Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 7-8/2003 **6. srpen 2003**

7-8/2003

Připravil : Mgr.Pavel Vondruška

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

Obsah : **Str.**

Příloha: „zábavná steganografie“ (steganografie.doc)

A. Cesta kryptologie do nového tisíciletí I.
(Od Kámasutry k osobním zápiskům K.H.Máchy)
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

V roce 2000 jsem uveřejnil v časopise COMPUTERWORD čtyř dílný seriál – Cesta kryptologie do nového tisíciletí. Články vzbudili poměrně kladný ohlas. Seriál byl do konce minulého roku dostupný na stránkách vydavatele i v elektronické podobě. Protože již uběhli tři roky a elektronická podoba článků již není dostupná, rozhodl jsem celý seriál na stránkách našeho e-zinu opět zpublikovat a to v původní, neupravené verzi. Dnes tedy začneme prvním dílem, který se věnuje základním pojmům a historickým kořenům kryptologie.

Základní pojmy

Kryptologie (zjednodušeně věda o utajení obsahu zpráv) je věda, která má stále mezi lidmi nádech tajemna. Není to tak dávno, co se dokonce knihy o kryptologii daly v knihovnách najít ve stejném oddělení jako knihy o alchymii nebo hvězdopravectví. V oficiálním třídění matematických věd také nebyla kryptologie dlouho uvedena a trochu živořila ve stínu matematiky a informatiky.

Kryptologie se dělí na kryptografii a kryptoanalýzu a někdy se také uvádí, že obsahuje steganografii.

Kryptografie se zabývá matematickými metodami se vztahem k takovým aspektům informační bezpečnosti, jako je důvěrnost, integrita dat, autentizace entit a původu dat. Ve starším chápání to byla především disciplína, která se zabývala převedením informace do podoby, v níž je obsah této informace skryt. Jejím úkolem bylo tedy především učinit výslednou zprávu nečitelnou i v situacích, kdy je plně prozrazená, zachycená třetí - nepovolanou stranou. Tím se liší od steganografie, jejímž úkolem je skrýt samotnou existenci zprávy, ale zpráva samotná může být napsána nebo předána ve srozumitelné podobě. Kryptoanalýza je pak jakýsi "opak" kryptografie. Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu (nebo alespoň část skrytých informací). Kryptoanalýza se zabývá analýzou odolnosti (síly) kryptografického systému a metodami vedoucími k proniknutí do kryptografického systému. Tento proces se nazývá luštění šifrové zprávy a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového systému, řekneme, že šifra byla zlomena nebo rozbita.

Hlavním cílem kryptografie byl tedy rozvoj algoritmů, které lze použít ke skrytí obsahu zprávy před všemi s výjimkou vysílající a přijímající strany (utajení) a mnohem později také přibyl rozvoj algoritmů sloužících k jednoznačnému určení osoby odesílatele (identifikaci) a k ověření správnosti zprávy přijímající stranou (autentizaci) a další související algoritmy. Původní vysílanou zprávu nazýváme otevřeným textem. Tato zpráva je následně šifrována pomocí nějakého kryptografického algoritmu. Zašifrované zprávě říkáme šifrový text. Odšifrování je opačný postup vzhledem k zašifrování, je to převedení šifrového textu zpět do podoby otevřeného textu.

Starověká kryptografie

Kryptografie prodělala dlouhý vývoj. Prvé pokusy o utajení obsahu zpráv jsou známé již ze starého Egypta a Mezopotámie. Jednalo se o nejprimitivnější systémy, které spočívaly v nějaké mírné, zpravidla neobvyklé úpravě písma. Takovéto malé změny zcela postačovaly, již samotná znalost písma byla v té době jistým druhem umění a pro většinu populace zůstával obsah nápisu stejně utajen.

Ve staré Indii se situace změnila. Zalistujme ve známé učebnici erotiky Kámasútře. V části "Smyslná žena" se hned v úvodu dozvíme mezi 64 radami ženám, které chtějí mít

úspěch u mužů : "Osvojte si tajná písma a šifry nebo si vynalezněte vlastní. Důležitá je také znalost nových způsobů mluvy, abyste mohla obratně měnit začátky a konce slov tak, jak právě potřebujete." V komentáři ke Kámasútře Yašodhara popisuje některé z používaných tajných písem. Jedním z uvedených systémů je "muladeviya", kde zašifrování spočívá pouze v použití reciproční abecedy. Existují záznamy, že tento systém byl používán i v mluvené podobě mezi obchodníky.

Kořeny skutečné kryptologie jsou však spjaty až s dějinami Řecka.

Téměř každá učebnice šifrování začíná popisem toho, jak Řekové pro utajení zpráv používali poněkud (dnešní terminologií neoperativní) způsob - oholili svému poslu hlavu, napsali na jeho lebku vzkaz a když mu vlasy opět narostly, mohl se vydat na cestu. Ve skutečnosti je však zaznamenán jen jeden takový způsob použití, popsal jej Herodotos ve svých Dějinách. Odesílatelem zprávy byl Histiaeus a zprávu napsal na hlavu svému oddanému otroku, který ji takto dopravil do Milétu a pomohl tak ke koordinaci povstání proti Peršanům.

Jedna z nejdůležitějších zpráv pro existenci západní civilizace byla také předána utajeně. Jednalo se o zprávu, která pomohla Řekům v boji proti Peršanům. Demaratus, syn Aristona, zjistil termín, kdy král Xerxes vytáhne s armádou proti Řekům. Rozhodl se o tom své krajany informovat, seškrábal vosk ze dvou dřevěných psacích destiček a přímo na dřevo zprávu napsal. Tyto destičky opět zalil voskem, aby to při náhodné kontrole vypadalo, že nejsou použité. Zpráva se dostala na místo určení, manželka krále Leonidase Gorgo odhalila tajemství destiček a zpráva byla přečtena. Zbytek známe z hodin dějepisu - následovaly slavné bitvy u Thermopyl, Salaminy a Plataea. Postup Peršanů do Evropy byl jednou pro vždy zastaven a v důsledku toho se mohla rozvinout západní civilizace.

Oba systémy - vyholená hlava a zápis na dřevo pod vosk - jsou představitelé systémů určených pro tajný přenos zprávy. Z hlediska dnešní terminologie jsme se tak seznámili s nejstaršími aplikacemi steganografie.

Řekové však neskončili jen u utajování přenosu zpráv - dokázali vyvinout skutečné šifrové systémy. Sparťané, nejbojovnější z Řeků, vymysleli a prokazatelně používali již v pátém století před naším letopočtem zařízení na utajení zpráv. Tento systém se skládal ze dvou holí ("skytale" nebo někdy psáno "scytale") přesně stanovené šířky (šířka = symetrický klíč zařízení), na prvou hůl se navinul pás látky, papyru nebo pergamenu. Na tento materiál se potom napsala zpráva, a to směrem dolů po délce hole. Pás s textem se sejmul a posel (komunikační systém) jej odnesl na místo určení. Tam byl pás látky navinut na druhou hůl a zpráva mohla být přečtena. Toto zařízení pracovalo na principu dnes nazývaném jako transpozice - promíchání otevřeného textu. Nepovolaná osoba sice mohla snadno přečíst všechna písmena otevřeného textu, ale díky použitému systému neznala jejich pořadí. Jedná se o nejstarší známé kryptografické zařízení.

Řecký spisovatel Polybius zase vynalezl systém signalizace, který byl později převzat jako další základní kryptografická metoda. Seřadil písmena do čtverce a jejich řady a sloupce očísloval. Každé písmeno tak je reprezentováno dvěma čísly - číslem řady a číslem sloupce. Polybius pak dále doporučoval, aby tato čísla byla předávána pomocí pochodní. Např. písmeno v prvém řádku a pátém sloupci by bylo odesláno pomocí jedné pochodně v levé ruce a pěti pochodní v pravé ruce. Zprávy tak mohly být odeslány bezpečně a rychle na velké vzdálenosti. Polybiův čtverec (šachovnice), který umožňuje převod písmen na číslice, se stal základem mnoha dalších šifrových systémů.

Římané nepřevzali tyto systémy od Řeků, vydali se vlastní cestou. Kolem přelomu našeho letopočtu prokazatelně zavedli vojenskou kryptografii. Zprávy mezi legiemi nebyly zasílány otevřeně, ale pomocí záměny otevřeného textu za šifrový text. Julius Caesar vypráví o využití těchto systémů v "Zápiscích o válce galské". Známý životopisec Suetonius pak dokonce prozrazuje, jak systém přesně vypadal. Každé písmeno zprávy bylo zaměněno za

písmeno, které leželo o tři místa dále v abecedě. Suetonius dále popisuje, že Caesarův synovec Augustus používal podobný systém, ale nahradil písmeno otevřeného textu písmenem stojícím v abecedě těsně za ním. Výjimkou bylo poslední písmeno X, které nahradil dvojicí AA. Kryptografie ve starém Římě se stala naprostou samozřejmostí. Mimo podobných záměn se ještě používalo vkládání kódů pro jména osob, zemí apod.

Hlavní systémy pro bezpečný přenos dat, byly na světě: utajování přenosu dat, transpozice, používání kódů a záměny znaků otevřeného textu podle určitých pravidel za jiné znaky. Všechny výše uvedené systémy jsou symetrické - příjemce i odesílatel jsou dohodnuti na stejném principu a klíči.

Středověká kryptologie

Skutečná kryptologie se však zrodila teprve díky vynikajícím arabským matematikům. Roku 855 našeho letopočtu Abú Bakr Ahmad ve své práci popisuje různé šifrové záměnné systémy. Jedna z popisovaných substitučních abeced se v arabském světě dokonce beze změny používala ještě v roce 1775 (!!!), kdy jí bylo použito v dopise s choulostivými informacemi pro alžírského vládce.

Arabové byli první, kdo objevili a popsali metody kryptoanalýzy. Souhrn arabských poznatků je uveden v jednom oddíle ("Utajování tajných zpráv v dopisech") rozsáhlé čtrnáctidílné encyklopedie Subh al-á sha, která byla dokončena r.1412.

Na práce arabských matematiků a kryptologů navázala středověká Evropa. Významným představitelem evropské kryptografie byl benediktinský opat ze Spanheimu Johannes Trittheim (1452-1518). Kolem roku 1500 napsal první významnější evropskou knihu o šifrování. Trittheim se zabýval převážně substitučními systémy. Zavedl a doporučoval vkládání klamačů do šifrového textu. Jednalo se o náhodné vkládání znaků do textu za účelem ztížení statistického rozboru. Panovnické rody (které běžně šifru ke komunikaci používaly) se však zalekly, že vyzradil příliš mnoho tajemství, a snad proto jej označily za čarodějníka.V 16. století se objevili i první slavní luštitelé. Jedním z největších byl francouzský právník a matematik Francois Viete (1540-1610), který luštil zašifrované depeše španělského krále a předával je francouzskému panovníkovi Jindřichu IV. Navarrskému. Trvalo několik let, než na to Španělé přišli. Nevěřili, že je možné jejich složitou záměnu rozluštit a žádali svatou stolici, aby postavila Vieta před soud, protože musí být spojen s ďáblem. I další významný kryptograf a kryptoanalytik Giovanni Battista della Porta (1541-1615) byl obviněn ze spojení s ďáblem. Porta navrhl tabulku složité záměny (odlišnou od systému Trittheima). V luštění složitých záměn byl velice úspěšný. Jeho hlavní povolání však bylo alchymista a dramatik. Do dějin se zapsal vedle kryptologie i přípravou kysličníku číničitého.

