Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 6/2001 16.červen 2001

6/2001

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

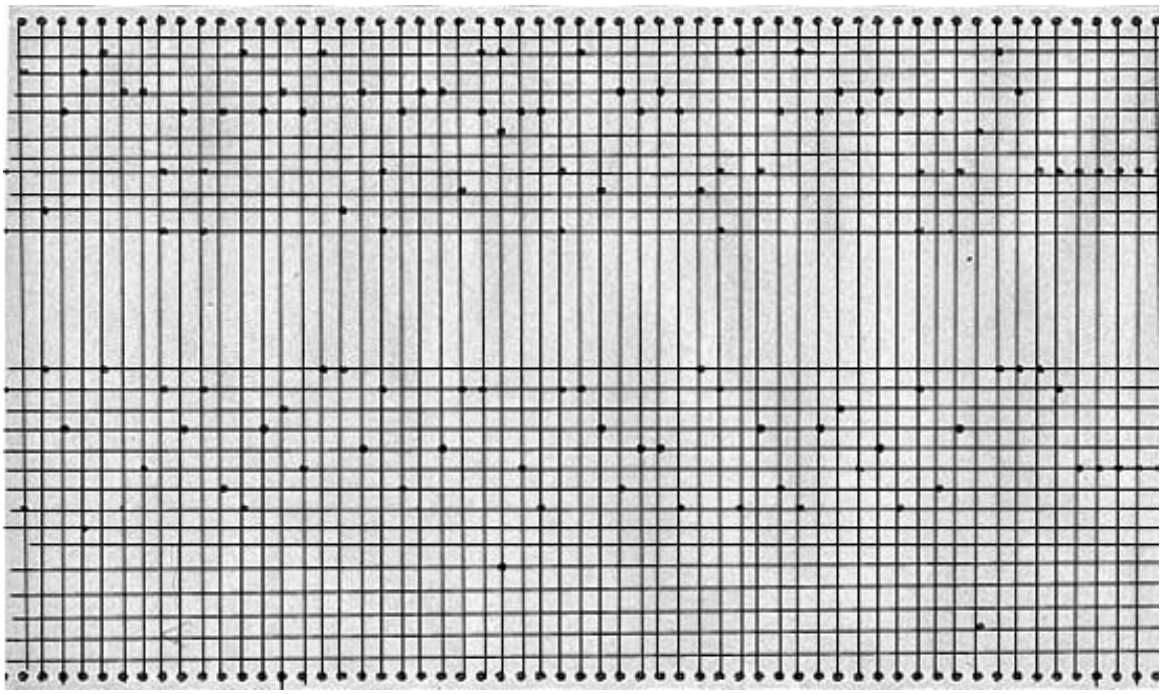
OBSAH : **Str.**

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)
ÚOOÚ hledá zaměstnance se zájmem o informační bezpečnost – více viz.
Letem šifrovým světem !

A. Záhadná páska z Prahy (II.díl)

Mgr. Pavel Vondruška, Mgr. Jan Janečko

V minulém čísle jsme skončili své vyprávění v okamžiku, kdy jsme provedli přepis dostatečného množství znaků z pásky do námi zvoleného kódu. Celý postup přepisu si popíšeme na konkrétním příkladě. Na oskenovaný úsek jsme nejprve umístili mřížku. V horním úseku se vyskytuje vždy jedna nebo dvě dírky, v dolním úseku vždy pouze jedna dírka. V "prostřední" lince se někdy (spíše výjimečně) vyskytuje velká dírka. Každý znak pásky lze tak popsat pomocí trojice čísel. Prvé dvě číslice udávají pozice dírky (dírek) v horní části, třetí číslice řádek, ve kterém se vyskytuje dírka v dolní části. Výskyt velké dírky jsme zapsali vložením písmena A. Podívejme se, jak vypadá přepis kódů podle výše uvedených pravidel např. u tohoto krátkého úseku z konce pásky.



							!		!									!									!	
3	10	5	3	2	4	4	8	5	8	5	2	5	4	5	2	10	4	8	5	4	4	9	2	2	5	5	8	2
0	0	0	0	0	0	0	11	0	11	0	0	0	0	0	0	0	0	11	0	0	0	0	5	6	0	0	11	0
8	1	4	9	1	8	6	2	4	2	7	8	4	3	6	1	1	5	2	7	8	5	2	2	11	6	8	2	2

						!										!											
9	4	5	4	5	9	8	2	8	5	2	5	4	5	4	5	8	5	8	6	2	4	8	8	8	8	8	8
0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0	0
4	7	5	5	8	1	2	8	4	7	8	4	3	6	5	8	2	7	4	14	1	1	1	2	6	6	6	6

Každý sloupek tabulky je přepis jednoho sloupku z pásky. Dále jsme předpokládali, že každý takovýto sloupek je jeden znak hledaného textu. Při přepisu si lze dále všimnout, že jeden ze znaků (8,11,2) se často opakuje. Vyskytuje se ve vzdálenostech, které by mohly odpovídat jednotlivým slovům a mohl by tedy odpovídat mezeře v hledaném (tzv. otevřeném) textu. Tento znak je pro lepší vyhledání v pásce a tabulce označen pomocí ! . Analýzou přepsaného textu jsme zjistili, že se jedná o jednoduchou záměnu. Vyluštění takovéto šifry pak již bylo otázkou rutinního postupu . Způsob luštění je dostatečně známý a nebudeme se

jím zde zabývat. Čtenáře, který by měl zájem o nějaké základní informace, odkazuji na loňský Crypto-World 10/2000, kde byl tento postup dostatečně popsán v souvislosti s vypsanou soutěží v luštění základních šifrových systémů. V tomto konkrétním případě byla použita čeština, zvláštní kódy jsou použity pro malá i velká písmena, interpunkci a dále se zde vyskytuje řada znaků, které jsme pracovně nazvali "zalamovací". Zalamovací znaky se vyskytují přibližně po 60 znacích a bylo jasné, že mají souvislost s ukončením jednotlivých řádek. Zjednodušeně jsme je pracovně nazvali "line feed(y)" a "form feed(y)" - analogie se znaky dálnopisu. Zde při zápisu pásky je však použito takovýchto znaků mnohem více druhů. Připojuji získanou převodovou tabulku a přepis výše uvedeného úseku pásky.

h	l	a	d	i	n	y	_	a	_	z	b	a	r	v	i	l	o	_	z	n	o	-			v	u	_	t
3	10	5	3	2	4	4	8	5	8	5	2	5	4	5	2	10	4	8	5	4	4	9	2	2	5	5	8	2
0	0	0	0	0	0	0	11	0	11	0	0	0	0	0	0	0	0	11	0	0	0	0	5	6	0	0	11	0
8	1	4	9	1	8	6	2	4	2	7	8	4	3	6	1	1	5	2	7	8	5	2	2	11	6	8	2	2

ě	ž	k	o	u		_	b	e	z	b	a	r	v	o	u	_	z	e	m	i								
9	4	5	4	5	9	8	2	8	5	2	5	4	5	4	5	8	5	8	6	2	4	8	8	8	8	8	8	8
0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0	0	0
4	7	5	5	8	1	2	8	4	7	8	4	3	6	5	8	2	7	4	14	1	1	1	2	6	6	6	6	6

malá písmena				velká písmena				speciální znaky			
a	5	0	4	**A**	3	0	13	**mezera**	8	11	2
á	6	0	4	**Á**				**čárka**	9	0	1
b	2	0	8	**B**	8	0	11	**rozdělení**	9	0	2
c	12	0	4	**C**				**tečka**	4	0	1
č	13	0	4	**Č**					4	0	4
d	3	0	9	**D**	8	0	14				
ď	3	0	10	**Ď**				**zalamavací**	2	5	1
e	8	0	4	**E**	7	0	12	**znaky**	2	5	2
ě	9	0	4	**Ě**					2	5	3
é	10	0	4	**É**					2	5	4
h	3	0	8	**H**					2	5	5
i	2	0	1	**I**					2	5	6
í	3	0	1	**Í**							
j	3	0	2	**J**	2	0	9		2	6	0
k	5	0	5	**K**					2	6	1
l	10	0	1	**L**					2	6	3
m	6	0	14	**M**	3	A	0		2	6	6
n	4	0	8	**N**	5	0	14		2	6	7
o	4	0	5	**O**					2	6	8
p	4	0	9	**P**					2	6	10
q				**Q**					2	6	11
r	4	0	3	**R**							
ř	5	0	3	**Ř**					5	0	1
s	3	0	3	**S**					5	0	2
š	4	0	2	**Š**	4	0	10				
t	2	0	2	**T**					8	0	0
u	5	0	8	**U**	10	0	14		8	0	2
v	5	0	6	**V**					8	0	6
y	4	0	6	**W**	4	A	0				
ý	3	0	6	**Y**							
z	5	0	7	**Z**							
ž	4	0	7	**Ž**							

Jako další přílohu uvádím přepis začátku pásky se všemi použitými znaky. Uvedeny jsou i chyby, kterých se autor dopustil (např. kdybste místo kdybyste). Na této ukázce jsou dobře patrné "zalamovací znaky" a jejich pravidelné rozložení.

