Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 1/2001 15. leden 2001

1/2001

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR.

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>240 e-mail výtisků)

OBSAH : **Str.**

Příloha:
trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)
- jedná se o jednu ze tří firem, které věnovaly ceny do krátkodobé soutěže (probíhala od 9/2000 do 12/2000); zbylé dvě firmy byly již představeny ve vánočním speciálním čísle V/2000

A. Je RSA bezpečné ?

Mgr. Pavel Vondruška (ÚOOÚ)

Otázka bezpečnosti algoritmu RSA se běžně redukuje na diskusi o délce klíče. Bezpečnost tohoto systému je však závislá i na správné implementaci, na velikosti soukromého a veřejného exponentu a na mnoha dalších detailech. Vzhledem k tomu, že právě algoritmus RSA hraje klíčovou úlohu v elektronickém podpise, pokusím se v tomto článku poukázat na známé i méně známé útoky, které mohou bezpečnost tohoto algoritmu ohrozit.

1.0. RSA

RSA je šifrový asymetrický systém používaný pro šifrování krátkých zpráv, výměnu klíčů a tvorbu elektronického podpisu. Patří již více jak dvacet let mezi (nepsané) standardy v této oblasti. Většinou využívá klíče délky 512 - 4096 bitů. Algoritmus byl v letech 19777 – 2000 patentovanou metodou americké společnosti RSA Data Security Inc. Jak je známo, název RSA byl vytvořen z počátečních jmen jeho tvůrců : Ron Rivest, Adi Shamir a Len Adleman. Bezpečnost RSA je založena na známé skutečnosti, že je obtížné rozložit velká čísla na prvočinitele (v tomto případě jde o součin dvou velkých prvočísel). Během dvaceti tří let používání byl systém podroben velice důkladné analýze ze strany kryptologů a matematiků a byla objevena řada slabin a možných útoků, kterými lze RSA prolomit nebo alespoň jeho bezpečnost oslabit.

1.1. Popis algoritmu RSA

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

a) nejprve náhodně (a nepredikovatelně) vygenerujeme dvě dostatečně velká prvočísla (jejich přibližná velikost, tj. počet bitů, je zadána) [1]

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 menší 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

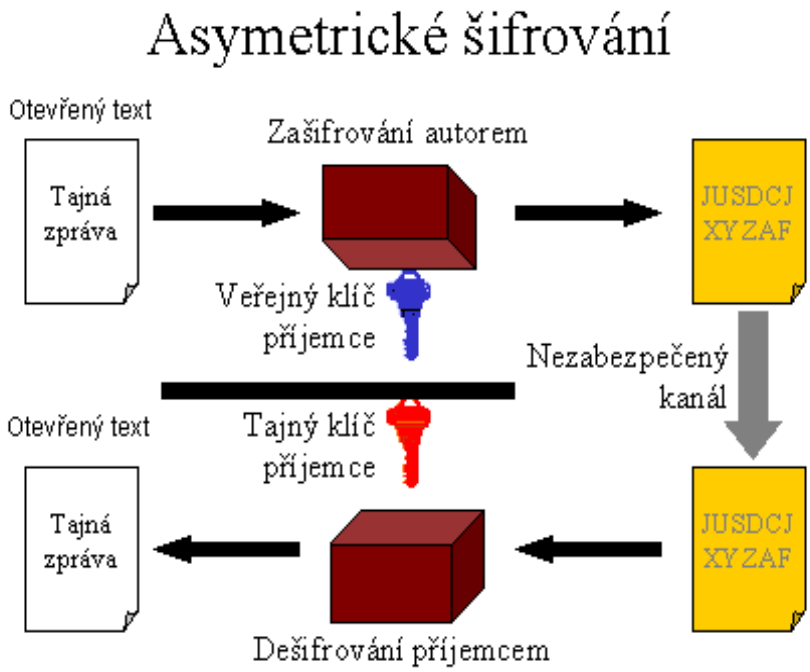
$e*d \equiv 1 \mod \Phi(N)$.

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.



1.2 Popis vlastního šifrování a dešifrování

Popíšeme, jak probíhá vlastní zašifrování a odšifrování. Předpokládejme, že strana B zná autentický veřejný klíč strany A, kterým je (N,e) a zašifrovává zprávu M pro A.
Strana B vyjádří zprávu M jako číslo m, $0 \leq m \leq N-1$ (resp. posloupnost takových čísel).
Dále strana B vypočte

$$c = m^e \mod N$$

a zašle tento šifrový text straně A.

Strana A nyní při dešifraci vypočte pomocí tajného klíče d

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

Výsledkem je skutečně m, což lze dokázat následovně :

Jelikož $e*d \equiv 1 \mod \Phi(N)$, existuje celé číslo k tak, že $ed = 1 + k\Phi(N)$.
Dále, pokud NSD (m,p) = 1, pak podle Fermatovy věty

$$m^{p-1} \equiv 1 \mod p.$$

Umocníme obě strany této kongruence číslem k(q-1) a posléze vynásobíme obě strany rovnice číslem m.
Dostaneme

$$m^{1 + k(p-1)(q-1)} \equiv m \mod p.$$

Pokud je NSD (m,p) = p (druhá možná situace), pak tato rovnost platí rovněž (obě strany jsou rovny nule mod p).

Vždy tedy

$$m^{ed} \equiv m \mod p .$$

Obdobně se dokáže

$$m^{ed} \equiv m \mod q .$$

Odtud plyne

$$m^{ed} \equiv m \mod N,$$

a tedy

$$c^d \equiv (m^e)^d \equiv m \mod N.$$

1.3. Bezpečnost algoritmu

Bezpečnost tohoto algoritmu je založena na složitosti úlohy faktorizace velkých čísel. Tímto klasickým problémem teorie čísel, se zabývají matematici již dlouhá desetiletí, v posledních dvaceti letech i v souvislosti s rozvojem kryptografie (kromě RSA je na stejném problému založeno např. Rabin-Williamsovo schéma, které je součástí normy P1363).

Lze lehce ukázat, že pokud dokáži faktorizovat N, pak samozřejmě dokáži spočítat $\Phi(N)$ a tudíž odvodit z veřejného exponentu e i soukromý exponent d. Obrácená implikace byla dokázána pouze pro Rabin-Williamsovo schéma, nikoliv pro RSA. Tedy zatímco pro RW schéma je úloha kryptoanalýzy stejně obtížná jako úloha faktorizace může být v případě RSA úloha kryptoanalýzy o něco jednodušší.

Přesněji: k "rozbití RSA" nepotřebujeme faktorizaci, stačí vyřešit problém nazývaný RSAP.

RSAP. Nechť p,q jsou prvočísla, N=p*q , a e je číslo takové, že NSD (e, $\Phi(N)$) =1 (kde $\Phi(n)$ značí Eulerovu funkci, e a $\Phi(N)$ jsou nesoudělná) . Úloha zní: 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 RSAP lze přeformulovat jako problém 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.

1.4 Útoky na RSA pomocí faktorizace modulu

Z minulého odstavce plyne, že nejschůdnější známou cestou vedoucí k rozbití RSA je faktorizace čísla N. K určení kryptologické odolnosti RSA použijeme výpočetní složitost faktorizačních algoritmů. Pro vyjádření a ohodnocení jejich složitosti se používá následující

symbolický zápis : $L_q(a,c) = O(\exp((c+O(1))(\ln q)^a * (\ln\ln q)^{1-a}))$ (některé pojmy z teorie složitosti + definice "velkého O" viz [2]).

