Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 5/2003 **19. květen 2003**

5/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(430 e-mail výtisků)

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. E-podpisy ?
Pavel Vondruška, ČESKÝ TELECOM, a.s.

Kdo se prokousal naším zákonem o elektronickém podpisu a naučil se rozeznávat různé zde použité kategorie (elektronický podpis, zaručený elektronický podpis, zaručený elektronický podpis založený na certifikátu, zaručený elektronický podpis založený na kvalifikovaném certifikátu, zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele, kvalifikovaný podpis) a vnímá rozdíl mezi elektronickým podpisem a digitálním podpisem, může si myslet, že jej v této oblasti kategorizace podpisů již nic příliš překvapit nemůže. Jenže existují i další typy podpisů, které se do předchozích škatulek tak úplně nevejdou. Právě několika takovým případům je věnován tento krátký příspěvek, který jsem nazval „e-podpisy s otazníkem“.

I. Strojový podpis

Úvodem (a pouze pro rozcvičku) uvádím známé dilema našeho zákona. Zákon zná pouze elektronické podpisy fyzických osob (viz příslušné definice zákona o elektronickém podpisu č.227/2000 Sb.). Na první pohled je to jistě v pořádku, ale jsou situace, kdy by bylo dobré např. automaticky potvrdit přijetí dokumentu a toto přijetí pro vyšší váhu „podepsat“. Technicky samozřejmě není žádný problém např. v elektronické podatelně vystavit doručenku a tu digitálně podepsat a odeslat příslušnému odesílateli, ale digitální podpis na doručence není elektronickým podpisem ve smyslu našeho zákona a nemůže nahradit podpis fyzické osoby (např. obsluhu podatelny).

II. Vícenásobné podpisy (Multi-Signatures)

Tento zdánlivě jednoduchý problém, jak uvidíme, bude motivací k definování celé řady podpisů, které se od sebe svými vlastnostmi výrazně liší.

Popis problému : mějme zprávu M, kterou chceme opatřit podpisy skupiny n různých uživatelů.

První přirozené řešení je, že každý z n uživatelů podepíše svým soukromým klíčem SK_i (i = 1, .., n) zprávu M a získáme tak celkem n podpisů (S_1 , S_2 , … , S_n). Při ověření musí ověřovatel postupně pomocí veřejných klíčů VK_i (i = 1, .., n) ověřit všechny podpisy S_1 až S_n.

Druhé přirozené řešení je, že první z n uživatelů podepíše svým soukromým klíčem SK_1 zprávu M, tuto zprávu opatřenou jeho podpisem označme $S_1(M)$. Druhý z uživatelů podepíše svým soukromým klíčem SK_2 zprávu M včetně přidaného elektronického podpisu – tedy $S_1(M)$ a tak postupujeme dále. Poslední n-tý podepisující podepíše svým soukromým klíčem SK_n zprávu $S_{n-1}(S_{n-2}(S_{n-3}(….(S_2(S_1(M)))…)))$. Při ověření musí ověřovatel postupně pomocí veřejných klíčů VK_i (i = n, .., 1) ověřit všechny podpisy S_n až S_1. Výhodou této metody je, že je jednoznačně určeno pořadí, ve kterém se podepisující osoby 1 až n podepisovaly.

Motivací pro další úvahy bude hledání řešení, kdy nebude muset ověřovatel ověřovat n podpisů. Neexistuje nějaké „jednodušší“ řešení pro vytváření podpisu skupiny n uživatelů ke zprávě M (nebo dokonce k více zprávám), kdybychom jedním ověřením zjistili, že všichni uživatelé se podepsali a jejich podpisy jsou platné? Co když budeme pomocí podpisů skupiny uživatelů potřebovat zajistit a ověřit jen některé specifické vlastnosti? Možné návrhy některých řešení těchto problémů si ukážeme v následujících odstavcích.

III. Kruhový podpis (Ring Signatures)

Začneme podpisem, který předchozí problém zdaleka ještě neřeší, ale pro další úvahy může být užitečný.

Mějme skupinu n různých uživatelů, kterou označíme U. Každý z těchto n uživatelů má svá párová data (soukromý a veřejný klíč). Párová data i-tého uživatele označíme : (SK_i , VK_i) . Kruhový podpis skupiny uživatelů U se vytváří pomocí všech n veřejných klíčů uživatelů této skupiny a jednoho soukromého klíče libovolného (např. i-tého) uživatele ze skupiny U. Formálně se tedy dá zapsat kruhový podpis skupiny U jako R(VK_1 , VK_2 , … , VK_n , SK_i), kde i je libovolná hodnota od 1 do n. Podmínkou, abychom takovou hodnotu R mohli nazývat kruhovým podpisem je, že :

- ověřovatel musí být schopen ověřit podpis ze znalosti všech n veřejných klíčů,
- nelze podpis R vytvořit bez znalosti alespoň jednoho z n soukromých klíčů,
- ověřovatel nezjistí, čí soukromý klíč SK_i byl použit ! (tato vlastnost se označuje jako podpisová nejednoznačnost)

Jinými slovy takto zkonstruovaný podpis může vytvořit každý ze skupiny U. Ověřovatel pouze zjistí, že podpis vytvořil jeden z uživatelů této skupiny, nezjistí však který. Kruhový podpis se hodí k prokazování příslušnosti ke skupině U. Může být použit jako podpis za skupinu U, ale se zachováním anonymity podepisujícího a s možným nesouhlasem ostatních členů skupiny.

Definice a možné aplikace takovéhoto podpisu naleznete například v příspěvku Rivesta, Shamira a Taumana How to leak a secret.

R.Rivest, A.Shamir, Y.Tauman : How to leak a secret. In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 552-65. Springer - Verlag, 2001.

IV. Skupinové podpisy (Group Signatures)

Existuje již celá řada různých modifikací schémat skupinového podpisu. Ve schématu představeném Chaumem a Heystem v roce 1991 se předpokládá vytvoření skupiny n uživatelů, která je spravována jedním manažerem. Pro tuto skupinu je vytvořen jeden ověřovací klíč nazývaný gpk (group public key). Každý člen skupiny má svůj vlastní podepisovací soukromý klíč, který je vytvořen tak, že „relativně odpovídá“ veřejnému skupinovému klíči gpk.

Vlastnosti :

- každý může ověřit, že někdo ze skupiny, kterou manažer spravuje, zprávu podepsal
- manažer skupiny pomocí speciálního klíče gmsk může zjistit, kdo ze skupiny zprávu podepsal (traceability)
- kdo nemá k dispozici maskovací klíč, nemůže zjistit, kdo ze skupiny podpis vytvořil (anonymity)
- zveřejnění klíče gmsk nevede k „oslabení“ podpisového schématu (tj. podpisy, které lze ověřit klíčem gpk, mohou i nadále vytvořit pouze členové skupiny daného manažera)

Postupem času bylo schéma modifikováno a byla zapracována a analyzována řada dalších možných požadavků např. neoddělitelnosti ze skupiny (unlinkabilita), omluvitelnost

(exculpabilita), různé typy odolnosti (collusion resistence, framing resistence), plná anonymita (full anonymity) . Přesné definice najdete například ve známých pracích G.Ateniesse.

D.Chaum, E. van Heyst: Group Signatures. In Proceedings of Eurocrypt 1991, volume 547 of LNCS, pages 257-265. Springer - Verlag, 1991.

G.Ateniese, G.Tsudik: Some open issues and directions in group signatures. In Financial Crypto ´99, volume 1648 of lNCS, pages 196-211. Springer - Verlag, 1999.

