Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 8, číslo 2/2006 **15. únor 2006**

2/2006

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1080 registrovaných odběratelů)

Obsah : str.

A. Statistika vydaných elektronických podpisů ….

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

Koncem ledna jsem zachytil upoutávku, že Ministerstvo informatiky ČR sestavilo a zveřejnilo na své stránce materiál nazvaný **„Statistika vydaných elektronických podpisů v roce 2005“.**

Označení statistiky mne zaujalo – ihned mne napadla fascinující myšlenka - Ministerstvo informatiky změnilo svoji gesci a náplň její práce se začala podobat dohledu Ministerstva informací z Gilliamova skvělého filmu Brazil, resp. Ministerstva pravdy ze známé Orwellovy knihy 1984! Jak jinak by dokázalo naše ministerstvo sestavit statistiku, **kolikrát se kdo v této zemi elektronicky podepsal?**

Originální zpráva z 20.1.2006 (http://www.micr.cz/scripsts/detail.php?id=3051)

Statistika vydaných elektronických podpisů v roce 2005

V rámci sledování vývoje využívání informačních a komunikačních technologií (ICT) v ČR a v zahraničí, uveřejňuje Ministerstvo informatiky na svých internetových stránkách statistiky v této oblasti.

Nově můžete nalézt v rubrice statistiky vývoj vydaných elektronických podpisů. V roce 2005 bylo celkem vydáno 12 941 kvalifikovaných certifikátů, 167 002 komerčních certifikátů a 980 473 časových razítek od třech akreditovaných poskytovatelů certifikačních služeb - První certifikační autorita, a.s., Česká pošta, s.p. – PostSignumQCA a eIdentity, a.s. podle zákona č. 227/2000 Sb., O elektronickém podpisu.

Ze zprávy vyplynulo, že gesce Ministerstva informatiky se samozřejmě nezměnila, jen se autor statistiky nevhodně vyjádřil. Zaměňuje totiž vydání elektronického podpisu s vydáním certifikátu. Tedy nešvar, který v českých médiích zcela zakořenil a již od schválení zákona o elektronickém podpisu proti němu vedu (a nejen já) Don Quijotský boj …

Viz např. můj článek *Kde si mohu koupit svůj elektronický podpis?*, Crypto-World 10/2000, kde hned v úvodním odstavci píši :

Jde o to, aby větu z nadpisu: "Kde si mohu koupit elektronický podpis?" čtenář nikdy sám nevyslovil a pokud ji od někoho uslyší nebo si ji někde přečte (což je bohužel v současných novinách zcela běžné), aby věděl, že je "nesmyslná".

http://crypto-world.info/casop2/crypto10_00.pdf.

Víme tedy, o čem statistika je, a dále, že její název je - diplomaticky řečeno - nepřesný. Nyní přejdeme k její informační hodnotě. Zde uvedený nárůst vydaných kvalifikovaných a tzv. komerčních certifikátů totiž příliš nevypovídá o tom, co je pro praxi nejdůležitější – tj. o počtu osob, které v daném období vlastní platný kvalifikovaný či nekvalifikovaný certifikát (ve statistice nazýváno komerční certifikát) k ověření jím vytvářeného zaručeného elektronického podpisu. Statistika počtu aktuálních držitelů platných certifikátů se z publikovaných údajů odvodit nedá …

Své výhrady jsem zaslal v podobě dotazů a připomínek k vyjádření na MIČR dne 7.2.2006. Potvrzení o přijetí jsem obdržel z elektronické podatelny až po své urgenci 8.2.2006. Odpověď jsem dosud (tj. do konce příprav tohoto čísla e-zinu tj. 15.2) ještě neobdržel….