Dále k ohodnocení složitosti jednotlivých faktorizačních metod budeme uvádět vždy jen dvojici parametrů (a,c).

Faktorizační algoritmy se dělí do tří základních skupin:

1) **Obecné algoritmy, kde složitost závisí na velikosti nejmenšího existujícího faktoru**
V současné době se považuje v této skupině za nejefektivnější ECM (eliptic curve method), složitost lze vyjádřit pomocí dvojice parametrů (1/2, √2), metoda není prakticky použitelná pro čísla, která nemají jeden z faktorů relativně malý (cca 10^{41} , závisí ovšem na výpočetním výkonu).

2) Obecné algoritmy, kde složitost závisí na velikosti faktorizovaného čísla
Všeobecně známý algoritmus kvadratického síta (QS) vytlačila v poslední době metoda "obecného číselného tělesa", general number field sieve (GNFS); složitost lze vyjádřit pomocí dvojice (1/3, 1.92).

Obecně se dá říci, že pro malé hodnoty n (řekněme n < 100 cifer) je metoda QS rychlejší než GNFS. Pro hodnoty n > 130 cifer je účinnější metoda GNFS . V oblasti čísel od 100 do 130 cifer pak výsledek závisí na druhu použitých počítačů, jemnosti programování a na hledaném tvaru rozkladu. Metoda GNFS slaví v posledních letech jednoznačný úspěch při rozkladu velkých těžko rozložitelných čísel. To bylo prokázáno i při rozkladu čísel ze souboru RSA (viz. tabulka z [3]).

Číslo	Datum	MIPS-roků	Dnů P II/450	Metoda
RSA-100	Duben 1991	7	5,67	Quadrqtic-sieve
RSA-110	Duben 1992	75	60,8	Quadrqtic-sieve
RSA-120	Červen 1993	830	673	Quadrqtic-sieve
RSA-129	Duben 1994	5000	4055 (11 let)	Quadrqtic-sieve
RSA-130	Duben 1996	500	405,5	Generalized number field sieve
RSA-140	Únor 1999	2000	1622,2 (4,5)	Generalized number field sieve
RSA-155	Srpen 1999	8000	6488,8 (17 let)	Generalized number field sieve

(MIPS-rok : definován jako výpočet, který zvládne za jeden rok samostatný počítač DEC VAX 11/780)

V roce 1999 bylo demonstrováno, že je prakticky možná faktorizace 512 -bitových čísel. Některé spekulace vedou k domněnkám, že cca za 15 let bude možná faktorizace 768-bitových čísel. Využití jiných technologií v procesu faktorizace (např. optoelektronické zařízení TWINKLE představené v roce 1999 v Praze na konferenci Eurocrypt) by mohlo zvýšit velikosti faktorizovaných čísel [4].

3) Algoritmy vhodné pro speciální situace, kdy má faktorizované číslo (nebo faktor) jisté známé (očekávané) vlastnosti
- Fermatova metoda - používá se k vyhledání faktorů blízkých k √N (proto není vhodné, aby se prvočísla p a q lišila jen "málo")
- Pollardova p-1 metoda
- Williamsova p+1 metoda
  Obě poslední metody jsou vhodné pro čísla, jejichž faktor je o jedničku větší resp. menší než hladké číslo. Tyto metody jsou poměrně účinné, a proto se někdy klade požadavek volit jako faktory N tzv. silná prvočísla. V současné době se však od tohoto požadavku při

generaci prvočísel upouští (bylo dokázáno, že pravděpodobnost výběru čísla, které je blízké hladkému číslu, je prakticky zanedbatelná) .

1.5 Společný modul

Pokud by několik osob mělo klíče (data pro vytváření elektronického podpisu) se stejným modulem, pak generování klíčů by bylo sice rychlé, ale jak dokázal Simmons není tento systém vůbec bezpečný. Každý z účastníků může ze znalosti svého veřejného a soukromého klíče faktorizovat modul a pak vypočítat soukromé exponenty ostatních účastníků z jejich veřejných klíčů (dat pro ověření elektronického podpisu).

V případě použití veřejných klíčů pro šifrování je zde ještě další možný útok. Pokud byla tatáž zpráva zašifrována dvěma různými veřejnými klíči se stejným modulem, existuje jednoduchý postup, který ze znalosti těchto dvou šifrových textů a příslušných veřejných textů umožňuje nalézt původní otevřený text zprávy !

1.6 Multiplikativní vlastnosti kryptosytému

Šifrování i odšifrování pomocí RSA je distributivní vzhledem k násobení, protože platí:
$\forall a,b \in Z , k \in N : (ab)^k \equiv a^k b^k \pmod N$.

Popíšeme si, jak může útočník této vlastnosti využít v případě elektronického podpisu a v případě luštění zašifrovaného textu.

Má-li útočník zprávu M, ke které chce získat podpis nějaké osoby (Boba), tj. hodnotu $M^d \bmod N$, pak může Bobovi předložit místo vlastní hodnoty M , kterou by Bob mohl odmítnout podepsat, jakoby náhodnou hodnotu $M\, c^e \bmod N$, pro nějaké náhodně zvolené c. Z výsledku je pak útočník schopen vypočítat podpis původní zprávy M.

Tento postup se dá výhodně využít pro některé aplikace, jako je systém digitálních bankovek (digital cash), který poskytuje určitý stupeň anonymity jednotlivým účastníkům (mluvíme o tzv. zaslepení - blinding).

V případě šifrování může útočník multiplikativní vlastnosti využít takto : odchytí-li zašifrovanou zprávu C adresovanou Bobovi, může ji pozměnit a Bobovi poslat hodnotu $C\, c^e \bmod N$, pro nějaké c. Bob se pokusí tuto zprávu rozšifrovat, ale výsledkem je hodnota $C^d\, c \bmod N$, která pravděpodobně nedává žádný smysl. Dokáže-li útočník tuto hodnotu získat, například z toho důvodu, že Bob si myslí, že odšifrování neproběhlo dobře, a proto zdánlivě nesmyslnému výsledku nevěnuje dostatečnou ochranu, nebo tak, že Boba přímo nějak přesvědčí, aby mu výsledek poskytnul ("provede analýzu, proč odšifrování neproběhla dobře …"), pak může vypočítat původní otevřený text [5] .

Útočník může diskutované vlastnosti RSA využít také tak, že bude kombinovat existující zašifrované texty nebo digitální podpisy a vytvářet z nich nové [6]. Aby to mělo nějaký praktický význam, je nutné, aby (smysluplné) texty zpráv, které jsou šifrovány nebo podepisovány, měly nějakou multiplikativní strukturu, protože jinak nebude útočník schopen syntetizovat nové smysluplné zprávy. Nicméně Desmedt a Odlyzko [7] ukázali, že získá-li hacker výsledky Bobovy dešifrovací funkce pro přibližně $(L_n\,[1/2,1])^{1/2}$ vhodně zvolených vstupů, pak bude schopen efektivně sám spočítat výsledek dešifrovací funkce pro libovolný vstup.

1.7 Malá hodnota soukromého exponentu

Výpočet mocnin v Z_N je časově náročná operace (složitost je úměrná logaritmu exponentu). Zdá se tedy výhodné volit soukromý exponent d relativně malý (třeba 10x menší než modul N) a tím výrazně zrychlit dešifrování a vytváření elektronických podpisů. M.Wiener ukázal, že tento postup je špatný, umožňuje dokonce vypočítat soukromý exponent pouze ze znalosti veřejného klíče (dat pro ověření elektronického podpisu) !