M.Bellare, D.Micciancio, B.Warinschi: Foundations of Group Signatures : Formal Definitions. Simplified Requirements, and a Construction Based on General Assumptions. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 614-30. Springer - Verlag, 2003.

V. Hromadné podpisy (Aggregate Signatures)

Zobecněním předchozího problému je tzv. hromadný podpis. Stručně jej lze charakterizovat takto: hromadný podpis je podpisové schéma, které umožňuje shlukování stávajících podpisů – tj. z n podpisů n různých zpráv, které vytvořilo n osob, lze vytvořit jediný krátký podpis, jehož ověřením se ověří všech n dílčích podpisů n osob k n zprávám.

Pravděpodobně je to jasné, ale přece jen uvedu, že hromadným podpisem není podpis S nějaké osoby (byť by to byl některý z výše uvedených uživatelů u_i), který vznikne podepsáním zprávy sestavené z podpisů $S_1 \dots S_n$. Takovýto podpis není závislý na platnosti, či neplatnosti jednotlivých podpisů S_i , a proto nesplňuje požadavek, že jeho ověřením se ověří jednotlivé podpisy S_i.

Formální konstrukce hromadného podpisu je následující :

Označíme-li S_i podpis i-tého uživatele u_i ke zprávě M_i , pak hodnota A bude hromadným podpisem vytvořeným pomocí hromadného podpisového schématu AS , pokud $A= AS ((u_1 , S_1 , M_1) , (u_2 , S_2 , M_2), \dots , (u_n , S_n , M_n))$, splňuje následující podmínky :

- A nelze vytvořit bez podpisů $S_1 \dots S_n$.
- ověření A je možné pouze tehdy pokud jsou platné všechny podpisy $S_1 \dots S_n$.

Hromadný podpis je výhodný vzhledem k tomu, že umožňuje snížit počet ověření n podpisů na jedno ověření a velkou výhodou je i snížení počtu certifikačních cest (chain).

S.Kent, C.Lynn, K.Seo: Secure border gateway protocol (Secure-BGP).IEEE J.Selected Areas in Comm., 18(4), pages 582-92, April 2000.

D.Boneh, C.Gentry, B.Lynn, H.Schaham: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 416-32. Springer - Verlag, 2003.

VI .Závěr

Výše uvedené typy podpisů nejsou jen kryptologickou hrátkou na sestavování nových možných protokolů, ale vzhledem k zajímavým „ekonomickým“ vlastnostem při ověřování podpisu, případně vzhledem k zcela novým možnostem (podpis se zachováním plné anonymity, prokazatelnost příslušnosti ke skupině apod.) se dá očekávat, že budou využívány pro speciální situace nebo se dokonce stanou běžným vybavením podpisových prostředků.

B. RFC (Request For Comment)
Pavel Vondruška, ČESKÝ TELECOM, a.s.

Náš krátký seriál bude pokračovat vyprávěním o de facto standardu RFC.

I.Úvod

Historickým vývojem vznikla tradice publikování dokumentů RFC. Její počátek se datuje do roku 1969 a souvisí se zprovozněním ARPANETu, ze kterého se později vyvinul dnešní Internet (blíže viz : 30 Years of RFCs, ftp://ftp.rfc-editor.org/in-notes/rfc2555.txt).

Postgraduální studenti a další řešitelé ARPANETu, kterým jejich postavení neumožňovalo, aby své četné nápady a podněty (mnohdy velmi užitečné a podnětné) nějak vnucovali svým profesorům a intenzivněji se domáhali jejich pozornosti, začali své návrhy sepisovat ve formě dokumentů, kterým dali výstižné pojmenování Request For Comment (doslova: žádost o komentář). Tyto dokumenty předkládali těm, kterých se týkaly, resp. kteří byli kompetentní je posuzovat, přijímat požadovaná rozhodnutí apod.

Tradice publikování dokumentů RFC vydržela až do dnešních dnů. Změnil se ale věcný obsah a celkový smysl dokumentů RFC - s postupem času to stále méně byly náměty a nápady, usilující o vznik nějakého řešení, a čím dál tím více to je popis nového řešení.

Dnes jsou dokumenty RFC používány jako specifická forma dokumentace, vydávána pro potřeby nejširší komunity kolem Internetu. „Vydavatelem“ RFC je IETF (*Internet Engineering Task Force).*

Autorem (navrhovatelem) RFC může být prakticky každý. Formální stránka dokumentu a proces schvalování jsou upraveny v publikaci Guidelines to Authors of Internet-Drafts (poslední změna dokumentu byla 5.září 2002 , ftp://ftp.ietf.org/ietf/1id-guidelines.txt).

Pro správné pochopení významu dokumentů RFC je potřebné ještě uvědomit a náležitě zdůraznit, že jejich obsahem nejsou zdaleka jen standardy - tedy popisy řešení, které mají povahu závazných standardů (byť standardů "de facto", a nikoli "de jure", ale přesto velmi důsledně uznávaných a dodržovaných). Ve formě dokumentů RFC jsou vydávány i jiné dokumenty, například návody, doporučení, či vysvětlení, a v poslední době i stanoviska a názory. Do dnešního dne bylo vydáno více než 3500 dokumentů RFC a početně mezi nimi převažují právě takovéto ne-standardy. Faktických standardů je tedy početně méně. Obecně se považují RFC za bezkonkurenčně „nejčtivější“ specifikace (doporučuji srovnat zejména s doporučeními ITU-T nebo normami IEEE či ISO).

II. Dostupnost dokumentů

RFC jsou veřejně dostupná (http://www.ietf.org/rfc.html), ale zdaleka ne všechno to jsou standardy v rámci internetové komunity.

V listopadu 2001 bylo pouze 61 RFC schválenými, plnoprávnými *de facto* normami (*RFC 3000 Internet Official Protocol Standards*) a jsou vyjma čísla RFC také označeny číslem normy (STD #). K 15.5.2003 je celkem 62 takovýchto specifických norem.

Dokumenty RFC v celkovém počtu 3536 (k 15.5.2003) již obsahují statisíce stránek textu. Pro vyhledávání se dá využít tzv. index, který je dostupný na : http://www.ietf.org/iesg/1rfc_index.txt , součástí citace v indexu je i aktuální status dokumentu.

Od května 2002 si můžete také nechat zasílat všechna nově vyšlá RFC na svoji e-mailovou adresu. Zapsat do distribučního seznamu (nebo naopak vyjmout z tohoto seznamu) se můžete na adrese: http://mailman.rfc-editor.org/mailman/listinfo/rfc-dist

III. Číslování dokumentů (RFC number)

Dokumenty RFC jsou číslovány - každý nově vydaný dokument je opatřen svým pořadovým číslem, a pod tímto číslem je také nejsnáze a přitom i jednoznačně identifikovatelný (k jednoznačnému určení stačí např. zápisy jako RFC1234, RFC2003 apod.). Další významnou vlastností dokumentů RFC je skutečnost, že se nikdy nemění - jakmile je konkrétní dokument jednou vydán pod určitým pořadovým číslem, nemění se ani jeho číslo, ani jeho obsah (ani jeho slovní název). Je-li potřeba provést nějakou změnu v tom, co dokument RFC popisuje, neřeší se to změnou již existujícího dokumentu RFC, ale vydáním nového dokumentu, s novým pořadovým číslem (takovým, jaké je právě "na řadě". Tento nový dokument RFC pak ve svém záhlaví nese poznámku o tom, že "zneplatňuje" předchozí dokument RFC s příslušným číslem (ev. několik takovýchto dokumentů).

