Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 2/2003 **17. únor 2003**

2/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp

(402 e-mail výtisků)

Obsah : **Str.**

Příloha : Crypto_p2.pdf
Přehled dokumentů **ETSI**, které se zabývají elektronickým podpisem
(ETSI - European Telecommunication Standards Institute)

(články neprocházejí jazykovou korekturou)

A. České technické normy a svět , II.část

Pavel Vondruška, ČESKÝ TELECOM, a.s.

2. Národní normalizační proces

V současné době se národní technická normalizace orientuje spíše na přejímání evropských a mezinárodních norem, než na vlastní tvorbu. Tvorba norem čistě domácího původu představuje pouze 10% ze všech normalizačních prací [1].

2.1 Tvorba norem

Návrh na zpracování normy může u Českého normalizačního institutu (ČSNI) podat kdokoliv.

Navrhovatel může současně navrhnout zpracovatele, kterým může být sám navrhovatel a popřípadě i způsob financování úkolu. ČSNI ve spolupráci s příslušnou technickou normalizační komisí, pokud je zřízena, návrh posoudí a výsledek v případě potřeby projedná s navrhovatelem. Pokud návrh předloží orgán státní správy v oblasti své působnosti, ČSNI s ním návrh projedná vždy, vzniknou-li nejasnosti nebo odlišná stanoviska. Je-li výsledek posouzení kladný, ČSNI dohodne zpracovatele úkolu.

Zpracovatelé jsou při tvorbě norem povinni postupovat podle zákona 22/1997 Sb. a respektovat platné metodické pokyny pro normalizaci.

Zpracovatel vypracuje návrh normy, který zašle všem účastníkům připomínkového řízení, včetně ČSNI. Po vyřešení všech připomínek a odsouhlasení návrhu účastníky připomínkového řízení je konečný návrh postoupen ke schválení ČSNI. ČSNI posoudí, zda návrh byl projednán stanoveným způsobem, zda odpovídá požadavkům zákona č. 22/1997 Sb. a podmínkám dohodnutým ve smlouvě se zpracovatelem. Poté návrh schválí, popřípadě upraví (po formální stránce) nebo vrátí k dopracování nebo zamítne [2].

2.2 Obecné zásady pro stavbu, členění a úpravu českých technických norem (ČSN)

ČSN má

- být úplná v rozsahu stanoveném předmětem normy
- být jednoznačná, přesná a srozumitelná
- brát v úvahu dosažený stav techniky
- umožnit budoucí technický vývoj

Sloh má být co nejjednodušší, co nejvýstižnější a pokud možno co nejstručnější. Termíny se používají normalizované, pokud existují, a ve spisovném tvaru.

ČSN se vydávají v jazyce českém, jejich součástí však může být i identický cizojazyčný text přejímané evropské nebo mezinárodní, popř. zahraniční normy.

Normy ČSN se člení na části, oddíly, kapitoly, články, odstavce a přílohy.

2.3 Přejímání evropských a mezinárodních norem

Všeobecně

Pod pojmem *evropská norma* se rozumí EN, HD, ENV, ETS, I-ETS, popř. další normy a normativní dokumenty vydané evropskými normalizačními organizacemi.

Pod pojmem *mezinárodní norma* se rozumí ISO a IEC, popř. další normy a normativní dokumenty vydané evropskými normalizačními organizacemi.

EN je norma CEN, CENELEC nebo ETSI, která je určena v členských státech k povinnému zavedení jako národní norma a vyžaduje současné zrušení národních norem, které jsou s ní v rozporu.

HD (harmonizační dokument) je norma CEN nebo CENELEC, která se zpracovává v případech, kdy není možné nebo účelné zpracovat EN a je určena v členských státech k povinnému zavedení na národní úrovni alespoň formou zveřejnění čísla HD a názvu při současném zrušení národních norem nebo jejich částí, které jsou s ní v rozporu.

ENV je předběžná norma CEN nebo CENELEC určená k ověření po dobu tří let (s možností jednorázového prodloužení o další dva roky). Národní normy, které jsou s ní v rozporu, mohou být ponechány v platnosti. Takto převzatá norma se označuje ČSN P ENV.

ETS je dřívější označení normy Evropského ústavu pro telekomunikační normy (ETSI), ke které se vážou stejné povinnosti, jako v případě EN. I-ETS je dřívější označení předběžné normy ETSI s obdobnou funkcí jako má ENV.

2.4 Zásady přejímání norem

Převzetím evropské nebo mezinárodní normy do české normalizační soustavy se rozumí udělení statusu české normy přejímané normě tím, že je bez jakýchkoliv změn obsahu, stavby, členění a úpravy schválena jako ČSN. K počátku platnosti této ČSN musí být zrušeny dříve vydané ČSN nebo jejich části, pokud jsou s ní v rozporu.
Zapracování jakékoliv normy nebo normativního dokumentu do ČSN s odchylkami se nepovažuje za převzetí těchto norem (dokumentů). Označení ČSN se zapracovanou normou nebo normativním dokumentem s odchylkami neobsahuje značku ani číslo zapracované normy (dokumentu). Tyto údaje však mohou být spolu s dalšími potřebnými informacemi uvedeny v předmluvě ČSN.

Označení takto převzatých norem znamená, že:
ČSN EN je česká technická norma identická s EN v technickém obsahu a stavbě.
ČSN P ENV je česká předběžná norma identická s ENV v technickém obsahu a stavbě.
ČSN ETS je česká technická norma identická s ETS v technickém obsahu a stavbě.
ČSN P I-ETS je česká předběžná norma identická s I-ETS v technickém obsahu a stavbě.
ČSN ISO je česká technická norma identická s normou ISO v technickém obsahu a stavbě.
ČSN IEC je česká technická norma identická s normou IEC v technickém obsahu a stavbě.
ČSN EN ISO je česká technická norma identická s normou EN ISO v technickém obsahu a stavbě.

Ve zdůvodněných případech lze do české normalizační soustavy přejímat i jiné normy a normativní dokumenty. Pro jejich přejímání platí obdobné zásady jako pro přejímání evropských a mezinárodních norem.

Evropské a mezinárodní normy se do ČSN přejímají následujícími způsoby:

1. překladem,
2. převzetím originálu
3. schválením k přímému používání
4. oznámením o schválení k přímému používání ve Věstníku

Způsob převzetí se volí podle účelu a rozsahu využití ČSN a dohodne se s ČSNI.

