Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 3/2004 **16. březen 2004**

3/2004

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

A. **Nastavení prohlížeče IE pro používání kontroly CRL (P.Vondruška)** **2-4**
B. **Jak jsem pochopil ochranu informace, část 2. (T.Beneš)** **5-9**
C. **Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), část 3. (J.Pinkava)** **10-12**
D. **Archivace elektronických dokumentů, část 4. (J.Pinkava)** **13-16**
E. **Letem šifrovým světem (TR,JP,PV)** **17-19**
F. **Závěrečné informace** **20**

(články neprocházejí jazykovou korekturou)

A. Nastavení prohlížeče IE pro používání kontroly CRL

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Mnoho serverů v síti Internet je nastaveno tak, aby bylo neoprávněným osobám zabráněno získat informace odeslané z těchto serverů nebo na ně. Tyto servery se nazývají zabezpečené. Aplikace Internet Explorer podporuje protokoly zabezpečení používané zabezpečenými servery SSL 3.0, SSL 2.0, TLS 1.0.

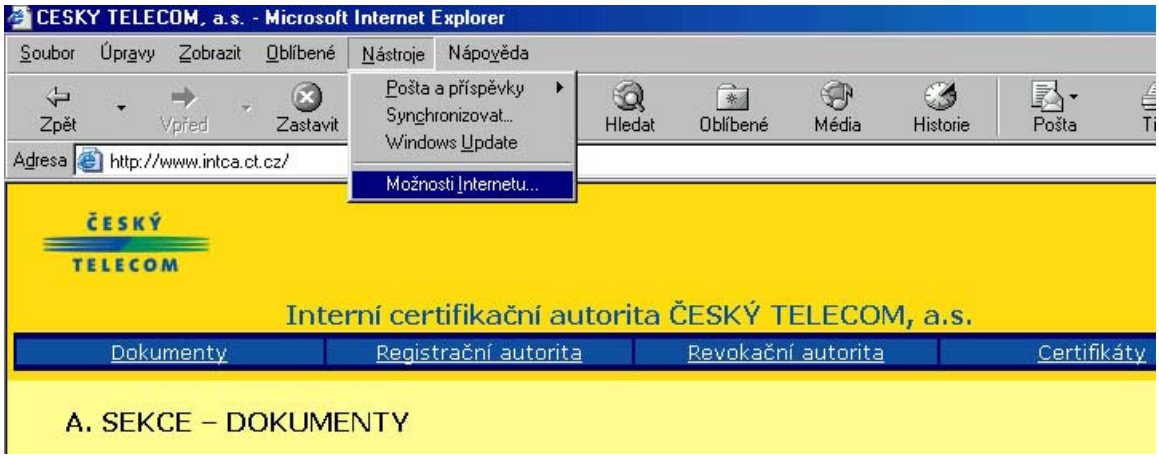
Pokud navštívíte zabezpečený www server, odešle k vám výzvu na ustanovení zabezpečeného spojení a pokud dojde k dohodě, aplikace Internet Explorer zobrazí ve stavovém řádku ikonu zámku. Nutnou podmínkou k ustanovení zabezpečeného spojení je :

- důvěra v certifikát (resp. v certifikační autoritu, která certifikát vystavila)
- samozřejmě časová platnost certifikátu
- správné umístění certifikátu na www stránce, pro kterou byl vydán.

Pokud chcete navíc zkontrolovat, zda certifikát uložený na zabezpečeném serveru nebyl zneplatněn (resp. nebyl zneplatněn certifikát poskytovatele, který jej vydal), je nutné správně nastavit příslušné parametry v prohlížeči, který používáte. Po instalaci většiny verzí Internet Exploreru není totiž tato kontrola odvolání certifikátů serveru nastavena.

V praxi to znamená, že při vstupu na zabezpečený server a při ustanovení zabezpečené komunikace (SSL) probíhá test certifikátu serveru jen na :

a) platnost data certifikátu (tj. zda v okamžiku vstupu na stránku již neuplynula doba, na kterou byl certifikát vydán)
b) zda je certifikát umístěn na www stránce, pro kterou byl vydán
c) zda jej vydala certifikační autorita, které důvěřujete, tj. je-li její certifikát uložen v kořenovém úložišti



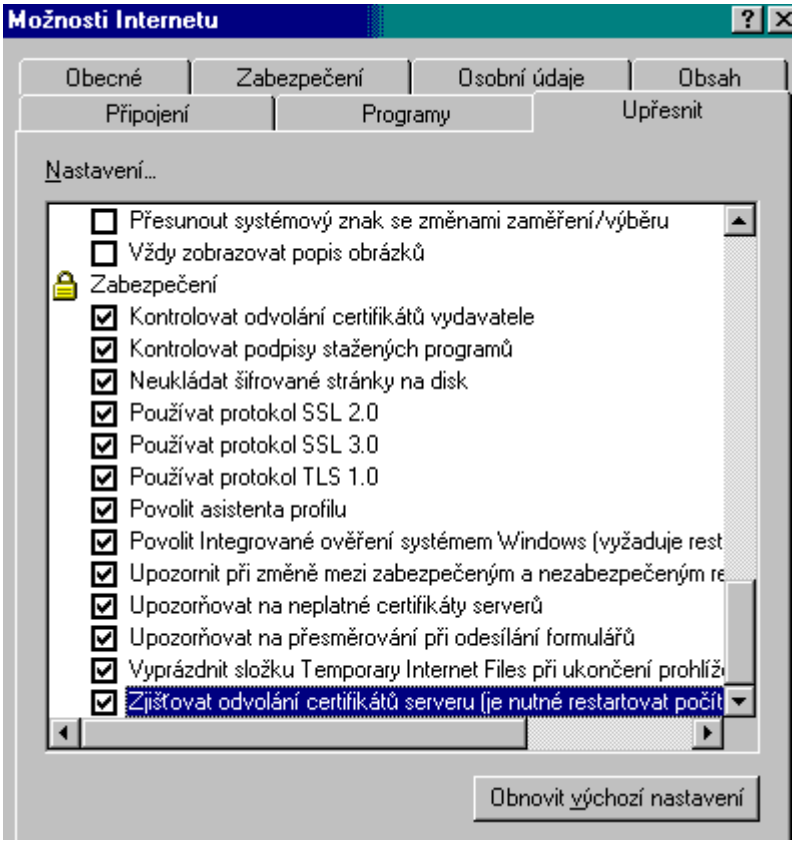
Pokud chcete zajistit i kontrolu, zda není certifikát uveden na seznamu zneplatněných certifikátů (CRL), je nutné

a) správně nakonfigurovat váš prohlížeč
b) zajistit stahování aktuálních CRL a jejich instalaci na vaše PC

V tomto článku si ukážeme, kde a jak lze nastavit testování www certifikátu na to, zda nebyl zneplatněn (tedy není uveden v CRL) a zda nebyl zneplatněn certifikát vystavitele tohoto certifikátu. Na závěr si pak řekneme něco málo ke stahování CRL.

