Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 9/2003 **15. září 2003**

9/2003

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

(články neprocházejí jazykovou korekturou)

A. Soutěž 2003 začíná !
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

ÚVOD

Vážení čtenáři, 15.9.2003 zahajujeme soutěž o ceny v luštění šifrových textů. Obdobná soutěž proběhla v našem e-zinu na podzim roku 2000 a 2001. V roce 2000 byly úlohy zaměřeny na různé klasické šifrové systémy. V roce 2001 soutěž pokračovala řešením "modernějších systémů". Letošní soutěž volně navazuje předložením devíti úloh, které jsou rozděleny do třech kol.

I.kolo - lehké úkoly (hříčky)
a) Transpozice I.
b) Jednoduchá záměna I.
c) Jednoduchá záměna II.

II.kolo - klasické šifrové systémy (lze řešit jednoduše pomocí nápadu)
d) Transpozice II.
e) Jednoduchá záměna III.
f) Jednoduchá záměna IV.

III.kolo - klasické šifrové systémy
g) Transpozice III.
h) Jednoduchá záměna V.
i) Periodické heslo I.

Úlohy v prvním a druhém kole jsou výrazně jednodušší než soutěžní úlohy v letech 2000 a 2001. Ve třetím kole jsou úlohy přibližně stejně obtížné, jako úlohy, které byly předloženy k řešení v roce 2000. Pokud jde o postupy řešení jednotlivých klasických šifrových systémů, doporučujeme se seznámit s články otištěnými v Crypto-Worldu v roce 2000. V těchto článcích byly systémy představeny a čtenář zde nalezne i doporučený postup luštění těchto systémů.

Jednoduchá záměna, Crypto-World 10/2000, str. 2-4
Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
Substituce složitá - periodické heslo, srovnaná abeceda , Crypto-World 11/2000, str. 4-10

Pokud se chcete seznámit s metodami luštění podrobněji, doporučuji doprovodné texty k přednášce Úvod do klasických a moderních metod šifrování ALG082. Kurs probíhal pod odborným vedením doc. RNDr. J.Tůmy, DrSc. na Katedře algebry MFF UK Praha v zimním semestru 2003 (http://adela.karlin.mff.cuni.cz/~tuma/ciphers.html).

PRAVIDLA

Soutěž začíná 15.9.2003 a končí 6.prosince 2003 ve 22.00 hod. Zúčastnit soutěže se může každý odběratel e-zinu Crypto-World. Registrace probíhá přes web. Vstup na tuto stránku soutěže bude přes domovskou stránku Crypto-Worldu – ikona Soutěž 2003.

Při registraci řešitel zadá svůj login, autentizační heslo pro opětovné přihlášení a e-mail, na který mu je zasílán Crypto-World. Tento e-mail se dále nezobrazuje a je pro ostatní návštěvníky nedostupný.

Na této stránce bude k dispozici všech devět soutěžních úloh. Registrovaný řešitel může přes www rozhraní zadávat odpovědi na soutěžní úkoly. Odpověď je automaticky vyhodnocena a řešiteli je oznámeno, zda je správná nebo ne. Registrovaní řešitelé, ale i obyčejní návštěvníci stránky, mohou sledovat aktuální stav soutěže. U každého řešitele je v celkovém žebříčku vidět nejen počet vyřešených úloh, ale i pořadí, ve kterém je soutěžící vyřešil.

Pro určení pořadí je rozhodující počet vyřešených úloh. Při rovnosti počtu vyřešených úloh rozhoduje o pořadí, kdo dříve úlohy vyřešil. První tři řešitelé získávají cenu automaticky. Další tři ceny se vylosují mezi řešitele, kteří vyluští alespoň tři úlohy a jsou současně i čtenáři Crypto-Worldu (tj. jimi zadané e-mail adresy při registraci jsou v seznamu e-mail adres na které se e-zin rozesílá).

CENY

Pro vítěze jsou připraveny zajímavé ceny. Celkový vítěz získá volnou vstupenku na Mikulášskou kryptobesídku, která se koná v Praze 8.-9.12.2003. Tato vstupenka je přenosná. To znamená, že vítěz ji může podstoupit někomu jinému.

Pro první tři řešitele a pro další tři náhodně vylosované luštitele (do slosování jsou zařazeni všichni, kteří vyřeší alespoň tři z devíti úloh) je připravena láhev kvalitního portugalského vína (MATEUS) a replika historické číše z doby Rudolfa II (originál je ze 2. poloviny 16. století a pochází z jižních Čech).

Ceny budou předány na závěr Mikulášské kryptobesídky. Pokud se řešitel této akce nezúčastní, bude mu cena předána dodatečně.

Ceny do soutěže věnovali sponzoři soutěže:

- pořadatel Mikulášské kryptobesídky – ecom-monitor.com, http://www.ecom-monitor.com/kryptobesidka
- sklárna Královská huť v Doksech, http://www.royal-glassworks.cz
- firma Dignita , s.r.o., http://www.dignita.cz

Linky:
Soutěž 2000: http://crypto-world.info/zdroje/soutez.html
Soutěž 2001: http://crypto-world.info/zdroje/soutez2.html
Soutěž 2003: http://crypto-world.info/ (ikona – Soutěž 2003)

B. Cesta kryptologie do nového tisíciletí, část II.
(Od zákopové války k asymetrické kryptografii)
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

První polovina dvacátého století

První světová válka přivedla na svět nejen letadla a tanky, ale i první masové použití šifrování v polních podmínkách. Podnětem k rozvoji kryptologie nebyla jen válka jako taková, ale i rozšíření bezdrátového telegrafu. Ten dával možnost snadného odposlechu a bylo proto potřeba zavést jednoduché a bezpečné systémy šifrování. Prokázala se úžasná síla kryptoanalytiků (luštitelů). Pokud dokázali prolomit příslušný používaný systém, pak takto získané informace byly pro výsledek ofenzívy nebo dokonce celé války důležitější než roty vojáků a letadla. Samotný vstup USA do války byl důsledkem vyluštění obsahu šifrového telegramu - dnes známého jako tzv. Zimmermannův telegram. Německý ministr zahraničí Zimmermann v telegramu mexické vládě vyzývá Mexiko k válce proti USA. Slibuje v ní mexické straně podporu a územní zisk. Britové telegram zachytili, rozluštili jej a předali USA (přičemž neprozradili svůj zdroj). Poté co se prezident Wilson s obsahem telegramu seznámil, svolává kongres. Kongres 2.4.1917 schvaluje vstup USA do války proti Německu. Tento akt rozhodujícím způsobem změnil poměr sil na evropském válčišti. První světová válka vychovala i prvního z velikánů kryptografie dvacátého století. Stal se jím William Frederic Friedman (1891-1969). V roce 1915 nastoupil dráhu úspěšného kryptologa v americké armádě a vybudoval pro USA vzorně fungující kryptoanalytickou službu. Opravdovou biblí všech kryptologů prvé poloviny dvacátého století se stalo jeho čtyřsvazkové dílo "Základy kryptoanalýzy" z roku 1923. Obsah této knihy zásadně ovlivnil rozvoj kryptografie ve všech státech mezi dvěma světovými válkami a dá se říci, že se znalosti právě díky tomuto dílu "na všech frontách" vyrovnaly. Toto dílo by pravděpodobně nikdy nebylo vydáno, kdyby Friedman neměl existenční problémy a nemusel se živit psaním. Američané se totiž dopustili neuvěřitelné chyby, která je stála těžce získaný náskok - zrušili kryptoanalytické oddělení a členy tohoto oddělení propustili (!). Americký ministr zahraničí Henry Stimson to komentoval dnes již proslulou větou "Gentlemani si navzájem nečtou dopisy". Velice brzy si tuto chybu uvědomují a povolávají Friedmana zpět ke službě a dávají mu k dispozici na tu dobu veliké prostředky; je pověřen zřízením dešifrovacího oddělení. Od tohoto okamžiku se již odborná veřejnost po dlouhou dobu nebude dovídat o tom, co se děje v kuchyních tajných služeb. Tyto služby - vzhledem ke svým prostředkům a možnosti naverbovat schopné lidi - získávají před akademickou a komerční veřejností obrovský náskok. Většina států si vzala z této události poučení a jen zcela výjimečně docházelo k propuštění kryptoanalytiků. Jednou ze známých výjimek byla Československá republika, která neváhala v rámci velkých politických čistek oslabit i toto oddělení na Ministerstvu vnitra a Ministerstvu národní obrany..

Nové vyzbrojování ve třicátých letech se tedy nesoustředilo jen na vývoj zbraní, ale i na výrobu šifrovacích zařízení. V Německu bylo sestrojeno snad nejznámější šifrovací zařízení všech dob - legendární ENIGMA, ale i řada dalších důmyslných zařízení, např. kryptografické zařízení LORENZ nebo poněkud slabší zařízení Kryha. Svá zařízení vyvíjelo i Japonsko (97-ši-ki-O-bun in-ji-ki - PURPLE, J19-K9), USA (Sigaba, Hagelin C-38, M-209), Anglie a další státy, které se připravovaly k válce. Jména tvůrců těchto kryptografických zařízení jsou Edward H. Hebern, Hugo Koch, Arvid Gerhard Damm, Alexandr von Kryha, Gilbert Vernam, Boris Hagelin a další ….