IV. Typy dokumentů

(The Internet Standards Process -- Revision 3, ftp://ftp.isi.edu/in-notes/rfc2026.txt)

Proposed standards
Draft standards
Internet standards (plné de facto normy)
Experimental
Informational
Prototype
Historic

Standards Track - Proposed Standard, Draft Standard, Internet Standard

První tři skupiny skupiny tvoří vlastně tři stádia, kterými musí projít každý návrh na cestě k definitivní podobě standardu (tedy: Proposed Standard, Draft Standard a Internet Standard). Představují jednu konkrétní trajektorii, určenou pro takové dokumenty, které aspirují na to, aby se staly standardem. Této trajektorii se přitom říká "Standards Track".

Každé řešení, které se má stát standardem, musí být předloženo nejprve ve formě tzv. navrhovaného standardu (Proposed Standard), a musí prokázat svou životaschopnost nejméně na dvou na sobě nezávislých implementacích. Nejdříve po půl roce pak může návrh přejít do stádia "Draft Standard" (předběžný standard), ve kterém se musí zdržet nejméně čtvrt roku, a k postupu do finálního stádia "definitivního standardu" (Internet Standard) musí být nashromážděny dostatečné provozní zkušenosti s příslušným řešením. Během všech tří těchto stádií jsou příslušné dokumenty publikovány jako dokumenty RFC.

Off-Track – Informational, Experimental, Prototype, Historic

Vedle výše popsané trajektorie "Standards Track“ existuje i druhá trajektorie, označovaná "Off-Track", do které patří hned čtyři druhy dokumentů (přičemž termín "trajektorie", resp. anglické "track", zde není až tak na místě, protože většina dokumentů zde "nepostupuje" podobným způsobem, jako je tomu u návrhů standardů). Patří sem čtyři kategorie dokumentů RFC: informational, experimental, prototype a konečně historic.

Informational RFC (informační) označuje dokument, který je zamýšlen jako informativní materiál - tedy takový, který vysvětluje, radí, přináší doplňující informace atd. Dokumentů RFC tohoto typu je početně zdaleka nejvíce.

Experimental RFC (experimentální) – takto označené dokumenty obsahují zajímavé informace o protokolech a technologiích, které nemají zřejmou šanci se masově ujmout, ale je dobré o nich veřejně vědět.

Prototype RFC – jedná se o řešení, která jsou zatím ve stádiu experimentu, ale se záměrem někdy v budoucnu přejít do "standards-track" a stát se standardem.

Historic RFC (historickou) se specifikace stává, jestliže je překonána svým následovníkem a/nebo se úplně přestane v Internetu používat.

V. RFC – jiné členění

Standard (STD)

Skutečnost, že dokument RFC se nikdy nemění, přináší mnoho výhod, ale také některé nevýhody. Nikomu se sice nemůže stát, že by měl v ruce neaktuální exemplář konkrétního dokumentu RFC (s konkrétním číslem), ale může se mu stát, že se zabývá určitou problematikou a má v ruce dokument RFC řešící tuto problematiku, který již byl překonán (zneplatněn) novějším dokumentem RFC, který řeší tutéž problematiku. Aby se nedorozuměním tohoto typu předešlo, zavedla se časem další klasifikace dokumentů RFC, označovaná nyní jako STD (od: standard). Důvodem pro její specifické pojmenování je fakt, že je omezena jen na dokumenty charakteru platných standardů (Internet Standard), a netýká se tedy všech dokumentů RFC. Pro názornou představu je možné připodobnit dokument RFC k prázdným deskám (rychlovazači), které mají na svém hřbetě pevně nadepsanou určitou konkrétní problematiku - do těchto "desek" se pak vkládají ty dokumenty RFC, které se zabývají příslušnou problematikou a v daném okamžiku nebyly zneplatněny novějšími dokumenty RFC. Dokument STD je tedy vždy totožný s některým dokumentem RFC (nebo s několika dokumenty RFC, které řeší jednotlivé části dané problematiky), ale na rozdíl od dokumentů RFC se dokumenty STD v čase mění (je vyměněn obsah pomyslných desek novým dokumentem RFC). Nikomu se tedy nemůže stát, že by měl v ruce dokument STD, který je překonán jiným dokumentem STD řešícím stejnou problematiku - na druhé straně se ale může stát, že někdo bude mít v ruce již neaktuální verzi dokumentu STD ("desky se starým obsahem").

FYI (For Your Information)

Dalším typem dokumentů RFC (resp. jejich jinak uspořádanou podmnožinou) se staly dokumenty FYI (doslova: pro vaši informaci). Jde o základní informační dokumenty, určené zejména pro začínající uživatele Internetu. Opět je nejlépe si je představit jako pevně nadepsané "desky", do kterých jsou vloženy konkrétní dokumenty RFC.

BCP (Best Current Practices)

Nejnovější "reinkarnací" dokumentů RFC je série dokumentů BCP (Best Current Practices, ve volném překladu: nejvhodnější postupy a praktiky). Jde o specifickou řadu dokumentů, které vyjadřují stanoviska, názory a postoje a doporučené postupy velmi široké Internetové komunity (příkladem může být postoj ke spammingu).

VI. Aprílová čísla

Dokumenty RFC jsou datovány pouze měsícem a rokem zveřejnění. Výjimkou jsou některá aprílová RFC. V indexu můžete u některých z nich najít datum zveřejnění 1 April. V těchto případech se nejedná o vážně míněné dokumenty RFC, ale jde o dílka, která vtipným způsobem (obsahem i zpracováním) jsou parodií na skutečná RFC.

```
3091 Pi Digit Generation Protocol. H. Kennedy. Apr-01-2001. (Format:
 TXT=10375 bytes) (Status: INFORMATIONAL)
```

```
3092 Etymology of "Foo". D. Eastlake 3rd, C. Manros, E. Raymond.
 April-01-2001. (Format: TXT=29235 bytes) (Status: INFORMATIONAL)

3093 Firewall Enhancement Protocol (FEP). M. Gaynor, S. Bradner.
 April-01-2001. (Format: TXT=22405 bytes) (Status: INFORMATIONAL)

3251 Electricity over IP. B. Rajagopalan. April-01-2002. (Format:
 TXT=18994 bytes) (Status: INFORMATIONAL)

3252 Binary Lexical Octet Ad-hoc Transport. H. Kennedy. April-01-2002.
 (Format: TXT=25962 bytes) (Status: INFORMATIONAL)

3514 The Security Flag in the IPv4 Header. S. Bellovin. 1 April 2003.
 (Format: TXT=11211 bytes) (Status: INFORMATIONAL)
```

VII. Přehled RFC pro PKI
(Internet X.509 Public Key Infrastructure)

RFC 2510 : Certificate Management Protocols
RFC 2511 : Internet X.509 Certificate Request Message Format
RFC 2459 : Certificate and CRL Profile
RFC 2527 : Certificate Policy and Certification Practices Framework
RFC 2528 : Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
RFC 2559 : Operational Protocols - LDAPv2
RFC 2560 : Online Certificate Status Protocol - OCSP
RFC 2585 : Operational Protocols: FTP and HTTP
RFC 2587 : LDAPv2 Schema
RFC 2797 : Certificate Management Messages over CMS
RFC 2802 : Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP)
RFC 2807 : XML Signature Requirements
RFC 3039 : Qualified Certificate Profile
RFC 3161 : Time-Stamp Protocol (TSP)
RFC 3279 : Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 : Certificate and Certificate Revocation List (CRL) Profile
RFC 3281 : An Internet Attribute Certificate Profile for Authorization

Všechna tato RFC naleznete na http://crypto-world.info/normy/index.htm .

