Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 11/2003 **18. listopad 2003**

11/2003

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Soutěž 2003 – průběžná zpráva
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Soutěž v luštění jednoduchých kryptologických úloh, kterou jsem vyhlásil v zářijovém čísle Crypto-Worldu se blíží ke svému závěru. Prvá tři místa (tj. místa, na nichž řešitel automaticky získal cenu) byla obsazena již v průběhu prvého týdne soutěže. Ve hře jsou však stále ještě tři další ceny (replika historické číše Rudolfa II. s láhví portugalského vína MATEUS). Tyto ceny budou vylosovány po oficiálním ukončení soutěže (6.12.2003, 22.00 hod) mezi ty řešitele – čtenáře Crypto-Worldu, kteří vyluští do té doby alespoň tři ze všech devíti zadaných úloh.

Dostat se mezi účastníky, o nichž rozhodne los, by nemělo být pro naše čtenáře problém. Celkový vítěz (CyberMage), který za své vítězství získal i exkluzivní cenu účast na kryptologické konferenci MKB (o které píšeme v tomto čísle na jiném místě) hodnotil prvé tři úlohy takto:

"Největší můj problém byly úlohy 1-3, protože byly extrémně lehké. V okamžiku, když jsem rozluštil úlohu číslo 1, tak jsem málem 'bil hlavou do zdi'. Přece jen jsem očekával větší složitost už v prvním kole".

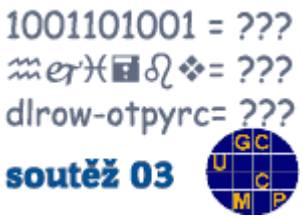
Do soutěže se zapojilo již **96 řešitelů**, z nichž však teprve **25 splnilo požadavek na zařazení do losování o zbývající 3 ceny** (tj. jedná se o odběratele Crypto-Worldu, kteří vyřešili minimálně 3 úlohy), všech **9 úloh vyřešilo již 9 soutěžících** (stav 15.11.2003).

Vítězové letošní soutěže:
registrační jméno, pořadí vyřešených úloh, e-mail)

```
1 CyberMage     01; 03; 02; 04; 05; 06; 09; 08; 07;   (jry2000@seznam.cz)
2 peta007       01; 04; 07; 02; 03; 05; 06; 08; 09;   (peta007@seznam.cz)
3 xnovakv       02; 05; 06; 03; 01; 04; 08; 07; 09;   (xnovakv@volny.cz)
```

Podle aktuálního přehledu vyřešených úloh a z e-mailové korespondence, kterou jsem dostal, dělají řešitelům stále největší problém obě úlohy na transpozici 04 (12 řešitelů) a 07 (11). Naopak jednoznačně za nejlehčí, považují soutěžící úlohu 01 (43). Za lehké také označují skupinu úloh 03 (29), 02 (22) a 05 (21).

Jména vylosovaných řešitelů, kteří získali zbývající tři ceny, jakož i řešení všech devíti úloh s průvodním komentářem bude zveřejněno v e-zinu Crypto-World 12/2003.



Závěrem vás srdečně k využití posledních týdnů a k zapojení do probíhající soutěže. Úlohy, aktuální stav, pravidla a ceny (včetně odkazů na sponzory) najdete na:
http://crypto-world.info ikona „soutěž 2003“.

B. Mikulášská kryptobesídka – Program

ECOM-MONITOR.COM

8. prosince (Úterý)

Kongresové centrum IKEM, Vídeňská 1958/9, 140 21 Praha 4

15:30 - 16:20	Registrace
16:20 - 16:30	Zahájení workshopu
16:30 - 17:30	Ross Anderson - The New Research Frontier - API Security

Prostor pro diskusi k tématu

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

9. prosince 2003 (Středa)

Kongresové centrum IKEM, Vídeňská 1958/9, 140 21 Praha 4

9:00 - 9:25	Registrace
9:25 - 9:30	Zahájení druhého dne workshopu
9:30 - 10:30	Serge Vaudenay - Matsui's Attack and Beyond: On Measuring Resistance to Linear Cryptanalysis
asi 10:35 - 11:05	Milan Vojvoda - On One Hash Function Based on Quasigroup
asi 11:10 - 11:40	Martin Drahanský, Luděk Smolík, Filip Orsag - Biometric Security Systems
asi 11:45 - 12:00	David C. Hájíček - Ověření času a služby elektronického notáře
do 13:30	Oběd
13:30 - 14:15	Alexandre Stervinou - Standards for Federated Network Identity: The Liberty Alliance
14:20 - 14:50	Daniel Cvrček - Using Evidence for Trust Computation
do 15:30	Přestávka na kávu
15:30 - 16:00	Jan Bouda - Úvod do kvantové kryptografie
16:05 - 17:30	Panelová diskuse - Kryptografie v praxi a teorii: jedno a totéž, či nikoliv?
Panelisté:	Jaroslav Dočkal , Otokar Grošek , Petr Hanáček Daniel Olejár , Tomáš Rosa - moderátor
Nosné otázky:	- proč se prakticky používané systémy příliš neblíží všem teoriím, které se probírají na kryptologických workshopech a konferencích - je teorie v době svého vzniku příliš vzdálená od praxe, nebo praxe nestačí teorii, nebo je to úplně jinak - máme s tím něco dělat a když, tak co?

Závěr workshopu

Mediální partneři:

Data Security Management

Crypto-World

C. Cesta kryptologie do nového tisíciletí IV. (Od NESSIE ke kvantovému počítači) Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Čtyřdílný seriál *Cesta kryptologie do nového tisíciletí* v dnešním čísle končí. Vznikl v létě 2000 a byl publikován v COMPUTERWORLDU 37/2000-40/2000. Zde jsem jej přetiskl v původní, neupravené verzi. Z tohoto důvodu obsahuje přehled důležitých informací do poloviny roku 2000 a z dnešního pohledu jsou v seriálu některé uvedené informace již zastaralé, ale informace jsou stále platné a neobsahuje chyby. Děkuji Vám také touto cestou za velký zájem o tento seriál a opakované přání, abych jej doplnil do současnosti, se pokusím někdy až bude vhodná příležitost splnit.

Zlomové roky 1999-2000

Odborná veřejnost na konci devadesátých let je již dostatečně sebevědomá. Cítí, že dospěla do situace, kdy je schopna konkurovat pečlivě střeženým tajemstvím agentur velkých mocností. Již se neobjevují slabé šifrové systémy, které ještě v polovině devadesátých let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code). Odborná veřejnost umí velice dobře a rychle ocenit kvalitu určitého systému. V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů. Takto úmyslně upraveným algoritmům se říká slabá kryptografie. Mimo území USA a Kanady se tak stále v těchto produktech nacházejí slabé šifrové produkty. Toto je ovšem výhodná situace pro evropské komerční firmy, které se snaží obsadit evropský trh svými produkty. Americké velké firmy se snaží donutit vládu USA k omezení vývozních restrikcí, ale ta neustupuje. Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás. Česká firma Decros úspěšně vyváží své produkty nejen do Evropy, ale i do Asie. Firma AEC se stává průkopníkem v použití asymetrické kryptografie na bázi eliptických křivek. Produkty se stávají bezpečnými a začínají je "prodávat" již jiné vlastnosti - uživatelská přítulnost, kvalita klíčového hospodářství apod.

Květen 1999 je pro Českou republiku určitým ohodnocením naší vyspělosti v této oblasti. Výbor IACR v roce 1997 rozhodl, že konference Eurocrypt 1999 se bude konat v Praze. Na konferenci je profesorem Shamirem předvedeno optické zařízení Twinkle, které je schopno zrychlit jednu z fází faktorizace velkých čísel a dochází tak k faktickému ohrožení klíčů RSA o délce 512 bitů. O Shamirově přednášce se píše po celém světě, informaci otiskuje i NewYork Times. Teprve tehdy se v několika českých novinách objevuje zmínka o konferenci.

V srpnu 1999 pak bylo skutečně dosaženo vytouženého cíle, bylo rozbito číslo ze souboru RSA s délkou klíče 512 bitů (155 ciferné dekadické číslo). Dodnes však nebyl přechod na klíče délky 1024 bitů (doporučená bezpečná délka klíčů pro RSA nejméně do roku 2002) důsledně proveden.

V létě 1999 německá vláda vydává prohlášení, ve kterém jasně proklamuje, že na dobu dvou let ruší všechny restrikce v používání silné kryptografie a dává celému světu najevo, že chce zaujmout rozhodující pozici v evropském trhu s kryptografií.

Tlak amerických firem, které přicházejí o milióny dolarů, nakonec slaví úspěch. V listopadu 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu 2000. S konečnou platností je tak uvolněn export šifrovacích algoritmů ze Spojených států (včetně zdrojových textů). Uvolnění se týká všech zemí kromě Kuby, Iránu, Iráku, Libye, Súdánu, Sýrie a Severní Koreje. V budoucnu může být jakýkoliv běžně prodávaný program pro šifrování dat exportován poté, co bude jednorázově prověřen ("one-time review") a obdrží výjimku z exportních licencí. Exportní licence se netýkají některých států (např.Kanady, Velké Británie). Během léta (18.7.2000) pak ČTK oznámila, že nebude licence pro vývoz do ČR potřeba a čekání na prověření odpadne.

Dospěli jsme v mnoha ohladech ke zlomovému roku 2000. Vstup do tohoto roku byl poznamenán svým populárním problémem Y2K - přechodem na datum 2000. Odborníci tvrdí, že na hladký přechod do nového tisíciletí bylo vynaloženo celkem 200 miliard dolarů. Významným aspektem byla inventura počítačových systémů, investice do modernizace a uvědomění si nutnosti mít připraven krizový plán organizace a zvýšení zájmu o bezpečnost dat vůbec. Poslední aspekt pak znamenal nepřímo i zvýšení zájmu veřejnosti o dění v oblasti zabezpečení dat a akceleraci vývoje v této oblasti.

NESSIE

Jak již jsme se zmínili, na jaře roku 2000 se provádělo důkladné hardwarové vyhodnocení algoritmů - kandidátů AES.

Především evropská veřejnost však není úplně jednotná v hodnocení kandidátů a v procesu výběru kandidátů a jejich hodnocení a vznikly proto v jejich kruzích určité rozpaky. Možná, že právě tento moment byl jedním z faktorů nové aktivity v rámci Evropské unie, kde vznikla vlastní iniciativa na výběr vhodných kryptografických modulů.

Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org). NESSIE je tříletý projekt, který byl zahájen 1. ledna 2000 a oficiálně vyhlášen v květnu na konferenci Eurocrypt 2000. Jednotlivé moduly budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou.

Celkem se jedná o celý systém kryptografických primitivů (blokové šifry, synchronní proudové šifry, samosynchronizující se proudové šifry, autentizační kódy zpráv - MAC, hashovací funkce, jednosměrné hashovací funkce, pseudonáhodné funkce, asymetrická schémata pro šifrování, asymetrická schémata pro digitální podpis, asymetrická schémata pro identifikaci). Nejedná se tedy jako v projektu NIST o výběr standardu pouze pro symetrický blokový algoritmus (AES), ale výběr standardů pro celou oblast kryptografie.

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s výjimkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). Tj. například blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a s klíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

První kolo končí v září 2000. Do tohoto data mají být odevzdány výchozí návrhy.