Z norem vyhlášených ve Věstníku ÚNMZ v roce 2001 bylo:

1246 norem evropských a mezinárodních vydáno překladem (včetně původních ČSN);

1191 norem evropských a mezinárodních vyhlášeno k přímému používání (vydána pouze titulní strana nebo jen oznámení ve Věstníku ÚNMZ);

19 evropských a mezinárodních norem vydáno převzetím originálu (bez překladu, tzn. jen úvodní část ČSN s přiloženým originálem převzaté normy). Jednou z těchto norem byl v minulém čísle zmiňovaná norma ČSN ISO 17799.

K 31. prosinci 2001 tvořilo soustavu ČSN celkem 25 817 platných norem [3].

Následující tabulka pak zobrazuje počet schválených ČSN (bez jejich změn a oprav) od počátku roku 2002 do 15.7.2002 :

	leden	únor	březen	duben	květen	červen
EN - CEN	109	210	310	372	561	735
EN - CLC	18	58	98	110	167	196
EN - ETS	51	62	66	145	152	164
ISO	3	8	31	34	43	48
IEC	7	10	11	17	17	19
ISO/IEC	8	8	10	18	23	25
ČSN	6	6	14	24	28	41
Celkem	202	362	540	720	991	1228

[1] ČSNI - NÁRODNÍ NORMALIZAČNÍ ORGANIZACE, Český normalizační institut.
http://www.csni.cz/wwwcsni/csni.htm

[2] TVORBA NOREM, Český normalizační institut.
http://www.csni.cz/wwwcsni/tvorba.htm

[3] Statistické údaje o tvorbě norem, Český normalizační institut.
http://domino.csni.cz/NP/NotesPortalCSNI.nsf/key/tvorba_norem_v_cr~statistika?Open

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 9. Protokol SCVP
Jaroslav Pinkava, PVT a.s.

1. Úvod

V současné době probíhá v rámci pracovní skupiny PKIX zajímavá diskuse. Jedná se o to, že dnes existují fakticky čtyři protokoly, které se problematikou ověřování (validation) certifikátů zabývají. Jsou to protokol OCSP (byl popsán v předešlých dílech), dále protokol CSVP (Simple Certifikate Validation Protokol), protokol v rámci DVCS (Data Validation and Certification Server Protocols) a konečně protokol CVP (Certificate Validation Protocol). To je již trochu moc kohoutů na jednom smetišti, a i když každý z nich byl vytvářen za trochu jiným účelem, bylo rozhodnuto, že pro další návazné práce bude z těchto čtyř vybrán pouze jeden.

Kritériem pro toto rozhodování je v zásadě vztah těchto protokolů k požadavkům, které jsou definovány v rámci protokolů DPV a DPD (viz [7], také [3] - náš seriál). Na základě dokumentu [7] byla zpracována tzv. matice shody (compliance matrix) – viz příloha. Tato matice obsahuje celkem 35 požadavků. Pro konečný výběr protokolu má být pak rozhodující právě jeho vztah k naplnění těchto požadavků. Je zajímavé, že po zformulování těchto kriterií přispěchali okamžitě s doplňkem k protokolu OCSP – viz [9]. Ze zatímní diskuse se zdá, že horkými favority jsou zejména protokoly OCSP a SCVP, přičemž poslední má malinko více přívrženců.

Obsahem tohoto dílu bude proto seznámení se z dalším "kandidátem" a to s protokolem SCVP. V příštím pokračování bude řeč o protokolu CVP.

2. Protokol SCVP

Tento protokol umožňuje klientovi přesunout práci s certifikáty na server. Server doručí klientovi informace o certifikátu různého typu, informace zda certifikát je platný, zdokumentuje certifikační cestu atd. SCVP je víceúčelový protokol, jeho cíly jsou zjednodušení klientských aplikací a umožnit organizacím centralizovat řízení důvěry a příslušných politik PKI.

Poznámka: Jeden z autorů protokolu je pracovníkem RSA Laboratories (R.Housley) a další (T.Freeman) je pracovníkem Microsoftu.

Protokol již byl konstruován tak, aby vyhovoval požadavkům, které plynou z [7]. Matice shody (příloha) však tyto nároky dále specifikovala, tj. ani tento protokol z hlediska požadavků této matice není stoprocentní. SCVP mohou používat ty klientské aplikace, které sami zpracovávají certifikáty, ale překládají na server (který zde není důvěryhodnou stranou) samotný sběr potřebných informací. Server také dodá klientovi příslušné revokační informace (CRL a odpovědi OCSP). Pokud ovšem klient může serveru SCVP plně důvěřovat, pak lze na něj delegovat i práci s konstrukcí a ověřením certifikační cesty a také dodržování příslušných politik organizace.

Samotný protokol používá jednoduchý model založený na zaslání požadavku a příslušné odpovědi. TJ. klient SCVP vytvoří požadavek, zašle ho na SCVP server a následně SCVP server vytvoří jednu odpověď a zašle ji klientovi. Obvykle je SCVP konstruováno nad HTTP, někdy lze používat i email.

3. Požadavek na ověření

Požadavek zasílaný klientem musí být jeden item SCVPRequest. Pokud je zabalen v tělu MIME, musí být používána k tomu náležející aplikace. Jsou dva formáty tohoto požadavku – nepodepsaný a podepsaný. Podepsaný požadavek lze použít k autentizaci klienta na serveru. Server může požadovat, aby všechny požadavky byly podepsány (a vyloučit nepodepsané). Nepodepsaný požadavek sestává z PSRequest zabaleném v ContentInfo:

```
ContentInfo {
  contentType        id-ct-scvp-psRequest,
                             -- (1.2.840.113549.1.9.16.1.10)
  content            PSRequest }
```

Podepsaný požadavek sestává z PSRequest zabaleném v SignedData, které jsou opět zabalená v ContentInfo.

```
ContentInfo {
  contentType        id-signedData, -- (1.2.840.113549.1.7.2)
  content            SignedData }

SignedData {
  version            CMSVersion,
  digestAlgorithms   DigestAlgorithmIdentifiers,
  encapContentInfo   EncapsulatedContentInfo,
  certificates       CertificateSet, -- (Optional)
  crls               CertificateRevocationLists, -- (Optional)
  signerInfos        SET OF SignerInfos } -- (only one in SCVP)

SignerInfo {
  version            CMSVersion,
  sid                SignerIdentifier,
  digestAlgorithm    DigestAlgorithmIdentifier,
  signedAttrs        SignedAttributes, -- (Required)
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature          SignatureValue,
  unsignedAttrs      UnsignedAttributes } -- (not used in SCVP)

EncapsulatedContentInfo {
  eContentType       id-ct-scvp-psRequest,
                             -- (1.2.840.113549.1.9.16.1.10)
  eContent           OCTET STRING } -- Contains PSRequest
```