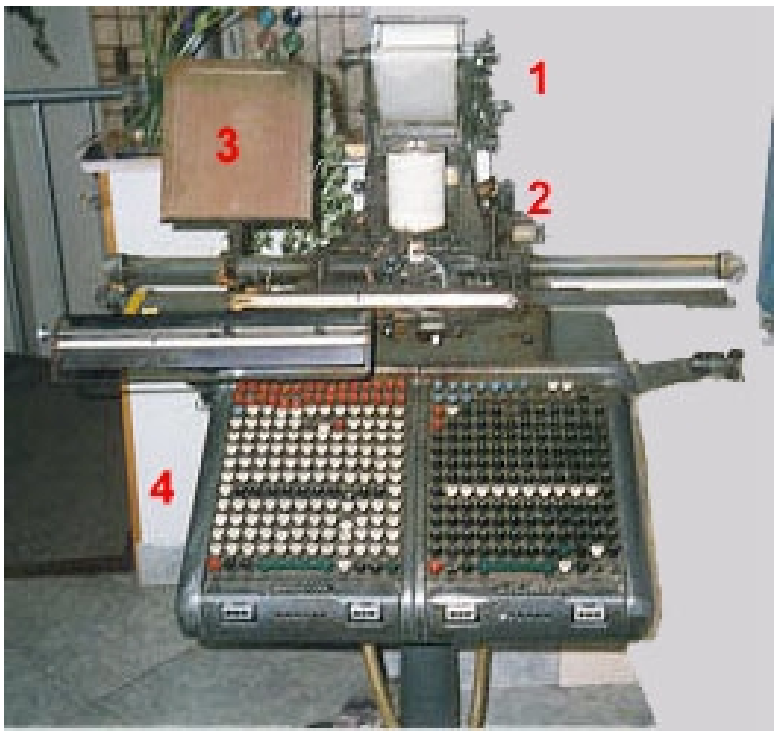
PÁSKA - přepis

(1,6,8)(8,0,6)(8,0,6)
„Udělali byste nejlíp, kdybste si teď šli po svých (4,0,4)
(5,0,1)(5,0,1)po (9,0,2)(8,0,0)(2,5,4)(2,6,6)
ručila jim s rukama založenýma v bok. „Měla bys teď právě být u mlíka, Marie
(10,0,11)hyllis(8,0,2)(7,0,11)(8,0,2)
víš to zrovna tak dobře jako(2,5,4)(2,6,1)
já. Myslím, že bych se sama styděla, pomáhat cizím lidem(2,5,2)(2,6,0)
při jejich týdenní čistce, pane Addisone a paní Addisono-(2,5,3)(2,6,14)
vá(4,0,4) A vy zrovna tak, (7,0,12)llimane Willkinsone, a možná ještě(2,5,4)(2,6,3)
trochu víc, když na to přijde(4,0,4) Nepatříte ještě do naší ro-(2,5,4)(2,6,0)
diny, ještě hezky dlouho ne, chlapečku (0,0,3) to ne, a ani to na(2,5,4)(2,6,2)
to nevypadá, jestli se nepolepšíte(4,0,4)(5,0,1)(5,0,1)
(8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6)
(8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6) (8,0,6)(8,0,6)
(2,5,3)(2,6,8)(8,0,6)(8,0,6)Eliška stále ještěěěěěěěěěěě(2,6,8)
(8,0,6)(8,0,6)
Eliška však stále ještě prodlévala, nespokojená, že ne-(2,5,6)(2,6,0)
řekla ještě všechno, co by byla chtěla, ale Jalka ji rázně od-(2,5,2)(2,6,11)
vedla ke dveřím. Bránila se, jak jen mohla, a ruka, které(2,5,5)(2,6,6)
bylo odepřeno provésti rozsudek nad Járou, se vymrštila(2,5,5)(2,6,10)
a uhodila Jalčinu tvář. Děvče na ni vzdorovitě pohlédlo.(2,5,5)(2,6,8)(8,0,6)(8,0,6)
„Nemůžeš nechat lidi na pokoji(2,0,7)(5,0,1)(5,0,1)
vyčítala jí trpce,tys to odjakživa nedovedla. Pamatuji říkal, že tě(2,5,2)(2,6,11)
kvůli tomu přímo nenáviděl, když jsme ještě děti. Pro-(2.5,2)(2,6,6)
to měl vždycky mnohem radši tetu Járu než tebe.(5,0,1)(5,0,1)(8,14,1)(8,0,6)(8,0,6)
„(12,0,4)ak ty už najde někoho jiného, kdo tě asi nenechá na pokoji,
.....

Další ukázka je ze samého konce pásky. Nyní již uvádíme přepis bez zalamovacích znaků :

… kdo zapomněl na správný čas. Šimonovi náhle připadlo, že už neviděl slunce vycházet nebo zapadat nejméně týden. Včera byl jen náhlý západ, pohlcený náraz náhle přikvapivši temnotou a dnes, projasnila-li se přechodně obloha vůbec, muselo to být ještě, když byli na farmě. Noc se stahovala neprávem nad šedozelenou zemí, které se vůbec nedostalo zaslouženého podílu slunce, právě tak jako se nespravedlivě stahovala noc nad lidskými životy, které minul jejich podíl kouzla a jasu. Šimon toužil po tom, aby zahlédl na západě světlo, které …

Jako základní představa o obsahu pásky to jistě stačí. Z uvedeného textu jsme usoudili, že na pásce není uložen nějaký "tajný" text nebo vzkaz, který by autor chtěl utajit, ale je zde pravděpodobně text nějaké knihy, nejspíše brakového žánru, něco jako "červená knihovna". Páska neobsahuje celou knihu, ale jen její část.



Dále jsme chtěli zjistit, na jakém zařízení byl text vlastně psán a co se dalo s takto zaznamenaným textem dále dělat. To, že je na pásce pravděpodobně uložena kniha, nás přivedlo k hledání informací o sázecích strojích. Jeden z našich známých obvolal tiskárny a sháněl se po informacích o starých sázecích strojích. Měl štěstí, v Grégrově knihtiskárně ihned podle popisu věděli, že takovéto pásky se používaly do zařízení MONOTYPE (s pořizovacím klávesovým zařízením TASTER), a dokonce jedno z těchto vyřazených zařízení mají prý stále ještě vystaveno ve vrátnici !

Samozřejmě, že jsme se na toto zařízení zašli podívat. A bylo to opravdu to, co jsme hledali. Zařízení , které je zde vystaveno, je stále ještě ve velice dobrém stavu. V zařízení je dokonce vložena páska. Stejný typ pásky jako je ta "naše" ! -

Typograf si odložil opisovaný text na "podávací desku" (na fotografii označeno číslem 3) a na uvedeném stroji připravoval text. Klávesnice zařízení je dělena na dvě části. Levá část obsahuje běžné znaky abecedy (malé i velké), pravá klávesnice pak speciální symboly (na obrázku označeno číslem 4). Klávesnice jsou výměnné. Zařízení umožňuje podle textu na pásce (umístění pásky označeno číslem 1) odlít jednotlivá písmena (lze i dodatečně např. na zařízení univerzálního licího stroje Supra Monotype – viz. fotografie č.2). Lití se zahájí vždy po ukončení řádku. Také se vysvětlil velký počet "zalamovacích znaků". Zařízení MONOTYPE obsahuje totiž pomocné počítadlo (mechanický otočný váleček na obrázku je označen číslem 2), který měří, kolik zbývá místa do konce řádky. Po naplnění řádku lze na válečku odečíst, jaká musí být velikost mezer (stejná velikost pro všechny mezery v řádku) tak, aby byly všechny řádky přesně stejně dlouhé. Typograf pak na konec řádku tento znak doplnil.

Jsme vlastně již u konce celé záhady.

Páska, k jejímuž luštění jsme byli vyzváni, ztratila svoji tajuplnost.
Zjistili jsme, co přibližně obsahuje a na jakém zařízení byla vytvořena.
Kdo ale text napsal a následně schoval a důvody proč tak učinil se nám zjistit nepodařilo.
Nepodařilo se nám zjistit, z jaké knihy je text uložený na pásce a kdo je autorem. Je také možné, že tento text nebyl nikdy „odlit“ a vytištěn, a to by také mohlo být důvodem, proč si neznámý autor pásku uschoval (s tím že ji třeba jednou ještě použije a knihu vytiskne ...).

Pozn. Fotografie č. 1 : literový sázecí stroj Monotype,
Fotografie č.2 : univerzální licí stroj Supra Monotype.

Příloha č.1 : Místo nálezu

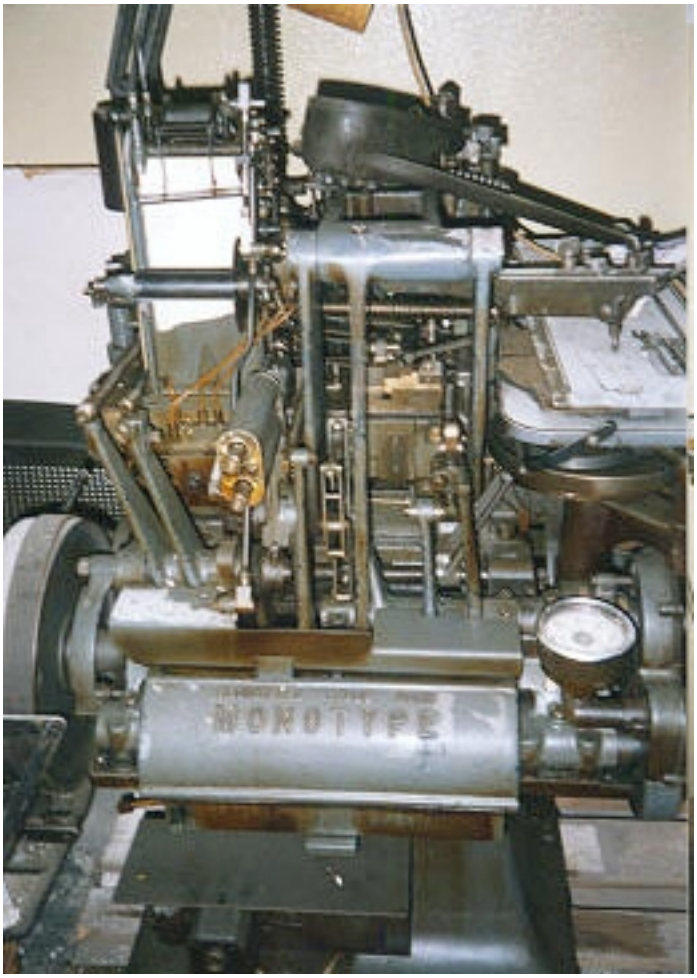
Obsahuje informace o budově, ve které byla páska uschována. Do výklenku byla zazděna pravděpodobně při některé z větších přestaveb.

Staré Město čp. 583/I (bývalý Dětský dům)
Funkcionalistický obchodní a kancelářský dům pojišťovny Praha navržený Ludvíkem Kyselou a postavený 1927 - 1929.
Rozdělen na dvě stavby se samostatnými konstrukcemi, celková dispozice tvaru L.
Stavebníkem byly majitelé parcely Pojišťovna Praha a Penzijní ústav čs. peněžnictví.
Úpravy:
a.. 1930, 1935 nové výkladce
b.. 1950 - 1952 adaptace na Dětský dům (Fr. Cubr)
c.. 1975, 1984 - 1985, 1990 - 1991 přestavba zadní fasády a střechy zadní části. Projektový podnik Praha.

Příloha č.2 : Zařízení Monotype

kniha : Typografie, Praha 1996, str. 32

Literové sázecí stroje



Zanedlouho po instalaci prvních řádkových sázecích strojů, především v novinových tiskárnách, se objevují i první sázecí a licí stroje Monotype v dílových tiskárnách. V roce 1908 byly instalovány dvě klávesnice C a jedna lička veWiesnerově tiskárně v Praze a brzy nato v Rohrerově tiskárně v Brně. Následovala Stiepelova tiskárna v Liberci a další čtyři instalace v Praze.Během první světové války byly dodávky dalších strojů přerušeny, avšak k rozmachu literové sazby dochází hned v prvních letech samostatné Československé republiky.Tiskárny zařazovaly sázecí stroje Monotype vedle řádkových sázecích strojů pro sazbu časopisů, publikací i drobných tiskovin. V praxi se prokázala možnost zhotovovat na literových strojích prakticky všechny druhy sazby, až po nejkomplikovanější a nejsložitější. Novinářské tiskárny Národní politika, Novina, Melantrich, Orbis, Právo lidu, Venkov i tiskárny časopisů a knih Průmyslová tiskárna, Legiografie, Prometheus, Kompas, **Grégrova** a Beaufortova v Praze úspěšně využívaly jak literových sázecích strojů, tak i univerzálního licího stroje Supra Monotype.

B. Radioaktivní rozpad a kryptografické klíče

Dr. rer. nat. Luděk Smolík
seculab s.r.o.
Hradec Králové, CZ
lsmolik@web.de

Abstrakt

Představujeme zde metodu pro generování statisticky ryze náhodných bitů s vysokou proudovou frekvencí pro kryprografické účely. Tato metoda využívá radioaktivní rozpad jako zdroj nepředvídatelných událostí. Měřená veličina je časový interval mezi dvěma následujícími signály malé ionizační komory, která registruje průchod ionizačních částic radioaktivního rozpadu. Tento časový interval se konvertuje do dvou logických stavů reprezentujících „0“ a „1“.

