Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 6/2006 **15. červen 2006**

6/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1116 registrovaných odběratelů)

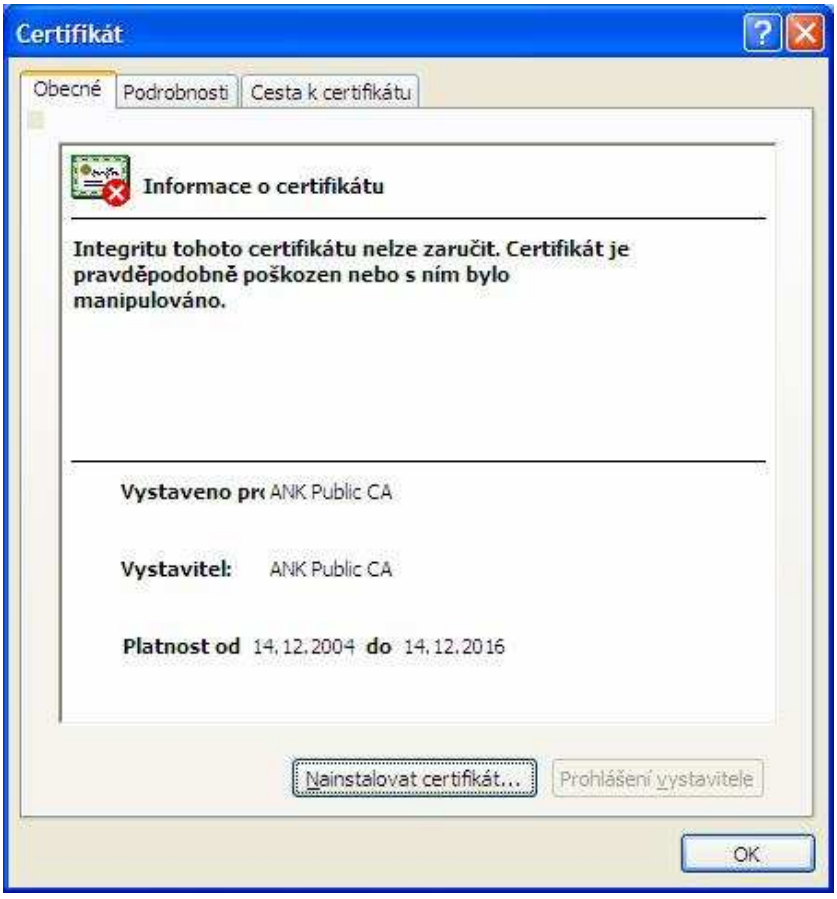
Obsah :

A. PKI roaming

RNDr. Libor Dostálek, Siemens s.r.o., (libor.dostalek@siemens.com)

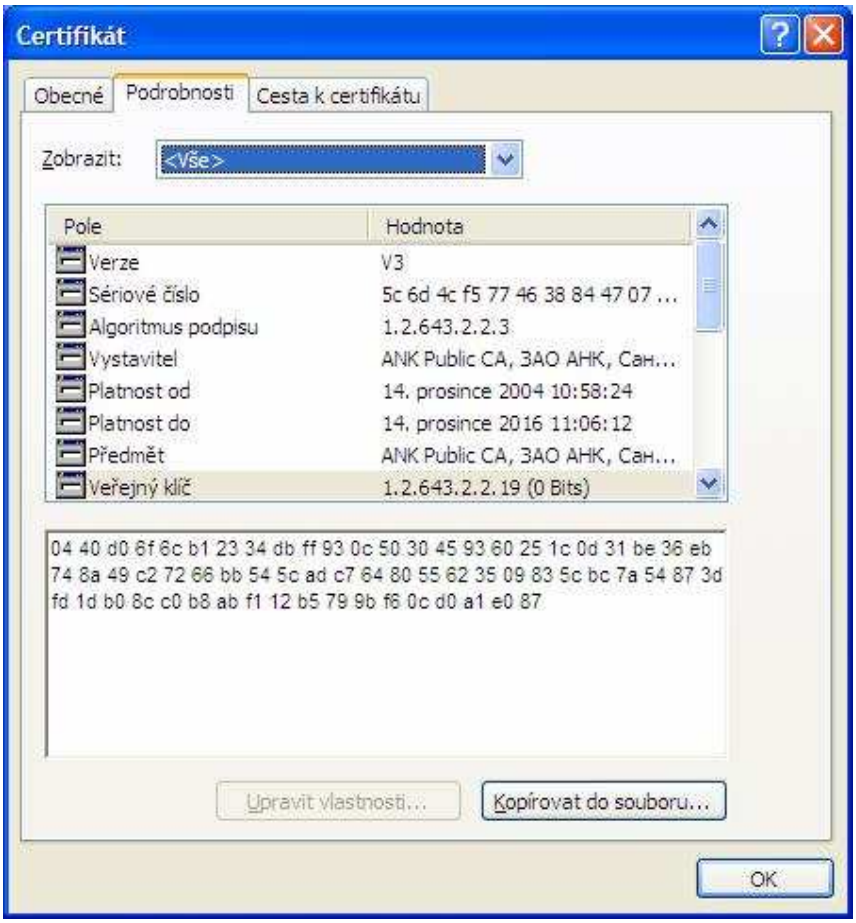
Právě jsem se vrátil z 6. evropského fóra o elektronickém podpisu (Polsko) a hned musím sdělit, že mne tam překvapila myšlenka PKI roamingu, která vzbudila velice rozporuplné reakce.

Pro pochopení situace musím hned v úvodu napsat, že Poláci pěstují intenzivní vztahy s Ruskem a Ukrajinou. Takže obratem jsem se dozvěděl, že v Rusku mají „drobné“ odlišnosti týkající se elektronického podpisu. Zatímco u nás podle zákona o elektronickém podpisu bychom měli pro styk se státní mocí používat zaručené elektronické podpisy postavené na kvalifikovaných certifikátech vydaných akreditovanými poskytovateli, pak v Rusku k tomu ještě dodávají jednu zdánlivou drobnost. Tou drobností je, že elektronické podpisy pro styk se státní mocí musí být vytvořeny algoritmy dle standardů GOST. Tj. musí se jednat o ruské algoritmy pro výpočet otisku i algoritmy asymetrické kryptografie. Takové algoritmy jako RSA se mohou používat nanejvýš v komerčním světě.