Syntaxe SignedData a ContentInfo je definována v RFC2630 (CMS). Dokument dále definuje syntaxi samotného PSRequest a požadavky na obsah jednotlivých objektů:

```
PSRequest ::= SEQUENCE {
  scvpVersion           INTEGER,
  query                 Query,
  checks                CertChecks,
  wantBack              WantBack,
  requestor         [0] OCTET STRING OPTIONAL,
  requestNonce      [1] OCTET STRING OPTIONAL,
  reqExtensions     [2] Extensions OPTIONAL }
```

4. Odpověď s ověřením

Odpovědí opět musí být pouze jediný item SCVPResponse a existují zde také dva formáty – nepodepsaný a podepsaný. Nepodepsaná odpověď musí být generována pouze v případě chybového stavu.

```
ContentInfo {
  contentType        id-ct-scvp-psResponse,
                             -- (1.2.840.113549.1.9.16.1.11)
  content            PSResponse }
```

Podepsaná odpověď obsahuje PSResponse, který je zabalen v SignedData a to jsou zabalena zase v ContentInfo.

```
ContentInfo {
  contentType        id-signedData, -- (1.2.840.113549.1.7.2)
  content            SignedData }

SignedData {
  version            CMSVersion,
  digestAlgorithms   DigestAlgorithmIdentifiers,
  encapContentInfo   EncapsulatedContentInfo,
  certificates       CertificateSet, -- (MUST include server cert)
  crls               CertificateRevocationLists, -- (Optional)
  signerInfos        SET OF SignerInfos } -- Only 1 in SCVP

SignerInfo {
  version            CMSVersion,
  sid                SignerIdentifier,
  digestAlgorithm    DigestAlgorithmIdentifier,
  signedAttrs        SignedAttributes, -- (Required)
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature          SignatureValue,
  unsignedAttrs      UnsignedAttributes } -- Not used in SCVP

EncapsulatedContentInfo {
  eContentType       id-ct-scvp-psResponse,
                             -- (1.2.840.113549.1.9.16.1.11)
  eContent           OCTET STRING } -- Contains PSResponse
```

Samotný objekt PSResponse má následující syntaxi:

```
PSResponse ::= SEQUENCE {
  scvpVersion           INTEGER,
  producedAt            GeneralizedTime,
  responseStatus        ResponseStatus,
  requestRef            RequestReference,
  requestor         [1] OCTET STRING OPTIONAL,
  responder         [2] OCTET STRING OPTIONAL,
  replyObjects      [3] ReplyObjects OPTIONAL,
  requestNonce      [4] OCTET STRING OPTIONAL,
  serverContextInfo [5] OCTET STRING OPTIONAL,
  respExtensions    [6] Extensions OPTIONAL }
```

5. Další poznámky

Server SCVP potřebuje dále informovat klienta o politice ověřování, kterou podporuje. Za tímto účelem je v rámci SCVP definována jiná dvojice typu žádost-odpověď. Nejprve klient zašle serveru žádost vzhledem k podporované politice ověřování objekt ValPoliciesRequest zabalený v ContentInfo. Server pak vytvoří objekt ValPoliciesResponse (je opět zabalený v ContentInfo). Tento objekt obsahuje posloupnost identifikátorů (OID). Každé OID identifikuje jednu politiku ověřování, která je serverem podporována.

Draft dále obsahuje modul ASN.1 pro zprávy protokolu SCVP a zabývá se příslušnými bezpečnostními nároky pro vlastní implementace protokolu.

6. Literatura

[1] PKIX Working Group:
http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html.

[2] Malpani A.; Housley. R.; Freeman, T.: Simple Certificate Validation Protocol (SCVP),http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-scvp-10.txt

[3] předešlé díly tohoto seriálu

[4] Pinkas, D.: Certificate Validation Protocol
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-cvp-01.txt

[5] Adams, C.; Sylvester, P.; Zolotarev, M.; Zucccherato, R.: Data Validation and Certification Server Protocols, http://www.ietf.cnri.reston.va.us/rfc/rfc3029.txt

[6] Myers, M.; Malpani, A.; Pinkas, D.: Online Certificate Status Protocol, version 2
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-ocspv2-ext-00.txt

[7] Pinkas, D.; Housley R.: Delegated Path Validation and Delegate path Discovery. Protocol requirements, http://www.ietf.cnri.reston.va.us/rfc/rfc3379.txt

[8] RFC 2560-Online Certificate Status Protocol - OCSP:
http://www.ietf.cnri.reston.va.us/rfc/rfc2560.txt

[9] DPV and DPD over OCSP,
http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-ocsp-dpvdpd-00.txt

7. Příloha

***Compliance matrix* (Tim Polk, Steve Kent, October 2002 + Denis Pinkas, January 2003)**

Topic 1: Basic Protocol

1. If the DPV server does not support the client requested validation policy, then the DPV server MUST return an error. (4.1.Basic Protocol)

2. If the DPV request does not specify a validation policy, the server response MUST indicate the validation policy that was used. (4.1. Basic Protocol)
3. The protocol MUST allow the client to include these policy dependent parameters in the DPV request; however, it is expected that most clients will simply reference a validation policy for a given application or accept the DPV server's default validation policy. (4.1. Basic Protocol)
4. The DPV server MUST obtain revocation status information for the validation time in the client request. (4.1. Basic Protocol)
5. If the revocation status information for the requested validation time is unavailable, then the DPV server MUST return a status indicating that the certificate is invalid. Additional information about the reason for invalidity MAY also be provided. (4.1 Basic Protocol)
6. The certificate to be validated MUST either be directly provided in the request or unambiguously referenced, such as the CA distinguished name, certificate serial number, and the hash of the certificate, like ESSCertID as defined in [ESS] or OtherSigningCertificate as defined in [ES-F]. (4.1 Basic Protocol)
7. The DPV client MUST be able to provide to the validation server, associated with each certificate to be validated, useful certificates, as well as useful revocation information. (4.1 Basic Protocol)
8. The DPV server MUST have the certificate to be validated. When the certificate is not provided in the request, the server MUST obtain the certificate and then verify that the certificate is indeed the one being unambiguous referenced by the client. (4.1 Basic Protocol)
9. The DPV server MUST include either the certificate or an unambiguous reference to the certificate (in case of a CA key compromise) in the DPV response. (4.1 Basic Protocol)
10. The DPV response MUST indicate one of the following status alternatives:

1. the certificate is valid according to the validation policy.
2. the certificate is not valid according to the validation policy.
3. the validity of the certificate is unknown according to the validation policy.
4. the validity could not be determined due to an error.