Jedním ze základních cílů projektu je také posílit pozice evropského kryptografického průmyslu v návaznosti na výsledky evropského výzkumu.

Prošli jsme se dějinami kryptologie od starověku po dnešní dobu. Shrneme-li celý několika tisíciletý vývoj, máme nyní k dispozici matematickou a informační teorii, kryptologie se stala uznávanou vědou, která se z kanceláří tajných služeb přesunula do laboratoří velkých počítačových firem a na akademickou půdu. Přestala být tajemstvím. Kryptologii je možné studovat. Základní kurzy jsou dostupné i pro naše studenty na Masarykově univerzitě v Brně nebo Matematicko-fyzikální fakultě UK v Praze. Byly zrušeny vývozní a jiné administrativní překážky. Legislativa upravuje použití elektronických podpisů. Vědci umí navrhnout bezpečné šifrovací algoritmy, které se liší spíše jen parametry implementačními (rychlost, nároky na paměť) než bezpečnostními. Jsou vypracovávány a přijímány mezinárodní standardy a normy. Zdá se, že vývoj je v podstatě ukončen.

Teoretické hrozby současné kryptografii

Je vůbec něco, co může ohrozit současné symetrické nebo asymetrické algoritmy mimo hrubou sílu - mimo zvyšující se výpočetní potenciál? Zvyšujícímu se výpočetnímu potenciálu, který má kryptoanalytik k dispozici, se dá lehce čelit zvětšováním klíčů. Současné používané délky klíčů 128 bitů by měly při zachování rychlosti vývoje výpočetní techniky (zdvojnásobení výkonu zhruba každé dva roky) odolat desítky let. Autoři Lenstra a Verheul na základě hluboce sofistikované analýzy docházejí přitom k poměrně velice přísným doporučením pro rok 2020 (aby bezpečnost elektronické informace byla garantována pro období 20 let); symetrické klíče by měly mít minimálně délku 86 bitů, modul RSA minimálně 1881 bitů, analogicky i modul pro diskrétní logaritmus, pro eliptické křivky by měla být minimální délka klíče 161 bitů.

Nyní zdánlivě odbočíme. CMI (Clay Mathematics Institut of Cambridge) vyhlašuje na konferenci v Paříži 24.5.2000 sedm matematických problémů tisíciletí. Současně je připraven fond se sedmi milióny dolary. Za řešení každého z problémů je vypsána odměna jeden milión dolarů. Neočekává se, že budou vyplaceny příliš brzy. První z problémů má velice jednoduchý název: "P versus NP". Problém vychází z teorie složitosti. Složitost algoritmu je dána výpočetním výkonem nárokovaným pro jeho realizaci. Často se hodnotí dvěma proměnnými - časovou nebo prostorovou náročností. Obecně se výpočetní složitost algoritmu vyjadřuje "velkým" O - řádem (Order) - hodnoty výpočetní složitosti. Bude-li například T=O(n), pak zdvojnásobení velikosti vstupu zdvojnásobí dobu zpracování; takový algoritmus nazveme lineární. Je-li složitost na n nezávislá, píšeme O(1). Doba zpracování algoritmu se při zdvojnásobení vstupu nezmění. Bude-li $T=O(2^n)$, pak zvětšení velikosti vstupu o 1 bit prodlouží dobu zpracování na dvojnásobek. Algoritmy mohou být z hlediska složitosti kvadratické, kubické apod. Všechny algoritmy typu $O(n^m)$ se nazývají polynomiální. Třída P potom obsahuje všechny algoritmy, které mohou být řešeny v polynomiálním čase.

Dále definujme Turingův stroj jako konečný automat s nekonečnou čtecí-zapisovací páskovou pamětí. Čtenář si může představit klasický domácí počítač, ale rozšířený o nekonečnou paměť. Třídu NP definujeme jako všechny problémy, které mohou být řešeny v polynomiálním čase pouze nedeterministickým Turingovým strojem: tj. variantou normálního Turingova stroje, která může provádět odhady. Stroj odhaduje řešení problémů - buď tak, že metodou pokusů hádá správné řešení nebo tak, že paralelně provede všechny pokusy - a výsledky těchto pokusů prověřuje v polynomiálním čase. Třída NP zahrnuje třídu P, protože jakýkoliv problém řešitelný v polynomiálním čase deterministickým Turingovým strojem je také řešitelný v polynomiálním čase nedeterministickým Turingovým strojem. Jestliže všechny problémy NP jsou také řešitelné v polynomiálním čase deterministickým strojem,

pak NP=P. Otázka platnosti P=NP je ústředním nevyřešeným problémem teorie výpočetní složitosti. Nyní se z naší zdánlivé odbočky vrátíme k samotným základům současné kryptografie. Kdyby někdo prokázal, že P=NP, pak bychom většinu toho, na čem je založena současná moderní kryptologie, mohli odepsat. Znamenalo by to, že pro všechny symetrické problémy existuje kryptoanalytický (luštitelský) algoritmus, který je časově polynomiální. Pro lepší pochopení jen podotkneme, že útok hrubou silou je "nesrovnatelně" horší - jeho složitost je tzv. superpolynomiální. V takovém případě by naše neschopnost řešit algoritmy typu 3DES a AES v rozumném čase znamenala jen to, že se nám zatím nepodařilo najít vhodný luštící algoritmus. Většina současných odborníků se však domnívá, že rovnost tříd problémů P a NP neplatí. Vyplacení jednoho miliónu dolarů matematikovi v případě, že dokáže nerovnost tříd P a NP (a tím zároveň dokáže, že současné blokové algoritmy jsou opravdu bezpečné), není ve světle právě popsaných skutečností přehnaně vysoké ocenění.

Je zde ještě jedna cesta, která může ohrozit pracně dostavěnou budovu kryptografie nebo alespoň některou z nejdůležitějších částí. Toto nebezpečí se nazývá kvantový počítač. Na rozdíl od klasického počítače, kde bit má jen dva stavy, u kvantového počítače je základem přenosu informace kvantový bit (qubit). Qubit může být podle kvantové mechaniky v lineární superpozici dvou klasických stavů. Heisenbergův princip neurčitosti formuluje základní vlastnosti tohoto qubitu. Východiskem algoritmů zatím hypotetického kvantového počítače jsou tzv. unitární transformace pracující s vektory qubitů. Na rozdíl od transformací probíhajících v klasickém počítači jsou unitární transformace vždy reversibilní, tj. vždy existuje možnost jít algoritmem pozpátku. V roce 1994 Shor prokázal existenci kvantového polynomiálního algoritmu pro řešení diskrétního algoritmu a úlohu faktorizace velkých čísel.To znamená, že pokud se zdaří konstrukce kvantového počítače, bude nutné přestat používat v podstatě všechny současné systémy s veřejným klíčem (RSA, Diffie-Hellman), které jsou založeny na obtížné řešitelnosti úlohy faktorizace a úlohy diskrétního logaritmu (tyto úlohy nepatří do třídy NP problémů, ale jen do speciální třídy těžce řešitelných problémů). Konstrukce kvantového počítače podle některých odborníků není takovou utopií, jak by se na prvý pohled mohlo zdát. Někteří experti odhadují, že doba k faktické realizaci by mohla být kolem dvaceti let. Výzkumem kvantové kryptologie se zabývají i pracoviště v České republice. Česká republika dokonce drží světové prvenství v realizaci kvantového šumátoru, který je možné využít jako kvalitní zdroj pro vytváření náhodných posloupností. V optické laboratoři v Olomouci byl vyvinut a je instalován i kvantový kryptograf. Cesta ke kvantovému počítači však je ještě daleká.

Na úplný závěr se vrátíme zpět do poloviny našeho roku 2000. Jaký dopad může čtenář osobně očekávat od celého tohoto vývoje ? Nastala doba, kdy softwarové a hardwarové firmy mohou tvořit na základě standardů a norem bezpečné aplikace. Pokud firmy vyřeší bezpečné a uživatelsky jednoduché uchovávání klíčů, pak se nebude muset čtenář bát, že produkty, které nějak prokáží svoji shodu s těmito celosvětovými standardy (na základě validace, certifikace apod.) jsou děravé. Bezpečné kryptografické produkty (společně s právními akty - zákony, vyhláškami) povedou k nebývalému rozšíření kryptografie. Zatímco aplikovaná kryptologie byla dříve výsadou tajných služeb, armád a diplomacie, stává se během posledních deseti let věcí veřejnou a současně i výnosným obchodem. Zahajuje svoje masové tažení za všemi uživateli výpočetní techniky. Pojmy jako státní informační systém, e-bussines, e-komerce, e-obchodování, elektronický notář, kvalifikovaný certifikát, ochrana osobních dat a další se stanou samozřejmou součástí našeho jazyka a jejich realizace bude možná právě díky kvalitním kryptografickým produktům a právnímu zajištění.

D. Kryptografie a normy - Digitální certifikáty. Politika pro vydávání atributových certifikátů - požadavky, část 2. (Technical report ETSI 102 044)

Jaroslav Pinkava, PVT a.s.

1. Úvod

První část tohoto příspěvku byla zveřejněna v předminulém čísle Crypto-Worldu (9/2003, str.4-7). Dnes pokračujeme druhou částí dokumentu pracovní skupiny ETSI - Electronic Signatures and Infrastructures (ESI) - Requirements for role and attribute certificates.

Cílem citovaného dokumentu je identifikace souboru požadavků, které by následně byly základem chystané normy pro požadavky na politiku pro vydávání atributů(ať již atributovými autoritami či certifikačními autoritami - jako součást atributového certifikátu či jako jedno z rozšíření digitálního certifikátu).

2. Umístění atributů v certifikátu

Atributy lze certifikovat dvěma způsoby - pomocí certifikátů veřejného klíče nebo atributových certifikátů. V každém případě subjekt potřebuje alespoň jeden certifikát veřejného klíče + možná atributový certifikát. CA, která je zároveň ACA (atributovou certifikační autoritou) může teoreticky vydat certifikát veřejného klíče (CVK), který obsahuje atributy, jejichž doba platnosti je kratší než platnost CVK. CA nemá za úkol průběžně hlídat platnost garantovaných atributů, avšak musí odvolat certifikát, pokud získá informaci, že atribut již není platný. Doporučuje se proto, aby CVK obsahovaly jen takové atributy, jejichž životní cyklus není kratší než je doba platnosti certifikátu. Také je třeba poukázat na jeden základní rozdíl mezi PKC a AC - PKC musí vydat CA, zatímco AC může být vydán atributovou autoritou (AA), která není CA.

Certifikáty veřejného klíče mohou některé atributy podporovat přirozenou cestou a to
- použitím atributového typu *Common Name* a/anebo
- použitím atributového typu *Title*.

Atributový typ *Common Name* specifikuje identifikátor objektu, jeho hodnotou je řetězec znaků.Např. CN = "Mr.John Smith BSc". Atributový typ *Title* specifikuje stanovenou pozici či funkci objektu v organizaci - např. T = ředitel, obchodní úsek".

Certifikáty veřejného klíče mohou obsahovat rozšíření **subjectDirectoryAttributes,** obsahující atributy spojené s certifikátem veřejného klíče. Dle rfc.3039 mohou zde být následující atributy: **title; dateOfBirth; placeOfBirth; gender; countryOfCitizenship; countryOfResidence**.