Druhá světová válka prověřila kvalitu přichystaných šifrovacích zařízení. Zní to až neuvěřitelně, ale s odstupem času, kdy byly příslušné materiály postupně odtajněny, se ukázalo, že většinu tehdy používaných šifrových systémů se podařilo druhé straně prolomit a příslušné zprávy z těchto kanálů využívat. Utajení před veřejností bylo dokonalé. V zájmu neprozrazení, že v Bletchley Parku (hrabství Buckinghamshire) luští zprávy z Enigmy, nezabránil W.Churchil rozbombardování Coventry. Vzhledem k luštění zpráv předávaných Enigmou a i Lorenzem o chystaném náletu předem věděl, ale dlouhodobé strategické využívání zpráv z těchto zdrojů postavil nad životy tisíců lidí z tohoto anglického města. Cesta k prolomení tehdejších systémů již nebyla jednoduchá - na luštění se podíleli nejlepší matematici a pro účely luštění zařízení Enigma a Lorenz byly postaveny první stroje, které můžeme dnes nazvat počítače. Úplný popis zařízení Colossus, které sloužilo k luštění zpráv kryptografického zařízení Lorenz, byl například uvolněn teprve letos v květnu.

V luštění byli úspěšní nejen Angličané a Američané. Řadu šifer USA prolomili i Němci. Němci četli i většinu zpráv naší exilové vlády v Londýně, které vysílala domácímu odboji. Luštění těchto zpráv prokazatelně přispělo k likvidaci některých výsadků a odbojových skupin.

Veřejnost se sice dozvěděla některé částečné informace hned po válce, ale řada zpráv se objevovala až v průběhu desítek let po skončení války. K tomu bylo několik důvodů - především i po válce řada států ještě používala své válečné systémy, o nichž se nevědělo, že v průběhu války byly prolomeny, nebo naopak byly tyto systémy úspěšné a vlády nechtěly zveřejněním informací o nich oslabit možnost jejich využití.

Příkladem může být poválečné používání kryptografických zařízení z dílny Kryha Maschinen Gesselschaft v německé diplomatické službě, ale i v československém Obranném zpravodajství. Tato zařízení se s malou obměnou používala ještě začátkem roku 1952. Ve skutečnosti zařízení produkovalo nekvalitní, krátké periodické heslo a již roku 1933 Friedmann se svými kolegy přišel na to, jak zprávy zašifrované tímto strojem luštit.

Druhým příkladem může být využití úspěšného systému i po válce. Za druhé světové války bylo využíváno indiánů kmene NAVAJO u americké námořní pěchoty k předávání tajných zpráv rádiem. Kódovou řeč, kterou Indiáni předávali ve své mateřštině , se Japoncům nepodařilo odhalit. Američané tento způsob s úspěchem použili ve válce v Severní Koreji a dokonce ještě v 60. letech ve Vietnamu. Veřejnost byla informována až koncem šedesátých let a úplná kódová kniha byla uvolněna k publikování teprve zhruba před rokem.

V době studené války byla kryptografie chápána jako tajná zbraň. Informace o ní byly záměrně potlačovány. Na civilních školách se nevyučovala. Instituce, které se použitím a vývojem šifrových technik zabývaly, si vybíraly do svých služeb nejschopnější matematiky už během studia a po nástupu do svých služeb je teprve seznamovaly s dosaženými výsledky, které patřily mezi nejutajovanější informace. Tento systém přispěl k tomu, že v šedesátých a sedmdesátých letech byl náskok těchto agentur (a nemyslím tím jen NSA a KGB) až desítky let před světovou odbornou veřejností, která se ovšem prakticky ještě nezformovala a vlastně tedy téměř neexistovala.

Druhá polovina dvacátého století

Jako blesk z čistého nebe zapůsobily dvě práce jednoho z velikánů kryptologie dvacátého století Claude Elwood Shannona. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů". Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl. Oba články fakticky odstartovaly moderní pojetí matematického zkoumání základů kryptografie a kryptoanalýzy a staly se pro rozvoj veřejné kryptologie stěžejními díly a pravděpodobně nejcitovanějšími pracemi v tomto oboru do konce sedmdesátých let.

Nová kvalitní kryptografická zařízení, která se v této době začala vyrábět po celém světě, byla zpravidla založena na velice jednoduchém principu: sčítání otevřeného textu s náhodným heslem. Systém navrhl roku 1917 Gilbert Vernam, ale z publikované teorie amerického vědce Shannona vyplynulo, že jediný absolutně bezpečný systém je právě sčítání otevřené zprávy se stejně dlouhým náhodným heslem. Velice jednoduché - jenže je zde problém. K odšifrování samozřejmě potřebujeme mít k dispozici příslušné náhodné heslo, které jsme přičetli k původní zprávě. Zde je právě onen základní problém celého systému. Místo tajného doručení původního otevřeného textu délky N musíme na místo určení doručit heslový materiál - náhodnou posloupnost stejné délky, tedy délky N. Problém je to tedy téměř ekvivalentní (samozřejmě, heslový materiál lze doručit ve velkém množství a do zásoby ještě před nutností vyslat zprávu). Při objemu dnes předávaných zpráv je tento systém nevyhovující. Jeho význam je v tom, že se jedná o jediný absolutně bezpečný systém - pokud jsou dodrženy následující podmínky:

- umíme vyrobit náhodné, stejně pravděpodobné heslo (výroba takovéhoto hesla byla v 60. letech velkým problémem)
- máme dostatečně důvěryhodný kanál k transportu hesla na místo určení
- korespondence je tak slabá, že nám nevadí velká spotřeba hesla
- každé heslo lze použít pouze jednou a je tedy potřeba dodržovat určitá přesně daná pravidla pro zacházení s heslovým materiálem.

Touto - v té době moderní cestou - se vydala i tehdejší česká kryptografie.

Kubánská krize na začátku šedesátých let vyvolala potřebu rychlého a bezpečného spojení mezi USA a SSSR. Obě mocnosti se domluvily na vybudování horké linky mezi hlavami obou států. Pro tuto linku byl také zvolen výše popsaný systém. Horká linka byla uvedena do provozu 30. 8. 1963 . Kreml i Bílý dům si vzájemně vyměnily heslové materiály - pásky. Otevřené texty se převedly do dálnopisného kódu a sčítaly se s heslovým materiálem, heslová páska byla ihned po použití automaticky ničena, čímž se mělo zamezit jejímu nechtěnému opětnému použití. Při zavedení tohoto systému se použilo zařízení ETCRRM-II (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II). Každou hodinu se přenášely zkušební relace. Z americké strany se přenášely výsledky basebalových zápasů, z ruské strany výňatky z Lovcových zápisků od Turgeněva. Použití kódových pásků, které se vyměňují prostřednictvím velvyslanectví jednotlivých států, zajišťuje naprostou bezpečnost přenášených zpráv a také - což je velmi důležité - nemožnost vpašování falešné zprávy.

Rozsah provozu právě v této době závratně rostl. V r. 1930 představoval telegrafní provoz v celých USA 2,2 miliony slov, v lednu 1960 jen Ministerstvo zahraničních věcí USA

vyslalo a přijalo stejné množství slov za 14 dní. V červnu 1961 bylo přeneseno 6,929 milionů slov za jeden měsíc. Jednalo se tedy o zvýšení zátěže provozu o 40 % za rok a půl!

Potřeba důvěrné komunikace mezi subjekty se dále zvyšovala a náklady na výrobu a transport heslového materiálu stále rostly. Současně se stávalo, že při nedostatku heslového materiálu byla porušena zásada nepoužít stejné heslo dvakrát, a také při distribuci tak ohromného množství šifrového materiálu nebylo neobvyklé, že se k heslovému materiálu dostala nepovolaná osoba.

Absolventi vojenských kateder 70. let si jistě pamatují na stále vtloukaný slogan: "Bez spojení není velení", a tak nastala doba inovace. Bylo nutno opustit předávání heslového materiálu délky zprávy a přejít na jiný systém. Řešením se zdálo generování hesla přímo kryptografickým zařízením. Přijímač a vysílač generoval pseudonáhodné heslo. Počáteční nastavení bylo dáno zpravidla tzv. inicializačním vektorem a klíčem. Stačilo se jen domluvit na počátečním nastavení. Kvalita tohoto systému závisí na kvalitě pseudonáhodné posloupnosti a počtu možných počátečních stavů, které pak generují různé pseudonáhodné posloupnosti. Tento problém je z matematického hlediska velice složitý a byl slabinou některých komerčně vyráběných zařízení té doby.

Kryptologie se v sedmdesátých letech přestala pěstovat jen v uzavřených komunitách tajných služeb a začala se stávat součástí světové vědy. Objevily se prvé významné výsledky této akademické obce. V roce 1976 publikovali Whitfield Diffie, Martin Hellman a Ralph Merkle článek o nové závratné myšlence - asymetrické kryptologii. Až dosud všechny šifrové systémy byly systémy tzv. symetrické. Odesílatel i příjemce museli znát stejný klíč a jím buď zašifrovali nebo odšifrovali. Pokud takto komunikovalo *n* lidí a zprávám měli rozumět vždy jen dva z nich, bylo zapotřebí distribuovat *n*(n-1)/2* různých klíčů. Dále bylo nutné přesně dodržovat tzv. pravidla klíčového hospodářství, tedy kdy který klíč začal platit, přestal platit, řešit kompromitace, záložní klíče, skupinové klíče apod. Správa takovéhoto systému se začala stávat nepřehlednou, těžkopádnou a byla slabinou většiny šifrových systémů té doby.

V příštím e-zinu 10/2003 pokračuje seriál částí :

Cesta kryptologie do nového tisíciletí, část III.
(Od asymetrické kryptografie k elektronickému podpisu)

C. Kryptografie a normy
Digitální certifikáty.
Politika pro vydávání atributových certifikátů - požadavky, část 1. (Technical report ETSI 102 044)

Jaroslav Pinkava, PVT a.s.