V některém z následujících příspěvků popíšeme měření statistické kvality generovaných bitových proudů, která byla úspěšně kontrolována testy podle FIPS PUB 140-1 a DIEHARD. Pro simulaci systematických chyb byla použita metoda Monte-Carlo.

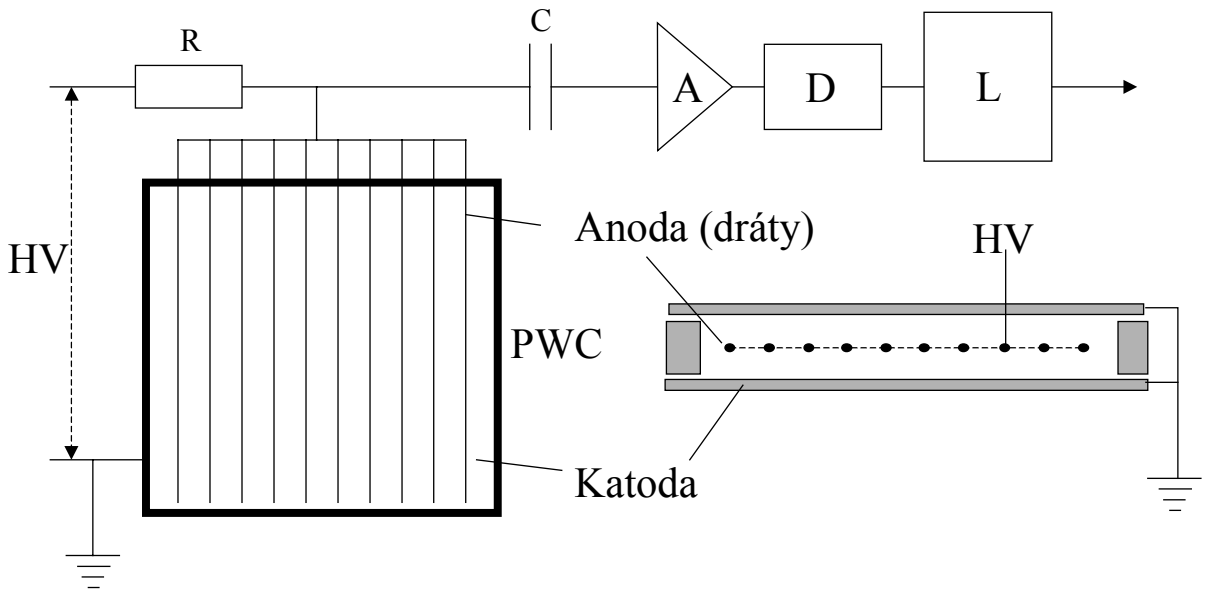
Úvod

Potřeba kvalitních, statisticky náhodných událostí v dnešní moderní komunikaci roste. Byl to snad právě veřejně dostupný, kryptografický software Pretty Good Privacy (PGP), který rozpoutal diskusi na téma jak generovat kryptografické klíče. Program PGP využívá jako náhodnou veličinu časový odstup mezi dvěmi klávesovými údery a zároveň hodnotu zvolené klávesy. V aplikacích požadujících vysoký stupeň bezpečnosti je zřejmě takový postup nedostačující. Národní zákony a vyhlášky o elektronickém podpisu požadují výrobu a distribuci zaručeně náhodných kryptografických klíčů od důvěryhodných třetích stran, tzv. certifikačních autorit. Dobře známými zdroji náhody jsou kupříkladu radioaktivní rozpad atomového jádra a volných elementárních částic, termický šum elektronů v atomové mřížce a jiné efekty kvantové mechaniky. V našem příspěvku popisujeme využití radioaktivního rozpadu. Tento kvantový efekt není prakticky závislý na vnějších makroskopických vlivech (jako jsou např. teplo, tlak, elektrický potenciál, chemické vlastnosti) a má proto daleko menší náchylnost k manipulaci ve srovnání kupříkladu s měřením elektrického šumu diody jako zdroje náhody. Elektrický šum diody je značně závislý právě na teplotě diody. U zařízení, které využívá elektrického šumu jako zdroje náhody, může proto vnější útok způsobit efekty korelace následných bitů. Pro další použití dat je potom potřeba další kryptografická úprava. V tomto případě se prakticky již nedá mluvit o pravém generátoru náhodných čísel, který je postaven pouze na fyzikální a nepředpověditelné náhodě. U zařízení používajících radioaktivní rozpad je vnější manipulace daleko obtížnější.

Experimentální sestava

Generátor se skládá z malé ionizační komory, zesilovače a diskriminátoru pro elektrické signály a z logického a komunikačního modulu pro zpracování dat. Schéma zařízení je znázorněno na obrázku 1. Ionizační komoru tvoří dvě elektrody velikosti ca. 100x100 milimetrů a rám tloušťky ca. 10 mm. Rám slouží zároveň jako mechanická podpora

pro napnuté tenké dráty, které probíhají v rovině paralelně mezi elektrodami. Elektrody jsou uzemněny, dráty jsou zapojeny na pozitivní potenciál velikosti několika set voltů. V prostoru mezi elektrodami a dráty se vytvoří silně nehomogenní elektrické pole, v kterém se volné elektrony ionizačního procesu urychlují. Ve vysokém elektrickém poli v bezprostřední blízkosti drátu získají primární elektrony tolik kinetické energie, že jsou schopny samy ionizovat okolní atomy plynu. Tento proces zmnohonásobení primárních elektronů (tak zvaná elektronová lavina) umožňuje detekci makroskopických elektrických signálů.



Obr. 1 :
Schéma generátoru, ionizační komora (proportional wire chamber PWC), high voltage HV, elektrický odpor R, kondenzátor C, zesilovač A, diskriminátor D, logický modul L

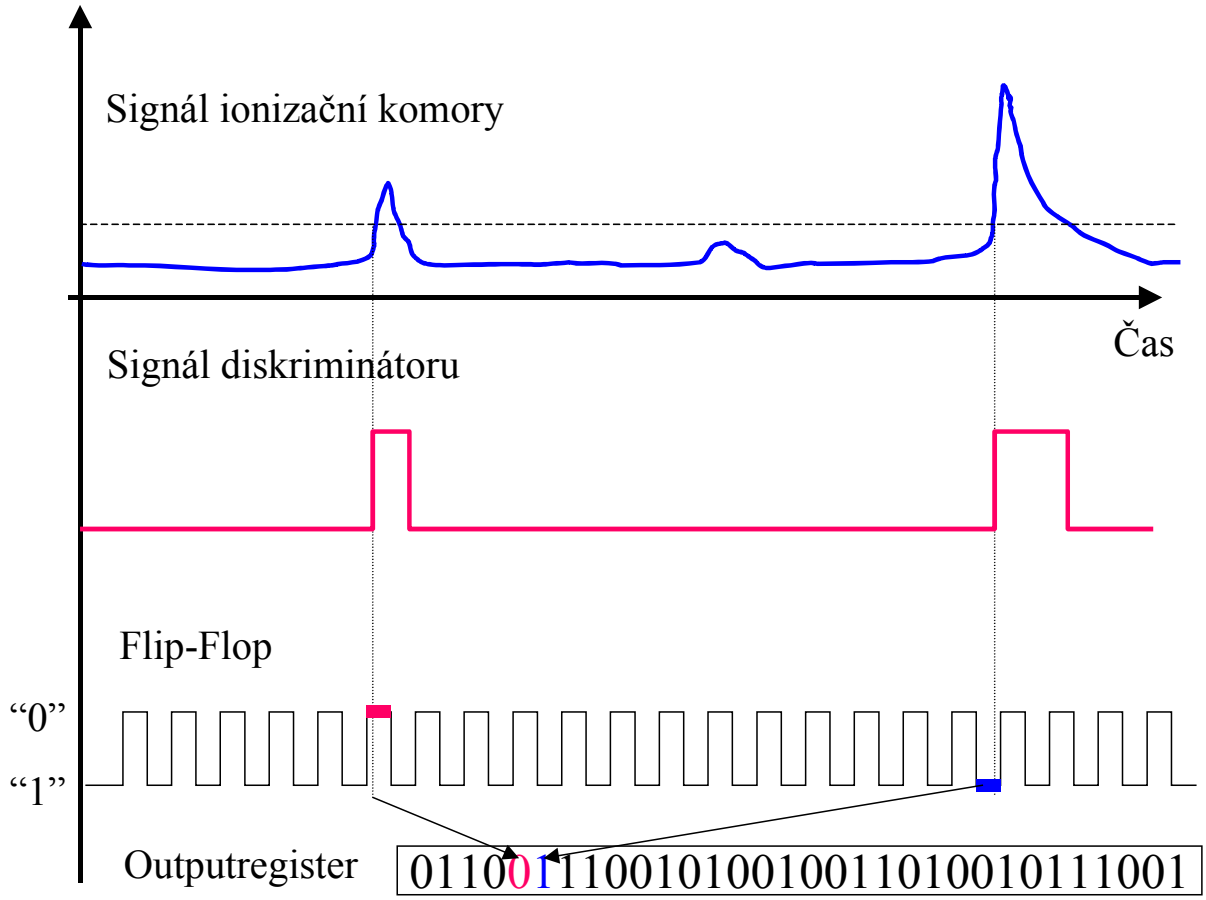
V generátoru je jako zdroj ionizace použito Thorium-232. Thorium je obsaženo ve speciální tkanině, kterou používáme při výrobě elektrodových desek. Tento materiál je volně dostupný a nepodléhá zákonným předpisům o ochraně proti záření. Thorium-232 vyzařuje částice α s energií 4.083 MeV. Každou částici α následuje několik vysokoenergetických fotonů, které emituje dceřiné jádro při přechodu do základního stavu. Ionizační α částice (respektive energetické fotony) vstupují do sensitivního prostoru komory přímo z obou elektrod. Problematika externího radioaktivního zdroje je tímto postupem eliminována. Při interakci produktů radioaktivního rozpadu s plynovým médiem detektoru a po lavinovém zesílení vznikne na kondenzátoru C malý elektrický signál, který je zesílen v zesilovači a následně diskriminován.

Nepředvídatelnost radioaktivního rozpadu se manifestuje v neurčitosti časového intervalu mezi dvěma registrovanými rozpady. Spektrum časových intervalů sice popisuje Poissonovo rozložení, ale deterministická předpověď následujícího radioaktivního rozpadu není možná.

Způsob měření je schématicky zobrazen na obrázku 2. Signály, které překračují určitou minimální amplitudu, jsou registrovány a vyvolají normovaný signál na výstupu diskriminátoru. Počátek tohoto signálu stanovuje logický stav „flip-flopu“, který osciluje s

pevnou frekvencí mezi „0“ a „1“. Výsledky měření jsou akumulovány v blocích délky 1 kb v logickém modulu, který provádí statistické testy a obsluhuje zároveň standardní rozhraní. Zařízení popsané velikosti dosahuje aktivitu 100 kBq (1 kBq na cm^2 detektorové plochy), což odpovídá řádově100 kilobitům za vteřinu.