Spusťte Internet Explorer. V horním menu vyberte položku **Nástroje –> Možnosti Internetu**

Rozvine se příslušná nabídka. Zde vyberte záložku **Upřesnit**. V seznamu parametrů nalezněte položky **Kontrolovat odvolání certifikátů vydavatele** a **Zjišťovat odvolání certifikátů serveru.** Aby byla prováděna důsledně kontrola certifikátu při vstupu na zabezpečený server (tj. navázání důvěryhodného protokolu SSL) – musíte obě položky mít vybrané. Výběr se provádí obyčejným zaškrtnutím. Aby byla tato akce skutečně účinná, je nutné zavřít příslušný prohlížeč a restartovat PC.



Ano jedna z výše jmenovaných položek není po instalaci (resp. po obnově výchozího nastavení vybrána). Doporučujeme ještě zkontrolovat položku **Upozornit na neplatné certifikáty serverů,** která bývá defaultně nastavena, a proto ji pravděpodobně již máte vybránu.

Máte-li tyto položky nastaveny, je váš prohlížeč správně nastaven pro kontrolu vstupu na zabezpečený server.

Z důvodu vyššího zabezpečení vaší stanice (nesouvisí však s námi zvoleným tématem) doporučujeme mít nastaveny i další tři položky, které nejsou po instalaci nebo po volbě výchozího nastavení vybrány : **Kontrolovat podpisy stažených programů** , **Povolit Integrované ověření systémem Windows** , **Vyprázdnit složku Temporary Internet Files při ukončení prohlížeče.**

Návod k instalaci seznamu zneplatněných certifikátů (CRL)

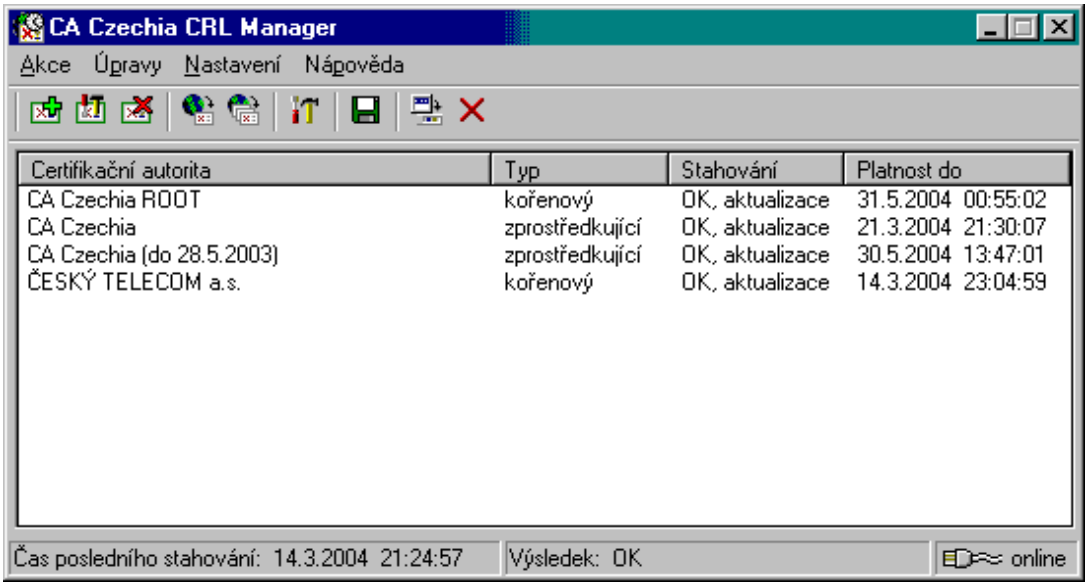
Na závěr si řekneme pár poznámek k využití seznamu zneplatněných certifikátů při ověření platnosti certifikátu. Před vlastní instalací je potřeba seznam zneplatněných certifikátů - Certificate revocation list (dále jen CRL) nejprve stáhnout z webu příslušné certifikační autority kamkoliv na váš pevný disk (nejlépe na plochu). Cesta k tomuto webu a k CRL je uvedena v certifkátu.

Například pro CRL Interní certifikační autority ČESKÝ TELECOM a.s. jej lze stáhnout z adresy : http://www.intca.ct.cz/crl/INT-CA-CRL.crl

Potom stiskněte nad uloženým souborem pravé tlačítko myši a zvolte příkaz **Nainstalovat seznam CRL**. Instalace proběhne za použití *Průvodce importu správce certifikátu* (obdobně jako při importu certifikátu poskytovatele).

Protože ovšem instalace nemusí na některých verzích Windows (především verze 95 a 98) proběhnout korektně a také protože uživatel při ověřování platnosti certifikátů je v některých verzích nucen instalovat CRL manuálně, doporučujeme využít CRL Manager, který stahuje a instaluje CRL v pravidelných intervalech zcela automaticky.

Program tak řeší problémy s aktualizací a navíc poskytuje značný uživatelský komfort pro práci s CRL seznamy. Uživatel si může sám nadefinovat CRL seznamy certifikačních autorit, kterým důvěřuje, nebo může využít již předem definované seznamy známých certifikačních autorit. CRL manager se již sám postará o aktualizace.



Podrobnější informace o programu: http://www.caczechia.cz/start.asp?file=crlmaninfo
Download programu : http://www.caczechia.cz/crlmanager/bin/crlmaninst.exe

B. Jak jsem pochopil ochranu informace, část 2

RNDr. Antonín Beneš, PhD., KSI MFF UK Praha

Minule jsem popsal spoustu papíru ve snaze přesvědčit vás, že celá bezpečnost je zábavně složitý propletenec povětšinou dosti triviálních pravd. Šance utratit hodně peněz a nic za ně nezískat je značná. Na druhou stranu kde není, ani smrt nebere, takže se nutně musíte smířit s tím, že bezpečnost něco stojí – peníze, čas, lidi. Jak najít správné řešení?

Každý dobrý konzultant přes bezpečnost vám poví, že potřebujete bezpečnostní politiku. Nejlépe od něho a když budete tiše naslouchat, můžete slyšet, jak mu v hlavě cinkají vaše miliony.

Základem je vědět, co chcete. Můžete to odhadnout, můžete si nechat poradit, a nebo se můžete podívat do norem. Ty vám napoví, co máte chtít a jak to má vypadat. Navíc existuje spousta organizací, které vydávají certifikáty, že ten který produkt vyhovuje té či oné normě a tak ani nemusíte být experty, abyste si mohli vybrat správně. Normy mají ještě jedno kouzlo – zavádějí jakousi jednotnou kulturu do aplikace bezpečnostních opatření a stanovují srovnatelná kriteria. I když věci rozumíte velmi dobře, můžete normu použít jako vodítko, abyste na nic nezapomněli. V neposlední řadě nemusíte auditorovi, nebo svým partnerům složitě vysvětlovat, jak je to u vás s bezpečností, ale můžete jen několika slovy říci, podle jaké normy a jakého stupně jste dosáhli. Je to stručné a pregnantní.

Někdo rád vdolky, někdo holky. O bezpečnosti to platí přiměřeně, takže nelze čekat, že by se dalo vystačit s jedinou normou. Navíc čas kvapí a jak se vyvíjí svět, chce to nové, lepší normy. Z mnoha desítek, ne-li stovek existujících ukážu tři, na kterých lze pozorovat vývoj normosloví v oboru za posledních asi tak pětadvacet let. Schválně jsem ponechal jistou syrovost textu, aby se zachoval dojem z čtení normy.