Nechci se zde však zabývat systematickým vývojem, který vedl dále přes různé formy záměn, nomenklátorů a polyalfabetických šifer. Základem všech těchto šifrových systémů byla vždy kombinace transpozice a jednoduché záměny již s vědomou snahou zakrýt charakteristiky jazyka.

Poznání, že výsledné šifrové texty lze na základě statistických metod luštit, vedlo ke zdokonalování šifrových systémů. Snahou bylo zahladit dodatečné informace, které byly v textu obsaženy, a tím zabránit analýze šifrového textu, která by mohla vést ke kompromitaci textu otevřeného. Spolehnutí se na nedokonalý systém tak například stálo skotskou královnu Marii Stuartovnu (1542-1587) život, neboť dopisy, ve kterých dala souhlas k připravovanému povstání a zavraždění anglické královny Alžběty, posloužily jako důkaz při soudním líčení. Používání slabé šifry k uchování osobního tajemství nám zanechalo i zajímavé svědectví ze života K.H.Máchy, který ve svých denících popisuje zašifrovaně své zážitky způsobem, který by mohl být po odšifrování přetištěn i dnešními erotickými časopisy.

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 14. Atributové certifikáty – díl 3.
Jaroslav Pinkava, PVT a.s.

1. Úvod

Dokument rfc.3281 (lit.[1]) definuje profil atributových certifikátů při použití v rámci internetových protokolů. V předešlých částech bylo hovořeno o požadavcích, které musí tento profil splňovat a dán popis samotného profilu. Dále budou popsány některé další podmínky pro práci s atributovými certifikáty.

2. Ověření platnosti atributového certifikátu.

K tomu, aby atributový certifikát byl platný, musí být splněno následující:

- pokud majitel AC používá ke své autentizaci vůči straně, která ověřuje atributový certifikát svůj certifikát veřejného klíče (CVK), pak se tento CVK musí nalézat na certifikační cestě, a verifikace CVK musí bát provedena způsobem, který odpovídá požadavkům dokumentu [7];
- podpis AC musí být korektní (z kryptografického hlediska) a rovněž tak certifikační cesta k vydavateli AC musí být ověřena v souladu s požadavky z [7];
-
- certifikát veřejného klíče vydavatele AC musí splňovat určité podmínky (jsou uvedené v odstavci 5 minulého dílu);
- vydavatel AC musí být v důvěryhodné úloze vydavatele AC (vhodně nakonfigurován atd.);
- čas v kterém je AC ověřován musí být uvnitř doby platnosti AC;
- cíl pro, který je AC určen musí splňovat podmínky definované pro příslušné rozšíření (3.10 v minulém dílu);
- pokud AC obsahuje nepodporované rozšíření, musí být zamítnut.

3. Odvolání AC

V některých prostředích je doba platnosti AC kratší než je čas nezbytný k vydání a distribuci informace o odvolání certifikátu. AC s krátkou dobou platnosti nevyžadují podporu pomocí systému odvolání. Avšak AC s dlouhou dobou platnosti a v prostředích, kde jsou prováděny transakce mající vysokou hodnotu (finanční, informační) lze vyžadovat podporu odvolávání AC.

Z tohoto důvodu jsou definována dvě revokační schémata. V prvním z nich ("never revoke") je AC označen tak, aby bylo spoléhající se straně zřejmé, že žádná informace o odvoláních již nebude dostupná (rozšíření noRevAvail).

Druhé schéma ("pointer in AC") umožňuje ukázat ověřující straně zdroj, kde nalezne příslušný revokační statut AC (použitím rozšíření `authorityInfoAccess extension` či rozšíření `crlDistributionPoints`).

4. Některé další (nepovinné) vlastnosti AC

Následující vlastnosti nemusí být v AC implementovány, pokud však implementovány jsou, musí to být níže popsaným způsobem.

- šifrování atributů: AC může obsahovat citlivé informace - např. hesla, pak lze vyžadovat šifrování atributů AC (použita je pak syntaxe dle CMS);
- AC a proxy na serverech - provádí se výhradně pod kontrolou vydavatele AC (použito je rozšíření ProxyInfo);
- v některých prostředích může být požadováno, aby AC nebyl přiřazen ke konkrétnímu jedinci či konkrétnímu CVK. Splnění tohoto požadavku umožňuje rozšíření `objectDigestInfo` v poli pro majitele AC. Lze pak vytvářet AC, které jsou přiřazeny např. k veřejným klíčům a ne ke jménům.
- rozšíření `AAControls` umožňuje provádět kontrolu důvěryhodnosti vydavatele AC (oprávnění vydat příslušný AC);

5. Bezpečnostní rozvaha

Kritickou je samozřejmě ochrana soukromých klíčů. V případě kompromitace soukromého klíče vydavatele AC musí být odvolány všechny jím vydané AC. Pokud dojde "jen" k poškození soukromého klíče vydavatele AC (a tedy jeho nenávratné ztrátě) nemůže pak tento vydavatel AC podepisovat odvolávací statut AC či provádět obnovu AC. Doporučuje se provádět bezpečné zálohování těchto klíčů. Dále - logicky je doporučováno použití silných kryptografických mechanizmů (krátký klíč limituje využitelnost AC). Při využívání (nepovinných) rozšíření je doporučováno dbát velice pečlivě na konfiguraci celého PKI, používání příslušných pravidel pro vytváření jmen jednotlivých aktérů PKI, je třeba používat (ověřující stranou) pouze ta rozšíření, která je atributová autorita oprávněna podepisovat. Je vhodné používat - pokud to konkrétní situace umožňuje - adekvátní bezpečnostní protokoly (TLS, S/MIME).

6. 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] Housley, R., Polk, T, Ford, W. and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002

C. Jak si vybrat certifikační autoritu

Ing. Dušan Doležal, CA Czechia, dusan.dolezal@interval.cz

Úvod

Cílem toho článku by měl být jakýsi „recept“ pro výběr certifikační autority a také přehled nejznámějších certifikačních autorit působících na českém trhu, a služeb, které nabízejí. I když člověk, který si certifikační autoritu vybírá, už by měl být alespoň rámcově seznámen s problematikou digitálního podpisu, dovolil bych se přesto na úvod stručně popsat, co to certifikační autorita je, co dělá, a k čemu ji vlastně potřebujeme.

Základním pilířem digitálního podpisu je asymetrická kryptografie. Ta sama o sobě je zárukou, že zpráva nebyla při přenosu pozměněna a hlavně že podpis vytvořil vlastník párového soukromého klíče (tedy samozřejmě za předpokladu, že je podpis platný). Abychom ovšem znali skutečného odesilatele zprávy, musíme jej nějak svázat se soukromým klíčem. Prostředkem, který tuto vazbu zajistí, je digitální certifikát. Certifikát je vlastně jakýmsi elektronickým průkazem, který potvrzuje, že daná osoba skutečně vlastní daný pár klíčů. Má to ale jeden háček, z technického hlediska může certifikát vystavit kdokoliv, dokonce ho může vystavit odesilatel sám sobě. Takový certifikát ovšem určitě není dostatečnou zárukou, že párový soukromý klíč opravdu vlastní osoba uvedená v certifikátu a že se za ní pouze někdo nevydává. Z tohoto důvodu je nutné, aby certifikát vydala nějaká třetí nezávislá strana, která bude dostatečně důvěryhodná pro obě komunikující strany. A tou je právě certifikační autorita.

Činnost certifikační autority by se dala přirovnat k činnosti notáře při ověřování klasického podpisu. Je zde ovšem jedna zásadní odlišnost - zatímco notář musí ověřit každý jednotlivý podpis, certifikační autorita neověřuje vlastní podpis, ale data pro vytváření digitálního podpisu, skutečných podpisů potom můžete pomocí těchto dat vytvořit libovolné množství. Jinak je ovšem postup analogický - certifikační autorita stejně jako notář musí zkontrolovat totožnost podepisující se osoby (respektive žadatele o certifikát), zajistit, že se skutečně podepisuje daná osoba (u klasického podpisu se osoba podepíše přímo před notářem, v případě digitálního podpisu musí prokázat vlastnictví daného páru klíčů), provést záznam potřebných údajů (do databáze, respektive do knihy), a následně vydá certifikát obsahující všechny potřebné údaje (notář připojí k dokumentu razítko, kde údaje vyplní) podepsaný svým soukromým klíčem (respektive vlastnoručním podpisem v případě notářského ověření).
Na rozdíl od notářského ověření podpisu, které je víceméně jednorázovým úkonem, je zde ovšem ještě jedna odlišnost. Protože digitální podpis se dá pomocí certifikátu (respektive s ním svázaného soukromého klíče) vytvářet opakovaně po celou dobu platnosti certifikátu, vzniká mezi certifikační autoritou a držitelem certifikátu obchodní vztah, který je také zpravidla podepřen uzavřením smlouvy, ze které pro obě strany vyplývají jisté povinnosti. Certifikační autorita na základě toho poskytuje další servis, jako například zneplatňování certifikátů a zveřejňování jejich seznamů, vydávání následných certifikátů a podobně. Držitel certifikátu se potom zavazuje, že poskytne certifikační autoritě přesné a pravdivé informace, bude ji informovat o případných změnách těchto údajů, bude chránit svůj soukromý klíč a, v případě jeho kompromitace, požádá certifikační autoritu o zneplatnění certifikátu.

Takže už víme, že se bez certifikační autority neobejdeme, proto bychom si měli říci, podle čeho vlastně certifikační autoritu vybírat. Nyní si tedy můžeme vyjmenovat

nejdůležitější kritéria, kterými bychom se měli při výběru certifikační autority řídit. Pořadí, v jakém budou jednotlivá kritéria uvedeny, by zhruba mělo odpovídat jejich důležitosti.

Důvěryhodnost certifikační autority

Toto kritérium je opravdu naprosto zásadní a zcela právem je uvedeno na prvním místě. Těžko nám pomůže, že certifikační autorita nabízí výborný produkt za dobrou cenu, když o ní nevíme zcela nic a ani nejsme schopni žádné údaje získat, případně si získané údaje ověřit. Přitom je třeba myslet na to, že certifikační autorita musí být důvěryhodná nejen pro nás, ale také pro toho, kdo se na podpis spoléhá, takže fakt, že certifikační autoritu provozuje můj kamarád, je pro mne zřejmě dostatečnou zárukou, zatímco pro příjemce zprávy to může být naprosto neznámá, a tudíž z jeho pohledu nedůvěryhodná certifikační autorita.