V některém z příštích příspěvků vás seznámíme s praktickým použitím generátoru pro potřeby certifikačních autorit, o jeho evaluaci a certifikaci.



Obr. 2 :

Konverze časového intervalu signálů ionizační komory na logický stav „0“ nebo „1“.

Literatura

FIPS PUB 140-1, Federal Information Processing Standard Publication 140-1, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, Gaithersburg, 1994

C. Kryptografie a normy
Díl 8. Normy IETF – S/MIME, část 3.
Jaroslav Pinkava, AEC spol. s r.o. & Norman Data Defense Systems, CZ

l. Úvod

Pokračování seriálu „Kryptografické normy“ v Crypto-Worldu navazuje na předešlá dvě čísla a bude tedy pojednávat o problematice bezpečnosti mailových zpráv - formátu **S/MIME**. První část byla věnována historii vzniku norem pro bezpečný mail a byla vysvětlena obsahová stránka formátu S/MIME. Druhá část se věnovala RFC dokumentům, tato poslední třetí část obsahuje přehled existujících draftů.

2. Drafty IETF S/MIME

Na webovské adrese http://www.ietf.org/html.charters/smime-charter.html najdete dnes (červen 2001) celkem 17 rozpracovaných draftů. Vzhledem k tomu, že tyto dokumenty jsou stále ještě vlastně v přípravné fázi (tj. jejich podoba není definitivní) bude následně proveden jen poměrně stručný přehled obsahu těchto dokumentů.

2.1. Cryptographic Message syntax (draft-ietf-smime-rfc2630bis-01.txt)

Jak již obsah napovídá, draft obsahuje přípravu nové verze dokumentu rfc2630. Pojednání o využití konkrétních kryptografických algoritmů bylo přesunuto do zvláštního dokumentu (odstavec 2.2.). Podstatné zásahy se objevily v nových či upravených definicích syntaxe.

Implementace např. nyní musí podporovat tři techniky řízení práce s klíči (označené jako ktri, kari a kekri). Podporovány jsou následující typy certifikátů: PKCS #6 rozšířený certifikát [PKCS#6]; X.509 certifikát; verze 1 X.509 attributového certifikátu (ACv1) [X.509-97]; a verze 2 X.509 attributového certifikátu (ACv2). Avšak PKCS #6 rozšířené certifikáty jsou podporovány jen z hlediska kompatibility se starými verzemi a neměly by být používány.

2.2. Cryptographic Message Syntax (CMS) Algorithms (draft-ietf-smime-cmsalg-00.txt)

Dokument v návaznosti na předešlý specifikuje používaní kryptografické algoritmy. Nahrazuje dvanáctý paragraf RFC2630. Algoritmy jsou rozděleny do dvou tříd – první z nich je třída algoritmů, kterou implementace musí podporovat, druhou třídou jsou algoritmy, které by implementace měly podporovat. Implementace samozřejmě mohou podporovat i další algoritmy. Přehledně je to znázorněno v následující tabulce.

Typ algoritmu	Musí být implementováno	Má být implementováno
Message Digest	SHA-1	MD5
Signature	DSA and RSA (*)	--
Key Management		
Key Agreement	--	X9.42 E-S D-H
Key Transport	RSA	--
Symmetric KEK Wrap	Triple-DES Key Wrap	RC2 Key Wrap
Content Encryption	Triple-DES CBC	RC2 CBC
Message Authentication	HMAC with SHA-1	--

2.3. Preventing the Million Message Attack on CMS (draft-ietf-smime-pkcs1-00.txt)

Dokument popisuje strategii obrany proti známému Bleichenbacherovu útoku vzhledem k PKCS1. Kromě OAEP jsou zde popsány další dvě techniky.

2.4. S/MIME Version 3.1 Certificate Profile Addendum (draft-ietf-smime-v31cert-00.txt)

Vzhledem k tomu, že vypršela platnost patentu na RSA algoritmus je navrhováno nahradit v třídě povinných algoritmů algoritmy DSS a Diffie-Hellman algoritmem RSA. Draft popisuje nezbytné úpravy v RFC2632 (S/MIME Version 3 Certificate Handling).

2.5. Use of the Advanced Encryption Algorithm in CMS (draft-ietf-smime-aes-alg-01.txt)

Dokument, jak název napovídá, se zabývá použitím AES algoritmu v rámci CMS. Dále je zde popsán postup pro aplikaci algoritmu RSA-OAEP pro přenos klíčů v návaznosti na novou verzi PKCS#1 (verze 2).

2.6. Reuse of CMS Content Encryption Keys (draft-ietf-smime-rcek-04.txt)

Draft specifikuje způsob, kterým lze zahrnout identifikátor klíče do CMS zabalené datové struktury, umožňující i následné použití klíče content encryption key pro další pakety (zprávy).

2.7. Electronic Signature Policies (draft-ietf-smime-espolicies-01.txt)

Dokument vychází z evropské normy připravené ETSI (ETSI TS 101 733 V1.2.2). O této normě bylo pojednáno v [3].

2.8. Electronic Signature Formats for long term electronic signatures (draft-ietf-smime-esformats-04.txt)

Stejně tak jako předešlý tak i tento dokument vychází z normy ETSI (ETSI TS 101 733 V1.2.2) a je zaměřen na problematiku podpisů s dlouhodobou platností.

2.9. S/MIME Symmetric Key Distribution (draft-ietf-smime-symkeydist-04.txt)

V tomto draftu je popsán mechanizmus řízení práce s klíči symetrické kryptografie.

2.10. Implementing Company Classification Policy with the S/MIME Security Label (draft-ietf-smime-seclabel-04.txt)

Daný dokument se zabývá problematikou firemní bezpečnostní politiky (pro klasifikaci jednotlivých stupňů ochrany dat) v návaznosti na bezpečnostní návěští v S/MIME. Toto je nepovinná služba v rámci S/MIME implementací.

2.11. Compressed Data Content Type for S/MIME (draft-ietf-smime-compression-04.txt)

Formát CMS dat neobsahuje žádný přístup umožňující využití komprese dat před odesláním zprávy. Vzhledem k nesporné výhodnosti takovéto komprese je v draftu definován postup jak použít komprimovaná data v CMS zprávě.

2.12. Use of ECC Algorithms in CMS (draft-ietf-smime-ecc-06.txt)

V návaznosti na normu ANSI X9.62 jsou v draftu definovány postupy, jak implementovat eliptickou kryptografii (ECDSA, ECDH a ECMQ) pro CMS.

2.13. Password-based Encryption for S/MIME (draft-ietf-smime-password-03.txt)

Dokument popisuje postupy pro šifrování dat opřené o využití uživatelova hesla.

2.14. Examples of S/MIME Messages (draft-ietf-smime-examples-06.txt)

Zde je dána celá rozsáhlá serie konkrétních příkladů těl zpráv při implementacích S/MIME. Jsou to příklady objektů CMS, S/MIME zpráv a rozšířených bezpečnostních služeb ESS. Cílem dokumentu je napomoci dosažení vysoké kompatibility jednotlivých konkrétních implementací S/MIME.

2.15. Domain Security Services using S/MIME (draft-ietf-smime-domsec-08.txt)

V dokumentu je popsáno, jak S/MIME protokol může být zpracováván a generován různými komponentami komunikačních systémů (poštovní agenti, brány atd.). Jsou zde popisovány přístupy k řešení interoperabilních problémů, problémů z hlediska omezení technického řešení.

2.16. Transporting S/MIME Objects in X.400 (draft-ietf-smime-x400transport-02.txt)

Zde je popsán protokol pro přenos CMS objektů (spojených s využitím S/MIME verze 3) v rámci přenosových systémů dle normy ITU X.400..

2.17. Securing X.400 Content with S/MIME (draft-ietf-smime-x400wrap-02.txt)

V návaznosti na předešlý dokument je zde popsán protokol pro vytváření digitálních podpisů a pro šifrování zpráv vzhledem k formátu X.400.

3. Shrnutí

Cílem této série tří článků bylo provést přehled normativních dokumentů pro S/MIME vzniklých v rámci příslušné pracovní skupiny IETF. Z přehledu lze získat informace o hlavních okruzích problémů, kterými se dokumenty zabývají a to jak z hlediska současně platných RFC, tak i vlastně z hlediska teprve rozpracovávaných přístupů.

4. Použité zkratky

V následujícím je stručně popsán význam zkratek, se kterými se čtenář může setkat v tomto článku.

ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One - ISO/IEC norma pro kódování
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List (seznam odvolaných certifikátů)
ECDH	Diffie-Hellman (schéma pro výměnu klíčů) pro elipt. křivky
ECDSA	DSA algoritmus pro eliptické křivky
ECMQ	Menezes-Qu-Vanstoneova varianta odvození společné utajované hodnoty při použití eliptického kryptosystému
ESS	Enhanced Security Services
IETF	The Internet Engineering Task Force
PKCS	Public Key Cryptographic Standard
RFC	request for comment
RSA	Rivest-Shamir-Adleman – algoritmus asym. kryptografie, první významný kryptosystém s veřejným klíčem
S/MIME	Secure/Multipurpose Internet Mail Extensions
X.400	přenosové protokoly definované CCITT
X.509	ITU-T norma pro práci s digitalními certifikáty

5. Literatura

[1] S/MIME Mail Security (smime) http://www.ietf.org/html.charters/smime-charter.html

[2] J.Pinkava:
Kryptografické normy díl.6. Normy IETF – S/MIME, část 1., CryptoWorld 4/2001
Kryptografické normy díl.7. Normy IETF – S/MIME, část 2., CryptoWorld 5/2001

[3] J.Pinkava: Připravované normy k EP v rámci Evropské Unie, Crypto-World 1/2001

D. Počítačový kurs Lidových novin
Mgr. Pavel Vondruška (ÚOOÚ)

Vážení čtenáři, často se setkávám s tím, že zavolají novináři s dotazem k připravované vyhlášce k zákonu o elektronickém podpisu a pokud nemáme ihned čas odpovídat, neopomenou podotknout, že čtenáři mají právo na informace (např. podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím). Domnívám se, že i čtenáři našeho e-zinu mají právo na informace - tentokráte o kvalitě informací v novinách. Dovoluji si proto publikovat svůj e-mail, který jsem zaslal redaktoru Stanislavu Drahnému z Lidových novin. Tento redaktor odpovídá za přílohy otištěné v těchto novinách. Obsahem mého e-mailu bylo poukázat ne nepřesné a zavádějící informace, které byly otištěny v rubrice počítačového kursu věnovaného elektronickému podpisu. Bohužel na můj e-mail ani pan redaktor, ani nikdo jiný z Lidových novin doposud neodpověděl.

Nemyslím si, že by mé "poučování" uvedené v dopise redakci bylo nějaké přehledné a úplné, ale šlo mi v něm o upozornění na chyby a nebylo původně určeno jako nějaký popis určený ke zveřejnění. Teprve po té, když jsem nedostal žádnou odpověď, jsem se rozhodl svůj názor na obsah příslušného počítačového kursu zveřejnit.

