Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 11/2001 15. listopad 2001

11/2001

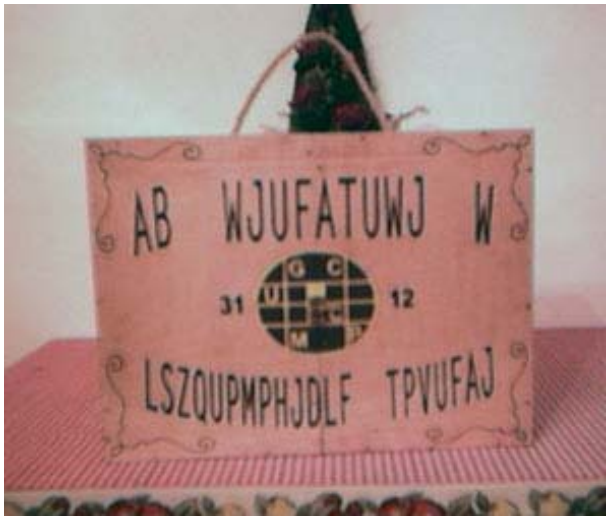
Připravil : Mgr.Pavel Vondruška,
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>330 e-mail výtisků)

OBSAH : **Str.**

A. **Soutěž 2001 , III.část - RSA**

Pavel Vondruška, ÚOOÚ

V dnešním čísle pokračuje soutěž v luštění různých jednoduchých problémů souvisejících se základními šifrovými systémy. Tak jako v loňském roce probíhá soutěž celkem ve čtyřech kolech. V každém ze sešitů 9/2001 až 12/2001 bude uveřejněna jedna nebo dvě soutěžní úlohy a současně bude uveden doprovodný text k této úloze. Řešitelé, kteří zašlou správné řešení ve stanoveném termínu, budou slosováni a výherce získá symbolickou cenu kola. I po tomto datu lze však řešení dále zaslat, všechna řešení budou zkontrolována a bodově ohodnocena. 30.12.2001 bude soutěž ukončena a z řešitelů, kteří získali nejvíce bodů, bude vylosován celkový vítěz. Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže později, např. až v prosinci, a řešení všech úloh odešle najednou v časovém limitu, tedy do 30.12.2001; přijde jen o možnost být vylosován jako vítěz příslušného kola. První číslo e-zinu v roce 2002 bude věnováno výsledkům a průběhu soutěže, uvedena řešení úloh všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Hlavní cenu soutěže věnoval jeden z loňských úspěšných řešitelů. Cena je velice lákavá - šest lahví kvalitního značkového bulharského vína ve speciálním balení, které bylo vyrobeno pro tuto soutěž (viz. obrázky). Cenou kola bude CD se staršími čísly Crypto-Worldu a placený certifikát od některého z předních poskytovatelů těchto služeb.



Máte zájem o tuto krásnou cenu? Pak se zapojte do soutěže! Začněte třeba touto následující malou rozcvičkou nazvanou úloha č.4.

Úloha č.4

Co je napsáno na obalu ceny pro vítěze?

(10 bodů za úplný text , včetně správné interpretace číslic)
(pozor : 31 12 není datum, kdy se má víno vypít…)

Nápověda : již staří Římané znali víno….

Připomeňme, jaké úlohy byly již čtenářům předloženy:
Září - jednoduchá záměna , kódová kniha
Říjen - absolutně bezpečný systém

Řešitel	I.kolo 1.úloha	I.kolo 2.úloha	II.kolo 3.úloha	III.kolo 4.úloha	III.kolo 5.úloha	IV.kolo 6.úloha	IV.kolo 7.úloha
Jan J.	19.09/ 10	19.09/ 10	18.10/ 10				
František P.	19.09/ 10	19.09/ 10	16.10/ 10				
Jozef K.	02.10/ 10	02.10/ 10	30.10/ 10				
Richard K.	04.10/ 10	04.10/ 10					
Karel Š.	10.10/ 10	10.10/ 10	31.10/ 10				
Tomáš V.	21.10/ 10	26.09/ 10					
Jan K.		30.09/ 10	21.10/ 10				
Mirek Š.	30.10/ 10	30.10/ 10	30.10/ 10				
Vítězslav S.		6.11 / 10	6.11 / 10				

Asymetrická kryptografie - RSA

Asymetrická kryptografie je založena na této myšlence: Každý subjekt má svůj soukromý klíč a k němu odpovídající veřejný klíč. Soukromý klíč je určen k zašifrování a veřejný klíč k odšifrování. K chráněné vzájemné komunikaci n subjektů je tak potřeba připravit jen 2n klíčů, přičemž veřejné klíče lze opravdu zveřejnit a odpadá tedy nutnost složité, nákladné a nebezpečné distribuce těchto klíčů. U symetrických šifer je situace značně složitější. K chráněné vzájemné komunikaci (tedy tak, aby vždy danou zprávu mohla číst jen vybraná dvojice komunikujících subjektů) je potřeba, aby každý z komunikujících n subjektů měl své klíče pro komunikaci s ostatními n-1 subjekty. Šifrování v případě asymetrické kryptografie mezi subjekty A a B pak probíhá takto: A má dvojici klíčů "AS" (soukromý klíč), "AV" (veřejný klíč), B má k dispozici obdobně klíče "BS" a "BV". Klíče "AV", "BV" jsou zveřejněny a jsou tedy A i B známy. Subjekt A připraví text, který chce utajit, zašifruje jej svým klíčem "AS" a dále jej zašifruje veřejným klíčem příjemce "BV" (jinak by zprávu mohl odšifrovat každý, kdo má přístup k veřejnému klíči "AV"). Příjemce B potom nejprve odšifruje přijatou zprávu pomocí svého soukromého klíče "BS" (ten zná jen on a tím je zaručeno, že se k této zprávě dostane jen tato oprávněná osoba) a dále pomocí veřejného klíče odesílatele AV.

Brzy po zveřejnění teoretického schématu asymetrické kryptografie (1978) se objevuje první šifrový systém založený na této myšlence. Vžil se pro něj název RSA (zkratka je složena z prvních písmen tvůrců systému Rivest, Shamir a Adelmann). Tento systém se po malých úpravách (především prodloužení klíče a stanovení jistých pravidel, která musí klíče splňovat) používá dodnes. Je založen na obtížném matematickém problému -- faktorizaci (rozkladu na prvočísla) velkých čísel. Vše si nejlépe uvědomíme na následujícím jednoduchém příkladě. Zkusíte najít celočíselné dělitele čísla 217502279? Jsou jimi dvě prvočísla 14713 a 14783. Zatímco vyhledání těchto čísel vám dalo relativně dost práce, pak vynásobení těchto dvou čísel je úkonem velice jednoduchým.

Vzhledem k tomu, že RSA ovlivnilo rozhodujícím způsobem kryptologii konce 20.století a význam celého systému v souvislosti se zavedením elektronických podpisů neustále roste, řekněme si dnes něco více o matematických principech tohoto systému.

Popis algoritmu RSA

Postup při vytváření dvojice veřejný a soukromý klíč pro RSA je následující:

a) nejprve náhodně (a nepredikovatelně) vygenerujeme dvě dostatečně velká prvočísla (jejich přibližná velikost, tj. počet bitů, se zadává)

b) Vypočteme

$N = p*q$ a

$\Phi(N) = (p-1)*(q-1)$

(Poznámka 1: $\Phi(N)$ je Eulerova funkce určující počet přirozených čísel nesoudělných s N a menších než N).

Poznámka 2: V praxi lze číslo $\Phi(N)$ nahradit číslem $L = NSN(p-1, q-1)$ tj. nejmenším společným násobkem čísel p-1 a q-1).

c) Zvolíme náhodné číslo e, kde

$1 < e < \Phi(N)$, tak, že $NSD(e, \Phi(N)) = 1$ (tj. e a $\Phi(N)$ jsou nesoudělná) .

Zde NSD značí největšího společného dělitele.

d) Užitím Eukleidova algoritmu vypočteme jednoznačně definované číslo d takové, že

$1 < d < \Phi(N)$ a

$e*d \equiv 1 \mod \Phi(N)$.

(Pozn. Zápis $A \equiv B \mod C$, znamená, že A - B je dělitelné C beze zbytku. Nebo lze také číst tak, že A děleno C dává zbytek B)

Existence takového čísla d je dána Bautzovou větou.

Veřejným klíčem je potom dvojice (N,e), soukromým klíčem uživatele je dvojice (N,d) (někdy nazývána "tajným" klíčem).

V případě použití systému RSA se pro elektronický podpis v souladu s terminologií Zákona o elektronickém podpisu č. 227/2000 používá odlišné názvosloví. Veřejný klíč se nazývá data pro ověření podpisu a soukromý klíč se nazývá data pro vytváření elektronického podpisu

Číslo N nazýváme modul, číslo e šifrovacím exponentem a číslo d dešifrovacím exponentem. Veřejný klíč zde tvoří čísla e, N, zadními vrátky je čtveřice čísel p, q, d, Φ (N). Přitom znalost jednoho z čísel p, q, Φ (N) vede k bezprostřednímu nalezení zbývajících tří a znalost čísla d nám dává pravděpodobnostní polynomiální algoritmus pro faktorizaci čísla N. Řešitelé dnešní úlohy se přesvědčí, že faktorizace modulu - tedy rozklad N na p a q vede k prolomení šifrování v RSA.

Popis vlastního šifrování a dešifrování

Popíšeme, jak probíhá vlastní zašifrování a dešifrování. Předpokládejme, že strana B zná veřejný klíč strany A, kterým je (N,e) a šifruje zprávu M pro A.

