Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 6/2010 **15. červen 2010**

6/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1360 registrovaných odběratelů)

Obsah:

A. Utajená míra složitosti?

Vlastimil Klíma, kryptolog konzultant, KNZ, s.r.o., Praha
(http://cryptography.hyperlink.cz, vlastimil.klima@knzsro.cz)

Článek navazuje na příspěvek v čísle 4 Crypto-Worldu 2010, v němž jsme chtěli stimulovat výzkum složitosti kandidátů na SHA-3. Navrhli jsme vyjít z algebraické normální formy. Protože ta je dost složitá - například jen po jedné jediné operaci ADD32 dvou 32bitových sčítanců vzniká přes 4 miliardy termů - navrhli jsme počítat počet (jednobitových) operací AND a XOR a počty meziproměnných (de facto paměťových buněk). V tomto článku navrhneme míru jednodušší, a to pouze jako minimální počet (jednobitových) operací AND, s kterými lze danou funkci obvodově realizovat. Tato míra se zdá být velmi dobrá, neboť je současně jednoduchá a současně dostatečně vypovídající. Původní složitost operace ADD klesne ze 4 miliard na hodnotu 31. Danou měrou jsme spočítali složitost nejrychlejších kandidátů na SHA-3 a byli jsme velmi překvapeni, jak jsou si tito kandidáti v naší míře blízcí! Jakoby tady pracovalo nějaké tajné pravidlo, které jejich návrháři dodržovali. Vzhledem k tomu, že tyto týmy pracovali nezávisle a v tajnosti, zanechává tento výsledek spíše více otázek, než jich řeší.

Míra složitosti

Mírou složitosti je tedy minimální počet operací AND. To lze u složitějších funkcí obvykle špatně spočítat. Stačí si zkusit toto spočítat pro malé substituční boxy 4 bity na 4 bity. Nicméně u operace ADD32 jsme v čísle 4 Crypto-Worldu tuto složitost spočítali, a je rovna 31, viz též následující rovnice.
$a = b + c$,
kde a, b, c jsou 32bitové proměnné, sčítání je v modulu 2^{32}.

Máme
pro bit i = 0: $a_0 = b_0 \oplus c_0$, $carry_1 = b_0$ AND c_0,
$a_i = b_i \oplus c_i \oplus carry_i$, i = 1, ..., 31,
kde $carry_{i+1} = (b_i \oplus carry_i)$ AND $(c_i \oplus carry_i) \oplus carry_i$ pro i = 1, ..., 30.
Tato míra složitosti hodně souvisí s praktickou elektronickou realizací, což je možná jedna z příčin oné utajené shody, viz tabulka.

Hašovací funkce typu XAR a ostatní

Složitost se nám dobře počítala pro funkce typu XAR, tj. funkce, používající pouze operace XOR, ADD a ROT (SHIFT). Zde stačí spočítat počet operací ADD a vynásobit složitostí 31. U ostatních funkcí může být výpočet jejich složitosti velice netriviální. Musíme umět prokázat, že máme vyjádření s nejmenším možným počtem operací AND, a to je obtížné. Proto hodnoty pro tyto funkce jsou jen orientační a je tu velké pole jak pro jejich přesnější výpočet, tak pro důkaz minima.

Algorit-mus	Používané operace	Rychlost (cyklů/bajt)	Počet operací AND na jeden bit zprávy	Koeficient rych-lost/složitost
SHA-1	XAR	9	17	1,89
BMW	XAR	7	24	3,43
BLAKE	XAR	9	29	3,22
Shabal	XAR a modulární násobení	10	13	1,30
CubeHash	XAR	13	992	76,31
SIMD	XAR a různé operace	12	23	1,92
Skein	XAR	21	26	1,24
SHA-2	XAR	20	40	2,00

Tabulka: Nejrychlejší kandidáti na SHA-3 a jejich míra složitosti

V tabulce je velice pěkně vidět, že SHA-2 je cca dvakrát složitější než SHA-1, za což platí svojí poloviční rychlostí. Avšak přece jen je trochu dokonalejší v tom, že za složitost algoritmu (počtu operací AND) se neplatí tolik ztrátou rychlosti jako u SHA-1, i když rozdíl je malý, viz koeficient rychlost/složitost v tabulce, což je (počet operací AND v algoritmu na jeden bit zprávy)/ (počet cyklů na jeden bit zprávy). Při přechodu od SHA-2 k SHA-3 však NIST chce tento koeficient ještě zvýšit, neboť požaduje současně vyšší bezpečnost (složitost), tj. většího čitatele, a současně menšího jmenovatele, tedy vyšší rychlost zpracování dat. Za normálních okolností bychom řekli, že je to nesmysl. Pouštíme se teď na tenkou půdu filozofování, ale je těžké si představit, že nějaký algoritmus, když ho máme před sebou "zadrátovaný" do logických operací, zesílíme tím, když nějaké operace AND z něho vyjmeme a nahradíme je operacemi XOR. Jistě, že bychom uměle takový příklad zkonstruovali, aby s vybranými operacemi AND vznikaly nějaké lineární závislosti mezi dílčími nelineárními bloky, zatímco, když je nahradíme operacemi XOR, tak tyto lineární závislosti zrušíme, a tím naopak zvýšíme složitost výsledného schématu. To je ale v případě umělého schématu, kde ve skutečnosti uměle vytváříme slabinu, abychom ji také uměle mohli odstranit. Jenže schémata, o nichž je řeč, mají být bez evidentních slabin, tj. taková, kde řešení příslušné soustavy booleovských rovnic je jedinou cestou, kterou kryptologové vidí, jak příslušný problém řešit. A zde je počet operací AND potom odrazem skutečné složitosti. Pokud bychom pokračovali dlouhým a rozsáhlým výzkumem, možná bychom nalezli hraniční hodnotu koeficientu složitost/rychlost pro současnou technologii. NIST svými požadavky na SHA-3 řekl, že chce,

aby výzkum tento koeficient zvýšil. Místo 50 let výzkumu jednoho týmu využil několik desítek týmů po dobu 5 let. Tímto způsobem pak přirozeně může vybrat nejefektivnějšího kandidáta. I když tento koeficient také souvisí se složitostí realizace (plochou křemíku apod.), určitě to nebude dělat jen podle něho, takže článek nesměřuje k tomu, že nejlepším kandidátem je BMW (odhlédneme-li od zcela vybočujícího CubeHash), ale spíše k pohledu na kandidáty z jiného úhlu, než je nabízen obvykle.
Poznamenejme, že značně odlišná čísla u CubeHash zatím nedokážeme vysvětlit, a možná, že někde je chyba v uvedených úvahách. Také počet operací u SIMD je hrubě odhadnutý a zasloužil by si řádný výpočet. Nicméně u ostatních algoritmů by měly být výpočty správné, což je podstatné, neboť shoda na složitosti je velmi překvapující.

Výpočet složitosti u kandidátů

V následujícím uvedeme, jak jsme dospěli k číslům v tabulce. Pro všechny kandidáty jsme posuzovali složitost jejich kompresní funkce, protože při prodlužování zprávy se složitost na bit pro kompresní funkci velmi rychle blíží složitosti na bit celé hašovací funkce. A použili jsme vždy variantu hašovací funkce, poskytující 256 bitů výstupu. Většinou jsou použity 32bitové operace, sčítání dvou 32bitových argumentů značíme proto místo ADD32 krátce ADD a sčítání 64bitových argumentů jako ADD64. Zkratka AND značí operaci AND dvou jednobitových argumentů, v níž složitost počítáme.