Od: Vondruška Pavel
Odesláno: 8. června 2001 18:07
Komu: 'stanislav.drahny@lidovky.cz'
Předmět: chyby, které byly uvedeny 7.6.2001 v počítačovém kursu LN

Mgr. Pavel Vondruška
Úřad pro ochranu osobních údajů
Odbor elektronického podpisu

Stanislav Drahný
vedoucí příloh
LN

Dobrý den,
dovoluji si zaslat pár řádků k poslednímu počítačovému kursu uvedenému v LN 7.6.2001.
Pevně doufám, že tyto chyby se již nebudou v "Počítačovém kursu"
(http://www.lidovky.cz/pocitacovykurs) opakovat.

S pozdravem
Pavel Vondruška

Vážená redakce,

Jako pracovník útvaru, který se zabývá elektronickým podpisem, si dovoluji upozornit na chyby, které byly uvedeny 7.6.2001 v počítačovém kursu LN (osmdesátý díl) **"Jak používat elektronický podpis".** Chyby, které zde jsou uvedeny , jsou zcela zásadního charakteru , jsou zavádějící a matoucí.

Jediné místo, kde autor kursu něco "vysvětluje", je toto:

(začátek citace)

"PETR: Nejdřív si opatříte program, který umožní **odesílané dokumenty šifrovat** a označovat. Pak si u tzv. certifikační autority necháte ověřit totožnost **a požádáte o certifikát garantující pravost vašeho elektronického podpisu. Tam také dostanete disketu nebo čipovou kartu s vaším elektronickým podpisem**, chráněnou PIN kódem. A pokud máte elektronický podpis na čipové kartě (což se doporučuje, protože to je bezpečnější než na disketě), musíte si ještě pořídit zvláštní čtečku připojenou k počítači."

(konec citace).

V tomto jediném odstavci jsou následující chyby:

... **odesílané dokumenty šifrovat** ... podepsané dokumenty se neodesílají zašifrované. Pokud chce odesílatel obsah šifrovat, může tak učinit, ale se samotným podepisováním to nemá nic společného.

... **a požádáte o certifikát garantující pravost vašeho elektronického podpisu. Tam také dostanete disketu nebo čipovou kartu s vaším elektronickým podpisem**,...- autor popisuje zakořeněnou chybnou představu, proti které se snažíme již přes rok neúspěšně bojovat a tato mylná představa je neustále živena podobnými výroky. Certifikát totiž obsahuje data pro ověření elektronického podpisu a další náležitosti (viz. např. u kvalifikovaného certifikátu paragraf 12 zákona o elektronickém podpisu). Čipová karta ani certifikát neobsahují a ani nemohou obsahovat elektronický podpis! Certifikát slouží k důvěryhodnému předávání dat pro ověření elektronického podpisu. Elektronický podpis sám o sobě neexistuje, a proto nemůže být uložen na čipové kartě. Pro každý text je jiný. Zaručený elektronický podpis (o kterém se, jak vyplývá z kontextu, mluví) totiž vznikne tak, že se nejprve z textu vypočte otisk (hash) a ten se šifruje daty pro vytváření elektronického podpisu (vhodným asymetrickým algoritmem). Výsledkem je elektronický podpis.

Podepisující osoba pak odešle :
text (nezašifrovaný !), elektronický podpis (vytvořený z textu a dat pro vytváření elektronického podpisu) a certifikát (s daty pro ověření podpisu).

Tento díl kursu zjevně místo vysvětlení příslušných pojmů jejich skutečný význam zatemnil.

Děkuji.
Mgr. Pavel Vondruška

E. Security and Protection of Information

Daniel Cvrček, VA Brno, člen organizačního výboru SPI
http://www.vabo.cz/cate

Jak asi všichni víte, začátkem května proběhl v Brně veletrh IDET. Část z Vás se možná již zúčastnila 1. ročníku konference, která se jmenovala **Bezpečnost a ochrana utajovaných skutečností**, s anglickým překladem **Security and Protection of Information (SPI)**. Český název pochází z doby, kdy vznikla myšlenka pořádání takovéto konference, a to v podobě národního semináře o ochraně utajovaných skutečností. Díky organizačnímu výboru, který byl tvořen skupinou na Katedře automatizovaných systémů velení a řízení (vojenské názvy jsou, jak jsem zjistil skoro vždy krkolomné) Vojenské akademie v Brně.

Předsedou výboru a hybnou pákou celé přípravy byl plk. doc. Ing. Jaroslav Dočkal, CSc., který se především zasloužil o to, že původní forma národního semináře se změnila na fakticky mezinárodní konferenci o bezpečnosti a kryptografii, s velmi solidní úrovní.

Výsledkem snahy organizačního výboru bylo jak výborné zajištění konference na místě (alespoň podle názoru většiny účastníků), tak i vytištění velmi pěkného sborníku s příspěvky konference a následně i vytvoření CD-ROM s většinou prezentací, které byly během konference odpřednášeny.

Co se týká samotného průběhu konference, tak zde celkem zaznělo přes třicet příspěvků, z toho třetina od zahraničních autorů (Rumunsko, Polsko, Slovensko, Belgie, USA). Témata se týkala nejen kryptografie jako takové (např. Tomáš Rosa s Random Oracle Model, nebo Ladislav Huraj s příspěvkem Cascaded Signatures). Velké množství příspěvků se týkalo i certifikačních autorit. Problematika prezentací byla volena jak z pohledu nasazení v armádě (Victor-Valeriu Patriciu, Aurel Serb), právních aspektů (Ján Matejka, Pavel Vondruška), používání (Petr Hanáček), až např. po rizika, které jejich nasazení přináší (Daniel Cvrček).

Další příspěvky se týkaly např. bezpečnosti v počítačových sítích a v neposlední řadě i hodnocení bezpečnosti informačních systémů. Nelze zapomenout ani na krátké příspěvky firem se vztahem k bezpečnosti, které si také získaly velké množství posluchačů.

Panu docentu Dočkalovi se podařilo získat i několik velmi zajímavých zahraničních řečníků, jen namátkou vyberu dva z nich. O správě informačních sítí US Army v Evropě mluvil Brooks B. Chamberlin (z 9th Signal Command, v Mannheimu, Německo) a úvod do standardů pro hodnocení bezpečnosti zazněl ústy Rogera Allana Frenche (fa. Compaq), jednoho z těch, kteří se podíleli na vytvoření standardu Common Criteria.

Vzhledem k tomu, že se přihlásilo dost účastníků (nakonec jsme museli přihlášky odmítat) a přálo nám i počasí (přestávky bylo možné trávit na otevřené terase s výhledem na jezírko), tak to snad ani lépe dopadnout nemohlo.

Využiji také tuto příležitost, abych poděkoval všem účastníkům konference za jejich přízeň a partnerům konference za podporu. Za organizační výbor také doufám, že při dalším ročníku (pravděpodobně v roce 2003) se setkáme i s těmi, kteří se letos, k vlastní škodě, účastnit nemohli.

Případní zájemci si mohou na adrese jdockal@vabo.cz objednat CD-ROM obsahující sborník konference v elektronické podobě a prezentace v PowerPointu. Cena 100 Kč + poštovné.

F. Odpovědnost poskytovatelů volného prostoru na internetu za cizí obsah

JUDr. Ján Matejka, Ústav státu a práva AV ČR (matejka@itlaw.cz)

MÍSTO ÚVODU

Právní odpovědnost představuje jednu ze základních a nepochybně také nejstarších právních institutů. Pokud se pokusíme analyzovat vývoj této právní úpravy, nepochybně dospějeme k závěru, že v historii existoval mnohdy velmi protikladný vývoj názorů na postavení a odpovědnost člověka ve společnosti, stejně tak jako na vztah jeho svobody a jeho povinností.

Jednou z takových nepochybně nejvíce kontroverzních otázek současnosti je problematika právní odpovědnosti v souvislosti s poskytováním volného prostoru na Internetu, tedy tzv. právní odpovědnosti za webhosting. Řada otázek zde však zůstává jak právní teorií tak i praxi dosud zcela neřešena. To se samozřejmě výrazným způsobem projevuje jak v názorech laické veřejnosti, tak i v chování těchto poskytovatelů, kteří – neznaje platnou úpravu – zveřejňují řadu různých smluvních ujednání, která jsou patrně ve svých důsledcích všechna buď přímo absolutně nebo „alespoň“ relativně (tedy ve své části) neplatná.

Smyslem tohoto článku je především nastínit tuto problematiku a upozornit na některá problematická ustanovení vybraných zákonných norem.

K NĚKTERÝM OBECNÝM ASPEKTŮM

Za cizí obsah je v tomto smyslu třeba považovat *elektronická data sítě Internet, náležící jinému subjektu než poskytovateli volného prostoru, která lze přenášet prostředky pro elektronickou komunikaci a v některých případech též uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou* (jde např. o webové stránky ve formátu HTML, formátovaný text z libovolného textového editoru, fotografie, hudbu, animace a zvuky, apod.).

Volným prostorem se pak rozumí *datový prostor na Internetu, kde může být na základě smlouvy tento obsah zpřístupněn.*

Poskytovatelem volného prostoru se pak rozumí *právnická nebo fyzická osoba, který na základě smlouvy poskytuje na Internetu datový prostor jiným subjektům a tak zpřístupňuje cizí obsah prostřednictvím počítačové sítě Internet, případně poskytuje další služby s tím spojené.*

Je nesporné, že na Internetu dochází také k poskytování vlastního obsahu. S ohledem na řadu odlišností v právní kvalifikaci mezi poskytováním obsahu vlastního a obsahu cizího, se budu v tomto článku zabývat výhradně odpovědností za poskytování obsahu cizího, nikoli tedy těmi případy, kdy subjekt, který obsah zpřístupňuje, je shodný s tím, kterému obsah náleží. Poskytovatelem obsahu je pak konkrétní subjekt, který vytvořil nebo si nechal vytvořit obsah (např. webové stránky) a který má tedy tento obsah (webovou stránku či jiná data) umístěn na diskovém prostoru k tomu vyhrazeném poskytovatelem volného prostoru.

ODPOVĚDNOST ZA CIZÍ OBSAH

Samotný pojem cizího obsahu lze samozřejmě dále vymezovat a upřesňovat (Již jen samotná problematika vymezení pojmů vlastní a cizí obsah by byla nepochybně velmi zajímavým námětem na článek – to snad někdy příště). V tomto směru je však ještě mnoho nevyřešených otázek a tak nelze jednoznačně konstatovat zda využívání tzv. vnořených

odkazů (embedded link, inlining), příp. využívání rámů (framing),lze označit za obsah vlastní či cizí.); v tomto článku se však těmito aspekty příliš zabývat nehodlám. **Podstatný je zásah do práva, příp. navozený protiprávní vztah, o kterém předpokládáme, že objektivně nastane** (zda a v jakém případě tomu tak bude či nikoliv, se zde podrobněji zabývat nebudeme, typicky však jde o porušování autorského práva, známkového práva, práva hospodářské soutěže apod.).