Ale na základě čeho máme vlastně důvěryhodnost posoudit a kde sehnat kýžené informace? Asi prvním místem, které navštívíme, budou webové stránky certifikační autority. Zde by rozhodně měli být k dispozici základní informace o certifikační autoritě, o organizaci, která ji provozuje, adresa jejího sídla, atp. Úplně nejdůležitějším dokumentem, který bychom tu měli nalézt, je tzv. Certifikační politika. S nadsázkou by se dalo říci, že certifikační politika je jakousi biblí certifikační autority a najdeme v ní veškeré údaje o certifikační autoritě, informace o typech vydávaných certifikátů a jejich atributech, způsob ověření totožnosti žadatele, podmínky pro vydání certifikátu, dostupnosti seznamu vydaných a zneplatněných certifikátů, odpovědnost za škody, atd. Přitom certifikační politika je pro certifikační autoritu závazná a není možné, aby se praktická činnost certifikační autority lišila od informací uvedených v certifikační politice - jestliže dojde k nějakým změnám oproti informacím uvedeným v certifikační politice, je třeba certifikační politiku revidovat.

Při posouzení důvěryhodnosti mohou hrát roli také další okolnosti, jako například reference ostatních uživatelů, praktická zkušenost s provozovatelem certifikační autority (certifikační autoritu často provozuje dceřinná, nebo jinak spřízněná, společnost jiné známé společnosti, v tom případě může samozřejmě znalost či zkušenosti s mateřskou firmou hrát významnou roli). V každém případě je důvěryhodnost certifikační autority částečně subjektivní záležitostí, pokud tedy dopředu víme, s kým budeme komunikovat, můžeme se pokusit předem dohodnout, zda je zvolená certifikační autorita důvěryhodná také pro příjemce a zda tedy bude certifikáty vydané touto certifikační autoritu akceptovat.

Při posuzování certifikační autority nám částečně pomáhá i zákon 227/2000 Sb. o elektronickém podpisu, které definuje následující tři typy certifikačních autorit (zákon používá označení Poskytovatel certifikačních služeb):
- poskytovatel certifikačních služeb
- poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
- akreditovaný poskytovatel certifikačních služeb

Přitom zákon (a dále vyhláška 366/2001 Sb.) poměrně přesně specifikuje povinnosti, které musí splnit certifikační autorita vydávající kvalifikované certifikáty a akreditovaná certifikační autorita a plnění těchto povinností může příslušný úřad (odbor elektronického podpisu Ministerstva informatiky, dříve Úřadu pro ochranu osobních údajů) kontrolovat, v případě akreditované certifikační autority je splnění těchto povinností posuzováno ještě před udělením akreditace. Vzhledem k tomu, že tyto podmínky jsou poměrně přísné, tak samotný

fakt, že certifikační autorita vydává kvalifikované certifikáty (nebo že dokonce obdržela akreditaci), je zřejmě dostatečnou zárukou její důvěryhodnosti.

Typ certifikátu

I když důvěryhodnost certifikační autority je zřejmě tím nejdůležitějším, čím bychom se měli řídit, je typ požadovaného certifikátu úplně prvním kritériem, podle kterého začneme certifikační autoritu vybírat. Existuje totiž velké množství typů certifikátu, a každá certifikační autorita vydává pouze určité typy certifikátů. Jestliže tedy potřebujeme např. serverový certifikát, a některá certifikační autorita jej nevydává, jejích služeb logicky nemůžeme využít a nemá smysl zkoumat její důvěryhodnost. Typickým příkladem jsou certifikáty pro autentizaci klienta v různých systémech elektronického bankovnictví, kdy banka většinou provozuje vlastní certifikační autoritu a certifikáty jiných certifikačních autorit zpravidla neuznává. Pokud tedy chceme takovýto produkt využívat, nezbývá nám v tomto případě nic jiného, než podmínky této certifikační autority akceptovat . To, jaké certifikáty certifikační autorita vydává, bychom měli opět najít na stránkách certifikační autority, zcela určitě potom musí být uvedeny v certifikační politice (zde je třeba upozornit na to, že certifikační autorita může mít více certifikačních politik, například pro každý typ certifikátu může mít samostatnou certifikační politiku).

Ještě bych se chtěl zastavit u jednoho typu certifikátu, a tím je kvalifikovaný certifikát a zejména potom kvalifikovaný certifikát od akreditované certifikační autority. Zákon 227/2000 Sb. totiž v paragrafu 11 říká, že v oblasti veřejné moci je možné používat pouze kvalifikované certifikáty od akreditované certifikační autority (resp. poskytovatele certifikačních služeb). Pokud tedy chceme například elektronicky podávat daňové přiznání, nebo žádat o sociální dávky, musíme zažádat o kvalifikovaný certifikát u certifikační autority, která obdržela akreditaci. V tomto případě ovšem fakticky nemáme možnost výběru, akreditace byla totiž udělena zatím pouze jediné certifikační autoritě (První certifikační autoritě), takže buď budeme její podmínky akceptovat, nebo si musíme počkat, zda akreditaci získá nějaký další subjekt.

Dostupnost certifikační autority

Dalším kritériem, které může výrazně ovlivnit výběr certifikační autority, je její dostupnost. Například u osobního certifikátu je totiž velmi často vyžadována osobní návštěva žadatele (někdy i vícekrát), a určitě není přijatelné, abychom kvůli získání certifikátu museli cestovat na druhou stranu republiky. Z tohoto důvodu certifikační autority často disponují sítí takzvaných registračních autorit, které provádí pouze ověření žádosti o certifikát a zkontrolování totožnosti žadatele, a dále všechny údaje předají certifikační autoritě, která na základě nich vystaví vlastní certifikát. Při výběru certifikační autority je proto vhodné zkontrolovat, jak daleko je nejbližší kontaktní místo, pokud bude tato vzdálenost příliš velká, asi bude vhodnější poohlédnout, zda není dostupnější jiná certifikační autorita.

Některé certifikační autority používají alternativní způsob ověřování totožnosti, kdy žadateli po podání elektronické žádosti zašlou papírovou smlouvu (případně si ji žadatel vytiskne sám v průběhu žádosti) a tuto smlouvu je třeba opatřit notářsky ověřeným podpisem a zaslat zpět do sídla certifikační autority. Notář (resp. jiný úřad, který má právo provádět úřední ověření podpisů) zde potom jakýmsi způsobem nahrazuje registrační autoritu, protože

při ověřování podpisu je povinen zkontrolovat totožnost podepisující se osoby. V tomto případě samozřejmě vzdálenost certifikační autority nehraje prakticky žádnou roli, na druhou stranu se tím poněkud prodlužuje doba potřebná pro získání certifikátu (protože doručení smlouvy poštou trvá jistou dobu) a také vznikají dodatečné náklady (poplatek za ověření podpisu).

Cena

I když cena, kterou za vystavení certifikátu zaplatíme, by rozhodně neměla být tím hlavním kritériem pro výběr certifikační autority, určitě to bude věc, která nás bude zajímat. Certifikátů totiž můžeme mít několik (a v budoucnu nám nepochybně jeden certifikát nebude stačit), takže pokud se na cenu nebudeme ohlížet, může nám jejich pořízení pěkně odlehčit peněženku. Vždy totiž záleží na účelu, pro který chceme certifikát využít, pro některé méně důležité případy použití může dostačovat certifikát nižší „kvality“ (třeba od méně známé certifikační autority, se slabším klíčem, atp.), naopak v případě důležitých transakcí určitě není vhodně šetřit a použijeme certifikát odpovídající úrovně.

Při porovnávání ceníků jednotlivých certifikačních autorit a různých typů certifikátů je také vždy třeba zohlednit další vlastnosti certifikátu, jako délka generovaného klíče (čím delší klíč, tím vyšší bezpečnost podpisu, ale často také vyšší cena), doba platnosti certifikátu (certifikáty jsou typicky vydávány na jeden rok, ale tato doba může být i jiná, například 6 měsíců, nebo dva roky), v ceně může být zahrnuto hardwarové zařízení pro uložení klíče, apod. Je také dobré zjistit, zda certifikační autorita vydává tzv. následné certifikáty a jaká je jejich cena, následný certifikát totiž bývá zpravidla levnější, než certifikát nový (navíc většinou není třeba znovu absolvovat proces ověření totožnosti, protože žádost o následný certifikát je podepsána platným stávajícím certifikátem.

Jenom pro úplnost je třeba dodat, že některé certifikáty je možné získat zdarma, například při různých akcích, jako doplněk nějaké další služby, apod. To že je certifikát zdarma vůbec nemusí znamenat, že je horší než certifikát placený, záleží jednak na atributech certifikátu (délka klíče, doba platnosti) a dále na tom kým a za jakých podmínek je certifikát vydáván. Na internetu je totiž možné například získat zdarma certifikát pro emailovou komunikaci, při níž ovšem není nijak kontrolována totožnost žadatele, ale například pouze existence zadané emailové schránky, takže důvěryhodnost takového certifikátu je pro příjemce pochopitelně prakticky nulová.

Další služby

Kromě výše uvedených kritérií je také dobré zhodnotit další služby, které certifikační autorita nabízí, například možnost uložení klíčů a certifikátů na bezpečném hardwaru (tokeny, čipové karty), sleva při objednání více certifikátů, možnost hromadného vydání více certifikátů v místě žadatele (například pro celou firmu), zda a za jakých podmínek je k dispozici technická podpora, případně školení, atp. Důležité je také, v jakých formátech je možné certifikát získat, zda je podporován internetový prohlížeč, který používáte (pozor, v tomto případě se nejedná o to, zda se vám správně zobrazí webové stránky, ale zda budou korektně vygenerovány podpisové klíče a zda bude možné správně nainstalovat a používat certifikáty, tyto funkce jsou v různých prohlížečích řešeny naprosto odlišně!), jak často je

vydáván seznam zneplatněných certifikátů (neboli CRL), jakým způsobem je možné o zneplatnění certifikátu požádat, a podobně.

Každopádně je výběr certifikační autority poměrně komplexní záležitost a není možné jednotlivá kritéria posuzovat odděleně bez ohledu na ostatní.

Dále bude následovat přehled nejznámějších certifikačních autorit v české republice a nejdůležitějších údajů o nich. Informace byly získány z webových stránek jednotlivých certifikačních autorit a z jejich certifikačních politik.

I.CA

Jedná se bezesporu o největší a nejznámější certifikační autoritu v České republice, která již na trhu působí několik let a vydala již více než 400.000 certifikátů. První certifikační autorita je zatím jedinou akreditovanou certifikační autoritou ve smyslu zákona o elektronickém podpisu a jako jediná také vydává kvalifikované certifikáty. Kromě kvalifikovaných certifikátů vydává I.CA také běžné komerční certifikáty.