Strana B vyjádří zprávu M jako číslo m, $0 \le m \le N-1$ (resp. posloupnost takových čísel).

Dále strana B vypočte

$c \equiv m^e \mod N$

a zašle tento šifrový text straně A.

Strana A nyní při dešifraci vypočte pomocí soukromého klíče d,N :

$m \equiv c^d \mod N$.

Příklad

Zvolíme prvočísla: p=47, q=71,

Spočteme modul : $N = p*q = 47*71 = 3337$

a dále: $\Phi(N) = (p-1)*(q-1) = 46*70 = 3220$

Zvolíme veřejný exponent e (nesmí mít společné dělitele s 3220) , volíme např. 79

Spočteme soukromý exponent d:

d …… $79*d \equiv 1 \bmod 3220$

$d \equiv 79^{-1} \bmod 3220$

$d = 1019$

(k výpočtu použijeme Eukleidův algoritmus)

Získali jsme:

e …….. veřejný klíč (3337, 79) ,

d …..…... soukromý klíč (3337, 1019)

Nyní si na příkladě předvedeme, jak se v tomto systému šifruje a dešifruje.

Vezmeme například otevřený text VESELE VANOCE !

Otevřený text převedeme "nějakým" vhodným způsobem do "nějaké" číselné soustavy (tedy zakódujeme). K tomu např. použijeme naši "známou" převodovou tabulku z minulého čísla doplněnou o znak !.

	0	1	2	3	4	5	6	7	8	9
6						**A**	**B**	**C**	**D**	**E**
7	**G**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
8	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
9	**Z**	**.**	**!**							

Získáme tak :

O = 86 69 83 69 76 69 86 65 78 79 67 69 92

Dále stanovíme určitá pravidla formátování. V praxi se používají poměrně složitá pravidla. Zájemcům doporučuji prostudovat standard PKCS o němž jsme v našem e-zinu již psali v minulém roce. My si však zavedeme následující jednoduchá pravidla. Nazvěme je nadneseně standard formátování Crypto#1.0 .

Crypto #1.0 :

1) Má-li modul délku k, budeme zprávu v dekadickém tvaru dělit na skupiny délky k-1.
2) Všechny skupiny musí mít délku k-1, nemá-li poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
3) Výsledek po šifrování má délku rovnou maximálně k, nemá-li ji doplníme výsledek zleva nulami.

Vezměme zprávu M= **86 6**9 83 69 76 69 86 65 78 79 67 69 92

M rozdělíme podle pravidla Crypto#1.0 , 1 - na na bloky m_1 m_2 m_3 …..

M = m_1 m_2 m_3 ….. = **866** 983 697 669 866 578 796 769 920

Poslední skupina vznikla doplněním 92 o 0 (pravidlo Crypto#1.0 , 2).

Pro pochopení stačí předvést konkrétní výpočet např. jen pro prvou skupinu:

Šifrování:

blok m_1 = **866**

$c_1 \equiv m_1^e \bmod N$

$c_1 \equiv 866^{79} \bmod 3337 \equiv 492$ (Pozn. tj. 866^{79} při dělení 3337 dává zbytek 492)

Výsledek zapíšeme jako **0492** (pravidlo Crypto#1.0 , 3)

Dešifrování:

$m_1 \equiv c_1^d \bmod N$

$\mathbf{0492}^{1019} \bmod 3337 \equiv 866$ (Pozn. tj. 492^{1019} při dělení 3337 dává zbytek 866)

blok $m_1 = \mathbf{866}$

Provedeme tento postup s celým textem a dostaneme:

M = **866** 983 697 669 **866** 578 796 769 920

Š = **0492** 1075 2833 0616 **0492** 0855 2474 1015 2469

Všimněte si, že se v šifrovém textu se objevila 2x stejná skupina 0492. V obou případech příslušný otevřený text obsahuje stejné písmeno - písmeno "V". Abychom zastřeli z kryptologického hlediska tuto nevhodnou vlastnost, budeme definovat složitější standard formátování. Např. tento:

Crypto #1.5 (nebudeme nyní formulovat obecně, ale pro modul délky 4) :

1) Má-li modul délku 4 , budeme zprávu v dekadickém tvaru dělit na skupiny délky 2.
2) Všechny skupiny musí mít délku 2, nemá-li poslední skupina tuto délku, doplníme ji zprava nulou.
3) Skupinu doplníme zprava vzestupně číslicemi 1,2, ..9,0 , pokud má text více jak deset skupin, začneme doplňovat zprava opět číslici 1,2 atd.
4) Výsledek po šifrování může má délku maximálně 4, nemá-li tuto délku doplníme výsledek zleva nulami.

Podle tohoto standardu zformátujeme náš otevřený text následovně:

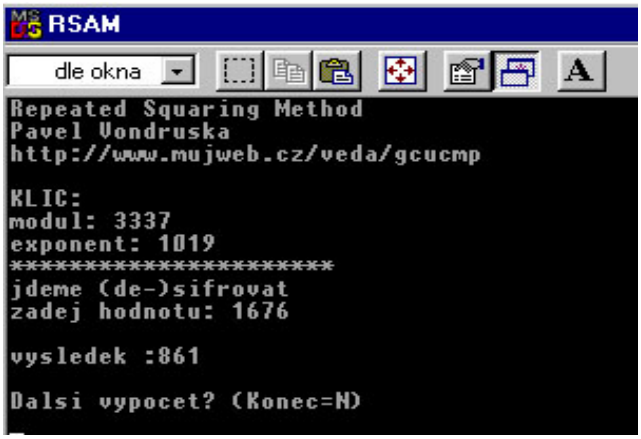
M = $m_1\ m_2\ m_3\ \ldots\ldots$ = 861 692 833 694 765 696 867 658 789 790 671 692 923

Šifrování:

blok $m_1 = \mathbf{861}$

$c_1 \equiv m_1^e \bmod N$

$c_1 \equiv 861^{79} \bmod 3337 \equiv \mathbf{1676}$.



Dešifrování:

$m_1 \equiv c_1^d \bmod N$

$\mathbf{1676}^{1019} \bmod 3337 \equiv 861$

blok $m_1 = \mathbf{861}$

O =	86	69	83	69	76	69	86	65	78	79	67	69	92
M =	**861**	692	833	694	765	696	867	658	789	790	671	692	923
Š =	**1676**	1130	1788	2909	3335	1638	2048	1833	0961	2954	2160	1130	2698

Vidíme, že tento způsob formátování je z hlediska utajení výhodnější. Písmeno "V" se nyní zašifruje pokaždé jiným způsobem (přesněji - zašifruje se jiným způsobem pouze tehdy, pokud vzdálenost mezi dvěma výskyty V není dělitelná deseti…).

Bezpečnost algoritmu

Otázka bezpečnosti algoritmu RSA se ne zcela správně často redukuje pouze na diskusi o velikosti modulu. Bezpečnost tohoto systému je však závislá i na správné implementaci, na velikosti soukromého a veřejného exponentu a na mnoha dalších detailech.

Obecně je však bezpečnost tohoto algoritmu skutečně založena na složitosti úlohy faktorizace velkých čísel. Lze lehce ukázat, že pokud dokáži faktorizovat N, pak samozřejmě dokáži spočítat Φ(N) a tudíž odvodit z veřejného exponentu e i soukromý exponent d.

K "rozbití RSA" však nepotřebujeme faktorizaci, stačí vyřešit následující problém (nazývaný RSAP) - Je-li zadáno číslo $C \in Z_N$, nalezněte pouze ze znalosti čísel N,e,C takové $M \in Z_N$, , že platí $M^e \equiv C \mod N$. Jinými slovy vypočítat e-tou odmocninu modulo složené číslo N bez znalosti rozkladu modulu na prvočinitele.

Takovýto algoritmus nebyl dosud nalezen a není ani znám důkaz toho, že existovat nemůže. Žádné konkrétní poznatky v tomto směru nebyly nalezeny, přesto je všeobecně kryptology předpokládáno, že složitost obou úloh je ekvivalentní.

Existuje i řada různorodých jiných útoků, které jsou založeny na využití skrytých či zjevných chyb při implementaci RSA nebo na jiných tricích jak obejít řešení faktorizace. Jmenujme zde alespoň následující „útoky" :

- útoky na RSA pomocí faktorizace modulu
- společný modul
- využití multiplikativní vlastnosti kryptosytému
- malá hodnota soukromého exponentu
- malá hodnota veřejného exponentu
- šifrování stejné zprávy různými klíči
- šifrování příbuzných zpráv jedním klíčem
- šifrování stejné zprávy s náhodným doplňkem
- útok proti formátování podle standardu PKCS #1 ve verzi 1.5
- útok proti formátování podle standardu PKCS #1 ve verzi 2.0
- útoky na vlastní implementace RSA
- analýza chyb
- postraní kanály !!!
- "kvantové počítače"

Více informací najdete např. v jednom z našich starších e-zinů (P.Vondruška, Je RSA bezpečné ?, Crypto-World 1/2001).

Úloha č.5 - RSA - Klíč pro šifrování (modul, e) = (2479, 101)

0385 1927 1713 1134 1519 0521 0142 0899 0544 2098 0920 1354 1502 1387 0927

Vaším úkolem je nalézt klíč pro dešifrování (tj. tajný exponent d) - (modul, d)=(2479,?) a dále zaslat původní otevřený text (10 bodů za zaslání textu a hodnoty d).