Kniha v barvě pomeranče

Klasikou v oblasti bezpečnostních norem je tzv. Trusted Computer System Evaluation Criteria (TCSEC), známá ovšem spíše pod označením Orange Book. To proto, že knižní vydání opravdu má oranžové desky. TCSEC je norma původně vojenská a tak není divu že hlavní důraz klade na důvěrnost informací. Z tohoto pohledu rozděluje systémy do čtyř hlavních tříd a několika podtříd.

- *třída D – žádná ochrana*, pochopí každý
- *třída C - volná ochrana*, jinými slovy požaduje se existence bezpečnostního mechanismu, který uživatel může použít.
  - *podtřída C1* – systém zajišťuje oddělení uživatelů od dat, musí existovat metody umožňující uživatelům chránit vlastní data před ostatními, uživatel si zvolí, zda tyto mechanismy bude používat.
  - *podtřída C2* – stejné požadavky jako C1, navíc ale granularita bezpečnostního mechanismu musí být až na úroveň jednotlivých uživatelů. Musí být veden access log. Požadována je ochrana proti residuím - obsahy paměti, registrů, … tj. daný prostředek je smazán před dalším přidělením.

- *Třída B – povinná ochrana* – tady to začíná být vážné, bezpečnostní mechanismus již musí zajišťovat úplné oddělení subjektů od objektů a nemůže být deaktivován nebo jinak obcházen.
  - *podtřída B1* – tzv. značkovaná ochrana. Každý kontrolovaný subjekt a objekt musí mít přiřazen stupeň utajení a musí být tímto stupněm označen, každý přístup musí být ověřován dle Bell-LaPadula modelu (rozeberu později). Musí existovat popis implementovaného formálního modelu. Systém je v rámci evaluace podrobován testování.
  - *třída B2* – tzv. strukturovaná ochrana. Musí být k dispozici verifikovatelný globální návrh systému. Systém musí být rozdělen do dobře definovaných nezávislých modulů. Návrh musí zohledňovat princip nejmenších možných oprávnění. Bezpečnostní mechanismy musí být uplatňovány vůči všem subjektům a objektům včetně všech zařízení. Musí existovat analýza možných skrytých kanálů. Vlastní systém musí běžet v rámci své bezpečnostní domény a provádět kontroly své integrity
  - *třída B3* – tzv. bezpečnostní domény. Systém musí být podrobitelný extenzivnímu testování, musí být konceptuálně jednoduchý. Musí existovat úplný popis celkové struktury návrhu systému,
  - musí existovat ochranné mechanismy na úrovni jednotlivých objektů, každý přístup musí být testován, kontrola na úrovni provádění jednotlivých typů přístupu daného subjektu
  - Systém musí být vysoce odolný vůči průnikům. Zařízení provádějící audit log musí umět odhadnout hrozící nebezpečí.

- *třída A1 - Verifikovaný návrh.* Návrh systému musí být formálně verifikován. Je vyžadován formální model bezpečnostního mechanismu s důkazem konzistentnosti. Součástí dokumentace musí být formální specifikace systému s ověřením, že odpovídá formálnímu modelu, a ověření, že implementace není odchylná od formální specifikace. Musí existovat formální analýza skrytých kanálů.

Všimněte si na tomto místě, že nestačí vzít na vědomí, že systém má certifikát podle normy XY. Musíte zejména vědět, jakého konkrétně stupně bylo dosaženo, za jakých podmínek a co přesně to znamená. Jinak se vám snadno může stát, že budete za vhodný pro správu kritických kasifikovaných informací považovat systém s hodnocením řekněme C2. Přitom hodnocení C2 znamená, že systém rozezná uživatele od souboru a když tvůrce nezapomene, může systém požádat, aby data nerozdával na potkání. Vy zíráte, my zíráme. Neméně zajímavé je zkoumat, co bylo předmětem certifikace, protože se může ukázat,že certifikován je server na zcela konkrétním HW bez připojení k síti, případně že certifikace se vztahuje pouze na velmi omezenou část jinak komplexního systému.

ITSEC – orange book znovu a lépe

Tvůrci The **I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria (ITSEC) si uvědomili, že bezpečnost se neskrývá jenom ve schopnosti systému zajistit důvěrnost zpracovávaných informací. Jako pasažér na lince Praha – New York spíše oceníte, že navigační systém funguje pořád a správně, než že z něho neuniká žádná informace, a to ani v případě, že čelo stroje již proniká do bezejmenné hory. A tak vznikla norma, která je vhodná pro mnohem širší použití, neboť ve svých kritériích zohledňuje mnohem více rysů informačního systému.

V podstatě můžeme ITSEC chápat jako nadmnožinu osvědčené normy TCSEC. Kriteria byla rozdělena na třídy funkčnosti (F) a korektnosti (E).

- *třídy funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3* obsahem svých požadavků odpovídají třídám C1 až B3 hodnocení TCSEC.

Na rozdíl od TCSEC ale přibyla spousta nových kritérií:

- F-IN – kriteria hodnocení funkčnosti rozdělena na hodnocení integrity systému
- F-AV– dostupnosti systémových zdrojů
- F-DI – integrity dat při komunikaci
- F-DC – utajení komunikace
- F-DX – bezpečnosti v rámci celé sítě

Podstatným myšlenkovým posunem ale je, že každé z těchto kriterií může být vyhodnocováno nezávisle na ostatních. A tak je tedy možné mít certifikovaný systém, který je vysoce spolehlivý, který přitom ve velmi malé, nebo případně žádné míře nezajišťuje utajení. To by podle TCSEC nešlo.

Další důležitou změnou jsou dosud nediskutovaná kriteria korektnosti. Ta totiž popisují ani ne tak vlastní certifikovaný systém, jako spíše proces evaluace. Podívejme se na ně:

- E1 - testování
- E2 - kontrola konfigurace a distribuce
- E3 - ověření detailního návrhu a zdrojového kódu
- E4 - zevrubná analýza slabin systému
- E5 - důkaz, že implementace odpovídá detailnímu návrhu
- E6 - formální modely, formální popisy a jejich vzájemná korespondence

Požadavky každé třídy korektnosti jsou vždy nadmnožinou předchozí třídy. Obsahem odpovídají požadavkům na důvěryhodnost kladeným třídami C2 až A1 hodnocení TCSEC.

Uvažte, že ITSEC je takto poměrně komplexní a velmi pružné kritérium bezpečnosti,které dokáže nezávisle hodnotit mnoho důležitých rysů zkoumaného systému. Přitom každá z posuzovaných vlastností může být podrobena různě rigoróznímu ověřování. Každý si tam může naordinovat bezpečnostní požadavky podle vlastních potřeb.