Samotný atributový certifikát je datová struktura (vydaná atributovou autoritou), která obsahuje množinu atributů pro koncovou entitu a některá další data umožňující přiřadit datovou stukturu k CVK. Celá struktura je digitálně podepsána soukromým klíčem vydávající atributové autority. Viz specifikace [1],[2] - avšak tyto specifikace (popisující příslušné

datové struktury) se netýkají politik pro vydávání atributových certifikátů (obdoby certifikační politiky CA).

Obecně řečeno - atributy mají svou vlastní dobu života lišící se od doby platnosti certifikátu veřejného klíče. Nemá proto smysl umisťovat atributy do CVK v případech, kdy životnost atributů je kratší než doba platnosti CVK (který propojuje totožnost jedince a veřejný klíč). Také uplatnění bezpečnostních hledisek ukazuje vhodnost rozdělit atributy a subjekt použije potom pouze ty, které jsou momentálně vyžadovány konkrétní politikou.

Podle rfc.3281 je autorita atributové politiky organizací, která přiděluje hodnoty atributů, zatímco vydavatelem AC je jeden ze serverů, který tato organizace řídí. Tento rozdíl je nutné specifikovat. Je to užitečné v situacích, kdy existuje jediná autorita atributové politiky, ale je více vydavatelů atributových certifikátů (z různých důvodů)..

3. Správa atributových certifikátů

Jedinou odpovědností CA, kterou lze odvodit ze směrnice EU pro elektronický podpis, aplikovatelnou ve vztahu k ověřování atributů najdeme v článku 6 bod 2. Jedná se o odpovědnost za situace, kdy v důsledku chyby poskytovatele nebyl certifikát odvolán. TJ. CA, který vydává CVK nemusí nutně verifikovat atributy, stejně jako další informace obsažené v certifikátu, v čase kdy certifikát již byl vydán. Tj. atribut lze ověřit pouze v čase, kdy je prováděna registrace. Na nositeli certifikátu leží odpovědnost za to, že bude o případných změnách informovat CA a požádá sám o odvolání certifikátu.

Pro AC je možné definovat politiky, které rozlišují mezi:
- atributy, které jsou ověřovány pouze v momentu registrace;
- atributy, které jsou postupně ověřovány, zda jsou stále platné.

V případě postupného ověřování musí být v určitých pravidelných intervalech vydáváno příslušné potvrzení - jinak atribut nebude již nadále s danou osobou asociován. Toto postupné ověřování nemusí nezbytně provádět AA, může být delegováno.

Atributový certifikát (obsahující atributy) je jednoznačně přiřazen k CVK daného subjektu pomocí baseCertificateID (jméno vydávající strany - Issuer name + pořadové číslo CVK vlastníka certifikátu). Pokud je požadován atribut, žadatel musí předložit jeden ze svých CVK. Atributová autorita se ujistí, že daný CVK byl skutečně vydán tomuto žadateli, v opačném případě by se nositelem atributu stal jiná (neoprávněná) osoba . Nemusí to být spojeno s autentizací osoby, ale je třeba se ujistit, že certifikát obdržela správná osoba.

Existují dvě základní cesty k zajištění tohoto cíle:
- identifikátor (např. jméno osoby - subject name a/anebo subjectAltName), obsažený v CVK obsahuje informace, které lze ověřit průkazem totožnosti, který je AA předkládán;
- CA musí klientovi poskytnout nějaký typ atestace, který umožní vydaný CVK asociovat s informací, kterou přeložil klient při žádosti o CVK.

Např. dle italského zákona musí kvalifikovaný certifikát obsahovat (v subject name) tzv. Fiscal Code (číslo odvozené z jména osoby a data a místa jeho narození). TJ. pokud osoba předloží atributové autoritě platný průkaz totožnosti, dále CVK, plastikovou kartu s vyraženým "Fiscal Code" a dokument, kterým prokáže oprávnění k atributu, který má být

certifikován (nebo například prostě za tento atribut zaplatí - v určitých situacích) - potom nelze mít pochyby o tom, že je oprávněným nositelem atributu.

Pokud končí platnost CVK, pak všechny AC k němu vázané se stávají nepoužitelnými. V případě, kdy daná osoba má již i nový certifikát, stačí aby AA ověřila shodu polí, která se týkají samotného subjektu, v obou certifikátech. Doporučuje se proto do pole DN subject name umisťovat dlouhodobě stabilní informace. Informace víceméně přechodného charakteru (mailová či poštovní adresa) se doporučuje umístit do rozšíření subjectAltName.

Jestliže doba platnosti atributových certifikátů je tak krátká, že samotný proces revokace (změna statutu certifikátu) by probíhal déle než je tato doba platnosti, pak samozřejmě není ani nutné ani užitečné, aby AC obsahovaly informaci o tomto revokačním statutu.

Pokud je ovšem třeba proces odvolání řešit, pak tento proces má odlišný charakter než proces pro odvolání CVK. Odvolání se nemusí týkat jednoho konkrétního AC, ale může se týkat všech aktivních AC, které obsahují nějaký konkrétní atribut. Atributová autorita tedy musí mít přehled o všech právě platných AC - aby byla schopna zvážit, které je třeba odvolat. V politice AA musí být obsaženy podmínky pro odvolání certifikátů. V prováděcí směrnici atributové autority musí být obsaženy postupy pro vyžádání si atributového certifikátu. Dále zde musí být také obsaženy postupy pro delegování AC.

4. Doporučení

Zatímco CVK jsou vždy vydávány v rámci pevných certifikačních politik, mohou AC být vydávány v rámci různých politik pro atributové certifikáty.Tedy tatáž atributová autorita může podporovat více politik.

Atributová certifikační autorita zodpovídá za správnou hodnotu atributů při jejich vstupní registraci. Záleží na ACA, jaký postup zvolí pro zajištění správnosti těchto hodnot (za tyto hodnoty ACA zodpovídá). ACA musí uchovávat kopie těch informací, které v rámci tohoto procesu získala. V prováděcí směrnici ACA může specifikovat detaily oficiálních informací a detaily praktik při vydávání atributových certifikátů.

Pro každý z atributů musí ACA specifikovat následující:

a) popis atributu v čitelné a srozumitelné podobě (včetně případného legislativního odkazu);
b) jak bude atribut reprezentován (např. znakový řetězec, OID);
c) zda je atribut certifikován důvěryhodným zdrojem (např. autoritou vydávající atributy) nebo je pouze ověřován. V druhé situaci musí být specifikovány dokumenty, které musí subjekt předložit pro tuto verifikační proceduru.
d) zda daný atribut je veřejně dostupný nebo zde existují omezení;
e) jak bude daný atribut poskytován (např. jako součást CVK či AC);

V atributovém certifikátu může být obsažen libovolný druh atributu (krátkodobý, dlouhodobý, doživotní). AA zodpovídá za správnost těchto atributů při jejich vstupní registraci. AA také může postupně ověřovat zda správnost atributů se v čase nemění. Pak vydává v určitých intervalech potvrzení o této skutečnosti (jinak by atributy již nebyly certifikovatelné). Ověřování může AA delegovat. Každý vydaný atributový certifikát musí být označen, která z následujících tří možností je použita:

- ověření atributu pouze při vstupní registraci, neexistuje revokace;
- ověření atributu pouze při vstupní registraci, existuje revokace;
- postupné ověřování atributu, revokace je podporována (může být zde i popsán časový interval, po kterém probíhá ověřování).

Konkrétní postupy pro práci s atributy musí být specifikovány v prováděcí směrnici atributové autority (ACPS). Atributová autorita by měla informovat klienty a spoléhající strany o nezbytnosti používat aplikace, které ověřují použité AC a asociované PKC (zjišťují zda nevypršela doba jejich platnosti či zda nejsou odvolány).

Poznámka 1: Dokument rfc.3281 specifikuje profil atributového certifikátu ve vztahu k autorizaci (k oprávněním). Netýká se tedy otázek nepopiratelnosti nebo autentizačních služeb. Autoři doporučují, aby byl zpracován nový dokument "Profil atributového certifikátu pro elektronické podpisy".

Poznámka 2: V dokumentu je dále proveden stručný odkaz na dva využitelné typy protokolů pro vydávání atributového certifikátu (na základě žádosti či přímo atributovou autoritou). Pro druhou situaci je např. využitelné schéma popsané v dokumentu draft-ietf-pkix-ldap-ac-schema-00.txt.

5. 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] Pinkava, J.: Atributové certifikáty a PMI, Datakon 2002

[4] Attribute Certificate Policy Extension, draft-ietf-pkix-acpolicies-extn-03.txt

[5] LDAP Schema for X.509 Attribute Certificates, draft-ietf-pkix-ldap-ac-schema-00.txt

[6] Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates, ETSI TR 102 044, v1.1.1, December 2002

[7] Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, ETSI TS 101 733

[8] Directive 1999/93/EC, Community framework for electronic signatures, 13.Dec.1999

E. Archivace elektronických dokumentů
Jaroslav Pinkava, PVT, a.s.

1. Úvod

V nedávné době zahájila svoji činnost nová pracovní skupina IETF: Long-Term Archive and Notary Services (ltans) - http://ltans.edelweb.fr/ . Přesněji - ustavena byla 21. října 2003 a 11. listopadu 2003 bylo naplánováno první zasedání této pracovní skupiny. O problematice archivace elektronických dokumentů a některých aktivitách souvisejících s hledáním doporučovaných postupů již byli čtenáři Crypto-Worldu informováni ([1]). V rámci pracovní skupiny PKIX vznikl dokument rfc.3029 (experimentální) popisující protokol DVCS. V letošním roce byl také navržen nový protokol TAP - trusted archive protocol (draft-ietf-pkix-tap-00.txt). Již tehdy se objevily ale názory, že problematika archivace by se měla vydělit ze skupiny pkix, nesouvisí totiž zas až tak bezprostředně s problematikou digitálních certifikátů.

Na webu skupiny lze nalézt několik úvodních dokumentů. Kromě již zmíněných rfc.3029 a draftu protokolu TAP je zde především úvodní (iniciální) draft skupiny - draft-ietf-ltans-reqs-00.txt. Jeho obsahu bude věnována podstatná část tohoto článku.

Obraťme se však ještě k dalším dokumentům, které dnes lze na webovské stránce ltans nalézt. Projekt OpenEvidence (http://www.openevidence.org) měl v rámci 5.rámcového programu IST připravit technologie umožňující dlouhodobou platnost elektronických dokumentů, s využitím problematiky elektronických podpisů a časových razítek. Lze zde proto nalézt dva klíčové dokumenty k této problematice. Jednak to je prezentace Petera Sylvestera z července 2003 ze zasedání IETF ve Vídni, která informuje o průběhu a výsledcích úkolu a jednak to je rozsáhlejší dokument "Protocol and data formats for time-stamping service (září 2002) vzniklý ve spolupráci s estonskou firmou Cybernetica.

Dále lze na stránce nalézt dokument německých autorů "Archive Time-Stamps Syntax (ATS)", který je jedním z výsledků velice aktivně pracující skupiny v rámci projektu ArchiSig (http://www.archisig.de/index.html). Využitelnost jimi popisovaných konceptů je zkoumaná i v rámci praktických projektů (Heidelberg - universitní klinika a jiná zdravotnická zařízení a také v oblasti jurisdikce - dolní Sasko). Výsledkům práce této skupiny bude věnován článek v některém z příštích čísel CW.