Večer jsem nelenil a požádal ruské kolegy o odkaz na jejich certifikační autority (rusky УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ). Stáhl jsem si jejich kořenový certifikát do svých XP:

Windows XP se pochopitelně těmto certifikátům vzpouzely (OID 1.2.643 je vyhrazeno pro Ruskou federaci, blíže viz http://www.ctel.msk.ru/x500/OIDS/inform.htm, lepší je ale si v Google nastavit ruštinu a přímo zadat OID).



Aby se moje Windows XP tyto algoritmy naučily, musí se do Windows XP nainstalovat odpovídající CSP (tj. DLL knihovna). Je to v podstatě podobné, jako kdybych si chtěl nainstalovat podporu nové čipové karty. Jelikož se příslušné kryptografické algoritmy z Ruské federace nesmí bez povolení exportovat, tak si tyto knihovny ani nemohu koupit, i kdybych měl těch cca 600 rublů na ně (kupodivu jsem je dosud ani na žádném veřejném webu ke stažení nenašel).

Také jsem si stáhnul CRL, jehož podpis byl rovněž vytvořen dle GOST. Výsledek byl takový, že po kliknutí myší se žádná chybová hláška neobjevila, prostě se vypsal obsah CRL s tím, že algoritmus podpisu je 1.2.643.2.2.3 (tj. GOST R 34.11/34.10-2001)…

Hned mne napadlo, jakže je to s čipovými kartami a HSM. Dozvěděl jsem se, že žádnou pořádnou nemají. Zajímalo mne, co je míněno tím „pořádnou“. Odvětili mi, že je jen jedna Java karta, která ty pravé algoritmy (rozuměj GOST) počítá v Javě. To mi připadalo divné, protože implementovat GOST algoritmy přece nemůže být více jak týden práce. Zeptal jsem se jednoho raději nejmenovaného dodavatele, proč to neudělali, a po značné konzumaci jsem pochopil, že pak by ta čipová karta sice uměla GOST, ale zase by nebyla ruská.

Základním problémem tak je, jak elektronicky komunikovat přes ruské hranice, když oni tam sice používají X.509, SSL/TLS, S/MIME atd., ale s jinými algoritmy. Řešením je právě PKI roaming, se kterým přišla Alla Stoljarova-Myc.

PKI roaming je ve své podstatě službou e-notary. Na elektronické hranici mezi Ruskem a EÚ (rusky Евросоюз) by se postavily dva e-notary servery. Jeden podle evropských standardů a druhý podle ruských standardů. Vzájemně by se považovaly za důvěryhodné a i přenos mezi nimi by byl považován za důvěryhodný. Kdyby dokument přišel např. z Ruska, pak by „ruský" e-notary systém dokument ověřil a pokud by byl výsledek ověření kladný, pak by jej předal dále. Jelikož by dokument byl ověřen důvěryhodnou stranou, pak by mohl být označen za důvěryhodný i pro „evropský" e-notary systém. Ten by jeho platnost stvrdil a poslal dále do Evropy…

Jako e-notary systém byl navržen protokol DVCSP (RFC-3029). P. Sylvester, který seděl hned vedle mne, si okamžitě přestal upravovat svou motorkářskou kombinézu a začal se nesmírně slastně rozhlížet na všechny strany: že by konečně někdo vzal zpět na milost jeho DVCSP?

Reakce byla bouřlivá. Nejbojovnější řečníci bohužel nepochopili (ať byli z Bruselu či Jižní Koreje), že se v Rusku opravdu používají zcela jiné algoritmy a i když si ruské certifikáty importují na svůj počítač, tak jim k ničemu nebudou.

Jiní si ale uvědomili, že nemusí jít jen o technický problém, ale i o problém přenosu dokumentů mezi různými právními systémy. Přinesu-li dnes ruský dokument před český soud, pak musím přiložit i jeho překlad. Překlad však nemůže být libovolný, musí být proveden soudním překladatelem. Pokud tedy informační společnost nesplaskne jako bublina, pak v budoucnu i takové služby budou třeba.

PKI roaming bude asi mnohými považován za sci-fi.

Na konferenci však byly i jiné příspěvky. Pro mne tím nejzajímavějším byl příspěvek Aljoši Blažíce z Lublaně. Pokud sledujete konference o dlouhodobé či trvalé archivaci elektronických dokumentů, pak toto jméno zajisté dobře znáte. Důležité pro nás je, že ve Slovinsku jsou v této oblasti podstatně dál než my. Mají tam totiž již parlamentem schválenou legislativu k dlouhodobé/trvalé archivaci elektronických dokumentů. Na večeři jsem chtěl vyloudit anglický překlad této legislativy, ale bohužel dosud neexistuje. Řekl mi, že je ve styku s Martou Vohnoutovou z ČR a že ona zná detaily. Budu se ji na to tedy muset zeptat.

Nesmírně zajímavé byly i německé příspěvky o tom, jak dělat elektronickou fakturaci. O tom ale až příště.

Na závěr jsme byli všichni pozváni do „Petěru" na listopadovou konferenci o PKI. Nevím, jestli bych ale dostal vízum.

B. Lehký úvod do časové synchronizace a vyhláška o podrobnostech atestačního řízení pro elektronické nástroje

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

Jak to vlastně spolu souvisí …

Všichni berou ohled na čas, jen čas na nikoho.
Německé přísloví.

Ministryně informatiky Dana Bérová podepsala před týdnem (9.6.2006) vyhlášku o atestačním řízení pro elektronické nástroje. Tato vyhláška upravuje ustanovení o dynamických nákupních systémech a elektronických aukcích zákona č. 137/2006 Sb., o veřejných zakázkách, který nabývá účinnosti již 1. 7. 2006. V atestačním řízení prováděném Ministerstvem informatiky se bude posuzovat shoda použitého elektronického nástroje v zadávacím řízení se zákonem o veřejných zakázkách a prováděcími předpisy, a to zejména z hlediska jeho bezpečnosti. Ministerstvo informatiky se tak stane garantem důvěryhodnosti elektronického zadávání veřejných zakázek. Vyhláška nabývá účinnosti spolu s novým zákonem 1. 7. 2006.