Provozovatel: První certifikační autorita, a.s. (dceřinná společnost PVT, a.s.)
Sídlo: Podvinný mlýn 2178/6, 190 00 Praha 9
Adresa webových stránek: www.ica.cz
Počet kontaktních míst (resp. registračních autorit): cca 300
Typy vydávaných certifikátů: osobní certifikáty pro fyzické i právnické osoby, serverové certifikáty, kvalifikované certifikáty
Délka klíče: 512-1024 bitů, u serverových i více
Doba platnosti certifikátu: 6-12 měsíců, závisí na délce klíče
Možnost bezpečného hardwaru: čipové karty u varianty comfort
Způsob ověření totožnosti: osobní návštěva kontaktního místa, předložení 1 platného dokladu totožnosti
Způsob podání žádosti o certifikát: on-line na swebu, případně pomocí speciálního programu, který je možná ze stránek stáhnout
Způsob vydání certifikátu: osobně předáním na médiu + zaslání na udanou mailovou adresu
Způsob zneplatnění certifikátu: osobně, mailem podepsaným zneplatňovaným certifikátem, běžným mailem s heslem pro zneplatnění, pomocí SMS, telefonicky
Interval vydávání CRL: 24 hodin u komerčních certifikátů, 12 hodin u kvalifikovaných certifikátů

CA KPNQwest

Certifikační autoritu CA KPNQwest provozovala společnost KPNQwest, která se ovšem před již více než rokem sloučila se společností GTS (v současné době vystupují pod společným jménem GTS). Bohužel se zdá, že certifikační autorita je zřejmě díky tomuto přechodu v současnosti poněkud zanedbávaná, informace na webu nejsou vůbec aktualizovány, jsou zde uvedená neplatná telefonní čísla (před přečíslováním), pokud si zjistíte správná čísla po přečíslování, telefony jsou bohužel nefunkční, takže bude zřejmě nutné pokusit se případné informace zjistit u firmy GTS. Jinak ale certifikační autorita zřejmě normálně funguje a také CRL jsou pravidelně vydávány.

Provozovatel: GTS Czech (?)
Sídlo: původně KPNQwest Czechia s.r.o., Generála Janouška 902, 190 00 Praha 9, v současně době je již možná sídlo jiné
Adresa webových stránek: http://ca.kpnqwest.cz
Počet kontaktních míst (resp. registračních autorit): 1
Typy vydávaných certifikátů: osobní certifikáty pro fyzické i právnické osoby, serverové certifikáty
Délka klíče: není uvedeno, zřejmě 1024 bitů
Doba platnosti certifikátu: 12 měsíců
Možnost bezpečného hardwaru: není v nabídce
Způsob ověření totožnosti: žadateli je zaslána smlouva, kterou musí opatřit notářsky ověřeným podpisem a zaslat do sídla certifikační autority
Způsob podání žádosti o certifikát: on-line na webových stránkách
Způsob vydání certifikátu: stažení z webu, zaslání poštou na disketě
Způsob zneplatnění certifikátu: on-line na webových stránkách s pomocí hesla pro zneplatnění, písemná žádost opatřená notářsky ověřeným podpisem zaslaná poštou
Interval vydávání CRL: 24 hodin

CA Czechia

Jedná se o nejmladší certifikační autoritu na našem trhu. Webové stánky jsou částečně budovány jako jakýsi portál, takže kromě informací o vlastní certifikační autoritě zde můžete najít obecnější informace a články týkající se elektronického podpisu. V rámci vstupu na trh jsou do konce roku 2003 vydávány osobní certifikáty zdarma. Certifikační autorita je projektem firmy ZONER software, s.r.o.

Provozovatel: Certifikační autorita Czechia, s.r.o.
Sídlo: Koželužská 7, 602 00 BRNO
Adresa webových stránek: www.caczechia.cz
Počet kontaktních míst (resp. registračních autorit): 1
Typy vydávaných certifikátů: osobní certifikáty pro fyzické osoby, serverové certifikáty
Délka klíče: 1024 bitů
Doba platnosti certifikátu: 12 měsíců
Možnost bezpečného hardwaru: USB tokenu u varianty PROFI
Způsob ověření totožnosti: při podání žádosti si klient vytiskne smlouvu, kterou musí opatřit notářsky ověřeným podpisem a zaslat do sídla certifikační autority
Způsob podání žádosti o certifikát: on-line na webových stránkách
Způsob vydání certifikátu: instalace na webových stránkách
Způsob zneplatnění certifikátu: on-line na webových stránkách s pomocí hesla pro zneplatnění
Interval vydávání CRL: nejpozději do 24 hodin od zneplatnění certifikátu, jinak 1x týdně

TrustPort

Certifikační autorita TrustPort (dříve TrustCert) je provozována firmou AEC, spol. s r.o. Kromě vydávání certifikátu certifikační autorita TrustPort jako zatím jediná v České republice provozuje Autoritu časové značky (TSA, TimeStemp authority), čili vydává tzv.

časové značky. Časové značky umožňují ověřit, že určitá data existovala před uvedeným časovým okamžikem, což je požadavek, který elektronický podpis nijak neřeší.

Provozovatel: AEC, spol s r.o.
Sídlo: Bayerova 799/30, 602 00 Brno, Vinohradská 184, 130 52 Praha 3, Pribinova 25, 810 11 Bratislava
Adresa webových stránek: www.trustport.cz
Počet kontaktních míst (resp. registračních autorit): 3
Typy vydávaných certifikátů: osobní certifikáty pro fyzické osoby (dvě varianty lišící se délkou klíče a způsobem ověření totožnosti), serverové certifikáty, certifikáty pro podpis kódu
Délka klíče: 1024, nebo 2048 bitů podle typu certifikátu
Doba platnosti certifikátu: 12 měsíců
Možnost bezpečného hardwaru: není v nabídce
Způsob ověření totožnosti: osobní návštěva kontaktního místa a předložení 1, resp. 2 dokladu totožnosti (u varianty Class 3), zaslání žádosti poštou + dobrozdání třetí nezávislé strany (pouze u varianty Class 2)
Způsob podání žádosti o certifikát: on-line na webových stránkách
Způsob vydání certifikátu: zaslaní emailem
Způsob zneplatnění certifikátu: osobně, on-line na webových stránkách s pomocí hesla pro zneplatnění, telefonicky s udáním hesla
Interval vydávání CRL: podle potřeby, minimálně jednou za 24 hodin

Certifikační autorita Globe Internet

Tuto certifikační autoritu provozuje firma Globe Internet, s.r.o. víceméně jako doplněk svých služeb a jsou určeny zejména pro komunikaci společnosti s klienty. Po zaregistrování sice mohou certifikát získat i osoby, které nejsou klienty Globe Internet (a navíc zdarma), ale pouze s platností 2 měsíce a délkou klíče 512 bitů.

Provozovatel: Globe Internet, s.r.o.
Sídlo: Pláničkova 1, Praha 6
Adresa webových stránek: www.ca.cz, www.certifikacniautorita.cz
Počet kontaktních míst (resp. registračních autorit): 1
Typy vydávaných certifikátů: osobní certifikáty (v subjektu je uvedena pouze mailová adresa), zákaznické certifikáty, serverové certifikáty
Délka klíče: volitelně 384-1024 bitů
Doba platnosti certifikátu: 2-12 měsíců podle typu certifikátu
Možnost bezpečného hardwaru: není v nabídce
Způsob ověření totožnosti: u zákaznických certifikátů je identita žadatele považována za ověřenou po provedení alespoň jedné platby za služby společnosti, jinak je kontrolována pouze existence udané mailové adresy zasláním kontrolního kódu na tuto adresu
Způsob podání žádosti o certifikát: on-line na webových stránkách
Způsob vydání certifikátu: instalace na webových stránkách
Způsob zneplatnění certifikátu: on-line na webových stránkách
Interval vydávání CRL: není uvedeno

PostSignum

Certifikační autorita PostSignum je provozována Českou poštou, a je v tomto přehledu uvedena pouze pro úplnost, neboť je určena prakticky výhradně pro vydávání certifikátu „ve velkém“, a je tedy orientována hlavně na právnické osoby. Z tohoto důvody ani nejsou uvedeny žádné podrobnější informace o této certifikační autoritě

ČESKÝ TELECOM, a.s.

(informace o této autoritě doplnil do článku P.Vondruška)

Autorita společnosti, která buduje komunikační infrastrukturu veřejné správy. Součástí této infrastruktury je i zajištění služeb PKI. Součástí těchto služeb musí být důvěryhodná správa certifikátů pro autentizaci, šifrování a tzv. technických certifikátů. Zatím není rozhodnuto zda tyto služby bude Český Telecom, a.s. poskytovat sám nebo tuto službu zajistí jiným způsobem. Autorita, která je dále představena, je budována podle nejpřísnějších standardů a procesy zde nastavené podléhají přísným bezpečnostním dohledům. Není vyloučeno, že by tato autorita mohla sehrát významnou úlohu v projektu KI IVS.

Provozovatel: Poskytovatelem certifikačních služeb je akciová společnost ČESKÝ TELECOM, a.s
Sídlo: Olšanská 55/5, 130 34 Praha 3
Adresa webových stránek: http://www.intca.ct.cz resp. http://194.228.46.41/ .
Počet kontaktních míst (resp. registračních autorit): 2 pevné a 1 mobilní
Typy vydávaných certifikátů: osobní certifikáty pro zaručený elektronický podpis, osobní certifikáty určené pro šifrování, serverové certifikáty a specifické certifikáty pro zařízení
Délka klíče: 1024 bitů
Doba platnosti certifikátu: 12 měsíců, u specifických certifikátů podle typu určení
Počet vydaných certifikátů: více jak 1000
Možnost bezpečného hardwaru: čipové karty pro VIP uživatele (certifikát FIPS 140-1, Level 2)
Způsob ověření totožnosti: osobní návštěva kontaktního místa, předložení 2 platných dokladu totožnosti, ověření údajů v adresářových službách
Způsob podání žádosti o certifikát: pomocí klientského programu Entrust
Způsob vydání certifikátu: osobně předán aktivační kód a dále zabezpečenou komunikací mezi klientským SW Entrust a Interní certifikační autoritou
Způsob zneplatnění certifikátu: osobně, mailem podepsaným zneplatňovaným certifikátem, běžným mailem s heslem pro zneplatnění, telefonicky, nařízením oprávněné osoby
Interval vydávání CRL: 8 hodin

Takže tímto jsme uzavřeli přehled certifikačních autorit působících na našem trhu a měli byste již mít všechny potřebné informace, takže by pro vás neměl být problém zvolit si tu správnou společnost. A pokud vás nabídka českých certifikačních autorit nezaujme (a nepotřebujete komunikovat se státní správou), můžete využít služeb některé ze zahraničních certifikačních autorit, z technického hlediska nestojí nic v cestě, protože certifikáty jsou vystavovány podle mezinárodně uznávaných norem a i zahraniční certifikát by měl bez problému fungovat ve všech aplikacích. Jenom bude možná obtížnější ověřit si důvěryhodnost takovéto certifikační autority a u renomovaných společností se také připravte na poněkud vyšší ceny. A pokud ani tuto variantu nechcete využít, nezoufejte, digitální podpisy se budou používat ve stále větší míře a v důsledku toho se jistě na trhu objeví další certifikační autority, takže si snad vybere opravdu každý.

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

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

Tato studie je jedním z hlavních výstupů grantu "Úprava elektronického podpisu v právním řádu ČR", který byl udělen Grantovou agenturou Akademie věd České republiky; číslo tohoto grantu je B7068203.