Literatura

- „domácí www stránka RFC“ : konkrétní odkazy použity v textu
- Jiří Peterka : Páni Internetu , Standardizace v Internetu , Dokumenty RFC,
- Rita Pužmanová : Jak se orientovat v RFC aneb Průvodce profesionála, Lupa, 30.4.2002
- Pavel Vondruška : Normy a standardy, přednáška na MFF UK Praha, květen 2003

C. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 12. Atributové certifikáty – profil dle rfc.3281 – díl 1.

Jaroslav Pinkava, PVT a.s.

1. Úvod

S problematikou atributových certifikátů se v českém jazyce lze seznámit např. v přehledovém článku [3] . V tomto článku jsou trochu podrobněji rozebrány takové pojmy jako atributový certifikát, atributová autorita a PMI (Privilege Management Infrastructure). Práce s atributovými certifikáty vychází zejména s novější verze normy X.509 (lit. [2]) – čtvrtá verze z roku 2000.

2. Základní definice

Nejprve stručně k použitým pojmům:
Atributový certifikát (AC): Datová struktura digitálně podepsaná atributovou autoritou, která propojuje některé hodnoty atributů s informacemi o identifikaci jejich držitele.
Atributová Autorita (AA): Autorita, která přiřazuje oprávnění vydáváním atributových certifikátů.
oprávnění: Atribut či vlastnost, která je entitě přiřazena autoritou.
uživatel AC: libovolná entita, která zpracovává AC
ověřovatel AC: libovolná entita, která ověřuje platnost AC a využívá výsledek tohoto ověření;
vydavatel AC: entita, která podepsala AC (=AA);
nositel AC: entita označená (možná nepřímo) v poli nositele AC;
klient: entita, která požaduje provedení akce pro níž bylo provedeno ověření;

Je dobré mít na paměti, že atributový certifikát na rozdíl od klasického certifikátu veřejného klíče neobsahuje žádný klíč.

Můžeme si také napomoci následující analogií. Certifikát veřejného klíče lze považovat za občanský průkaz (pas), s jehož pomocí je ověřována totožnost uživatele, platí po dlouhé období, je obtížné ho padělat a existuje přísný postup pro autentizaci žadatele o tento certifikát. Atributový certifikát je potom něco jako vstupní vizum, je vydáván odlišnou autoritou a nemá tak dlouhou dobu platnosti jako certifikát veřejného klíče (např. to může být i velice krátké časové období definované v hodinách atd.).Při žádosti o vizum je obvykle předkládán pas pro ověření totožnosti uživatele, vstupní vizum je pak přímo vázáno k tomuto pasu, v pasu je definováno přímo období platnosti víza popř. další podmínky.

Atributové certifikáty jsou prostředkem, s jehož pomocí je přenášena informace o oprávněních a to bezpečnou cestou.

Užitečná je následující analogie modelu PKI (Public Key Infrastructure) a PMI.

Entita PMI	**Entita PKI**
zdroj autority (SOA)	kořenová CA
atributová autorita (AA)	certifikační autorita (CA)
držitel oprávnění	majitel certifikátu
ověřovatel oprávnění	spoléhající se (ověřující) strana

3. Profil atributových certifikátů

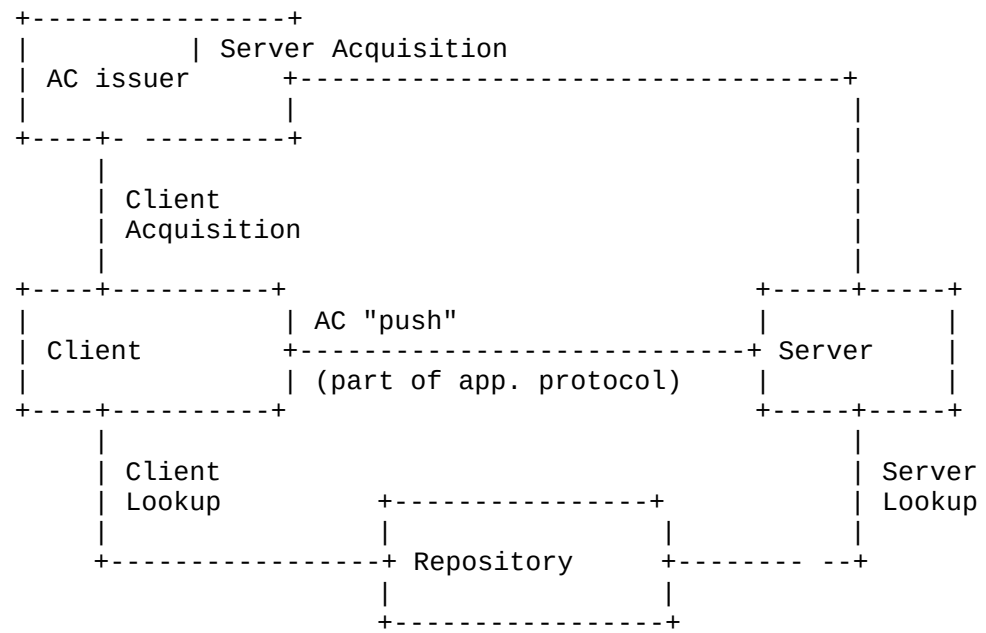
V loňském roce bylo vydáno rfc3281 (lit. [1]), které nahradilo předchozí drafty. Cílem dokumentu je definice profilu atributových certifikátů při jejich využití v rámci internetových protokolů. Týká se to zejména elektronické pošty, protokolu IPSEC a bezpečného přístupu přes webovské stránky. Atributový certifikát může obsahovat atributy, které specifikují příslušenství k určité skupině uživatelů, definují roli, bezpečnostní odbavení či jinou autorizační informaci vztaženou k majiteli atributového certifikátu.

Norma X.509 (lit. [2]) definuje autorizaci jako přenesení oprávnění z jedné entity (která je majitelem tohoto oprávnění) k jiné entitě. Atributový certifikát je pak jedním z mechanizmů pomocí nichž se prakticky autorizace provádí. Lze také například zřetězením uspořádané posloupnosti atributových certifikátů ověřit autentičnost oprávnění strany, která oprávnění vyhlašuje. Dané rfc však zatím nedoporučuje používání takovýchto řetězců – vzhledem k složitosti administrace a zpracování takovýchto postupů. není však vyloučeno, že v budoucnosti bude tato možnost povolena.

V některých situacích je pro klienta výhodné "přesunout" atributový certifikát na server. Následně již pak není vyžadována komunikace mezi klientem a serverem, server nemusí pak provádět potřebná vyhledávání (zlepší to výkon serveru) a ověřovateli AC je přenášeno pouze to co potřebuje vědět. Tento model je zejména vhodný při relacích mezi doménami, kde potom uživatelova práva se stávají právy jeho domovské domény.

Naopak v jiných situacích je vhodnější, aby se klient autentizoval vůči serveru a ze serveru si stáhl klientův AC (od vydavatele AC či ze skladu). Tento model může být implementován takovým způsobem, že neovlivní klienta a protokol mezi klientem a serverem. Model je vhodný při relacích mezi doménami, kde práva klienta lze přenést spíše v rámci domény serveru než v rámci klientovy domény.