Common Criteria – všem společná kriteria bezpečnosti

Zdálo by se, že ITSEC by mohl být všelékem. Opak je pravdou. Rostoucí povědomí o bezpečnosti způsobilo v poslední dekádě pravou explozi nejrůznějších oborových norem a požadavků na bezpečnost. Svojí představu mají personalisté, doktoři, letecká doprava, ale i pekaři, chci říci potravinářský průmysl. V případě těch posledních se není čemu divit, potravinářství je dnes už čistá chemie a stačí malá chyba a klobásky budou nejen pikantní, ale i vysoce brizantní.

Přítrž vznikající houštině navzájem nesrovnatelných norem a normiček má učinit jeden z posledních počinů standardizátorů – norma *Common Criteria (CC).* Při prvním přečtení vás udeří do očí, že je to norma, která nic konkrétního nepožaduje. Skutečně, CC jsou metanormou stanovující principy a postupy, jak odvozovat konkrétní technické normy pro vývoj, testování, výsledné vlastnosti a provoz technických bezpečnostních protiopatření

v různých prostředích. Jinými slovy, až budete chtít vlastní bezpečnostní normu řekněme v oblasti provozování veřejných latrín, vezmete CC a v jimi definované obecné struktuře si budete škrtat, co považujete za významné a jak moc. Vyrobíte si normu, která má vaše vlastní konkrétní požadavky, ale standardní strukturu a formu. To je velmi důležité. Uvažte, že výrobci ledniček a vrtaček také nemají mnoho společného, ale skutečnost, že obojí končí stejnou vidlicí do zásuvky vám mimořádně usnadní život.

Common Criteria oddělují, funkcionalitu (co tvůrce říká, že systém dělá) od „zajištění" (jak moc je na zajištění bezpečnosti pamatováno v rámci životního cyklu). Sada konkrétních funkčních a „zajišťovacích" požadavků tvoří *profil zabezpečení (protectin profile).*

Funkční třídy
- FAU - bezpečnostní audit
- FCO – komunikace
- FCS - kryptografická podpora
- FDP - ochrana uživ. Dat
- FIA - identifikace a autentizace
- FMT - bezpečnostní management
- FPR – soukromí
- FTP - ochrana bezp. Mechanismu
- FRU - využívání prostředků
- FTA – přístup
- FTP - důvěryhodná cesta/kanál

Zajišťovací třídy:
- ACM - správa konfigurací
- ADO - dodávka a provoz
- ADV – vývoj
- AGD - dokumentace, návody
- ALC - podpora životního cyklu
- ATE - testování
- AVA - vyhodnocení slabin

Vyhodnocení kvality bezpečnostního mechanismu v rámci evaluačních kriterií potom podléhá následující klasifikaci:
- APE - vyhodnocení profilu bezpečnosti
- ASE - vyhodnocení cíle hodnocení

Zastavím se na chvíli u vyhodnocení kvality bezp. mechanismu. Všimněte si, že nejprve se zkoumá, zda použitý profil bezpečnosti odpovídá vaší konkrétní situaci a až poté se provádí vlastní posuzování předmětného IS.

Podobně jako ITSEC i CC odděleně hodnotí vlastnosti systému proklamované dodavatelem a kvalitu, nebo chcete-li důslednost, provedeného ověřování. Vlastní CC proto úzce souvisí s materiálem *Common Evaluatin Methodology* (CEM). To jsou pravidla pro vyhodnocování konkrétních systémů (cíl evaluace) vůči daným požadavkům (profilům).

Úrovně vyhodnocení (eval. assurance level) dle kriterií:

- EAL1 – funkční testování
- EAL2 – strukturální testování
- EAL3 – metodické testování a kontroly
- EAL4 – metodický návrh, testování a ověření
- EAL5 – semiformální návrh a testování
- EAL6 – semiformálně verifikovaný návrh a testování
- EAL7 – formální návrh a testování

Dvojice CC – CEM tak formalizuje následující proces vyhodnocování vhodnosti, správnosti a dostatečnosti bezpečnostního profilu:
evaluační kriteria → evaluační metodologie → evaluační schéma → evaluace → výsledky evaluace → certifikace → registr certifikátů

Nic ovšem není zadarmo. Orange Book je útlá knížka formátu A5, kterou dáte do kapsy u kabátu, v pohodě přečtete za týden v Metru či ve vlaku a máte JASNO. Tandem Common Criteria – Common Evaluation Methodology do kapsy nedáte, leda byste byli klokan. Je to do kopy přes 1000 stran A4, což je husté, uvážíte-li, že to nic konkrétního neříká. Ale dává nám to naději, že bezpečnost se z oblasti umění pomalu přesouvá mezi běžné technické disciplíny, které mají jednotné normy, podle kterých se vyšívá.

Smutným faktem zůstává, že vlastní proces evaluace je velmi zdlouhavý, jde o měsíce až roky. Příprava na něj je navíc velice nákladná – u vyšších stupňů hodnocení jde řádově o tytéž částky, jako stojí samotný vývoj. Není proto divu, že se výrobci příliš nehrnou a k certifikaci svých produktů přistupují až když to jinak nejde. Tady je chyba na straně nás – uživatelů informačních systémů. Přemýšlejte za domácí úkol, proč je většina lidí ochotna investovat do ABS, airbagů, ESP a dalších „fičurek“, bez kterých by auto taky jezdilo, ale nechtějí ani slyšet, že by to samé měli dělat v případě informačních systémů.

C. Kryptografie a normy - Digitální certifikáty

Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158)

Část 3.

Jaroslav Pinkava, PVT a.s.

1. Úvod

Vracíme se k dokumentu ETSI 102158 (lit. [1]), který specifikuje základní požadavky politiky na prováděcí směrnice atributových autorit vydávající atributové certifikáty určené pro podporu kvalifikovaných elektronických podpisů a jsou tedy dostupné pro používání veřejností a jsou přiřazovány ke kvalifikovaným certifikátům podporujíce tak certifikační politiku "QCP public + SSCD". V první části tohoto článku (Crypto-World 01/2004) byly popsané základní definice, byla zmíněna existence dvou typů atributových certifikačních politik (z hlediska popisu v tomto dokumentu) a diskutována problematika závazků a odpovědností (klienta, subjektů, spoléhajících se stran a samotné atributové autority). V druhé části článku byly popsány požadavky, které se týkají atributové certifikační prováděcí směrnice. V této třetí (věnované dokumentu ETSI 102158) části se budeme zabývat "interními" problematikami atributové autority (životní cyklus podpisového klíče AA a administrativní a řídící procedury AA).

2. Životní cyklus správy klíčů atributové autority

Klíče atributové autority mohou být používány pro následující tři různé účely:

- podepisování atributových certifikátů (AC);
- podepisování ACRL;
- podepisování odpovědí OCSP.