1.ÚVOD

V poslední době dochází stále častěji ke změnám platné právní úpravy, a to zejména z důvodů společenské potřeby regulovat nové právní vztahy, které vznikají v souvislosti s dosud nevídaným rozvojem a stále častějším užíváním informačních a komunikačních technologií (dále jen ICT), zejména pak Internetu. Rozvoj tohoto, v mnoha ohledech bezesporu fenomenálního média, tak sebou přináší nejen stále narůstající počet jak aktivních tak i pasivních uživatelů, ale také řadu právních otázek týkajících se jeho právního režimu. Jedním z problémů, které se tohoto média bezesporu týkají, je právní regulace tzv. nevyžádaných a obtěžujících sdělení, či přesněji problematika spamu, resp. Spammingu. (Nevyžádaná (nebo obtěžující) elektronická sdělení se označují anglickým pojmem "spam", samotné jednání spočívající v jejich šíření pak "spamming". "Spam" tedy představuje širší pojem než jenom zprávy elektronické pošty, ale také Telefaxové zprávy, SMS, MMS, ICQ zprávy a další typy nevyžádaných elektronických sdělení. Vzhledem k značnému rozšíření tohoto termínu se bude této terminologie držet i tento článek.)

Smyslem tohoto článku je spíše stručně nastínit základní principy, možné způsoby řešení, jakož i některé návrhy de lege ferenda a upozornit na některá sporná místa stávající právní úpravy, než podat ucelený výklad, ve kterém bude pamatováno na všechny související otázky.

2. PRÁVNÍ ÚPRAVA POŠTOVNÍCH SLUŽEB SE ZŘETELEM KE KOMUNIKACI PROSTŘEDNICTVÍM DATOVÝCH ZPRÁV (ELEKTRONICKÉ POŠTY)

Jednou z klíčových otázek jakékoliv statě zabývající se právními aspekty doručování, resp. odesílání datových zpráv, a to zejména pomocí elektronické pošty, je otázka existence či neexistence její výslovné právní úpravy. Nejinak tomu bude i v tomto případě a je tedy nezbytné zvážit zda vůbec a do jaké míry lze na elektronické poštu vztáhnout zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (dále jen zákon o poštovních službách), který upravuje obecné podmínky pro poskytování a provozování poštovních služeb a související práva a povinnosti, které při poskytování a provozování poštovních služeb vznikají.

Ze samotné obecné definice poštovní služby vymezené v tomto zákoně (§1 odst. 2) vyplývá, že jde o činnost prováděnou na základě poštovní smlouvy a podle podmínek stanovených tímto zákonem za účelem dodání poštovní zásilky nebo poukázané peněžní částky, přičemž za poštovní zásilku tento zákon považuje mimo jiné také písemnosti (§2 písm. a). Vzhledem k poměrně volnému vymezení pojmu poštovní smlouvy (§4 a násl.) by bylo možné předpokládat, že se na elektronickou poštu tento zákon vztahuje. Jak ale vyplývá z některých dalších ustanovení, nebude tomu tak vždy.

Jak ostatně vyplývá z § 3 tohoto zákona, **písemné zprávy** (písemnosti, které obsahují sdělení určené konkrétní osobě[1]**), které jsou dodávány bezúplatně jsou z jinak výlučné působnosti tohoto zákona vyloučeny.** Z uvedeného vyplývá, že za písemné zprávy lze považovat zejména dopisy, pohlednice, korespondenční lístky aj. obsahující adresné písemné sdělení[2]. Služby spočívající v bezúplatném dodávání těchto písemných zpráv tak lze tedy uskutečňovat i jinak než jen prostřednictvím poštovních zásilek, tedy i jinak než za pomoci zvláštního režimu tohoto zákona.

Zákon však nikterak výslovně neuvádí, zda lze za písemnou zprávu považovat rovněž zprávu zasílanou elektronicky (datovou zprávu). Jak ale vyplývá z ustanovení § 3 odst. 2 tohoto zákona, „*...za dodání písemné zprávy se nepovažuje služba spočívající v přepravě sdělení v jiné než písemné podobě*“. Vzhledem ke skutečnosti, že zpráva zasílaná elektronicky (datová zpráva) je bezpochyby přepravována ve formě elektronické a nikoli písemné (koneckonců jde pouze o řetězce nul a jedniček) lze konstatovat, že se toto ustanovení týká zejména telekomunikačních služeb, při nichž je sdělení transferováno (dodáváno) ve formě elektrických, resp. elektronických impulsů. Aplikace tohoto ustanovení tak připadá v úvahu nejenom v případě zpráv zasílaných elektronicky, ale též u telegramů, u nichž je sdělení přemísťováno telefonem, dálnopisem nebo faxem. Skutečnost, že v tomto případě sdělení v určitou chvíli (bezprostředně před a po transferu) skutečně v písemné formě nemusí být v tomto případě relevantní[3]. V tomto ohledu lze tedy vyslovit domněnku, že zákon o poštovních službách sice na jedné straně považuje zprávu zasílanou elektronickou poštou za zprávu písemnou, avšak přepravu takové elektronické zprávy za její dodání již nepovažuje.

Z těchto důvodů lze učinit závěr, že výše zmíněné vyloučení, resp. omezení zákonné působnosti pro případy **„***bezúplatně dodávaných písemných zpráv***“** se na elektronickou poštu vztahuje, a to jak z toho důvodu, že ve většině případů půjde o zprávy zasílané bezúplatně, tak i z toho důvodu, že vzhledem k ustanovení § 3 odst. 2 zákona o poštovních službách, nelze přepravu takové zprávy považovat za její dodání, resp. dodávání ve smyslu zákona o poštovních službách.[4]

3. ELEKTRONICKÁ POŠTA A JEJÍ VÝZNAM

3.1 Obecný význam elektronické pošty

Navzdory obrovským možnostem Internetu je elektronická pošta stále jednou z nejčastěji využívaných internetových služeb, její obliba pak navíc stále stoupá. Důvodů lze nalézt hned několik. Prvním takovým důvodem je zde zejména rychlost přenosu zprávy (doručení), která se pohybuje v řádech milisekund a umožňuje tedy interaktivní výměnu několika zpráv během několika málo minut. Dalším takovým důvodem je pak nepochybně samotná cena těchto služeb (přenosu), která je v případě elektronicky zasílaných zpráv zásadně bezúplatná (viz. výše), Dalším je poté bezesporu stále větší dostupnost a rozšířenost těchto služeb. Stručně řečeno, elektronická pošta nabízí ve srovnání s (dosud tradičními) papírovými poštovními službami řadu výhod a návrat k papíru s tradičními poštovními známkám je dnes již nepředstavitelný.

Samotný obecný význam elektronické pošty tak spočívá zejména v jejích výhodách oproti tradičním formám. Z právního hlediska (významu) na ni však lze nahlížet také jako na významné komunikační médium (podobně jako např. tisk, rozhlas či televize) a marketingový nástroj; v tomto ohledu pak bývá také hojně zne/využívána (viz.dále).

---

1 Podle definice jsou tak písemnými zprávami zejména dopisy, pohlednice, korespondenční lístky aj. obsahující adresné písemné sdělení. Z definice tak jednoznačně vyplývá, že tento pojem nezahrnuje knihy, časopisy, deníky apod. neboť ty zjevně neobsahují sdělení určené jednotlivé konkrétní osobě.

2 Naopak pak z definice vyplývá, že tento pojem zjevně nezahrnuje knihy, časopisy, deníky apod. neboť ty neobsahují sdělení určené jednotlivé konkrétní osobě.

3 Viz. důvodová zpráva k zákonu o poštovních službách, komentář k § 3 odst. 2

4 O bezúplatnost ale zjevně nepůjde v případě SMS, resp. MMS zpráv, které jsou naopak ve většině případů dodávány za úplatu. Ani zde ale nepůjde o dodání, resp. těchto zpráv a tudíž vyloučení z působnosti tohoto zákona lze použít.

3.2 Elektronická pošta a její nevyžádané (reklamní) vsuvky

Jak již bylo výše uvedeno, elektronická pošta představuje významný marketingový nástroj. Za tímto účelem se používají jak celé zprávy elektronické pošty, jejichž jediným účelem je zejména reklama, tak i části běžných zpráv elektronické pošty (tzv. reklamní vsuvky), které slouží zejména pro komunikaci. Tyto reklamní vsuvky se vyskytují zejména u

- freemailových služeb, kde všechny zprávy zasílané elektronickou poštou procházejí centrálním serverem, který je zpracovává (přijímá a odesílá) a na jejich konec poté obvykle umisťuje krátkou reklamní vsuvku;
- tzv. newsletterů (tj. pravidelných zpravodajů zasílaných elektronickou poštou, které si uživatelé výslovně vyžádají);
- řady dalších zejména potvrzovacích elektronických služeb (např. potvrzení o přihlášení, o nákupu zboží, o přihození v internetové aukci atd.), které jsou generovány automaticky, tj. programem a ne člověkem.

Tyto reklamní vsuvky se pak mohou v samotných zprávách elektronické pošty vyskytovat v různé podobě, za nejčastější umístění těchto vsuvek lze považovat:

- na konci zprávy (nejčastěji tomu tak bývá u freemailových služeb, kde je tato vsuvka přidávána, jako určitá protiplnění za bezplatně poskytované služby);
- na začátku zprávy (velmi častý výskyt v newsletterech);
- uprostřed zprávy či na několika místech ve zprávě najednou (obvyklé pro newslettery).

Samotnou existenci tzv. reklamních vsuvek je vzhledem k povaze spamu velmi významná a v tomto ohledu si rovněž zasluhuje o poznání hlubší analýzu. Paušálně zjevně nelze považovat všechny reklamní vsuvky za důsledek jakéhosi zjevného protiprávního jednání, avšak v tomto ohledu lze minimálně tvrdit, že balancují na hraně legality. A to v některých případech i za předpokladu, že byl k tomuto jednání udělen souhlas.

Pokud by k souhlasu nedošlo, mohlo by jít také o trestný čin **porušování tajemství dopravovaných zpráv** ve smyslu ustanovení § 239 odst. 2 písm. c) trestního zákona, který spáchá „*pracovník provozovatele poštovních služeb nebo telekomunikační služby, který pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo jiným dopravním zařízením anebo zprávu podanou telefonicky, telegraficky nebo dopravovanou podobným způsobem*“.

V případě některých zavádějících vsuvek (např. reklamní vsuvka, která se zjevně snaží navodit dojem, že je součást zprávy pisatele (např. osobního dopisu) by mohlo dojít k nekalé soutěži (patrně by tímto jednáním došlo k naplnění generální klauzule) a to i v případě uděleného souhlasu ze strany uživatele.

V některých méně závažných případech by umístění reklamní vsuvky bez souhlasu odesilatele do samotné zprávy mohlo být také důvodem pro vydání bezdůvodného obohacení.