Konečně lze zde také nalézt dokument českých autorů (Libor Dostálek, Marta Vohnoutová: Long Term Archive Architecture). K jeho obsahu se vrátíme v příštím čísle Crypto-Worldu.

2. Dokument Požadavky na službu dlouhodobé archivace (Long-term Archive Service Requirements)

Cílem dokumentu jakožto úvodního materiálu pracovní skupiny je dle autorů (Wallace, C.; Brandner, R. a Pordesch, U.) specifikovat technické požadavky, které souvisí s poskytováním služba dlouhodobé archivace podporující možnosti ubezpečovat se (a prokazovat) existenci a nenarušenost dat, speciálně digitálně podepsaných dat. Vzhledem k

tomu, že se jedná o úvodní verzi, lze samozřejmě předpokládat, že se objeví zásahy upravující některé části materiálu - předpokládá to i zveřejněný plán pracovní skupiny.

2.1. Úvodní poznámky

Potřeba dlouhodobě uchovávat digitální data jako průkazná materiál vzniká v rámci celé řada praktických situací. Často je zapotřebí, aby takováto archivace splňovala určité podmínky. Například důležitým může být hledisko bezpečnosti a trvalosti dat, může (při důkazním řízení) být nutné, aby zde byla možnost prokázat, že tato data existovala v určitém čase v minulosti a že nebyla od té doby změněna. Pokud za tímto účelem (podpis, časové razítko) byly použity kryptografické algoritmy je nezbytné dokázat, že podpis či časové razítko existovaly předtím než se použité kryptografické algoritmy staly slabými (Např. z hlediska délky použitého klíče) či dříve než příslušné certifikáty vypršely či byly odvolány.

Služba dlouhodobé archivace má mj. za úkol provádět takové aktivity, které umožní uchovat nepopiratelnost existence a nenarušenost dat a stejně tak i jejich dostupnost. Za tímto účelem je nutné použít celou řadu technických a operačních prostředků, které přesahují kryptografický rámec - média pro ukládání dat, plány pro případ živelných pohrom, změny technologií pro zpracování dat, legislativní požadavky atd.

Pro použití technologií digitálního podpisu a časového razítka je nezbytné vytvořit všechny předpoklady pro jejich dlouhodobou funkčnost (hledisko ověřování).

2.2. Použitá terminologie

Arbitrátor: osoba, která bude posuzovat různé autentizační aspekty (původ, nenarušenost, čas existence) archivovaných datových objektů
Archivovaný datový objekt: jednotka dat, která je archivována a která má nýt dlouhodobě uchována službou dlouhodobé archivace.
Balík archivu: soubor informací obsahující archivované datové objekty a s nimi asociovaný průkazní záznam.
Důkaz: Informace, kterou lze použít pro rozhodnutí sporu, který se vztahuje k různým autentizačním aspektům archivovaných datových objektů
Průkazní záznam Soubor důkazů, který byl v čase vytvořen k jednomu či více archivovaných datových objektů. Průkazná záznam může obsahovat časoví značky a další verifikační údaje jako certifikáty, revokační informace, důvěryhodný kořen, detaily politiky, informace o rolích atd.
Původce: Role (osoba nebo proces), která vytváří a možná i podepisuje datový objekt, který bude archivován. Původce nemusí být nezbytne tím, kdo vytváří či požaduje vytvoření průkazního záznamu k datům.
Časové razítko: Podepsané potvrzení generované autoritou časových razítek, které říká, že data existovala v určitém čase. Strukturu časových razítek a příslušných komunikačních protokolů popisuje rfc.3161.
Důvěryhodné archivování: Proces jehož obsahem je ukládání datových objektů na dlouhou dobu, přitom je zachována jejich integrita (nenarušenost), periodicky jsou generovány časová razítka a soubory důkazů podporující dlouhodobé uchování integrity dat.

Důvěryhodná archivační autorita: Služba, která odpovídá za uchování dat v dlouhých časových obdobích, obsahující vytváření a sběr důkazů, ukládání archivovaných datových objektů a důkazů. (= služba dlouhodobé archivace).
Uživatel: Role (osoba nebo proces), která předkládá datové objekty pro archivaci, vyžaduje přístup k balíkům archivu a ověřuje důkazy spojené s archivovanými datovými objekty použitím asociovaných průkazních záznamů, případně včetně ověření libovolného podpisu, který je připojen a samotnému archivovanému datovému objektu.

2.3 Scénáře aplikací

V řadě praktických situací se lze setkat s problémem jak uložit bezpečným způsobem elektronické dokumenty na nějakou často neurčitou dobu. Jedná se např. o digitální smlouvy, daňová přiznání nebo elektronické rodné listy. Často je také důležité prokázat, že tyto dokumenty existovaly v určitém čase v minulosti a že od té doby nebyly pozměněny.

V průběhu času však může docházet k tomu, že průkazní hodnota digitálních podpisů či časových razítek klesá či dokonce mizí a to z řady příčin:
- již není dostupná příslušná informace o revokacích (přestala pracovat odpovídající CA či protokol OCSP);
- nejsou dostupné certifikáty, které jsou zapotřebí pro verifikaci digitálního podpisu;
- certifikát asociovaný s digitálním podpisem vypršel či byl odvolán;
- vývoj kryptoanalytických či výpočetních technik již pokročil tak, že lze vnutit dokumenty či podpisy nebo spočítat utajované klíče.

Abychom se těmto problémům vyhnuli, je vhodné uchovávat spolu s dokumenty i příslušné průkazní záznamy (certifikáty, CRL, odpovědi OCSP a časové značky), periodicky obnovovat potřebné záznamy a přidávat další nezbytné informace - například nové časové značky používající silnější algoritmus.

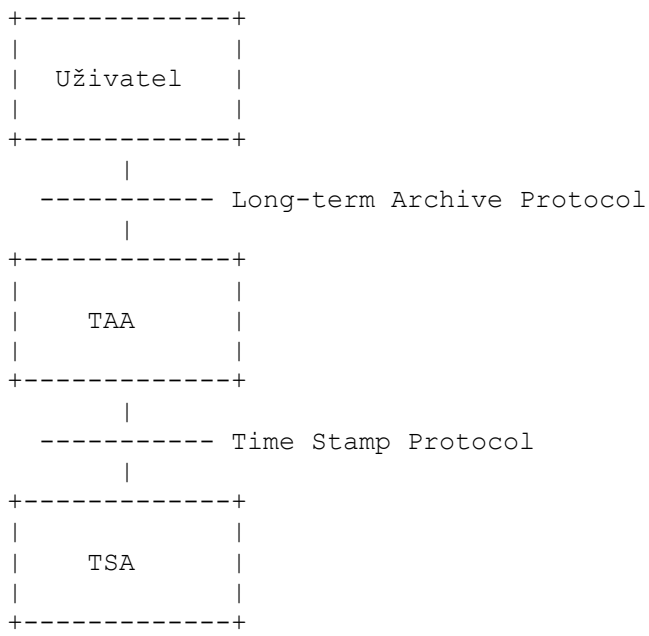
2.4 Služba dlouhodobé archivace

Služba dlouhodobé archivace je navržena tak, aby řešila podstatné části výše zmíněných problémů. Archivované datové objekty budou ukládány na dlouhá resp. nedefinovaná časová období a bude použita celá řada prostředků, které budou garantovat dostupnost těchto dat (plány obnovy, redundatní ukládání, havarijní plánování).

Služba poskytuje materiál nezbytný k prokazování existence a nenarušenosti dat a to jak ve vztahu k uživatelům, tak i ve vztahu k jurisdikci. Poskytuje prostředky pro uchování průkazních záznamů pro podepsané archivované datové objekty. Neřeší však všechny myslitelné problémy související s dlouhodobou verifikací digitálních podpisů - např. neposkytuje prostředky pro ověření podpisů, které jsou přímo součástí archivovaných datových objektů. Toto provádí ověřovací služby v rámci PKI jako SCVP či DVCS. Neposkytuje také prostředky, jak zahrnout ověřovací data do datových objektů. To zase by mělo být prováděno dle jiných specifikací (např. dle rfc.3029 a s ohledem na formát dokumentu).

Naopak služba dlouhodobé archivace poskytuje prostředky pro nepopiratelnost v dlouhém časovém období prostřednictvím periodického vytváření časových razítek.

Základní funkce služby dlouhodobé archivace jsou realizovány v několika instancích:



Uživatel převádí datové objekty, které by měly být archivovány důvěryhodnou archivní autoritou (Trusted Archive Authority - TAA) a používá k tomu aplikace dle svého výběru. Prostřednictvím protokolu služby dlouhodobé archivace a specifikací formátu dat balíku archivu pak uživatel může požadovat uložené datové objekty a asociované průkazní záznamy. TAA uloží dokumenty a získá k nim nezbytná ověřovací data (speciálně časová razítka prostřednictvím protokolu pro časová razítka - rfc.3161, resp. prostřednictvím jiných protokolů jako SCVP získá další ověřovací data). TAA může poskytovat služby TSA (autority časových značek), je zde však nezbytné určité rozlišení. Jako TAA může sloužit server uvnitř počítačové sítě organizace, který využívá lokální archivní servery nebo i vnější služby dosažitelné prostřednictvím Internetu.

2.5. Funkční a kvalitativní požadavky na službu dlouhodobé archivace

Služba dlouhodobé archivace musí poskytovat následující základní funkce:

- přijímat datové objekty či skupiny datových objektů pro jejich uchovávání;
- ukládat převzaté datové objekty pro dané časové období;
- vytvářet, ukládat a provozovat průkazní záznamy (např. prostřednictvím periodického získávání časových razítek) pro datové objekty, které byly převzaty pro uchování;
- sbírat a ukládat další ověřovací data nezbytná pro ověření průkazních záznamů;
- poskytovat balíky archivu obsahující archivovaná data, průkazní záznamy či oboje;
- poskytovat služby podle politiky dlouhodobé archivace;
- být schopna poskytovat archivní balíky i v případě, že se technologie pro ukládání či technologie pro zpracování změnily během života archivovaného datového objektu;
- být schopna poskytovat informace, že datový objekt existoval v určité době jako alternativu v situacích, kdy uživatel není schopen interpretovat průkazní záznamy;
- fungovat podle archivační politiky, která jako minimum stanoví kvalitu časových razítek a podmínky pro jejich obnovu, atd.

Služba dlouhodobé archivace musí být schopna efektivní činnosti i pro obrovská množství archivovaných datových objektů. Je proto třeba minimalizovat příslušné objemy činností (počty časových razítek, přístupy k archivovaných datovým objektům atd.).

2.6 Požadavky na strukturu archivovaných dat

Datová struktura balíku archivu má obsahovat archivovaný datový objekt a průkazní záznam.