V těchto situacích je možná celá řada různých výměn mezi třemi entitami – klient, server a vydavatel AC. Také přitom může existovat podpora adresářů či jiných skladů, odkud jsou získávány atributové certifikáty. Obrázek znázorňuje tyto možnosti.



Obr. 1. Pohyby atributového certifikátu

V rfc.3281 definovaný profil atributového certifikátu splňuje následující požadavky:

Požadavky vzhledem k času a platnosti:

1. Jsou podporovány atributové certifikáty jak krátkodobě platné, tak i platné dlouhodobě. Typicky je platnost krátkodobých certifikátů definována v hodinách - zatímco platnost certifikátu veřejného klíče je definována v měsících. Takováto krátká doba platnosti atributových certifikátů umožňuje práci s nimi bez potřeby existence cesty pro jejich odvolání.

Typy atributů:

2. Vydavatelé atributových certifikátů by měli umět definovat vlastní typy atributů v rámci uzavřených domén.

3. Měly by být definovány některé standardní typy atributů obsažené v atributových certifikátech. Jsou to např. následující:

"access identity," "group," "role," "clearance," "audit identity," and "charging identity."

4. Standardní typy atributů by měly být definovány takovým způsobem, aby umožňovaly ověřovateli AC rozlišit použití téhož atributu v různých doménách. Například je vhodné rozlišovat administrátory ve smyslu používaném Baltimorem a ve smyslu definovaném SPYRUSem.

Využívání atributových certifikátů:

5. Mělo by být umožněno zacílení atributových certifikátů vůči jednomu serveru či vůči malému počtu serverů. To mj. značí, že důvěryhodný server, který není cílem, zamítne atributový certifikát ve svém procesu rozhodování o autorizaci.

Přesun AC versus stáhnutí AC (Push vs. Pull):

6. Atributový certifikát by měl být definován tak, že může být buď přenesen od klienta na sever nebo naopak může být stáhnut ze skladu či od jiné síťové služby a to včetně od online vydavatele atributových certifikátů.

V následující části vyjdeme při popisu vlastnosti profilu AC z jeho ASN definice.

4. Literatura

[1] rfc3281: An Internet Attribute Certificate Profile for Authorization
[2] ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information technology –open systems interconnection – the Directory: Public-Key and Attribute Certificate Frameworks, Version 4, 2000
[3] J. Pinkava: Atributové certifikáty a PMI, Datakon 2002 (v nejbližší době bude tento článek dostupný na webovské stránce autora zde na Crypto-Worldu)
[4] Attribute Certificate Policy extension, draft-ietf-pkix-acpolicies-extn-03.txt, April 2003
[5] LDAP Schema for X.509 Attribute Certificates, draft-ietf-pkix-ldap-ac-schema-00.txt

D. Konference Eurocrypt 2003
Jaroslav Pinkava, PVT a.s.

Ve dnech 4. až 8. května se ve Varšavě konala každoroční konference Eurocrypt (připomeňme pražský Eurocrypt v roce 1999). Webovské stránky konference lze nalézt na adrese http://www.iacr.org/conferences/eurocrypt2003/ . Samotný program konference je zase na adrese http://www.iacr.org/conferences/eurocrypt2003/program2.html .

Nakladatelství Springer vydalo ke konferenci sborník obsahující celkem 37 přijatých článků (z celkového počtu 156 přihlášených). Navíc v úterní večer proběhla rump-session, kde v krátkých vystoupeních prezentovalo své výsledky několik dalších desítek autorů (některá z vystoupení se objevila potom v archivu Cryptology e-print (http://eprint.iacr.org/).

V krátkém článku nelze samozřejmě charakterizovat celý obsah konference, proto jen k některým momentům (samozřejmě kritériem výběru jsou vystoupení blízká zájmům autora). Nejprve k bezpečnosti kryptoschemat asymetrické kryptografie. V Crypto-Worldu bylo již komentováno zařízení TWIRLE (Shamir, A.; Tomer, E.: Factoring Large Numbers with the TWIRL Device, preprint Cryptome, January 2003). Vlastnosti tohoto zařízení byly na Eurocryptu krátce komentovány v rump-session (Lenstra aj.). Bylo konstatováno (1), že je to dnes nejrychlejší existující metoda faktorizace velkých čísel, dále (2), je reálná faktorizace 1024 bitového čísla pomocí tohoto zařízení a konečně (3) finanční náklady na takovouto kryptoanalýzu budou asi vyšší než byly uváděny v článku Shamira a Tomera.

Mladičký, ale již dostatečně známý německý matematik Florian Hess pracující v oblasti eliptické kryptografie se ve svém vystoupení (The GHS Attack Revisited) zabýval perspektivami momentálně nejsilnějšího kryptoanalytického postupu ve vztahu k eliptickým kryptosystémům (metoda Weilova spádu). Uvedl některá nová zobecnění již známých postupů (díky těmto postupům se množství zranitelných eliptických křivek zvětšilo kvadraticky). Zároveň však konstatoval, že tyto postupy lze úspěšně aplikovat jen na některé speciální typy eliptických křivek – např. křivky v binárních tělesech 2^n, kde n je složené číslo. Takovéto křivky byly navrhovány pro použití v protokolech IPSEC. O slabosti těchto křivek se však již ví delší dobu. Zároveň bylo konstatováno, že metodu v současné podobě nelze využít pro křivky v binárních tělesech, kde n je prvočíslo a podobně ji nelze použít ve vztahu k eliptickým křivkám v prvočíselných tělesech.

Asymetrické kryptografii byla věnována celá řada dalších vystoupení, objevily se návrhy některých nových algoritmů, diskutována byla bezpečnost již existujících postupů (NTRU, RDSA, uzlíčkové algoritmy atd.).

Otázkám práce s certifikáty bylo věnováno vystoupení amerického odborníka C.Gentryho – Certificate-Based Encryption and the Certificate Revocation Problem. Autor se zde pokouší trochu netradiční cestou vypořádat se s problémem odvolávání (revocation) digitálních certifikátů. Zavádí pojem certifikátového šifrování. Certifikát zde slouží zároveň jako dešifrovací klíč.

Nesporně velice zajímavým bylo zvané vystoupení (invited talk) francouzského kryptologa Jacquese Sterna (mj. byl šéfem programového výboru pražského Eurocryptu). Týkalo se problematiky prokazatelné bezpečnosti (Why Provable Security Matters?) a velice

hezky diskutuje některé koncepty současných pohledů na bezpečnost kryptografických postupů.

K problematice se ještě autor chce v Crypto-Worldu vrátit, každopádně doporučuji všem zájemcům o moderní pohledy v kryptografii (článek mj. obsahuje i obšírnou bibliografii k problematice).

ENIGMA vystavená na konferenci Eurocrypt 2003
foto: P.Vondruška

Určitým odlehčením bylo vystoupení z oblasti historie kryptologie. Samozřejmě vzhledem k tomu, že se Eurocrypt konal ve Varšavě, nebylo možné se nezmínit o proslulém německém šifrátoru ENIGMA a o úloze polských kryptologů při nalézání kryptoanalytických postupů, které vedly spojence k luštění německých zpráv a v historii druhé světové války sehrály důležitou roli. Pánové Kris Gaj a Arkadiusz Orlowski ve svém vystoupení (Facts and Myths of Enigma: Breaking Stereotypes) velice hezky popsali tato historická fakta i ve světle některých možná dosud méně známých skutečností včetně např. životních osudů polských kryptologů (Marian Rejewski, Jerzy Róycki a Henryk Zygalski), kteří v třicátých letech položily základy kryptoanalýzy Enigmy.