A kde je ta časová synchronizace ? Ve vyhlášce se v § 4 (Podrobnosti atestačního řízení) uvádí:

V případě, že elektronický nástroj zajišťuje elektronický přenos a příjem nabídek, případně elektronický příjem žádostí o účast a návrhů v soutěži o návrh nebo elektronickou aukci či dynamický nákupní systém, doloží provozovatel pro potřeby atestačního řízení
…
b) splnění požadavků podle § 149 odst. 6 písm. b) zákona
1. kalibračním listem měřidla času podle zvláštního právního předpisu (Zákon č. 505/1990 Sb., o metrologii, ve znění pozdějších předpisů), pokud nepoužívá pro měření času operační systém podle bodu 2, nebo
*2. dokumentací měřidla času, pokud je pro měření času použit operační systém provozovatele; v dokumentaci se dokládá nejistota měření času a návaznost na zdroj reprodukující světový koordinovaný čas dokumentující měřidla času**, **kde je popsán způsob provádění synchronizace se zdrojem světového koordinovaného času, a to i v případě výskytu přestupné sekundy,***

To je tedy důvod, proč je tento článek věnován základům časové synchronizace informačních systémů a informaci o získání dodávky garantovaného přesného času z kalibrovaného NTP serveru, který je synchronizován se zdrojem světového koordinovaného času …

Neskromně si článek klade za cíl jakousi „úvodní bezplatnou konzultaci“ těm subjektům, které tuto informaci potřebují – tedy uživatelům, vývojářům, hodnotitelům a sponzorům (tedy těm, kteří nákup a provoz výše uvedených elektronických nástrojů platí, platí vývojářům a v neposlední řadě platí hodnotitelům – atestačním střediskům).

Lehký úvod do časové synchronizace

Člověk s jedněmi hodinkami ví přesně, kolik je hodin. Člověk s dvojími si není nikdy jistý.

V současné době je nejpoužívanějším standardem pro přenos času protokol NTP (Network Time Protocol). Je to protokol pro synchronizaci vnitřních hodin počítačů po paketové síti s proměnným zpožděním, který byl navržen tak, aby odolával následku proměnlivého zpoždění v doručování paketů. NTP klient umožňuje stanovit čas z odpovědí více časových serverů. Používá se čas UTC se speciálními příznaky pro přestupné sekundy. Protokol NTP verze 4 je schopen zajistit po internetu čas s chybou pod 10 milisekund (1/100 s), v lokální síti může při ideálních podmínkách dosáhnout přesnosti až 200 mikrosekund (1/5000 s).

NTP je jeden z nejstarších dosud používaných TCP/IP protokolů. NTP původně navrhl Dave Mills z univerzity v Delaware (RFC 958 NTP , RFC 1059 NTP V1) a stále jej, spolu se skupinou dobrovolníků, udržuje. Verze 3.0 tohoto protokolu byla formalizována v de facto standardu FRC 1305. Verze 4.0 je stále ještě vyvíjena a to skupinou IETF NTP Working Group.

Jednodušší forma NTP je známá jako SNTP (Simple Network Time Protocol). Klient neuvažuje zpoždění paketů v síti a nepamatuje si stav předchozí komunikace (RFC 1361 SNTP, 1769 SNTP V3). Poslední verzí je verze 4.0, která je formalizována ve verzi RFC 2030.

Domácí stránka projektu NTP je http://www.ntp.org/

Každý systém, který synchronizuje čas pomocí NTP, má přidělenu hodnotu Stratum. Nabývá hodnot od 0 do 16 a charakterizuje jeho vzdálenost od zdroje přesného času.
Stratum-0 je tedy přímo napojen na zdroj přesného času. Vzdálenost větší než Stratum -16 se již v definici NTP protokolu neuvažuje.

Zdroj času pro primární NTP server Stratum-0 se nejčastěji zajišťuje pomocí:

- atomových hodin (césiové hodiny nebo rubidiové generátory)
- radiový synchronizační signál učený pro přenos času (zejména DCF77 v Evropě nebo WWV v USA)
- navigační systém (např. GPS nebo Loran)

Pokud to však jde, využívá se jako primární NTP server stroj, který je napojen na atomové hodiny. Ostatní systémy jsou zatíženy různými problémy a nedostatky.

Příčinou nesprávného času NTP serveru (kromě chyb softwaru a nevhodného hardware) bývají právě časové zdroje, při kterých nemá systém možnost ověření, že jím reprodukovaná časová stupnice skutečně odpovídá příslušné stupnici UTC (např. při použití GPS UTC(GPS)). Stupnice takovýchto serverů proto nemohou být považovány za metrologicky navázané.
Pokud jde o přesnost, pak např. GPS přijímač, který přes sériové rozhraní komunikuje s řídícím systémem, předává údaje o poloze a čase standardně s přesností 1 sekunda.

Dodávka garantovaného přesného času z kalibrovaného NTP serveru (Stratum-1), který je synchronizován se zdrojem světového koordinovaného času …

Není větší škody nad ztracený čas.
Michelangelo Buonarroti

V technicky vyspělých zemích, které mají propracovaný národní metrologický systém a vytvářejí etalonovou stupnici UTC(i) navázanou na UTC, je z důvodu metrologické návaznosti a spolehlivosti poskytované časové informace žádoucí odvozovat čas primárního NTP serveru z etalonové stupnice UTC(i). Taková stupnice je v České republice vytvářena v Ústavu radiotechniky a elektroniky AV ČR (URE), který je z pověření Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (UNMZ) a v gesci Českého metrologického institutu zodpovědný za státní etalon času a frekvence.

Zde postavený NTP server, jehož časový údaj je navázán na státní etalon času má výlučné a referenční postavení mezi ostatními NTP servery v ČR. Přesnost tohoto NTP serveru je v reálném čase kontrolována a vyhodnocována. V případě zjištění odchylek mimo stanovené meze je výstup procesu ntpd automaticky pozastaven, aby byla vyloučena situace, kdy server poskytuje nesprávné údaje.

Systém státního skupinového etalonu frekvence a času ČR (ECM 100-1/97-001) se opírá o čtyři césiové svazkové generátory HP5071A tzv. „atomové hodiny“ (jejich provozovatelem jsou Ústav radiotechniky a elektroniky AV ČR (2ks) a ČESKÝ TELECOM a.s. (2ks)), z jejichž přirozených frekvencí se vytvářejí čtyři nezávislé atomové stupnice. Hlavním frekvenčním zdrojem etalonu je césiový svazkový generátor HP5071A vybavený speciální trubicí (high-performance tube). Z jeho přirozené frekvence se jemným frekvenčním odsazením (frequency steering) odvozuje česká realizace sekundy SI. Z ní se dále vytváří koordinovaná časová stupnice UTC(TP) [TP značí Tempus Pragense], která reprezentuje **čas etalonu a je zároveň českou realizací světové časové stupnice UTC.**

Používaná zařízení svou kvalitou předčí požadované standardy, generují totiž frekvenci s přesností $2x10^{-14}$, což je o dva řády přesnější než požaduje norma. Od roku 1997 bylo rozhodnuto o začlenění výše uvedených čtyř atomových hodin do státní metrologie času a frekvence a staly se tak základem Státního skupinového etalonu času a frekvence.