Přehled známých výsledků
Wienerův útok [8]
Nechť N=p*q je RSA modul a e,d jsou veřejný a soukromý klíč. Dále nechť platí $q < p < 2q$ a $d < 1/3 * N^{1/4}$. Pak lze ze znalosti N a e efektivně vypočítat d.

Boneh a Durfee [9]
Boneh a Durfee našli vylepšení předchozí útoku takové, že lze použít pro větší hodnoty d a e, konkrétně pro $d < N^{1-\sqrt{2}/2} \cong N^{0.292}$ a $e < N^{15/8}$.

Někteří kryptologové se domnívají, že by mohla existovat další vylepšení a to až pro hodnotu $d < N^{1/2}$. Tento odhad nebyl zatím potvrzen a je známým otevřeným problémem.

Z vlastní dřívější praxe mohu potvrdit, že celá řada komerčních programů, které v rámci nabízených služeb také generují veřejné a soukromé klíče, zpravidla neprovádí kontrolu vztahu d,e,N nebo dokonce z důvodu rychlých výpočtů volí úmyslně hodnotu d nízkou (jako jedno z komerčních hledisek se totiž uvádí rychlost šifrování).

1.8 Malá hodnota veřejného exponentu

Podobně by se mohlo zdát výhodné volit malou hodnotu veřejného exponentu a to opět z důvodu urychlení procesu šifrování a ověřování elektronických podpisů. Malá hodnota veřejného exponentu implicitně zaručuje, že hodnota soukromého exponentu bude velká (d nemůže být principiálně menší než $\Phi(N)/e$) . Ukazuje se, že i použití malých hodnot e je riskantní. Na rozdíl od Wienerova útoku a jeho modifikací nejsou již tyto útoky tak účinné a nevedou k úplnému prolomení šifry. V praxi jsou ovšem skutečně malé exponenty často používány. Hodnota e=3 (nejmenší možná) se v komerčních programech běžně vyskytovala. V literatuře se nyní doporučuje hodnota $F_4 = 2^{16} + 1$ (4-té Fermatovo číslo). Tato hodnota je dostatečně veliká, aby známé útoky byly prakticky neproveditelné, a zároveň výhodná, neboť lze vypočítat mocniny $M^e \bmod N$ velice efektivně (pouze 17-ti operacemi v Z_N) .

Možné známé útoky jsou založeny na hledání kořenů polynomů v Z_N . Otázky, za jakých podmínek lze tyto kořeny najít a jakým algoritmem, řeší práce D.Coppersmitha [10]. Problematika je velice náročná a stále se ještě rozvíjí. Existuje celá řada útoků teoretického charakteru (Hastad's Broadcast Attack, Franklin-Reiter Releted Message Attack, Coppersmith's Short Pad Attack, Partial Key Exposure Attack). Při zachování hodnoty veřejného exponentu F_4 a dodržení dalších běžných pravidel (délky textů, neexistující závislosti mezi texty apod.) jsou tyto útoky neúčinné.

1.8.1 Šifrování stejné zprávy různými klíči

Předpokládejme, že zpráva M je rozesílána zašifrovaně k subjektům (B_1,B_2,…B_k). Zpráva je zašifrována postupně veřejnými klíči subjektů B_i označme je (e_i, N_i). A dále nechť je otevřený text zprávy menší než min N_i. Zachytí-li útočník dostatečný počet (e) zašifrovaných zpráv $C_i = M^{ei}$, může zjistit otevřený text M! Z důvodu reálnosti takového útoku – jde o schopnost zachytit dostatečný počet zpráv a provést patřičné výpočty – je možné tento útok provést také jen pro malé hodnoty veřejného exponentu e.

Popsanou situaci lze ještě značně modifikovat [11], nevyžaduje se, aby veřejné exponenty byly totožné a dokonce se připouští, aby byla zpráva M před zašifrováním pozměněna (změna ale musí být luštiteli známa a jde o lineární či polynomiální změny).

1.8.2 Šifrování příbuzných zpráv jedním klíčem

Určité možnosti má útočník dokonce v případě, kdy jsou odesílány některému jedinému adresátovi různé zprávy, mezi kterými je nějaký (luštiteli známý) vztah. To v praxi nastává např. tehdy, kdy jsou zasílány stejné zprávy, které se liší pořadovým číslem nebo časovým údajem [10].

Poznamenejme, že i zde úspěšnost útoku závisí na velikosti veřejného exponentu. Např. při odeslání dvou zpráv s lineární závislostí jednomu adresátovi je šance na úspěch ještě pro hodnoty veřejného exponentu 2^{32} !.

1.8.3 Šifrování stejné zprávy s náhodným doplňkem

Předchozí útok byl založen na tom, že zachycené zprávy byly v nějakém známém (jednoduchém) vztahu. Coppersmith ve svých pracích popsal způsob, jak předchozí útok modifikovat na situaci, kdy útočník zachytí dva zašifrované texty, které odpovídají stejnému otevřenému textu doplněnému o dva různé neznámé doplňky (padding) - tj. řetězec náhodných bitů pevné délky, který je připojen k původnímu otevřenému textu [10,12]. V praxi se to dá docílit např. tak, že útočník zachytí první zprávu a čeká, že odesílatel odešle zprávu novou s jinou (náhodně vygenerovanou) vycpávkou.

Klíčovou podmínkou úspěchu je, že vycpávka nesmí tvořit více než $1/e^2$ bitů celkové délky zprávy.

1.9 Útok proti standardu PKCS #1

Public-Key Cryptographic Standards - PKCS # 1 popisuje postup (symbolicky značený jako rsaEncryption) pro zašifrování dat pomocí kryptosystému RSA.

Ve verzi 1.5 PKCS #1 zasílá strana *A* straně *B* zprávu, která je vytvářena následovně. Otevřená zpráva m je doplněna na potřebný počet bitů (zde budeme používat termín doplněk pro překlad anglického výrazu padding, dle PKCS #1, version 1.5) a tak je získána zpráva *M*. Pak *A* spočte

$$C = M^e \mod N .$$

Strana *B* spočte

$$M' = C^d \mod N,$$

a odstraněním doplněných bitů (doplňku) získá zprávu *m´*. Přitom strana *B* analyzuje tento doplněk a pokud jeho vlastnosti odpovídají očekávání, zprávu přijme, a obráceně. Označme toto rozhodnutí *R*; *R=1*, pokud je doplněk správný, *R = 0*, pokud je doplněk nesprávný.

V Bleichenbacherově útoku narušitel E (eavesdropper) se vydává za stranu *A* a zasílá straně *B* speciálně vytvářené zprávy. Z reakce strany *B* zjišťuje, zda doplněk zprávy je či není správný. Z toho, jak byl dle PKCS 1, v.1.5 tento doplněk vytvářen, získá pak potřebné informace.

Např. pro modul RSA v délce 1024 bitů útok vyžaduje zhruba 1 000 000 volených šifrových textů (pro modul v délce 1025 bitů stačí dokonce méně než 10 000 těchto šifrových textů). Obdobný útok lze zformulovat i proti jiným analogickým protokolům např. SSL v.3.0. Tento odstaveček byl zpracován podle [13].

1.10 Útoky na vlastní implementace RSA

Tyto útoky mohou být účinné jen tehdy, když útočník má možnost sledovat funkci zařízení ve kterém se provádí šifrování nebo elektronické podepisování textů. Příklady toho, co se útočník snaží sledovat a použít k útoku na příslušnou část implementace RSA, jsou : spotřeba elektrické energie během výpočtu (power analysis [14]), sledování času (timing attack [15]), který implementace potřebuje při dešifrování textu, měření elektromagnetického vyzařování (PEM).