11. When the certificate is not valid according to the validation policy, then the reason MUST also be indicated. Invalidity reasons include:

1. the DPV server cannot determine the validity of the certificate because a certification path cannot be constructed.
2. the DPV server successfully constructed a certification path, but it was not valid according to the validation algorithm in [PKIX-1].
3. the certificate is not valid at this time. If another request could be made later on, the certificate could possibly be determined as valid. This condition may occur before a certificate validity period has begun or while a certificate is suspended.

12. The protocol MUST prevent replay attacks, and the replay prevention mechanism employed by the protocol MUST NOT rely on synchronized clocks. (4.1 Basic Protocol)
13. The DPV request MUST allow the client to request that the server include in its response additional information which will allow relying parties not trusting the DPV server to be confident that the certificate validation has correctly been performed.
[...] When the certificate is valid according to the validation policy, the server MUST, upon request, include that information in the response. However, the server MAY omit that information when the certificate is invalid or when it cannot determine the validity.
14. The DPV server MUST be able, upon request, copy a text field provided by the client into the DPV response.
15. The DPV response MUST be bound to the DPV request so that the client can be sure that all the parameters from the request have been taken into consideration by the DPV server to build the response. This can be accomplished by including a one-way hash of the request in the response.
16. For the client to be confident that the certificate validation was handled by the expected DPV server, the DPV response MUST be authenticated, unless an error is reported (such as a badly formatted request or unknown validation policy).
17. The DPV server MAY require client authentication, therefore, the DPV request MUST be able to be authenticated.
18. When the DPV request is authenticated, the client SHOULD be able to include a client identifier in the request for the DPV server to copy into the response. Mechanisms for matching this identifier with the authenticated identity depends on local DPV server conditions and/or the validation policy. The DPV server MAY choose to blindly copy the identifier, omit the identifier, or return an error response.
19. Protocols designed to satisfy these requirements MAY include optional fields and/or extensions to support relaying, re-direction or multicasting. [...] If the protocol supports such features, the protocol MUST include provisions for DPV clients and DPV servers that do not support such features, allowing them to conform to the basic set of requirements.
20. When a server supports a relay mechanism, a mechanism to detect loops or repetition MUST be provided.

21. When a protocol provides the capability for a DPV server to redirect a request to another DPV server (that is, the protocol chooses to provide a referral mechanism), a mechanism to provide information to be used for the re-direction SHOULD be supported. If such re-direction information is sent back to clients, then the protocol MUST allow conforming clients to ignore it.
22. Optional parameters in the protocol request and/or response MAY be provide support for relaying, re-direction or multicasting. DPV clients that ignore any such optional parameters MUST be able to use the DPV service. DPV servers that ignore any such optional parameters MUST still be able to offer the DPV service, although they might not be able to overcome the limitations imposed by the network topology. In this way, protocol implementers do not need to understand the syntax or semantics of any such optional parameters.
23. Clients MUST be able to specify whether they want, in addition to the certification path, the revocation information associated with the path, for the end-entity certificate, for the CA certificates, or for both.
24. If the DPD server does not support the client requested path discovery policy, the DPD server MUST return an error.
25. The DPD request MUST allow more elaborated path discovery policies to be referenced.
26. If the trust anchor is a self-signed certificate, that self-signed certificate MUST NOT be included. In addition, if requested, the revocation information associated with each certificate in the path MUST also be returned.
27. By default, the DPD server MUST return a single certification path for each end-entity certificate in the DPD request.
28. Therefore, the DPD client MUST have a means of obtaining more than one certification path for each end-entity certificate in the DPD request. At the same time, the mechanism for obtaining additional certification paths MUST NOT impose protocol state on the DPD server.
29. Path discovery MUST be performed according to the path discovery policy. The DPD response MUST indicate one of the following status alternatives:

1. one or more certification paths was found according to the path discovery policy, with all of the requested revocation information present.
2. one or more certification paths was found according to the path discovery policy, with a subset of the requested revocation information present.
3. one or more certification paths was found according to the path discovery policy, with none of the requested revocation information present.
4. no certification path was found according to the path discovery policy.
5. path construction could not be performed due to an error.

30. For the client to be confident that all of the elements from the response originate from the expected DPD server, an authenticated response MAY be required. For example, the server might sign the response or data authentication might also be achieved using a lower-layer security protocol.
31. The DPD server MAY require client authentication, allowing the DPD request MUST to be authenticated.
32. Using a separate request/response pair, the DPV or DPD client MUST be able to obtain references for the default policy or for all of the policies supported by the server.
33. In order to succeed, one valid certification path (none of the certificates in the path are expired or revoked) MUST be found between an end-entity certificate and a trust anchor and all constraints that apply to the certification path MUST be verified.
34. The validation policy MUST specify the source of revocation information:

1. full CRLs (or full Authority Revocation Lists) have to be collected.
2. OCSP responses, using [OCSP], have to be collected.
3. delta CRLs and the relevant associated full CRLs (or full Authority Revocation Lists) are to be collected.
4. any available revocation information has to be collected.
5. no revocation information need be collected.

35. The validation policy MUST specify the source of revocation information:

- full CRLs (or full Authority Revocation Lists) have to be collected.
- OCSP responses, using [OCSP], have to be collected.
- delta CRLs and the relevant associated full CRLs (or full Authority Revocation Lists) are to be collected.
- any available revocation information has to be collected.
- no revocation information need be collected.

Final note: It should be observed that no OIDs are being used for requests or responses parameters, except for two options that will be automatically ignored by thin clients since there are non-critical. This allows compact requests and responses, but it is also much more easy to read and debug.

C. Faktorizace a zařízení TWIRL
Jaroslav Pinkava, PVT a.s.

V roce 1999 (v době konání pražského Eurocryptu) se objevil článek známého izraelského kryptologa Adi Shamira (je to to prostřední S ve zkratce RSA), který popisoval nový přístup k problematice faktorizace velkých čísel využívající některé nepříliš standardní postupy – optoelektronické zařízení. Celé specializované zařízení nazval autor TWINKLE.

Toto zařízení umožňovalo faktorizace celých čísel až zhruba do velikosti 512 bitů (faktorizovat takto velká čísla se zhruba ve stejné době podařilo i klasickými postupy, resp. za pomocí paralelních výpočtů několika tisíc počítačů).