1. Úvod

V předešlých pokračováních byl popsán profil atributového certifikátu ve smyslu dokumentu rfc.3281 (požadavky, samotný profil, typy atributů, podmínky pro práci s atributovými certifikáty - ověření platnosti, odvolání).

V loňském roce (červenec, prosinec 2002) se postupně objevily dvě verze dokumentu pracovní skupiny ETSI - Electronic Signatures and Infrastructures (ESI). Requirements for role and attribute certificates. Cílem dokumentu je identifikace souboru požadavků, které by následně byly základem chystané normy pro požadavky na politiku při vydávání atributů(ať již atributovými autoritami či certifikačními autoritami - jako součást atributového certifikátu či jako jedno z rozšíření digitálního certifikátu). Protože rozdíl mezi atributovou autoritou a certifikační autoritou je v tomto směru nepodstatný, dokument používá termín atributová certifikační autorita (ACA).

Atributem je míněna kvalifikace osoby , která ji opravňuje vykonávat určité specifické funkce - jako jsou např. pověření jednat v zastoupení firmy - anebo jí uděluje určitá privilegia - např. členství v klubu atd.

Materiál ETSI konstatuje, že vzhledem k zatímnímu minimálnímu používání takovýchto atributů existuje velmi málo praktických zkušeností. Přesto jsou zde uvedeny konkrétní odkazy kontaktovaných certifikačních organizací (Francie, Německo, Itálie, Nizozemsko) a zmíněn projekt PERMIS (Itálie, Španělsko, Velká Británie), v jehož rámci byl zpracován určitý přehled praktických přístupů k problematice.

2. Některé definice.

Materiál se opírá o následovně definované pojmy:

atribut: informace vztažená k entitě, která specifikuje její charakteristiku (např. členství ve skupině, roli či jiná oprávnění);

atributová autorita (AA): autorita, důvěryhodná třetí strana, která vytváří a podepisuje atributové certifikáty;

atributový certifikát (AC): datová struktura obsahující množinu atributů koncové entity a další informace, které jsou digitálně podepsány soukromým klíčem vydávající AA;

politika atributových certifikátů (ACP): jmenovitý soubor pravidel, který vyznačuje použitelnost atributových certifikátů v rámci určité komunity resp. aplikace se společnými bezpečnostními požadavky či vyznačuje pravidla pro registraci, rozesílání a odvolávání atributů, které jsou obsaženy v certifikátech;

atributová certifikační autorita (ACA): důvěryhodná autorita, která včleňuje atributy do PKC či AC;

doba platnosti atributového certifikátu: doba, po kterou jsou atributy obsažené v atributovém certifikátu považovány za platné;

certifikační období atributu : doba, po kterou jsou AC obsahují daný atribut vydávány AA;

prováděcí směrnice atributové certifikace (ACPS): směrnice obsahující postupy, které ACA používá při vydávání certifikátů;
atributy vydávající autorita (AIA): spolehlivý zdroj atributů;
certifikát: buď atributový certifikát (AC) či certifikát veřejného klíče (CVK);
certifikační autorita (CA): důvěryhodná autorita vytvářející a podepisující certifikáty veřejných klíčů;
skupinové členství: stav členství ve skupině (klub, firma, organizace,...)
infrastruktura oprávnění (PMI): infrastruktura, která podporuje řízení oprávnění pro komplexní autorizační služby a v návaznosti na infrastrukturu veřejných klíčů;
certifikát veřejného klíče (PRC): datová struktura obsahující veřejný klíč koncové entity a další informace, která je podepsána soukromým klíčem CA, která daný certifikát vydala.
kvalifikovaný certifikát (QC): certifikát veřejného klíče splňující podmínky přílohy I Směrnice EU a který byl vydán certifikační autoritou, která splňuje podmínky přílohy II téže Směrnice;
role: funkce, pozice či statut někoho v organizaci, ve společnosti či v jiné spojitosti;
Poznámka: Samotný dokument vychází z terminologie Směrnice EU pro elektronický podpis (lit.[8]).

3. Různé druhy atributů

Samotné atributy mohou vyjadřovat různé specifikace - členství v nějaké skupině, roli či informaci o jiném oprávnění.
Členství ve skupině - to se může týkat skupin s hierarchickým uspořádáním nebo skupin s určitou funkcí. Hierarchicky uspořádané skupiny obvykle charakterizují nějakou instituci, firmu, podnik a zde je pak specifikována pozice jednotlivce v hierarchii skupiny. Naopak funkční skupiny zahrnují více osob, které mají tutéž funkci či pracují na témže projektu.
Role - to je způsob, kterým je vyjádřena organizační či funkční odpovědnost. Tato odpovědnost často odráží uživatelovo pracovní zařazení (název pracovní funkce). Role může být plněna jednou či více osobami (např. ve firmě může být více účetních ale jen jeden hlavní účetní atd.).
Přitom jedna konkrétní osoba (subjekt) může současně zastávat více rolí a to i ve více organizacích. Samotná role je definována v nezávislosti na konkrétním subjektu, který ji zastává.
V rámci jedné instituce je prováděna určitá administrace rolí (jejich definice, rozdělení na konkrétní subjekty). Aplikace pak pracují s rolemi a nikoliv s konkrétními osobami, které tyto role zastávají.
Informace o jiných oprávněních - dokument uvádí dvě kategorie takovýchto informací: jednání v zastoupení (proxy) a způsobilost (capability).
V zastoupení subjekt může jednat jménem jiného jedince a to ať již jeho jménem nebo v rámci atributu tohoto jedince. Osoba, která deleguje svůj podpis může jeho použití omezit (z hlediska svých atributů), pak podpis lze použít pouze v určitých podpisových politikách a pro sdělení určitých typů. Tj. každý atribut lze při jeho individuálním používání omezit. Technicky jednání osoby v zastoupení druhé osoby může probíhat dvěma způsoby:
- AA vydá delegátovi (zastupující osobě) AC, který obsahuje všechny nebo jen část delegátových atributů;
- delegující osoba přímo deleguje delegátovi všechny či část svých funkcí tím, že mu vydá atributový certifikát podepsaný buď přímo delegující osobou anebo AA (důvěryhodnou třetí stranou). V tomto případě ještě je možné rozlišit situace, kdy při delegování je prováděn výběr konkrétních atributů pro konkrétního delegáta a situace, kdy je přesně specifikován kontext, v rámci kterého jsou předané atributy použitelné.

Pojem *způsobilosti* se obvykle objevuje v kontextu kontrol přístupu. V systémech založených na způsobilosti například přístup k chráněným souborům je možný tehdy pokud, příslušná přistupující osoba je k tomu způsobilá. To je realizováno např. použitím tokenu, který nositeli dává právo přístupu k daným zdrojům. Vlastnictví tohoto tokenu je považováno za důkaz, že příslušná osoba je oprávněná k přístupu k označeným zdrojům.

4. Nárokovaný a certifikovaný atribut

Samotný atribut může být pouze nárokován, namísto toho aby byl již přímo certifikován. Pokud je vznesen příslušný nárok, je pak nárokující osoba odpovědná za jeho uplatnění a pokud se prokáže, že toto uplatnění bylo nesprávné, ponese tato osoba za to příslušné následky. Například pokud někdo se bude vydávat za vyššího funkcionáře organizace (jejímž je členem, zaměstnancem) a bude konat v tomto smyslu - např. podepíše něco, co neměl oprávnění podepsat - potom vznikají příslušné zákonné dopady jak nejprve mezi verifikující stranou a příslušnou organizací a následně pak mezi organizací a konkrétní osobou. Některé aplikace mohou přijímat atributy, které jsou pouze nárokované, zatímco jiné aplikace akceptují pouze certifikované atributy.

Certifikaci atributu provádí ACA na základě informace, kterou ji dá AIA. Některé organizace mohou plnit obě funkce (ACA i AIA), v tom případě jsou to *přímo certifikované atributy*. Pokud jsou obě funkce rozděleny, musí být atributy verifikovány. Směrnice klade příslušnou odpovědnost na CA (kvalifikované certifikáty mohou obsahovat atributy). Totéž platí i pro ACA.

AIA je autorita, která zjišťuje, zda "příslušná osoba je kompetentní provádět specifické služby". Musí mít samozřejmě k tomu patřící zkušenosti a dovednosti (aby dokázala charakterizovat kompetence dané osoby). Kompetence ACA jsou pak orientovány na oblast PKI a PMI. V případech, kdy kompetence AIA a ACA vykonává jedna organizace, je nutné, aby toto rozlišení proběhlo na úrovni personálu, tj. ve vydělení příslušných pracovních funkcí.

1. Obsahový význam atributů a jejich reprezentace

Pokud se rozhodujeme zda v aplikaci využijeme konkrétní atribut, potřebujeme zřejmý popis významu tohoto atributu. Tento popis musí být zadán odpovídající formou (dostupným způsobem čitelnou) a pokud je to možné, musí obsahovat i odkazy na příslušnou legislativu.

Atribut může být:

- srozumitelný pouze pro přímého uživatele;
- pouze strojově zpracovatelný;
- jak strojově zpracovatelný tak i uživatelsky srozumitelný.

První typ atributů je obvykle popsán řetězcem znaků, pro druhý typ atributů je používáno OID nebo DN (distinguish name).

Atribut role je jediný atribut, který je specifikován v normě ISO/IEC 9594-8 - obsahuje informaci o rolích. Má dvě složky - *role Authority* a *role name*. Složka *role Authority* je nepovinná, je používána pokud AIA není současně AA, umožňuje identifikaci AIA v její roli. Složka *role name* obsahuje definici role (v různých syntaxích).