Část textu odeslaného e-mailu :

…

*K uvedené statistice mám několik **dotazů a připomínek.***

*a) zjevně se nejedná o statistiku **elektronických podpisů**, ale **vydaných certifikátů k ověřování těchto podpisů**. Elektronických podpisů samozřejmě může každý držitel certifikátu vytvořit libovolný počet a tedy jejich efektivní statistika není možná. Název je tedy zavádějící, matoucí a jedná se o hrubou chybu, která by mohla být při předání těchto dat např. do EU vnímána jako diletantismus.*

*b) Zajímala by mne použitá metodika výpočtu nárůstu vydaných kvalifikovaných certifikátů. Jsou odečítány **expirované certifikáty** (tj. ty, kterým již vypršela platnost) ? a dále **certifikáty, které byly zneplatněny vlastníkem** (tj. před vypršením platnosti)? Není přece důležité, kolik jich bylo vydáno, ale kolik je v daném okamžiku **platných kvalifikovaných certifikátů** - tj. kolik osob může pomocí zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu komunikovat...*

*Ještě přesněji - vhodná by byla **statistika počtu držitelů platných kvalifikovaných certifikátů**. Jedině tato statistika objektivně charakterizuje penetraci kvalifikovanými certifikáty v populaci a tedy kolik lidí takto může využívat komunikaci v oblasti veřejné moci (viz §11 zákona o el. podpisu).*

*c) Ke statistice tzv. komerčních certifikátů mám dotaz k použité metodice. **Od kterých certifikačních autorit máte údaje?***

Domnívám se, že vám chybí údaje od řady certifikačních autorit, které certifikáty vydávají, např. banky, spořitelny, Český Telecom, Zoner, ... I tyto autority vydávají certifikáty a z hlediska zákona o el. podpisu jsou jejich certifikáty zcela srovnatelné (zejména co do použití) s komerčními certifikáty vydávanými akreditovanými CA (jejich ***akreditace se vztahuje totiž POUZE na výdej a správu kvalifikovaných certifikátů****...).*
Připomínám i zde nutnost odečítat již neplatné certifikáty (propadlé a expirované).

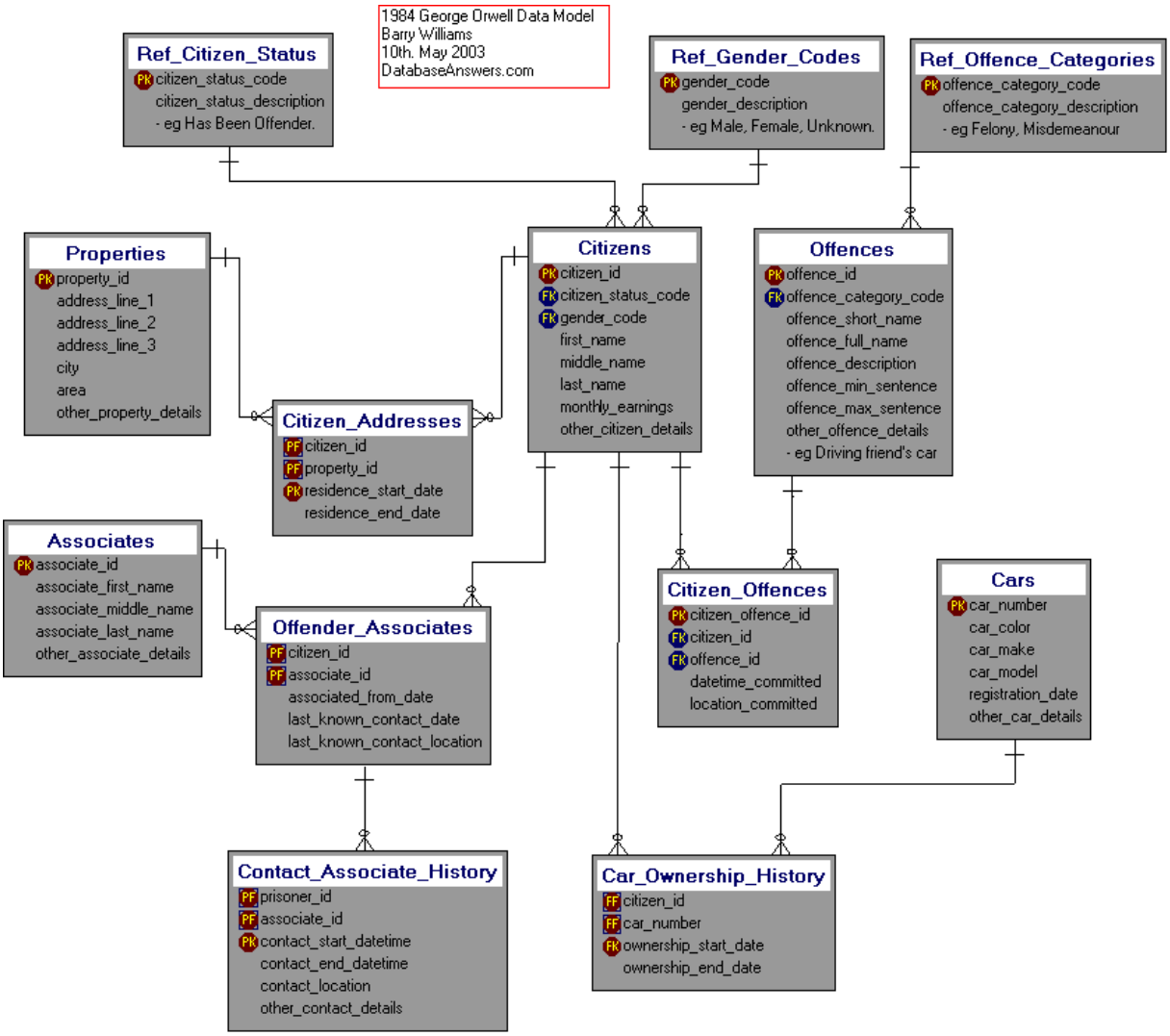
d) Příklady ...
Pokud nebudete odečítat propadlé certifikáty, dostanete časem zcela absurdní čísla ....
Např. v roce 2003 bude vydáno 100 000 certifikátů s platností 12 měsíců ....
v roce 2004 100 000 certifikátů z roku 2003 bude obnoveno a vydáno dalších 20 000 ...
v roce 2005 bude obnovena platnost 120 000 certifikátům z roku 2004 a vydáno dalších 30 000 ...
Podle jedné metodiky (počet uživatelů, kteří mají platný certifikát) je na konci roku 2005 150 000 uživatelů s certifikátem, podle druhé metodiky (vydané certifikáty bez odečtu propadlých ...) dostanu 380 000 vydaných certifikátů...
Tato čísla jsou zjevně v nepoměru a druhý údaj je z hlediska závěrů zkreslující.
Správný závěr je, že od roku 2003 do konce roku 2005 je přírůstek 50 000 nových držitelů certifikátů a nikoliv možný závěr, že od roku 2003 je již vydáno skoro 4x více certifikátů (tento závěr může být pro další úvahy zavádějící...).