V novém článku Factoring Large Numbers with the TWIRL Device (autoři – Adi Shamir a Eran Tromer), jehož preprint byl koncem ledna opublikován, je popsána nová hardwarová implementace. Opírá se o využití metody Number Field Sieve, přičemž se zabývá krokem, ve kterém probíhá vlastní "síto". Autoři tvrdí, že daný postup umožňuje podstatné zvýšení efektivnosti této části NFS – ve srovnání se zařízením TWINKLE resp. ve srovnání s jiným specializovaným hardwarem (které navrhli pánové Geiselmann a Steinwandt, [2]).

Algoritmus síta (Number Field Sieve) je dnes nejznámější faktorizační metodou, v zásadě tento algoritmus obsahuje dvě podstatné části, část ve které je prováděno "síto" a získávány určité matematické vztahy a část "maticovou", ve které probíhá vlastní zpracování těchto vztahů. Bernsteinovy výsledky ukazují na možnost řešit (s využitím specializovaných obvodů) maticovou část algoritmu i pro dnes v praxi využívaní délky modulu – 1024 bitů.
Zatím však žádné zařízení nebylo schopné zpracovávat (vzhledem k délce modulu 1024 bitů), sítovou část algoritmu.

Návrh nového zařízení TWIRL vychází z postupů, které byly obsaženy již v zařízení TWINKLE, avšak příslušné postupy síta ještě navíc paralelizuje.

Podstatou NFS (stejně jako metody kvadratického síta) je snaha nalézt dvě celá čísla x a y a to tak, že

$$x^2 \equiv y^2 \mod n,$$

kde n je příslušný modul a přitom chceme, aby neplatilo $x \equiv y \mod n$. Za tímto účelem jsou využívány dvě faktorové báze, jedna sestává z prvočísel, která jsou menší než nějaká předem daná mez a druhá sestává z prvočíselných ideálů, jejichž norma je menší než určitá zadaná mez v okruhu celých čísel ve vhodném tělese algebraických čísel (přesnější detaily lze nalézt v literatuře, dnes již poměrně rozsáhlé).

V sítové části algoritmu jsou zadány čísla R (šířka síta), T (mez) a množina dvojic čísel (p_i,r_i), kde jsou p_i z výše zmíněné faktorové báze. Každé takové dvojici odpovídá aritmetická posloupnost všech čísel a kongruentních s číslem $r_i \mod p_i$. Jsou vyhledávána taková a (menší než R), která patří do hodně takových posloupností (při velkých p_i). Následně jsou prováděny pro takto získaná a určité testy, a čísla a která projdou těmito testy spolu se všemi příslušnými (p_i,r_i), tj . kde a je členem odpovídající aritmetické posloupnosti se nazývají vztahem (relation).

Zařízení TWINKLE v sobě obsahovalo destičku, která sestávala z řady nezávislých buněk, každá buňka odpovídala jedné z výše zmíněných posloupnosti P_i. Následně po inicializaci zařízení proběhlo celkem R kroků (tj. pro všechna $0 < a < R$). V každém kroku a buňka odpovídající posloupnosti P_i vydá pozitivní výsledek, pokud příslušná kongruence je splněna.

Jestliže v daném kroku je těchto pozitivních výsledků tolik, že byla překročena zadaná mez T, pak algoritmus ohlásí příslušnou hodnotu a. Sčítání probíhá s využitím analogové optiky, přitom byly využité destičky s technologií na bázi "Gallium Arsenide". V současné době jsou cenově podstatně dostupnější technologie používající křemíkové destičky.

V navrhovaném zařízení TWIRL je jednotlivá buňka nahrazena jinou jednotkou (autoři ji nazývají stanicí). Každá ze stanic se zabývá pouze malou částí celé zkoumané posloupnosti, tj. toto je podstatou paralelizace. Kompletní návrh zařízení je celkově podstatně sofistikovanější, rozděluje např. zkoumaná prvočísla do několika skupin (podle jejich velikosti) a pro každou z těchto skupin volí při vyhodnocování poněkud odlišný přístup.

Autoři se dále zabývají náklady na konstrukci zařízení TWIRL s využitím dnešních technologií. Pro modul o velikosti 1024 dospívají k následujícím závěrům.
Zařízení v počtu 44 kusů v celkové ceně 4.5 miliónů dolarů při paralelním zpracování by potřebnou sítovou část algoritmu prováděly 1 rok. Přitom poznamenávají, že další náklady spojené s provozem zařízení (spotřeba proudu, chladící systémy, sběr dat) zvednou tyto náklady na cca. 10 miliónů dolarů.

Jaké z tohoto vyvozují autoři závěry? Dosavadní hodnocení označovala existující postupy pro faktorizaci čísel v délce 1024 bitů jako výpočetně neuskutečnitelné. Avšak spolu se závěry Bernsteina (bylo o nich hovořeno v článcích Crypto-Worldu na jaře loňského roku) – maticový krok je výpočetně jednodušší, hovoří autoři již o reálné možnosti takovouto faktorizaci provést (s uvedenou výší nákladů).

Pro čísla v délce 512 bitů odhady autorů při využití zařízení TWIRL jsou následující – zařízení se zanedbatelnou cenou by provedlo sítový krok za 9 hodin, resp. zařízení v ceně deset tisíc dolarů provede výpočty za méně než 10 minut (!).

A konečně pro čísla v délce 768 bitů odhady autorů při využití zařízení TWIRL jsou – zařízení v ceně 5 000 dolarů by provedlo sítový krok za 95 dní.
Formulace autorů článku : *Vyvstávají určité pochybnosti o bezpečnosti těchto délek klíčů.*

Literatura:

[1] Shamir, A.; Tomer, E.: Factoring Large Numbers with the TWIRL Device, preprint Cryptome, January 2003

[2] Geiselmann, Steinwandt, R.: A dedicated sieving hardware, proceedings of PKC 2003, LNCS 2567, pp.254-266

[3] Lenstra, A.K.; Shamir, A; Tomlinson, J.; Tromer, E.: Aanlysis of Bernstein´s facorization circuit, proceedings of Asiacrypt 2002, LNCS 2501, pp. 1-26,

D. NIST – dokument Key Management
Jaroslav Pinkava, PVT a.s.

3. Úvod

V návaznosti na probíhající diskuse o délkách klíčů (konkrétně pro RSA, viz článek autora v tomto čísle Crypto-Worldu – Shamirovo TWIRL) je velmi zajímavým materiálem dokument NIST, který je v současnosti v podobě draftu a nazývá se Key Management Guideline (http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html).