1.11 Analýza chyb

Během odšifrování textu (tento postup se skládá z velkého počtu elementárních operací) může dojít k chybě. Příčinou takové chyby může být chybný návrh, zásah do softwaru nebo hardwaru, krátkodobá změna napájení nebo synchronizace, zvýšená teplota, ionizující záření apod. Přitom tyto vlivy mohou vzniknout jak nahodile, tak i záměrně. Boneh, DeMillo a Lipton popsali způsoby, jak výskyt těchto chyb využít při snaze ohrozit bezpečnost RSA [16].

Z informací předních kryptologů vyplývá, že právě tato metoda je velice účinná a útoky i proti speciálním čipovým kartám přináší stále významné kryptoanalytické výsledky.

1.12 Útok pomocí kvantového počítače

Na závěr našeho malého přehledu známých a méně známých útoků na RSA uvedu často v literatuře popularizovaný útok pomocí hypotetického kvantového počítače. V současné době existuje 5-ti qubitová verze takového počítače a i ti nejoptimističtější odhady hovoří o dvaceti až třiceti letech výzkumu, než bude jasné, zda takový počítač bude prakticky sestrojen nebo ne. Co by jeho realizace z hlediska RSA znamenala ?

Kvantový počítač (na rozdíl od klasického) se nachází během výpočtu v superpozici všech svých možných stavů. Každé takové superpozici přísluší určité rozdělení pravděpodobnosti ovlivňující výsledek případného čtení hodnot, které jsou určeny tím, jak jsou vzájemně provázány (entangled).

Pozoruhodný výsledek, který by mohl znamenat konec RSA, dokázal v roce 1994 Shor [17]. Ve své práci uvedl pravděpodobnostní algoritmus, kterým by bylo možno za

pomoci kvantového počítače provést faktorizaci libovolného čísla N v očekávaném čase, který je polynomiální vzhledem k počtu bitů čísla N.

Literatura

[1] P.Vondruška, Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla. Crypto-World 6/2000

[2] P.Vondruška , P=NP aneb jak si vydělat miliony!. Crypto-World 9/2000

[3] P.Vondruška, Faktorizace - přehled. Přednáška z informační bezpečnosti na MFF UK Praha, http://www.mujweb.cz/veda/gcucmp/mff/

[4] P.Vondruška, TWINKLE (Faktorizace velkých čísel pomocí zařízení TWINKLE). Přednáška z informační bezpečnosti na MFF UK Praha, http://www.mujweb.cz/veda/gcucmp/mff/

[5] M. Joye and J.-J. Quisquater, On the importance of securing your bins: The garbage man-in-the-middle attack, Proc. of the 4th ACM Conference on Computer and Communications Security, 135-141, ACM Press, 1997

[6] V. Shoup, Why Chosen Ciphertext Security Matters, Technical Report RZ 3076, IBM Research Division, Zurich Research Laboratory, 1998

[7] Y. Desmedt and Y. Odlyzko, A chosen text attack on the {RSA} cryptosystem and some discrete logarithm schemes, H. C. Williams, Advances in Cryptology, CRYPTO '85, volume 218, Lecture Notes in Computer Science, 516-522, Springer-Verlag, 1985

[8] M.Wiener. Cryptoanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36, 553-558, 1990

[9] D. Boneh and G. Durfee, New Results on the Cryptanalysis of Low {RSA} Exponent, EUROCRYPT '99, 1-11, Springer-Verlag, 1999

[10] D. Coppersmith and M. Franklin and J. Patarin and M. Reiter, Low-exponent {RSA} with related messages, EUROCRYPT '96, 1-9, Springer-Verlag, 1996

[11] J.Hastad, Solving simultaneous modular equations of low degree. SIAM J. of Computing, 17, 336-341, 1988

[12] D. Coppersmith, Finding a Small Root of a Univariate Modular Expression, Technical Report RC-20223, IBM Research Division, T.J. Watson Research Center, 1995

[13] J. Pinkava, Kryptografie a normy I. (PKCS #1), Crypto-World 9/2000

[14] P. Kocher and J. Jaffe and B. Jun, Differential Power Analysis, CRYPTO '99, 388-397, Springer-Verlag

[15] P. Kocher, Timing Attacks on Implementations of {Diffie-Hellman}, {RSA}, {DSS}, and Other Systems, CRYPTO '96, 104-113, Springer-Verlag, 1996

[16] D. Boneh and R. DeMillo and R. Lipton, On the importance of checking cryptographic protocols for faults, EUROCRYPT'97, 37-51, Springer-Verlag, 1997

[17] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124 ,1994

[18] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing, 26, 1484-1509, 1997

[19] D. Boneh, Twenty years of attcks on the RSA cryptosystem. Notice of the AMS, 46, 203-213, 1999

[20] P.Kaňkovský, Útoky na kryptosystém RSA, seminář MFF, 1999

[21] P.Vondruška, Přehled možných útoků na RSA, odborný seminář Vojenská kryptografie III, VBÚ Praha, 2000

B. Připravované normy k EP v rámci Evropské Unie

Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)

Celkový přehled

Práce odborných skupin navazují na Final Report ICTSB European Electronic Signature Standardization (http://www.ict.etsi.org/eessi/Final-Report.pdf).

V návaznosti na tuto závěrečnou zprávu byla Evropskou komisí předložena a Evropským parlamentem přijata (30.11.1999) Směrnice Evropské Unie pro elektronické podpisy (http://www.ict.etsi.org/eessi/e-sign-directive.pdf).

Toto jsou dva základní dokumenty, ze kterých potom vychází další postupy. První z nich komplexně vytyčuje celkovou strategii Evropské Unie při řešení problematiky elektronických podpisů. Ukazuje nezbytné směry v legislativě a především v oblasti norem resp. dalších nezbytných aktivit. Jeho základní závěry jsou formulovány následovně:

1) převzetí resp. vývoj průmyslových norem by mělo maximálně zmenšit potřebu detailizace zákonů a vyhlášek v dané oblasti;
2) normy jsou nezbytně nutné a všude, kde je to možné, je třeba preferovat odkazy na existující mezinárodní normy před vývojem nových norem;
3) požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů;
4) podepisovací prostředky (produkty), pokud vyhovují požadavkům Direktivy, musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí pod EN 45000 (Evropské akreditační schéma);
5) je třeba vytvořit společný referenční bod na základě definice výchozí množiny technologických komponent, který bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty;
6) vzhledem k poskytovatelům certifikačních služeb je třeba použít vhodné bezpečnostní normy:

- obecné zásady v oblasti bezpečnosti (např. BS7799 č. 1 a č. 2),
- specifikace bezpečnostních požadavků vzhledem k důvěryhodným systémům, které tito poskytovatelé používají; první požadavky v této oblasti se týkají především kryptografických modulů (např. FIPS 140-1) a využití rizikové analýzy,
- výchozí certifikační politika pro poskytovatele certifikačních služeb – je doporučováno vyjít z materiálu IETF PKIX – rfc. 2527,
- obdobně pro poskytovatele služeb v oblasti časových razítek je třeba provést specifikaci požadavků vzhledem k jejich politice;

7) vzhledem k produktům sloužícím k vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:

- specifikace bezpečnostních požadavků vzhledem k důvěryhodným hardwarovým zařízením, která jsou použita jako bezpečná zařízení pro vytváření podpisů (FIPS 140-1, Common Criteria – ISO 15408),
- specifikace pro vytváření elektronických podpisů (včetně uživatelova interface) a specifikace produktů a postupů k ověřování podpisů;

8) je nezbytná koordinace jednotlivých aktivit v oblasti norem;
9) z hlediska interoperability jsou nezbytné následující normy:

- technické normy pro syntaxi a kódování elektronických podpisů (včetně vícenásobných podpisů); je doporučováno vyjít z rfc.2315,

- operativní protokoly pro řízení PKI (rfc skupiny PKIX),
- profily kvalifikovaných certifikátů na bázi X.509.