Jako další příklad, tentokráte reálný, uvedu statistiku autority, za kterou odpovídám:
Držitelů osobních zaměstnaneckých certifikátů jsme na konci roku měli 2640, ale vydáno bylo v tomto roce 6560 certifikátů (nepoměr je dán vydáním následných certifikátů po vypršení platnosti stávajících, vydáním certifikátu po zneplatnění certifikátu žadatelem, vydáním certifikátů po různých technických problémech, dvojím klíčovým hospodářstvím (jeden certifikát určen pro ověření podpisu a druhý pro šifrování) atd.)
Vzhledem k tomu, že máme cca 7000 zaměstnanců, bych (v případě, že se budu dívat jen na počet vydaných certifikátů) mohl podlehnout mylnému dojmu, že skoro každý zaměstnanec již vlastní certifikát....

Důležité tedy není uvádět počet vydaných certifikátů, ale počet držitelů platného certifikátu.
…. konec citace ….

Závěr

Jedno ze tří ústředních hesel Orwellovy knihy 1984 zní: **Nevědomost je síla.**
Z tohoto důvodu nebylo vydávání objektivních statistik v tomto fiktivním státě dovoleno …



Obrázek „ A DATA MODEL FOR GEORGE ORWELL's 1984“ (podobnost s „elektronickým občanským průkazem“ je čistě náhodná ..), obrázek převzat z http://www.databaseanswers.org/

Ukázka z knihy George Orwella „1984“:

Tento proces neustálého pozměňování se používal nejen v novinách, ale i v knihách, časopisech, brožurách ... - v každém druhu literatury nebo dokumentace...

Ale vždyť to vlastně ani podvrh není, pomyslel si, když měnil cifry Ministerstva hojnosti. Jde jen o to nahradit jeden nesmysl jiným. Většina materiálu, s nímž člověk pracoval, se netýkala reálného světa ani tolik, jako se ho týká přímá lež. Statistické údaje byly pouhá fantazie v originální verzi stejně jako ve verzi opravené...