Provozované zařízení je navázáno na frekvenci mezinárodní atomové stupnice TAI (ve spolupráci s mezinárodním úřadem pro váhy a míry v Paříži). Srovnání ukazují, že frekvence provozovaného zařízení patří dlouhodobě k jedné z nejkvalitnějších ve světovém měřítku. Během dosavadního provozu nebyla ani jedna negativní připomínka od spolupracujících mezinárodních společností a ostatních připojených národních operátorů na kvalitu synchronizačního signálu.

Po začlenění do skupinového etalonu času a frekvence bylo rozhodnuto poskytovat **garantovanou službu přesného času**. Přesný čas je dodáván od roku 2003 protokolem Network Time Protocol, verze 4.0, včetně varianty se zaručením původu paketů (od 2006). Zdrojem času pro primární, tedy Stratum-1 server jsou výše uvedené atomové hodiny. Odebírat informace o přesném čase je možné přímo z těchto NTP serverů.

Výběr vhodného ntp serveru

V pravý čas - v pravou chvíli.
Quintus Flaccus Horatius

1. NTP servery Stratum-1, které jsou výše popsaným způsobem synchronizovány se světovým koordinovaným časem, jsou v ČR na adresách:

   ÚRE AV ČR:
   server 195.113.144.20 # tik.cesnet.cz alias ntp.cesnet.cz
   server 195.113.144.238 # tak.cesnet.cz

   ČESKÝ TELECOM,a.s.:
   194.228.72.249
   194.228.72.250

   Přehled ntp serverů Stratum-1 ve světě:
   http://ntp.isc.org/bin/view/Servers/StratumOneTimeServers

2. Využívání serverů Stratum-1 je primárně určeno pro klienty se správně zkonfigurovanými Stratum-2 servery ve větších sítích a zákazníky, kteří potřebují garantovanou dodávku přesného času včetně původu paketů. Není přípustné, aby jej využívalo více (např. 5 a více) strojů ze stejné lokální sítě. Není také vhodné, aby vůči externím Stratum-1 serverům nastavovaly svůj čas jednotlivé koncové uživatelské stanice.

3. Přístup na výše uvedené servery není v současnosti omezen. Pokud ovšem uživatel potřebuje průkaznost původu synchronizačních paketů a doklad o navázání na světový čas (včetně dokladu o pravidelné kalibraci) je tato služba placená. Uživatelé by také měli dobrovolně zachovávat „politiku“ bodu 2. Uživatelé dále nesmějí poskytovat placenou službu synchronizace přesného času jako ntp server Stratum-2 jiným subjektům.

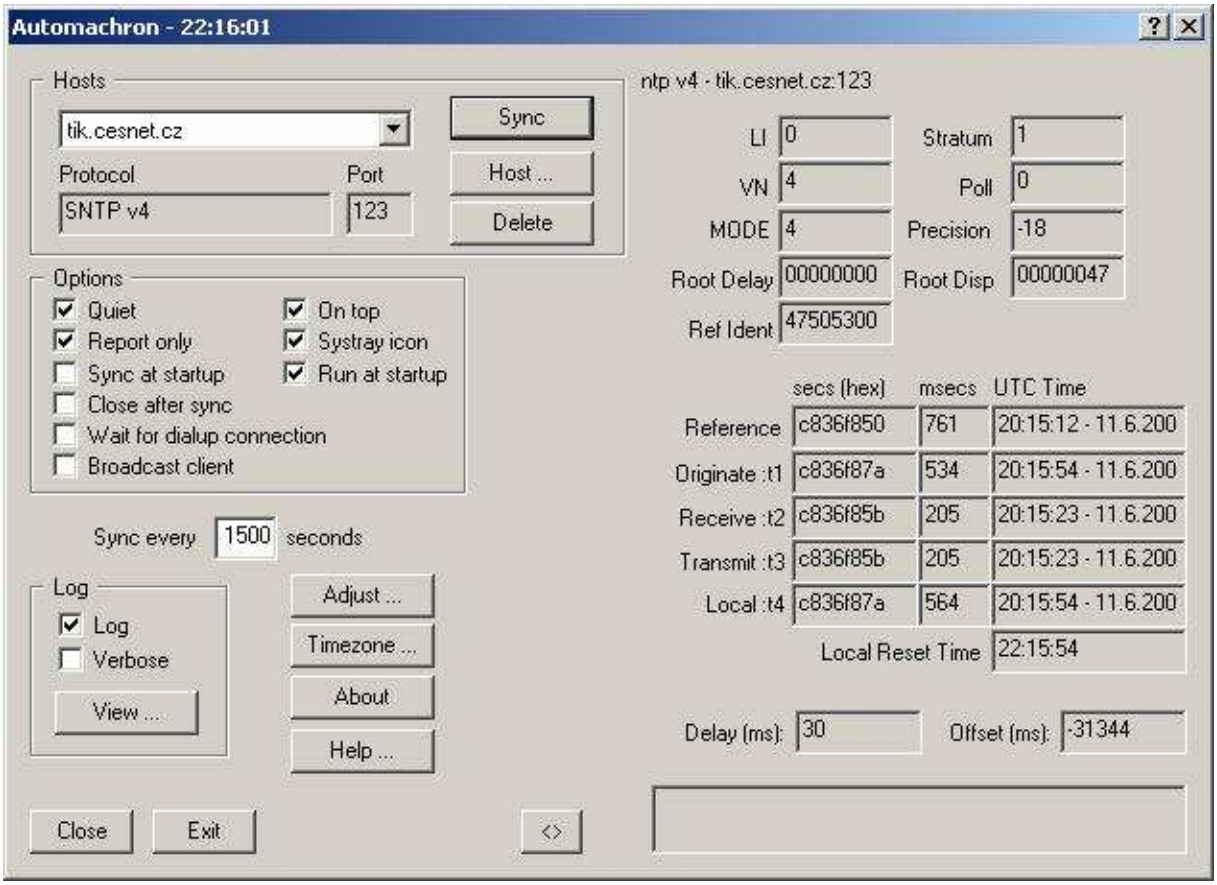
4. Pro potřeby běžných uživatelů bohatě postačí server Stratum-2. Na těchto serverech se zpravidla dosahuje přesnost pod 1 ms. Přehled některých volně dostupných ntp serverů Stratum-2 v ČR: http://bass.wz.cz/ntp.html.
   Přehled světových ntp serverů http://www.eecis.udel.edu/~mills/ntp/servers.html. Také je možné použít jeden ze 700 ntp serverů ze známého projektu „public ntp time server for everyone“ http://pool.ntp.org.