2. Jiné charakteristiky atributů

a) Časový interval atributu:
   Atributy mohou být - doživotní, dlouhodobé, krátkodobé
b) Certifikační období atributu

Pokud se atribut stane součástí certifikátu veřejného klíče či atributového certifikátu, pak příslušná autorita zároveň rozhoduje jak dlouho bude akceptovat certifikaci tohoto atributu.

c) Doba platnosti atributového certifikátu:
I v situacích, kdy časový interval atributu je veliký, není nutné certifikovat tento atribut pro celý tento časový interval. Doba platnosti atributového certifikátu je období, kdy některé atributy obsažené v certifikátu jsou považovány za platné.

d) Zneplatnění atributů a zneplatnění atributových certifikátů:
V řadě případů je žádoucí vynechat možnost ověřování revokačního statutu atributového certifikátu - např. vzhledem k skutečnosti, že atributový certifikát má dobu platnosti řádově v hodinách, maximálně v dnech. Pokud je však možnost zneplatnění podporována, lze k tomu využít např. OCSP (on-line mechanismus) či seznam zneplatněných certifikátů (CRL - off-line mechanismus).

e) Ochrana atributů (utajení):
V řadě případů nemusí být vhodné rozkrývat všechny uživatelovy atributy. Je pak vhodné použít nikoliv certifikáty veřejného klíče, ale vložit atributy do atributového certifikátu, který je připojován pouze k těm dokumentům, kde je to vyžadováno.

f) Jak získat atributy:
To lze v zásadě třemi způsoby - standardně, když jsou obsaženy v PKC; na základě požadavku, pokud jsou umístěny v AC; získáním AC z úložiště.

g) Delegovatelné atributy:
Některé (zdaleka ne všechny) atributy lze delegovat jiné osobě. Obvyklé je to například v situacích, kdy jedna osoba zastupuje druhou (dovolená, nemoc). Je vhodné, aby delegovanou osobou byl konkrétní jedinec, pokud možno po celou dobu týž. Delegace může v určitých situacích obsahovat určitá omezení (vzhledem k účinnosti původních atributů).

Poznámka: Příští pokračování bude věnováno druhé části dokumentu (lit. [6]).

3. Literatura

[1] rfc3281: An Internet Attribute Certificate Profile for Authorization

[2] ITU-T Recommendation X.509/ISO/IEC 9594-8: Information technology – open systems interconnection – the Directory: Public-Key and Attribute Certificate Frameworks, Version 4, 2000

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

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

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

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

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

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

D. K problematice šíření nevyžádaných a obtěžujících sdělení prostřednictvím Internetu, zejména pak jeho elektronické pošty, část II.

Ján Matejka
(*Ústav státu a práva AV ČR, Praha,* **Právnická fakulta ZČU, Plzeň, jan@matejka.us)**

4.5 Obchodní zákoník[1]

Jak ostatně vyplývá mimo zejména z povahy nevyžádaných zpráv, jejich rozeslání může naplňovat, a dle mého soudu tomu tak v mnoha případech opravdu bude, znaky generální klauzule nekalé soutěže (§44 odst. 1 ObchZ), případně dalších výslovně zmíněných skutkových podstat (§ 46 a násl. ObchZ).

Osoby, jejichž práva byla nekalou soutěží porušena nebo ohrožena, mohou se proti rušiteli domáhat, aby se tohoto jednání zdržel a odstranil závadný stav. Dále mohou požadovat přiměřené zadostiučinění, které může být poskytnuto i v penězích, náhradu škody a vydání bezdůvodného obohacení (§53 ObchZ).

4.6 Telekomunikační zákon[2]

V určitých případech se lze domáhat též ochrany prostřednictvím úpravy uvedené v telekomunikačním zákoně. Tento zákon totiž ve věcech telekomunikací upravuje jak podmínky pro zřizování a provozování telekomunikačních zařízení a telekomunikačních sítí, podmínky pro poskytování telekomunikačních služeb, tak i výkon státní správy včetně regulace. Vzhledem k legálním definicím pojmu telekomunikační zařízení[3] (§2 odst. 1 TelZ), telekomunikační síť[4] (§2 odst. 2 TelZ) a telekomunikační služba[5] (§2 odst. 5 TelZ) totiž lze tuto úpravu, v určitých případech vztáhnout také na šiřitele nevyžádaných zpráv.

Z pohledu TelZ lze totiž spamming považovat za zneužívání sítě, v tomto ohledu není poskytovatel povinen vymazat nebo učinit anonymními ta data, která slouží mimo jiné k identifikaci zneužívání sítě (§85 odst. 7 TelZ) a lze tedy předpokládat, že tato data mohou být na vyžádání užita pro účely soudního řízení. Na základě § 84 odst. 9 TelZ si totiž provozovatelé veřejných telekomunikačních sítí a poskytovatelé veřejných telekomunikačních služeb mohou vzájemně předávat data uvedená v odstavci 3 písm. c)[6], je-li to nezbytné pro

1 zákon č.. 513/1991 Sb., Obchodní zákoník; v platném znění (dále jen ObchZ)

2 zákon č. 151/2000 Sb., o telekomunikacích; v platném znění (dále jen TelZ)

3 Telekomunikačním zařízením se rozumí technické zařízení, včetně vedení, pro vysílání, přenos, směrování, spojování a příjem informací prostřednictvím elektromagnetických vln.

4 Telekomunikační sítí se rozumí funkčně propojený soubor telekomunikačních zařízení k přepravě informací mezi koncovými body této sítě nebo soubor rádiových zařízení k přepravě informací nebo jejich vzájemná kombinace.

5 Telekomunikační službou se rozumí služba, jejíž poskytování spočívá zcela nebo zčásti v přepravě nebo směrování informací telekomunikačními sítěmi třetím osobám. Touto službou je i pronájem telekomunikačních okruhů. Za telekomunikační službu se nepovažuje přepojení (přesměrování) hovoru tísňového volání na jiné pracoviště základní složky integrovaného záchranného systému, které je kompetentní k jeho odbavení.

6 Jde o data související s poskytováním telekomunikační služby, zejména údaje o účastnících telekomunikačního spojení.

zajištění propojení a přístupu k síti, ke vzájemnému vyúčtování a **k identifikaci zneužívání sítě** a služeb.

4.7 Trestní zákon[7]

Z pohledu závažnějších následků spammingu, jako např. opakované celkové zahlcení mailserveru nevyžádanými zprávami o velkém rozsahu, lze pak hovořit o případně trestněprávní odpovědnosti takového šiřitele. V souvislosti s spammingem lze hovořit zejména o následujících trestných činech, a to jak ve formě přímého pachatelství (§ 9 odst. 1 TrZ), tak i spolupachatelství (§ 9 odst. 2 TrZ) případně i účastníka (§ 10 TrZ - *organizátora, návodce či pomocníka*). Vyjma trestného činu ***neoprávněného nakládání s osobními údaji*** (§ 178 TrZ), který lze spáchat též z nedbalosti však jde zejména o úmyslné trestné činy. Nedomnívám se ale, že by trestní odpovědnost za spamming mohla být až tak častým jevem.

Jako nejpravděpodobnější trestný čin, který lze v souvislosti se spammingem spáchat je zejména trestný čin ***neoprávněného nakládání s osobními údaji*** (§ 178 TrZ), tohoto činu neoprávněné se dopustí ten, „*kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy…“* (§ 178 odst. 1 TrZ), *případně ten,* „*kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.“* (§ 178 odst. 2 TrZ).

Další skutková podstata, která může být v některých případech v souvislosti se spammingem naplněna je porušování autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 152 TrZ). Tohoto trestného činu se dopustí ten, „*kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.*“. Znakem skutkové podstaty tohoto trestného činu dle § 152 odst.1 však není vznik majetkové škody.

Vzhledem k převládajícímu restriktivnímu výkladu norem trestního zákona (a norem veřejného práva vůbec) patrně nelze předpokládat, že by mohla být spammingem naplněná také skutková podstata trestného činu poškození a zneužití záznamu na nosiči informací dle § 257a TrZ. Tato (byť poměrně široká) skutková podstata totiž předpokládá *získání přístupu k nosiči informací*, čímž se zde patrně rozumí takové jednání, které umožní pachateli volnou dispozici s nosičem informací a využití informačního obsahu. Ke splnění této podmínky nemusí nutně dojít pouze fyzickou účastí u nosiče informací, ale také získáním přístupu k tomuto nosiči na dálku (tedy např. modemem a telefonem připojeným na Internet). Sotva však lze hovořit o tom, že by pouhé získání adresy mohlo být považováno za získání přístupu k nosiči informací.

5. ÚPRAVA V PRÁVU ES

Jednou z prvních vlaštovek zabývajících se problematikou nevyžádaných elektronických zpráv na půdě Evropských společenstvích byla směrnice evropského parlamentu a rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb

7 Zákon č. 140/1961 Sb., trestní zákon; v platném znění (dále jen TrZ)

informační společnosti, zejména elektronického obchodu, na vnitřním trhu („**směrnice o elektronickém obchodu**“) [8]. Motivy vedoucí k přijetí této směrnice lze spatřovat zejména ve skutečnosti, že zasílání nevyžádaných obchodních sdělení elektronickou poštou může být pro spotřebitele a poskytovatele služeb informační společnosti nevýhodné a může narušovat řádné fungování interaktivních sítí. Otázka souhlasu uživatele s určitými formami nevyžádaných obchodních sdělení není předmětem této směrnice, ale je již upravena zejména směrnicemi 97/7/ES a 97/66/ES. V členských státech, které připouští zasílání nevyžádaných obchodních sdělení prostřednictvím elektronické pošty, by mělo být podporováno a usnadňováno zavádění zařízení na vhodné filtrování těchto sdělení. Kromě toho musí být nevyžádaná obchodní sdělení v každém případě jasně rozeznatelná, aby mohla být zlepšována průhlednost a usnadňována funkčnost těchto zařízení zaváděných podniky. Nevyžádaná obchodní sdělení zasílaná elektronickou poštou nesmí pro uživatele představovat žádné dodatečné výdaje.