První verze materiálu se objevila v listopadu 2001, zabývá se poměrně zeširoka celou kryptografickou infrastrukturou. Ve středu pozornosti jsou především otázky spojené s klíčovým hospodářstvím, generování klíčů, jejich použití a jejich eventuální zničení. Diskutovány jsou i příbuzné otázky jako volba algoritmů, velikosti klíčů, kryptografických politik a výběr kryptografických modulů.

Nyní (v lednu 2003) se objevila nová verze materiálu, který bude rozdělen do tří částí. První část (General Guidance - http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf) se objevila již jako draft Special Publications 800-57 - v této podobě bude příručka rozdělená do tří dílů následně vydána. Objevila se i nová verze druhého dílu (Best Practices for Key Management Organization - http://csrc.nist.gov/CryptoToolkit/kms/guideline-2-Jan03.pdf). Tato část se zabývá řídícími infrastrukturami, ustavením vhodných politik pro řízení klíčového hospodářství i vlastní řídící praxí. Část 3 je určena především správcům systémů, provádí použitím kryptografických algoritmů v konkrétních aplikacích, poukazuje na produkty, které jsou vhodné pro specifická prostředí a je návodem pro vhodnou konfiguraci těchto produktů. Nový draft této části se zatím neobjevil, je obsažena zatím pouze ve výchozím starším dokumentu (http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf).

Samotný materiál je poměrně rozsáhlý a nelze jej v krátkém článku kompletně okomentovat. Čtenáři, který se zajímá o tuto problematiku, je proto doporučováno obrátit se přímo k vlastním dokumentům

2. K obsahu KMG

Samotná první část má v dnešní podobě 130 stran, pro přiblížení obsahu jsou dále uvedeny názvy jednotlivých kapitol.

1. Introduction
2. Glossary of Terms and Acronyms
3. Security Services
4. Cryptographic Algorithms
5. Protection Requirements for Cryptographic Information
6. Key States
7. Key Management Phases

8. General Key Management Guidance

Appendix A. Cryptographic and non-Cryptographic Integrity and Authentication Mechanisms
Appendix B. Key Recovery
Appendix C. Keys Generated from Passwords
Appendix X. References.

Dokument navazuje na příručku SP 800-21 Guideline for Implementing Cryptography in the Federal Government, z listopadu 1999 a podstatně ji rozšiřuje.

V oddílu 3 jsou definovány bezpečnostní služby, které mohou být poskytnuty prostřednictvím kryptografických mechanizmů (utajení, integrita dat, autentizace, autorizace a nepopiratelnost). Stručně se zabývá i podpůrnými službami a službami kombinovanými.. Oddíl 4 dává základní informace ohledně kryptografických algoritmů (opírajících se o použití kryptografických klíčů). Jsou zde uvedeny tři základní třídy kryptografických algoritmů (hashovací algoritmy, symetrické a asymetrické algoritmy). Jako odkazy na konkrétní typy algoritmů jsou zde uvedeny algoritmy z norem FIPS (SHA-1, SHA-256, SHA-384, SHA-512, AES, Triple DES, MAC, DSA, RSA, ECDSA). Mj. je zde rovněž uvedeno, že je chystána revize dokumentu FIPS 186-2 (podpisové algoritmy). Je připravována příručka SP 800-56, která popisuje schémata pro ustavení klíčů (key establishment).

V oddíle 5 je provedena klasifikace různých typů klíčů a souvisejících informací kryptografického charakteru. Jsou zde uvedeny požadavky na ochranu jednotlivých informací kryptografického typu (je zde rozebráno celkem 19 typů kryptografických klíčů a pro každý z nich jsou uvedeny příslušné ochranné mechanizmy; kromě toho je zde uvedeno dalších 11 typů kryptografických informací a opět rozebrány požadavky na ochranu těchto informací).

Oddíl 6 identifikuje stavy, ve kterých se může kryptografický klíč nacházet během svého životního cyklu (je zde popsáno celkem sedm základních stavů – 1.Stav před aktivací, 2.Aktivní stav, 3. Procesní stav- klíč je používán pouze k zpracování informace, nikoliv k její ochraně, 4. Deaktivovaný stav, 5. Archivní stav, 6. Zkompromitovaný stav, 7. Stav, ve kterém je klíč již zničen). V návaznosti na to jsou popsány i procesy přechodu z jednoho stavu do stavu jiného.

Oddíl 7. popisuje klíčové hospodářství a životní cyklus klíčů z širšího pohledu. Jsou zde zahrnuty i otázky okolo mechanizmů pro ustavení klíčů a pro řízení souvisejících atributů. Objevuje se zde již i problematika certifikačních resp. registračních autorit (CA, RA). Rovněž tak jsou zde popisovány i otázky okolo zálohování a archivace klíčů atd.

Konečně oddíl 8. diskutuje různorodé momenty řízení klíčového hospodářství (užití klíčů, doba jejich životnosti, ověřování klíčů, audit, je zde příručka kryptografických algoritmů a volby délek klíčů a schémata pro ustavení klíčů).

Nesporně zajímavou je tabulka 8. která uvádí srovnání délek klíčů u různých algoritmů při "ekvivalentní síle těchto algoritmů" (Equivalent Algorithm Strength):

Bits of security	Symmetric key algs.	Hash functions (collision concerns)	Hash functions (no collision concerns)	DSA, D-H,MQV	RSA	Elliptic Curves
80	2TDES	SHA-1		1024+160	1024	160
112	3TDES			2048+221	2048	224
128	AES-128	SHA-256		3072+256	3072	256
160			SHA-1			
192	AES-192	SHA-384		7680+384	7680	384
256	AES-256	SHA-512	SHA-256	15360+512	15360	512
384			SHA-384			
512			SHA-512			

Z této tabulky vychází tabulka 9, která definuje doporučované algoritmy a minimální délky klíčů.