Nápověda :

1) převodová kódová tabulka je shodná s tabulkou v předchozím cvičném případě
2) formátování je podle námi zavedeného standardu Crypto #1.0 (!)
3) pokud máte problémy s "velkými čísly" , pak mohu pro pohodlné výpočty nabídnout mnou napsaný krátký program **RSAM** (9 kB), který využívá k modulárním výpočtům "Repeated Squaring Method"
4) program RSAP naleznete na mé www stránce, protože je v poslední době tato stránka opravdu těžko dostupná, jedná se tak vlastně také o úkol - (ovšem nehodnocený ☺) a to o úkol typu "záchyt".

Závěrečné pokyny pro řešitele

Řešení zasílejte e-mailem na adresu pavel.vondruska@post.cz (kopii prosím zaslat na pavel.vondruska@uoou.cz). Předmět označte heslem : ULOHA-4,5

Termín: do slosování budou zařazena všechna správná a úplná řešení, přijatá do 14.12.2001 !

B. New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report

Bart Preneel

Dept. Electrical Engineering-ESAT,
Katholieke Universiteit Leuven
Kasteelpark Arenberg 10,
B-3001 Leuven-Heverlee, BELGIUM,
bart.preneel@esat.kuleuven.ac.be
http://www.cryptonessie.org

Vážení čtenáři, nemůžete se zúčastnit Mikulášské kryptobesídky? Zajímá vás přednáška zvaného řečníka Barta Preneela? Pak jistě uvítáte právě tento článek. Využívám možnost otisknout v našem e-zinu jím připravený příspěvek určený právě pro tuto besídku. Další informace o chystané akci najdete na straně 23 tohoto čísla. Přeji všem čtenářům příjemný zážitek a těm, kteří se v prosinci zúčastní besedy s panem Preneelem na naší Mikulášské kryptobesídce, umožňuji připravit si na základě článku zasvěcené dotazy.

Abstract

The NESSIE project intends to put forward a portfolio containing the next generation of cryptographic primitives. These primitives will offer a higher security level than existing primitives, and/or will offer a higher confidence level, built up by an open evaluation process. Moreover, they should be better suited for the constraints of future hardware and software environments. In order to reach this goal, the project has launched an open call; in response to this call, 39 primitives have been received, many of these from major players. Currently, the NESSIE evaluation process is under way; it considers both security and performance aspects. This article presents the status of the NESSIE project after 18 months.

Introduction

NESSIE (New European Schemes for Signature, Integrity, and Encryption) is a research project within the Information Societies Technology (IST) Programme of the European Commission. The participants of the project are:
Katholieke Universiteit Leuven (Belgium), coordinator;
Ecole Normale Supérieure (France);
Royal Holloway, University of London (U.K.);
Siemens Aktiengesellschaft (Germany);
Technion - Israel Institute of Technology (Israel);
Université Catholique de Louvain (Belgium); and
Universitetet i Bergen (Norway).

NESSIE is a 3-year project, that started on January 1st 2000. This paper intends to present the state of the project after 18 months.

1.Call for Primitives

In the first year of the project, an open call for the submission of cryptographic primitives, as well as for evaluation methodologies for these primitives has been launched. The scope of this call has been defined together with the project industry board (PIB), and it was published in March 2000. The PIB consists of 25 major security European vendors and users. The deadline for submissions was 29 September 2000. In response to this call NESSIE received 40 submissions, all of which met the submission requirements.

The NESSIE call includes a request for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption and identification schemes. In addition, it asks for evaluation methodologies for these primitives. The scope of this call has been determined together with the project industry board during the first PIB meeting. The PIB has given several important suggestions with regards to market requirements.

The scope of this call is much wider than that of the AES call launched by NIST. It is comparable to that of the RACE Project RIPE (1988-1992) and that of the Japanese CRYTPREC project.

In response to the call 40 submissions were received: 39 primitives in 7 categories and 1 evaluation methodology. The breakdown per type of primitive is as follows: 17 block ciphers, 6 synchronous stream ciphers, 2 MAC algorithms, 1 collision resistant hash function, 5 asymmetric encryption schemes (two of these have three variants each), 7 digital signature schemes, and 1 identification scheme. An interaction process of about a month with the submitters resulted in all the submissions meeting the formal submission requirements and entering the evaluation phase of NESSIE.

Approximately seventeen submissions originated within Europe (6 from France, 4 from Belgium, 2 from Sweden and Switzerland), nine in North America (7 USA, 2 from Canada), nine in Asia (8 from Japan), three in Australia and three in South America (Brazil). The majority of submissions originated within industry (27); seven came from academia, and six are the result of a joint effort between industry and academia. Note however that the submitter of the algorithm may not be the inventor, so the share of academic research is probably underestimated by these numbers.

On 13-14 November 2000 the first NESSIE workshop was organised in Leuven (Belgium), where 35 submissions were presented. All submissions are available on the NESSIE web site, http://www.cryptonessie.org/

2. Evaluation

The evaluation criteria of NESSIE are the following: security criteria, implementation criteria, other criteria, and licensing requirements. Security criteria are resistance against generic attacks for the type of primitive, conformance to the security claims of the submitter, and vulnerability to side channel attacks (such as timing attacks and power analysis). Implementation criteria are software and hardware, efficiency in the environments specified

by the submitter, code and data size, and efficiency in other environments than specified by the submitter. Other criteria are simplicity and clarity of design. Variable parameter size is considered to be of less importance. If selected by NESSIE, the primitive should preferably be available royalty-free. If this is not possible, then access should be non-discriminatory. The submitter should state the position concerning intellectual property and should update it when necessary.

The security evaluation resulted in an extensive report, assessing the security of the primitives. This report also describes the external inputs received. The performance evaluation focused on a theoretical evaluation (counting the number of operations), and a measurement of optimized C-code on PCs and workstations (due to the large number of submissions, it was not possible to fine tune the optimizations). The evaluation process was supported by the developments of tools. These include a very extensive statistical tool set (built on the toolset developed by RIPE) and a number of dedicated tools, that is, tools developed to evaluate a specific submission. The security and performance evaluation report are available on the NESSIE homepage. This homepage also contains a document describing the tools.

On 12-13 September 2001 the second NESSIE workshop was organised in Egham (UK). At this workshop technical contributions from inside and outside the projects were presented. 3. Selection

On 24 September 2001, NESSIE has announced the following selection of contenders for the 2nd phase:

Block ciphers:
IDEA: MediaCrypt AG, Switzerland;
Khazad: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium;
MISTY1: Mitsubishi Electric Corp., Japan;
SAFER++$_{64}$, SAFER++$_{128}$: Cylink Corp., USA, ETH Zürich, Switzerland, National Academy of Sciences, Armenia;
Camellia: Nippon Telegraph and Telephone Corp., Japan and Mitsubishi Electric, Japan;
RC6: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
SHACAL: Gemplus, France.

Stream ciphers:
SOBER-t16, SOBER-t32: Qualcomm International, Australia;
SNOW: Lund Univ., Sweden;
BMGL: Royal Institute of Technology, Stockholm and Ericsson Research, Sweden.

Public-key encryption:
ACE Encrypt: IBM Zurich Research Laboratory, Switzerland;
EPOC-2: Nippon Telegraph and Telephone Corp., Japan;
PSEC-2: Nippon Telegraph and Telephone Corp., Japan;
ECIES: Certicom Corp., USA and Certicom Corp., Canada
RSA-OAEP: RSA Laboratories Europe, Sweden and RSA Laboratories, USA.

MAC algorithms and hash functions:
Two-Track-MAC: K.U.Leuven, Belgium and debis AG, Germany;
UMAC: Intel Corp., USA, Univ. of Nevada at Reno, USA, IBM Research Laboratory, USA, Technion, Israel, and Univ. of California at Davis, USA;

Whirlpool: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium.
Digital signature algorithms:
ECDSA: Certicom Corp., USA and Certicom Corp., Canada;
ESIGN: Nippon Telegraph and Telephone Corp., Japan;
RSA-PSS: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
SFLASH: BULL CP8, France;
QUARTZ: BULL CP8, France.

Identification schemes
GPS: Ecole Normale Supérieure, Paris, BULL CP8, France Télécom and La Poste, France.

At this stage, no substantial weaknesses have been identified in any of the finalists. However, the designers have been invited to make minor alterations to the algorithm to address any security concerns identified during the first phase. It should also be pointed out that the NESSIE project will compare these submissions to existing and emerging standards such as AES/Rijndael, SHA-256, SHA-384 and SHA-512. NESSIE is inviting the community at large to further analyse the candidates for the 2nd phase, and to offer comments on their security, performance and intellectual property status. All the candidates of the 2nd phase will be discussed at a workshop in November 2002. The project is accepting comments until mid November 2002. The final selection will be announced by December 2002.

4. Conclusion

The NESSIE project has succeeded in attracting an interesting set of submissions from major players in the field. The most promising submissions have been selected for the 2nd phase. Both the call and the selection process have been open; input has been sought from major players in industry. They should result in an improved security level for all cryptographic primitives, comparable to the evolution from DES to AES. We are convinced that these submissions will allow to define a strong portfolio of new cryptographic algorithms for the 21st century.

Pokračování a dotazy na Mikulášské kryptobesídce, kam jste všichni velice srdečně zváni

---

Program Mikulášské kryptobesídky

V podvečer pondělí 10. prosince 2001 se koná panelová diskuse se zvanými přednášejícími a neformální setkání účastníků.
V úterý 11. prosince 2001 probíhají prezentace zvaných a vybraných příspěvků. Přesný program bude upřesněn později.

Zvaní řečníci:
Bart Preneel (KU Leuven) o projektu NESSIE,
Fabien Petitcolas (Microsoft Research) o vztahu watermarkingu a kryptografie.