Tato směrnice ve svém článku 7 (rubrika: Nevyžádaná obchodní sdělení) obsahuje základní pravidla, která mají být do právních řádů členské států Evropských společenství promítnuty. Vedle ostatních požadavků práva ES jsou ty členské státy, které umožňují nevyžádaná obchodní sdělení elektronickou poštou, povinny zajistit, aby uživatel mohl tato obchodní sdělení poskytovatele služeb usazeného na jejich území při jejich přijetí jasně a jednoznačně rozeznat (čl. 7 odst. 1). Aniž je dotčena směrnice 97/7/ES a směrnice 97/66/ES, přijmou členské státy opatření, aby zaručily, že poskytovatelé služeb, kteří zasílají nevyžádaná obchodní sdělení elektronickou poštou, budou pravidelně porovnávat seznamy, do nichž se mohou zapisovat fyzické osoby, které si nepřejí, aby jim byly takové informace zasílány, a že poskytovatelé těchto služeb budou tento seznam respektovat.

Další (poslední) směrnicí komunitárního práva, která upravuje tuto problematiku, je směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracovávání osobních údajů a ochraně soukromí v odvětví elektronické komunikace (směrnice o soukromí a elektronické komunikaci)[9].

6. NÁVRHY DE LEGE FERENDA

6.1 Celkové řešení problematiky spammingu

Navzdory řadě existujících, a to mnohdy zcela protichůdných, názorů a celkové složitostí této problematiky se domnívám, že ideálním řešením této problematiky je pouze řádné právní zakotvení institutu seznamu nevyžádaných adres elektronické pošty (tedy tzv. opt out registru**)**, a to zároveň s jasnou a vymahatelnou možnosti kdykoliv a bez obtíží již zaslané, ať vyžádané či nevyžádané elektronické sdělení, do budoucna odmítnout.

Uvedené by znamenalo promítnutí výše zmíněných principů do platných zákonných norem. Za vyhovující předpis, který by měl tuto problematiku upravovat lze dle mého názoru považovat buď zákon o reklamě, zákon o poštovních službách, případně telekomunikační zákon.

Výše uvedeným postupem bychom pak rovněž harmonizovali jeden ze zbývajících závazků směrnice evropského parlamentu a rady 2000/31/ES ze dne 8. června 2000 o

8 Úřední věstník č. L 178, 17.07.2000, s.1; Celex: 32000L0031

9 Úřední věstník č. L 201, 31.07.2002, s.37; Celex: 302L0058,

některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („**směrnice o elektronickém obchodu**“).

6.2 Orgán dozoru nad spammingem

Zejména vzhledem k poněkud problematickému dokazování spammingu (viz. výše) se zdá být stávající orgán dozoru v podobě živnostenských úřadů poměrně nevyhovující. Osobně bych se tedy spíše přikláněl ke změně platné právní úpravy ve formě přenesení většiny pravomocí, které stávající regulátor (orgánu dozoru) vůči spammingu má, na Český telekomunikační úřad. Pravomoc a působnost Českého telekomunikačního úřadu by tak byla výrazně rozšířena a vztahovala by se výlučně na spamming šířený prostřednictvím telekomunikačních sítích ve smyslu §2 odst. 2 zákona č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, v platném znění. Živnostenské úřady by tak přišly o část pravomoci a působnosti, avšak podstatná část dohledu by jim zůstala[10].

6.3 Využití elektronického podpisu

Vzhledem k již zmíněné možné anonymitě (neodhalitelnosti) elektronické pošty, se zdá být významné stanovení určitých povinností, resp. opatření pro šiřitele (event. i zpracovatele) nevyžádané zprávy elektronické pošty, jejichž účelem bude zejména zajištění identifikace odesílatele takovýchto zpráv. V tomto ohledu by si jistě našel své uplatnění i institut zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu ve smyslu zákona č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů, v platném znění (dále jen ZoEP)

7. MÍSTO ZÁVĚRU

Jak vyplývá z výše uvedeného, prostředků proti spamu je celá řada. Nejvýznamnějším legislativním počinem v této oblasti je ale bezesporu zákon o regulaci reklamy, který výslovně zakazuje určité reklamy (a potírá tak velkou část těchto nevyžádaných zpráv). Z teoretického hlediska však také nelze vyloučit ochranu dle zákona o ochraně osobních údajů, případně též občanský nebo obchodní zákoník.

Co se týče samotné úpravy v zákoně o regulaci reklamy, lze zde ale nepochybně vyslovit názor, že tato ustanovení novelizovaného zákona o regulaci reklamy sice odstraňují některé jejich dosavadní legislativní nedostatky a výkladové problémy, ale zároveň s sebou přináší očekávané interpretační obtíže nové. Problematika spamu tudíž zůstává v některých dalších otázkách nadále otevřena.

10 Např. nevyžádaná a obtěžující reklama realizovaná prostřednictvím jiných než telekomunikačních sítí (např. pomocí software, apod.)

E. Informace o konferenci CRYPTO 2003

RNDr. Jaroslav Hrubý,CSc., GCUCMP

Ve dnech 17-21.srpna 2003 se konala třiadvacátá mezinárodní kryptologická konference CRYPTO 2003 na universitě v Santa Barbaře (UCSB), které se zúčastnilo přes 400 specialistů z celého světa.

Konference se konala pod záštitou mezinárodní kryptologické asociace IACR, technického výboru pro bezpečnost IEEE počítačové společnosti a UCSB, přičemž byla obeslána 169 příspěvky, z nichž bylo 34 vybráno programovým výborem v čele s prof. D.Bonehem ze Standfordské university pro prezentaci.

Vybrané příspěvky byly rozděleny do následujících skupin :

1. Kryptoanalýza šifer s veřejným klíčem I a II
2. Alternativní protivníkovy modely
3. Protokoly
4. Kryptoanalýza symetrických šifer I a II
5. Univerzální skládání protokolů
6. Tzv. „ Zero-Knowledge“ protokoly
7. Algebraická geometrie
8. Konstrukce šifer s veřejným klíčem
9. Nové problémy
10. Konstrukce šifer se symetrickým klíčem
11. Nové modely

a dále byly zařazeny dvě zvané přednášky, o kterých se zmíním později. Ve večerních hodinách 19.8.03 se jako obvykle konala tzv “Rump session“ , na kterou bylo vybráno přes 40 pětiminutových příspěvků, zhruba pokrývajících témata z výše uvedených skupin.

Alespoň stručně rozebereme témata jednotlivých příspěvků ve skupinách s tím, že zájemci o danou tématiku si přečtou příspěvek ve sborníku konference vydaném jako obvykle nakladatelstvím Springer, Lectures Notes in Computer Science, LNCS 2729, D.Boneh (Ed.), Advances in Cryptology - CRYPTO 2003, ISBN 3-540-40674-3, http://www.springerlink.com/series/lncs/ .

Ve skupinách byly prezentovány následující příspěvky:

1.1 A:Shamir, E.Tromer: Faktorizace velkých čísel přístrojem TWIRL - v přednášce byla demonstrována reálná možnost rozbití 1024 bitového RSA klíče v horizontu jednoho roku, a to pomocí zařízení TWIRL.

1.2 J.Blomer, A.May : Nový útok na RSA z částečné znalosti soukromého klíče – v příspěvku je ukázána možnost útoku pomocí algoritmu v polynomiálním čase v případné znalosti významných, či méně významných bitů soukromého klíče, pomocí tzv.Coppersmithovy metody.

1.3 J.CH.Faugere, A.Joux: Algebraická kryptoanalýza šifer založených na utajených polních rovnicích užitím Grobnerových bazí- je zde ukázána nová algebraická kryptoanalýza založená na rychlých algoritmech pro výpočet Grobnerových bazí a je revidována bezpečnost šifer založených na utajených polních rovnicích.

1.4 J.H.Cheon, B.Jun : Algoritmus v polynomiálním čase pro tzv. copatý („braid“) Diffie-Hellmanův konjugační problém - aplikace neabelovských grup v kryptologii analogická např. Diffie-Hellmanovu schématu a ElGamal schématu na abelovských

grupách byla veřejně publikována v r.2000 a od té doby se datují heuristické algoritmy pro řešení těchto tzv. uzlíčkových šifer. Jednu z nových metod ukazují i autoři.

1.5 N.Howgrave-Graham a ost.: Vliv dešifrovacích poruch na bezpečnost NTRU šifrování – autoři ukazují nový útok na tuto šifru. Použitím poruch při dešifrování získají privátní klíč.

2.1 S.P.Vadhan : O konstrukci lokálně vypočítatelných vytěžení a kryptosystémech v ohraničeném skladovém modelu – autor uvažuje problém konstrukce náhodných vytěžení, která jsou lokálně vypočitatelná (tj. na vstupu je pouze k dispozici málo bitů) a tento postup dále zobecňuje.

2.2 R.Renner, S.Wolf : Bezpodmínečná autenticita a soukromí z libovolně slabého tajemství – autoři v prácí ukazují, že i v případě nezabezpečeného komunikačního kanálu, sdílené bity, i když je libovolně velký zlomek z nich znám protivníkovi, mohou být užity pro kryptografické účely, jako je autentizace zpráv a šifrování, a to s využitím oboustranné komunikace.

3.1 J.Katz, M.Young : Škálovatelné protokoly pro výměnu klíče k autentizaci ve skupině – v práci je nově navržen tzv. škálovatelný protokol pro výměnu klíče mezi n-účastníky.