BMW-256

- blok je 512bitů (16 32bitových slov)
- funkce f0: 16 operací v f0, jedna operace má čtyři ADD (SUB) = 64 ADD, poté 16 ADD
- funkce f1: 2 rundy typu 1 + 14 rund typu 2 = 2*(18) + 14*(18) = 16*18=288 ADD
- funkce f2: 8+16 = 24 ADD
- celá kompresní funkce =64+16+288+24=392 ADD na 1 blok 512 bitů,
- složitost kompresní funkce = 392*31 = 12152,
- složitost na bit = 12152/512=**24**

Skein-256

- používá vždy 64bitová slova
- pro Skein-256 má blok 512bitů (4 slova)
- kompresní funkce se skládá z přičtení dat na průběžnou haš = 4 ADD
- potom 9 velkých rund, každá se skládá z 16 sčítání 64bitových slov a dvou přičítání průběžné haše
- celá kompresní funkce = 4 + 9*(8rund)= 4+9*(8+8+2*inject_key) = 4+9*(8+8+2*4) = 4+9*24 = 216 ADD64
- složitost kompresní funkce = 216*63=13608 AND
- složitost na bit = 13608/512=**26**

CubeHash

- nezávisí na délce haše
- na každý bajt nejprve provádí xor bajtu zprávy na vnitřní stav haše, stav má 1024 bitů (jakožto 32 32bitových slov)
- potom stav zpracuje 8 velkými rundami
- 1 velká runda má 10 kroků
- sčítají se vždy 32bitová slova, v jedné velké rundě je 32 ADD
- 8*32=256 operací ADD na jeden bajt zprávy
- složitost na 1 bit = 8*32*31/8= **992**

BLAKE

- Pro 256bitovou haš používá 16 32bitových slov zprávy (512bitový blok) a 8 32bitových slov průběžné haše
- kompresní funkce zpracovává průběžnou haš pomocí rund, v každé rundě je 8 operací G po šesti ADD, které promíchávají stav se dvěma slovy zprávy, má 10 rund
- celkem 10*8*6 = 480 operací ADD
- složitost je 480*31=14880
- složitost na 1 bit = 14880/512=**29**

Shabal

- používá mj. operace 3*x a 5*x modulo 2^{32},
- pracuje s 32bitovými slovy, blok zprávy je 512 bitů
- používá registry B (16 slov), C (16 slov), A (12 slov)
- Shabal-256 je typu double-pipe (Shabal-512 je single pipe), odlišnost je pouze v tom, kolik bitů se vezme z výsledku
- kompresní funkce se skládá z permutace P(A, B, C, M) a z počátečního a závěrečného přičítání,
- vstupem permutace je B = B + M, M se poté od výstupu permutace odečítá, tj. před a po permutaci je to 16 + 16 operací ADD (SUB)
- permutace obsahuje 3*(16*(U a V a jednu 32bitovou operaci AND))+ 3*12 ADD
- operace U = 3*x modulo 2^{32}, složitost je 30 AND (sčítá se x + 2x, druhý argument má o 1 bit méně, tj. jeden bit carry se ušetří)
- operace V = 5*x modulo 2^{32}, složitost je 29 AND (sčítá se x + 4x, druhý argument má o 2 bity méně, tj. dva bity carry se ušetří)

- permutace = 3*16*(U + V + AND32) + 36*ADD = 48*(30+29+32)+36*31 = 48*91+36*31=5484 AND
- počáteční a závěrečné +/- = 32 ADD = 32*31 = 992 AND
- složitost = 992 + 5484 = 6476 AND
- složitost na 1 bit = 6476/512=**13**

SIMD

- dost modifikovaná D-M konstrukce: (h, m) --> P(h, E_m(h xor m))
- blok má 512/1024 bitů podle délky haše 256/512
- vnitřní stav má 16 slov (32/64b)
- nejprve expanduje blok zprávy 512/1024 na osminásobek (4096/8192) a poté následuje tzv. Feistelovo schéma
- expanze:
- první úroveň: NTT je lineární MDS kód nad 64/128 "bajty" (prvky tělesa), vytvoří 128/256 bajtů
- druhá úroveň: vnitřní kódy, z bajtu udělá dva, tj. 256/512 bajtů
- třetí úroveň (permutace): také zdvojnásobí šířku, nakonec máme 128/256 slov
- složitost expanze odhadnuta = 7360 operací AND (tento výsledek není zatím příliš ověřen)
- Feistelovo schéma:
- slova se zpracovávají po čtyřech (krok), celkem 36 kroků
- krok = 3 ADD + AND32 = 125 AND
- Feistelovo schéma celkem = 36*125 AND = 4500 AND
- složitost = 4500 + 7360 = 11860 AND operací na 512 bitů zprávy
- složitost na 1 bit = 11860/512 = **23**

Literatura

Kandidáti druhého kola SHA-3: http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html

B. Ze vzpomínek armádního šifranta III.

Jeroným Knížek, knizek@centrum.cz

Volně navazuje na předchozí články *J.Knížek: Paměti armádního šifranta, Crypto-World 10/2007* a *J.Knížek: Ze vzpomínek armádního šifranta, Crypto-World 9/2009*, J.Knížek: *Ze vzpomínek armádního šifranta II, Crypto-World 5/2010*

Šifry 2. stupně

Na stupni pluk – prapor – rota a níže se odbývá za bojů nejvíce událostí a změn. Protože protivník bývá na dostřel, musí se před ním aspoň krátkodobě utajovat rozhodování velitelů. K tomu se nejčastěji užívaly signální a hovorové tabulky s kódovanými mapami. Aby skutečně tyto prostředky zajistily utajení pro nejbližší dobu (max. několika hodin), byly šifranty vyšších štábů pro jednotlivé druhy vojsk sestavovány na základě zkušeností velitelů a podle typizovaných a odzkoušených vzorů tabulky s nejfrekventovanějšími povely, jakož i s větami typických činností. Musely tam být i názvy jednotek, zbraní, zásob a dopravních prostředků, jakož i součinnostní signály. Takovou typizovanou signální tabulku s obsahem asi 80 – 200 výrazů šifrant zpracovával asi 3 hodiny, a protože odpovídala typizovanému vzoru, stačilo k ní vydat ze zásoby hotové heslové sešitky a vložit je s tabulkou do typizovaných obalů, platnou heslovou stránkou navrch. Tím okamžikem byly tabulky bez dalších úprav použitelné k vzájemnému styku velitelů pojítky. Hovorové tabulky byly obsažnější. Některé tabulky však mohly mít i několik volných řádků k dodatečnému vepsání potřebných a dohodnutých výrazů.