Ve vystoupeních na Eurocryptu se odrazilo celé široké spektrum teoretických otázek, které provází vývoj moderní kyptografie (např. metody symetrické kryptografie, protokoly s nulovou znalostí, protokoly pro výměnu klíčů, otázky budování teoreticko-filosofických základů kryptografie – teorie výpočetní složitosti, vztah k teorii informace atd.).

E. Standard pro kategorizaci bezpečnosti vládních informací a informačních systémů - FIPS PUB 199
Pavel Vondruška, ČESKÝ TELECOM, a.s.

Opravdu žhavou novinkou řady **FIPS PUB** (The Federal Information Processing Standards Publication Series), kterou vydává americký národní institut standardů a technologie NIST (The National Institute of Standards and Technology), je nenápadný, pouze dvanáctistránkový inicializační draft označený FIPS PUB 199. Tento draft nese datum vyhotovení květen 2003 a byl zveřejněn společně s žádostí o veřejnou diskusi 16.5.2003 (Federal Register: May 16, 2003, Volume 68, Number 95) .

Název tohoto dokumentu je „Standard pro kategorizaci bezpečnosti vládních informací a informačních systémů“ (**Standards for Security Categorization of Federal Information and Information**). Připomínky a komentáře k tomuto draftu musí být zaslány do 14.8.2003 na e-mail adresu fips.comments@nist.gov . Potom bude následovat proces zpracování a vyhodnocení doručených připomínek, který povede k vyhlášení upraveného standardu. Neodpustím si srovnání s lhůtami k veřejným připomínkám návrhů standardů, které na svých www stránkách zveřejňuje naše Ministerstvo informatiky (http://www.micr.cz), kde např. návrh ke standardům informační bezpečnosti KI ISVS byl vyvěšen 7.5.2003 a připomínky musí být zaslány do konce května).

Dokument „Standard pro kategorizaci bezpečnosti vládních informací a informačních systémů“ je určen pro americké vládní úřady, které jej mají použít ke kategorizaci zpracovávaných informací a informačních systémů. Připomeňme, že se týká pouze oblasti senzitivních informací, které však nejsou utajované. V tomto smyslu nemá podobná kategorie u nás obecné pojmenování. V ČR existují pouze předpisy, které nařizují jak klasifikovat utajované skutečnosti a příslušné informační systémy, které tato data zpracovávají (zákon č.148/98 O ochraně utajovaných skutečností). Ostatní data zpracovávaná v oblasti veřejné moci nebo v soukromé sféře nejsou nijak oficiálně označena a nijak klasifikována (v ČR se místo pojmu kategorizace dat používá termín klasifikace dat). V případě soukromé sféry zpravidla existuje třídění na základě interní celkové bezpečnostní politiky a není tedy jednotné a není žádným předpisem nebo doporučením upraveno.

Známé systémy, které se dosud používají pro klasifikaci (nebo slovy předloženého standardu kategorizaci), jsou „lineární“. Tím míním, že používají hierarchickou strukturu typu:

- Vyhrazeno, důvěrné, tajné, přísně tajné (zákon č.148/98 Sb.)
- Veřejná data, senzitivní data, chráněná data (takovéto třídění lze nastavit uvnitř organizace např. pomocí pojmenování aktiv v Celkové bezpečnostní politice)
- Data kategorie 0, 1, 2
- Veřejná data , data jen pro interní potřebu, obchodní tajemství

Apod.

Předložený draft k veřejné diskusi, však zavádí novou, zcela revoluční myšlenku kategorizace dat (alespoň já jsem se s ní zatím nikde nesetkal ☺), která vychází ze dvou odlišných charakteristik.

První charakteristika si všímá, co je u daného dokumentu / informačního systému důležité z hlediska zpracovávaných informací. Předkladatelé (U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology) vybrali tyto vlastnosti : Důvěrnost, Integritu a Dostupnost.

Pro účely tohoto dokumentu používají tyto pojmy následovně :
Důvěrnost : Opatření zajišťující pouze oprávněný přístup k informacím a chránící proti jejich neoprávněnému zveřejnění, včetně prostředků pro ochranu osobních údajů a ochranu vlastnických práv.
Integrita : Ochrana před nevhodnou modifikací či zničením informace, zahrnuje také otázky autentičnosti a nepopiratelnosti původu informace.
Dostupnost : Opatření zajišťující včasný a spolehlivý přístup k použití informace.

Za druhou charakteristiku vybrali navrhovatelé míru rizika (Level of Risk). Tuto míru rizika zvolili třístupňovou : nízkou (low), průměrnou (moderate), vysokou (high). Pro každý stupeň přesně definovali, co se tím rozumí. Je zde tedy celkem devět definic 1-9, které můžeme formálně sestavit do následující tabulky :

	LEVEL OF RISK Stupeň rizika		
	Low Nízký	**Moderate Střední**	**High Vysoký**
Confidentiality Důvěrnost	1	2	3
Integrity Integrita	4	5	6
Availability Dostupnost	7	8	9

Tyto definice slovně charakterizují a popisují, co by ztráta příslušné vlastnosti znamenala : např. ohrožení (negativní výsledek) operace , nepříznivý až katastrofický scénář pro operaci, ohrožení ztráty lidského života, atd. ….

Tuto část, společně s myšlenkou dvouparametrového třídění, považuji za nejdůležitější z celého dokumentu a bude podstatná vzhledem ke správnému roztřídění dokumentů /

informačních systémů a předpokládám, že právě k těmto definicím a správnému zatřídění vyjmenovaných dopadů bude nejvíce zaslaných připomínek.

Po zařazení a ohodnocení podle předchozí tabulky bude každý vládní informační sytém nebo chráněná informace zařazena do **kategorie,** která bude popsána příslušným dvou parametrovým systémem.

KATEGORIE = [(**důvěrnost**, stupeň rizika), (**integrita**, stupeň rizika), (**dostupnost**, stupeň rizika)].

CATEGORIZATION = [(**confidentiality**, RISK-LEVEL), (**integrity**, RISK-LEVEL), (**availability**, RISK-LEVEL)].

Výhodou takto navrženého třídění je (i když to nemusí být na první pohled zřejmé) ochrana investic na zabezpečení dat a informačních systémů, ve kterých se tato data zpracovávají. Dá se očekávat, že budou vyvíjeny a vyráběny účelové ochranné prostředky, které zabezpečí ochranu podle takto stanovených požadavků. Dříve používané prostředky (např. hodnocené podle FIPS 140-2 Level 1 až Level 4) musely pro úspěšné vyhodnocení a zařazení do určitého stupně bezpečnosti mít implementovány všechny funkce, které byly na tento stupeň hodnocení požadovány a které ne vždy koncový uživatel potřeboval nebo využíval.

Dá se očekávat, že toto jemnější třídění umožní implementovat do zařízení funkce, které koncový uživatel potřebuje k pokrytí hrozeb, který jeho konkrétní informační systém zařazený do výše definované **kategorie** (např. kategorie (1,1,3)) skutečně vyžaduje a správce takto zařazeného informačního systému nebude muset platit za funkčnost zařízení, které jeho systém nevyužije. Další výhodou by mohlo být i zkrácení doby hodnocení (evaluace) takovéhoto prostředku, neboť zařízení bude obsahovat jen omezený počet funkcí a tedy zkrácení cyklu vývoj – hodnocení – výroba – nasazení prostředku. V současnosti se v některých případech vyžaduje, v souladu s příslušnými předpisy, nasazení pouze hodnocených prostředků. Vzhledem k tomu, že tato hodnocení trvají i několik let, stává se, že vyhodnocené prostředky jsou v okamžiku nasazení již zastaralé.