Struktura průkazního záznamu by měla mít následující vlastnosti:
- musí být umožněno zahrnutí všech časových značek, které jsou nezbytné pro ověření existence archivovaného datového objektu;
- struktura časového razítka by měla umožnit efektivní poskytnutí důkazů mnoha archivovaných datových objektů;
- mělo by být umožněno poskytnutí důkazů pro skupiny archivovaných datových objektů;
-pokud jsou předloženy k archivaci skupiny datových objektů, musí důkaz nepopiratelnosti být dostupný i odděleně pro každý archivovaný datový objekt;
- odstranění některých archivovaných datových objektů nesmí vést k rizikům při důkazech pro jiná archivovaná data;
- musí být možné vytvořit časová razítka bez nutnosti přístupu k samotným archivovaným datovým objektům. Takováto nezbytnost přístupu k archivovaným datovým objektům může vzniknout pouze v případě, že jsou narušeny bezpečnostní vlastnosti použitého hashovacího algoritmu;
- všechny v čase použité hashovací algoritmy musí být identifikovány (v jednom místě), tak aby bylo umožněno jednorázové ověřování;
- další požadavky se týkají vytváření balíků obsahujících průkazní záznamy, zašifrovaných archivních datových objektů resp. zařazení dalších informací.

2.7. Požadavky vzhledem k protokolu pro interakci se službou dlouhodobé archivace

Tento odstavec dokumentu zvažuje nároky, které by měl splňovat protokol pro komunikaci se službou dlouhodobé archivace. Protokol musí logicky zabezpečit základní funkce služby jako jsou předkládání datových objektů k archivaci, přístup k balíkům archivu, odstraňování dat resp. průkazních záznamů z archivu. Musí také vyhovět některým bezpečnostním nárokům a umožnit i práci s průkazními záznamy, které vytvořila jiná TAA.

Literatura:

[1] J.Pinkava: Archivace elektronických dokumentů, Crypto-World 04/2002

[2] webovská stránka ltans: http://ltans.edelweb.fr/ .

[3] Long-term Archive Service Requirements – http://ltans.edelweb.fr/draft-ietf-ltans-reqs-00.txt

F. Unifikace procesů a normy v EU

RNDr.Jaroslav Hrubý,CSc. , hruby@gcucmp.cz

RNDr.Jaroslav Hrubý,CSc. je vědeckým pracovníkem FzÚ AV ČR a řešitelem grantu MŠTV v oblasti kvantového počítání. Je předsedou odborné skupiny kryptologie při matematické sekci JČMF (GCUCMP), a byl předsedou kryptologických konferencí PRAGOCRYPT 96 a EUROCRYPT'99. Je členem ISACA a IACR, kde v r.98-99 byl členem předsednictva, dále je členem FVS JČMF a EPS.

Abstrakt

V posledních letech se v mnoha společnostech ve světě prosazuje idea procesně řízené firmy, což klíčový způsobem prosazuje jejich konkurence schopnost. Tento vývoj je charakterizován jednak nutností integrace systémů ICT, dále nutností analýzy , optimalizace a integrace procesů ve společnosti a nakonec provázaným bezpečným sjednocením obou integrací. Integrace systémů ICT a integrace řízení procesů, služeb, projektů atd. ve společnosti musí být realizováno jak bezpečně, tak i kvalitně, a to v rámci platné legislativy a norem Evropské unie (EU). V této práci rozebíráme některé z norem, které podmiňují možnost realizace unifikace procesů v průniku s komplexní bezpečností. Realizace této vize může pomoci společnostem v ČR obstát ve vývoji elektronizace informatiky a řízení po vstupu ČR do EU. Je známo, že komplexní pojetí všech aspektů bezpečnosti ve společnosti se týká všech jejich procesů a řízení, a to představuje z matematického hlediska složitý matematický systém, který má díky rychlým změnám dynamický vývoj. V práci proto ukazujeme nutnost zavedení matematizace do procesní unifikace. Komplexní bezpečnost, která je jádrem procesní unifikace, musí garantovat neoddělitelnou provázanost bezpečnostních procesů se všemi ostatními procesy ve společnosti. Bez matematizace a kvantifikace komplexní bezpečnosti a řízení procesů, tj. zavedení metrik a aplikaci známých i nových matematických modelů na bezpečnostní i procesní data a veličiny, nelze složitý systém bezpečnosti v provázanosti na řízení společnosti hodnotit jako celek, a tedy procesy bezpečně, kvalitně a efektivně řídit, kontrolovat, modelovat a predikovat v reálném čase. V práci rovněž naznačujeme způsob, jakým je možné postupovat v procesní integraci a naplňovat tak vizi bezpečné, normy EU splňující a procesně řízené společnosti s využitím ICT, která stěžejním způsobem posiluje její schopnost konkurence v EU.

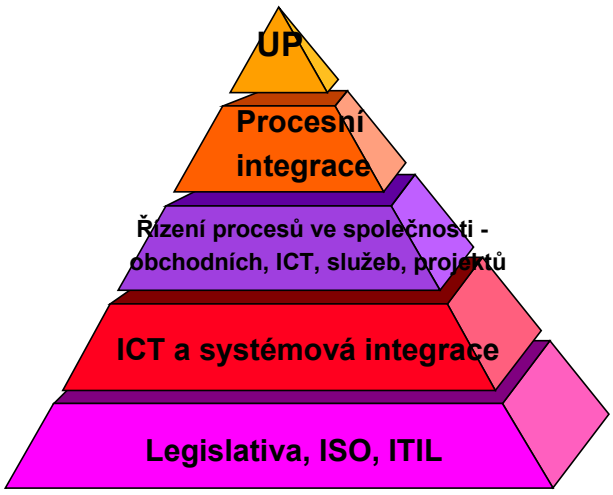
Úvod

V poslední době je možné ve světě zaznamenat zřetelný přechod ve společnostech , které využívají pro své vlastní řízení a řízení poskytovaných služeb informační technologie a systémy (IT/IS), včetně jejich vzájemné komunikace (ICT), od systémové integrace k procesní integraci, a to na bázi systémově integrovaného ICT. Lze hovořit o unifikaci procesní a systémové integrace.

Vstupem ČR do EU v r.2004 se bude řada společností i u nás snažit o unifikaci procesů (UP) na bázi legislativy ČR a EU s využitím platných norem pro ICT. Struktura vedoucí k UP ve společnosti může být znázorněna následovně:

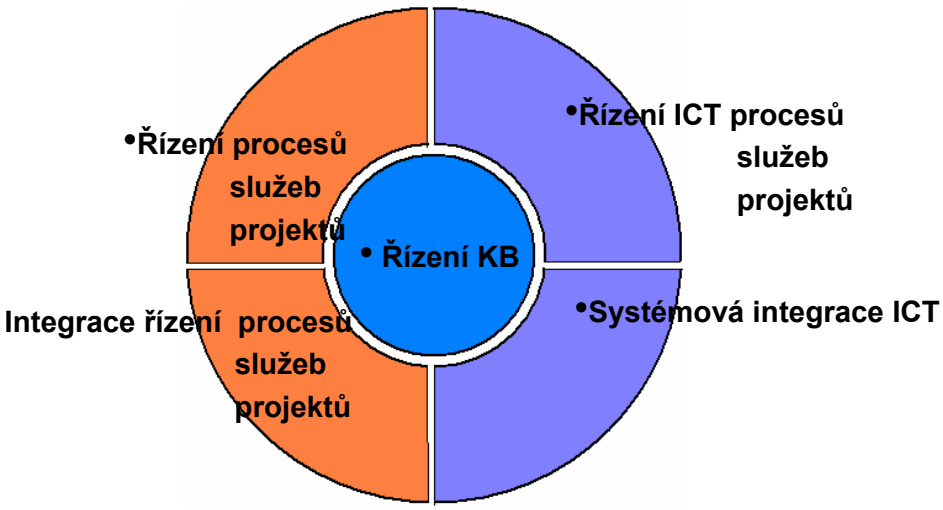
Vstupem ČR do EU v r.2004 se bude řada společností i u nás snažit o unifikaci procesů (UP) na bázi legislativy ČR a EU s využitím platných norem pro ICT. Struktura vedoucí k UP ve společnosti může být znázorněna tak, jak je uvedeno na obrázku č.1.

Hierarchie vedoucí k UP ve společnosti



Obrázek č.1

Unifikace procesů (UP)



Obrázek č.2

V současnosti je bezpečnost nedílnou součástí obchodování. Úspěšné řešení BPR (Business Process Reengineering), ERP (Enterprice Resource Planning) a CRM (Customer Relationship Managment) ve společnosti musí vycházet z unifikovaných procesů, pro které je garantována komplexní bezpečnost (KB) a její aktuální znalost ve společnosti. To vše musí stát na základě platné legislativy ČR , ISO norem a knihovny infrastruktury informačních technologií ITIL. Řízení KB je jádrem procesní integrace i UP a provazuje procesní a systémovou integraci i řízení procesů – viz obrázek č.2.

Stanovení míry bezpečnosti a bezpečnostních rizik je nedílnou součástí informační , a tedy i KB . Samotné stanovení KB u každé společnosti závislé na ICT, není možné bez znalosti bezpečnostních procesů a jejich provázanosti se všemi ostatními manažerskými procesy v této společnosti.

Pro aktuální znalost a říditelnost procesů v reálném čase je zapotřebí stanovit měřitelnost , kvantifikaci a realizovat matematizaci KB v provázanosti s bezpečnostními procesy. Dále je nutná její provázanost s ostatními řídícimi procesy ve společnosti, tak aby tato mohla být efektivně řízena nástroji ICT. Proto je zároveň nezbytné stanovit měřitelnost , kvantifikaci a realizovat matematizaci všech řídících procesů společnosti jako provázaného celku s KB.

Toto je vize nezbytná pro realizaci e-managmentu a e-administrativy, které by se měla v daném časovém horizontu blížit každá společnost v ČR, jenž chce obstát ve vývoji elektronizace informatiky a řízení společnosti v Evropské unii (EU).

Samotná realizace e-administrativy a e-managmentu však vyžaduje od společnosti , aby zvolila specifickou optimální cestu pro dosažení tohoto cíle, a to z hlediska vyváženosti vynaložených nákladů na získání zvýšené kontroly, účinnějšího řízení a bezpečnosti ve společnosti.

Specifická optimální cesta k tomuto cíli by mohla právě začít analýzou KB ve společnosti a s ní souvisejících bezpečnostních procesů a jejich provázaností na procesy ostatní, a to dle platných norem v EU, týkajících se této oblasti. Je to nejenom proto, že tímto zmapováním získáme přehled o stavu všech ostatních procesů, ale především proto, že konsolidací KB v prvé řadě zabráníme ztrátám, které způsobuje realizace hrozeb na aktiva společnosti. Proto se v tomto článku zaměříme na tuto oblast.