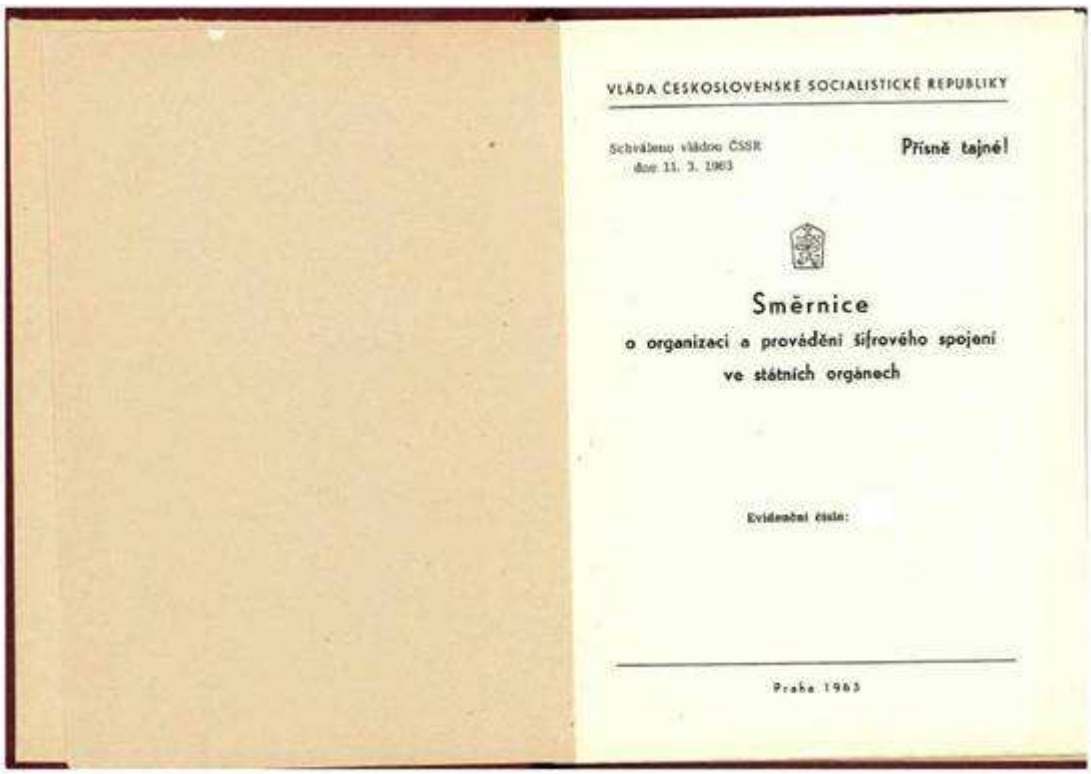
Heslový sešit spolu se stránkami výrazů tabulky umožňoval zakódovat daný výraz i několika různými způsoby pomocí nastavené heslové stránky a zároveň přecházet z povelů tabulky na kódovanou mapu a zpět, aniž by to na výsledném textu kódované zprávy bylo jednoduše k poznání. Zpravidla se užívalo číselných kódů, z počátku však i posuvných heslových proužků. Podobně byly užívány i tabulky k součinnosti s letcem apod., musely být snadno a hbitě ovladatelné a srozumitelné i jednotlivým vojákům (zakývání letounem vlevo/vpravo, vystřelení smluvené série barevných raket, apod.). Jednoduchý byl způsob kódování map, stačilo od určeného koordinátu sítě vypsat svisle a vodorovně stanovené řady čísel, přičemž detailní tvar obrazce byl neměnný. Každý bod mapy se kódoval dvěma třímístnými číselnými skupinami, podobně jako u tabulek. Velitelé byli tak vycvičení, že dokázali takto velet za každých podmínek diktátem do pojítka bez zapisování (to si poznamenali dodatečně).

Šifrant z KVS Č. Budějovice si nechal v tamním podniku vyrobit pravítkovou otočnou soupravu ke kódování map a podal ji jako zlepšovací návrh. Podobných zlepšovacích návrhů i k tabulkám se na MNO sešlo několik ročně, některé se i do armády zavedly. Ale jakmile se začaly užívat počítače (zprvu sálové), většina prostředků se na nich pravidelně ověřovala a jimi zpracované heslové sešity se po sériích tiskly ve speciálních tiskárnách.

Pseudonymy

V r. 1951 přišlo tehdejší Šifrovací oddělení (ŠO) na GŠ s utajovacím požadavkem, aby místo skutečných jmen používali vybraní vojenští představitelé při telefonických a rádiových hovorech tzv. "pseudonymy", které jim měli přidělovat velitelé od stupně svazku výše na návrh místních orgánů šifrové služby. K tomu byly na ŠO GŠ sestaveny a vydány tlusté mnohastránkové seznamy neopakujících se jmen v číslovaných oddílech po deseti jménech.

Zpracování seznamu bylo pracné - ruční. Jména nesměla mít nádech nadávky či být jakkoliv pejorativní a nevhodná (jako třeba Hitler, Bábinský, Rošťák). V praxi se to ukázalo jako těžkopádné a složité. Tehdy byl šéfem ŠO GŠ plk. Sedlák a sklidil za to vlnu kritiky. Užívání pseudonymů bylo zrušeno a plk. Sedlák byl přeřazen r. 1952 do funkce šéfa karlovarského Grand hotelu Moskva (dříve PUPP). Do funkce Náčelníka ŠO GŠ byl ustanoven plk. Frant. Rubeš, dosavadní pracovník Hlavní kádrové správy (HKS) MNO. Nedlouho poté z HKS uprchl na západ generál Šejna s tajnými dokumenty (známý jako handlíř s jetelovým semínkem) a odtud ČSR očerňoval různými výmysly. Stupňovala se studená válka a stát přitvrdil.



VLÁDA ČESKOSLOVENSKÉ SOCIALISTICKÉ REPUBLIKY

Schváleno vládou ČSSR dne 11. 3. 1963

Přísně tajné!

Směrnice

o organizaci a provádění šifrového spojení ve státních orgánech

Evidenční číslo:

Praha 1963

Krycí jména terénních předmětů

V přípravě jakékoli polní činnosti vojsk bylo k operačním plánům připojováno Nařízení pro utajení velení [NUV], kde byly vyjmenovány všechny utajovací prostředky, rozpis platnosti šifer, kódů a součinnostních opatření pro spolupůsobící druhy vojsk. Zainteresovaným štábům pak byly vydávány jen nezbytné výpisy. Od svazků dolů se užívaly prostředky vyhrazené jim vyšším štábem s jinými kódy, takže na štábu svazku (divize, brigády) měli dvojí utajovací prostředky (v jedné mapě) – jedny pro styk s vyšším štábem a sousedy a jiné pro styk s podřízenými vojsky, přičemž dostali nutné výpisy k součinnostnímu spojení (s letci aj.).

Zároveň s pseudonymy, o kterých jsem psal jinde, byly v padesátých letech do armády zavedeny k utajené domluvě velitelů tzv. Krycí jména terénních předmětů (KJTP). Štáb svazu či svazku nejprve stanovil zakroužkováním zájmové body [obce, kóty, řeky, rybníky, terénní celky - obecně markantní body] na slepené mapě. Šifrant pak ze zvláštní tištěné pomůcky o mnoha listech s terénními jmény bez abecedního pořádku, uskupenými v číslovaných oddílech, z ní k jednotlivým bodům připojil krycí jména (pokud kdekoliv na dané mapě existovalo skutečné jméno uvedené i v tištěné pomůcce, nesměl jej k označení vybraných bodů použít). Hotový písemný seznam KJTP se souřadnicemi byl poté vydán jako součást

NUV (spolu s dalšími pokyny pro danou polní akci). Tato krycí jména pak používali velitelé ve spojení se signálními či hovorovými tabulkami, obsahujícími krátké povely, zakódované zpravidla kódem řádku a sloupce toho signálu (bývalo jich více druhů). Vepisování KJTP do map však bylo velice pracné; proto bylo po několika málo letech používání KJTP zcela zrušeno, zůstaly v používání jen systémy Kódování map, převážně založené na předtištěné souřadnicové síti mapy.