3.2 J.Camenisch, V.Shoup: Prakticky ověřitelné šifrování a dešifrování pomocí diskrétního logaritmu - autoři prezentují nové varianty asymetrického šifrování s aplikací na protokoly a jejich konkrétní využití

3.3 Y. Ishai a ost.: Výkonnější rozšíření tzv. nevnímaných sdílení – autoři prezentují výkonnější způsob rozšíření tzv. nevnímaných sdílení v náhodném „oracle“ modelu..

4.1 F. Armknecht, M. Krause : Algebraické útoky na směšovače s pamětí – A(k,l) směšovačem s pamětí autoři rozumí k paralelních lineárních registrů se zpětnou vazbou a nelineárním filtrováním konečným automatem s k vstupujícími a l paměťovými bity. V příspěvku ukazují, že na takováto zařízení je možný algebraický útok.

4.2 N.T.Courtois : Rychlé algebraické útoky na proudové šifrátory s lineární zpětnou vazbou – v práci je prezentována metoda urychlující algebraické útoky na tyto šifrátory, která je založena na Berlekamp-Masseyových algoritmech.

4.3 A. Biryukov a ost.: Kryptoanalýza SAFER++ - autoři ukazují kryptoanalýzu této 128-bitové blokové šifry až do čtvrtého cyklu.

4.4 B. Canvel a ost.: Zachycení hesla v SSL/TLS kanálech – je rozšířena Vaudenayova práce z EUROCRYPTU´02 a ukázána možnost zachycení hesla v SSL/TLS kanálech.

4.5 E.Barkan a ost.: Okamžitá kryptoanalýza pouze ze zašifrovaného textu u GSM šifrované komunikace – v práci je ukázána kryptoanalýza GSM šifrované komunikace a zpochybněna bezpečnost GSM.

4.6 P.Oechslin : Vytvoření rychlejší kryptoanalytického „trade-off“ s časovou pamětí – autor ukazuje zkrácení času potřebného ke kryptoanalýze použitím předvýpočtem dat uložených v paměti.

5.1 I.Damgard, J.B.Nielsen : Universální složený účinný mnohostranný výpočet z prahového homomorfického šifrování – v práci je prezentován nový mnohostranný výpočetní protokol pro bezpečný scénář šifrování, který je universálně složitelný.

5.2 R.Canetti a T.Rabin : Universální složení se spojovým stavem – autoři prezentují nové operace složení , kdy různé komponenty mají jisté množství spojení a nahodilostí, a ukazují dostatečné podmínky, kdy tyto nové operace složení zachovávají bezpečnost.

6.1 D..Micciancio, S.P.Vadhan : Statistické „ Zero-Knowledge“ důkazy s účinnými prokazovateli: Mřížkové problémy a více – v práci se konstruují nové statistické „ Zero-Knowledge“ důkazy a aplikují se na problémy výpočetní složitosti.

6.2 B.Barak a ost. : Derandomizace v kryptografii – jsou zde ukázány dvě aplikace pseudonáhodných Nisan-Wigdersonových generátorů v kryptografii.

6.3 R.Pass : O odmítnutí v modelech „ Společně zmíněného řetězce“ a „Náhodného oracle“ –v této práci je revidovaná definice „ Zero-Knowledge“ v uvedených modelech.

7.1 Qi Cheng : Prokazování prvočíselnosti pomocí jednoho cyklu ECPP a jedné interakce v AKS – v práci je ukázáno zjednodušení složitosti při prokazování prvočíselnosti jedním z výše uvedených algoritmů.

7.2 K.Rubin, A.Silverberg : Kryptografie založená na torusu – je zde prezentována nová kryptografie s veřejným klíčem založená na jistých vlastnostech algebraického torusu.

8.1 Y.Komano, K.Ohta : Účinná universální vycpávková metoda pro jednocestnou multiplikativní permutaci se zadními vrátky – v práci je prezentované nové schéma elektronického podpisu založené na optimálním asymetrickém šifrování.

9.1 C.Dwork a ost. : Paměťově omezené funkce pro boj se „spam“- autoři ukazují, že paměťově omezené funkce pro boj se „spam“ (nežádoucí komerční e-mail) jsou účinnější, než použití CPU- funkcí pro tyto účely.

9.2 N.Buchbinder, E.Petrank: Dolní a horní hranice pro obdržení historie nezávislosti – autoři se zabývají historiií datových struktur a stanoví omezení nezávislosti dat, tj. kdy tato byla nezávislá na protivníkově manipulaci.

9.3 Y.Ishai a ost.: Soukromé obvody: bezpečný hardware proti sondovým útokům – v práci jsou položeny teoretické základy bezpečnosti proti útokům postranními kanály.

10.1 S.Halevi, P.Rogaway: Zakroucená šifrovací forma – autoři v práci popisují novou formu blokové šifry a ukazují její bezpečnost.

10.2 M.Carry , R.Venkatesan: Textový autentizační kód založený na unimodulárních maticích – v práci je prezentována nová konstrukce, založená na modulárních grupách.

10.3 J.Patarin: Luby-Kackoff: 7 cyklů je dostatečných pro bezpečnost… - v práci jsou řešeny nové problémy související s náhodnými Feistelovými schématy.

11.1 O.Horowitz, V.Gligor: Autenticita slabého klíče a vypočítatelná úplnost formálního šifrování – v práci jsou ukázány nutné a postačující podmínky pro vypočitatelnou úplnost v kryptografii.

11.2 J. Herzog a ost. : Povědomí otevřeného textu přes registraci klíče – autoři prezentují nový model tzv.“ plaintext-aware“ šifrování.

11.3 R.Canetti a ost. : Rekreační „Chosen – Ciphertext“ bezpečnost – je prezentována nová relaxační varianta útoků pomocí vybraných zašifrovaných textů a navrhnuta tzv. RCCA bezpečnost.

Kromě výše uvedeného výčtu přednášek, byly prezentovány dvě přednášky zvané, uvedené rovněž ve sborníku konference:

I. M. Naor : O kryptografických předpokladech a výzvách – autor řeší problém výpočetních předpokladů potřebných pro bezpečná šifrovací schémata.

II. H.Krawzyk : SIGMA: „SIGn-and-Mac“ přiblížení k Diffie-Hellmanově autentizaci a použití tohoto pro IKE protokoly – autor ukazuje že SIGMA zaručuje dokonalou bezpečnost při Diffie-Hellmanově autentizaci s digitálním podpisem.

Konference CRYPTO´03 kromě oficiálního přednáškového obsahu přinesla účastníkům možnost řady osobních setkání a osobních diskusí k odborným tématům. Byla jako obvykle doprovázena prodejem krypto-literatury ve zlevněných cenových relacích, čehož řada účastníků využila ke koupi zajímavých titulů. Celkově byla jak účastníky , tak IACR hodnocena na jeho zasedání jako úspěšná.

Pro možné praktické aplikace v nejbližších letech se řadě účastníků jevil pokrok se zařízením TWIRL, ukazující reálnou možnost rozbití 1024 bitového RSA klíče v horizontu jednoho roku, a tudíž nutnost např. pro bezpečné bankovní transakce k přechodu k 2048 bitovým klíčům.

Velice varovná je situace v GSM komunikaci, kde je použito slabých algoritmů a např.GSM bankovní transakce nemusí být bezpečné, což je alarmující a vyzývá to k přechodu na třetí generaci mobilní komunikace, jelikož se ukazuje, že druhá a ani „dvaapůltá“ generace plně zabezpečit nelze. To je výzva pro většinu světových mobilních operátorů.

DATAKON 2003

Nezapomeňte:

ZA 4 DNY KONČÍ OBDOBÍ VČASNÝCH REDUKOVANÝCH PLATEB!

termín konaní konference: 18. - 21. 10. 2003

včasná platba : do 19.9.2003

místo konaní konference: Hotel SANTON, Brno

podrobné informace viz : http://www.datakon.cz/

nebo e-mailem: staudek@informatics.muni.cz

F. AEC Trustmail (recenze)

Michal Till, student MFF UK (http://www.krypta.cz, michal.till@krypta.cz)

Při práci s osobním počítačem uživatel každou chvíli narazí na pojmy jako certifikát, certifikační autorita, klíč apod. Čas od času někdo pošle podepsanou zprávu, sem tam na nás v prohlížeči vyskočí okénko se "zámečkem" (říkaje něco o důvěře v certifikát…). Na platformě Windows je přitom implementace těchto bezpečnostních technologií pro uživatele z velké části omezena jen na koncové produkty, typicky Outlook a Internet Explorer. Cílová skupina, která bývá označována jako "home-users" si tak, často dle hesla "Nemusím vědět proč, jak a co to dělá, hlavně když to funguje a moc mě to nezatěžuje...", přijde často na své, ovšem častokrát by byl vhod nástroj, který by (mimo jiné) zmiňované prvky dokázal spravovat inteligentněji a s důrazem na alespoň základní znalosti uživatele v oboru bezpečnosti.

Produkt TrustMail, od Brněnské společností AEC, který je předmětem této recenze, by měl v sobě, dle materiálů, kombinovat několik výše popisovaných funkcí a proto neváhejme a pojďme se podívat, jak na tom skutečně je.

Instalace: bez problémů

TrustMail je k dispozici ve dvou verzích: Vedle té „plné“ je zde ještě Lite, kde jste licenčním klíčem omezeni na funkčnost - je určena pouze pro stranu příjemce, tj. umí dešifrovat a ověřit podpis).

Balík má necelých 7 MB, což je velikost snesitelná i pro vytáčené připojení, na webu AEC si můžete stáhnou prakticky všechny výše popisované verze. V době testování redakcí byl poslední build k dispozici zatím jen v angličtině, což nevadí.