Směrnice Evropské Unie pro elektronický podpis byla vyvíjena několik let – existovala v podobě draftu. Nakonec ji 30.11.1999 schválil Evropský parlament. Přitom členské země EU jsou povinovány uvést své zákony, vyhlášky a administrativní postupy v platnost do souladu s touto Směrnicí do 19. července 2001. Směrnice byla formulována tak, aby byly naplněny následující tři základní principy:

I. Technologická neutralita
II. Vydávání oprávnění pro poskytovatele certtifikačních služeb není direktivně omezeno žádným schématem
III. Nezbytnost rozpoznání zákonné platnosti elektronických podpisů

ETSI
(ETSI Electronic Signatures and Infrastructures - EESSI Program)

V první fázi prací byl zpracován dokument určující osnovu dalších prací Electronic Signature Report (http://docbox.etsi.org/tech-org/security/open/el-sign/ESRep042.pdf) . Druhá fáze prací započala na počátku roku 2000 a zahrnuje (dokument Workplan) následující okruhy problémů:

Policy Requirements for CSPs Issuing Qualified Certificates;
Qualified Certificates Profile;
Time Stamping Profile;
Electronic Signature Formats.

První ze série norem „ETSI standard ES 201 733 (**Electronic Signature Formats**)" byla již schválena v květnu 2000. Obsahuje zejména definice různých formátů elektronických podpisů v návaznosti na používání časových značek (podrobněji např. v článku J. Pinkava: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, březen 2000).

Samotnému procesu vytváření časových značek je věnována norma **Time Stamping Profile**, která se opírá především o dokument Internet X.509 Public Key Infrastructure Time Stamp Protocols (v současné době je nejnovější draft-ietf-pkix-time-stamp-12.txt). Dokument byl již také schválen, dostal označení TS 101 861 a bude opublikován jakmile se příslušný draft stane dokumentem RFC.

V normě **Qualified Certificates Profile** jsou na podobu kvalifikovaného certifikátu kladeny některé základní doplňující nároky. Např. v poli, kde je označen vydavatel certifikátu musí být obsaženo i jméno vydávající země (v příslušném atributu). V profilu musí být obsaženy následující údaje:

- formulace, že certifikát je vydán jako kvalifikovaný certifikát;
- formulace omezující hodnotu transakce pro kterou lze certifikát využít;
- formulace ukazující časový interval po který je archivována informace poskytnutá uživatelem při registraci.

Dokument byl již schválen, dostal označení TS 101 861 a byl opublikován v prosinci 2000.

Posledním z těchto dokumentů je norma zabývající se požadavky na politiku poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty - **Policy Requirements for CSPs Issuing Qualified Certificates.** Toto je samostatný dokument upřesňující požadavky na CP (certifikační politiku) a CPS (certifikační prováděcí směrnici) poskytovatelů certifikačních služeb - životnost klíčů, certifikátů, management certifikátů,

bezpečnostní aspekty, atd. Svojí filosofií vychází dokument z RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
Dokument byl již schválen, dostal označení TS 101 456 a byl opublikován v prosinci 2000.
S aktuálním stavem se lze seznámit na adrese http://www.etsi.org/sec/el-sign.htm .

CEN ESSI

V současné době jsou prováděny práce pro zpracování následujících pěti dokumentů:

Security Requirements For Trustworthy Systems and Products
Security Requirements for Signature Creation Devices
Signature Creation Environment
Signature Verification Process nad Environment
Conformity Assessment of Products and Services for Electronic Signatures

Aktuální informace lze nalézt na adrese: http://www.ni.din.de . Zde došlo na posledním jednání (E-SIGn Workshop, 20-21.11.2000) k posuvu obsahu jednotlivých dokumentů, odsud pramení i změna jejich názvů.

První z dokumentů - **Security Requirements for Trustworthy Systems and Products** - se zabývá bezpečnostními požadavky na důvěryhodné systémy poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty. Jedním ze závěrů projednaných v listopadu je rozhodnutí, že bude zpracován nový dokument - pracovní název „*Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems*“. První draft bude k dispozici v lednu 2001 a v březnu 2001 bude tento materiál projednán. Bylo zde konstatováno, že je problém odkazovat se v Evropě na dokument (FIPS 140-1), který není uznáván jako evropská norma. Současně s tím vzniká i problém evaluace produktu dle dokumentu FIPS. Z hlediska obsahu FIPS 140-1 je otázkou nakolik lze požadavky v něm formulované vztáhnout i na specifika certifikačních autorit. Nový dokument bude vycházet z formátu a obsahu ISO 15408 (Barcelona, říjen 2000) a měl by tvořit celosvětový základ pro evaluace. Byly stanoveny oblasti, kterých se bude chystaný dokument týkat.

Velice důležitou je norma **Security Requirements for Signature Creation Devices**, tj. norma stanovující požadavky na bezpečný podpisový nástroj (v duchu terminologie Směrnice EU o elektronickém podpisu a i našeho zákona o elektronickém podpisu).
Poznámka.: Momentálně existují dvě verze tohoto dokumentu – EAL 4 a EAL4+, které se tudíž (jak ukazuje název verze) liší v nárocích na bezpečné podpisové zařízení. Při jednání k tomuto dokumentu došlo totiž k rozporným stanoviskům při formulaci požadavku vzhledem k zranitelnosti evaluovaného podpisového prostředku. Podle EAL 4 (Common Criteria) stačí požadovat, aby objekt evaluace byl rezistentní vůči útokům narušitele „s nízkou schopností útočit“. Oproti tomu zpracovatelé dokumentu přišli s návrhem, aby zde byla použit požadavek, aby objekt evaluace byl rezistentní vůči útokům narušitele „s vysokou schopností útočit“. Na jednání nedošlo k dohodě a nakonec bylo rozhodnuto, že vedení EESSI má přijít před Evropskou komisi paralelně s oběma návrhy.

Problematika **Signature Creation Environment** - zde je k dispozici zatím pouze materiál „*Security Requirements for Signature Creation Systems*“ (říjen 2000) a shrnuty komentáře k tomuto materiálu, nová verze zatím není k dispozici.

V dokumentu je mimo jiné řečeno: Systém na vytváření podpisů (SCS) bude obsahovat specifické komponenty ve vztahu k důvěryhodnému prostředí a k vlastním aplikacím. Důvěryhodnými komponentami jsou všechny závazné komponenty jako:

· SDV - (Signer´s Document Viewer) používáno pro prohlížení podepsaných dokumentů;
· SAV - (Signature Attributes Viewer) používáno pro prohlížení atributů podpisu;
· SIC - (Signer Interaction Component) pomocí této komponenty probíhá interakce podpisující strany s SCS, tak, aby bylo vytváření podpisu pod kontrolou uživatele;
· SAC - (Signer´s Authentication Component) - to je např. čipová karta s PINem, která je používána k autentizaci podepisující strany na základě autentizujících dat anebo biometrických vlastností takovou cestou, že výsledek lze porovnat s hodnotou uloženou v SSCD.
· DHC - (Data Hashing Component) - vytváří dat, která mají být
· SSC - (SSCD/SCS Communicator) řídí interakce mezi SCS a SSCD;
· SSA - (SSCD/SCS Authenticator) ustavuje důvěryhodnou cestu mezi SSCD a SCS.