A ještě pravděpodobnější bylo, že nikdo nevěděl, kolik se vyrobilo, a ani se o to nezajímal. ... A tak tomu bylo se všemi zaznamenávanými údaji, ať šlo o věci velké či malé. Všechno se ztrácelo v jakémsi světě, v němž se nakonec i letopočet stával nejistým...

B. Kryptologie, šifrování a tajná písma

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

Vondruška, P.: Kryptologie, šifrování a tajná písma, nakladatelství Albatros, edice OKO, Praha, v tisku (říjen 2006),
odborný lektor : Vlastimil Klíma.

Ukázka z kapitoly *5. Důležitá data a mezníky v dějinách kryptologie*

1415

Pravděpodobně prvním dochovaným dokladem o používání šifer v Čechách jsou listy Mistra Jana Husa z Kostnice. Jeho šifrový systém byl velice jednoduchý, šifroval pouze samohlásky a to tak, že je nahradil písmenem, které jej v abecedě následuje. Místo A psal B, místo E napsal F atd. OKO, ALBATROS by zašifroval jako MKM, BLBBTRMS. Systém je z kryptologického hlediska velmi slabý a navíc nejednoznačný. Příjemce může mít v některých případech problém s dešifrováním, neboť nemusí být na první pohled zřejmé, které písmeno je v otevřeném tvaru (souhláska) a které je šifra (samohláska). Nejednoznačnosti mohou vzniknout především v krátkých textech.

1835

Používání slabé šifry k uchování osobního tajemství nám zanechalo i zajímavé svědectví ze života Karla Hynka Máchy (1810-1836). Máchův Deník z roku 1835 obsahoval i šifrované pasáže, které se podařilo rozluštit novináři a historikovi Jakubu Arbesovi v 80. letech 19. století. Vzhledem k jejich intimní povaze a s ohledem na budovaný kult Karla Hynka Máchy nebyly zahrnuty do žádného vydání Máchových spisů. Poprvé vyšly v 70. letech 20. století (česky jako bibliofilie v počtu 20 kusů, italsky v Benátkách). Oficiální úplné české vydání Deníku, včetně překladu zašifrovaných částí, pochází až z roku 1993.
Mácha použil jednoduchou záměnu, kdy šifrový text nejprve píše podle běžného zvyku zleva doprava, ale na konci řádku nepřejde na začátek nového řádku, ale píše zprava do leva – tj. jako když kůň oře pole.

1914-1918

Tajná komunikace české protirakouské politické opozice během první světové války je dobře vylíčena v knize Karla Čapka „Hovory s T.G.Masarykem“.

Prezident Tomáš Garrigue Masaryk v ní vzpomíná :
„Mnoho práce a starostí bylo s vypravováním poslů do Prahy. Nechtěl jsem užívat obvyklých a rakouským úřadům jistě známých prostředků, jako je zašít zprávy do límce nebo je vložit do podpatků a podobně. To byly někdy dost těžké technické problémy: například dát papírek pod regulátor rychlosti do hodinek; vhodně navrtat deštník, dát stočený dopis do plavajzu (zastaralý název pro tužku), ze kterého se musel šikovně odstranit kousek tuhy; ty kumšty prováděl hlavně inženýr Baráček. Jeden český stolař nám dělal kufry ne s dvojím dnem, ale s dvojitou stěnou; hlavní vtip byl, aby ta stěna při zaklepání nezněla dutě, ale aby zrovna zvonila - ten stolař to dovedl. Jindy jsme dali své zprávy do sudů s olejem, a to se zas musely nenápadně označit ty sudy.“
Pro psaní senzitivních zpráv mezi domácím a zahraničním odbojem se používal i neviditelný inkoust, který byl za I.světové války velmi rozšířen a s oblibou používán špióny na všech frontách. Konkrétně to bylo v korespondenci mezi pražským průmyslníkem J. J. Fričem a jeho obchodním zástupcem v Itálii a Švýcarsku Z. Rohlou.
Mimo těchto typických steganografických metod se používalo i šifrování. Svědectví o jeho použití se dochovalo v již zmíněné knize, kde prezident Masaryk uvádí, že inženýr Baráček v Ženevě pro účely odboje zkonstruoval dokonce šifrovací stroj.