Poválečné podmínky štábu

Když jsem jako šifrant v létech 1952 - 1956 sloužil v Písku u Velitelství 2. armádního sboru, byl velitelem sboru fronťák - gen. Sedláček (ze sboru pozdějšího prezidenta Svobody). Tehdy u štábů mnohde sloužili i sovětští poradci. Od 8. md z Kolína k nám byl převelen za náčelníka operačního oddělení kapitán Pézl, pozdější generál u prezidenta Havla. Patřily nám 1. pěší divize v Č. Budějovicích, 2. pěší divize v Sušici (ze Slovenska), 8. mechanizovaná divize v Kolíně, místní sborové útvary a dále výcvikové prostory (VVP) Boletice a Dobrá Voda na Šumavě. Pro vstup do VVP jsme sami vydávali a rozesílali průkazky na jméno.

Činnost šifrantů neměla nic společného s kontrarozvědkou apod. Museli jsme však plánovitě školit a kontrolovat opatření k utajení u podřízených štábů i jednotek a podávat o tom písemná hlášení. K výjezdu si šifrant musel objednat dopravu, často to byl jen motocyklista i na stovky km, někdy vlak či veřejný autobus. Nedostatky pak řešili velitelé a náčelníci štábů, případně vojenské soudy. Mnohde se důstojníci před blížící se kontrolou raději ukrývali. Osobní auto měl jen velitel sboru, štáb měl jen dva terénní džípy, jeden štábní autobus a 2 běžná nákladní auta Praga RND s polní stanovou výbavou. Další potřeby včetně kuchyně nám zajišťovaly sborové jednotky. Každé oddělení štábu mělo bednu na spisy.

Za plánovaných cvičení nám jednotky stavěly téměř pro každé oddělení stan - kapličku s kamínky, skládací postelí, stolem, židlemi, polním telefonem a nějakým osvětlením (často jen petrolejkou); také společnou umývárnu a shromažďovací stan - sloužící i za jídelnu. Spojovací ústředna měla jen pro nohy vyhloubené jámy s chvojím, šňůrový přepojovač postavený na bedně a po zemi k ní přivedené linky, stejně umístěné 2 dálnopisy Lorenz na chvojí a osový dálkový kabel; to vše kryté zavěšenými stanovými dílci z osobní výbavy vojáků obsluhy. Etablování na novém stanovišti trvalo obyčejně max. jednu hodinu, přemísťovali jsme se asi 3x - 4x denně. Šifrant používal ruční šifry uložené ve své brašně a zprávy v pětimístných skupinách dával k odeslání dálnopisu (příp. k odeslání morseovkou rádiem); v nouzi je sám diktoval hláskovací abecedou telefonem. Často musel pracovat jen někde za keřem s baterkou v puse a v povzdálí ho hlídal strážný. Na spaní nezbýval čas.

C. Hláskovací tabulka

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Cyril Rudolf Ypsilon Petr Tomáš Oto Pomlčka Dvojité V Ota Rudolf Ludvík David Charlie Romeo Yankee Papa Tango Oscar Pomlčka Whisky Oscar Romeo Lima Delta

Během přípravy úloh do podzimní soutěže jsem potřeboval jednu zprávu hláskovat. Vyvstala otázka správného hláskování podle nějaké platné oficiální hláskovací tabulky. Předkládám čtenářům své pátrání po oné potřebné platné pomůcce pro hláskování.

Internet je silný pomocník, a tak jsem nabyl dojmu, že jsem velmi rychle našel to, co jsem hledal. Mezi desítkami odkazů byl i dokument „STATUT MĚSTSKÉ POLICIE VARNSDORF 2003“ [1]. Vzhledem k tomu, že mne zajímala nejen samotná tabulka, ale např. i správný způsob hláskování čísel, začal jsem pracovat s tímto dokumentem, protože se dalo očekávat, že obsahuje i konkrétní pokyny pro policisty ve službě.

Zpočátku se skutečně zdálo, že jsem našel to pravé. Příloha č. 9 odkazuje na „Hláskovací tabulku dle ČSN 01 1690“ [2].

	Znění české	Znění slovenské
A	Adam	Adam
B	Božena	Božena
C	Cyril	Cyril
Č	Čeněk	Čadca
D	David	Dávid
Ď	Ďumbier	Ďumbier
E	Emil	Emil
F	František	František
G	Gustav	Gustáv
H	Helena	Helena
CH	Chrudim	Chrudim
I	Ivan	Ivan
J	Josef	Jozef
K	Karel	Karol
L	Ludvík	Ludvík
Ľ	Ľubochňa	Ľubochňa
M	Marie	Mária
N	Norbert (Neruda)	Norbert (Neruda)
Ň	Nitra	Nitra
O	Otto (Otakar)	Oto
P	Petr	Peter
Q	Quido, vyslov kvído	Quido, vyslov kvído
R	Rudolf	Rudolf
Ř	Řehoř	Řehoř
S	Svatopluk	Svätopluk
Š	Šimon (Šárka)	Šimon

Navíc jsem ještě v odkaze našel postup ke sdělování čísel; zdálo se, že mám vše potřebné, co jsem hledal.

Postup sdělování čísel

Mezinárodní dohoda také stanovuje, jak sdělovat čísla. Všechna čísla s výjimkou celých set a tisíců a kombinací celých set a tisíců mají být sdělována po jednotlivých číslicích. Desetinná čárka se čte jako „čárka“.

Příklady: 300 = tři sta, 240 = dva čtyři nula, 3400 = tři tisíce čtyři sta, 12 400 = jedna dva tisíce čtyři sta, 127.3 = jedna dva sedm čárka tři.

Ve vnitrostátním užití používáme pro čísla běžné výrazy, počet set a tisíců uvádíme vždy (např. „dvě stě šedesát dva"). Desetinnou čárku a mezeru hlásíme také. Začíná-li číslo nulami, vyslovujeme každou nulu zvlášť. Detailní pravidla upravuje norma ČSN 01 1690 (011690).

Spíše ze zvědavosti než z důvodu kontroly jsem si ještě vyhledal odkazovanou normu a najednou jsem zjistil, že je to o něco složitější, než to zpočátku vypadalo. Tato norma je především pěkně letitá. Nahradila ČSN 01 1690 z června 1954 a začala platit 1. 1. 1957! Stojí 176,- Kč. Nemusíte si ji však hned kupovat, protože k prezenčnímu studiu si ji lze zapůjčit v Ústřední knihovně ČVUT v 5. NP Budovy NTK - sektor A. [3].

Norma platí pro hláskování písmen a číslic ve vnitrostátním telefonickém a radiotelefonickém styku. Lze ji použít i v jiných případech, kde je třeba zřetelně udat písmena a číslice. V normě jsou uvedeny hláskovací tabulky pro písmena a pro číslice v českém a slovenském znění a v dodatku hláskovací tabulky užívané v mezinárodním telefonním styku a mezinárodní letecké tabulky [4].

Jenže najednou jsem narazil na velmi zvláštní a důležitou informaci, **norma totiž byla zrušena k 1. 10. 2000 a to bez přímé náhrady**! Znamená to tedy, že nemáme žádný platný standard pro hláskování? Řekl jsem si, pravděpodobně asi ano - nemáme, proč by jinak pokyny pro městskou policii (a mnohé další dokumenty, které jsem na Internetu našel) odkazovaly na tento zrušený standard?