Poznámka : SSCD = Secure Signature Creation Device.

Aplikačními specifickými komponentami jsou:

-SDC - (Signer's Document Composer) - např. textový editor, sloužící pro vytváření, výběr dokumentu podepisující osoby a jejích atributů.

-CCV - (Certificate Content Viewer) - ten dokáže zobrazit úplný obsah certifikátu podepisující osoby.

-SDOC - (Signed Data Object Composer) - přetváří složky podepisovaného objektu do bitového řetězcea jeho výstupem je určitý normalizovaný formát (ETSI Electronic Signature Formats Document);

-CSPC - (Certification Service Provider Interaction Component) používán pro získání certifikátu podepisující strany či získání časové značky;

-SHI - (SSCD Holder Indicator) zobrazuje jméno majitele SSCD.

Požadavky na ověřování elektronického podpisu stanoví norma **Signature Verification Process nad Environment**. Jsou zde analyzovány různé aspekty verifikačního procesu (časové značky, kvalifikované certifikáty), popis jednotlivých komponent verifikačního systému, příklady různých prostředí a zformulovány požadavky na systém verifikující podpisy z řady hledisek (právní aspekty, atd.). Je zde také analýzována problematika vícenásobných podpisů a otázky dlouhodobé archivace podpisů.

Poslední materiál **Conformity Assessment Products and Services for Electronic Signature** je věnován otázkám harmonizace implementací norem pro elektronické podpisy – slouží zejména jako příručka certifikujícím a testujícím laboratořím.

Týká se čtyř základních oblastí:

- služeb CA a procesů navazujících na řízení PKI, informační bezpečnosti, organizační spolehlivosti ve vztahu ke kvalifikovaným certifikátům;
- systémů pro vytváření elektronických podpisů ;
- procedur pro verifikaci podpisu;
- bezpečných podpisových prostředků.

V současné době zatím ještě neexistují definitivní verze těchto dokumentů.

C. Kryptografie a normy

Jaroslav Pinkava, Josef Krčál (AEC spol. s r.o./ Norman Czech Republic)

Díl 5.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #9, PKCS #10, PKCS #11, PKCS #15, PKCS #12

Úvod

V tomto díle našeho seriálu budou uvedeny zbývající PKCS normy s pořadovými čísly 9-12 a 15. Některé z těchto dokumentů mají stěžejní význam pro práci např. s čipovými kartami, zejména normy PKCS#11 a PKCS #15 jsou zde ústředními, ale týká se to i PKCS#12.

PKCS #9

Norma nese název „Selected Object Classes and Attribute Types" a v současné době její poslední verze má číslo 2.0. Z anotace: Dokument definuje pomocnou třídu objektů pkcsEntity a určité typ atributů pro užití v této třídě. Jsou zde rovněž definovány atributové typy v návaznosti na PKCS#7 (a také S/MIME CMS) – digitální podpis zpráv, PKCS#10 – žádost o certifikát a PKCS#15 (kryptografické tokeny). Tato typy jsou v normě následně vyjmenovány (kapitola 5). Příloha A obsahuje příslušnou notaci ASN, příloha B pak BNF definice tříd objektů a jednotlivých typů atributů v návaznosti na užití v LDAP.

PKCS #10

Poslední verze PKCS#10 pochází z května 2000 a je označena jako verze 1.7. Jejím úkolem je popis syntaxe žádosti o certifikát. Tato žádost obsahuje unikátní jméno (distinguished name), veřejný klíč a volitelně množinu atributů, toto je podepsáno pak entitou žádající o certifikát. Žádost o certifikát je zasílána certifikační autoritě, která na jejím základě vytvoří X.509 certifikát. Určitý seznam použitelných atributů je přitom dán v PKCS#9.

Žádost o certifikát sestává ze tří částí: informační část žádosti (certification request information), identifikátor podepisujícího algoritmu a digitální podpis informační části žádosti. Informační část žádosti obsahuje unikátní jméno entity (distinguished name), veřejný klíč entity a sadu atributů, která je zdrojem dalších informací o entitě.

Konstrukce žádosti probíhá v těchto krocích:

1. Vytvoří se informační část žádosti (**CertificationRequestInfo**)
2. Tato je podepsána soukromým klíčem entity,
3. Spojí se všechny tři výše uvedené části (informační část, identifikátor algoritmu a podpis) a je vytvořena žádost o certifikát.

Certifikační autority při zpracování této žádosti nejprve provede autentizaci požadující entity a ověří její elektronický podpis, pokud je žádost platná, zkonstruuje digitální certifikát dle X.509 (obsahující unikátní jméno, veřejný klíč, jméno vydávající strany, pořadové číslo v rámci dané CA, dobu platnosti a podpisovací algoritmus, popř. atributy dle PKCS #9).

PKCS #11 a PKCS #15

Tyto normy jsou orientovány především na práci s čipovými kartami. PKCS #11 definuje tzv. Cryptographic Token Interface (CRYPTOKI- Cryptoki.dll). Je to nejrozsáhlejší materiál řady PKCS a obsahuje popis aplikačního programového rozhraní (API) k zařízením, která obsahují kryptografickou informaci a provádí kryptografické funkce. Rozhraní si klade za cíl být technologicky nezávislé (vzhledem k libovolnému typu zařízení) a rovněž tak je jeho cílem umožnit sdílení jednotlivých zdrojů (pro více aplikací, které přistupují k více zařízením). Přitom norma pracuje s pojmem kryptografického tokenu jako obecného zařízení. V dokumentu jsou následně popsány typy dat a funkce, které má přístupné aplikace požadující nějakou kryptografickou službu (popis používá jazyk ANSI C) – tento konkrétní popis je obsahem většiny normy.

Cryptoki vlastně odděluje aplikaci od podrobností používaných kryptografickými zařízeními na základě jednotného rozhraní. Poslední verze normy již podporují velký počet jednotlivých kryptografických mechanizmů a jsou rovněž tak otevřeny k připojování nových mechanizmů.

Nejnovější verze normy PKCS #11 je verze 2.11, která byla opublikována v listopadu 2000. Je orientována na kryptografická zařízení individuálních uživatelů, nemá tedy v sobě prostředky k rozlišení vícenásobných uživatelů. Tj. předpokládá se existence klíčů jediného uživatele a určitého malého počtu certifikátů k tomuto klíči. Existují ještě další klasifikace objektů (např. objekty tokenové a oproti nim „session“ objekty, které mají kratší životnost, nebo rozlišení na objekty veřejné a soukromé dle požadavku na vstupní práva, atd.).

Cryptoki uvažuje token jako zařízení, které ukládá objekty a může provádět kryptografické funkce. Cryptoki definuje tři třídy objektů: data, certifikáty a klíče. Objekt data je definován aplikací. Objekt certifikát ukládá certifikát a objekt klíč ukládá kryptografický klíč. Klíč může být veřejný, soukromý resp. tajný, přitom existují subtypy těchto typů dle užitého specifického kryptografického mechanizmu.