C. Dostupnost informací o ukončení platnosti, zneplatnění a zrušení kvalifikovaného certifikátu

Mgr. Pavel Vondruška, ÚOOÚ

Rozboru pojmů ukončení platnosti a zneplatnění kvalifikovaného certifikátu jsme se již v předchozích číslech našeho e-zinu věnovali ([3], [4], [5]). Nejrozsáhlejší diskuse okolo tohoto tématu proběhla v době příprav návrhu prováděcí vyhlášky ÚOOÚ k zákonu o elektronickém podpisu. Vyhláška byla podepsána 3.10.2001 [2]. Vzhledem k tomu, že se jedná o jeden z nejdůležitějších momentů, který zásadně ovlivňuje důvěru v celý systém vztahů : podepisující se osoba – poskytovatel certifikačních služeb – osoba spoléhající se na podpis, je pravděpodobné, že se k tomuto tématu budeme stále vracet.

Dnes na toto téma uveřejňujeme dva články. První se věnuje některým vybraným technickým aspektům a různým možnostem přístupu k informaci o certifikátech, které byly zneplatněny, druhý se věnuje právním otázkám (odpovědnosti a přechodu odpovědnosti ve smyslu zákona o elektronickém podpisu) vztahujícím se k otázce ukončení platnosti a zneplatnění.

I.Úvod

Úvodem uvedu citace relevantních požadavků na ukončení platnosti a zneplatnění ze zákona o elektronickém podpisu [1] a prováděcí vyhlášky[2].

V Zákoně o elektronickém podpisu č.227/2000 je řešeno ukončení platnosti, zneplatnění a přístup k těmto informacím v následujících paragrafech:

§6, odst. 7

Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.

§6, odst.1 g)

Zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem.

§15, odst. 2

Seznam certifikátů podle § 6 odst. 1 písm. g) musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn.

Vyhláška č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu, platná od 10.10.2001, upřesňuje předchozí požadavky následovně:

§ 3, odst. 6

Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné.

§ 3, odst. 7

Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, datum a čas s uvedením hodiny, minuty a sekundy, od kdy byl kvalifikovaný certifikát zneplatněn.

II. Norma X.509

Vraťme se ke zveřejňování informací o ukončení platnosti kvalifikovaného certifikátu. Obsah certifikátů a způsoby získání informací o jejich stavu (statutu) vychází z norem X.509. Norma X.509 byla vytvořena s cílem dát rámec pro autentizaci ve vztahu k adresářovým službám popsaným v dokumentech řady X.500. Jak X.500, tak i X.509 jsou součástí série X mezinárodních norem navržených organizacemi ISO a ITU. Normy X.500 byly navrženy pro popis adresářových služeb ve velkých počítačových sítích, X.509 pak zabezpečuje pro služby v rámci X.500 příslušný autentizační rámec. První verze normy X.509 se objevila v roce 1988 (a je to současně nejstarší návrh modelu PKI). Do roku 1997 byla používána (a je ještě stále implementována v některých starších produktech) verze 2 normy X.509; tato verze používala velice jednoduchý formát pro CRL, který se záhy ukázal jako překonaný. Proto byla publikována třetí verze normy X.509, která (na základě získaných zkušeností) podstatně rozšířila funkční záběr normy a v dnešní době již většina produktů v oblasti PKI se řídí právě touto normou. Norma prodělala základní změnu - umožnila existenci libovolných rozšíření (tzv.extenzí) pro certifikáty a různá další rozšíření pro CRL (Certification Revocation List). CRL je v terminologii našeho zákona o elektronickém podpisu označován jako : „seznam certifikátů, které byly zneplatněny“. Dále budeme používat střídavě oba dva výrazy, tedy CRL i termín definovaný v našem zákoně. Předpokládáme, že tato dvojjazyčnost nepřinese čtenáři potíže. Pojem rozšíření (extension) byl definován především proto, aby mohl obsahovat informaci o certifikační politice, o atributech držitele certifikátu i vydavatele certifikátu, o cestě, kterou probíhá ověřování certifikátu, ale i mnohé další informace, které s ukončením platnosti nesouvisí.

III. Obecná definice certifikátu podle X509

Formát certifikátu definovaný podle doporučení ITU-T X509 [6] a užívaný v RFC2459 [7] lze pomocí kódování ASN.1 zapsat následovně:

Version : Version of the certificate (DEFAULT v1), (v2, v3)
serialNumber: CertificateSerialNumber,
signature : AlgorithmIdentifier,
issuer :Name,
validity : Validity, (period)
subject : Name,
subjectPublicKeyInfo,
issuerUniqueID UniqueIdentifier OPTIONAL (v2 or v3)
subjectUniqueID UniqueIdentifier OPTIONAL (v2 or v3)
extensions Extensions OPTIONAL(v3)

Aktuální verze RFC2459 pro podpisové schéma podporuje následují hašovací a asymetrické funkce :

- hašovací funkce : SHA-1, MD2 and MD5,
- podpisové algoritmy : RSA, DSA and Diffie-Hellman.

Vyhláška 366/2001 v příloze č.1 (algoritmy, které si generuje žadatel o certifikát) povoluje následující algoritmy (doplněné o předepsané minimální parametry):

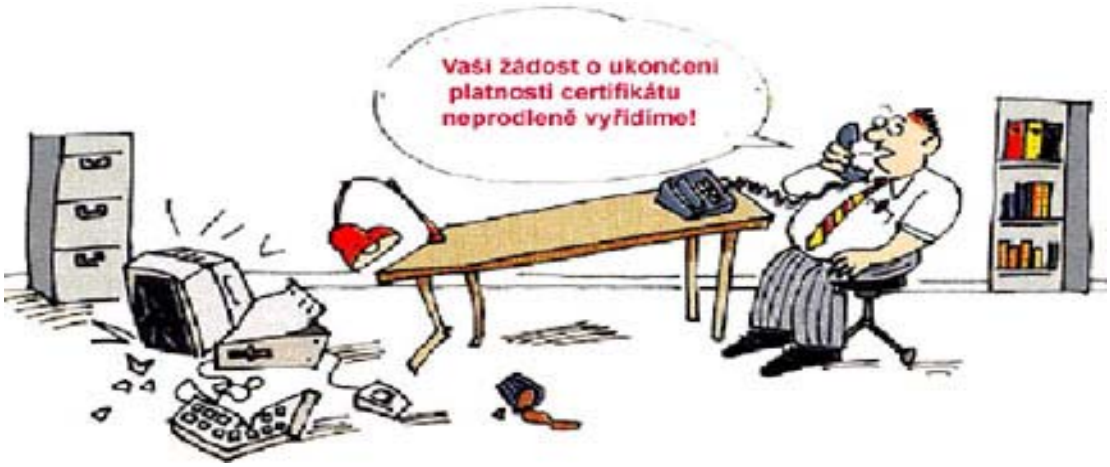
- hašovací funkce : SHA-1, RIPEMD 160 a MD5,
- podpisové algoritmy : RSA, DSA, ECDSA-F_p, ECDSA-$F2^m$.

Stejné algoritmy (včetně algoritmů pro eliptické křivky) doporučuje také nejnovější draft dokumentu “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [12].

IV. Ověřování statutu certifikátu

IV. a - CRL

Většina současných aplikací používá při ověřování certifikátu informace ze seznamu zneplatněných certifikátů (CRL - Certificate Revocation List). Tento protokol byl v době vzniku prvních norem a standardů jediným protokolem, který byl k získání informace o ukončení platnosti (zneplatnění) zvažován. Náš zákon o elektronickém podpisu [1] upravuje ze všech metod přístupu k informaci o ukončení platnosti certifikátu pouze požadavky na tento přístup ke statutu certifikátu. Provozování této metody přístupu je pro poskytovatele, kteří režimu zákona podléhají (tj. pro akreditované poskytovatele a poskytovatele vydávající kvalifikované certifikáty), povinné.



CRL (Certificate Revocation List) je definován např. v dokumentu RFC 2459 [7]. Perioda zveřejňování musí být uvedena v certifikační politice. V dokumentu se dále uvádí, že perioda zveřejňování může být v hodinách, dnech nebo třeba i týdnech. Vše záleží na konkrétní certifikační politice a na agendě, ve které se certifikáty používají. Úřad v návrhu vyhlášky prosazoval stanovení periodického vydávání CRL 24 hodin (a to jako doby maximální). Vycházel přitom z dokumentů, které navazují na směrnici EU o elektronických podpisech, konkrétně z dokumentu ETSI [14] : ES 201 456 „Policy requirements for certification authorities issuing qualified certificates“. V průběhu připomínkového řízení příslušný paragraf vyhlášky 366/2001 získal tuto konečnou podobu:

§ 3, odst. (7)

„Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin“.

Formulace je poněkud nešťastná. Při přesném dodržení tohoto paragrafu totiž nemusí být zachována periodicita vydávání CRL. Pokud poskytovatel neobdrží žádnou žádost o ukončení platnosti - není nucen (dle dikce tohoto paragrafu) vydat příslušné CRL. V praxi se periodicita vydávání důsledně zachovává (CRL se číslují) a CRL se vydává i v případě, že k žádné změně nedošlo.

Další důležité informace vztahující se k CRL

CRL Distribution Point (CRL DP) – v certifikátu musí být uveden nejméně jeden distribuční bod. Vzhledem k podmínce vyhlášky 366/2001, §3, odst. 6 plyne, že toto rozšíření musí být u kvalifikovaného certifikátu použito vždy a musí zde být uvedeny alespoň dva distribuční body pro CRL!