Znovu nastalo hledání a za chvíli se zdálo, že mám odpověď. V roce 2000, kdy byla norma ČSN 01 1690 zrušena, byla přijata ***Vyhláška Ministerstva dopravy a spojů č.200/2000 Sb***. (ze dne 30. června 2000) ***o způsobu tvorby volacích značek, jejich používání a o druzích radiokomunikačních služeb, pro které jsou vyžadovány*** [5]**.** Jedná se o prováděcí vyhlášku k **Zákonu č. 151/2000 Sb. O telekomunikacích** [6]. Příloha k této vyhlášce obsahuje hláskovací tabulku v českém a anglickém jazyce. Kontrolou s tabulkou uvedenou v ČSN 01 1690 zjistíte, že česká verze hláskování je téměř shodná s hláskovací tabulkou v uvedené normě. Jsou zde pouze drobné výjimky, např. pro Ď se místo Ďumbier zavádí české slovo Ďáblice, jsou vypuštěny zdvojené možnosti hláskování pro N Norbert/Neruda – nyní jen Norbert, totéž pro Š Šimon/Šárka – nyní jen Šimon apod. Zajímavé je, že tabulka obsahuje slovo pro hláskování Ľ a to Ľubochňa, i když v češtině měkké L neexistuje.

Příloha k vyhlášce č. 200/2000 Sb.
Hláskovací tabulka

Písmeno	Česky	Anglicky [výslovnost]
A	Adam	Alpha [alfa]
B	Božena	Bravo [brávou]
C	Cyril	Charlie [čárli]
Č	Čeněk	-
D	David	Delta
Ď	Ďáblice	-
E	Emil	Echo [ekou]

F	František	Foxtrot
G	Gustav	Golf
H	Helena	Hotel [houtel]
CH	Chrudim	-
I	Ivan	India [indja]
J	Josef	Juliett [džúljet]
K	Karel	Kilo [kílou]
L	Ludvík	Lima
Ľ	Ľubochňa	-
M	Marie	Mike [majk]
N	Norbert	November [novembr]
Ň	Nina	-
O	Oto (Otakar)	Oscar [oskr]
P	Petr	Papa [papá]
Q	Quido [vysl. Kvído]	Quebec [kvíbek]
R	Rudolf	Romeo [roumiou]
Ř	Řehoř	-
S	Svatopluk	Sierra
Š	Šimon	-
T	Tomáš	Tango [tengou]
Ť	Těšnov	-
U	Urban	Uniform [júnyfórm]
V	Václav	Victor [vyktr]
W	Dvojité V	Whisky [visky]
X	Xaver	X-Ray [eksrej]
Y	Ypsilon	Yankee [jenky]
Z	Zuzana	Zulu [zúlú]
Ž	Žofie	-

Ale ani tato verze tabulky není aktuální. Další změna nastala v roce 2005.

V tomto roce byl přijat ***Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů*** [7], který transponuje platný regulační rámec Evropské unie a který nahradil zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů. Zákon 127/2005 v § 151 ruší výše uvedenou vyhlášku 200/2000 Sb., která má ve své příloze hláskovací tabulku.

O oficiální hláskovací tabulku jsme zrušením vyhlášky 200/2000 nepřišli, neboť je nově obsažena přímo v prováděcí vyhlášce k výše uvedenému zákonu a to konkrétně ve ***Vyhlášce 155/2005 Sb. ze dne 19. dubna 2005 o způsobu tvorby volacích značek, identifikačních čísel a kódů, jejich používání a o druzích radiokomunikačních služeb, pro které jsou vyžadovány*** [8] .

Zde uvedené hláskovací tabulky v českém a anglickém jazyce jsou shodné s verzí uvedenou v příloze k vyhlášce č. 200/2000 Sb. Liší se jen v tom, že je vypuštěno „nečeské“ písmeno Ľ a hláskovací ekvivalent Ľubochňa.

Písmeno	Česky	Anglicky [výslovnost]	Písmeno	Česky	Anglicky [výslovnost]
A	Adam	Alpha [alfa]	Ň	Nina	-
B	Božena	Bravo [brávou]	O	Oto (Otakar)	Oscar [oskr]
C	Cyril	Charlie [čárli]	P	Petr	Papa [papá]
Č	Čeněk	-	Q	Quido [vysl. Kvído]	Quebec [kvíbek]
D	David	Delta	R	Rudolf	Romeo [roumiou]
Ď	Ďáblice	-	Ř	Řehoř	-
E	Emil	Echo [ekou]	S	Svatopluk	Sierra
F	František	Foxtrot	Š	Šimon	-
G	Gustav	Golf	T	Tomáš	Tango [tengou]
H	Helena	Hotel [houtel]	Ť	Těšnov	-
CH	Chrudim	-	U	Urban	Uniform [júnyfórm]
I	Ivan	India [indja]	V	Václav	Victor [vyktr]
J	Josef	Juliett [džúljet]	W	Dvojité V	Whisky [visky]
K	Karel	Kilo [kílou]	X	Xaver	X-Ray [eksrej]
L	Ludvík	Lima	Y	Ypsilon	Yankee [jenky]
M	Marie	Mike [majk]	Z	Zuzana	Zulu [zúlú]
N	Norbert	November [novembr]	Ž	Žofie	-

Jsme u konce. Zjistil jsem, že aktuálně platná a tedy ta „správná“ hláskovací tabulka je uvedena ve vyhlášce 155/2005 Sb.

Nyní si můžete ověřit, že v úvodu tohoto článku je správně hláskováno slovo Crypto-World, a to jak podle platné české, tak podle anglické hláskovací tabulky.

Literatura:

[1] STATUT MĚSTSKÉ POLICIE VARNSDORF http://www.varnsdorf.cz/files/status-mp.pdf
[2] ČSN 01 1690 Hláskovací tabulky http://nahledy.normy.biz/n.php?i=37
[3] ČSN 01 1690 http://as.ntkcz.cz/stm/el_cas.normy_package.informace?norma=1142
[4] ČSN 01 1690 Hláskovací tabulky http://shop.normy.biz/d.php?k=37
[5] Vyhláška Ministerstva dopravy a spojů č.200/2000 Sb. ze dne 30. června 2000 o způsobu tvorby volacích značek, jejich používání a o druzích radiokomunikačních služeb, pro které jsou vyžadovány
http://www.sagit.cz/pages/sbirkatxt.asp?cd=76&typ=r&zdroj=sb00200
[6] Zákon č. 151/2000 Sb., o telekomunikacích
http://aplikace.mvcr.cz/archiv2008/micr/files/390/telekomunikacni_zak._151.pdf
[7] Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů http://portal.gov.cz/zakon/127/2005
[8] Vyhlášce 155/2005 Sb. ze dne 19. dubna 2005 o způsobu tvorby volacích značek, identifikačních čísel a kódů, jejich používání a o druzích radiokomunikačních služeb, pro které jsou vyžadovány
http://www.portal.gov.cz/wps/portal/_s.155/696/_s.155/701?b=155/2005

D. Chcete si zaluštit? Díl 6.

Martin Kolařík (marram.mail@gmail.com)

Červnová dávka luštění

Tento měsíc se podíváme za keškami do Brna. Je jich tam ohromná spousta, takže vybrat tři hezčí nebylo vůbec lehké, ale některé opravdu povedené jsem zde uvedl již v minulých dílech, takže Brno nebude odbyto jen třemi kousky. Mimoto jsou všechny tři z různých sérií, takže si můžete dohledat jejich „sestřičky“, bohužel poslední je již archivovaná, to znamená, že již není keš fyzicky na místě, ale není problém si i tak zaluštit, mě řešení pobavilo. :)

BB# 1/Brnenské budovy/ aneb... (http://coord.info/GC158JP)

Project Enigma: ASCII (http://coord.info/GC239DX)

Cryptic coordinates III (http://coord.info/GC1QMKH)

Přeji úspěšné luštění a šťastný lov.