4. ÚPRAVA SPAMMINGU V PRÁVNÍM ŘÁDU ČR

4.1 Potřeba právní regulaci spammingu

Zatímco v tradiční poštovní schránce (té z kovu či plastu) se objevují nevyžádané tiskoviny (ať již reklamních či jiných sdělení) poměrně často, a to aniž by to vzbuzovalo nějaký zjevný nesouhlas, v případě spamu je situace zcela jiná. A to nepochybně právem. Je zde totiž nikoliv nevýznamný rozdíl v nákladech, a to jak za přijetí[5] takové písemnosti, tak i za její odeslání[6]. **Spamming, velmi často používaný k marketingovým cílům, tak v zásadě přenáší rozhodující část nákladů marketingové kampaně na někoho jiného**.

5 Zatímco odstranění tištěného reklamního letáku Vás stojí pouze zanedbatelné množství času, za odstranění nevyžádané elektronické pošty, platíte (podle způsobu připojení) za každou vteřinu připojení.

6 Zatímco například přípravu, vytištění a následné rozeslání jednoho milionu reklamních letáku lze pořídit řádově za několik milionů korun, milión zpráv o stejném obsahu rozeslaných elektronickou poštou pořídíte nanejvýš v řádech několika málo haléřů.

Problémem spammingu začala zabývat i Evropská společenství, která si, za účelem jeho lepšího pochopení a následného efektivnějšího boje proti spammingu, nechala vypracovat poměrně rozsáhlou studii tohoto problému. Studie má dvě části, přičemž první je věnována spíše věcným (technologickým) aspektům a rozebírá situaci zejména v USA, kde s celým problémem bojují zřejmě nejdéle. Druhá část studie se pak zabývá legislativou ES i jednotlivých členských zemí s ohledem na problém spammingu a jeho řešení[7]. Jedním z výsledků této studie je i celkový odhad škod, které spam přináší a to na až 10 miliard ECU celosvětově. Tímto pak autoři ilustrují skutečné rozměry tohoto problému.

Spamming lze tedy obecně vymezit jako efektivní zneužití fungujících distribučních mechanismů pro jiné účely, než pro jaké byly vyvinuty a jsou provozovány. Spamming představuje takovou hromadnou distribuci nevyžádaných zpráv (obsahujících texty, ale také např. nejrůznější přílohy), která je iniciována pouze jednostranně, sleduje výhradně jednostranné zájmy a je ostatním stranám podbízena, často i navzdory jejich zásadnímu nesouhlasu. Nadále však využívá kolektivního způsobu financování, tj. náklady na jednostranně výhodné aktivity nutí nést i ostatní strany, které tyto aktivity neiniciovaly a většinou s nimi ani nesouhlasí. V tomto se elektronický spamming zásadně odlišuje od rozesílání nevyžádaných zásilek běžnou listovní poštou (kde veškeré náklady nese pouze iniciátor takovéto kampaně).

Obsah těchto spamu je velmi různorodý; zásadně však jde o pornografii a místy též o poznání kuriosnější nabídky[8]. Pro vymezení spamu není ale jakkoliv významný samotný jeho obsah (může jít tedy o obsah ryze komerční, charitativní, náboženský nebo jiný) ale zejména prvek jeho nevyžádanosti.

Tyto skutečnosti, včetně stále se zvyšujícího počtu spamu, pak vedou jak ke společenské regulaci[9] tohoto jednání, tak i k regulaci právní.

4.2 Právní prokazatelnost spammingu

V zásadě nejjednodušší je zjistit, v čí prospěch je spam šířen. Určité úskalí pak lze ale spatřovat v prokázání skutečnosti, zda subjekt v jehož prospěch je spam šířen, ho rovněž šířil, event. zadal. Lze však předpokládat, že šiřitel takových sdělení (spammer) bude činit veškeré kroky vedoucí k tomu, aby jednoznačné určení své totožnosti znemožnil či alespoň významně znesnadnil. V případě reklamy šířené elektronickou poštou to však může být v řadě případů téměř nemožné. Prostředí Internetu, vzhledem k poměrně staré technologii, na které jsou některé jeho služby postaveny, lze totiž považovat za relativně anonymní a zásadně tedy umožňuje utajení identity. V tomto ohledu lze, v případě sofistikovaného šiřitele spamu, zajistit, aby jeden z komunikujících (např. příjemce) nemohl identifikovat svůj protějšek (třeba konkrétní www server nebo adresu původního šiřitele), či znemožnit jednoznačné určení, zda vůbec konkrétní adresát v určitém časovém období danou zprávu přijal (v takovém případě hovoříme o anonymit příjemce)[10]. S ohledem na právní prokazatelnost takového jednání lze uzavřít, že tato skutečnost výrazně znesnadňuje, či spíše v některých případech paralyzuje, téměř jakýkoliv efektivní zásah.

4.3 Zákon o regulaci reklamy[11]

7 Celý text studia lze nalézt na: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamstudy.pdf

8 Poměrně světoznámou je např. nevyžádaná elektronická nabídka zaslání jakéhosi návodu, jak si snadno, jen za pomocí určitých cviků, prodloužit penis o 20 centimetrů. Stačí prý jen poslat deset dolarů na jakýsi účet a zaručený návod přijde do pěti minut e-mailem. :-)

9 Ačkoliv výslovná právní úprava v tomto ohledu donedávna neexistovala, vyvinula se řada souvisejících pravidel, které byla dodržována zejména ze strany poskytovatelů obsahu a připojení. Více o tom na www.spam.cz nebo www.antispam.cz .

10 Více k problematice anonymního reklamního sdělení, viz. Beneš, T., Anonymní spojení v prostředí Internetu, DSM 2/2002, s.36-38

11 Zákon č. 40/1995 Sb. ČR, o regulaci reklamy; v platném znění

Dne 1. června 2002 nabývá účinnosti[12] zákon 138/2002 Sb., kterým mimo jiné mění a doplňuje zákon č. 40/1995 Sb. ČR, o regulaci reklamy, a tak zásadně vymezuje nová pravidla pro zadavatele, zpracovatele a šiřitele reklamy[13].

Jednou ze zjevných novinek, kterou tato právní úprava zavádí, je nová formulace, resp. znění § 2 zákona o regulaci reklamy, kde je v odst. 1 písm. e) uvedeno, že „***se zakazuje šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje***". Z hlediska legislativně technického jde nepochybně o vhodnou formulaci, pod kterou lze zahrnout jak reklamu prostřednictvím Internetu (nejenom tedy nevyžádané zprávy, ale také www bannery, apod.), ale také reklamu telefaxovou, reklamu umístěnou v software, reklamu příliš hlučnou apod. Vzhledem k zaměření tohoto článku se tedy budeme dále zabývat zejména právě postihem spamu.

Vyjma některých nesprávných tvrzeních v denním tisku[14] je třeba říci, že, že mezi podmínkou výdajů a obtěžování adresáta stojí spojka „nebo", jež činí obě podmínky zástupnými. Spam ale obvykle splňuje obě náležitosti (tedy nejenom obtěžování, ale také požadavek na výdaje). Nevyžádané zprávy elektronické pošty jsou nepochybně **obtěžující**, a vzhledem k tomu, že její doručení zásadně hradí adresát, vznikají mu tím tedy i **výdaje**, jakkoli mohou být zanedbatelné.

Zatímco ustanovení § 2 písm. e) lze nepochybně aplikovat na spam, nemusí se jej obávat šiřitelé reklamy prostřednictvím protokolu *HTTP* (tedy prostřednictvím www stránek). Přestože i reklamní bannery mohou být obtížné a za jejich doručení nepochybně zvyšuje náklady, je třeba připomenout, že § 2 odst. 1 písm e) se vztahuje toliko na vyžádanou reklamu, kdežto reklama prostřednictvím protokolu *HTTP* je doručována výhradně na vyžádání (request).

Zákon o regulaci reklamy tedy spam, pokud splňuje výše uvedené požadavky, výslovně zakazuje. Vzniká však otázka, jak a jakými prostředky se lze domáhat této ochrany v případě, že k porušení tohoto ustanovení dojde.

Dozor nad dodržováním tohoto zákona provádějí živnostenské úřady (§7 písm. d) a tak lze očekávat, že na základě konkrétního a dostatečně určitého podání, se bude tento orgán dozoru snažit zjistit totožnost skutečného šiřitele. Vzhledem k existujícím technologiím to nebude zdaleka jednoduchá záležitost (viz. výše).

Orgán dozoru však může využít příslušných zákonných pravomocí a zjistí alespoň skutečnou identitu alespoň jednoho z článku *zadavatel – zpracovatel – šiřitel* a v tomto ohledu pak rovněž zjistí skutečného šiřitele, případně uloží příslušné zákonné sankce (a to až do výše 2 000 000 Kč podle závažnosti porušení povinnosti, a to i opakovaně). Za zadavatele reklamy se zde (§1 odst 4) považuje zákona právnická nebo fyzická osoba, která objednala u jiné právnické nebo fyzické osoby reklamu. Za zpracovatele reklamy pak právnická nebo fyzická osoba, která pro sebe nebo pro jinou právnickou nebo fyzickou osobu zpracovala reklamu (§1 odst 5).Za šiřitele reklamy pro účely tohoto zákona považuje právnická nebo fyzická osoba, která reklamu veřejně šíří (§1 odst. 6). Z pohledu používané technologie však nemusí být vždy zřejmé, zda lze za šiřitele reklamy také považovat vlastníka poštovních serverů, přes něž je reklama k adresátovi šířena.

12 Tento zákon, byť nabývá účinnosti 1.6.2002, se patrně s ohledem na nevhodnost (nepravé) retroaktivity, po dobu dvou let se nevztahuje na reklamní kampaně realizované na základě smluv uzavřených před jeho účinností.

13 Více k této nové právní úpravě Hajn, P., K novele zákona o regulaci reklamy (obecná ustanovení), Právní zpravodaj, č.4/2002, s.6-7

14 V tisku se krátce po schválení zákona objevily informace, které hranici mezi legálností a nelegálností spamu staví až k datovému objemu 100 MB. Redaktor tehdy pravděpodobně vycházel z ceny přenosu těchto dat pro koncového zákazníka, aby vypočítal finanční újmu dostatečně vysokou k ospravedlnění nákladů na úřední zásah. Krom toho, pokud má e-mail doručený k jednomu adresátovi objem 20 KB (velikost doporučovaná pro newslettery), pak u tisíce adresátů jde o 19,5 MB, u deseti tisíc adresátů o 195 MB. Vzhledem k tomu, že spamy bývají rozesílány třeba až statisíci příjemců, překonání smyšlené hranice 100 MB není nijak náročné. Živnostenský úřad by si tedy měl vyžádat i úplný seznam příjemců reklamního sdělení (může mu jej poskytnout případně i ISP spamera), aby byl s to přesně odpočítat finanční postih, protože i u ostatních adresátů se dá považovat nevyžádaná reklama za obtěžující a náklady vznikají všem (dokonce i správcům tranzitních serverů a linek). Nikde v zákoně ovšem není hranice objemu dat stanovena.