CRL DP je definováno v [7]. Každý distribuční bod musí být popsán následujícím způsobem:
DistributionPointName : GeneralNames or RelativeDistinghuishedName
Reason flag : FLAG
CRLIssuer : GeneralNames

Pořadová čísla CRL a kódy označující důvod k odvolání. Pořadová čísla musí umožnit uživateli se přesvědčit zda nějaké CRL postrádá nebo ne. Každý certifikát v CRL je také označen kódem, který popisuje důvod odvolání daného certifikátu. Náš zákon ani vyhláška toto nijak dále neupravuje.

Delta-CRL. Vydávání tzv. delta-CRL umožňuje výraznou redukci velikosti rozesílaných a stahovaných CRL. V datové zprávě jsou obsaženy pouze změny oproti poslednímu vydanému CRL. Změnou se myslí nejen informace o nově zneplatněných certifikátech, ale i vypuštění certifikátů z CRL z důvodu vypršení platnosti. Certifikáty se po ukončení platnosti totiž v CRL neuvádějí. Náš zákon ani vyhláška vydávání takovýchto seznamů neupravuje.

IV. b - OCSP

Nově vyvíjené aplikace mohou využít i moderní přístupový protokol k informaci o stavu certifikátů. Takový protokol se nazývá Online Certificate Status Protocol – OCSP. Jedná se o relativně nový protokol, který zatím v aplikacích není příliš rozšířen. Definován je např. v RFC 2560. Tento dokument byl zveřejněn teprve v červnu 1999. V úvodu dokumentu se popisuje hlavní výhoda tohoto protokolu – dostupnost informace o stavu certifikátu v době mezi vydáním dvou CRL.

Žádost podle protokolu OCSP obsahuje následující data:

-- protocol version
-- service request
-- target certificate identifier
-- optional extensions which MAY be processed by the OCSP Responder

Odpovědí na dotaz je indikace stavu certifikátu, na který se žadatel ptá. Odpověď může mít jen následující tři možnosti:

-- good (znamená, že nebyla přijata žádost o ukončení platnosti a certifikát není v aktuálním CRL, certifikát však nemusí být platný – tj. doba platnosti již mohla vypršet)
-- revoked (certifikát je uveden v CRL nebo byla přijata žádost o ukončení platnosti!)
-- unknown (poskytovatel certifikačních služeb není schopen na otázku odpovědět, o certifikátu nic „neví“) .

IV. c - Rozesílání informací

Poskytovatelé certifikačních služeb mohou nabídnout další službu spojenou s možností informovat o ukončení platnosti certifikátu také jiným smluvním způsobem. Konkrétně se jedná o zasílání informací na adresu žadatele a to v okamžiku ukončení platnosti nějakého certifikátu. V takovém případě je nutné smluvně stanovit způsob a formát dodávané informace. Výhodou je, že příslušný subjekt může být vzhledem k získání aktuálních informací pasivní a přesto získá aktuální informace o ukončení platnosti každého certifikátu. Takovéto systémy nejsou zcela běžné a používají se pro velice speciální účely. Pokud vím, neexistuje žádný standardizovaný protokol pro takovouto službu.

Běžnou službou je zasílání delta-CRL nebo CRL zákazníkům, kteří s PCS uzavřeli smlouvu o této službě.

IV. d - Poskytování informací

PCS zpravidla poskytují informace o jím vydaných certifikátech i např. telefonicky nebo e-mailem. Mezi těmito informacemi je samozřejmě i statut certifikátu. Služba může být za úplatu nebo zdarma – závisí na typu smlouvy mezi PCS a subjektem/subjekty spoléhajícími se na podpis. Je např. možné, že PCS vydává certifikáty, které se používají jen pro komunikaci s jediným subjektem.

IV. e - Nahlédnutí do seznamu vydaných certifikátů

Jsou však předchozí způsoby jedinými možnostmi, jak získat informaci o statutu kvalifikovaného certifikátu? Další možností, jak se může osoba spoléhající se na podpis přesvědčit o stavu certifikátu, je nahlédnutí do seznamu vydaných certifikátů (samozřejmě pokud zde statut certifikátu je uveden). Pro tuto službu poskytovatel certifikačních služeb umísťuje svůj komunikační server do tzv. demilitarizované zóny a zde zveřejňuje příslušný seznam certifikátů (ETSI : Electronic Signature Formats).

Zajímavý způsob využití právě této eventuality nabízí náš zákon o elektronickém podpisu.Zákon totiž stanoví poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty, tuto povinnost:

§6, odst.1 f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat.

V tomto seznamu zveřejňuje poskytovatel informace o vydaných certifikátech. Jednou ze zveřejněných informací je dle zvyklosti i statut certifikátu. Zákon nikde nestanoví jaké položky mají být zveřejňovány a uvedení statutu je tedy nepovinné a není vynutitelné. Je-li však ukončení platnosti (statut certifikátu) součástí zveřejněných informací o certifikátu, pak pokud byla ukončena platnost některého z certifikátů, musí být podle citovaného paragrafu tato změna zde zveřejněna, a to okamžitě. Informace o statutu certifikátu zveřejněná v tomto seznamu tak může být aktuálnější než informace v té době zveřejněném CRL. Využitelnost je vhodná především pro subjekty, které provádí ověřování jen výjimečně a záleží jim na rychlosti ověření podpisu (nechtějí čekat do vydání následného CRL).

[1] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
[2] Vyhláška č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu
[3] Vondruška, P.: Dostupnost informací o ukončení platnosti a zneplatnění kvalifikovaného certifikátu , Crypto-World 9/2001
[4] Prokeš J.: Ukončení platnosti, zneplatnění (a zrušení) certifikátu I., Crypto-World 5/2001
[5] Prokeš J.: Ukončení platnosti, zneplatnění (a zrušení) certifikátu II., Crypto-World 6/2001
[6] ITU-T Recommendation X.509 (1997), Data Networks and Open System communications. Information Technology (totéž vyšlo jako: ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Authentication framework").
[7] RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
[8] RFC 2527 (1999) : “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”
[9] ETSI TS 101 862 V1.2.0 “Qualified certificate profile”
[10] RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -OCSP"
[11] RFC 3039 (2001) : “Internet X.509 Public Key Infrastructure Qualified Certificate Profile”
[12] draft-ietf-pkix-scvp-04 (10-2000) “Simple Certificate Validation Protocol (SCVP)”
[13] draft-ietf-pkix-ipki-pkalgs-02 “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile”
[14] ES 201 456 „Policy requirements for certification authorities issuing qualified certificates“
[15] Zákon č. 40/1964 občanský zákoník

D. Odpovědnost a přechod odpovědnosti ve smyslu zákona o elektronickém podpisu

Bc. Jan Hobza, ÚOOÚ

Tento článek navazuje na seriál článků ([3], [5], [6]), které byly v tomto e-zinu již otištěny a to k tématu „ukončení platnosti, zneplatnění a zrušení kvalifikovaného certifikátu“ . Tentokráte se budeme věnovat aspektu odpovědnosti a přechodu odpovědnosti ve smyslu zákona o elektronickém podpisu.

Zákon o elektronickém podpisu (dále jen ZoEP) definuje povinnosti jednotlivých stran v procesu používání elektronického podpisu zejména v §§ 5 a 6 respektive 13 a 15. Vznikne-li v důsledku porušení povinností stanovených tímto zákonem škoda, odpovídá za ni škůdce podle občanského zákoníku. Škodu mohou ve smyslu tohoto zákona způsobit v zásadě tři subjekty. Podepisující osoba, spoléhající se strana a poskytovatel certifikačních služeb vydávající kvalifikované certifikáty (dále jen kvalifikovaný poskytovatel); teoreticky může škodu způsobit i Úřad pro ochranu osobních údajů ☺. K tomu, aby vznikla odpovědnost kvalifikovaného poskytovatele za škodu, musí být naplněny objektivní předpoklady, a k tomu, aby vznikla odpovědnost podepisující se osoby či spoléhající se strany, musí být naplněny i subjektivní předpoklady vzniku škody. Mezi objektivní předpoklady patří:

1. porušení právní povinnosti – aktivní protiprávní chování, opomenutí
2. existence škody – majetkové i nemajetkové povahy
3. příčinná souvislost mezi škodou a porušením právní povinnosti

Subjektivním předpokladem je zavinění (úmyslné či nedbalostní).

Podepisující osoba poruší právní povinnost, jestliže nedodrží povinnosti stanovené v § 5 odst. 1 ZoEP. Zde se podepisující osobě ukládá, aby

a) zacházela s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
b) uvědomila neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,
c) podávala přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

Budou-li naplněny výše zmíněné předpoklady vzniku škody a poruší-li podepisující osoba tyto své povinnosti, bude odpovídat za vzniklou škodu dle příslušných ustanovení občanského zákoníku. Dle § 5 odst. 2 ZoEP se však podepisující osoba zprostí této odpovědnosti (a to i přes to, že nedodržela své povinnosti), pokud prokáže, že ten, komu vznikla škoda (spoléhající se strana), neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn. Důkazní břemeno tedy leží na podepisující osobě.

Z tohoto ustanovení se odvozují povinnosti spoléhající se strany. Ta musí ověřit platnost elektronického podpisu a to, zda kvalifikovaný certifikát podepisující se osoby nebyl zneplatněn (možnosti ověření zneplatnění byly pojednány v první části tohoto referátu). Spojení „veškeré úkony“ v § 5 odst. 2 je třeba chápat v souvislosti s postupy ověřování elektronického podpisu a ověřování zneplatnění kvalifikovaného certifikátu, které kvalifikovaný poskytovatel stanoví ve své certifikační politice, případně v certifikační prováděcí směrnici, podle kterých tento certifikát bude vydávat. Kvalifikovaný poskytovatel a podepisující osoba spolu uzavírají písemnou smlouvu o vydávání kvalifikovaného certifikátu dle konkrétní certifikační politiky (případně certifikační prováděcí směrnice; záleží na interpretaci dokumentu RFC 2527, který je obecně uznávanou předlohou pro zmíněné dokumenty), a v ní zmíněné postupy ověřování tedy obě strany pokládají za dostatečné.