ODPOVĚDNOST ZA ŠKODU DLE OBČANSKÉHO ZÁKONÍKU

V občanském zákoníku (Zákon č. 40/1964 Sb. Občanský zákoník v platném znění (dále jen ObčZ, případně občanský zákoník)) je odpovědnost za škodu upravena v jeho části šesté § 415 až § 450. V souvislosti se zaměřením tohoto článku lze výklad rozdělit zejména do následujících oblastí:

- *předcházení vzniku škod* (zakročovací povinnost, krajní nouze, nutná obrana – vzhledem k rozsahu článku se jimi však dále zabývat nebudeme)
- *obecná odpovědnost*
- *zvláštní odpovědnost*
- *způsob a rozsah náhrady*

Předcházení vzniku škod (prevence)

Právní řád vždy klade důraz na to, aby ke škodě vůbec nedošlo, a proto upravuje určité instrumenty, kterými se má škodě předcházet (Jako např. právo zakročit způsobem přiměřeným okolnostem ohrožení, právo odvrátit nebezpečí hrozící v krajní nouzi a právo nutné obrany). Předcházení hrozícím škodám je upraveno v § 415 občanského zákoníku, podle něhož ***„Každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí.“.*** Je nesporné, že jde o velmi obecné ustanovení proklamativní typu; v praxi však má velmi široké důsledky. Jak tomu případě takovýchto obecných ustanovení obvyklé bývá, velmi významný podíl na výkladu zde hraje judikatura. Např. bylo odvozeno (Rozsudek Vrchního soudu v Praze sp. Zn. 5 Cmo 347/96.), že v případě, že by banka znala závažné skutečnosti, které by předem vážně ohrožovaly zjištěný podnikatelský plán klienta, přicházela by v úvahu obecná odpovědnost předcházet škodám a odpovědnost s tím související podle § 415 ObčZ, pokud by na tyto okolnosti klienta neupozornila (Rozsudek Vrchního soudu v Praze sp. Zn. 5 Cmo 347/96.) V tomto směru je zde třeba si uvědomit, že toto základní prevenční ustanovení se týká jak škod majetkových, tak i nemajetkových.

Otázka případného porušení výše uvedené povinnosti ze strany poskytovatele volného prostoru je pro další kvalifikaci takovéhoto jednání více než klíčová. Protože neexistuje žádná zvláštní úprava, která by stanovila povinnosti poskytovatelů volného prostoru, bude porušení této obecné povinnosti hlavním právním základem pro jeho případnou odpovědnost. **V tomto směru je nepochybně zapotřebí, aby poskytovatel učinil určitá opatření směřující k ochraně práv třetích osob.** Naprostá pasivita ze strany poskytovatele vůči jím zpřístupňovaného obsahu může mít za následek porušení povinnosti uvedené v § 415 ObčZ. Jednání poskytovatele, který v rámci svého tržního chování veřejně deklaruje nezájem o svůj obsah, případně prohlašuje (byť pravdivě) svou objektivní nemožnost kontroly tohoto obsahu či snad jednostranně prohlašuje likvidaci stop po osobách,

kteří tento obsah na jeho stránky umístili, patrně bude porušením povinnosti ve smyslu § 415 ObčZ.

Obecná odpovědnost za škodu

Tato část se již přímo týká odpovědnosti poskytovatele volného prostoru za cizí (právně závadný) obsah vůči třetím osobám.

V občanském zákoníku pojednává o obecné odpovědnosti za škodu část šestá, hlava druhá, oddíl první. Tento oddíl obsahuje dvě ustanovení, a to § 420 a § 420a. Generálním ustanovením zde však nepochybně je pouze § 420, nikoli § 420a, který pojednává o odpovědnosti způsobené provozní činností. Rubrika obou ustanovení však naznačuje, že zákon považuje i § 420a za obecnou odpovědnost založenou na objektivním principu.

V rámci obecné odpovědnosti dle občanského zákoníku tedy lze rozlišovat odpovědnost subjektivní (dle § 420) a objektivní (§ 420a).

Obecná odpovědnost za škodu na subjektivním základě

Obecná odpovědnost za škodu na subjektivním principu vyplývá z ustanovení § 420 a násl.) občanského zákoníku, které stanoví, že „*Každý odpovídá za škodu, kterou způsobil porušením právní povinnos*ti„. Z toho vyplývá, že základními předpoklady takové povinnosti jsou:

A. porušení právní povinnosti (existence protiprávního úkonu, který má povahu buď jednání nebo opomenutí)
B. způsobení škody (existence škody)
C. příčinná souvislost mezi způsobením škody a porušením právní povinnosti (tzv. kauzální nexus)
D. zavinění (a to jak nedbalostní, tak i úmyslné)

Ad A) Existence protiprávního úkonu, tedy úkonu *contra legem*, resp**. jednání, které je v rozporu s objektivním právem nebo smlouvou**. Protože neexistují žádné zvláštní zákonné povinnosti poskytovatele volného prostoru, bude hrát nejvýznamnější roli výše uvedené porušení § 415 ObčZ (obecná prevenční povinnost). V tomto směru se i několikrát judikatura zabývala otázkou způsobením škody „nedovoleným“ způsobem hry při sportovním utkání. Judikatura k tomu uvádí: „Zásadně nelze vyloučit odpovědnost hráče za škodu vzniklou protihráči během sportovní hry na hřišti podle ustanovení § 420 odst. 1 ObčZ. Ustanovení § 420 upravuje ObčZ upravuje právní povinnost a důsledkem jejího porušení je odpovědnost za způsobenou škodu. Hráč může ovšem takto odpovídat za takto způsobenou škodu jen za splnění všech zákonných předpokladů uvedených v ustanovení § 420 ObčZ. Pravidla hry sice nejsou právními předpisy, avšak pro hráče této hry nedodržení pravidel hry znamená nesplnění povinnosti předcházet hrozícím škodám, tj. povinnosti uložené v ustanovení § 415 ObčZ.

Ad B) Škodou se ve smyslu občanského práva **rozumí majetková újma (ztráta), kterou lze objektivně vyjádřit (vyčíslit) penězi**. (např. škoda vzniklá v důsledku zásahu do práva na ochranu osobnosti – např. zveřejněním nepravdivých údajů o určité osobě).

Ad C) Skutečnost, že **škoda musí být důsledkem protiprávního úkonu**, vyjadřuje vztah, aby mezi protiprávním úkonem na straně jedné a škodnou událostí na straně druhé existoval vztah příčiny a následku (příčinná souvislost).

Ad D) Při úpravě obecné odpovědnosti za škodu (dle § 420 a násl.) se vychází ze zavinění předpokládaného (nikoli tedy ze zavinění dokazovaného), což znamená, že **je to poškozený, kdo musí v jednotlivém případě prokazovat porušení právní povinnosti** (protiprávní úkon), **dále vznik a rozsah (výši) škody a příčinnou souvislost mezi způsobenou škodou a porušením právní povinnosti** (protiprávním úkonem). § 420 odst. 2 ale zároveň říká, že „.*Odpovědnosti se občan zprostí, jestliže prokáže, že škodu nezavinil*."

V souvislosti s možnými odpovědnostními důsledky pro poskytovatele je třeba zdůraznit, že v případě splnění výše uvedených požadavků **nepochybně za způsobenou škodu odpovídat bude**. Klíčovou otázkou zde však zůstává zda vůbec lze hovořit o zaviněném porušení právní povinnosti (a tedy základního předpokladu vzniku této odpovědnosti), pokud poskytovatel neví a ani od něj nelze očekávat aby věděl o protiprávnosti obsahu, který poskytuje.

Uvedli jsme, že právní povinností, jejíž porušení může založit odpovědnost za škodu, bude při absenci zvláštní úpravy povinnost dle § 415 ObčZ o předcházení škodám. Vzhledem k poměrně širokému výkladu této povinnosti ze strany soudů předpokládejme, že tuto povinnost má v souvislosti s cizím obsahem i poskytovatel volného prostoru. Aby byla založena obecná subjektivní odpovědnost dle § 420 ObčZ, musí být tato povinnost porušena zaviněně, tedy alespoň z nedbalosti. Pojem nedbalosti občanský zákoník neupřesňuje, a proto se vykládá v souladu s ustanovením trestního zákona.

Nevědomou nedbalost (i ta postačuje ke vzniku odpovědnosti) poskytovatele volného prostoru je tedy třeba vykládat tak, že „poskytovatel nechtěl škodu způsobit, ani nevěděl, že ji způsobit může, avšak vzhledem k okolnostem a svým osobním poměrům o tom vědět mohl a měl." Rozhodující zde je vazba „vědět mohl a měl". Vymezení tohoto pojmu je poměrně komplikované ani trestní zákon jej neupravuje. **Podle mého názoru nelze od poskytovatele volného prostoru spravedlivě požadovat takovou míru opatrnosti, která by mu přikazovala monitorovat a zkoumat cizí obsah.** Taková kontrola není při stávajícím množství dat a jejich neustálým změnám technicky ani časově možná. Proto zde konstatujeme, že poskytovatele volného prostoru nelze činit odpovědného za cizí obsah na základě zavinění z nevědomé nedbalosti.

Vědomá nedbalost je definována tak, že „poskytovatel nechtěl škodu způsobit, ale věděl však, že ji způsobit může, přičemž bez přiměřených důvodů spoléhal, že ji nezpůsobí." Zde je třeba, aby poskytovatel volného prostoru věděl o možnosti vzniku škody. To v našem případě znamená, že ví, že určitý cizí obsah může být právně závadný. Vše je jasné, pokud poskytovatel obdrží pravomocné rozhodnutí soudu o závadnosti cizího obsahu. Na druhou stranu nelze e-mail od soukromé osoby upozorňující například na porušování autorského práva apriori považovat za jasný důkaz závadnosti cizího obsahu. Takové upozornění je však ze strany poskytovatele volného prostoru třeba patrně prověřit, aby se tak zbavil případné nedbalostní odpovědnosti.

Dle mého soudu tedy obecná odpovědnost poskytovatele volného prostoru dle § 420 ObčZ může vzniknout **pouze na základě vědomé nedbalosti a to pokud tento poskytovatel**

ví o cizím obsahu a v přiměřeném rozsahu si neověří jeho případnou právní závadnost. Případně ověří, ale dále nedbá toho.

Ještě malá zmínka o obecná odpovědnost za škodu na objektivním základě (§ 420a ObčZ)

Jak vyplývá z výše uvedeného, obecná odpovědnost založená na subjektivním základě není odpovědností jedinou. V tomto směru je třeba nejprve zvážit otázku, zda nelze poskytování volného prostoru podřadit i pod jiný (speciální) druh odpovědnosti, který by aplikaci odpovědnosti subjektivní vylučoval. Takovou odpovědnosti je nepochybně odpovědnost objektivní, kde není třeba existence prvku porušení právní povinnosti (což může mít pro poskytovatele zásadní následky – odpovídal by tedy téměř vždy !). Základním problémem je zde především otázka **posouzení a vymezení pojmu „*škoda způsobená činností, která má provozní povahu*“, resp. toho, zda poskytování volného prostoru touto činností je či nikoliv.** Vzhledem k rozsahu tohoto článku se zde však omezím pouze na konstatování, že dle mého soudu se touto odpovědností činnost poskytovatelů volného prostoru neřídí. Připouštím však, že v tomto směru lze jen těžko argumentovat jednoznačně.