Jsou rozlišovány dva typy uživatelů, jedním z nich je Bezpečnostní Důstojník (SO – Security Officer) a druhým normální uživatel. Pouze normální uživatel má přístup k soukromým objektům v tokenu a tento přístup je umožněn po proběhnutí autentizace tohoto uživatele. SO má za úkol inicializovat token, nastavit uživatelovo PIN a může manipulovat s určitými veřejnými objekty. Obvyklý uživatel se nemůže přihlásit do té doby než SO nastavil uživatelovo PIN.

Pokud se týká normy PKCS #15 – Cryptographic Token Information Format Standard - pak poslední verze (červen 2000) nese označení 1.1 a jsou k ní připojeny některé doplňky (Technical Corrigendum a Conformance Profile Specifikations).

Norma PKCS #15 se zabývá vlastními kryptografickými tokeny a definuje k tomu čtyři obecné třídy objektů. klíče, certifikáty, autentizační objekty a datové objekty.

Obecně kryptografické tokeny (jako jsou čipové karty) jsou v zásadě bezpečné počítačové platformy vhodné k tomu, aby přispěly k bezpečnostním a ochranným prvkům aplikací. Obhospodařují autentizační informace (digitální certifikáty), problematiku autorizace a samotné kryptografické klíče. Jsou schopny zajišťovat bezpečné ukládání (a mít i odpovídají výpočetní kapacitu) pro:

- soukromé klíče;
- čísla účtů a uloženou hodnotu;
- hesla a sdílená tajemství;
- autorizace a oprávnění.

Spolu s tím, řada z těchto tokenů disponuje i určitými možnostmi z hlediska zpracování těchto informací. Přitom se tato informace nedostává do prostředí, kde by ji mohly

narušit některé nepřátelské vlivy (trojské koně, viry, atd...). To je důležité zejména při provádění určitých operací jako jsou:

- generování digitálních podpisů, používání soukromých klíčů, osobní identifikace
- autentizace v síti na základě sdíleného tajemství
- udržování elektronické podoby hodnot
- přenositelná povolení pro použití off-line.

Cílem dokumentu je:

- umožnit interoperabilitu mezi komponentami, které fungují na různých platformách (nezávislost na platformě);
- umožnit aplikacím, aby mohly těžit z využívaní produktů a komponent pocházejících od různých dodavatelů;
- umožnit užití pokroku v technologiích bez nutnosti přepisu softwaru na aplikační úrovni;
- udržet konzistenci s existujícími příbuznými normami, přitom rozšíření mimo jejich rámec probíhá pouze tehdy, pokud je to nezbytné a praktické.

Pro dosažení těchto cílů specifikuje dokument formát souborů a adresářů, který je používán pro ukládání informací bezpečnostního charakteru na kryptografickém tokenu. Tento formát má následující charakteristiky:

- jeho dynamická struktura umožňuje implementace na široké škále médií (včetně např. karty pro ukládaní sumární hodnosty);
- umožňuje na jedné kartě koexistenci více aplikací;
- podporuje ukládání libovolného typu objektů (klíče, certifikáty a data);
- podporuje vícenásobný PIN, pokud sám token toto podporuje.

Každá ze čtyř výše zmíněných tříd objektů má podtřídy. Např. klíče mohou být: soukromé klíče, tajné klíče, veřejné klíče, atd. Všechny objekty mají řadu atributů – tyto jsou podrobně definovány v kapitole 6. dané normy.

Ústředním smyslem PKCS #15 je ovšem již vlastní spolupráce s tokeny. Např. pro chipové karty (v návaznosti na normy ISO7816-4,8) jsou formulovány základní příkazy k obsluze souborů a adresářů (Files & Dirs & SecurityRelatedCommands).

Na Token je užitečné ukládat klíče, pomocí CardOS znemožnit jejich čtení, a umožnit jejich použití (šifrovací primitiva) přímo na kartě. Toto je podstatný krok k bezpečnosti, spolu s řízením přístupu k těmto funkcím pomocí autentizace PINem, případně PIN může být pro každý klíč jiný.

PKCS#15 přináší návrh, jak na kartu umístit soukromé klíče a ceritfikáty do souborů a adresářů dle ISO7816, a její dodržení zajišťuje dostatečné informace pro nezávislé aplikace, a ty jim umožní použít na kartě uložené klíče a certifikáty, a případně na kartu některá další data uložit bez negativního dopadu na prvotní aplikaci.

Využívá se přitom pomocných datových souborů se zde (v PKCS#15) definovanou strukturou, a obsahem těchto souborů jsou doplňující údaje k primárním souborům (klíče a certifikáty), a jejich identifikátor (cesta k nim). Na následujícím schématu je znázorněn postupný přístup k jednotlivým souborům.

```
EF-Dir:
 -> App1, App2, ...

App1:
 ODF:
  -> PuKDF -> PubKey1, PubKey2, ..
```

-> PrKDF -> PrivKey1, PrivKey2, ...
-> CDF -> CERT1, CERT2, ...
-> AODF -> PIN1, PIN2, ...
...

Doplňující údaje v xxxDirectoryFile(s) umožňují přiřadit k sobě odpovídající klíče, certifikáty, PINy a podobně. Jsou zde též identifikátory algoritmů klíčů, minimální a maximální délka PINu a podobně.

Soubory s obsahem kódovaným dle DER, přístupová práva definuje uživatel:

EF-Dir (2F00)
DF-Application (5015)
EF:
ObjectDirectoryFile (5031)
TokenInfo (5032)
UnusedSpace (5033)

PrivateKeyDirectoryFile (4402)
PrivateKey1/2 (4B01/2) (no access!)
CertificateDirectoryFile (4403)
Certificate1/2 (4331/2) (CERT store)
AutenticateObjectDirectoryFile
Secret keys, data objects

Konečně detailním konkrétním popisem čipových karet se zabývá výše zmíněná ISO norma ISO/IEC 7816. V současné době tato norma má celkem deset částí (podrobněji v přehledu ISO norem).

Tato norma je již orientována na víceméně fyzické charakteristiky karet, způsoby kontaktů, elektrické signály a přenosové protokoly a další bezprostředně navazující datové operace. Např. z hlediska pohledu využívání příkazů pro práci s bezpečnostními objekty je ústřední část 8, atd. Norma ISO/IEC 7816 sestává z následujících částí:

- Part 1: Physical characteristics
- Part 2: Dimensions and location of the contacts
- Part 3: Electronic signals and transmission protocols
- Part 4: Interindustry commands for interchange
- Part 4: Amd 1:1997 secure messaging on the structures of APDU messages
- Part 5: Numbering system and registration procedure for application identifiers
- Part 5: Amd 1:1996
- Part 6: Interindustry data elements
- Part 6: Cor 1:1998

- Part 6: Amd 1:2000 IC manufacturer registration
- Part 7: Interindustry commands for Structured Card Query Language (SCQL)
- Part 8: Security related interindustry commands
- Part 9: Additional interindustry commands and security attributes
- Part 10: Electronic signals and answer to reset for synchronous cards

PKCS #12

Toto je vlastně poslední norma z řady PKCS o které budeme hovořit v našem seriálu (PKCS#13 vlastně ještě nebyla vydána, PKCS#14 neexistuje a o PKCS#15 jsme již hovořili - současně s PKCS#11).

Norma vznikla v roce 1999 nejprve v draftu a v současné době existuje její verze 1.0 (červen 1999).