Years	Symmetric key algs. (encryption+ +MAC)	Hash functions (collisions)	Hash functions (no collisions)	DSA,D-H, MQV	RSA	Elliptic Curves
- 2015	2TDES 3TDES AES-128 AES-192 AES-256	SHA-1 SHA-256 SHA-384 SHA-512	SHA-1 SHA-256 SHA-384 SHA-512	Min: 1024+160	Min: 1024	Min: 160
2016- -2035	3TDES AES-128 AES-192 AES-256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-384 SHA-512	2048+224	2048	224
2036-	AES-128 AES-192 AES-256	SHA-384 SHA-512	SHA-384 SHA-512	3072+256	3072	256

Poznámka

K této poslední tabulce měl autor článku možnost diskuse s jedním z autorů materiálu šéf-kryptologem firmy RSA Security panem Burtem Kaliski (srpen 2002). Jeho tehdejší připomínka se nesla v tom duchu, že vzhledem k existujícím názorům bude zde možný i posun – ve vztahu k algoritmu RSA (zpřísnění). Samozřejmě je třeba vidět také fakt, že kromě bezpečnostního hlediska se zde uplatňuje i hledisko technologické realizovatelnosti.
Pro úplnost ještě uvedeme tabulku 10 z přílohy C dokumentu, která definuje vztah mezi délkou klíče a délkou hesla (Key Size/Password Size Equivalence).

Key Bits	10 decimal digits	26 letters	36 letters + numbers	94 keyboard characters	1000 word dictionary
56	17	12	11	9	6
64	20	13	13	10	7
80	25	17	16	12	8
112	34	24	22	17	11
128	39	27	25	20	13

Druhá část materiálu (Best Practices for Key Management Organization - celkem 94 stran) je orientována již na vlastní praxi řízení klíčového hospodářství. Popisovaná infrastruktura je založena na přizpůsobení PKI (Public Key Infrastructure) a dalších v praxi široce používaných infrastruktur. Materiál je dotažen až na úroveň řízení v jednotlivých organizacích a popisuje i příslušné politiky a prováděcí směrnice. Pro správce odpovídající za koncepci kryptografické bezpečností v infrastrukturách jednotlivých organizačních celků je nesporně velice zajímavým a užitečným dokumentem.

Třetí část materiálu zatím v nové verzi publikována nebyla. Původní verze obsahovala tři kapitoly. Prví z nich popisuje vybrané existující infrastruktury (PKI, Kerberos). Druhá popisuje vybrané protokoly (S/MIME, SSL). Z třetí kapitoly je v původním materiálu pouze nadpis – Vybrané aplikace – ukládání zašifrovaných dat.

E. Letem šifrovým světem

Kurs „kryptologie“ na MFF UK Praha

Na katedře algebry MFF UK Praha bude v zimním semestru 2003 zahájen "náborový kurs" ke studiu Matematické metody informační bezpečnosti.Toto studium (bakalářské i magisterské) bude pro zájemce poprvé otevřeno ve školním roce 2003/2004.

Kurs probíhá pod odborným vedením Doc. RNDr. J.Tůmy, DrSc. V kursu budou dále přednášet RNDr. Vlastimil Klíma, Ing. Tomáš Rosa a Mgr.Pavel Vondruška.

Předběžný program:

19.2.2003	Klasické šifry I.	(Tůma)
26.2.2003	Klasické šifry II.	(Tůma)
5.3.2003	Klasické šifry III.	(Tůma)
12.3.2003	Generovaní (pseudo)náhodných čísel + generování prvočísel	(Tůma)
19.3.2003	Symetrická kryptografie I.	(Klíma)
26.3.2003	Symetrická kryptografie II.	(Klíma)
2.4.2003	Hashovací funkce	(Klíma)
9.4.2003	Asymetrická kryptografie I.	(Rosa)
16.4.2003	Asymetrická kryptografie II.	(Rosa)
23.4.2003	Elektronicky podpis	(Vondruška)
30.4.2003	Standardy a normy	(Vondruška)
7.5.2003	Závěrečné shrnutí kurzu	(Tůma)
12.5.2003	Historie kryptografie 20.století a další zajímavosti	(Tůma,Klíma,Rosa,Vondruška)

Všichni studenti MFF UK jsou srdečně zváni. Další zájemci se mohou zúčastnit pouze po dohodě s doc. Tůmou (tuma@karlin.mff.cuni.cz).

Za použití šifrování do vězení

Americké ministerstvo spravedlnosti hodlá dramaticky posílit své možnosti ve sběru dat a vládní elektronické špionáži. Vyplývá to z textu připravovaného 120 stránkového návrhu nového anti-teroristického zákona Domestic Security Enhancement Act, který byl předán Bílému domu 9.1.2003. Zákon navazuje na známý USA-PATRIOT Act z roku 2001, který v mnoha ohledech zpřísňuje. Mimo jiné má např.v úmyslu zavést mnohaleté tresty odnětí svobody za použití „nezákonného šifrování“ na území USA ! Za nezákonné užití šifrování by byl podle tohoto návrhu uvězněn každý, kdo vědomě využije šifrování k utajení komunikace v souvislosti s kriminálními činy. Za tento nový trestný čin může být stanoveno odnětí svobody ve výši deset let. Minimální sazba za ilegální použití šifrování by měla být pět let! Přičemž definice ilegálního použití je zde nezřetelná a zcela obecná.

Více naleznete v článku Kevina Poulsena : „Ashcroft proposes vast new surveillance powers“ z 10.2.2003 (http://theregister.co.uk/content/55/29249.html).

Hoax jdbgmgr.exe

Také jste v posledních dnech dostali zprávu varující před neexistujícím virem? Vzhledem k tomu, že během pátku 14.2.2003 ke mně dorazila celkem desetkráte, rozhodl jsem se šíření této poplašné zprávy věnovat místo i v našem Crypto-Worldu.

Všechny e-maily vypadaly následovně (případně malinko modifikovány, jak byly upravovány snaživými odesílateli):

„ Tato zprava není žert !!

Vážení přátelé,
náš počítač byl napaden záludným virem, který se automaticky rozesílá na všechny adresy v adresáři. Jelikož v našem adresáři jste i Vy, posílám Vám návod na odstranění. Antivirové programy Norton a McAfee ho nemohou zachytit. Virus sedí 14 dní tiše v systému a potom ho ničí. Rozesílá se automaticky přes Messenger a adresář.

Je jedno jestli jste e-mail odeslali nebo ne!!!

Dá se jednoduše odstranit:
1. Stisknete START - potom NAJÍT
2. hledat soubor - napsat: jdbgmgr.exe
3. ujistěte se, že jste na hard disku C
4. klikněte na "najít"
5. virus je logo medvídka se jménem jdbgmgr.exe
6. pravým tlačítkem myši klikněte na medvídka a potom na odstranit/vymazat
7. přejděte do koše a vymažte virus i tam
8. jestliže jste virus našli, musíte poslat zprávu každému, kdo je ve Vašem adresáři, jinak se Vám bude virus od nich vracet zpět.“

Byl to samozřejmě hoax (poplašná zpráva)! Hoax JDBGMGR.EXE se nešíří poprvé, ovšem jak jsem si ověřil, opět se díky těmto e-mailům našla spousta uživatelů internetu, kteří jej sami dále rozeslali všem lidem ze svého kontakt listu a ještě se zachovali přesně podle toho, k čemu "medvídek" nabádá. Přitom tento text je napsán naprosto typickým jazykem „hoaxu“.