Zvláštní druhy odpovědnosti

Případy zvláštní odpovědnosti jsou upraveny v § 421 až 437 ObčZ. Vzhledem k odpovědnostní problematice poskytovatelů webhostingu za obsah, která je hlavním předmětem tohoto článku však lze v tomto případě aplikovat zejména ***odpovědnost za škodu způsobenou úmyslným jednáním proti dobrým mravům*** (§ 424 ObčZ). S ohledem na rozsah se tímto dále zabývat nehodlám. Pouze bych však zmínil, že jako jednání odporující dobrým mravům si lze jistě představit takové jednání poskytovatele, který byť v souladu se smluvními podmínkami začne bezdůvodně uzavírat přístup k obsahu jiných subjektů. Takový šikanózní výkon práva by patrně mohl splňovat předpoklady ke vzniku této zvláštní odpovědnosti.

Společná odpovědnost

Spoluodpovědností za škodu se rozumí odpovědnost v případech plurality odpovědných subjektů. Jde tedy o takové situace, kdy za škodu odpovídá více osob. V případě takové odpovědnosti pak občanský zákoník stanoví jako pravidlo odpovědnost solidární. To znamená, že v případě více škůdců může poškozený subjekt požadovat úhradu celé škody na kterémkoliv z nich.

V případě solidární odpovědnosti mají pak subjekty stanovenu povinnost vypořádat se navzájem podle účasti na způsobení vzniklé škody. Otázka spoluodpovědnosti má svůj význam v případě odpovědnosti poskytovatele volného prostoru a poskytovatele obsahu zároveň. Takto vzniklá škoda může být způsobena jednak „primárně“ poskytovatelem závadného obsahu (který tak porušuje například autorskoprávní normy) a zároveň „sekundárně“ poskytovatelem volného prostoru (který porušuje obecnou povinnost stanovenou v § 415 ObčZ).

Způsob a rozsah náhrady škody

Způsobem náhrady škody se rozumí určení formy, jakou se škoda nahrazuje. Rozsahem náhrady škody pak určení výše této náhrady. Samotnou náhradou škody se

konečně rozumí právně relevantní jednání, jehož podstatou je odstranění nebo zmírnění důsledků, které byly škodou způsobeny.

V souvislosti s určením způsobu a rozsahu náhrady škody je dále třeba zmínit také **otázku vyčíslení případné škody**. Pro vyčíslení případné škody je nepochybně velmi podstatné zjistit, **jak často byl právně závadný obsah čten popřípadě kopírován (stahován koncovým uživatelem).** To platí hlavně u jiných než textových souborů (hudba, video).

V případě stránek WWW lze toto nejčastěji vysledovat prostřednictvím monitoringu FTP přístupů. Nejen v těchto případech, ale v řadě dalších (např. IRC, apod.) se tak činí prostřednictvím tzv. log files. S tím nepochybně souvisí otázka archivace a případná integrita obsahu těchto log files. V našem právním řádu navíc **neexistuje povinnost poskytovatelů volného prostoru tyto log files archivovat** (tomuto problému se věnuji ve svém článku na LUPĚ, http://jason.lupa.cz/clanek.phtml?show=1076) Tyto log files přitom představují nenahraditelný důkazní prostředek v soudním řízení; jedině prostřednictvím těchto log files lze identifikovat pravého poskytovatele obsahu (content providera), resp. uploadera, stejně tak jako určit jak často byl tento obsah čten. Vzhledem k zásadě minimalizace ukládaných dat v informačních systémech se však tato data (log files) průběžně odstraňují, čímž je prakticky znemožněno jak určení osoby, která tento závadný obsah na své stránky umístila., tak i přesné vyčíslení případné škody. Stanovit povinnost uchovávat tyto log files v přiměřené míře **by patrně mohlo být účelné, stejně tak jako povinnost zajistit integritu dat (log files) např. prostřednictvím zaručeného elektronického podpis.**

ODPOVĚDNOST DLE OBCHODNÍHO ZÁKONÍKU

Stejně tak, jak je tomu v případě úpravy v občanského zákoníku, i v zákoníku obchodním (Zákon č. 513/1991 Sb. Obchodní zákoník; v platném znění (dále jen ObchZ, případně obchodní zákoník) je upravena odpovědnost za škodu. Její aplikace však bude s ohledem na posuzovanou problematiku spíše výjimečná, a to i v případě, že poskytovatel bude podnikatel.

ODPOVĚDNOST DLE AUTORSKÉHO ZÁKONA

Jednou z nejčastěji porušovaných norem na Internetu je bezesporu autorský zákon. (Zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů - dále jen AutZ, případně autorský zákon). Tento zákon uvádí ve svém 5. dílu tři skupiny nároků (a tedy sankcí) plynoucích z porušení tohoto zákona. Těmito nároky jsou zvláštní nároky podle § 40 odst 1 a 2 AutZ, právo na náhradu škody a právo na vydání bezdůvodného obohacení (§ 40 odst. 3 AutZ). Nárok na náhradu škody je upraven v občanském zákoníku. (viz.výše) Případná odpovědnost poskytovatele volného prostoru za škodu způsobenou porušením autorského práva ze strany poskytovatele obsahu je tedy zcela stejná jako u obecné odpovědnosti za škodu.

ODPOVĚDNOST DLE TRESTNÍHO ZÁKONA *(Zákon č. 140/1961 Sb. Trestní zákon; v platném znění (dále jen TrZ, případně trestní zákon)*

V souvislosti s výše uvedeným nelze také současně vyloučit možnost vzniku trestněprávní odpovědnosti. Vyjma některých obecných kategorií trestných činů. kterými se zde zabývat nebudeme, může jít o následující trestné činy:

- ***Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi*** (§ 152 TrZ)
- ***Neoprávněné nakládání s osobními údaji*** (§ 178 TrZ)
- ***Poškození a zneužití záznamu na nosiči informací*** (§ 257a TrZ)

Stejně tak lze hovořit o možném výskytu i dalších trestných činů, jejichž spáchání Internet výrazně usnadňuje. Jde zejména ***porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu*** (§ 150 TrZ) a ***porušování průmyslových práv*** (§ 151 TrZ). Těmi se však s ohledem na rozsah tohoto článku zabývat nehodláme.

V případě naplnění všech znaků trestného činu pak lze na poskytovatele volného prostoru pohlížet jako na pachatele (§ 9 odst. 1 TrZ), případně spolupachatele (§ 9 odst. 2 TrZ) či 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. Nedomníváme se, že by trestní odpovědnost poskytovatelů volného prostoru byla až tak častým jevem.

ODPOVĚDNOST DLE DALŠÍCH PŘEDPISŮ

Vzhledem k velmi průřezové úpravě odpovědnosti v našem právním řádu patrně nelze v příspěvku tohoto rozsahu plně zohlednit všechny možné odpovědnostní důsledky poskytování volného prostoru. Lze např. také hovořit o možné odpovědnosti z dalších zákonů (např. **ze zákona č. 37/1995 o neperiodických publikacích**; v platném znění), vzhledem k rozsahu toto však zde řešit nelze.

ZÁVĚR

Jak vyplývá z výše uvedeného, poskytovatel volného prostoru může být za určitých podmínek odpovědný v rozsahu § 420 ObčZ za nedbalostní porušení § 415 ObčZ. Nedbalost pak spočívá v tom, že ví o cizím obsahu a neověřil jeho závadnost, nebo jí ověřil a zjistil a cizí obsah neodstranil.

V tomto směru je však třeba hodnotit otázku znalosti závadného obsahu, resp. skutečnost, nakolik je poskytovateli volného prostoru znám, či může být znám obsah, resp. nakolik od něj lze očekávat aby obsah prostoru který poskytuje znal, případně i kontroloval. V tomto směru je tedy třeba vyslovit především následující:

- ***poskytovatel volného prostoru nepochybně odpovídá za cizí obsahy, které mu jsou známy, případně mu měly být známy a je technicky schopen a může být od něj rozumně očekáváno uzavření přístupu k nim***
- ***poskytovatel volného prostoru pak patrně neodpovídá za cizí obsahy, které není technicky schopen kontrolovat***

V některých – spíše výjimečných – případech pak může být odpovědný i podle úpravy v obchodním zákoníku, případně též odpovědný trestněprávně.

G. Ukončení platnosti, zneplatnění (a zrušení) certifikátu (II.díl)

Mgr. Josef Prokeš, ÚOOÚ, josef.prokes@uoou.cz

Hovoříme-li o zneplatnění certifikátu, rozumíme tím jednak postup poskytovatele, jednak úkon (akt) poskytovatele, jejímž adresátem je podepisující osoba. Tato je však s poskytovatelem ve smluvním vztahu, případná (a předvídatelná) rizika se dají smluvně „ošetřit". Na certifikát a seznam zneplatněných certifikátů však spoléhá mnoho dalších osob, které buď teprve hodlají jednat s podepisující osobou nebo již skutečně spoléhají na podpis - provedly ověření platnosti certifikátu, sjednaly s podepisující osobou plnění a plní s důvěrou v certifikát, s „dobrou vírou". (Zatím pouze pomysleme na to, že – nic nemůže být tak zlé, aby to nebylo ještě horší – největší skupinou osob dotčených elektronickým podepisováním bude skupina osob poškozených.)

Pro začátek se můžeme pokusit odpovědět, kdy je certifikát zneplatněn. Domnívám se, že okamžik zneplatnění nelze vždy (a pravděpodobně většinou) ztotožňovat s časem uvedení do seznamu zneplatněných certifikátů a již vůbec ne s dobou zveřejnění seznamu. Tomu napovídají ustanovení § 6 odst. 1 písm h) zákona o elektronickém podpisu, podle něhož je poskytovatel povinen zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát zneplatněn, byl dostupný třetím stranám, a dále § 15 odst. 2 zákona, který stanoví, že seznam musí obsahovat přesný časový údaj, kdy byl certifikát zneplatněn (pohleďme také na zcela nesystematické „nakopírování" ustanovení do tohoto paragrafu).

Zneplatnění, byť na základě nařízení úřadu, není úřední akt, zneplatnění sestává z řady úkonů poskytovatele, náležitosti upravuje zákon, ukládá poskytovateli řádné provedení zneplatnění formou více povinností. Zákonná úprava je provedena rámcově, a to je správné, bohužel však nedůsledně. Jednání poskytovatele při zneplatnění může zasáhnout do mnoha existující právních vztahů, každé opomenutí poskytovatele může mnoho sporných případů vytvořit.

Detailní a spolehlivější způsob zneplatnění by měl být někde upraven (tedy: zbývá politika poskytovatele), především z důvodu možné odpovědnosti, resp. rizika přechodu této odpovědnosti z podepisující osoby, která požádala o ukončení platnosti. Pokusím se rozvést obecný případ zneplatnění, konkrétně si lze představit, jak ze smluvního ujednání lze nepřímo dovozovat závislost podmínek ujednání nebo okolností případu na určení přesného času ukončení platnosti certifikátu. Nepochybně bude také čas zneplatnění certifikátu uváděn jako rozvazovací podmínka smlouvy.