Z výše uvedených důvodů doporučuji věnovat tomuto nenápadnému draftu patřičnou pozornost, neboť by v budoucnu mohl zcela zásadním způsobem ovlivnit sféru klasifikace (kategorizace) informací a informačních systémů, a to by mělo přímý dopad (v horizontu několika let) na způsob hodnocení bezpečnosti informačních systémů a kryptografických prostředků.

Draft standardu je dostupný ve formátu PDF na adrese:
http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf

F. Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti

Pavel Vondruška, ČESKÝ TELECOM, a.s.

Ministerstvo informatiky (http://www.micr.cz) je za ČR gestorem spolupráce s Výborem pro informační, počítačovou a komunikační politiku OECD, v jehož rámci působí Pracovní skupina pro informační bezpečnost a ochranu soukromí. Významným výstupem této pracovní skupiny je ***Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti*** (OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security), která stanovuje devět zásad v oblasti bezpečnosti informačních systémů a sítí. Tato směrnice byla přijata jako Doporučení Rady OECD na jejím 1037. zasedání dne 25. července 2002.

Ve smyslu závěrečných doporučení k této Směrnici, kde se mimo jiné doporučuje, aby byla tato Směrnice šířena prostřednictvím veřejného a soukromého sektoru včetně státních správ, podniků, ostatních organizací a individuálních uživatelů za účelem prosazování kultury bezpečnosti a doporučení všem dotčeným stranám, aby byly přijímány nezbytné kroky k provedení Směrnice způsobem přiměřeným jejich individuální úloze, si i na stránkách našeho e-zinu stručně představíme základní cíle a zásady uvedené v této Směrnice.

I. Cíle Směrnice jsou

- prosazovat kulturu bezpečnosti mezi všemi účastníky jako prostředek ochrany informačních systémů a sítí,
- zvyšovat informovanost o riziku pro informační systémy a sítě, politice, praxi, opatřeních a postupech, které jsou k řešení těchto rizik k dispozici, a potřebě jejich přijetí a realizace,
- pěstovat větší důvěru účastníků v informační systémy a sítě a ve způsob, jakým jsou poskytovány a využívány,
- vytvořit obecný referenční rámec, který účastníkům pomůže porozumět bezpečnostním otázkám a ctít etické hodnoty při vytváření a realizaci promyšlené politiky, praxe, opatření a postupů k bezpečnosti informačních systémů a sítí,
- prosazovat spolupráci a sdílení informací, jak bude vhodné, mezi všemi účastníky vytváření a realizace bezpečnostních politik, praxe, opatření a postupů,
- prosazovat zohlednění bezpečnosti jako důležitý cíl všech účastníků zapojených do vytváření a realizace standardů.

II. Zásady Směrnice

Následujících devět zásad se navzájem doplňuje a neměly by být vykládány samostatně, ale vždy jako jeden komplexní celek.

1) Informovanost
Účastníci by měli být informováni o potřebě bezpečnosti informačních systémů a sítí a o tom, co mohou udělat, aby bezpečnost prohloubili.

2) Odpovědnost
Všichni účastníci jsou odpovědní za bezpečnost informačních systémů a sítí.

3) Reakce

Účastníci by měli jednat včas a vzájemně spolupracovat při předcházení bezpečnostním incidentům, jejich odhalování a reagování na ně.

4) Etika

Účastníci by měli respektovat legitimní zájmy ostatních.

5) Demokracie

Bezpečnost informačních systémů a sítí by měla být slučitelná se základními hodnotami demokratické společnosti.

6) Odhad rizika

Účastníci by měli provádět odhady rizik.

7) Navržení a realizace bezpečnosti

Účastníci by měli bezpečnost zahrnout mezi základní prvky informačních systémů a sítí.

8) Řízení bezpečnosti

Účastníci by měli k řízení bezpečnosti zaujmout komplexní přístup.

9) Přehodnocování

Účastníci by měli revidovat a přehodnocovat bezpečnost informačních systémů a sítí a provádět příslušné úpravy bezpečnostní politiky, praxe, opatření a postupů.

III. Doporučení

Tato Směrnice není vynutitelná, ale má pouze doporučující charakter. V závěrečných doporučeních se mimo jiné doporučuje členským zemím, aby:

- zavedly novou nebo upravily stávající politiku, praxi, opatření a postupy, aby tyto odrážely a zohledňovaly Směrnici pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti, přijetím a prosazováním kultury bezpečnosti vyložené v této Směrnici;
- navzájem konzultovaly, koordinovaly a spolupracovaly na národní a mezinárodní úrovni při provádění této Směrnice;
- daly Směrnici včas a vhodným způsobem k dispozici nečlenským zemím;
- každých pět let Směrnici revidovaly za účelem podpory mezinárodní spolupráce v otázkách týkajících se bezpečnosti informačních systémů a sítí;
- šířily Směrnici prostřednictvím veřejného a soukromého sektoru včetně státních správ, podniků, ostatních organizací a individuálních uživatelů za účelem prosazování kultury bezpečnosti a doporučení všem dotčeným stranám, aby byly odpovědné a přijímaly nezbytné kroky k provedení Směrnice způsobem přiměřeným jejich individuální úloze (již v úvodu citované doporučení o šíření Směrnice);

Oficiální český překlad této osmnáctistránkové Směrnice je od tohoto května k dispozici ke stažení zde: http://www.micr.cz/upload_file/20030422114605_smernice_oecd.pdf

G. Letem šifrovým světem

OpenSSL hodnoceno podle FIPS 140-2 na Level 1

The Open Source Software Institute (Oxford, http://www.oss-institute.org) oznámil 3.5.2003, že OpenSSL vstupuje do procesu hodnocení podle FIPS 140-2 na Level 1. Splnění těchto požadavků je nezbytné k tomu, aby šifrovací subsystém mohl být používán pro potřeby US vlády pro zpracování citlivých, ale neutajovaných informací. Ukončení hodnocení a udělení certifikátu se očekává ke konci roku 2003.
http://newsvac.newsforge.com/article.pl?sid=03/05/01/1851208

Chip CD 05/03 (http://www.chip.cz/3/chipcd.php)

Na CD, které je přílohou k Chipu 5/2003, naleznete i rozsáhlou ukázku našich e-zinů Crypto-World. Ve verzi pro toto CD je dostupný kompletní ročník 2002 a čísla ze začátku roku 2003. Na CD jsou umístěny i soutěžní úlohy z roku 2000 a 2001. Bohužel od předání podkladů do jejich vydání na CD došlo ke změně domácí stránky Crypto-Worldu, a tak všechny zde uvedené odkazy vedou na dnes již opuštěnou starou adresu:
http://www.mujweb.cz/veda/gcucmp/ místo na nově zřízenou doménu : http://crypto-world.info

Standardy informační bezpečnosti KI ISVS

Ministerstvo informatiky zveřejnilo 7.5.2003 návrhy osnov k připravovaným standardům ISVS (informační systém veřejné správy), které se týkají řešení informační bezpečnosti v KI ISVS. Dokument je uvolněn k veřejnému připomínkování. Vaše názory a náměty lze zasílat do konce května 2003.
Obsah připravovaných standardů:
Mapa základních řídících dokumentů SŘIB
Standard ISVS pro organizační bezpečnost KI ISVS
Standard ISVS pro klasifikaci a řízení aktiv KI ISVS
Standard ISVS pro personální bezpečnost KI ISVS
Standard ISVS pro fyzickou bezpečnost a bezpečnost prostředí KI ISVS
Standard ISVS pro řízení provozu KI ISVS
Standard ISVS pro řízení přístupu KI ISVS
Standard ISVS pro vývoj a údržbu KI ISVS
Standard ISVS pro řízení kontinuity činností KI ISVS
Standard ISVS pro zajištění shody KI ISVS
Standard ISVS pro připojení ISVS k Internetu
Standard ISVS pro připojení resortních VPN ke GovNet
Standard ISVS pro využívání služeb GovNet KI ISVS
Standard ISVS pro využívání kryptografických prostředků
Dokument naleznete zde : http://www.micr.cz/?idm=15 .