Jako každý hoax, i tento sděluje uživateli "důležitou" zprávu. Jedná se o to, že v systému má být soubor JDBGMGR.EXE - vir, který se po určité době nečinnosti sám aktivuje. Navíc jej nemají rozeznat žádné antiviry. Chybí jen běžně dodané upozornění, že informaci ohlásil nějaký důvěryhodný zdroj…V hoaxu je rovněž doplněno, jak "vir" ze systému odstranit (dokonce i z koše, aby nešel obnovit). Toho se má docílit obyčejným smazáním souboru, ale.. JDBGMGR.EXE jak již víme NENÍ žádný vir, nýbrž systémový soubor.

I když jej nějaký naivka smaže, nic tak hrozného se nestane, soubor se dá naštěstí opět nainstalovat (a to dokonce běžným zkopírováním z vedlejšího PC !) a chod systému jeho absenci stejně nepozná.

Interview

Rozhovor Michal Tilla s Pavlem Vondruškou naleznete v sekci KRYPTOGRAFIE V PRAXI (14.1.2003) na serveru www.krypta.cz. Michal Till, který kladl otázky jej uvedl následovně:

„S Mgr. Pavlem Vondruškou o elektronickém podpisu a jeho stavu v ČR. Zájem okolo elektronického podpisu v naší společnosti vzniká a zaniká vždy s nějakou klíčovou událostí. Schválení zákona Parlamentem, akreditování první CA apod. Jaký je tedy stav věcí? Kdy budeme místo na úřad chodit na internet a co k tomu je ještě zapotřebí? O tom a o mnohém dalším se dočtete v dnešním rozhovoru na http://www.krypta.cz/articles.php?ID=239 „

AEC uvedla do provozu certifikační autoritu TrustPort

Společnost AEC Data Security Company (http://www.aec.cz) zahájila provoz nové certifikační autority TrustPort, která bude jako jedna z prvních v České republice v dohledné době doplněna o vlastní řešení autority časových značek.

TrustPort byla vybudována na základě dlouholetých zkušeností v daném oboru, které společnost AEC získala provozováním předchozí certifikační autority TrustCert. Ta vydala první plnohodnotné digitální certifikáty pro elektronický podpis již v roce 1999.

Certifikační autorita TrustPort byla budována v souladu s podmínkami stanovenými Zákonem o elektronickém podpisu ve znění pozdějších úprav a dalších souvisejících předpisů a je připravena na akreditaci Ministerstvem Informatiky ČR.

Řešení TrustPort představuje nejen certifikační autoritu jako takovou, ale především celý pilotní projekt její realizace. Společnost AEC je schopna nasadit svoje řešení kterémukoliv zájemci tzv. „na klíč“, včetně zohlednění jeho specifických požadavků a potřeb. Vlastní certifikační autorita se tak může stát základním pilířem PKI infrastruktury v řadě různých organizací (bankovnictví, telekomunikace, státní správa apod.).

Unikátnost řešení TrustPort podtrhuje i skutečnost, že autorita má i vlastní řešení tzv. autority časových značek (Time Stamp Authority) a bude tak pravděpodobně jako první v České republice schopna vydávat i časová razítka. To představuje především účinný nástroj, který snižuje možnost zneužití elektronického (nebo chcete-li digitálního) podpisu vzhledem k určení času, kdy již podepsaný dokument existoval (např. smlouva). Může tak významně přispět ke zvýšení důvěryhodnosti elektronických transakcí a být využito v případných právních sporech.

Certifikační autoritu TrustPort můžete najít na adrese http://www.trustport.cz/ . Její základní funkce můžete vyzkoušet přímo na těchto stránkách vygenerováním zkušebního „trial“ certifikátu, který je zdarma.

6. ročník konference
Information Systems Implementation and Modelling ISIM'03
(informaci připravil Daniel Cvrček)

Součástí konference bude letos poprvé i zvláštní část věnovaná bezpečnosti informačních systémů a počítačové kriminalitě.

Důležité termíny:
14. února - zaslání příspěvků
14. března - oznámení o přijetí
30. března - zaslání upravených příspěvků
30. března - ukončení registrace
28.-30. dubna - konání konference

Pořadatelé: Fakulta informačních technologií
Vysoké učení technické v Brně
Katedra informatiky
VŠB-TU Ostrava
ve spolupráci s Českou a slovenskou společností pro simulaci

Kontaktní adresa: Předseda programového výboru
Miroslav Beneš
miroslav.benes@vsb.cz

Poštovní adresa: Jan Štefan
Katedra informatiky, FEI VŠB-TU Ostrava
17. listopadu 15
708 33 Ostrava-Poruba

Další informace najdete na www stránkách konference: http://www.isim.cz/

Program
Přivítáme originální příspěvky popisující výsledky, nové myšlenky a aplikace v oblasti teorie, vývoje, správy a používání pokročilých informačních systémů. Zároveň je možné zasílat příspěvky pokrývající oblast vývoje a údržby reálných systémů. Témata obsahují, ale nejsou limitovány následujícími oblastmi:

Bezpečnost informačních systémů a počítačová kriminalita
- bezpečnost Internetu, firewaly
- hackerské techniky, principy útoků a zajištění incidentů
- pohotovostní a reakční počítačové týmy (emergency and response teams)
- legislativa
- technologie pro prozkoumávání hardware a programového vybaveni
- kryptografie, digitální podpisy, PKI
- analýza rizik, stanovení zranitelnosti

Teoretické základy pro modelování informačních systémů:
Návrh a implementace informačních systémů
Informační systémy v obchodním prostředí
Modelování informačních systémů ve výuce

O čem jsme psali v únoru 2000 - 2002

Crypto-World 2/2000

Crypto-World 2/2001

Crypto-World 2/2002

Příloha:
Program pro naše čtenáře : "Hašák ver. 0.9" (viz. letem šifrovým světem) hasak.zip

!! Původní příloha – program hasak.zip obsahoval chybu. Z tohoto důvodu jsem tuto přílohu později nahradil novější verzí – programem DataHash.

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 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://www.mujweb.cz/veda/gcucmp

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://www.mujweb.cz/veda/gcucmp/ . 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@ct.cz
vondruska.p@seznam.cz
pavel.vondruska@post.cz