Závěrem ještě nutno dodat, že za reklamu se dle §1 odst. 1 považuje oznámení, předvedení či jiná prezentace šířené zejména komunikačními médii[15], mající za cíl podporu podnikatelské činnosti, zejména podporu spotřeby nebo prodeje zboží, výstavby, pronájmu nebo prodeje nemovitostí, prodeje nebo využití práv nebo závazků, podporu poskytování služeb, propagaci ochranné známky. Zákon o regulaci reklamy se tedy vztahuje pouze na reklamu, kterou bychom mohli označit za komerční, nikoli však na jiné druhy reklamy, zejména pak reklamu politických stran. Tomu výkladu pak také nasvědčuje i ustanovení § 2 odst. 3 poslední věty, podle něhož reklama nesmí napadat politické přesvědčení; takové přímé či nepřímé napadání" pak patří k samé podstatě předvolební agitace uskutečňované mj. i pomocí reklamních prostředků a reklamních technik. Ze samotné definice reklamy však nepřímo vyplývá, že za reklamu se zde patrně také nepovažuje reklama výlučně nekomerční, tedy zejména podpora různých humanitárních projektů.(tedy např. reklama, která vystupuje proti xenofobii, domácímu násilí atd.). S ohledem na příkladný výčet vymezující reklamu však je však třeba říci, že bude až záležitostí soudní praxe a právní doktríny, aby při posuzování jednotlivých případů přesněji a jednoznačněji vymezila, na které případy reklamy se vztahuje § 1 odst. 1 vztahuje a které již nikoliv. Jak ostatně vyplývá z § 2 odst. 3 reklama rovněž nesmí být v rozporu s dobrými mravy, zejména nesmí obsahovat jakoukoliv diskriminaci z důvodů rasy, pohlaví nebo národnosti nebo napadat náboženské nebo národnostní cítění, ohrožovat obecně nepřijatelným způsobem mravnost, snižovat lidskou důstojnost, obsahovat prvky pornografie, násilí nebo prvky využívající motivu strachu. Reklama nesmí napadat politické přesvědčení. V tomto ohledu je třeba říci, že se samotné právní vymezení pojmu pornografie, je už letitým předmětem sporů a rozhodovací praxe a tak se, jak uvádí Hajn, P.[16], budou i naše soudy muset uchylovat k myšlence jednoho ze soudců Nejvyššího soudu USA, který měl prohlásit: „*Nevím, co je to pornografie, ale poznám ji, když ji spatřím*."

4.4 Zákon o ochraně osobních údajů[17]

Pojmovým znakem nevyžádanosti, je v zásadě jakési (zne)užití specifického druhu adres, která mohou identifikovat konkrétní osobu a lze je tedy v určitých případech považovat za osobní údaje. Pokud tedy subjekt údajů (v našem případě zřejmě tedy adresát spamu) zjistí, že došlo k porušení povinností správcem nebo zpracovatelem, má právo obrátit se na Úřad pro ochranu osobních údajů s žádostí o zajištění opatření k nápravě. V souladu s § 21 toto zákona má poté tento subjekt údajů právo požadovat zejména:

- aby se správce či zpracovatel zdržel takového jednání, odstranil takto vzniklý stav či poskytl na svoje náklady omluvu nebo jiné zadostiučinění,
- aby osobní údaje byly zablokovány nebo zlikvidovány,
- zaplacení peněžité náhrady, jestliže tím bylo porušeno jeho právo na lidskou důstojnost, osobní čest, dobrou pověst či právo na ochranu jména.

Této odpovědnosti se správce nebo zpracovatel zprostí, pokud prokáže, že porušení povinnosti nebylo možno zabránit ani při vynaložení veškerého úsilí, které lze od něj požadovat. Přesto však může subjekt údajů požadovat, aby se správce nebo zpracovatel zdržel závadného jednání, odstranil závadný stav, provedl opravu, doplnění, blokování nebo likvidaci osobních údajů. (§21 odst. 3 ZoOÚ)

(pokračování v Crypto-Worldu 9/2003)

15 Komunikačními médii, kterými je reklama šířena, se dle §1 odst. 2 zákona o regulaci reklamy rozumí prostředky umožňující přenášení reklamy, zejména periodický tisk a neperiodické publikace, rozhlasové a televizní vysílání, audiovizuální produkce, počítačové sítě, nosiče audiovizuálních děl, plakáty a letáky.

16 Hajn, P., K novele zákona o regulaci reklamy (obecná ustanovení), Právní zpravodaj, č.4/2002, s.6-7

17 zákon č. 101/2000 Sb., o ochraně osobních údajů; v platném znění (dále jen ZoOÚ)

E. TWIRL a délka klíčů algoritmu RSA (vývoj doporučení)

Jaroslav Pinkava, PVT a.s.

O principu a potenciálu zařízení TWIRL byli čtenáři Crypto-Worldu informováni v článku [1]. Nedávno se na webovských stránkách RSA Laboratories [2] objevila reakce společnosti RSA Security na tyto nové výsledky vztahující se k bezpečnosti algoritmu. Doporučení jsou shrnuta v následující tabulce:

Protection Lifetime of Data	Present – 2010	Present – 2030	Present – 2031 and Beyond
Minimum symmetric security level	80 bits	112 bits	128 bits
Minimum RSA key size	1024 bits	2048 bits	3072 bits

Table 1. Recommended minimum symmetric security levels and RSA key sizes based on protection lifetime.

V slovním komentáři závěru článku [2] Kaliski doporučuje provést přechod z bezpečnostní úrovně, která odpovídá 80 bitové délce klíče pro symetrický algoritmus (sloupec 1 tabulky) na bezpečnostní úroveň odpovídající 112 bitové délce klíče pro symetrický algoritmus (sloupec 2 tabulky) nejdéle do konce tohoto desetiletí.

V této souvislosti má také smysl se podívat na obdobná doporučení jinde. Např. pro Německo platí následující (dle BSI Empfehlung: "Geeignete Kryptoalgorithmen" Anf.§ 17 Absatz 1 SigG - v.22.Mai 2001 –
http://www.bsi.bund.de/esig/basics/techbas/krypto/bund02v7.pdf):
Do konce roku 2005 : 1024 bitů
Do konce roku 2006 : 2048 bitů doporučováno, 1024 bitů minimální hodnota
Do konce roku 2007 : 2048 bitů doporučováno, 1536 bitů minimální hodnota
(obdobná omezení jsou i na algoritmus DSA).

V evropských doporučeních
(http://www.ict.etsi.org/eessi/Documents/20011019_Algorithm_Proposal_V2.11.doc)
je uvedena platnost těchto doporučení (pro délku klíče algoritmu RSA - 1024 bitů) do konce roku 2005.

[1] Pinkava, J.: Faktorizace a zařízení TWIRL, Crypto-World 02/2003

[2] Kaliski, Burt: TWI|RL and RSA Key Size,
(http://www.rsasecurity.com/rsalabs/technotes/twirl.html)

[3] NIST. Special Publication 800-57: Recommendation for Key Management.
Part 1: General Guideline. Draft, January 2003.
(http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html.)

[4] Adi Shamir and Eran Tromer. *Factoring Large Numbers with the TWIRL Device.*
Draft, February 9, 2003. (http://www.wisdom.weizmann.ac.il/~tromer.)

F. Postranní kanály v Cryptobytes

Jaroslav Pinkava, PVT a.s.

Na adrese http://www.rsasecurity.com/rsalabs/cryptobytes/index.html můžete najít nové číslo nepravidelného občasníku Cryptobytes , který vydává RSA Laboratories (výzkumná laboratoř společnosti RSA Security). Toto číslo ([4]) obsahuje celkem tři články ([1],[2],[3]). Obsahu posledních dvou je věnován tento článeček.

Článek [2] je věnován postupům asymetrického šifrování (šifrování založené na identitě), kde veřejným klíčem může být libovolný řetězec, konkrétně i řetězec, který slouží jako identifikátor uživatele - majitel odpovídajícího soukromého klíče (například jeho e-mailová adresa).

V článku [3] autoři popisují dva nové výsledky rozšiřující podstatným způsobem současné postupy kryptoanalýzy postranních kanálů. První výsledek těží z úniku informací při elektromagnetickém vyzařování. Druhý výsledek umožňuje redukci nezbytného množství dat pro útoky z postranních kanálů. Rizika takovýchto úniků existují u všech kryptografických implementací, včetně takových, která byla imunní vůči dřívějším útokům z postranních kanálů - uvádí autoři.

Zejména komerční implementace kryptografických postupů jsou náchylné na takovéto útoky. Fyzické realizace algoritmů jsou přeci jen něco více než abstraktní matematický algoritmus. Dnes již existuje celá řada obdobných útoků, které jsou společně nazývány útoky z postranních kanálů. Takovým zlomovým bodem v tomto směru bylo opublikování několika článků P. Kochera a jeho spolupracovníků (http://www.cryptography.com). Prvními útoky tohoto typu byly spojené s měřením spotřeby proudu (power analysis) a s měřením času (timing analysis). Například protiopatření proti analýze spotřeby se již staly nezbytnou součástí při vývoji čipových karet, kde je možnost provádění takovýchto útoků snadno dostupná.

V článku popsané dva útoky ukazují rizika kryptografických implementací. Elektromagnetické vyzařování je zdrojem dalších informací, které jsou užitečné pro kryptoanalýzu. Přitom existují dvě kategorie EM vyzařování - přímé (vzniká při protékání proudu obvody - v širokém spektru, přitom často nejužitečnějšími - pro kryptoanalytika - bývají vyšší frekvence) a nepřímé (unintentional), které vzniká díky interakci různých elektronických komponent - což bývá problémem zejména u složitých miniaturizovaných zařízení typu CMOS. Právě však tento nepřímý typ vyzařování hodnotí autoři jako klíčový z hlediska využívání protivníkem. Jako příklad dané metody je uváděn útok na RSA-akcelerátor (komerčního typu, který je instalován na Intelovském serveru). Oproti útokům při nichž je využíváno měření času standardním způsobem zde dochází k význačnému posunu právě z hlediska možností měření času (akcelerátory přitom byly již konstruovány tak, aby splnily normy FIPS z hlediska ochrany proti vyzařování). Autoři dále ukazují i zranitelnost některých čipových karet (konstruovaných již tak aby byly odolné proti DPA - analýze spotřeby proudu). Druhý typ útoku (template attack) použili autoři úspěšně ve vztahu k implementaci symetrického kryptografického algoritmu RC4.

[1] Sarma, Sanjay E.; Weis, Stephen A.; Engels, Daniel W.: Radio-Frequency Identification: Security Risks and Challenges
[2] Gagné, Martin: Identity-based Encryption: a Survey
[3] Agrawal, Dakshi; Archambeault, Bruce; Chari, Suresh; Rao, Josyula R.; Rohatgi, Pankaj: Advances in Side-Channel Cryptanalysis, Electromagnetic Analysis and TemplateAttacks
[4] Cryptobytes Technical Newsletter, Spring 2003
http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_March_2003_lowres.pdf

G. Podařilo se dokázat, že P není rovno NP?
Jaroslav Pinkava, PVT a.s.

O známém matematickém problému stručně formulovaném jako otázka zda P je rovno NP byli již čtenáři Crypto-Worldu informováni v článku Pavla Vondrušky [3]. Obsahem problému je vztah dvou tříd úloh. Jsou to jednak úlohy, pro které existuje algoritmus řešící je v polynomiálním čase (třída P) a jednak úlohy, pro které existuje algoritmus, který v polynomiálním čase dokáže ověřit správnost již nalezeného řešení (třída NP). Exaktní formulace úlohy vyžaduje poněkud preciznější práci s použitými pojmy (Turingův automat atd.).