Samotná instalace proběhla bez problémů, stačilo „odenterovat“ několik klasických obrazovek instalačního programu a bylo hotovo. Nyní stačí jen kliknout na ikonku na ploše...

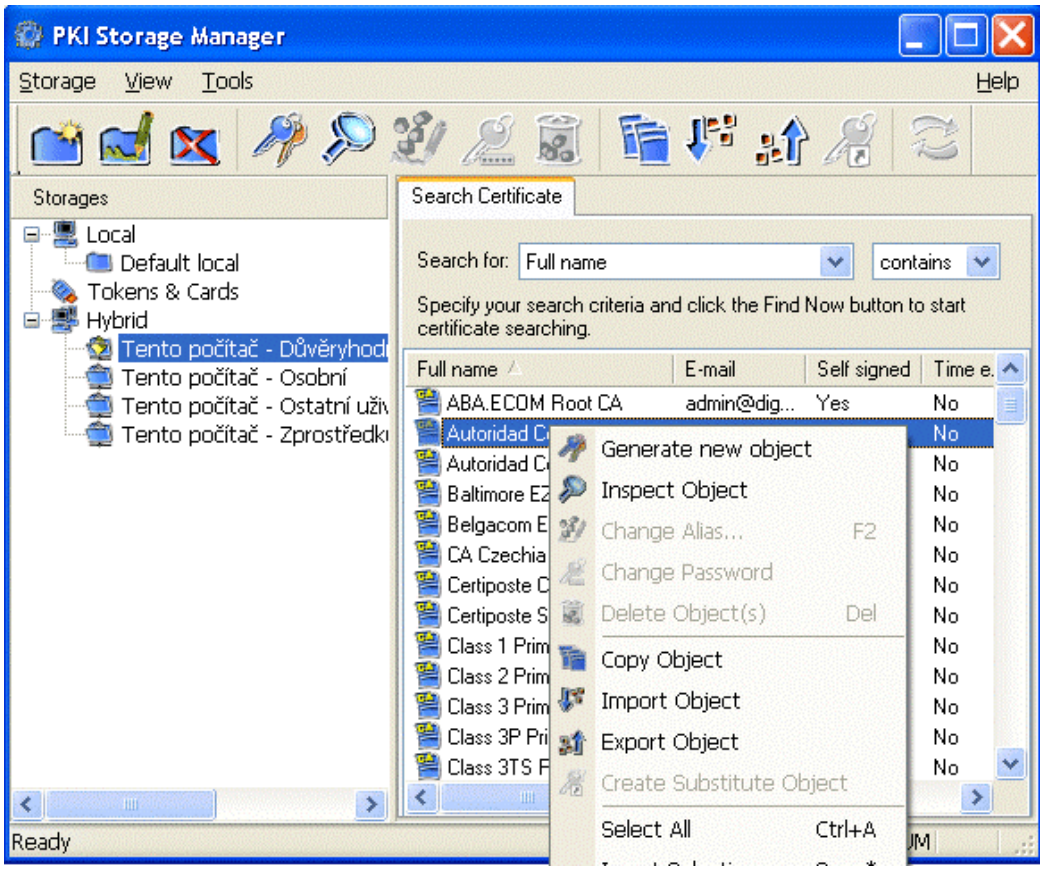
Jak do toho?

Řekne-li se "šifrování" na osobním počítači, nebo ještě lépe "asymetrická kryptografie", leckomus se vybaví staré známé PGP, neboli Pretty Good Privacy. Máte-li s tímto produktem zkušenosti, nebude pro vás rozhodně těžké pochopit TrustMail, na druhou stranu si dobře uvědomíte rozdíl v pojetí infrastruktury veřejných klíčů, který mezi těmito produkty, resp. mezi PGP a nyní používanými systémy, je. Já se, také částečně z nostalgie, ještě o PGP párkrát zmíním, ukážeme si rozdíly a podíváme se také jako to je/není s kompatibilitou.

Několik komponent programu dohromady tvoří celek, jemuž vládne tzv. PKI Storage Manager. Podíváme-li se na obrázek základního uživatelského prostředí, bude nám patrně jasné, k čemu tato aplikace slouží.

Jejím cílem je správa klíčů a certifikátů (vpravo), které se mohou fyzicky vyskytovat na několika úložištích (Storages, vpravo). Čtyři tzv. Hybrid storages jsou základní úložiště implementované v systému Windows - s nimi jste se možná setkali při práci s Outlookem apod. Vedle toho pomocí Tokens&cards můžete ukládat a číst klíče uložené na nejrůznějších externích zařízeních (např. v PKCS#11/PCSC kompatibilních USB tokenech, čipových kartách apod. - více viz technické specifikace). Vlastní úložiště si můžete samozřejmě

vytvořit, a navíc i publikovat pomocí LDAP protokolu. To se může hodit mimo jiné například v menších firemních sítích a proto o této funkci ještě bude řeč.



V pravém panelu se zobrazují jednotlivé certifikáty obsažené v daném úložišti, popřípadě si můžete zvolit záložky, které zobrazují seznam zneplatněných certifikátů a další. V lokálním úložišti jsou objekty rozděleny do několika záložek: Private Keys, User's Personal Certificates, Other People's Certificates, Certification Authorities, CRLs a Search Certificates. Pokud náhodou vlastníte starší verzi a podivujete se nad tím, že obsažené certifikáty se zobrazí až po kliknutí na tlačítko "Search", a to ještě s jistou časovou prodlevo v řádu pár sekund, zamiřte na webové stránky AEC, protože v minulosti volený způsob zobrazování nedává uživateli mnoho informací , které certifikáty jsou jeho a které jsou cizí.

Generování klíče a příslušného certifikátu začnete kliknutím na ikonku dvojitého klíče. Hned na první obrazovce se vás průvodce zeptá jak, resp. kam chcete klíč vytvořit. Můžete si totiž zvolit "Generate into storage", kdy se nový klíč přidá do úložiště, nebo "Generate by storage", kdy se klíč pro větší bezpečnost vytvoří v úložišti samotném (různé karty apod.). Poslední volba nabízí uložení jen do externího souboru. Další proces je velmi intuitivní a prakticky není čemu nerozumět - vyplníte osobní údaje, délku klíče, můžete si zvolit i algoritmy či použití klíče. Náhodná čísla, které program k výpočtu potřebuje, "dodáte" asi půlminutovým mačkáním kláves a hýbáním myši.

Poté, co jsme vygenerovali pár klíčů nám ještě zbývá tvorba certifikátu - program umožňuje tvorbu tzv. self-signed certifikátu, kde pár klíčů je podepsán jen vlastním klíčem privátním, nebo vám vytvoří do extra souboru žádost o certifikát (Certificate Request). Já jen doplním, že pokud není klíč alespoň self-signed (tj. prostě není "něčím" podepsán), Windows s ním pochopitelně odmítají spolupracovat. To je logické mimo jiné proto, že podpis stvrzuje, že klíč nebyl pozměněn, i když útočník by samozřejmě podvrhnutý klíč podepsal také.

Pokud chceme kryptografii používat například pro ochranu elektronické pošty, musíme vygenerovaný certifikát vložit do systému (Windows) - to, že po vygenerování skončil v Lokálním úložišti nestačí. Tam ho ale bohužel nedostaneme přímo (například "přetáhnutím" - to by uživatel určitě ocenil), ale musíme ho vyexportovat a následně po kliknutí systém spustí vlastního "importovacího" průvodce, což celou proceduru poněkud prodlužuje. Pak už jen zbývá příslušnému účtu přiřadit klíče (Outlook tomu říká "Digitální ID") a bezpečná e-mailová komunikace je na světě.

Mimochodem zde jsem v rámci testování omylem exportoval a importoval jen veřejný klíč, což má samozřejmě katastrofální následky na funkčnost. Zvláště, když Outlook je natolik "inteligentní", že například při pokusu o digitální podpis (což bez privátního klíče samozřejmě nejde) napíše vskutku vyčerpávající hlášku "Zpráva nelze odeslat. Nastala chyba.". Uživateli pak nezbývá nic než hledat příčinu - když si necháte zobrazit použitý certifikát, musí tam být výslovně uvedeno, že jste majitelem soukromého klíče... Bohužel ani v TrustMailu se z výpisu certifikátů obsažených v úložišti nedá nijak jednoduše poznat (např. podle ikonky), zda jsem vlastníkem celého páru klíčů nebo zda jde jen o veřejný klíč někoho jiného.

Ostatní součásti

Vedle Storage Manageru se Trustmail skládá z několika dalších modulů. Jsou to defacto malé aplikace, které se nám často objevují v podobě dialogových oken a rozdělení balíku na tyto další funkční komponenty není pro běžného uživatele podstatné.

Zmiňme např. Trustmail Configurator, který mimo nastavení produktu (jak již název napovídá) spravuje i jednotlivé licence a právě zde se importují licenční klíče. Dále takzvaný LDAP Publisher, který, jak již bylo řečeno, umožňuje zpřístupnit úložiště pomocí LDAP protokolu ostatním počítačům sítě. Přistupovat k němu pak lze samozřejmě nejen Trustmailem, ale i dalšími aplikacemi ostatních výrobců. Menší nástroj Password Changer umožňuje měnit hesla k uloženým klíčům.

Používáme Trustmail

Správa certifikátů je pouze jednou částí produktu. Podívejme se nyní na program z druhé, praktické stránky. K čemu by aplikace sloužila, kdybychom nemohli klíče používat v praxi, tj. pohodlně šifrovat, dešifrovat, podepisovat apod.