Pro každý z těchto účelů by měl být používán jiný klíč. Atributová autorita musí zajistit kontrolu nad generováním těchto klíčů, konkrétně:

a) generování klíčů atributové autority (AA) musí být prováděno v prostředí fyzicky zabezpečeném, personálem v důvěryhodných rolích (minimálně dva pracovníci). Přitom počet pracovníků, který je oprávněn vykonávat tuto činnost, musí být minimalizován a být v souladu s prováděcí směrnicí AA.

b) generování klíčů atributové autority (AA) musí být prováděno zařízením, které
   - splňuje podmínky z dokumentu CEN WA 14167-1 nebo
   - splňuje podmínky z dokumentu CEN WA 14167-3 nebo
   - v důvěryhodném systému certifikovaném na úroveň EAL-4 či vyšší (dle ISO/IEC 15408 – Common Criteria). Tato činnost musí být popsána jako bezpečnostní cíl či ochranný profil, který splňuje požadavky dané v tomto dokumentu (ETSI 102158), je opřený o analýzu rizik a bere do úvahy i další opatření (fyzické zabezpečení, netechnická bezpečnostní opatření).

c) generování klíčů atributové autority (AA) musí být provedeno s využitím algoritmů, které byly identifikovány jako vhodné pro účely atributových certifikátů.

d) také zvolená délka klíče a zvolený algoritmus pro podpisový klíč AA musí být jedním z algoritmů, který byl identifikován pro tyto účely.

Atributová autorita musí zajistit, že soukromé klíče AA zůstanou utajeny a musí zajistit jejich integritu (nenarušenost). Konkrétně:

- soukromý podpisový klíč AA musí být uchováván v bezpečném kryptografickém zařízení, které splňuje jednu z výše uvedených podmínek (bod b).
- pokud klíče jsou uloženy v odpovídajícím zařízení, musí být provedena kontrola přístupu, která ověří, že klíče nejsou dostupné mimo toto zařízení.

Klíče AA mohou být zálohovány, potom

- mimo bezpečné kryptografické zařízení musí být soukromý podpisový klíč AA chráněn bezpečným kryptografickým algoritmem;
- soukromý podpisový klíč může zálohovat, uchovávat a obnovovat pouze personál v důvěryhodných rolích (minimálně duální kontrola, tj. dva pracovníci);
- záložní kopie musí být chráněny minimálně stejně bezpečně (nebo ještě bezpečněji) jako aktuálně používané klíče;
- pokud jsou klíče uloženy v zálohovacím modulu, musí být uplatněny prostředky kontroly přístupu k tomuto modulu, které zajistí, že k modulu nemá přístup neautorizovaný personál (a přístup je opět s duální kontrolou).

AA musí zajisti neporušenost a autentičnost AA klíčů pro ověření podpisu (veřejných klíčů) a dalších s nimi spojených parametrů. AA klíče pro ověření podpisu musí být zpřístupněny spoléhajícím se stranám způsobem, který zajistí jejich nenarušenost a autentizuje originál. Například AA veřejné klíče mohou být obsaženy (a distribuovány) v certifikátu veřejného klíče, který vydala CA.

Atributová autorita zajistí, že soukromé podpisové klíče nejsou používány neodpovídajícím způsobem. AA podpisové klíče užívané pro podepisování AC nesmí být používány pro jiné účely s výjimkou podepisování ACRL a/anebo podepisování odpovědí OCSP. Podpisové klíče AA, které jsou používané pro podepisování AC mohou být používány pouze při splněných bezpečnostních podmínkách.

AA zajišťuje, že po skončení životního cyklu podpisových klíčů AA nejsou tyto již nadále používány a že všechny kopie těchto klíčů jsou zničeny tak, že nemohou být rekonstruovány.

AA také zajišťuje bezpečnost odpovídajícího kryptografického hardware.

3. Řídící procedury AA

AA zajišťuje, že používané administrativní a správní procedury jsou v souladu s doporučeními z rozpoznaných norem a normativních dokumentů. Obecně AA

- zajišťuje provedení analýzy rizik včetně obchodních rizik a na tomto základě stanoví nezbytné bezpečnostní požadavky a pracovní postupy.
- AA je zodpovědná za všechny aspekty poskytování certifikačních služeb a to i tehdy, když některé služby jsou poskytovány smluvně (outsourcing).
- management vydává směrnice ohledně informační bezpečnosti
- infrastruktura informační bezpečnosti (zajišťující bezpečnost AA) je neustále v provozu. Veškeré změny, které mají dopad na dosaženou úroveň bezpečnosti musí být schváleny managementem AA.
- bezpeční kontroly a pracovní postupy musí být zdokumentovány, implementovány a používány.
- AA musí zajistit bezpečnost informací s nimiž pracuje a to i v případě, že s nimi pracují jiné organizace či entity (outsourcing).

AA zajišťuje odpovídající úroveň bezpečnosti pro všechna svá aktiva a informace, konkrétně musí vést seznam všech informačních aktiv a mít klasifikovány bezpečnostní požadavky vůči všem aktivům, které byly zvažovány v analýze rizik.

AA musí zajisti, že personál a užití příslušných směrnic směřuje k zaručení a podpoře postupů AA. Atributová autorita:

- musí zaměstnávat personál, který má odpovídající odborné znalosti, zkušenosti a kvalifikaci, která je nezbytná pro provádění nabízených služeb a pro zastávanou pracovní funkci.
- bezpečnostní role musí být specifikovány v popisu pracovní náplně. Důvěryhodné role musí být zřetelně identifikovány.
- popis pracovní náplně personálu by měl zahrnovat i požadavky vztahující se k zkušenostem pracovníků.
- personál musí cvičit administrativní a řídící postupy, které vyplývají ze správy informační bezpečnosti AA.
- v řídících funkcích musí být personál, který má dostatečné zkušenosti s technologií elektronického podpisu a je v dostatečném stupni obeznámen s bezpečnostními postupy, odpovědnostmi a má zkušenosti v oblasti informační bezpečnosti a stanovením rizik.
- personál AA v důvěryhodných rolích nesmí mít zájmy, které jsou v konfliktu s pracovními postupy AA.
- důvěryhodné role zahrnují následující odpovědnosti: bezpečnostní ředitel, systémový administrátor, systémový operátor, systémový auditor.
- veškerý AA personál musí být formálně ustaven do důvěryhodných rolí řídícím managementem zodpovědným za bezpečnost.
- AA nesmí zaměstnávat osoby, které nemají čistý trestní rejstřík.

AA zajišťuje, že fyzický přístup ke kritickým službám je pod kontrolou a jsou minimalizována s tím související rizika. Konkrétně:

- fyzický přístup k vybavení AA, které se zabývá generováním AC, správou odvolání je omezen pouze na autorizované jedince;
- je implementován systém kontrol s cílem zabránit ztráty, poškození či kompromitaci aktiv a přerušení obchodní aktivity;
- kontroly zabraňují kompromitaci či krádež informací a vybavení, které informace zpracovává.
- vybavení, které se zabývá generováním atributových certifikátů (a správou odvolání) musí operovat ve fyzicky zabezpečeném prostředí;
- zřetelně jsou definovány odpovídající bezpečnostní zóny
- je implementován celý systém kontrol v návaznosti na zpracovanou bezpečnostní politiku AA(viz ISO 17799).

V příští části budeme pokračovat v popisu řídících procedur AA.