Úloha (kromě své matematické podstaty) je zajímavá i z dalších hledisek. Jednou ze základních NP-úplných úloh (úloh, které jsou v třídě NP jaksi nejtěžší, které se dají jedna na druhou převádět polynomiálním algoritmem, úloh pro které dnes není znám žádný polynomiální algoritmus) je úloha splnitelnosti booleovských výrazů resp. její varianta 3-splnitelnosti booleovských výrazů (3-SAT). Úloha splnitelnosti, resp. složitost řešení této úlohy má zásadní význam pro hodnocení bezpečnosti současných symetrických šifrovacích algoritmů. Úloha nalezení neznámého klíče (v známém algoritmu) při známém otevřeném textu (known plaintext attack) se dá totiž přeformulovat jako soustava booleovských (někdy se také říká logických) rovnic, pro kterou je třeba najít její řešení. Obvykle se totiž klade rovnítko mezi pojmy polynomiální a efektivní algoritmus.

Poznámka: Toto nemusí platit vždy. Například pro úlohu lineárního programování je nejčastější používaným algoritmem simplexová metoda, která však ve svých nejhorších (naštěstí málo pravděpodobných) situacích má exponenciální složitost. Oproti tomu Karmarkar nalezl polynomiální algoritmus pro řešení úlohy lineárního programování. Výpočetní praxe však ukázala jeho malou praktickou užitečnost (je náročnější než simplexová metoda).

Naopak, pokud by se skutečně podařilo dokázat, že P není rovno NP (a této skutečnosti věří dnes většina matematiků) byl by získán velice silný argument podporující tvrzení o bezpečnosti současných kryptografických algoritmů (kvantové počítače necháme mimo náš zorný úhel - takové, co by byly použitelné pro řešení kryptoanalytických problémů, jsou zatím stejně víceméně jen čistou teorií).

Druhým momentem, který staví úlohu zda P je rovno NP do popředí zájmu i široké matematické veřejnosti je skutečnost, že problém byl zařazen mezi tzv. Millenium Prize Problems [2]. Existuje sedm takovýchto problémů, za řešení každého z nich lze získat částku jednoho milionu dolarů.

Na jaře letošního roku se objevil článek pana C.A. Feinsteina (na adrese [1] lze nalézt jeho "opravenou" verzi). Autor, který není profesionální matematik (pracuje jako pojistný matematik - doufám - anglické slovo actuary má do češtiny několik různých překladových významů), tj. nepracuje jako teoretik v dané oblasti, v článku předvádí důkaz daného tvrzení.
Tj. dokazuje zde, že P není rovno NP. Svůj důkaz formuluje pomocí konstrukce, která ukazuje, že libovolný algoritmus pro řešení NP-úplné úlohy SUBSET-SUM musí pro určitý specifický vstup provést "superpolynomiální" množství výpočtů. Slovo superpolynomiální zde znamená, že danou charakteristiku nelze shora omezit žádným polynomem.

Rozsáhlou diskusi k článku lze nalézt na adrese (je třeba se prolistovat do vzdálenější historie) http://webnews.kornet.net/group.cgi?group=comp.theory&page=1.

Problémem je zde především skutečnost, že důkaz pana Feinsteina není dostatečně rigorózní (možná díky tomu, že Feinstein není profesionální matematik, možná zde je opravdu obsažena nějaká chyba) a zatím matematiky nepřesvědčil. Každopádně však vyvolal zajímavou diskusi k problému a vřele doporučuji se s ní seznámit. Mj. jedná se přeci o milión dolarů, ne?

Literatura:

[1] Feinstein, Craig Alan: P ≠ NP, http://xxx.lanl.gov/PS_cache/cs/pdf/0305/0305035.pdf

[2] Millenium Prize Problems, http://www.claymath.org/Millennium_Prize_Problems/

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

H. Letem šifrovým světem

Návštěva v Bletchley Parku

Chcete navštívit Bletchley Park, místo kde se za války luštila legendární Enigma? A chcete jej navštívit v podobě, jak vypadal za druhé světové války? Nepotřebujete k tomu stroj času, ale stačí Vám zasednout ke svému PC a zahájit virtuální procházku na adrese http://www.codesandciphers.org.uk/bletchleypark/

Sovětské šifry byly prolomeny

To, že za druhé světové války angličtí kryptologové luštili německé šifry, speciálně Enigmu, je všeobecně známo. Jak však byli úspěšní v luštění sovětských šifer v době studené války? Tyto z pochopitelných důvodů přísně tajené informace se v poslední době přece jen začínají objevovat. O rozlomení sovětských šifer Caviar, Poet system (sovětský šifrátor), Coleridge v letech 1945-1948, ale i o tak zvaném černém pátku (29.září 1948), kdy Varšavská smlouva změnila svůj šifrový systém a používané postupy se na Internetu začaly objevovat stručné informace
http://portal.telegraph.co.uk/news/main.jhtml?xml=/news/2003/06/02/ncode02.xml

Echelon

Na internetu byly během června zpřístupněny fotografie základen, které jsou zapojeny v monitorovacím systému Echelon, v rozsáhlém programu, který monitoruje prakticky veškerou elektronickou komunikaci na celém světě. Máte zájem si je prohlédnout? Pokud ano, pak jsem pro Vás připravil přehled adres, kde fotgrafie těchto stanic byly dostupné (alespoň 1.8.2003):
http://www.ozpeace.net/graphics/thegap2.jpg - Pine Gap, AU
http://www.heise.de/tp/english/inhalt/co/5993/5993_1.jpg , Geraldton, AU
http://kai.iks-jena.de/bilder/misawa.jpg , Misawa, JP
http://aib.de/station11.jpg , Bad Aibling, DE
http://www.hackhull.com/ontour/menwith/images/menwith-31b.jpg , Menwith Hill, UK
http://www.gcsb.govt.nz/images/dscub3.jpg , Waihopai, NZ
http://watserv1.uwaterloo.ca/~brobinso/leitrim.jpg , Leitrim, CA
http://www.iptvreports.mcmail.com/sugar_grove.jpg , Sugar Grove, US
http://www.zdnet.de/news/report/echelon/graphics/yakima.jpg , Yakima, US

Nové bezpečnostní standardy pro Evropu ?!

Na začátku června se sešli evropští experti k diskusi nad bezpečnostními standardy pro informační technologie. Součástí setkání byl celodenní seminář Network and Information Security (NIS) Focus Group Evropské unie na téma celoevropských bezpečnostních standardů. Předmětem diskuse byla téměř sedmdesátistránková zpráva, která obsahuje 30 doporučení ke zvýšení bezpečnosti. Cílem těchto aktivit není prosadit závazné normy, ale spíše dospět ke shodě a spolupráci mezi jednotlivými evropskými zeměmi. Finální verze zprávy by měla být publikována koncem léta.

Zveřejněno RFC k AES ! (RFC 3565)

Title: Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)
Author(s): J. Schaad
Status: Standards Track
Date: July 2003, Pages: 14
URL: ftp://ftp.rfc-editor.org/in-notes/rfc3565.txt

ZNALOSTI 2004

Předběžné oznámení konference

Srdečně Vás zveme k účasti na 3. ročníku interdisciplinární konference,věnované aktuálním problémům získávání, zpracovaní, zpřístupňování a využívaní znalostí. Program konference bude zahrnovat tutorialy, zvané přednášky, panelovou diskusi, vybrané příspěvky a industriální sekci (firemní prezentace sponzoru konference).

Termín konaní konference:	25.2. - 27. 2. 2004
Místo konání konference:	Hotel SANTON, Brno
Podrobné informace viz:	www.fi.muni.cz/znalosti2004/
Programový výbor (členové viz	www.fi.muni.cz/znalosti2004/)

Důležitá data:

20.10.2003	- termín podání abstraktu návrhu příspěvku
27.10.2003	- termín podání plných verzí návrhu příspěvku
1.12.2003	- vyrozumění o přijetí/odmítnutí návrhu příspěvku
2. 2.2004	- camera-ready forma

Kontaktní adresy

Organizační záležitosti:	staudek@fi.muni.cz
Program a zasílání příspěvků:	michal.kratky@vsb.cz

Organizují

Česká informatická společnost
Gerstnerova laboratoř, FEL CVUT Praha
Katedra informačního a znalostního inženýrství, VSE Praha
Katedra informatiky, VSB-TU Ostrava,
Katedra softwarového inženýrství, MFF UK, Praha
Fakulta informatiky, Masarykova universita, Brno

Organizační výbor (členové viz www.fi.muni.cz/znalosti2004/)
Jan Staudek, Fakulta informatiky, FI MU Brno, předseda

Přehled vybraných konferencí v srpnu 2003 (informační bezpečnost, kryptologie)

CRYPTO 2003

August 17-21
University of California, Santa Barbara
Conference Information and Registration Form is available at
http://www.iacr.org/conferences/crypto2003/
Full program information is available at
http://www.iacr.org/conferences/crypto2003/2003Program.html

WOMEN'S INFOSECURITY FORUM
(první konference o informační bezpečnosti, která je určena pouze ženám !)
Organizuje : Joyce Brocaglia, Alta Associates
Termín konání September 10-12
http://www.infidel.net/ewf

Def Con
August 1-3, Las Vegas, Nev.
http://www.defcon.org/

IT Audit Training Week
August 4-8, Boston, Ma.
http://www.misti.com/

12th USENIX Security Symposium
August 4-8, Washington, D.C.
http://www.usenix.org/

Ultimate Hacking
August 5-8, San Francisco, Calif.
August 5-8, Orlando, Fla.
August 12-15, New York, N.Y.
http://www.foundstone.com/

Windows Security
August 6-8, Washington, D.C.
http://www.foundstone.com/

Secure Coding
August 11-13, Washington, D.C.
http://www.foundstone.com/

Computer Forensics and Cyber Investigations Course
August 12-15, Atlanta, Ga.
http://www.trcglobal.com

Ultimate Hacking: Expert
August 12-15, Irvine, Calif.
August 19-22, New York, N.Y.
http://www.foundstone.com/

OSSTMM Professional Security Tester course
August 25-29, Orange County Calif.
http://www.dyadsecurity.com/services/education.htm

Hack Asia 2003 Singapore
August 26-27, Suntec City, Singapore
http://www.hackexpo.com/singapore/

O čem jsme psali v létě 2000 - 2002

Crypto-World 78/2000

Příloha :
10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha :
priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

I. Závěrečné informace

1. Sešit

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

Články neprocházejí jazykovou kontrolou!

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

http://crypto-world.info

2. Registrace / zrušení registrace

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

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

3. Spojení

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