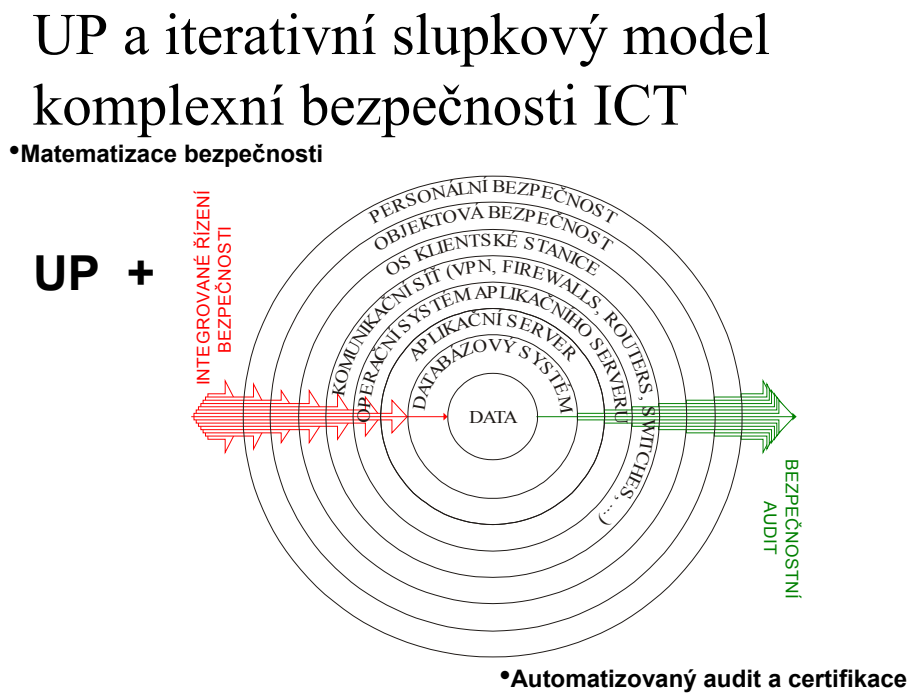
V práci [1] je rozebrána potřeba matematizace a kvantifikace KB, včetně použití nových technologií a bezpečnostních manažerských systémů řízení pro predikci vývoje KB a i pro predikci nových rizik v globálním světě.

Je v ní ukázáno, že bezpečnost společnosti se stává jedním z jejích nejvýznamnějších aktiv, a že informační bezpečnost je nedílnou součástí KB každé společnosti v informačním světě a je rovněž součástí všech jejich aktiv. To platí jak pro komerční společnost, státní orgán i společnost jako celek. Představme si pro konkrétnost komerční společnost s rozvinutým ICT, na kterém je závislá většina jejich aktiv.

Dokonalou ochranu informační bezpečnosti v této společnosti lze dosáhnout pouze jejím nerozdělitelným vnořením do KB a provázáním všech řídících procesů ve společnosti s bezpečnostními procesy. Hovoříme o nezbytnosti unifikace procesů ve společnosti a řízení informačních rizik (obrázek č.3).

KB spojuje korporátní a informační bezpečnosti ve společnosti, což znamená, že korporátní bezpečnost organizace prolíná informační bezpečnost v řadě jejich oblastí a naopak. KB ve společnosti je realizována bezpečnostními procesy, unifikovanými se všemi ostatními procesy ve společnosti, bezpečnostní politikou a bezpečnostní strategií KB, která musí být integrovaně řízena a auditovatelná.

Pro názornost integrovaného řízení KB si představme slupkový model bezpečnostních vrstev, chránící ve svém jádře data, který musí být v průniku s UP. Informace obsažená v datech je chráněna vrstvami bezpečnostních mechanismů, týkající se předpisů, personalistiky, budov, klientských stanic, komunikační sítě, operačních systému aplikačních serverů, databázového systému, ale také naopak - bezpečnostní informace o budovách, lidech, počítačích, sítích , změnových řízeních atd. jsou součástí jejich ochrany .



Slupkový model je inverzní v tom smyslu, že i informace obsažená v datech chrání osoby, budovy, a také informační technologie a systémy.

Bezpečnost ICT je tudíž od korporátní bezpečnosti neoddělitelná a průnikem do všech řídících procesů ve společnosti se stává jejich vazebním činitelem pro unifikaci všech procesů ve společnosti a základem pro realizaci e-administrativy a e-managmentu .

Takto komplexně provázané bezpečnosti ICT, korporátní, personální, fyzické atd. včetně bezpečnostních procesů a jejich provázanosti do všech procesů společnosti chápeme jako jednu KB společnosti.

Je zřejmé, že tato KB je z matematického hlediska složitý dynamický systém sám o sobě, který je v průniku všech částí, činností a existence celé společnosti, složité popsat. Pokud se vedení společnosti pokouší nějakými metodami, např. ekonomickými modely, ekonometrií apod. řídit celou společnost z hlediska ekonomického růstu a nárustu aktiv, mělo by umět mapovat, popsat , řídit a předpovídat vývoj tohoto ústředního aktiva – KB, který všechna ostatní aktiva chrání.

Tento problém je o to složitější, že ICT prorůstá téměř do každé činnosti společnosti, že rychlost změn v tomto prorůstání uvnitř společnosti je značná, ale i změny ve vývoji ICT jsou dynamické – KB společnosti není tedy stacionární komplexní systém, ale systém nesmírně dynamický, tj. s vysokým gradientem změn v čase.

Vzhledem k dynamickému rozvoji hlavně v oblasti ICT a oboru informační bezpečnosti a kryptologie, je nezbytné se vstupem ČR do EU, aby správa ICT bezpečnosti a všech procesů byla v souladu s KB společnosti a dále se sérií základních mezinárodních dokumentů vydaných v sérii ISO/IEC [2], platných u nás i v EU, a to takovým způsobem, aby:

- bezpečnostní opatření byla komplexní a dostatečně rychle implementována,
- systém správy komplexní a ICT bezpečnosti byl měřitelný a řiditelný v reálném čase, a také otevřený pro jakékoliv budoucí změny,
- systém správy KB včetně ICT bezpečnosti plně akceptoval zákony v ČR, normy a direktivy EU týkající se této oblasti [3],
- v maximální míře využil stávajících systémů a procesů v organizaci tak, aby bezpečnostní procesy byly provázané se všemi ostatními a aby realizace bezpečnosti a unifikace s ostatními procesy byla v optimalizovaném poměru mezi finančními náklady a výsledkem dosažené bezpečnostní úrovně,
- aby úroveň bezpečnostních procesů bylo možno jednoznačně hodnotit v reálném čase, včetně jejich historie.

Cílem je dosáhnout stabilní vysokou úroveň KB ve společnosti s minimální hodnotou míry rizika pro aplikace, jako plánování zdrojů a celý e-management a e-administrativu ve společnosti, dále řízení vztahů se zákazníky, on-line bankovnictví, účetnictví atd.

Cesta k tomuto cíli vede pouze přes matematizaci a kvantifikaci KB (v návaznosti na matematizaci a kvantifikaci ostatních procesů ve společnosti, které jsou s bezpečnostními procesy provázány) , včetně aplikace modelů popisujících dynamiku systému a jeho vývoj od regulárního chování k chaotickému, jako je např. na nelineárním modelovém příkladu uvedeno v práci [4].

V tomto článku se pokusíme nastínit klíčovou úlohu mezinárodních norem a hlavně norem EU pro bezpečnostní procesy spojené s ICT, dále jejich důležitost pro ostatní procesy ve společnosti a její celkové řízení. Ve 2.kapitole uvedeme o jaké normy se jedná , budeme je stručně charakterizovat a zmíníme také, na co jsou jednotlivé normy zaměřeny i jejich klíčové součásti. Ve 3.kapitole ukážeme jejich význam pro aplikaci na KB ve společnosti, unifikaci a matematizaci procesů řízení bezpečnosti, která může být použita i pro ostatní řídící procesy.

Stručný přehled některých norem týkajících se bezpečnosti ICT

V tomto přehledu se zmíníme o následujících normách a dokumentech, týkajících se bezpečnosti ICT:

- ISO/IEC 17799, ISO/IEC TR 13335, ISO/TR TC68,ISO/IEC 15408, CobiT.

V první řadě musí KB v ICT garantovat maximální míru přijetí a zapracování platných mezinárodních norem série ISO/IEC.

Tzv. „Code of practice“ pro řízení bezpečnosti ISO/IEC 17799 poskytuje prostředky pro změření a porovnání ICT procesů s procesy používajícími nejlepší postupy s cílem zlepšit výkon v dané společnosti. Norma pokrývá všechny aspekty bezpečnosti ICT, vysvětluje jejich základní pojmy, důvody jejich zavedení a postupy pro jejich zajištění. Definuje dále základní kontroly, nutné pro dosažení statutu nejlepších postupů rozdělené do následujících tříd:
bezpečnostní politika, organizační bezpečnost, klasifikace a řízení aktiv, personální, bezpečnost, fyzická bezpečnost a bezpečnost prostředí , komunikační a operační managment, řízení přístupu, vývoj a správa systémů, managment kontinuity obchodní činnosti a zajištění shody.

Série norem ISO/IECTR 13335, týkajících se správy informační bezpečnosti a technické normalizace, včetně rozšířeného pohledu na bezpečnost, poskytuje především návod pro řešení, ne však přímo řešení manažerských aspektů bezpečnosti.

Mezinárodní normy vytváří komise specialistů z ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), sdružených v

technické komisi ISO/IEC JTC I/SC 27, která připravila sérii pěti vzájemně navazujících dokumentů ve formě technické zprávy (TR):

- ISO/IEC TR 13335-1 Koncepce a modely informačních technologií
- ISO/IEC TR 13335-2 Správa a plánování bezpečnostních informačních technologií
- ISO/IEC TR 13335- 3 Techniky pro správu bezpečnostních informačních technologií
- ISO/IEC PRF TR 13335- 4 Výběr bezpečnostních opatření
- ISO/IEC CD TR 13335- 5 Bezpečnostní opatření pro vnější připojení.

Na výběr bezpečnostních opatření navazuje směrnice ISO/TR TC68, týkající se informační bezpečnosti v bankovnictví a souvisejících finančních službách [5]. Ta je určena jak finančním ústavům všech velikostí a typů, jejichž záměrem je využít obezřetný a komerčně rozumný program informační bezpečnosti, tak i organizacím poskytujícím služby finančním ústavům.

Vycházíme z předpokladu, že v organizacích a společnostech je v ČR vše v souladu s platnými zákony a normami dle [2]. Bezpečnostní audity a doporučení, které se většinou soustředí na oblast bezpečnosti ICT (méně již na korporátní celkovou bezpečnost a ještě méně na jejich průnik, tj. celkovou bezpečnost všech aktiv a procesů ve společnosti , a tedy nejenom informačních aktiv a procesů) jsou však pouze subjektivní, pokud nevychází z jednotné kvantitativní metriky pro hodnocení aktiv , rizik a hrozeb, působících na tato aktiva ve společnosti.

Taková jednotná metrika v ČR není a proto se jedná o pouhou „dojmologii“ hodnotitelů (auditorů), kteří hodnotí soulad, či nesoulad stavu se zákony, předpisy a normami, pouze ze svého subjektivního hlediska, pokud to co posuzují nebylo kvantifikováno podle jednotného měřítka. Pro kvantifikaci je nezbytná znalost všech hodnotitelů, kteří doplňují informace do bezpečnostní databáze, jak bezpečnostní informace hodnotit a jak měřit . Pro hodnocení KB v dané společnosti je tedy nezbytná jednotná metrika, která by měla být v souladu s metrikou EU.

Proto vyvstává jednoznačná potřeba aplikovat metriku EU pro národní prostředí, a to ve státní i v komerční sféře, aby nezávislí hodnotitelé docházeli alespoň v limitním případě ke shodnému výsledku.