V případném soudním sporu tak soud může přihlédnout k těmto sjednaným postupům. Na druhé straně však soudu nic nebrání, aby interpretoval spojení „veškeré úkony“ jiným způsobem. Pokud spoléhající se straně vznikne škoda vyplývající z použití kvalifikovaného certifikátu v důsledku nedodržení omezení pro jeho použití, či pokud se bude spoléhat na certifikát, jehož platnost již vypršela, bude za tuto škodu odpovídat podle občanského zákoníku.

V § 7 odst. 1 ZoEP se říká: „Za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podle zvláštních právních předpisů“ (občanský zákoník). Splní-li tedy podepisující osoba a spoléhající se strana povinnosti vyplývající ze zákona, bude za vniklou škodu odpovídat kvalifikovaný poskytovatel.

Jak jsme viděli, zákon o elektronickém podpisu v zásadě dobře vymezuje oblasti odpovědnosti jednotlivých zúčastněných stran. Velice problematickou oblastí je ale přechod odpovědnosti mezi subjekty v případě ukončení platnosti, respektive zneplatnění kvalifikovaného certifikátu. Mezi povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen kvalifikovaný poskytovatel) mimo jiné patří zajištění provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat a dále zajištění provozování bezpečného a veřejně přístupného seznamu **kvalifikovaných certifikátů, které byly zneplatněny**, a to i dálkovým přístupem. V § 6 odst. 7 a 8 se dále říká: „(7) Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů; (8) Poskytovatel certifikačních služeb musí rovněž ukončit platnost kvalifikovaného certifikátu, dozví-li se prokazatelně, že podepisující osoba zemřela nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, nebo pokud údaje, na základě kterých byl certifikát vydán, přestaly platit“. V těchto situacích se ukládá kvalifikovanému poskytovateli povinnost **ukončit platnost kvalifikovaného certifikátu**. Jedná se zde ale o zvláštní případ ukončení platnosti a tím je zneplatnění (v obecné praxi a v zahraničí se používá přesnější výraz revokace). Kvalifikované certifikáty, kterým byla takto ukončena platnost, přesněji byly zneplatněny, se objeví na seznamu zneplatněných certifikátů (CRL), případně se tato skutečnost musí okamžitě objevit i v seznamu vydaných kvalifikovaných certifikátů, pokud se zde status zneplatnění uvádí. V § 15 ZoEP, který je nazván **zrušení kvalifikovaného certifikátu**, se uvádí důvody, pro které může Úřad pro ochranu osobních údajů (dále jen Úřad) nařídit kvalifikovanému poskytovateli zneplatnění kvalifikovaného certifikátu. I tyto certifikáty se musí objevit v CRL dle § 6 odst. 1 písm. g).

Jak vidíme, zákon obsahuje velice nekonzistentní terminologii, a proto je třeba si uvědomit, jaké jsou rozdíly mezi běžným ukončením platnosti a zneplatněním. Ukončení platnosti kvalifikovaného certifikátu, jejímž následkem je jeho neplatnost, zahrnuje jak vypršení doby platnosti, tak samotné zneplatnění. Na tomto místě ještě zdůrazněme, že zneplatněním se rozumí jak samotný akt ukončení platnosti z výše uvedených důvodů, tak stav, ve kterém se poté nachází kvalifikovaný certifikát. Zneplatnění ve smyslu aktu, je zvláštní forma ukončení platnosti, které musí kvalifikovaný poskytovatel provést na základě:

1. nařízení Úřadu
2. žádosti podepisující osoby
3. svého rozhodnutí

Zde se dostáváme k jádru problému přechodu odpovědnosti. Zákon přesně nestanoví, ve kterém okamžiku přechází odpovědnost podepisující osoby, která pojala podezření ve smyslu § 5 odst. 1 ZoEP na kvalifikovaného poskytovatele, a zda vůbec tato odpovědnost přechází na kvalifikovaného poskytovatele v době mezi podáním žádosti o zneplatnění a

uveřejněním informace o zneplatnění podle § 6 odst. 1 písm. g), případně f). Vyhláška Úřadu č. 366/2001 stanoví v § 3 odst. 7, že doba mezi ukončením platnosti (zneplatněním) kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin. Kvalifikovaný poskytovatel musí ukončení platnosti (zneplatnění) provést neprodleně, tedy ihned po přijetí žádosti o zneplatnění. Má ale nejvýše 12 hodin na to, aby tuto skutečnost zveřejnil v CRL. Tato doba je kamenem úrazu, neboť v jejím průběhu je výše diskutovaná odpovědnost za škodu, respektive odpovědný subjekt neurčitý: podepisující osoba uvědomila dle § 5 odst. 1 kvalifikovaného poskytovatele o nebezpečí, ten neprodleně zneplatnil a spoléhající strana ověřila v seznamu (CRL), který byl v té určité době aktuální, platnost kvalifikovaného certifikátu. Tento problém se v celosvětové praxi řeší v certifikační politice. Dle dokumentu RFC 2527 kvalifikovaný poskytovatel uvádí v dokumentu certifikační politika, podle kterého se ten který kvalifikovaný certifikát vydává, na koho v tomto kritickém období přechází odpovědnost. Podepisující osoba buď souhlasí s takovouto politikou a uzavře s kvalifikovaným poskytovatel smlouvu o vydávání, nebo nesouhlasí a tuto smlouvu neakceptuje. Poslední slovo však má spoléhající se strana, která buď souhlasí a bude se spoléhat na takto vydaný certifikát, nebo nesouhlasí a nebude se na tyto certifikáty spoléhat.

Při interpretaci zákona o elektronickém podpisu může vznikat ještě další problém, který s přechodem odpovědnosti nepřímo souvisí. ZoEP ani vyhláška č. 366/2001 přímo neukládají kvalifikovaným poskytovatelům povinnost zveřejňovat CRL periodicky po určité době, například po 12ti hodinách. Vyhláška ukládá kvalifikovaným poskytovatelům povinnost aktualizovat CRL po této době v případě, že došlo ke zneplatnění jakéhokoli kvalifikovaného certifikátu. Může tedy nastat situace, že v průběhu delší doby (např. 48 hodin) kvalifikovaný poskytovatel nezneplatní žádný kvalifikovaný certifikát a nebude mít tedy povinnost aktualizovat svoje CRL minimálně po dobu 48 hodin. Z hlediska bezpečnosti systému nám tato situace nemusí vadit. Co ale v případě, že kvalifikovaný poskytovatel ve své certifikační politice stanoví, že žádosti o ukončení platnosti (zneplatnění) přijímá pouze v omezenou dobu (např. pouze v pondělí od 10 hod. do 12 hod.). Doba mezi podáním žádosti o ukončení platnosti (zneplatnění) a zveřejněním aktuálního CRL by pak mohla být až 1 týden! Zákon však takovou situaci nedovoluje. Dle § 5 odst. 1 písm. b je podepisující osoba povinna **uvědomit neprodleně** poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu. Poskytovatel by tak v našem hypotetickém případě znemožnil podepisující se osobě plnění povinností vyplývajících ze zákona a dopustil by se tak nezákonného jednání. Z toho vyplývá, že kvalifikovaný poskytovatel je povinen provozovat svoji činnost tak, aby **neznemožnil** podepisujícím se osobám podávání žádostí neprodleně po pojmutí podezření ve smyslu § 5 odst. 1 ZoEP a zároveň tato nebyla diskriminována způsobem, který kvalifikovaný poskytovatel k podávání žádostí vyžaduje.

Literatura:

[1] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
[2] Vyhláška č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu
[3] Vondruška, P.: Dostupnost informací o ukončení platnosti a zneplatnění kvalifikovaného certifikátu , Crypto-World 9/2001
[4] Vondruška, P.: Dostupnost informací o ukončení platnosti a zneplatnění kvalifikovaného certifikátu , Crypto-World 11/2001
[5] Prokeš J.: Ukončení platnosti, zneplatnění (a zrušení) certifikátu I., Crypto-World 5/2001
[6] Prokeš J.: Ukončení platnosti, zneplatnění (a zrušení) certifikátu II., Crypto-World 6/2001
[7] RFC 2527 (1999) : "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices
[8] Zákon č. 40/1964 občanský zákoník

E. Eliptické křivky a kryptografie

Ing. Jaroslav Pinkava, CSc., AEC spol. s r.o.

Úvod

Vzhledem k neblaze známým událostem z 11. září tohoto roku došlo k posuvu termínu každoročně pořádané konference ECC (The Workshop on Elliptic Curve Cryptography. Letošní již pátý ročník konference se (místo původního termínu 17-19. září) nakonec konal ve dnech 29-31. října 2001 a to v areálu University of Waterloo (asi 100 km jihozápadně od Toronta).

Organizátory konference byli A. Menezes, E.Teske a S. Vanstone z University of Waterloo (S.Vanstone je zároveň hlavním kryptologem firmy Certicom). Z hlediska kryptografie založené na eliptických křivkách je tato konference vlastně ústřední aktivitou a její obsah poskytuje přehled o současném dění v problematice. Na konferenci bylo přítomno asi 130 účastníků (dvojího typu - z univerzit a z realizačních firem), z toho 25 z evropských zemí.