Podá-li podepisující osoba žádost dle § 6 odst. 7 zákona, musí ukončit poskytovatel platnost certifikátu neprodleně. Ptáme-li se na význam příslovce „neprodleně", pomůžeme si anglickým „as soon as possible". Poskytovatel prostě jedná přiměřeně - s využitím všech technických a lidských zdrojů, které je schopen mít ke své dispozici. Je možno si představit zneplatnění během pěti minut od obdržení žádosti, ale také 24 hodin nebo déle, uvážíme-li, že při zajištění veškerých pečlivých technických opatřeních selže vždy nevypočitatelný lidský faktor nebo zasáhne „vis maior".

Ani do doby ukončení ve smyslu § 6 odst. 7 zákona si však nemůžeme být jisti pouhou oporou zákona. Vznikne-li osobě spoléhající na podpis nebo jakékoliv jiné („třetí") osobě škoda, je v prvé řadě odpovědna za škodu způsobenou porušením povinností uložené

podepisující osobě sama podepisující osoba (§ 5 odst.2 zákona), pokud má ke škodě alespoň nedbalostní vztah. Tato se však odpovědnosti může zprostit poukazem na skutečnost, že poškozený neučinil veškeré kroky nezbytné pro ověření platnosti certifikátu.

Poskytovatel se tedy nemusí v daném případě obávat soudní žaloby o náhradu škody za podmínky, že zneplatnění provedl „okamžitě, neprodleně, do uplynutí 10 hodin“ (termín zůstává klíčovým) v souladu se zákonem a také v souladu se zákonu odpovídajícími upřesňujícími podmínkami postupu poskytovatele (uvedenými v jeho politice), kteréžto předtím učinil součástí smluvních podmínek sjednaných s podepisující osobou.

Naproti tomu podepisující osoba, která pochybila (porušila zákonné povinnosti, příp. způsobila škodu), může marně argumentovat, že např. uvědomila poskytovatele ve smyslu § 5 odst. 1 písm b) zákona a podala žádost o ukončení platnosti certifikátu. (Je také důležité si uvědomit, že nepostačí pouhé vyrozumění poskytovatele. V takovém případě nebude možno většinou aplikovat ustanovení § 6 odst. 7 nebo § 15 odst. 1 zákona a zneplatnit certifikát. Nebylo by vhodné, aby zákon obecně dával poskytovateli možnost zneplatňovat certifikáty na základě vlastního uvážení, již z důvodu možného poškození podepisujících osob, příp. dalších osob. Zde bude záležet na podepisující osobě, aby uvážila, zda hrozící a možná škoda je - ku podivu - nižší než negativní následky zneplatnění.)

V oblasti otázek zůstává případ následující po ukončení platnosti dle § 6 odst. 7 zákona. V daném případě již pravděpodobně učinila podepisující osoba vše nezbytné a zákon volá k činnosti poskytovatele. Je v zájmu poskytovatele, aby také zveřejnění údajů o zneplatnění bylo provedeno „neprodleně“. Děje se tak pod hrozbou odpovědnosti dle občanskoprávních předpisů - poskytovatel musí podstoupit povinnost k podniknutí všech nezbytných opatření k odstranění hrozby či existence závadné stavu s přihlédnutím k ochraně práv jiných osob.

Aby poskytovatel nutnost řešení dané situace minimalizoval, musí učinit podrobný popis procesu zneplatnění součástí své politiky. Dále musí tuto politiku učinit součástí smluvní dokumentace, především pro vztahy s podepisujícími osobami. V neposlední řadě, by měl s danými podmínkami zneplatnění (především s časem, příp. intervalem zneplatnění) seznámit každou třetí osobu před přístupem (poskytnutím) k seznamu zneplatněných certifikátů.

Zmiňované rozpory a nejasnosti zákona budou možná rychle odstraněny, praxe pravděpodobně objeví jiné, třeba významnější. Některé lze rozvinout a upřesnit a objasnit v rámci zákonného zmocnění (§ 20 zákona). Připomeňme si však, že jednoznačně ve smyslu závaznosti může pojmy zákona, které jsou podobné, avšak zákonem rozlišované („ukončení platnosti“ a „zneplatnění“, odlišnosti zveřejňovaných seznamů certifikátů), vykládat pouze zákonodárce a soud. Ostatní se mohou pouze dohadovat, co bylo úmyslem zákonodárce - úsměvné tvrzení, pokud si uvědomíme, jak vznikají některé právní normy.

Výše uvedené popisy nám ukazují, že schválený zákon, přes dané nedostatky, je použitelný. V soukromoprávní sféře je nutno, jako v případě mnoha jiných předpisů, pečlivě ošetřit závazky účastníků smluvních vztahů, klade se důraz na politiku poskytovatele certifikačních služeb. Ve sféře veřejnoprávní (státní správy, samosprávy, veřejné správy, nejšířeji veřejné moci) některé požadavky zákona upřesní a aplikaci některých nepřesností zamezí novely zákonů připravované v souvislosti s komunikací elektronickým způsobem (procesní předpisy).

H. Letem šifrovým světem - přehled vybraných akcí

1. **Volná místa na ÚOOÚ – Odbor elektronického podpisu !!!**
   Dejte prosím o nich vědět svým známým, studentům a kamarádům !!!
   V souvislosti se zavedením prováděcí vyhlášky k Zákonu o elektronickém podpisu do praxe hledáme zájemce o práci na Odboru elektronického podpisu. Hledáme dva zájemce o informační bezpečnost (absolventy VŠ po vojenské službě) a jednoho programátora / administrátora. Uplatnění může najít i mladý právník se zájmem o výpočetní techniku. Nabízíme velice zajímavou, tvůrčí práci a možnost seznámit se s nejmodernějšími, rychle se rozvíjejícími technologiemi. Veškeré další informace e-mailem pavel.vondruska@uoou.cz nebo telefonicky 02 / 721 88 314 (Vondruška) http://www.uoou.cz

2. Ve dnech 6.-11.5.2001 se konala v Innsbrucku (Rakousko) mezinárodní konference **Eurocrypt´2001**. Konference je jednou ze tří nejprestižnějších konferencí v oblasti kryptologie (Crypto – USA, Asiacrypt - Asie, Eurocrypt - Evropa). Všechny tyto konference jsou pořádány IACR (International Association for Cryptologic Research) ve spolupráci s příslušnou národní kryptologickou institucí / organizací. Eurocyrpt 2001 byl již 20-tou konferenci v pořadí. Organizace IACR (http://www.iacr.org) se sídlem v Santa-Barbaře (USA) má přibližně 1000 členů po celém světě. Povinností člena je mimo jiné zúčastnit se jedné z tří výše jmenovaných konferencí. Mimo těchto klíčových konferencí pořádá nebo podporuje IACR během roku přibližně 30 dalších konferencí s tématikou kryptologie. Na konferenci jsou prezentovány nejdůležitější poznatky v oboru kryptologie v příslušném roce. Sborníky z těchto konferencí jsou nejvíce citovaným zdrojem v daném oboru. Na konferenci Eurocrypt´ 2001 bylo znát, že se výrazně zvýšil zájem o eliptické křivky a asymetrickou kryptografii. Byl předvedeno také další podpisové schéma. Osobně mě překvapilo, že jednotlivé příspěvky se nezabývaly hodnocením připravovaných primitivů z okruhu NESSIE (Evropská iniciativa) a Cryptrec (Japonská iniciativa). Na této konferenci ani nebyly předneseny zásadní příspěvky jako např. v roce 1999 v Praze (TWINKLE, prolomení RSA 512 bitů hrubou silou apod.). Celkem se konference zúčastnilo přes 420 lidí. Z ČR se zúčastnila skupina 11 odborníků (vůbec největší účast na těchto konferencích, mimo roku 1999, kdy se konference konala v Praze). Konference byla přítomna celá evropská i světová kryptolgická špička. Organizátoři zajistili hladký průběh a velice přátelskou a příjemnou atmosféru po celou dobu konference. Program konference viz. příloha k dnešnímu Crypto-Worldu.

3. NIST publikoval 30.5.2001 dlouho očekávaný draft k hashovacím funkcím s „dlouhým otiskem“. V současné době je k dispozici jediný hashovací algoritmus, který je standarizován pomocí schváleného dokumentu FIPS (SHA-1, FIPS 180-1). Zveřejněn byl draft dokumentu FIPS 180-2 obsahuje návrh hashovacích funkcí SHA-256 , SHA-384, SHA-512. http://csrc.nist.gov/encryption/tkhash.html

4. Dne 7. června 2001 v Národním domě na Vinohradech (Praha) uspořádala firma AEC (http://www.aec.cz) jednodenní konferenci **Security 2001**. Více jak 400 účastníků se seznámilo s řadou příspěvků z oblasti elektronického podpisu, informační bezpečnosti a samozřejmě virů. Účastníci obdrželi sborník s přednáškami a CD s prezentacemi jednotlivých účastníků (na CD jsou mimo jiné i naše e-ziny Crypto-World 9/99 až 5/201 ☺). Program konference s krátkou anotací je dostupný na http://www.security2001.cz/default.asp?what=prg

5. Claude Shannon - otec informační teorie a jeden ze zakladatelů vědecké kryptologie - zemřel letos v únoru ve věku 84 let.
   Více např. na ná sledujících adresách:
   MIT http://web.mit.edu/newsoffice/nr/2001/shannon.html
   Bell Labs http://www.bell-labs.com/news/2001/february/26/1.html

6. (Common Criteria for Information , Technology Security Evaluation, Smart Card Security User Group). 22.3.2001 byl zveřejněn draft obsahující bezpečnostní profil (PP Protection Profil) pro vyhodnocování smart-cart. Tento PP popisuje bezpečnostní IT požadavky na smart carty určené pro užívání v senzitivních aplikacích.
   http://www.netimperative.com/technology/newsarticle.asp?ArticleID=10646&ChannelID=3&ArticleType=1

7. Bylo vytvořena nové sdružení (aliance) s názvem **OpenPGP Alliance.** Cílem tohoto nového sdružení je sjednotit se na standardu, jehož dodržování zajistí kompatibilitu mezi jednotlivými uživateli (výrobci) rodiny produktů založených na PGP, předpokládá se využití PKI a nadále podpora silné kryptografie. Klíčové postavení v tomto sdružení bude mít Philip Zimmerman, který stojí u PGP od samého zrodu. Zakládajícími členy aliance jsou Biodata, Gnu Privacy Guard, Hush Communications, Laissez Faire City, LokTek, Qualcomm, SSH, Tovaris,Veridis, ZendIt and Zero-Knowledge.

8. Pika, Pika, Pikachuuuu. **China Digital Army** („pracovní“ název jedné skupiny slovenských hackerů) na přelomu května a začátkem června doslova řádila. Během jednoho dne se jim např. podařilo vyřadit na 212 slovenských serverů. Všechny postižené weby běžely na jednom stroji s neošetřenou chybou „ .printer „ . Na některých serverech se tak díky hackerům objevila poněkud nečekaně i tématika Pokémonů.

I. Závěrečné informace

1. Sešit

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

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

http://www.mujweb.cz/veda/gcucmp

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

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

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

3. Spojení

běžná komunikace**, zasílání příspěvků k otištění** , informace

pavel.vondruska@uoou.cz (**vondruskap@uoou.cz**)

vondruska.p@seznam.cz

pavel.vondruska@post.cz