Nastavení lokálních hodin

Čas ubíhá různě, podle toho s kým.
William Shakespeare

Pro využití služby NTP / SNTP existují ve všech operačních systémech klienti, kteří umí nastavit čas svých lokálních hodin, ale nekorigují jejich rychlost. Pro periodické nastavení času v unixových systémech existuje nástroj ntpdate, který nastaví místní čas podle jednoho nebo několika určených NTP serverů (ntpdate tak.cesnet.cz).

Ve Windows je pro práci s NTP k dispozici příkaz net time (net time /setsntp: tik.cesnet.cz). Doporučuje se tyto příkazy spouštět při startu systému a následně v hodinových intervalech.



Pro stejný účel lze výhodně použít řadu shareware nebo freeware programů, např. již poněkud stařičký, ale nenáročný d4time (http://www.amt.org/Downloads/amt_downloads.htm) nebo oblíbený Automachron (http://www.oneguycoding.com/automachron/), který pracuje pod Win95/98, NT4, Win2000 a WinXP. Automachron podporuje SNTP a také TIME (UDP i TCP) – viz doprovodný obrázek. Poněkud rozsáhlejší je volně šiřitelná verze (open source) velmi dobrého programu nettime-2b7 (http://prdownloads.sourceforge.net/nettime/NetTime-2b7.exe?download). Při větších požadavcích na stabilitu a přesnost hodin se doporučuje nainstalovat programový balík NTPD. NTPD je možné provozovat i v prostředí MS Windows.

C. Univerzální posilovače hašovacích funkcí, včetně MD5 a SHA1 aneb záchranné kolo pro zoufalce

Vlastimil Klíma, nezávislý kryptolog, (v.klima@volny.cz)

Motto: Hašovací funkce, u níž byla nalezena kolize, ztrácí obecně smysl, neboť hypotéza o tom, že se chová jako náhodné orákulum, byla prakticky vyvrácena.

Tak to je teorie. A teď k praxi.

Volně navazujeme na článek Pavla Vondrušky z minulého čísla. Velmi vtipně uvedl na pravou míru zjednodušené tvrzení, že konstrukce MD5 || SHA1 nepřináší nic nového. Pravda je, že uvedené zřetězení vrací SHA1 její původní sílu, tj. složitost nalezení kolize 2^{80} namísto dnešních 2^{63}. Za necelé dva roky nám složitost nalezení kolizí u obou hašovacích funkcí rapidně klesla. U MD5 umíme najít kolizi za 17 sekund na obyčejném PC [3,10], u SHA1 za 127 dní na 5 péčkách, vybavených 16 zákaznickými zásuvnými deskami [7,4,5]. Proč se do tohoto HW experimentu nikdo ještě nepustil, je na první pohled záhada. Příčinou je známý trik Wangové - detaily metody, která umí nalézt kolize SHA-1 s onou složitostí 2^{63}, neuveřejnila.

Místo toho tým Wangová - Lenstra - Weger pracuje (?) na nalezení kolize SHA1, a to přímo v certifikátu veřejného klíče dle X.509 respektive RFC 3280. Jejich cílem je nalezení dvou platných certifikátů typu "RSA-SHA1" dvou různých klíčů RSA, z nichž jeden (padělek) certifikační autorita vůbec nikdy neviděla. Tento experiment navazuje na tentýž dokonaný experiment s funkcemi MD5 - RSA [6].

Je to jen strašení ? Možná ano, protože to tomu týmu trvá už nějak moc dlouho. Jakmile bude kolize SHA1 zveřejněna, nastane ale kromě kolotoče s certifikátem podvodného klíče RSA i problém podvodu, který jsme popsali u MD5 [10].

Prodlužování hašovacího kódu u slabých funkcí má tedy jako obrana smysl. Například ono použití 128 + 160 = 288 bitového kódu MD5 || SHA1 místo pouze 160bitového kódu SHA1 zesložiťuje nalezení kolize 131072 krát (2^{80-63}) oproti "čisté" SHA1.

V téhle konstrukci jsme kombinovali dvě hašovací funkce. Jsou však případy, kdy máme k dispozici jen jednu z nich. Třeba je to knihovna, kterou nemůžeme vyměnit, jen z ní volat funkce. Nebo to může být firmware, kde je také k dispozici jen volání funkce. V těchto případech je ale k dispozici většinou možnost nastavení inicializačního vektoru příslušné hašovací funkce. Většinou máme také možnost volat několik instancí té funkce najednou. A toho nyní využijeme.

Bezpečnost *k*-násobné SHA-1 a *k*-násobné MD5

Uvažujme tedy hašovací funkci F, jejíž hašový kód F(M) zprávy M se skládá ze zřetězení *k* hašových kódů $F_1(M) \| F_2(M) \| ... \| F_k(M)$. Za F_i uvažujeme hašovací funkci s inicializační konstantou IV_i (místo standardní hodnoty IV) tj. $SHA\text{-}1_{IVi}$ nebo $MD5_{IVi}$. Ještě před rokem a

půl se všeobecně myslelo, že složitost nalezení kolize takové funkce bude zhruba $2^{80} * 2^{80} * ... * 2^{80} = 2^{80k}$ pro SHA-1, kde 2^{80} je, jak víme, složitost nalezení kolize SHA-1 narozeninovým paradoxem. Metody Wangové [9] však z čísla 80 nyní udělaly 63 a metody Jouxové [2] pak celý vzorec zdegradovaly na:

2^{63} (pro k = 1), 2^{80} (pro k = 2) a pouhých $2^{80 + 6.5(k-2)}$ pro k větší než 2.

Podobně pro MD5, kde složitost je:

17 sekund (pro k = 1), 2^{64} (pro k = 2), pouhých $2^{64 + 6(k-2)}$ pro k větší než 2.

Abychom vrátili SHA-1 a MD5 jejich původní složitosti nalezení kolizí 2^{80} a 2^{64}, museli bychom použít k = 2 zřetězení. Tím bychom hašový kód natáhli na 320 a 256 bitů.

Existuje možnost, jak vrátit hašovacím funkcím MD5 i SHA-1 původní kvalitu?