Přednášky

1. Brian Snow: We need more assurance in security products
2. Darrel Hankerson: Performance comparisons of elliptic curve systems in software
3. Dan Bernstein: A software implementation of NIST P-224
4. Jerome A. Solinas: Some computational speedups and bandwidth improvements for curves over prime fields
5. Raymond Laflamme: Quantum Computing
6. Gerhard Frey: Algebraic-geometric discrete logarithms: An overview
7. Alfred Menezes: Cryptographic implications of Weil descent
8. Florian Hess: An extension of the GHS Weil descent attack
9. Tatsuaki Okamoto: Generic conversions for constructing IND-CCA2 public-key encryption in the random oracle model
10. Dan Brown: A security analysis of the elliptic curve digital signature algorithm
11. Alice Silverberg: Elliptic curves: The state of the art
12. Pierrick Gaudry: Algorithms for point counting on elliptic and hyperelliptic curves
13. Annegret Weng: The CM-method for hyperelliptic curves

Odpoledne posledního (třetího) dne bylo věnováno volným vystoupením:

Rump Session

Berit Skjernaa: Point counting on elliptic curves over finite fields of small characteristics
Robert Harley: Generating secure elliptic curves using the AGM and early abort strategies
Erik Knudsen: Point halving-How it works
Richard Schroeppel: Point halving

Ke konferenci nebyl vydán sborník, ale k většině přednášek lze z webovské adresy http://www.cacr.math.uwaterloo.ca/ stáhnout příslušné prezentace (12 ze 13, chybí již pouze přednáška R.Laflamma ke kvantovým počítačům).

Komentáře k přednáškám

Velmi zajímavou (i když z obecného pohledu, samotných eliptických křivek se netýkala) byla úvodní přednáška Briana Snowa (National Security Agency). Přednáška hodnotila současnou situaci v oblasti IT Security, motivující byla paralela s vývojem automobilového průmyslu.

V počátcích automobilů (příkladem bylo poukázání na situaci v třicátých letech) bylo důležité, že stroj byl vůbec schopen pohybu, pak např. vzhled automobilu a bezpečností jízdních vlastností se téměř nikdo nezabýval. Pokud automobil havaroval, pak pasažéři skoro jistě zahynuli nebo utrpěli váná poranění. Teprve později se tato problematika dostává do popředí a dnes jsou již téměř samozřejmostí bezpečnostní pásy, airbagy, kvalitní pneumatiky, brzdový systém atd. Cílem těchto opatření je samozřejmě ochránit život a zdraví pasažérů a v řadě případů (i když bohužel ne vždy) jsou opatření úspěšná. Další srovnání se přímo nabízejí – např. tanky a bezpečnost výpočetních systémů určených k ochraně informací důležitých z hlediska vojenských a bezpečnostních cílů státu. Snow se dále zabýval rozborem jednotlivých dílčích oblastí (operační systémy, softwarové moduly, vlastnosti hardwaru,…), kterých se problematika bezpečnosti dotýká.

Jedna poznámka k oblasti ochrany dat v USA. Dle odhadu NSA je šifrová ochrana dat dnes z 95 procent používána na neklasifikovaná data a pouze pět procent na data utajovaná dle platné legislativy.

S ohledem na konkrétní aplikace eliptické kryptografie v softwaru měla nesporně největší význam přednáška D. Hankersona (přednášku připravili také čtyři další spoluautoři). Přednáška byla orientována především na **implementace křivek** s parametry definovanými dle doporučení NIST a to jak křivky v prvočíselných tělesech tak i v binárních tělesech. Celou řadu užitečných informací o časových nárocích jednotlivých dílčích algoritmů lze získat ze slajdů k této přednášce. Přednáška také poukazuje na jednotlivé implementační techniky a hodnotí jejich praktický přínos. Zajímavý je jeden ze závěrů (slajd 14), který hodnotí (z hlediska současných technik) softwarové realizace křivek v prvočíselných tělesech jako rychlejší (oproti křivkám zhruba v stejně velkých binárních tělesech).

Některými implementačními technikami pro křivky v prvočíselných tělesech se zabývala i přednáška J. Solinase, známého kryptologa z NSA.

Z hlediska posuzování bezpečnosti eliptické kryptografie hraje momentálně jednoznačný prim rozbor metody **Weilova spádu**. K této metodě vystoupil její autor profesor Frey (Universita Essen, Německo) a zabývali se jí také další přednášející (Menezes, Hess, Silverbergová). Sama metoda je vlastně určitý obecný přístup k řešení problematiky eliptického diskrétního logaritmu a v současné době je přímo aplikovatelná pouze v některých specifických situacích. Přesto zaznělo z úst celé řady účastníků (přednášejících i v diskusi) hodnocení této metody jako současně nejvýznamnějšího trendu v matematice eliptické kryptografie. Je zde třeba podotknout, že se to týká té oblasti teorie čísel, která využívá jeden z nejnáročnějších matematických aparátů dneška.

Pro aplikace eliptických křivek v kryptografii mají stěžejní význam metody **výpočtu řádu křivky** (počet celočíselných bodů eliptické křivky). Přehled o současných metodách poskytla přednáška P. Gaudryho, speciální problematikou se pak zabývala A. Wengová.

Určitě zajímavým osvěžením byla přednáška R. Laflamma, který donedávna působil v Los Alamos a teprve nedávno přešel na univerzitu ve Waterloo. Týkala se hodnocení současného stavu teorie a praxe **kvantových počítačů**. Autor zde ukázal přehled asi 12 technologických implementačních přístupů ke kvantovým počítačům. Jako nejúspěšnější hodnotí NMR (nuclear magnetic resonance), kde se momentálně konají pokusy s qubitovými řetězci v délce sedm (kryptologii dneška začnou ohrožovat teprve řetězce řádově v stovkových délkách). Dle slov přednášejícího lze očekávat praktické výstupy (tj. kvantové počítače pracující s qubitovými řetězci zajímavých délek) teprve tak za dvacet resp. dvacet pět let. Přitom tuto předpověď mohou ovlivnit výsledky dvou typů. Jeden může ukázat některá faktická omezení technik, která vyústí v praktickou nerealizovatelnost kvantových výpočtů. Výsledky druhého typu naopak mohou znamenat nějaký fundamentální objev, který vývoj dané oblasti zásadně ovlivní a uspíší.

Poslední oblastí, které byly věnovány přednášky na konferenci je problematika **prokazatelné bezpečnosti**. Tento nesporně vysoce zajímavý trend současné kryptografie zasahuje dnes již téměř do všech kryptografických aplikací (pozn. – pro zájemce – v prvním čtvrtletí 2002, tomuto tématu bude věnován jeden seminář na MFF). Pan Brown z Certicomu se na bázi tohoto přístupu (prokazatelné bezpečnosti) pokusil zhodnotit DSA a ECDSA. Dle jeho vyjádření to umožňuje formulace některých nových nároků na bezpečnost těchto podpisových schémat, výsledky však ještě nemají definitivní podobu. Je však pravděpodobné, že takovéto výsledky ovlivní i nové podoby norem pro podpisová schémata, které jsou již po nějakou dobu v USA připravovány (jako náhrada za současnou normu FIPS-186). Problematikou se zabýval také T.Okamoto.

Protože některé modely prokazatelné bezpečnosti zasahují již i do oblasti připravovaných norem (Cryptonessie, Cryptrec, ale i materiály P1363) je nanejvýš užitečné nepustit je ze zřetelu. Už jen proto, že základním cílem přístupů prokazatelné bezpečnosti (přes možná některou složitost či nezvyklost používaného matematického aparátu) je zvýšit praktickou bezpečnost dnešních konkrétních aplikací.

Jeden závěrečný citát:

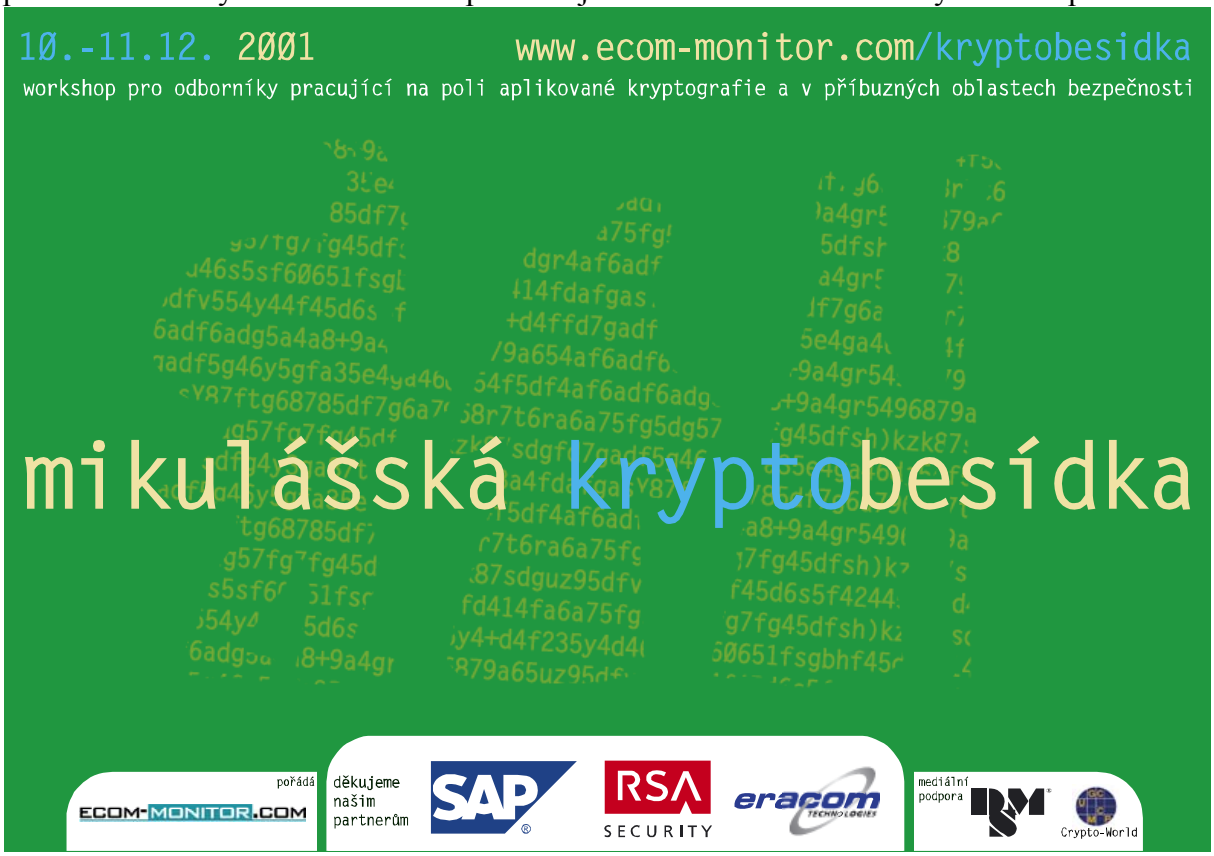
Companies should produce a **„Series of unbroken products“**
instead of **„An unbroken series of products“.**