4. Literatura

[1] Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates (ETSI TS 102 158, V.1.1), http://portal.etsi.org/esi/el-sign.asp
[2] rfc3281: An Internet Attribute Certificate Profile for Authorization
[3] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002

D. Archivace elektronických dokumentů
Část 4.
Jaroslav Pinkava, PVT, a.s.

1. Úvod

V minulé části jsme se zmínili o draftu [5], který vznikl v rámci německého projektu Archisig. Projekt Archisig běžel v rámci většího souboru (celkem sedmi) projektů VERNET – "Secure and reliable transactions in open communication networks" a byl rozvržen na období od července roku 201 do září roku 2003. V tomto článku podáme stručný přehled obsahu zmíněného draftu. V současné době je tento dokument jedním z podkladových materiálů skupiny LTANS (http://ltans.edelweb.fr/).

Cílem dokumentu je popis cest při generování a obnově archivačních časových značek. Tyto značky mají za úkol prokázat nepopiratelnou existenci dat i po uběhnutí delšího časového úseku (např. po 30 letech). Postupy pro práci s těmito značkami, pro použité datové formáty a metody zpracování je nezbytné nějakým způsobem standardizovat (prvním pokusem v tomto směru je rfc.3126).

V dokumentu popsaná syntaxe archivních časových značek (ATS - Archive Time-Stamps Syntax) tento přístup dále rozpracovává a zobecňuje (pro data v libovolném formátu, pro práci s velkým množstvím takovýchto dat). S každým souborem je ukládán tzv. "Archive Time-Stamp Element" a to buď jako oddělený soubor, nebo je přímo součástí podepisovaných dat.

2. Požadavky na ATS a celkový přehled problematiky

- nepopiratelnost existence dat musí být zachována i v situacích, kdy použitý hashovací algoritmus či kryptografický algoritmus s veřejným klíčem se stanou slabými či v situacích, kdy vyprší platnost certifikátu či certifikát je odvolán;
- náklady na ATS nesmí být velké ani pro velká množství datových objektů a častou obnovu časových značek. Počet použitých časových značek by přitom měl být minimalizován;
- pro případy, kdy se provádí obnova archivních časových značek (ATS) musí být maximálně omezen přístup k archivovaným datovým objektům (uchovaným např. na vnějších a nepřepisovatelných médiích);
- musí být možné přidat časovou značku k skupině datových objektů, jako jsou soubor a jeho podpis, tak aby měly tutéž archivní časovou značku. Přitom musí zůstat zachována i separátní nepopiratelnost každé součásti této skupiny objektů ;
- pokud bude nezbytné některé z datových objektů odstranit z archivu (např. z bezpečnostních důvodů), nesmí toto vést k rizikům pro prokazování nepopiratelnosti u ostatních objektů;
- musí být možné zašifrovat data před přenosem k poskytovatelům služby a generovat archivní časové značky i pro takto zašifrovaná data. Musí to být přitom provedeno tak, aby tato archivní časové značky sloužily jako důkaz nepopiratelnosti i pro původní nezašifrovaná data.

Základem ATS jsou tzv. rozšířené časové značky (Enhanced Time-Stamps) - v principu jsou to časové značky aplikované na více objektů. Data jsou uspořádána v podobě stromu hashí (lit.[6]), ke každému prvku stromu jsou počítány hashe, časová značka však pouze pro kořen tohoto stromu.

Než nastane situace, kdy použité kryptografické algoritmy již svoji silou nezabezpečují požadovanou bezpečnost, dochází k obnově prostřednictvím vygenerování nové archivní časové značky. Jsou navrženy dvě cesty.
Pro jednoduchou obnovu archivní časové značky je pro původní archivní časovou značku spočten nový hash a nová časová značka. Není přitom nezbytné jít až na původní dokumenty.

Tento postup je možné použít v situacích, kdy ztratil svou bezpečnost některý z algoritmů pro vytvoření konečné časové značky.
Pokud ztráta bezpečnosti se týká hashovacího algoritmu, který byl použit pro vytvoření hashovacícho stromu, pak je nezbytné provést komplexní obnovu hashovacího stromu, tj. spočítat nové jednotlivé hashe a k nim novou archivní časovou značku.

3. Prvek ATS (ATS Element)

Prvkem archivní časové značky rozumí autoři jednotku dat, která je použita k důkazu existence datového objektu či skupiny datových objektů v určitém časovém momentu. Tento ATS prvek obsahuje rozšířené časové značky, které byly generovány v průběhu delšího období a některá nezbytná či užitková data. Má následující syntaxi dle ASN.1:

```
ArchiveTimeStampsElement ::= SEQUENCE {
Version                              INTEGER { v1(1) },
       Usefulinformation             [1] OCTET STRING OPTIONAL,
       Encryption                    [2] EncryptionMethod OPTIONAL,
       ArchiveTimeStampSequence      ArchiveTimeStampSequence}
```

Zde platí následující:
- verze - je to číslo verze syntaxe (z důvodů kompatibility s budoucími variantami této specifikace);
-ArchiveTimeSequence je posloupnost ArchiveTimeStampChain (viz dále)
- usefull information, je nepovinné pole, které lze použít pro uložení dalších užitečných dat, jako jsou názvy souborů, které dokumenty obsahují;
- nepovinné pole encryption obsahuje data nezbytná při dešifraci objektů.

Generování ArchiveTimeStampsElement probíhá následovně:
1. Je zvolen datový objekt či datové objekty (resp. jejich podstatné části - to závisí na aplikaci).
2. Je vytvořena prvotní archivní časová značka (viz dále).
3. Pokud je třeba, je tato časová značka obnovována.

Verifikace pak probíhá následovně:
1. Je zvolen datový objekt či datové objekty, ke kterým byla spočtena archivní časová značka a ověřena správnost této volby.
2. Pokud byl objekt zašifrován, je provedena jeho dešifrace.
3. Je ověřována posloupnost archivních časových značek.

4. Rozšířená časová značka

Rozšířená časová značka má následující syntaxi dle ASN.1:

```
EnhancedTimeStamp ::= SEQUENCE {
```

```
digestAlgorithm AlgorithmIdentifier OPTIONAL,
reducedHashtree [0] SEQUENCE OF {SEQUENCE OPTIONAL,
TimeStamp       ContentInfo}
```

kde digestAlgorithm identifikuje použitý algoritmus a s ním spojené parametry (pro strom hashí) a reducedHashtree obsahuje seznam hodnot hashí.

Seznam hodnot hashí lze generovat v podobě Merklova stromu:

1. Jsou zvoleny datové objekty, ke kterým bude generována časová značka.
2. Zvolen je hashovací algoritmus H a generovány hodnoty hashí datových objektů.
3. Pokud je hashí více než jedna, jsou z hashí vytvořeny skupiny a uspořádány v binárně rostoucím pořadí. Konkatenovány tyto hodnoty jsou vstupem pro výpočet další hashe, která je pak vnitřním uzlem stromu. Postup je opakován až zbyde pouze jen jedna hash.
4. Pro tuto kořenovou hodnotu hashe je spočtena časová značka. hashovací algoritmus pro požadavek na časovou značku musí být týž, který byl použit při vytváření stromu hashí.