Martin

E. Bezpečnostní střípky

Jaroslav Pinkava, jaroslav.pinkava@gmail.com

*Jako připomínku toho, že **Crypto-World** není jen elektronický časopis, který vydáváme 1x měsíčně (s výjimkou léta, kdy vychází na přelomu července a srpna letní dvojčíslo 7-8) a není to také jen podzimní soutěž v luštění a není to jen denní přehled NEWS z oblasti kryptologie a informační bezpečnosti na našem webu, který je díky neúnavné práci J.Pinkavy průběžně rozšiřován o odkazy na nejdůležitější události, přikládám do tohoto čísla ukázku ze seriálu **Bezpečnostní střípky**. Tento seriál sestavuje každý týden na základě nejdůležitějších událostí zachycených v NEWS J.Pinkava a publikuje jej na webu root.cz. Zájemci najdou na tomto webu všechna čísla seriálu http://www.root.cz/serialy/bezpecnostni-stripky/ .*
Využívám této příležitosti a děkuji za celou redakci J.Pinkavovi za mravenčí a dlouhodobou práci při vyhledávání a zpracování těchto informací.
Na ukázku a jako upoutávku na tento zajímavý seriál předkládám s laskavým svolením autora a vedení redakce root.cz poslední vyšlé pokračování v plném znění.

P.Vondruška

Jaroslav Pinkava

Bezpečnostní střípky: Amerika pátrá po ukradených tajných telegramech

Pravidelný pondělní přehled informací vztahujících se k problematice bezpečnosti IT. Z novinek právě uplynulého týdne lze upozornit na informaci o tom, jak si můžete zkontrolovat své bezpečnostní nastavení na Facebooku, opravu kritické chyby v Adobe Flash a přehled záchranných CD pro boj s malware.

Konference a přehledy

Ninth Workshop on Economics and Information Security, diskuzi k této akci, která se v minulých dnech uskutečnila v Harvardu, si můžete přečíst na Schneierově blogu http://www.schneier.com/blog/archives/2010/06/ninth_workshop.html.
Jednotlivá vystoupení (články) jsou k dispozici na této stránce: Program http://weis2010.econinfosec.org/program.html

Program konference RECON 2010, která se koná 10–11. července v Montrealu (Kanada), najdete na stránce Speakers http://recon.cx/2010/speakers.html. Připojeny jsou krátké anotace jednotlivých vystoupení.

Obecná a firemní bezpečnost IT

Každý desátý IT profesionál podvádí při auditu IT – 1 in 10 IT pros cheat on an IT audit http://www.net-security.org/secworld.php?id=9378. K tomu výsledku dospěly závěry rozboru, který provedla společnost Tufin Technologies. S kompletními statistikami rozboru se lze seznámit na této stránce – InfoSecurity UK 2010 Firewall Management Survey Results http://www.tufin.com/downloads/infosecurity_uk_2010_survey_results.pdf .

Do vězení půjde analytik americké vojenské zpravodajské služby – U.S. Intelligence Analyst Arrested in Wikileaks Video Probe http://www.wired.com/threatlevel/2010/06/leak/. Dvaadvacetiletý SPC Bradley Manning byl zatčen nedaleko od Bagdadu. Za úplatu předal hackerovi video s helikoptérou, která měla zaútočit v Bagdadu a zabít i nevinné civilisty.

Další podrobnosti jsou také v článku – Hacker turns in soldier in Iraq airstrike video leak http://news.cnet.com/8301-27080_3-20007024-245.html. Zadržený navíc tvrdí, že Wikileaks předal 260 000 utajovaných diplomatických depeší. Pokud Wikileaks má tyto dokumenty a zveřejní je, povede to k dosud nevídané kompromitaci americké zahraniční politiky a národní bezpečnosti USA – State Department Anxious About Possible Leak of Cables to Wikileaks http://www.wired.com/threatlevel/2010/06/state-department-anxious/ .

Čína hájí své právo na cenzuru internetu – China defends internet censorship http://news.bbc.co.uk/2/hi/americas/8727647.stm. Byl k tomu tamní vládou vydán speciální dokument. Článek rozebírá jeho obsah.

Socializing safely via the Internet aneb rodina na internetu, Mich Kabay v článku shrnuje své úvahy http://www.networkworld.com/newsletters/sec/2010/060710sec2.html, které směřují na tyto aspekty bezpečnosti. Nepřehlédněte také odkazy v závěru článku, např.: A Parent´s Guide to Internet Safety http://www.fbi.gov/publications/pguide/pguidee.htm.

Největší obavy ve vztahu k národní bezpečnosti USA jsou z možných kybernetických útoků – Cyberattacks are biggest fear, survey shows http://gcn.com/articles/2010/06/10/cybersecurity-biggest-risk.aspx. Vyplývá to z přehledu, na kterém se podílelo 250 IT profesionálů (březen 2010). Kompletní výsledky přehledu jsou zde: Single Point of Security Coordination Drives Accountability/Risk Mitigation. Survey Finds Cyberattacks and Cybersecurity to Be Top Security Priorities http://www.usis.com/documents/GovSec%20Survey%20WP%20052510P.pdf

FBI vyšetřuje únik e-mailů z iPad – FBI investigating iPad e-mail leaks http://www.computerworld.com/s/article/9177961/FBI_investigating_iPad_e_mail_leaks?source=rss_security . Mělo uniknout 114 000 adres uživatelů iPad. Není zatím jasné, zda a jaké byly porušeny zákony. Další komentář k tomu najdete na stránce – Exposed Apple´s Worst Security Breach: 114,000 iPad Owners http://gawker.com/5559346/ .

Techniky sociálního inženýrství: 4 cesty, kterými se kriminální strana dostává dovnitř, vyjmenovává Joan Goodchild http://www.csoonline.com/article/596512/social-engineering-techniques-4-ways-criminal-outsiders-get-inside :

- Alternativní komunikační kanály
- Zprávy osobního charakteru
- Apelace na sociální cítění
- Spolehnutí se na bezpečnostní mechanizmy nemusí také vždy fungovat

Sociální sítě

Rychlá kontrola bezpečnosti Facebooku http://jnp.zive.cz/rychla-kontrola-bezpecnosti-facebooku, autorem tohoto článku je Ondřej Bitto: Nejste si jisti, jestli sociální síť sítí používáte opravdu bezpečně a zda zbytečně nevyzrazujete příliš ze svého soukromí? Poradíme vám, jak si zabezpečení zkontrolovat s ReclaimPrivacy.org.

O Facebooku vyšla kniha – Book about Facebook's beginnings may dim spotlight on privacy http://www.computerworld.com/s/article/9177836/Book_about_Facebook_s_beginnings_may_dim_spotlight_on_privacy?taxonomyId=17 . Jejím autorem je novinář David Kirkpatrick. Jeho kniha The Facebook Effect http://books.simonandschuster.com/Facebook-Effect/David-Kirkpatrick/9781439102114 popisuje historii Facebooku a zabývá se také Markem Zuckerbergem (CEO Facebooku).

Jaká jsou hlavní rizika sociálních médií pro podnikání? Sharon Gaudin v článku Group lists top five social media risks for businesses http://www.computerworld.com/s/article/9177786/Group_lists_top_five_social_media_risks_for_businesses?taxonomyId=17 komentuje studii, kterou vydala ISACA – Social Media: Business Benefits and Security, Governance and Assurance Perspectives http://www.isaca.org/Knowledge-Center/Research/Documents/Social-Media-Wh-Paper-26-May10-Research.pdf . Viz také další komentář – Advisory body names top five social media business risks http://www.computing.co.uk/computing/news/2264444/isaca-names-top-five-social .