Někdy ovšem hašový kód prodlužovat nemůžeme, protože na něj v protokolu, certifikátu apod. už není místo. Existuje možnost jak vrátit hašovacím funkcím MD5 i SHA-1 původní kvalitu? Byla by to záchrana "nejhorších" situací, kdy máme k dispozici pouze původní hašovací funkci a pro hašovací kód pouze původní délku v datovém formátu. Zdá se, že taková úloha nebude mít řešení, ale má. Z dosud uvedeného vyplývá, že kdybychom mohli místo SHA-1 použít $SHA1_{IV1} \parallel SHA1_{IV2}$, byla by složitost 2^{80} zpátky. Příliš dlouhý hašový kód můžeme zkrátit pomocí SHA-1! V tomto případě "zpráva", kterou hašujeme originální hašovací funkcí, se skládá z vysoce závislé a strukturované zprávy $SHA1_{IV1}(M) \parallel SHA1_{IV2}(M)$, kterou nelze libovolně "posunovat" pro potřeby útoku, jako původní zprávu M. Proto (zatím) jediná cesta, jak docílit kolize $SHA\text{-}1_{IV}(SHA\text{-}1_{IV1}(M) \parallel SHA\text{-}1_{IV2}(M))$ je narozeninovým paradoxem, a to dává složitost 2^{80}. Vidíme, že řešení se našlo, neboť délka takového hašového kódu je pouze 160 bitů. Podobně u MD5 by to byla místo původní MD5(M) haš $MD5_{IV}(MD5_{IV1}(M) \parallel MD5_{IV2}(M))$, která jí vrací složitost 2^{64}. Jednu nevýhodu tento přístup má. Je postaven na funkcích, u nichž došlo k nalezení slabin a pravděpodobně ještě dojde k rozvoji metod jejich prolamování. Čili takové záchrany je potřeba akceptovat i s určitým rizikem.

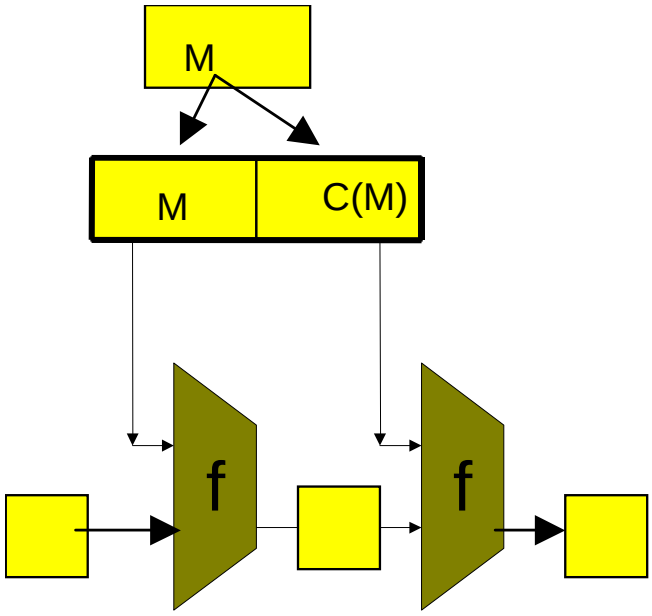
$$\mathbf{SHA\text{-}1_{IV}(SHA\text{-}1_{IV1}(M) \parallel SHA\text{-}1_{IV2}(M))}$$
$$\mathbf{MD5_{IV}(MD5_{IV1}(M) \parallel MD5_{IV2}(M))}$$

Obr.: Vzorce, které vracejí funkcím MD5 a SHA-1 jejich původní kvalitu

Další univerzální posilovače

Další možností, jak řešit popsanou situaci, je upravit hašovací funkci uvnitř. Budeme hovořit o SHA-1, ale platí to i o MD5 a o ostatních hašovacích funkcích. Otázka je, kdo za takovou

úpravu SHA-1 ponese záruku, ale stejná otázka platí pro SHA-1 bez úpravy, protože po roce 2010 ji nikdo garantovat nebude (viz prohlášení NIST k okamžité výměně SHA-1 za bezpečnější). Současné metody tvorby kolizí využívají určitých slabin uvnitř hašovacích funkcí. Proto vznikl pracovní návrh nového standardu SHA1-IME, který zavádí do SHA-1 malé změny z hlediska jejich algoritmu a programového kódu, ale velké změny z hlediska aplikace současných útoků. Proto SHA1-IME je proti nim odolná. Podrobný popis SHA1-IME naleznete v [8], programová realizace této funkce se od SHA-1 liší jen v jednom řádku navíc - v tzv. lepší expanzi zprávy. Podobné úpravy lze dělat i uvnitř jiných prolomených hašovacích funkcí.



Obr.: Obecné doporučení pro všechny hašovací funkce

Obecně fungující metoda

Když bychom nemohli modifikovat hašovací funkci jako výše, máme ještě jednu zcela obecnou metodu, jak se bránit současným útokům. To je opatření šité na míru proti současným útokům, ale určitě bude účinné i na mnohé jiné útoky. Většinou je to tak, že u hašovací funkce otevřeme její kontext tím, že ji inicializujeme příslušnou konstantou IV a potom jí posíláme datové bloky. V tomto případě místo 512-bitového datového bloku m, který máme zpracovat, pošleme hašovací funkci bloky dva, a to m || C(m), kde C bude nějaký (nejlépe nelineární) kontrolní kód bloku m (například rychlé Fletcherovy kódy). Zbytek odstavce je jen pro ty, kdo rádi riskují. Samozřejmě je možné pro výpočet C využít i volání hašovací funkce, ale velmi opatrně! Například není vhodné volit C = h, kde h je původní hašovací funkce. V současné době by tato konstrukce ještě ustála, ale v budoucnu asi ne. Při konstrukci kontrolního kódu C je naopak vhodné 512 bitový blok m rozdělit, několikrát aplikovat hašovací funkci, a výsledky opět vhodně "spojit" do 512 bitového bloku C(m). Vhodně znamená nějakou netriviální funkcí. Tady se meze fantazii nekladou a je tu hodně

prostoru. Jen je vhodné znát podstatu současných útoků, aby jim konstrukce C nenahrávala. Docela se těším, že by tady někdo v příštím čísle mohl něco navrhnout (i anonymně).