Certifikáty (resp. CRL či odpovědi v rámci OCSP) by měly být uloženy v samotné časové značce (dle rfc.3161 resp. dle rfc.3126).
Verifikace rozšířené časové značky probíhá následovně:

1. Je spočten hash h datového objektu (algoritmem z pole digestAlgorithm).
2. Je vyhledána hodnota h v prvním seznamu reducedHashtree (není-li nalezena verifikační postup je ukončen se záporným výsledkem).
3. Jsou konkatenovány hodnoty hashí aktuálního seznamu a spočten nový hash. Tento hash musí být součástí seznamu další vyšší úrovně hashí. Postup pokračuje, dokud není spočtena hodnota kořenového hashe.
4. Je ověřena časová značka.

5. Řetězce a posloupnosti ATS

Rozšířené časové značky jsou používány pro vytváření archivů s časovými značkami. Archivní časová značka dokazuje existenci konkrétního datového objektu či skupiy datových objektů v určitém čase. Pokud v důsledku oslabení použitých algoritmů se vzniklá prvotní časová značka stává neplatnou je třeba vytvořit novou archivní časovou značku.

Jsou použity následovně definované pojmy řetězec a posloupnost časových značek (syntaxe ASN.1):

```
ArchiveTimeStampChain          ::= SEQUENCE OF EnhancedTimeStamp
ArchiveTimeStampSequence       ::= SEQUENCE OF ArchiveTimeStampChain
```

V případě, kdy dochází k obnově stromu hashí (Hash-Tree Renewal) je postupováno následovně:
1. Zvolen bezpečný hashovací algoritmus H.
2. Zvoleny jsou datové objekty, ke kterým se vztahovala původní archivní časová značka a je spočtena hodnota hashe h pomocí H.
3. Jsou konkatenovány řetězce archivních časových značek a spočten hash výsledku ha (s pomocí H).
4. Je Spočtena hodnota h´ = H (h + ha).

5. Je vytvořena nová archivní časová značka a otevřen řetězec ArchiveTimeStampChain, do kterého je značka přidána.

Tento postup je zvolen pouze pokud se slabým stal algoritmus, z jehož pomocí byly počítány hashe v stromu hashí. Pokud je třeba obnovit pouze časovou značku, je generována pouze nová časová značka (z hashe obsahu staré časové značky).

Postup pro verifikaci (a tedy pro potřebný důkaz nepopiratelnosti existence datového objektu v určitém časovém momentu) vyžaduje tedy provést:
- verifikaci prvotní časové značky;
- verifikaci každého ArchiveTimeStampChain dle logiky jeho vzniku a konečně ujištění se, že poslední archivní časová značka je platná.

6. Šifrování

V některých situacích se stává aktuální otázka šifrování archivovaných dat. V takovýchto okolnostech je třeba pečlivě zvažovat použité metody a postupy. Je třeba navíc zajistit, že bude možné následně prokázat , že zašifrovaná dat jednoznačně reprezentují nezašifrované datové objekty, které byly označeny archivními časovými značkami. Všechny údaje nezbytné pro provedení takovéhoto důkazu musí být součástí dat, pro které je vytvářena archivní časová značka. Tyto údaje jsou součástí pole s následující syntaxí:

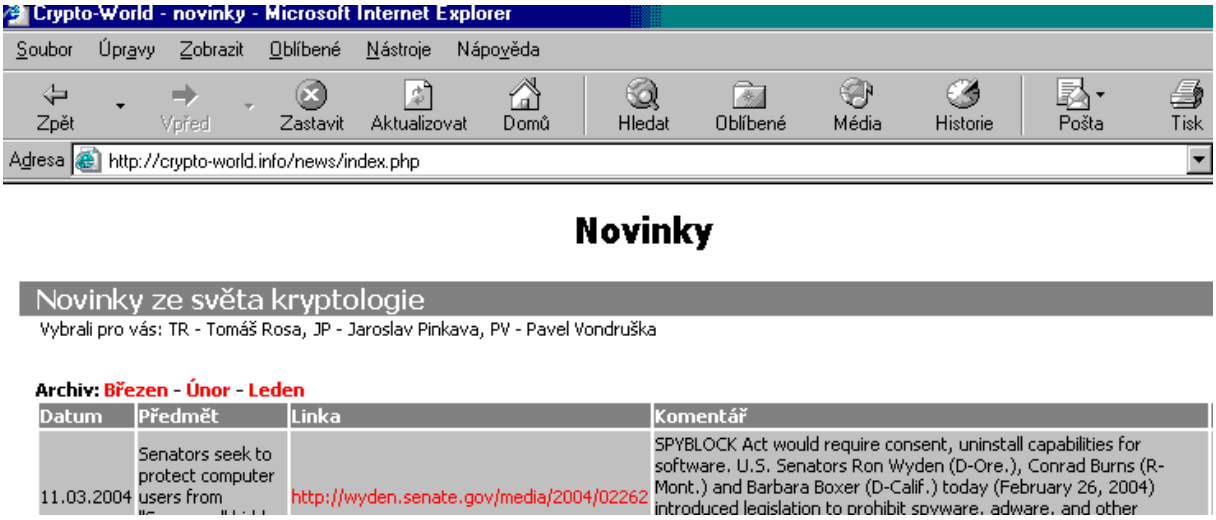
```
Dle ATS je specifikována následující Encryption Method:

 id-EncryptionCMS_encryptedmessage ::= {id-ATS-1}

 CMS_encryption_params::= SEQUENCE {
        encryptionCover ContentInfo,
        encryptionKey  OCTET STRING,
        additional_data CHOICE {
                [0] privateKey   BIT STRING,
                [1] randomValue  BIT STRING}}
```

kde
- encryptionCover je CMS-zpráva (zabalená) bez zašifrovaného obsahu;
- encryptionKey je použitý šifrovací klíč, není součástí údajů, pro které je vytvářena archivní časová značka, ukládán je jinou cestou.

Literatura:
[1] Jaroslav Pinkava: Archivace elektronických dokumentů, Crypto-World 11/2003,1/2004, 2/2004
[2] webovská stránka ltans: http://ltans.edelweb.fr/ .
[3] Long-term Archive Service Requirements draft-ietf-ltans-reqs-01.txt
[4] Projekt ArchiSig: http://www.archisig.de/index.html
[5] Archive Time-Stamps Syntax (ATS), draft-brandner-etal-ats-00.txt - Archive Time-Stamps Syntax (ATS)
[6] Merkle, R. Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA, April 1980): pages 122-134.

E. Letem šifrovým světem

Od 15.2.2004 (tj. od rozeslání posledního čísla Crypto-Worldu 2/2004 do vydání tohoto čísla) se v oblasti bezpečnosti IT a v kryptologii uskutečnila řada zajímavých událostí. Část z nich jsme průběžně zaznamenávali v novinkách na domácí stránce našeho e-zinu (http://crypto-world.info/news/). Tyto novinky pro vás připravili Tomáš Rosa, Jaroslav Pinkava a Pavel Vondruška.



Podívejme se krátce, co tento měsíc přinesl.

Normy a standardy

Období bylo neobyčejně bohaté na normotvornou a standardizační činnost.
(odkazy na jmenované standardy vyhledáte v sekci news na domácí stránce Crypto-Worldu nebo je naleznete přímo na stránkách příslušných standardizačních organizací).