Sjednocení pohledu na hodnocení je také hlavní požadavek kritérií pro hodnocení bezpečnosti v informačních technologií (ITSEC)[6] a metodologie hodnocení (ITSEM) [7] v US , jejichž analogem v EU je ISO/IEC 15408 . Norma ISO/IEC 15408 prezentuje dvě hlavní kategorie bezpečnostních požadavků : funkcionalitu a zaručitelnost, že vývoj a užití dané ICT aplikace splňuje danou úroveň bezpečnosti.

Bezpečnostní požadavky na funkcionalitu jsou děleny na 11 tříd, přičemž každá z nich obsahuje “rodiny” se specifickými bezpečnostními cíli a požadovaným bezpečnostním chováním. Těchto 11 tříd se týká následujícího: bezpečnostního auditu , identifikace a autentizace, využití zdrojů, kryptografické podpory, řízení bezpečnosti, kontroly přístupu, komunikací, zachování informačního soukromí , důvěryhodnosti spojení a komunikačních kanálů, ochrany dat uživatele a ochrany bezpečnostních funkcí.

Požadavky zaručitelnosti jsou založeny jak na otázce důvěrnosti při zavedení bezpečnostních funkcí, tak i na jejich účinnosti. Požadavků zaručitelnosti je 8 a týkají se: řízení konfigurace, předpisové základny, hodnocení narušitelnosti, dodávky a provozu, podpory životního cyklu systému, zajištění údržby, vývoje a testování. Výpočet úrovně bezpečnosti (EAL) je dán předdefinovanými skupinami výše zmíněných požadavků zaručitelnosti. Každá úroveň bezpečnosti má zvýšený potenciál bezpečnosti a indikuje stupeň důvěryhodnosti systému.

Nejnižší úroveň EAL 1 indikuje, že systém byl pouze funkcionálně testován, zatímco nejvyšší úroveň EAL 7 indikuje, že systém byl maximálně testován na funkcionalitu a zaručitelnost a i jeho návrh byl důvěryhodně ověřen a chráněn.

Další mezinárodní normou je tzv.COBIT [8] (Control Objectives for Information an related technology). Tato norma není normou ISO/IEC, ale je určujícím řádem pro kontrolu a audit ICT v obchodních aplikacích.

COBIT popisuje rozsah informačních kriterií pro vývoj celkového bezpečnostního programu a pro veškeré informace v obchodních aplikacích. Obsahuje 34 procesů rozdělených do čtyř skupin:
plánování a organizace, osvojení a provedení, dodání a podpora, monitorování.

Procesy jsou dále děleny na dalších 318 specifických kontrolních cílů a s nimi spojených auditních postupů. COBIT takto vytváří základ pro bezpečnostní praktiky, které spojují bezpečnostní cíle, kontroly a procedury.

ITSM , unifikace a matematizace procesů řízení a bezpečnosti

V současné době některé společnosti prezentují IT Service Management (ITSM) , použitelný v libovolném ICT prostředí v každé společnosti. Model správy služeb v sobě zahrnuje většinu osvědčených postupů z ITIL (IT Infrastructure Library), jejíž hlavním cílem je zlepšení kvality služeb v oblasti IT. Nicméně řízení ITSM služeb bez unifikace procesů a jejich řízení a kontrolu v reálném čase nedává managmentu společnosti dostatečně úplný nástroj pro klíčové rozhodování, predikci a zpětnou vazbu pro možnost případné bezpečné a kvalitní realizace změn.

Samotné ITSM, musí být vždy unifikovaný s bezpečnostními normami uvedenými ve 3. kapitole a zároveň i splňovat ISO 9000. Je nutné přitom použít osvědčený následující postup:

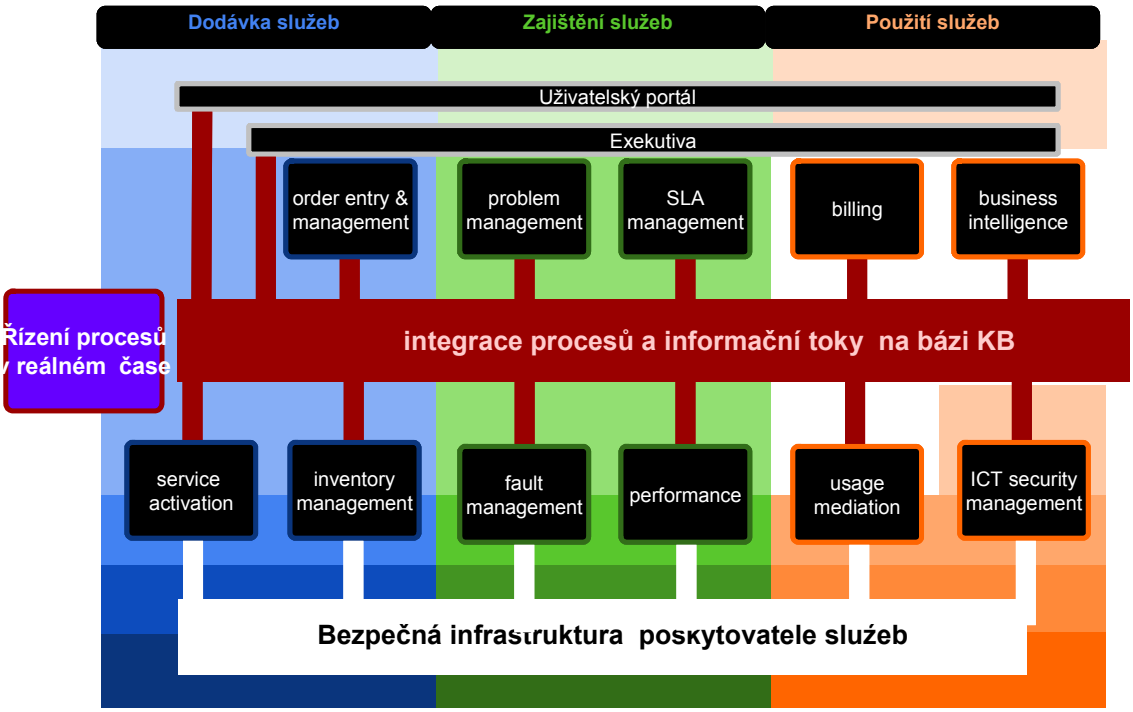
- Tvorba plánu řízení procesu v unifikaci a integraci s ostatními procesy ve společnosti , v provázanosti s bezpečnostními procesy KB, legislativou a normami platnými v ČR.
- Matematizaci a kvantitativní i kvalitativní vyhodnocení procesu s cílem jeho optimalizace.
- Realizace optimalizace procesu na základě modelování jeho vstupů a výstupů, dále vazbami s jinými procesy, unifikace a integrace s ostatními procesy, definice požadavků na změnu metrik apod.
- Sledování výkonu procesu v reálném čase a kontinuální provádění optimalizace procesu při jakýchkoliv vnějších změnách.
- Identifikace příležitostí pro zlepšení procesu vynucená na základě vnějších změn a vazeb působících na proces, predikce vývoje procesu na základě historie dat o procesu a aplikace modelů.
- Na základě modelového ověření příprava a realizace kroků pro zlepšení procesu.

Každá společnost by si měla vytvořit jednoznačné postupy, jak měřit a hodnotit, podobně jako je tomu v přírodních a technických vědách, včetně implementace norem pro měření na všechny oblasti KB a řízení procesů. To se zatím v ČR běžně nerealizuje a zde je optimální příležitost využít spolupráce akademické obce, státních orgánů , ale také komerční sféry pro vytvoření těchto metrik a postupů ve shodě s legislativou ČR a tím, co je již v EU akceptováno.

Je nezbytné realizovat matematizaci hodnocení a řízení procesů bezpečnosti v provázanosti na ostatní procesy řízení, a to v celé společnosti, počínaje globální bezpečnostní

politikou, analýzou rizik, návrhem bezpečnostních opatření, bezpečnostní politikou pro ICT, a to až do bezpečnostního projektu a implementaci ITSM, všech opatření do jednotlivých činností a provozu ve společnosti, včetně vzdělávání ITSM/ITIL, integrace ISM (Integrated Service Management) a nakonec realizovat UP a řízení procesů ve společnosti v reálném čase na bázi KB, což lze jako vizi znázornit následovně:

Řízení procesů v reálném čase a architektura UP na bázi KB



Řízení KB a jejich procesů, s čímž se obvykle začíná jako se základem, by mělo být na stejné úrovni jako celkové ekonomické řízení společnosti, a to právě z důvodu průniku KB do všech ekonomických aktivit společnosti. O matematickém modelování, ekonometrii v oblasti ekonomického řízení nikdo nepochybuje a má i v ČR dobrou tradici a úroveň. V oblasti KB je situace na mnohonásobně nižší úrovni a mnohdy je hrubě podceněna. Proto každá společnost by měla věnovat bezpečnostnímu programu mimořádnou pozornost, provazovat jej s procesním řízením společnosti, realizovat kvantifikaci a matematizaci všech procesů z důvodu možnosti jejich řízení, kontroly a modelování v reálném čase a uplatňovat v něm poslední výsledky výzkumu v dané oblasti.

Bylo zmíněno, že KB i procesní řízení společnosti jsou z matematického hlediska stejně složitým systémem, jako např. ekonomie s řadou skrytých parametrů, nahodilostí atd., a že je nezbytné stanovit měřitelnost , kvantifikaci a realizovat matematizaci všech řídících procesů společnosti jako provázaného celku s KB.

Co se rozumí pojmem matematizace, si podrobněji rozebereme na matematizaci procesů KB a analogicky tomu je i u ostatních procesů ve společnosti. Pojmem matematizace KB a bezpečnostních procesů se zde nerozumí pouze to, co se jí běžně rozumí ve velmi kvalitní metodice analýzy rizik , ale na universální úrovni následující:

- výběr vhodných metodik pro dotazníkové metody pokrývající celou problematiku KB a procesů a výběr
- vhodných technických detektorů bezpečnostních dat a informací , týkajících se dané oblasti.

- škálování otázek v dotazníkových metodách pro různé bezpečnostní úrovně EAL požadované na ICT, včetně škálování množství a požadavků na technické prostředky získávající bezpečnostní informace
- aplikovaní matematických statistických metod na tato hodnocení, za účelem prověření věrohodnosti získaných bezpečnostních informací a korelací mezi odpověďmi a hodnoceními různých dotazovaných subjektů v průniku s informacemi získanými z technických prostředků (z měřičů průniku do sítě, z firewalů apod.)
- modelování funkce míry rizika f(a,h,z), která je pro každou oblast specifická a je funkcí aktiv(a), hrozeb (h) a zranitelnosti (z).
- matematický výpočet dopadu hrozby, vypočíst expozici pro každé riziko (tj. f(p,d), kde p je pravděpodobnost, že incident nastane v dané časové periodě a d je poškození), profit atd.
- výběr dat bezpečnostní databáze, která mají časový vývoj, sestavení časových řad, včetně aplikace modelů predikujících jejich dynamiku a vývoj, predikce vývoje bezpečnosti a predikce nových rizik
- aplikaci manažerských bezpečnostních systémů na bezpečnostní databázi, včetně modelovacího a kontrolního software
- matematické modelování různých strategií při vzniku havárií, použitím optimalizace metod, aplikace různých matematických modelů (např. chaosu, neuronových sítí, teorie her apod.)