Jednoho dne budeme muset MD5 a SHA-1 opustit

Pokud budeme chtít docílit vyšší bezpečnosti, nezbude, než jednoho dne změnit aplikace, v nichž se slabé hašovací funkce používají a místo slabé hašovací funkce h začít volat silnou funkci H. U rozsáhlých avšak uzavřených systémů, kde jakákoliv změna není jednoduchá, je možné částečné řešení téměř ihned, i když stále velmi náročné. Místo slabé hašovací funkce h lze od jistého data začít používat silnou hašovací funkci H s kódem zkráceným na délku hašovacího kódu h. Přitom je možné ponechat starý identifikátor hašovací funkce, staré formáty a délky dat. Pro aplikaci kontrolující například certifikát bude v tomto případě rozhodující datum vydání certifikátu. Je-li vyšší než den změny (například 1.1.2007), místo hašovací funkce h se použije už nová funkce H. Důležité je, že funguje jak starý systém, tak nový a že se nemusí měnit struktura certifikátu, datové formáty a délky, pouze aplikace. Ta se však musí změnit vždy, pokud se má hašovací funkce zlepšit. S ohledem na důvěryhodnost celého systému je také nutné odtud plynoucí zásady pro výpočet hašových kódů jasně popsat v příslušné systémové (či certifikační) politice. Je otázka, zda zavádět uvedené nebo podobné bezpečnostní berličky. V některých případech (například u uzavřených systémů) to může být jediné dobré dočasné řešení, snižující bezpečnostní riziko.

Skutečné řešení

Samozřejmě je to výměna slabých hašovacích funkcí za silné. Pokud se někomu nechce do výměny MD5 a SHA-1 za některou z funkcí SHA-2, je tu ještě jedna možnost, a to použít hašovací funkci Whirlpool [1]. Má 512bitový hašovací kód a osobně jí věřím více než SHA-2, která je také 512 bitová. Poté, co byla Whirlpool přijata jako kryptografická technika v rámci evropského projektu NESSIE, byla vydána i jako mezinárodní norma ISO, a to ISO/IEC 10118-3. To ji svým významem a garancí staví na roveň SHA-2.

Závěr

Pokud bychom před necelými dvěma lety řekli, že dnes bude možné během několika sekund vytvářet kolize hašovací funkce MD5 na notebooku, asi by nám nikdo nevěřil. Než se obdrží takový výsledek pro SHA-1, může to trvat měsíc, půl roku nebo deset let, to nikdo neví. Do žádných hurá výměn nikoho nenutíme, uvedli jsme jen trochu více informací, abyste si mohli ohodnotit bezpečnost a upřesnit riziko dalšího používání té či oné hašovací funkce nebo zvolit nějaké jiné alternativy.

Článek vznikl rozšířením [4] a [5].

LITERATURA

[1] Paulo S.L.M. Barreto and Vincent Rijmen:The WHIRLPOOL Hashing Function, (Revised on May 24, 2003), pozor, musí to být verze z 24.5.2003, verze předchozí jsou odlišné ! http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip
převzatá jako ISO/IEC 10118-3

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

[3] Vlastimil Klima: Tunnels in Hash Functions: MD5 Collisions Within a Minute, IACR ePrint archive Report 2006/105 , http://eprint.iacr.org/2006/105.pdf, 18 March, 2006, v češtině na http://cryptography.hyperlink.cz/2006/tunely.pdf, zdrojové kódy na http://cryptography.hyperlink.cz/2006/web_version_1.zip

[4] Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (32) – Praktická obrana proti kolizím MD5 a SHA1, Sdělovací technika, 4/2006, str. 10 - 11

[5] Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (35) – Zesílení hašovací funkce třídy SHA-1, Sdělovací technika, č. 7/2006, v tisku

[6] A. Lenstra and X. Wang and B. de Weger. Colliding X.509 Certificates, IACR Eprint archive, Report 2005/067. http://eprint.iacr.org/067.pdf

[7] A. Satoh: Hardware Architecture and Cost Estimates for Breaking SHA-1, ISC 2005, Singapore, September 20-23, 2005, LNCS 3650, pp. 259-273, 2005.

[8] SHA1-IME, Internet draft, November 2005, <draft-irtf-cfrg-sha1-ime-00.txt>, http://www1.ietf.org/mail-archive/web/cfrg/current/msg01157.html

[9] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin: Finding Collisions in the Full SHA-1, Crypto 2005, http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf
Na Rump Session Crypto 2005 dne 17. 8. 2005, týmem Wang-Yao-Yao (v zastoupení Adi Shamira) bylo oznámeno zlepšení prezentovaného útoku z 2^{69} na složitost 2^{63}

[10] Domácí stránka projektu kolizí:
http://cryptography.hyperlink.cz/2004/kolize_hash.htm

D. NIST (National Institute of Standards and Technology - USA) a kryptografie.
Recommendation on Key Management – část 2.

Jaroslav Pinkava, CA Czechia, (Jaroslav.Pinkava@zoner.cz)

1. Úvod

Po víceméně vstupní části, jejímž obsahem je především celková charakteristika problematiky správy kryptografických klíčů, se materiál [1] věnuje některým konkrétnějším otázkám. Jsou to klasifikace typů informací souvisejících s používáním kryptografických algoritmů, vlastnosti jednotlivých typů klíčů - např. z hlediska jejich životního cyklu, z hlediska práce s jednotlivými klíči, vazba délky klíče a použitého kryptografického algoritmu apod.

2. Správa klíčů – celkový pohled

Pátá kapitola materiálu nejdříve uvádí určitou klasifikaci typů kryptografických klíčů.
Autoři rozlišují následujících devatenáct (!) typů:

1. Soukromý podpisový klíč
2. Veřejný klíč pro ověření podpisu
3. Symetrický autentizační klíč
4. Soukromý autentizační klíč
5. Veřejný autentizační klíč
6. Symetrický klíč pro šifrování dat
7. Symetrický klíč pro zabalení klíče (key wrapping)
8. Symetrické a asymetrické klíče pro generování náhodných čísel
9. .Symetrický hlavní klíč (master key)
10. Soukromý klíč pro přenos klíčů
11. Veřejný klíč pro přenos klíčů
12. Symetrické klíče pro dohodu na klíči
13. Soukromý statický klíč pro dohodu na klíči
14. Veřejný statický klíč pro dohodu na klíči
15. Soukromý efemerální klíč pro dohodu na klíči
16. Veřejný efemerální klíč pro dohodu na klíči
17. Symetrický autorizační klíč
18. Soukromý autorizační klíč
19. Veřejný autorizační klíč

A dále je uvedena klasifikace souvisejících, resp. na kryptografii navazujících informací:

1. Doménové parametry
2. Inicializační vektory
3. Sdílená tajemství
4. Zárodek pro náhodný generátor (RNG seed)

5. Některé další veřejné informace (typu nonce – hodnota, která není nikdy používaná dvakrát, např. pořadové číslo)
6. Některé mezihodnoty (vzniklé v průběhu kryptografických operací)
8. Informace spojené s klíčem (identifikátor, čítač,…)
9. Náhodná čísla
10. Hesla
11. Informace pro audit

3. Použití klíčů

Obecně by mělo platit pravidlo – jeden konkrétní klíč má být používán pouze za jediným účelem (např. šifrování, autentizace, zabalení klíče, generování náhodného čísla resp. digitální podpis). Je to z několika důvodů.

