskytovat požadovanou bezpečnost)
- Zvažte využívání oddělených účtů pro jednotlivé uživatele
- Zaveďte postupy pro faktické používání počítače (pokud ho používá více lidí, např. děti, měli by všichni znát meze a chovat se tak, aby data, která je třeba chránit, chráněna byla)

- Používejte hesla a šifrujte citlivé soubory
- V pracovním prostředí dodržujte politiky společnosti pro práci s informacemi a jejich ukládání.
- S citlivými informacemi pracujte odpovídajícím způsobem

Jak již bylo zmíněno v úvodu, rostoucí složitosti používaných technologií vedou i k růstu počtu bezpečnostních problémů, které je nezbytné řešit. Týká se to jak přístupu společností - konstituování bezpečných informačních systémů, jejich audity, certifikace atd., tak i jednotlivců, jejich domácích počítačů, nakupování na webu, komunikací s bankovními systémy a šlo by tu vyjmenovat mnohé.

Neexistuje proto jedno univerzální řešení, ani v běžném životě tomu tak není. Pokud podstupujeme určitá rizika, je třeba je znát a znát i cesty vedoucí k jejich minimalizaci. Každý by měl zvládnout alespoň ty jednodušší. Zopakujme je třeba vědět, že je nezbytné:

- mít v počítači nastaveno kvalitní heslo
- udržovat svůj systém záplatami
- mít nainstalovaný antivirový program a program hlídající spyware
- neotvírat neznámé přílohy
- zálohovat důležitá data
- a seznamovat se s aktuálními informacemi

Některé odkazy na související informace dostupné na internetu

- Blog Bruce Schneiera
- Online dostupná kniha Rosse Anderssona: Security Engineering – http://www.cl.cam.ac.uk/~rja14/book.html

E. Mikulášská kryptobesídka 2006

Mikulášská kryptobesídka (http://mkb.buslab.org/) – workshop o kryptografii a příbuzných oborech se letos koná pošesté. Programový výbor už vybral příspěvky, které budou letošní rok prezentovány a dohodl se na zvaných řečnících i tématech jejich přednášek. Pokud máte zájem se letos zúčastnit, **je třeba se zaregistrovat** – **ušetřit můžete, když se vám podaří vše vyřídit do 17. listopadu**, do kdy platí sleva na registrační poplatek – podrobné informace naleznete na našich www stránkách.

Mikulášská kryptobesídka je pořádána za podpory

TRUSTED NETWORK SOLUTIONS

Microsoft

Sponzor soutěže KEYMAKER

GRISOFT

Sponzor Mikuláše

RSA
The Security Division of EMC

Předběžný program

7. prosince 2006 (čtvrtek)

U každého příspěvku je min. 5 minut pro dotazy a diskuzi k tématu

8:30 –	*Registrace*
9.33 – 9:40	*Zahájení workshopu*
9:40 – 10.40	*zvaný příspěvek*
	Alex Biryukov – Block and Stream Ciphers, and the Creatures In Between
10:40 – 11.40	*zvaný příspěvek*
	Riccard Focardi – Static Analysis of Authentication
11:40 – 12.40	*KEYMAKER*
	informace o soutěži
	prezentace nejlepších příspěvků
do 13:45	*Oběd*
13:45 – 14.45	*zvaný příspěvek*
	Vlastimil Klíma – Hašovací funkce nové generace
14:45 – 15:15	Martin Stanek – Overovanie RSA podpisov v dávke – takto nie
– 15:45	*Přestávka na kávu*
15:45 – 16:15	Jiří Sobotík, Antonín Mazánek – Extraktor entropie
16:15 – 16:45	Jan Krhovják – Analysis, demands, and properties of pseudorandom number generators
16:45	Rump session
18.00 –	*Večeře*

MKB 2006

http://mkb.buslab.org

Následuje série neformálních diskuzí v prostorách centra vyhrazených pouze pro účastníky kryptobesídky.

Mikulášská kryptobesídka je pořádána za podpory

Sponzor soutěže KEYMAKER

Sponzor Mikuláše

8. prosince 2006 (pátek)

U každého příspěvku je min. 5 minut pro dotazy a diskuzi k tématu

9:09 – 9:15	Zahájení druhého dne workshopu
9:15 – 10:15	*zvaný příspěvek* Pavel Vondruška – Přehled a historie polyalfabetických šifer
10:15 – 10:30	Jan Sutora – Užití kombinatorických designů pro plánování turnajů u watermarkingu databáze
– 11:00	*Přestávka na kávu*
11:00 – 12:00	*zvaný příspěvek* Petr Hanáček – Bezpečnost informačních systémů a chyby při návrhu – jsme schopni jim zabránit?
12:00	**Tombola**
12:12	**Ukončení workshopu**

Mediální partneři

F. O čem jsme psali v listopadu 1999 – 2005

Crypto-World 11/1999

Crypto-World 11/2000

Crypto-World 11/2001

Crypto-World 11/2002

Crypto-World 11/2003

Crypto-World 11/2004

(V.Klíma : Nedůvěřujte kryptologům, ke stažení na adrese : http://crypto-world.info/index2.php?vyber=casop6)

Crypto-World 11/2005

G. 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@zoner.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/