Je zřejmé, že tento výčet není úplný a že lze aplikovat ještě další řadu známých vědeckých metod pro zkoumání složitých dynamických systémů, i na KB a bezpečnostní procesy.

Aby matematické zpracování bezpečnostních dat bylo efektivní, je nutné mít kvalitní bezpečnostní i celkovou databázi společnosti, přičemž pro jejich vytvoření je nutné vytvořit společná měřítka a kriteria, jako např. :

- jak unifikovaně bodově hodnotit proměnné a,h,z,
- jak škálovat dotazy (na procesy, služby, řízení apod.) a požadavky pro technické detektory bezpečnostních dat pro různé kategorie bezpečnostní úrovně (např.pro bezpečnostní úrovně EAL dle ISO 15408),
- jak volit funkce f(a,h,z) např. pro banky, telekomunikační společnosti, energetické společnosti, různé oblasti státní správy apod.
- jakými matematickými a bezpečnostními modely popisovat samotné bezpečnostní procesy a jejich vazby na ostatní procesy pro danou společnost při požadované bezpečnostní úrovni atd..

Kvantifikace hodnocení KB a bezpečnostních procesů umožňuje vytvořit databázi s časovým vývojem,nad kterou fungují matematické modely, bezpečnostní modely a řídící systémy, tedy to co se nazývá matematizací bezpečnosti.

Jedině takto lze konstruovat výše zmíněný kvantitativní nástroj, který v průniku s kvalitativní hodnocením umožňuje kvalitní manažerská rozhodnutí, chránící všechna aktiva společnosti vůči téměř všem hrozbám. Zároveň je to jediná cesta k efektivnímu a bezpečnému řízení společnosti nástroji ICT v reálném čase, což je vizí všech manažerů.

Slovo téměř je zde podstatné, protože tak, jako neexistuje absolutní bezpečnost (a vrcholem veškerého bezpečnostního snažení je se ji v nějaké rozumné limitě přiblížit), tak principiálně nelze předpovídat všechny možné hrozby v delším časovém horizontu, popřípadě rozkrýt všechny skryté parametry, které mohou mít na řízení procesů vliv.

V kratším časovém horizontu je predikce možná, a to s vysokou pravděpodobností výskytu nové hrozby.

Bezpečnostní databází se zde rozumí multidimensionální datový sklad věrohodných bezpečnostních, informací (transformovaných na data), získaných netechnickými dotazníkovými metodami na úroveň procesů ICT infrastruktury ve společnosti v provázanosti na KB dle platných norem a legislativy. Tyto jsou doplněny informacemi z technických prostředků jako např. měřičů průniku, manažerských bezpečnostních systémů pro dohled nad sítí, detektorů garantujících objektovou a personální bezpečnost, atd. až po data ze zpravodajských prostředků.Tato data jsou řazena do časových řad pro podchycení dynamiky změn KB.

Takto by měla vypadat i celková databáze společnosti, přičemž obě databáze mohou být odděleny a z té bezpečnostní pouze nezbytné informace eskalovány do celkové databáze společnosti.

Věrohodnost dat je nezbytné zajistit aplikací metod matematické statistiky a studiem korelací mezi jednotlivými informacemi s následným vyloučením informací nevěrohodných.

Závěr

V tomto článku jsme se snažili ukázat na nezbytnost komplexnosti pohledu na aplikaci bezpečnostních procesů a norem v EU, v provázanosti na ostatní procesy jejich integraci, unifikaci a potřebě jejich kvalitativního i kvantitativního hodnocení a matematizaci.
Kvantitativní hodnocení procesu, matematizace procesu a manažérské bezpečnostní systémy řídící bezpečnost v reálném čase se jeví v současnosti jako jediný způsob, jak efektivně chránit s minimálními náklady klíčové aktiva společnosti a jak realizovat aplikaci bezpečnostních procesů a norem při vstupu ČR do EU v r.2004.

Tato tématika je vysoce aktuální v době probíhající privatizace společností v ČR a s tím souvisejících rizik s doprovodným jevem propouštění zaměstnanců, a také při privatizaci možnosti dosažení vyšší tržní ceny společnosti. Ve společnosti , kde unifikace procesů chybí může docházet k řadě ztrát, které nejsou vůbec detekovány a zůstávají skryty v nákladech na vytváření příjmů společnosti. To samozřejmě snižuje zisk společnosti. Většina společností ve světě, která investovala do řízení procesů a bezpečnosti, snížením svých ztrát a zefektivněním činnosti, zaznamenala vysokou návratnost této investice. Přitom na zvýšení zisku se nepodílelo pouze snížení ztrát z ICT zločinnosti, která je ve světě u společností značná [8], ale zároveň snížením ztrát plynoucích z neefektivního řízení. Podle Gartner Group pokud organizace správně používá procesní model pro odpovídající procesy, její náklady na správu mohou být redukovány nejméně o čtvrtinu.

Problematika unifikovaného hodnocení je v současnosti také aktuální proto, že v ČR dochází k realizaci používání zákona o elektronickém podpisu č. 227/2000 Sb. a vyhlášky k tomuto zákonu , která otevírá cestu pro akreditaci certifikačních autorit (CA) , dále k budování CA pro komerční využití a k realizaci zavádění infrastruktury s veřejnými klíči (PKI), a to nejrůznějšími aplikacemi nad touto infrastrukturou (PKA), včetně budování e-všechno. Proto každá společnost by měla provést optimální výběr z hlediska nákladů na způsob pro efektivní řízení společnosti konkrétními nástroji a postupy v ICT, a to na bázi toho co je ve společnosti již realizováno.

Nezbývá než doufat, že unifikace procesů ve společnostech v ČR po jejím vstupu do EU nezůstane pouze vizí, ale bude se prakticky realizovat.

Literatura:

[1] J.Hrubý, O kvantifikaci a matematizaci bezpečnosti, Sborník konf."Informačmí společnost",prosinec 2001,ISBN 80-86433-07-2
[2] Série norem ISO/IEC TR 13335 vydávané od r.1996.ISO/IEC 17799 (Code of Practice for Information Security Managment), www.ansi.org, www.iso.org, www.securityauditor.net. Dále normy ISO/IEC 15408 pro hodnocení bezpečnosti IT, atd.
[3] Zákon č.101/2000 Sb. o ochraně osobních údajů, zákon č 148/1998 Sb. o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů. Vyhláška NBÚ 79/1999 Sb. o zajištění kryptografické ochrany utajovaných skutečností, provádění certifikace kryptografických prostředků a náležitostech certifikátu, zákon č.227/2000 Sb. o elektronickém podpisu, státní informační politika, schválená usnesením vlády ČR ze dne 31. Května 1999 č.525 a standardy státního informačního systému ČR vydanými tehdejším USIS (dnes viz. MI ČR), předpisy upravujícími výstavbu informačních systémů v EU (Schengenská dohoda), obchodní zákon, telekomunikační zákon atd.
[4] J.Hrubý, Matematizace komplexní bezpečnosti a Lorentzův model, Sborník přednášek Vel, kryptologie, duben 2002,ISBN 80-903083-1-7.
[5] ISO/TR 13569, Banking, securities and other financial services – Information security quidleines (1997,1998).
[6] ITSEC, Kritéria pro hodnocení bezpečnosti v informačních technologiích (1990).ITSEM, Příručka pro hodnocení IT bezpečnosti (1992), csrc.nist.gov/cc . ISO/IEC15408-1, Evaluation Criteria for IT Security (1999)
[7] Control Objectives for Information and related Technology (COBIT) 3rd Edition, www.isaca.org/cobit.htm
[8] 2002 Computer Crime and Security Survey, Computer Security ISSUE&Trends vol.VIII,n.1 (spring2002)

G. Letem šifrovým světem
(připravil Pavel Vondruška)

I. Vláda schválila novelu zákona o elektronickém podpisu

datum:05.11.2003

Na svém dnešním jednání vláda schválila Ministerstvem informatiky předkládanou novelu zákona o elektronickém podpisu. Novela harmonizuje právní úpravu elektronického podpisu s legislativou Evropské unie a zavádí do českého právního řádu dva nové instituty, takzvané časové razítko a elektronickou značku. Novela v budoucnu umožní získávat elektronické veřejné listiny, například výpisy z katastrů a rejstříků, dálkově a automaticky, bez zásahu úředníka.

II. Přednášky z informační bezpečnosti IS na MFF UK

Přednášky z informační bezpečnosti *„Bezpečnost IS v praxi"* pod vedením dr.A.Beneše a dr.V.Jákla byly v tomto semestru již zahájeny.

Zveme opět všechny příznivce o tuto problematiku (nemusí se jednat pouze o studenty MFF UK, ale i o studenty z jiných VŠ a případně i středních škol a samozřejmě i pracovníky

informační bezpečnosti z praxe). Přednášky se konají každé pondělí od 19.00 hod na KSI (Katedra systémového inženýrství) MFF UK na Malé Straně ve 3.poschodí v učebně S4.

III. Nová RFC pro PKI

Začátkem listopadu byly publikovány dva důležité dokumenty v řadě de-facto standardů RFC. První se zabývá strukturou a obsahem Certifikační politiky a Certifikační prováděcí směrnice. Nahrazuje známé RFC 2527, které je např. doporučováno ve výkladu prováděcí vyhlášky k elektronickému podpisu č.366/2001 Sb. pro vytváření dokumentace poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty.

Druhý dokument se zabývá politikou poskytovatelů, kteří vydávají časová razítka.

RFC 3647
Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework
Velikost : 233 kB
Datum: listopad 2003
Kategorie : Informational
Autor: S. Chokhani (Orion Security Solutions, Inc.), W. Ford (VeriSign, Inc.), R. Sabett (Cooley Godward LLP), C. Merrill (McCarter & English, LLP), S. Wu (Infoliance, Inc.)
Počet stran: 94
URL: ftp://ftp.rfc-editor.org/in-notes/rfc3647.txt

RFC 3628
Policy Requirements for Time-Stamping Authorities (TSAs)
Velikost : 95 kB
Datum: listopad 2003
Kategorie : Informational
Autor: D. Pinkas, Bull, N. Pope, J. Ross
Počet stran: 43
URL: ftp://ftp.rfc-editor.org/in-notes/rfc3628.txt

IV. Normální je fakturovat elektronicky

Pod tímto heslem se skrývá aktivita SPIS pro podporu elektronické fakturace. Současná legislativa použití elektronických faktur dovoluje, stanovisko ministerstva financí je k jejímu používání kladné a denně jsou i v České republice vytvářeny a přijímány stovky elektronických faktur. Cílem projektu je sjednocení pravidel elektronické fakturace a následné prosazení a rozšíření používání elektronické faktury jako plnohodnotného daňového dokladu.

Výsledky pracovní skupiny (které jsem členem) budou za účasti ministra informatiky V.Mlynáře předloženy veřejnosti na konferenci 26.11.2003. Setkání se bude konat od 14.00 hod v Kaisersteinském paláci na Malostranském náměstí. Účast na setkání je zdarma, vzhledem k omezenému počtu míst se musí zájemci předem přihlásit. Zájemci najdou další podrobnosti a registrační formulář na http://www.spis.cz/spis/SPIS.home .

V. O čem jsme psali v listopadu 1999 - 2002

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 na e-mail pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu !). 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