1) **Organizace NIST** (National Institute od Standards and Technology) vydala dva zajímavé dokumenty. Jednak doplněk ke standardu popisujícímu hashovací funkce řady SHA FIPS 180-2 SHA, ve kterém je diskutována nedávno vyhlášená specifikace SHA-224 a dále DRAFT Special Publication 800-67 (Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher), který upravuje použití algoritmu TDES (dříve označován jako Triple DES). Podle tohoto návrhu se předpokládá využívání algoritmu TDEA souběžně s AES minimálně do roku 2030. Jiné implementace DES (než popsané v tomto dokumentu) nebudou povoleny pro použití ve státní správě US.

2) **Organizace ETSI** vydala dva důležité dokumenty z oblasti elektronického podpisu (Technical Report), které obsahují požadavky na harmonizaci v této oblasti. Jsou to TR 102 047 (International Harmonization of Electronic Signature Formats) a TR 102 040 v1.2.1 (International Harmonization of Policy Requirements for CAs issuing Certificates).
Organizace ETSI dále naplánovala na rok 2004 revizi technických specifikací požadavků na certifikační politiku poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty (dokumenty TS 101 456 a TS 102 042).

3) Mezi zajímavé de-facto standardy z oblasti kryptologie vydané jako **RFC** bezesporu patří druhý draft RSASSA-PSS, RSA-OAEP, který je doplňkem dokumentu rfc.3279. Jsou v něm popsány konvence pro přídavné algoritmy a identifikátory k algoritmu RSA. Po této druhé verzi by již mělo následovat příslušné rfc.
Velice zajímavé je i RFC 3709 (Logotypes in X.509 Certificates, Internet X.509 Public Key Infrastructure). V dokumentu jsou definovány extense (logotypes) určené pro "klasické PKI" certifikáty a atributové certifikáty, které umožňují vkládat do certifikátu obrázek - fotku držitele, logo apod. nebo dokonce krátké zvukové nebo obrazové záznamy (avi/mpeg).

Útok proti MD5

Začátkem března byl zahájen dlouho očekávaný globální distribuovaný útok hrubou silou na MD5 (http://www.md5crk.com/). Skupina experimentálních kryptoanalytiků se rozhodla pomocí útoku hrubou silou najít alespoň jednu kolizi hašovací funkce MD5 a pokořit tím její bezpečnost. Projekt je založen na často využívaném principu sdílení výpočetní síly, kdy každý, kdo chce, může instalací příslušného klienta poskytnout část výkonu svého počítače. Doba běhu celého projektu je odhadována na cca 2 roky. Vlastní útok je velmi obecný a je postaven čistě na faktu, že MD5 má malou délku výstupu (128 b). Pokud se chcete o použitém postupu luštění dozvědět víc, můžete využít čtivý článek Tomáše Rosy, který vyšel v roce 2001 v časopise CHIP
ftp://ftp.decros.cz/pub/Archiv/Publications/2001/chip-2001-08-131-133.pdf

Boj proti spamu, spywaru atd.

Ve světě pokračovaly iniciativy spojené se zajištěním větší bezpečnosti Internetu a bojem proti spamu, spywaru apod. Za všechny jmenujme alespoň dvě:

1) Americký návrh zákona "SPYBLOCK Act", který koncem února představil senátor Ron Wyden. Zákon má zajistit ochranu soukromých počítačů amerických občanů tím, že zakáže aktivity typu spyware, adware a dalších softwarů, které se jako nevyžádané ukládají na počítače uživatelů Internetu.

2) Dále je nutné samozřejmě zmínit iniciativu představenou šéfem Microsoftu Billem Gatesem, která má zajistit vizi bezpečné e-mailové komunikace (iniciativu známou jako Caller ID).

Bezpečnost SecurID karet

Poslední informace je věnována bezpečnosti i v Čechách oblíbeným SecurID kartám, které se používají k autentizaci – např. při vzdáleném přístupu do informačního systému. Na stránce http://www.crypto-world.com/securid_faq naleznete nejen stručný a výstižný popis bezpečnostního problému některých typů SecurID karet, ale i odkazy na práci Alexe Biryukova, Joe Lanoa a Barta Preneela, ve které je příslušný útok popsán, a dále na práci Scotta Continiho, který útok významně optimalizoval.

VIII. O čem jsme psali v březnu 2000 - 2003

Crypto-World 3/2000

A. Typy elektronických podpisů (P.Vondruška) 2 - 9
B. Tiskové prohlášení č.14, Microsoft, 15.2.2001 10
C. Kryptografický modul MicroCzech I. (P. Vondruška) 11 - 16
D. Názor na článek J.Hrubý, I.Mokoš z 2/2001 (P. Vondruška) 17 - 18
E. Názor na článek J.Hrubý, I.Mokoš z 2/2001 (J. Pinkava) 19 - 20
F. Letem šifrovým světem 21 - 22
G. Závěrečné informace 23

Crypto-World 3/2001

A. Nehledá Vás FBI ? (P.Vondruška) 2-3
B. Aktuality z problematiky eliptických křivek v kryptografii (J. Pinkava) 3-4
C. Hrajeme si s mobilním telefonem Nokia (anonym) 5
D. TISKOVÉ PROHLÁŠENÍ - POZMĚŇOVACÍ NÁVRHY K ZÁKONU O ELEKTRONICKÉM PODPISU BUDE PROJEDNÁVAT HOSPODÁŘSKÝ VÝBOR PARLAMENTU 6
E. Digital Signature Standard (DSS) 7-8
F. Matematické principy informační bezpečnosti 9
G. Letem šifrovým světem 9-10
H. Závěrečné informace 11

Crypto-World 3/2002

A. Vysvětlení základních pojmů zákona o elektronickém podpisu (D.Bosáková, P.Vondruška) 2-17
B. Digitální certifikáty. IETF-PKIX část 1. (J.Pinkava) 17-20
C. Bezpečnost RSA – význačný posun? (J.Pinkava) 21
D. Terminologie II. (V.Klíma) 22
E. Letem šifrovým světem 23-26
   1. O čem jsme psali v březnu roku 2000 a 2001
   2. Encryption in corporate networks can be 'pried open'
   3. ISO-registr kryptografických algoritmů byl zpřístupněn On-Line!
   4. Velikonoční kryptobesídka , 3. - 4. dubna 2002 v Brno
   5. Uľahčí elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti, 20.2.2002, Bratislava
   6. Seminář GnuPG, 5. 4. 2002 v Praze
   7. DATAKON 2002, 19. - 22. 10. 2002, Brno

Crypto-World 3/2003

A. České technické normy a svět, III.část (Národní normalizační proces) (P.Vondruška) 2 – 6
B. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem (P. Wallenfels) 7-10
C. Digitální certifikáty. IETF-PKIX část 10. CVP(J.Pinkava) 11-13
D. Obecnost neznamená nejednoznačnost, aneb ještě malá poznámka k některým nedostatkům zákona o elektronickém podpisu před jeho novelizací (J.Matejka) 14-19
E. Letem šifrovým světem 20-23
F. Závěrečné informace 24
Příloha : crypto_p3.pdf
Mezinárodní a zahraniční normalizační instituce 3 strany

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 21 dní po jeho rozeslání) a předchozí sešity GCUCMP, informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

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

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@ct.cz