Doporučujeme pro výukové potřeby:

Free ELPI - Elektronický podpis 1.4a (http://www.slunecnice.cz/product/FreeELPI/)
Program na podepisování, ověřování podpisů, šifrování a nenávratné vymazání. Skartování souborů, generování RSA klíčů, certifikátů X509 a žádostí o certifikát Typ: Program i s vaším soukromým klíčem si nahrajete na USB "disk" nebo disketu. Zjednodušíte si tak podepisování a soukromý klíč pro podepisování na cizím počítači., protože ELPI není nutné instalovat.
Detaily o produktu Autor: Ing. Peter Rybár
Web produktu: http://elpi.host.sk

Jak jsme již informovali v našem e-zinu 3/2003 - vychází zajímavý text:
Simon Singh : Kniha kódů a šifer. Utajování od starého Egypta po kvantovou kryptografii. Překlad *Petr Koubský a Dita Eckhardtová*, odborná lektorace *Vlastimil Klíma*, 382 stran, 180 ilustrací, tabulek a příloh, cena 350 Kč, ISBN 80-86569-18-7, nakladatelství DoKořán, řada Aliter. Singhova kniha mapuje v osmi kapitolách historii šifrování i současný stav kryptologie. Díky přístupnému stylu lze knihu doporučit každému zájemci o tuto nesporně zajímavou oblast lidské činnosti. (http://www.dokoran.cz/ep2003/sifry.html).
Pokud se chcete s knihou blíže seznámit a nechcete si ji kvůli tomu hned kupovat, máte možnost si přečíst nejdříve jednu z osmi kapitol této knihy. Nakladatel byl tak laskav, že povolil Science Worldu (http://www.scienceworld.cz/) publikování čtvrté kapitoly „Boj s Enigmou“.
Ukázka č.1 : Velká knih kódů a šifer: Zrod Enigmy
Ukázka č.2 : Enigma podruhé: Spojenci získávají repliku stroje
Ukázka č.3 : Enigma potřetí: Úspěch polských kryptoanalytiků
Ukázka č.4 : Enigma počtvrté: Přichází Turing
Ukázka č.5 : Enigma popáté a naposled: Turingův úspěch
Ve formátu MS Word lze stáhnout všechny tyto ukázky najednou z adresy:
http://www.scienceworld.cz/sw.nsf/ID/3CD0758FBF3272B3C1256D0A00294D05

Kalendář vybraných akcí

EurOpen.CZ
XXII.konference
25.5-28.5.2003
Nové Hrady
http://www.europen.cz

Nové služby certifikační autority, hierarchická časová razítka a elektronické občanské průkazy
Workshop
28.5.2003, Praha (PVT)
ida.luxova@pvt.cz

Information Security Summit
4.ročník mezinárodní konference
28.-29.května 2003
Míčovna Pražského hradu
http://www.dsm.tate.cz/is2/2003
http://www.dsm.tate.cz/index.php?typ=DAA&showid=218

KONFERENCE SYSTÉMOVÁ INTEGRACE 2003
11.ročník
16. a 17. června 2003 , Praha na Žofíně.
http://si.vse.cz/

Standardy Informační bezpečnosti
(předběžný název)
Seminář ČSNI
24.6.2003
http://www.csni.cz
doucek@vse.cz (informace)

TATRACRYPT 2003
Central European Conference on Cryptology
June 26-28, 2003
Bratislava, Slovak Republic
List of plenary speakers:
- *Professor Spyros S. Magliveras*, Florida Atlantic University, USA:
Cryptographic Primitives Based on Groups of Hidden Order
- ***RNDr. Vlastimil Klima,* ICZ a.s, Praha 10, Czech Republic:**
Side Channel Attacks - Highly Promising Directions in Modern Cryptanalysis
- *Professor Pino Caballero Gil*, Universidad de la Laguna, Tenerife, Spain:
Practical Design of Two-Party Cryptographic Protocols
- *Professor Attila Pethö*, University of Debrecen, Hungary:
Application of unusual number theoretical functions in cryptography
Conference webpage: http://www.elf.stuba.sk/Katedry/KM/TATRACRYPT/index.htm

DATAKON 2003
termín konaní konference: 18. - 21. 10. 2003
23.5. - termín podaní návrhu příspěvku
místo konaní konference: Hotel SANTON, Brno
podrobné informace viz: http://www.datakon.cz

The Eighth Australian conference on Information Security and Privacy (ACISP 2003)
9-11 July 2003
University of Wollongong
Sydney, Australia
http://www.itacs.uow.edu.au/research/NSLabs/acisp03

The 7th Workshop on Eliptic Curve Cryptography (ECC 2003)
University of Waterloo
Waterloo, Ontario, Canada
August 11,12 and 13, 2003
http://www.cacr.math.uwaterloo.ca/conferences/2003/ecc2003/announcement.html

Workshop on Cryptographic Hardware and Embedded System 2003 (CHES 2003)
Cologne, Germany
September 7-10, 2003
http://www.chesworkshop.org
Přehled přijatých příspěvků : http://islab.oregonstate.edu/ches/accepted.html
Vlastimil Klima, Ondrej Pokorny, Tomas Rosa : **Attacking RSA-based Sessions in SSL/TLS**

CRYPTOGRAPHY Fundamentals and Aplications
(Lecturer: Ueli Maurer, ETH Zurich)
Engelberg, Switzerland
October 6-9, 2003
e-mail: seminars@dplanet.ch
International Conference on Applied Cryptography and Network Security (**ACNS ´03**)
Kumming, China
October 16-19, 2003
http://www.onets.com.cn/dhe.htm

The 6th International Conference on Information Security and Cryptology (ICISC 03)
Seoul, Korea
November 27-28, 2003
http://cist.korea.ac.kr/icisc03

ASIACRYPT 2003
Taiwan
Noveber 30 – Decenber 4
http://conf.ncku.edu.tw/ac03

Advanced Course on Contemporary Cryptology
February 2 to 13, 2004
Centre de Recerca Matematica
Campus of the Universitat Autónoma de Barcelona
http://www.crm.es

Financial Cryptography ´04
Key West,
Florida, USA
http://www.ifca.ai/fc04/

2nd IEEE International Workshop on Information Assurance (IWIA04)
University of North Carolina at Charlotte
Charlotte, North Carolina, USA
http://iwia.org/2004

O čem jsme psali v květnu 2000 - 2002

Crypto-World 5/2000

Příloha : J.Hrubý , soubor QNG.PS

Crypto-World 5/2001

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 5/2002

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

H. 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 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), 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@post.cz (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@post.cz (předmět: ruším odběr Crypto-Worldu !). 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@post.cz
pavel.vondruska@ct.cz