K tomu zde slouží kontextové menu, které se zobrazí po kliknutí pravým tlačítkem na daný soubor. Vybavujete-li si obdobnou funkci u PGP, máte výhodu, neboť výše zmiňované akce jsou zde implementovány téměř shodným způsobem. Podle typu souboru systém vybere akce, které lze použít: standardně podepsat a/nebo zašifrovat, u zašifrovaného dešifrovat, u podepsaného ověřit atd. Dále po nás program může požadovat výběr šifrovacího klíče či zadání hesla k němu.

Při podepisování se vytvoří nový .sgn soubor, při šifrování .enc, inverzní operace se aplikují právě na tyto soubory. Ve starších mi chyběla možnost oddělit podpis do samostatného souboru (PGP: detached signature ;-), v současné verzi je již tato možnost podporována. Podpis lze také opatřit časovým (relativně nová služba AEC, o které možná příště).

Je zde implementována vlastnost, kterou jsem u PGP dlouhou dobu požadoval, a to sice vícenásobné podepisování souborů. Je totiž možné podepsaný soubor podepsat (jiným klíčem) ještě jednou, ale přitom se podepíše původní obsah a nikoliv obsah s prvním podpisem, čemuž se u PGP šlo obtížně vyhnout. Představíme-li si například obchodní smlouvu, může jeden soubor obsahovat několik podpisů jejího textu, přitom se vždy podepisuje právě text, i když soubor již může nějaké podpisy obsahovat.

Samozřejmostí je funkce současného podepsání a zašifrování, stejně tak jako kontextové funkce pro import nových klíčů/certifikátů do systému.

Formát podepsaných a šifrovaných dat vychází z PKCS#7, dnes upravené do Cryptographic Message Syntax (CMS) nebo RFC3369, což jsou de facto standardy.

Vzpomínáte na PGP?

Pro svoji intuitivnost a rozšířenost se stále používá, ovšem vše se pochopitelně ubírá jiným směrem. Pokud vás zajímá kompatibilita, patrně vás zklamu. PGP úspěšně „pozře“ klíče ve formátu PKCS#12 (.p12), stejně tak jako některé verze rozumí certifikátům X.509, jenže tím vše končí. Balení podepsaných/zašifrovaných zpráv je pochopitelně jiné, stejně tak jsou problémy s certifikáty. Jak jsem se dozvěděl přímo od výrobce, samotná konverze PGP klíčů na p12 není teoreticky problém, nicméně veřejné klíče X509 mají jinou strukturu (chybí issuer apod…) a proto není tato „větev“ perspektivní, i když by to jistou komerční výhodu patrně představovalo.

Pokud se budete snažit provést něco jako „Podepsat klíč“, narazíte. Trustmail není certifikační autoritou a filozofii PGP je třeba opustit.

Publikování úložišť

Zvláště v prostředí malých sítí, kde není k dispozici na tuto funkci speciální hardware a software, může přijít vhod možnost vytvořit centrální databázi certifikátů, která pak může být přístupná ostatním uživatelům. Pro tento účel se Trustmail hodí, neboť podporuje všechny potřebné protokoly.

Z kontextového menu úložiště vyvoláme LDAP Publisher, kde lze publikaci či její zrušení provést. Na systémech Windows řady 9x budeme nuceni restartovat počítač, používáme-li řadu NT, spustí se služba systému. Její status můžeme opět zkontrolovat v LDAP Publisheru. Zbývá jen dodat, že připojení se provádí pomocí funkce "Add LDAP connection..." z menu Storage.

Závěr

Bez pochybností mohu říci, že již samotnou existenci takovéhoto produktu považuji za velmi pozitivní věc. Jde totiž o to, že v současné době je dle mého názoru velmi velká nerovnováha mezi povědomím o kryptografii a jejími skutečnými možnostmi. Zatímco v dnešním světě plném přebujelé byrokracie a různých spoléhání-se v bezpečnosti na to či ono je teoretické uplatnění asymetrického šifrování obrovské, povědomí (i pokročilejších)

uživatelů počítačů o tomto oboru je nedostačující. Co se popularizace jako takové týče, myslím, že jsme se posunuli o velký kus kupředu, nicméně v praxi stále ještě zaostáváme, a to především v těch každodenních situacích, kdy nám přístupová hesla leží na freemailu či na serveru ICQ atd…

Troufám si tvrdit, že instalace produktu, jako je Trustmail, na takřka každém počítači, který je připojen k Internetu je z dlouhodobého hlediska nevyhnutelná věc a jedná se o nutnou podmínkou posunu k nějaké sofistikovanější e-společnosti, ve které se nebude uvádět kolik tisíc lidí „již" podalo daňové přiznání elektronicky, ale naopak kolik ještě lidí ho stále podává u přepážky.

Použitelnost recenzované aplikace pro tento účel po delším zkoumání hodnotím jako velmi dobrou, snad jen celkový dojem působí snad až moc profesionálně, včetně uživatelského prostředí. Nicméně výběr cílové skupiny uživatelů je samozřejmě záležitost výrobce. Mě bych patrně, vzhledem k mému zájmu o kryptografii a její využití v širších oblastech, potěšilo, kdyby verze Lite (či některá obdobná zdarma) poskytovala alespoň „kompletní základní" nástroje pro použití asymetrického šifrování.

Z funkčního hlediska jsem nenašel žádný zásadní a objektivní nedostatek, přijmu-li filozofii PKI, jakou Trustmail a podobné produkty razí. Otazník, který jsem v průběhu recenzování v mysli připsal k některým funkcím a vlastnostem, se týká jen méně podstatných drobností, ne-li mých vlastních subjektivních názorů a zvyků. Myslím, že jde o více než příjemnou volbu pro všechny, kteří chtějí kryptografii aktivně využívat ke svému užitku a požadují skutečně osobní dohled nad vším kolem.

Technické údaje (uváděné výrobcem):

TrustMail podporuje tyto mezinárodní standardy:
- pro vytváření digitálního podpisu: PKCS#11/PCSC;
- pro digitální certifikáty: PEM, P7C;
- pro podpisové klíče: P12.

Použité algoritmy a délky klíčů:
- asymetrické: RSA 1024 až 4096 bitů, DSA 1024 bitů, ECC 192 až 256 bitů;
- symetrické: CAST 128 bitů, RC2 40 –128 bitů, BlowFish, DES, 3DES;
- HASH: SHA1, SHA-256 až 512 bitů, MD5, RIPEMD 160.

Hardwarová zařízení:
Rainbow iKey 2000 (2032), Eutron CryptoIdentity, Eutron SocketReader, ActivCard, DataKey, Towitoko ChipDrive, Spyrus USB Token, Aladdin eToken Pro, Chrysalis Luna (potřebují vlastní ovladače)

Systémové požadavky
- procesor Pentium (doporučeno Pentium II 200 MHz nebo vyšší);
- Microsoft Windows 98, Me, 2000, XP, NT 4.0 (nutný Service Pack 6);
- Internet Explorer 4.01 a vyšší;
- 32 MB RAM (doporučeno 64 MB);
- 10 MB volného diskového prostoru

G. Letem šifrovým světem

1. Volné pozice v kryptologii

Společnost **Ace Point** hledá vhodné kandidáty na následující pozice:
1. Konzultant specializující se na autentizaci, šifrování a elektronické certifikáty pro externí spolupráci na peer-to-peer networking projektu. Nutností je velmi dobrá znalost dané problematiky a kreativita.
2. Programátor C++, velmi zkušený, do týmu vyvíjejícího novou generaci P2Pnetworking klienta. Znalost MFC a kryptografie výhodou.
Zajímavé mzdové podmínky. V případě zájmu kontaktujte Simonu Tymichovou na tymichova@acepoint.cz.

2. AEC RoadShow 2003

(text převzat z eBulletinu AEC 11/2003)

Na přelomu září a října 2003 se uskuteční třetí ročník akce zaměřené na šíření osvěty o počítačové bezpečnosti po České republice - AEC RoadShow. Jedná se o tradiční cyklus seminářů pořádaný v šesti městech České republiky pod záštitou odborníků z AEC.

Vstup na akci je ZDARMA!

AEC RoadShow 2003 se bude konat v následujících termínech a městech:
23. září - Brno, sídlo společnosti AEC (Bayerova ul. 799/30).
24. září - Ostrava, Hotel Imperial (Tyršova 6).
25. září - Zlín, Interhotel Moskva (Nám . Práce 2512).
30. září - Hradec Králové, Hotel Alessandria (Třída SNP 733).
1. října - Praha, Stimbuilding - pobočka AEC (Vinohradská 184).
2. října - Plzeň, Hotel Victoria (Borská 19).

Program akce bude ve všech lokalitách stejný: od 9:00 hod. začíná prezence účastníků, vlastní program v 9:30 hod. a konec je naplánován na 13:30 hod. Účastníci AEC RoadShow 2003 si letos budou moci vyslechnout následující přednášky:

- Síťoví červi
- Představení bezpečnostního produktu
- Velké bezpečnostní incidenty
- Novinky z vývojových laboratoří AEC
- Elektronický podpis - mýty, sliby, realita
- Zbytečné otázky v antivirové ochraně

Každý účastník AEC RoadShow 2003 obdrží informační a odborné materiály, v průběhu akce je zajištěno občerstvení.

Mediálním partnerem celé akce je počítačový měsíčník PC World.

Svoji účast zaregistrujte pomocí webového formuláře, který najdete spolu s dalšími informacemi na http://roadshow.aec.cz , nebo e-mailem na adrese seminare@aec.cz , telefonní spojení 541 235 466.

3. O čem jsme psali v září 1999 - 2002

Crypto-World 9/1999

Crypto-World 9/2000

+ příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

H. Závěrečné informace

1. Sešit

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

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

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

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

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@ct.cz