Norma popisuje syntaxi, která je používána k transferu informace týkající se osobní identity - např. soukromé klíče, certifikáty, různá tajemství a rozšíření (extensions). Podpora této normy umožňuje zařízením, aplikacím, vyhledávačům (browserům) atd. importovat, exportovat a používat jednu konkrétní dávku takovýchto informací vztahujících se k osobní identitě. Může existovat několik módů takovéhoto převodu - kriteriem jsou hlediska utajení a integrity. Nejbezpečnější mód vyžaduje použití jak na výchozí tak na cílové straně důvěryhodné dvojice veřejný klíč / soukromý klíč (pro digitální podpis resp. zašifrování). Popisované módy se ještě liší v tom, zda je použito heslo a odsud odvozený klíč resp. MAC anebo je použita kryptografie s veřejným klíčem. Konkrétní formáty jsou odvozeny z PKCS#7 a PKCS#8. Norma je určena k použití jak pro software tak i pro hardware.

Závěr

V prvních pěti částech našeho seriálu jsme se věnovali normám PKCS firmy RSA Security Inc. Tyto normy jak již bylo řečeno jsou dnes velice široce používány a zahrnují přitom poměrně velmi široké spektrum problematik.

Čím bude náš seriál pokračovat? Je nyní celá řada možností. Např. jít jaksi do prvopočátků a věnovat se samotným algoritmům (normy P1363 pro systémy s veřejným klíčem, AES -Rijndael) nebo se spíše orientovat do komunikačních technologií (rfc a drafty IETF), popř. aktuální jsou určitě i jiné možnosti.

Pokud chtějí čtenáři sami tuto volbu ovlivnit, lze tak učinit zasláním mailu (do 30.1.2001) na adresu jaroslav.pinkava@normancz.cz (pozor - je tam dvakrát cz!). Přitom na webovské stránce Úřadu na ochranu osobních údajů (http://www.uoou.cz/normy.php3) lze nalézt poměrně rozsáhlý přehled norem z problematiky kryptografie a elektronických podpisů.

D. Letem šifrovým světem

Informace pro odběratele e-zinu. Prosím nepřehlédněte změnu e-mail spojení!
Mé nové adresy jsou pavel.vondruska@uoou.cz nebo vondruskap@uoou.cz .
Adresa pavel.vondruska@post.cz zůstala zachována.

1. National Institute of Standards and Technology (NIST) zveřejnil 5.1.2001 draft Draft Federal Information Processing Standard pro Keyed-Hash Message Authentication Code (HMAC). Jedná se o zobecnění HMAC specifikovaný v dokumentu RFC 2104 a ANSI X9.71. Připomínky a komentáře se mohou zasílat do 5.4.2001 na adresu HMAC@nist.gov . Draft je přístupný ve formátu PDF na adresách :
   http://csrc.nist.gov/publications/fips/dfips-HMAC.pdf
   nebo
   http://csrc.nist.gov/cryptval/hmac.html

2. Department of the Treasury zveřejnil ve Federal Register (Vol. 66., No.2) 3.1.2001 nejnovější verzi dokumentu Electronic Authentication Policy. Dokument se zabývá otázkou autentizace v oblasti elektronických plateb , je zde rozebírána i otázka použití elektronického podpisu. Text je možné získat na adrese
   http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.fms.treas.gov/eauth/index.html
   Stanoví se různé úrovně spoléhání se na autentizaci pomocí výše uvedených technik (rizika). Např. pro vysoký stupeň rizika se požaduje :
   - elektronický podpis
   - klíče smějí být generovány, drženy a používány pouze v bezpečných HW modulech
   - certifikační autority musí být pod dohledem státní autority

3. V předvánočním shonu trochu zanikl „úspěšný útok“ známé „Binary Division“ na stránky Policie ČR a MV ČR (6.12.2000). Na obou stránkách byla umístěna rozostřená fotografie ministra vnitra Stanislava Grosse s německým nápisem „Wilkommen Sie zum Gross Sicherheitsdienste" („Vítejte u velké (nebo také Grossovy) bezpečnostní služby"). Hackeři následně umístili tento výtvor ještě na webové stránky MV ČR . Výsledek jejich práce lze nalézt např. na internetové adrese http://underground.cz/download/hacked/www.mvcr.cz .
   Tyto a jim podobné útoky skupiny, která si říká "Binary Division", přimělo specialisty společnosti ICZ a.s. k vytvoření balíčku programů, který činnost hackerů znesnadní a pomůže zjistit napadení vašeho počítače. Celý tento balík s popisem a návodem k použití najdete na adrese http://www.i.cz/hacker.html (server patří společnosti ICZ).
   Jenže se zdá, že s kvalitou tohoto balíčku to nemusí být tak úplně v pořádku. Doporučuji si přečíst zdrcující kritiku v článku Pavla Veselého, který můžete najít na http://www.underground.cz/539 nebo ve „světě namodro“ : http://svet.namodro.cz/go/r-art.asp?id=1010106512&t=security .
   Domnívám se že instalace tohoto softwaru na váš linuxový server těžko zabrání nečekanému objevení se známého textu
   0% CzERT, 666% Dastych, 100% [dastych@mvcr]#, 100% binary.division,
   který „Binary Division“ v různých obměnách umisťuje na jimi napadené www stránky.

4. Do boje o Českou televizi se zapojili i „hackeři“, kteří dokonce dvakrát pozměnili stránku podporující generálního ředitele Hodače (http://www.ct-inforum.cz/) (2.1 a 3.1.2001). Z některých informací se zdá, že možná o úplně klasický hack typu „Binary divison“ tentokrát nešlo. Podle sdělení providera se totiž někdo ke stránce připojil ftp protokolem a po uhodnutí hesla mohl upravovat obsah jako legální správce stránky. Což o to, slovníkový útok přes všechna varování bývá účinný, ale malinko je na celém případě podezřelé, že k uhodnutí (podle záznamu) potřeboval jen dva pokusy…

5. 23. až 24. ledna 2001 se koná v Bruselu důležité pracovní setkání CEN/ISSS - Open Forum. Jedna z částí je věnována otázkám elektronického podpisu. Tato část má pracovní název : „Electronic Commerce Standardization - time for consensus?“
http://www.cenorm.be/ISSS/Workshop/ec/OpenForum/Programme.htm

6. Dne 16.1.20001 pořádá ECONOMIA a. s. (Konferenční a seminární servis), celodenní seminář **ELEKTRONICKÝ PODPIS V PRAXI** (e-Business a e-Government).
Přednášející:RNDr. Ivan Svoboda,CSc. (T-SOFT s.r.o.) a Mgr. Pavel Vondruška (Úřad pro ochranu osobních údajů).
Místo konání:Dobrovského 25, Praha 7 (stanice “Letenské náměstí“, TRAM č.1, 8, 25, 26 ze stanic metra Vltavská nebo Hradčanská).
Přihlášky:ECONOMIA, Konferenční a seminární servis, Dobrovského 25, 170 55 Praha 7
Fax: 02/ 33 07 20 30, tel.: 02/ 33 07 14 28, 33 07 14 30, e-mail: seminare@economia.cz

7. O čem jsme psali před rokem ?
Crypto-World 1/2000
http://www.mujweb.cz/veda/gcucmp/casop2/Crypto1_00.html
A. Slovo úvodem (P.Vondruška)
B. Země vstoupila do roku 19100 (P.Vondruška)
C. Nový zákon o ochraně osobních údajů (P.Vondruška)
D. Soukromí uživatelů GSM ohroženo (P.Vondruška)

E. Závěrečné informace
1. Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "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 použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Pokud máte zájem o zasílání tohoto sešitu, můžete se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků, informace
pavel.vondruska@uoou.cz
vondruskap@uoou.cz
pavel.vondruska@post.cz