Nové hrozby na sociálních sítích podle AVG http://digitalne.centrum.cz/nove-hrozby-na-socialnich-sitich-podle-avg/ , David Silmen: Společnost AVG vydala zprávu o nové hrozbě, která se šíří skrz sociální sítě. Jedná se o takzvaný „hackaktivismus“, kdy dochází využití digitálních nástrojů k dosažení politických cílů.

Jak vytvářet politiky ve vztahu k sociálním médiím? Mike Hrabik v článku Crafting a social media policy poukazuje na nezbytnost takovéto politiky v organizacích a rozebírá její hlavní součástihttp://www.computerworld.com/s/article/9177946/Crafting_a_social_media_policy?source=rss_security . Za zmínku stojí také odkaz na starší slideshow 12 tips for safe social networking http://www.networkworld.com/slideshows/2008/101308-12-tips-social-net.html .

Software

Adobe Flash – útočníci zneužívají kritickou chybu – Update: Attackers exploit critical bug in Adobe's Flash, Reader http://www.computerworld.com/s/article/9177705/Update_Attackers_exploit_critical_bug_in_Adobe_s_Flash_Reader?source=rss_security . Tato chyba je i v nejnovější verzi Flash Playeru – 10.0.45.2 (ve verzích pro Windows, Macintosh, Linux a Solaris). Zranitelné jsou i Acrobat reader 9.x a Adobe Acrobat 9.x (Windows, Macintosh a Unix). Útočníci využitím této chyby mohou získat kontrolu nad počítačem.

Adobe si proto tentokráte pospíšil a vydal novou verzi Flash Playeru 10.1 – Adobe Flash Update Plugs 32 Security Holes http://krebsonsecurity.com/2010/06/adobe-flash-update-plugs-32-security-holes/ . V článku Brian Krebs komentuje toto vydání a ukazuje odkazy, kde si můžete zjistit, jakou verzi vlastně máte a odkud si můžete novou verzi stáhnout.

Poet, to je nástroj využívající slabiny webových stránek. Dan Goodin na stránce Researchers release point-and-click website exploitation tool. ‚Tons‘ of vulnerable sites http://www.theregister.co.uk/2010/06/08/padding_oracle_attack_tool/ popisuje vlastnosti tohoto nástoje, který byl tento týden zpřístupněn veřejnosti – Padding Oracle Exploit Tool http://netifera.com/research/ . Viz také – Tool for cracking encrypted session data http://www.h-online.com/security/news/item/Tool-for-cracking-encrypted-session-data-1017626.html.

Je Open Source SW bezpečný? Tradiční otázka, tentokrát odpověď na ní hledá ve svém článku Lincoln Spector. Takové programy jako Password Safe a TrueCrypt by za jiné nevyměnil – Is Open Source Safe? http://www.computerworld.com/s/article/9177760/Is_Open_Source_Safe_?source=rss_security .

Jedna třetina výsledků vyhledávačů je otrávená. Na základě analýzy svých odborníků přichází s touto informací Symantec. Jeho pracovníci dva týdny zkoumali horní stovku výsledků vyhledávání pro 300 populárních objektů – One third of search engine results are poisoned http://www.networkworld.com/news/2010/060710-one-third-of-search-engine.html?hpg1=bn .

Jak se v podniku chránit před pdf útoky? Michael Cobb v článku Enterprise PDF attack prevention best practices přichází se sadou doporučení http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1513908,00.html?track=NL-422&ad=769730&asrc=EM_NLT_11739032&uid=4169286 .
Jsou zde také uvedeny některé další související odkazy.

Google zaplatilo 2 000 dolarů za oznámenou chybu v Google Chrome – Google pays $2,000 for report of a vulnerability in Chrome. Tuto sumu obdržel Sergey Glazunov. http://www.h-online.com/security/news/item/Google-pays-2-000-for-report-of-a-vulnerability-in-Chrome-1018495.html .

Analytik společnosti Google dává Microsoftu 5 dní na opravu kritické chyby ve Windows XP – Google researcher gives Microsoft 5 days to fix XP zero-day bug http://www.computerworld.com/s/article/9177948/Google_researcher_gives_Microsoft_5_days_to_fix_XP_zero_day_bug?source=rss_security . Po pěti dnech, kdy informaci odeslal Microsoftu, zveřejnil kód programu, který umožňuje útok zneužitím této zranitelnosti. Podle komentáře to svědčí o narůstající válce obou společností.

Windows Help lze zneužít k útoku – Windows Help used as attack surface http://www.h-online.com/security/news/item/Windows-Help-used-as-attack-surface-1019381.html . Na chybu v Microsoft's Help and Support Center přišel Tavis Ormandy.

Malware

Záchranná CD pro boj s malware, informaci k nim najdete na stránce Rescue CDs: Tips for fighting malware http://blogs.techrepublic.com.com/security/?p=3803 . Michael Kassner připravil přehled takovýchto nástrojů a vysvětluje jejich vlastnosti a co tato CD umožňují.

Trojan Zeus zahájil další svoji kampaň – ZeuS Trojan Attack Spoofs IRS, Twitter, Youtube http://krebsonsecurity.com/2010/06/zeus-trojan-attack-spoofs-irs-twitter-youtube/ . Podvržené maily s označením Notice of Underreported Income upozorňují jakoby na chyby v daňovém přiznání (USA) a nutí adresáta kliknout na odkaz s jejich přiznáním. Ve skutečnosti ovšem se jedná o útok, který se pokouší zjistit hesla uživatele.

Viry

Týždeň staré antivírusy detekujú maximálne 63% nového malwaru http://www.dsl.sk/article.php?article=9285 , z úvodu: Najlepšími antivírusmi v detekcii nového škodlivého kódu, ktorého detekciu tvorcovia antivírusov ešte nezahrnuli do definičných databáz, sú v súčasnosti antivírusy Trustport a Panda (jedná se o výsledky testu AV-Comparatives).

Hackeři

Odbor města New York pro výchovu byl podvodem hackery obrán o 644 000 dolarů – Crooks siphon $644,000 from school district's bank account. Napaden byl jeho bankovní účet a trvalo tři roky než si toho někdo všiml.
http://www.theregister.co.uk/2010/06/07/electronic_account_raided/ .

Varování před počítačovým útokem ze Severní Koreje zaznělo v Seoulu z úst korejského ministra obrany, a to v souvislosti s přípravou summitu G-20, který se zde má konat v listopadu – Military leaders warn of NK cyber attack

http://www.koreatimes.co.kr/www/news/nation/2010/06/113_67314.html .

Hackeři infikovali stránky novin Jerusalem Post – Hackers plant malware on Jerusalem Post website http://www.theregister.co.uk/2010/06/08/jerusalem_post_malware/ . Podle firmy Sophos to však nemělo politické pozadí.

Dále – hromadný útok na tisíce webů byl podniknut v uplynulých dnech, pomocí SQL injection bylo napadeno statisíce webů – Mass hack plants malware on thousands of webpages http://www.theregister.co.uk/2010/06/09/mass_webpage_attack/ . Viz také komentář – Mass Web attack hits Wall Street Journal, Jerusalem Post http://www.computerworld.com/s/article/9177904/Mass_Web_attack_hits_Wall_Street_Journal_Jerusalem_Post?taxonomyId=17 .