1. Používání téhož klíče pro různé účely může vést ke snížení bezpečnosti použité kryptografie.
2. Tím, že omezíme používání klíče, omezujeme také potenciální škody při eventuální kompromitaci klíče.
3. Některá použití klíče mohou vést k problémům při jiných použitích téhož klíče - např. omezená doba platnosti soukromého klíče pro podpis (po ukončení doby své platnosti má být klíč zničen) a situace, kdy je párový veřejný klíč použit pro přenos klíče – nemohu pak příslušný obsah již dešifrovat (řídím-li se správně pravidly).

4. Životní cykly kryptografických klíčů

Pojem kryptoperioda (cryptoperiod) klíče zde označuje dobu, v jejímž průběhu je konkrétní klíč autorizován pro používání (legitimními, oprávněnými uživateli).
Vhodnou cestou definovaná kryptoperioda:

1. omezí množství informací, které jsou daným klíčem chráněny a které je pak dostupné k využití při kryptoanalýze;
2. omezí velikost úniků v případě kompromitace;
3. omezí i využívání konkrétního algoritmu na dobu jeho životnosti;
4. časově omezí dobu, během které se protivník může pokoušet o různé akce (fyzického, procedurálního typu, či narušením přístupových mechanizmů) vedoucí ke kompromitaci daného jednotlivého klíče;
5. omezí časový interval, ve kterém vzniklé informace budou prozrazeny, pokud dojde ke kompromitaci klíče;
6. omezí dobu použitelnou pro intenzivní kryptoanalýzu (v situacích, kdy není vyžadována dlouhodobá ochrana informací).

Existuje řada faktorů, které ovlivňují rizika spojená s volbou délky kryptoperiody (např. síla použitého kryptografického algoritmu, bezpečnost implementace algoritmu, operační prostředí, postupy pro práci s klíči atd.).

Kryptoperioda klíče souvisí také s jeho použitím, tedy typem klíče (ve smyslu výše uvedené klasifikace). Materiál [1] obsahuje v tomto smyslu podrobnější rozbor a také doporučení pro jednotlivé typy klíčů /ve vztahu k jejich kryptoperiodám).

5. Typy záruk

Materiál uvádí následující potřebné typy záruk:

1. Záruky neporušenosti (integrity) klíče.
2. Záruka platnosti používaných doménových parametrů.
3. Záruka, že je používán platný veřejný klíč (zde tedy ve smyslu, že to není slabý klíč, nebo klíč nějakým způsobem porušený).
4. Záruky ohledně vlastnictví soukromého klíče

6. Možné kompromitace

Informace chráněné kryptografickými prostředky jsou bezpečné pouze tehdy, pokud algoritmy zůstávají dostatečně silnými a použité klíče nejsou kompromitovány. Samozřejmě kompromitace klíče má různé dopady závisející na tom, čeho se použití kryptografie týká, tedy na typu kryptografického klíče. Existují také však určité prostředky, jejichž použitím omezíme pravděpodobnost či možné dopady kompromitace klíče. Např.
- omezení doby, kdy symetrický klíč nebo soukromý (asymetrický) klíč se nachází v otevřeném tvaru;
- jsou vytvořeny zábrany tak, aby člověk neviděl klíče v otevřené podobě;
- klíče v otevřeném tvaru se nachází pouze ve fyzicky chráněných zařízeních;
- jsou používána ověření integrity klíče
- v rámci protokolů je prováděna kontrola klíče druhou stranou tak, aby došlo ještě k dodatečnému ujištění, že je použit správný klíč.
- klíče jsou ničeny okamžitě, jakmile již nejsou zapotřebí.

Doporučuje se také mít zpracován detailní postup při případné kompromitaci klíče (plán obnovy při kompromitaci).

7. Volby kryptografického algoritmu a délky klíče.

Materiál používá pojem srovnatelná síla kryptografických algoritmů. Souvisí to především s postupy pro kryptoanalýzu (v návaznosti na známé metody – jako např. složitost faktorizačních algoritmů, složitost úlohy řešení obecného diskrétního logaritmu resp. eliptického diskrétního logaritmu atd.). V budoucnu toto mohou ovlivnit i realizované kryptoanalytické algoritmy na kvantových počítačích.

Následující tabulka je poměrně známá a objevila se již i v řadě jiných publikací.

Počet bitů	Symetrický algoritmus	Alg. na bázi diskr.logaritmu (DSA, D-H)	Algoritmy vycházející ze slož. faktorizace (RSA)	Alg. na bázi eliptického diskr.logaritmu (ECDSA)
80	2TDEA	L = 1024 N= 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N= 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N= 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N= 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N= 512	k = 15360	f = 512+

Řádky v tabulce odpovídají zvolenému stupni bezpečnosti. Pokud se jedná o krátkodobou bezpečnost s nároky spíše obvyklého typu (tj. nejsou to informace s nejvyššími stupni důvěrnosti), pak lze samozřejmě začít s volbami obsaženými v prvním řádku. S rostoucími nároky na dobu ochrany informací atd. se budeme v tabulce pohybovat po řádcích směrem dolů. Např. pokud chceme chránit informace tak, aby ochrana byla funkční až do roku 2030 – materiál doporučuje volbu délek klíčů dle druhého řádku tabulky. Má-li být ochrana informací funkční i po roce 2030, pak je třeba se řídit délkami klíčů dle třetího řádku. Doufejme, že kvantové počítače hned tak tuto filosofii nenaruší.
Materiál uvádí i odpovídající tabulku pro hashovací funkce. Tady však bude asi lépe si počkat na další (možná nepříliš) vzdálený vývoj této problematiky.

8. Literatura

[1] NIST Special Publication SP 800-57 Recommendation on Key Management, Part 1
(http://csrc.ncsl.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf)

E. O čem jsme psali v červnu 1999 – 2005

Crypto-World 6/2000

Příloha : Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 6/2001

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

Crypto-World 6/2002

Crypto-World 6/2003

Crypto-World 6/2004

Crypto-World 6/2005

F. 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/