Brian Snow (NSA) on ECC 2001, Waterloo University

F. Mikulášská kryptobesídka –
Vašek Matyáš, Zdeněk Říha
10. - 11. prosinec 2001, Praha

Chceme vás pozvat na jednu (snad zajímavou :-) akci, která se bude konat za necelý měsíc. Jedním z oficiálních mediálních partnerů této akce je i Crypto-World, druhým je časopis Data Security Management. Toto setkání je organizováno za účelem výměny informací a nápadů mezi odborníky – a to bez zbytečných problémů a starostí s šéfy, (potenciálními) zákazníky a dalšími rozptylujícími faktory. ;-)

10. prosince (pondělí) se sejdeme v pizzerii "PIZZA IL CARNE" u zastávky metra Nové Butovice. Na programu je (mimo registrace) panelová diskuze se zvanými přednášejícími (Bart Preneel a Fabien Petitcolas) a společná večeře s dostatečným prostorem pro neformální výměnu informací s přednášejícími i s ostatními účastníky workshopu.



11. prosince budou prezentovány zvané i nabízené příspěvky, opět s potřebným časem prostorem k diskuzím. V době uzávěrky Crypto-Worldu právě finišuje výběr nabízených příspěvků. Na závěr workshopu proběhne panelová diskuze na téma "*e-podpis a praxe pohledem odborníků*". Druhý den workshopu probíhá v prostorách společnosti SAP.

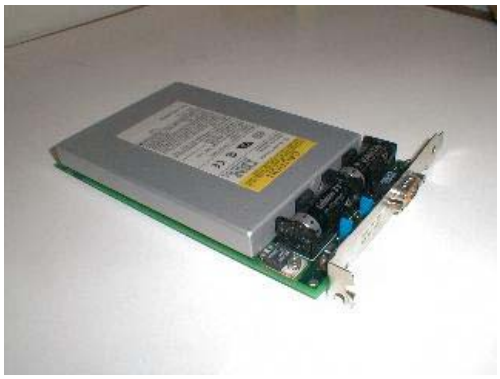
Jedná se nám o uspořádání akce se skutečně aktivní výměnou informací a kapacita workshopu je tedy omezená (70 registrovaných účastníků) – po jejím naplnění již nebude možné přijímat další registrace. Ke 12.11. byla obsazena již téměř polovina kapacity.
Partnery akce jsou společnosti SAP, RSA Security a Eracom Technologies. Podrobné a aktualizované informace, včetně mapek, registrace a brzy i podrobného programu můžete najít na www stránce http://www.ecom-monitor.com/kryptobesidka .

G. Letem šifrovým světem

Vojenská kryptografie IV.

Ve dnech 30.10.-31.10. uspořádal Odbor kryptografické bezpečnosti Vojenského bezpečnostního úřadu Praha ve spolupráci s Vojenskou akademií Brno již tradiční setkání vojenských kryptologů a kryptografů ze státní a komerční sféry. Toto setkání již bylo v pořadí čtvrté. Vlastnímu zahájení programu předcházelo slavnostní předání pozlaceného poháru doc. ing. Oldřichu Pekárkovi, CSc. (VBÚ) za jeho celoživotní zásluhy o českou kryptografii a především za výchovu mnoha českých kryptologů. Tento slavnostní akt byl doprovázen dlouhodobým potleskem cca 100 přítomných účastníků. Mezi přednášejícími byli např. pánové doc.Dočkal, doc.Burda, prof. Lúč, doc.Sobotík, Dr.Klíma, ing.Rosa, Mgr.Vondruška a další. Celkem zde zaznělo 13 příspěvků. Příspěvky byly velice hodnotné a zajímavé. Bohužel k diskusi v oficiálním čase nezbývalo vzhledem k náročnému programu příliš místo. To, co nestihli posluchači během přednášek, mohli si vynahradit v úterý večer, neboť všichni přítomní byli pozváni na večerní setkání v jihomoravském sklípku. Toto krásné překvapení mohlo být zajištěno díky sponzorským darům firmy AEC spol. s r.o. a ICZ a.s..Všichni účastníci dostali vytištěný rozsáhlý sborník přednášek a pořadatelé dále stihli do konce setkání připravit i CD se všemi přednesenými prezentacemi, které si tak účastníci mohli odvést na památku tohoto vydařeného setkání.

Před čtrnácti dny odstartoval svoji činnost nový server věnovaný kryptografii a bezpečnosti pod názvem http://www.krypta.cz . Vedle systematických informací z oblasti kryptologie a informační bezpečnosti server publikuje i články a novinky ze sledované oblasti.Tento projekt s neuvěřitelným elánem začali budovat pánové Michal Till a Jan Kulveit. Server vyniká kvalitním grafickým prostředím (pro ty, kteří nechtějí použít grafické prostředí je umožněn přístup pouze k textové verzi !) a velkým množstvím dobře roztříděného materiálu. Všem čtenářům návštěvu tohoto serveru vřele doporučuji.



IBM 4758 bývá označován jako jeden z nejbezpečnějších kryptografických koprocesorů (hodnocen podle FIPS 140-1 na level 4). Je užíván ve velkých bankovních systémech a dále všude tam, kde je potřeba udržet v bezpečí tajný klíčový materiál. Je navržen tak, aby znemožnil útočníkovi získat uchovávané klíče a uchovávaná data byla přístupná pouze autorizované osobě.

Začátkem listopadu pánové Mike Bond a Richard Clayton z Cambridge University Computer Laboratory oznámili, že našli způsob jak vyexportovat klíče pro DES i pro 3DES z IBM 4758, které pracuje v prostředí IBM ATM (cash machine) a používající podporu "Common Cryptographic Architecture" (CCA). Pro úplnost dodejme, že se jim nepodařilo "rozlomit" certifikované zařízení, ale využili "slabost" systému, který se zařízením komunikuje. Tento software nebyl podle FIPS 140-1 hodnocen. Podrobnosti (včetně popisu jim použitého útoku) naleznete na:
http://www.cl.cam.ac.uk/~rnc1/descrack/attack.html

Máte zájem o příručku "Bezpečná komunikace v otevřené síti (příručka pro paranoiky)" ? Příručku připravil J.Ranum, má celkem 91 stran, v PDF formátu má 2 897 kB a lze ji získat na adrese : http://web.ranum.com/pubs/pdf/securecommunications-2up.pdf . Jedná se o velmi zajímavý přehled. Čtenáře J.Ranum seznamuje s různými možnými útoky. Nejedná se o souvislý text, ale soubor 181 "ppt slidů", které jsou věnovány různým souvisejícím problémům. Doporučuji zvláště studentům.

Pokud pracujete v oblasti PKI nebo dokonce musíte vytvářet certifkační politiku pro CA (poskytovatele certifikačních služeb) a potřebujete ji napsat tak, aby mohla být uznávána mezi různými státy světa, jistě uvítáte, že byla konečně zveřejněna dlouho avizovaná modelová mezistátní certifikační politika PKI (9.11.2001).
Model Interstate PK Certificate Policy /PP : http://www.cryptome.org/micp.doc

---

Na závěr našich toulek jeden "lákavý inzerát".
Kontrašpionážní výcvik.
Naši instruktoři mají léta zkušeností s vyzvědačstvím, kontrašpionáží a s oblastí bezpečnosti a jsou připraveni vám předat své zkušenosti. Kde jinde se můžete setkat s instruktory, kteří pracovali 20 až 30 let v FBI, CIA, DOD nebo KGB?
http://cicentre.com/COURSES.htm

O čem jsme psali v listopadu roku 1999 a 2000

Crypto-World 11/1999
http://cryptoworld.certifikuj.cz/casop1/Crypto11_99.pdf **(312 kB)**
http://www.mujweb.cz/veda/gcucmp/casop1/Crypto11_99.pdf

Crypto-World 11/2000
http://cryptoworld.certifikuj.cz/casop2/Crypto11_00.pdf **(254 kB)**
http://www.mujweb.cz/veda/gcucmp/casop2/Crypto11_00.pdf

H. Závěrečné informace

1. Sešit

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

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

Pokud se zajímáte pouze o sešit Crypto-World, můžete jej najít na lépe dostupné adrese:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.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@uoou.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@uoou.cz (**vondruskap@uoou.cz**)

pavel.vondruska@post.cz

vondruska.p@seznam.cz