Esej Bruce Schneiera na téma najímání hackerů je součástí diskuze na jeho blogu – Hiring Hackers http://www.schneier.com/blog/archives/2010/06/hiring_hackers.html . Párovou (pohled z druhé strany) esej připravil Marcus Ranum, obě eseje najdete na stránce Weighing the risk of hiring hackers
http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1514250,00.html

Hardware

S fotoaparátem Olympus Stylus Tough 6010 přibalí i červa – Hardware: Olympus Digital Camera Ships With a Worm http://hardware.slashdot.org/story/10/06/09/007203/Olympus-Digital-Camera-Ships-With-a- . Je na vnitřní paměťové kartě. Prodáno snad mělo být asi 1700 takových fotoaparátů. Takovéto jevy se stávají stále častěji a proto doporučení: na svém počítači mějte zakázáno spuštění Autorun a oskenujte nejprve libovolné takové zařízení před jeho připojením k PC.

Bezpečnostní rizika USB flash disků rozebírá Richard W. Walker – Making USB thumb drives secure enough for government work
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1514379,00.html?track=NL-1626&ad=770406&asrc=EM_NLN_11750547&uid=4169286 . Poukazuje na jedné straně na užitečnost těchto malých médií pro uchování a přenos dat a na druhé straně na rizika s nimi spojená. Vysvětluje, že existují rozdíly v zabezpečení těchto flash disků podle typu a výrobce.

Bezdrát

Společnost Google sběrem dat z bezdrátu pravděpodobně porušila i americké zákony – Former Prosecutor: Google Wi-Fi Snafu 'Likely' Illegal. Bývalý žalobce Paul Ohm upřesňuje, v čem podle jeho názoru byly zákony porušeny.
http://www.wired.com/threatlevel/2010/06/google-wifi-debacle/ .

Mobilní telefony a zařízení

Temná stránka mobilních aplikací http://digitalne.centrum.cz/temna-stranka-mobilnich-aplikaci/, článek Davida Silmena vychází z materiálu na stránce Dark Side Arises for Phone Apps http://online.wsj.com/article/SB10001424052748703340904575284532175834088.html.
Množství aplikací pro chytré mobilní telefony narůstá obrovským tempem. Roste tím však i potenciální nebezpečí, které se v některé z nich může skrývat. Příklad najdete v článku Hackers plant virus in smartphone games http://www.brisbanetimes.com.au/digital-life/mobiles/hackers-plant-virus-in-smartphone-games-20100607-xp59.html (hry 3D Anti-Terrorist a PDA Poker Art) .

Jaké jsou výhledy ohledně hrozeb pro chytré mobily? Chad Perrin se v What are the prospects for smartphone security threats? zamýšlí nad možným vývojem. http://blogs.techrepublic.com.com/security/?p=3752&tag=leftCol;post-3752. Podle autora jsou s těmito mobily spojena dvě základní nebezpečí. Jedno spočívá v možnosti (jednodušší než u počítačů) jeho krádeže, druhé pak při jeho používání pro bankovní transakce. Samozřejmě tato zařízení budou do budoucna v rostoucí míře předmětem útoků různých typů malware, mohou se stát i součástí botnetů.

Bezpečnost mobilních telefonů – co lze a co nelze ve vztahu k bezpečnosti, k této otázce dává Bill Brenner ve svém článku na csoonline.com dohromady vyjádření celé řady odborníků – Mobile phone security dos and don'ts http://www.csoonline.com/article/596163/mobile-phone-security-dos-and-don-ts .

Spam

Objevil se falešný e-mail o deaktivaci účtu Facebooku – Fake Facebook account deactivation email http://www.net-security.org/secworld.php?id=9375 . Naštěstí kliknutí na odkaz „Sing In" v e-mailu oběť přivede jen na stránky kanadské farmaceutické firmy. Viz také – Malicious tweets keep coming and changing http://www.net-security.org/malware_news.php?id=1369 (co vše se na Facebooku urodilo, aby mohlo škodit).

Elektronické bankovnictví

Aktualitu na téma bankomatové podvody najdete na stránce Skimming from the sofa http://www.h-online.com/security/news/item/Skimming-from-the-sofa-1016534.html .
Autor krátkého článku komentuje současnou situaci, přidává některé odkazy.

Pracovník Bank of America se přiznal, ukradl chráněná data zákazníků – Bank of America insider admits he stole sensitive customer data
http://www.theregister.co.uk/2010/06/08/bank_insider_data_theft/ . Brian Matty Hagen se je pak pokoušel prodat – bohužel pro něho agentům FBI.

Finanční instituce investují nyní podstatně více do bezpečnosti – Financial institutions increase security spending, as threats and regulatory penalties rise http://www.scmagazineuk.com/financial-institutions-increase-security-spending-as-threats-and-regulatory-penalties-rise/article/171986/. Vede je k tomu pochopitelně narůstající množství různorodých hrozeb.

Autentizace, hesla

Proč DRM Ubisoftu fungovalo? Autor článku Devil's Advocate: Why Ubisoft's DRM worked http://games.on.net/article/9147/Devils_Advocate_Why_Ubisofts_DRM_worked říká, je jedno, jak tuto jejich novou ochranu autorských práv nesnášíte, ona prostě zafungovala.

Špatné praktiky pro práci s hesly znehodnocují bezpečnost jako celek – Researchers: Poor password practices hurt security for all
http://www.computerworld.com/s/article/9177780/Researchers_Poor_password_practices_hurt_security_for_all?taxonomyId=17 . Elizabeth Heichler komentuje studii dvou odborníků z univerzity v Cambridgi (Anglie). Joseph Bonneau a Soren Preibusch ji prezentovali na akci Workshop on the Economics of Information Security (Cambridge, Mass.).

Normy a normativní dokumenty

Americký NIST v uplynulém týdnu vydal dokument:
Special Publication 800–34, Revision 1, Contingency Planning Guide for Federal Information Systems. SP 800–34 Revision 1 http://csrc.ncsl.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf

Kryptografie

Byly zahájeny práce na projektu pro digitalizaci zpráv ze 2. světové války, které byly šifrovány Enigmou – Archive project will digitize WWII Enigma messages http://www.computerworld.com/s/article/9177759/Archive_project_will_digitize_WWII_Enigma_messages?taxonomyId=17 . Realizaci celé rozsáhlé akce napomáhají sponzoři. Viz také diskuzi na Schneierově blogu – Bletchley Park Archives to Go Online http://www.schneier.com/blog/archives/2010/06/bletchley_park_1.html .

Zemřel Sir Peter Baldwin (87 let), za války pomáhal rozbíjet japonské šifry. Článek Sir Peter Baldwin obituary http://www.guardian.co.uk/politics/2010/jun/08/sir-peter-baldwin-obituary je věnován jeho památce.

Zveme na večer s šifrou do Science Cafe Poděbrady
http://www.facebook.com/pages/Science-Cafe-Podebrady/402349520184 .
Téma: Od jednoduché záměny po absolutně bezpečnou šifru
Přednáší a diskutuje: kryptolog Pavel Vondruška
Datum: 17. červen 2010
Čas: 19:30 – 21:00
Lokalita: Hotel BELLEVUE Poděbrady

Různé

Přehled vychází z průběžně publikovaných novinek na Crypto – News http://crypto-world.info/news/index.php .

F. O čem jsme psali v červnu 2000 – 2009

Crypto-World 6/2000

Příloha : Navajo Code Talkers, revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 6/2001

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

Crypto-World 6/2002

Crypto-World 6/2003

Crypto-World 6/2004

Crypto-World 6/2005

Crypto-World 6/2006

Crypto-World 6/2007

Příloha: Mikulášská kryptobesídka (6.-7.12.2007)- MKB2007_CallForPapers_cerven.pdf

Crypto-World 6/2008

Crypto-World 6/2009

Příloha: javascript-priloha.pdf (179 kB)
javascript-priloha_1_3.rtf (64 kB)

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/