1939

V předvečer obsazení Československa Německem odlétalo 14.3.1939 do Londýna v tajnosti letadlo, kde bylo vyčleněno 11 míst pro československé zpravodajské důstojníky. Do výběru se nedostal nikdo z tehdejších kryptologů a to ani vedoucí českých šifrérů - zkušený kryptolog Rohatý. Ten pouze stačil připravit popis doporučených šifrových systémů pro komunikaci s Londýnem a předat jej plukovníku Moravcovi, který odpovídal za vytvoření československé zpravodajské londýnské centrály. Moravec však zjistil, že navrženým postupům nerozumí, a tyto systémy proto nebyly použity. Důsledkem tohoto jeho rozhodnutí pak bylo použití slabých šifer a řada dalších osudových chyb naší centrály.

1941

V Londýně nebyl v době války k dispozici žádný český kryptolog, a proto depeše mezi centrálou a českým odbojem trpěly řadou základních chyb. To bohužel mělo za následek i to, že pravděpodobně byly některé odbojové skupiny odhaleny na základě analýzy dešifrované komunikace.

Jako příklad chyb, kterých se centrála dopouštěla, si uvedeme ukázku textu depeše odeslané 24.6.1941 z Londýna do Prahy.

DOM. Pro tajné depeše navrhuji jiný šifrovací způsob. Pod zašifrovací heslo se píší místo písmen a jiných znaků už jejich šifry a to do každého čtverečku jedna číslice. Počet čtverečků pod heslem musí být dělitelný pěti. Není-li, přidá se v poslední řádce tolik nul, aby se dosáhlo nejbližšího tohoto čísla. Ze zašifrovacího obrazce se pak čtou sloupce s čísly svisle podle číselného pořadí hesla a píší se vodorovně pod zašifrovací heslo. Zde se opět čtou svisle ve sloupcích podle číselného pořadí hesla a tvoří se pětimístné šifrové skupiny. Způsob je naprosto jistý, protože šifrové dvojice jsou transpozicí rozlomeny. Není však to rychlé jako způsob dosud používaný. Pro tento šifrovací způsob platná jen jedna jediná abeceda a to pro prvý den v měsíci. Dá se tedy naučit nazpaměť. Sdělte mi váš názor. Dík. SUDAR.

V české centrále se dopustili hned dvou velkých chyb:

1) předpokládali, že navržený kombinovaný šifrový systém STT – substituce a úplná dvojitá transpozice - je bezpečný („jistý“), přestože způsob luštění systému byl již na začátku třicátých let popsán v dostupné kryptologické literatuře,
2) domluva na šifrovém systému touto cestou je klasické porušení základních pravidel konspirace.

2004

Čínští vědci Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu na konferenci Crypto 2004 oznámili, že dokáží prolomit hašovací funkci MD5 a dále méně odolné funkce MD4, RIPEMD a HAVAL-128. Vědci nalezli nové obecnější techniky využití slabin iterativních hašovacích funkcí pomocí diferenciální kryptoanalýzy. Prolomením hašovací funkce zde máme na mysli praktické nalezení kolize, tj. dvou různých zpráv vedoucích na stejnou haš. Problematika byla intenzívně studována i v ČR. Kryptolog Vlastimil Klíma jako druhý na světě našel metodu, jak hledat kolize hašovacích funkcí. Jeho metoda je rychlejší než původní čínská metoda. V Čechách byla také zveřejněna prvá práce (autor Ondrej Mikle) ukazující, jak lze nalezené kolize využít k útoku, který zpochybňuje důvěru v předaná podepsaná data.

C. NIST (National Institute of Standards and Technology - USA) a kryptografie, část 1.

Jaroslav Pinkava, CA Czechia, (Jaroslav.Pinkava@zoner.cz)

1. Úvod

Americký vládní NIST (http://www.nist.gov/) sehrává svými ustanoveními, normativními a dalšími publikovanými dokumenty velkou roli ve vztahu k praktickému používání kryptografických postupů nejen v USA, ale i ve světě. Příkladů lze jistě vyjmenovat mnoho, za všechny zde stačí zmínit např. roli dokumentu FIPS 140-2, který se stal široce využívanou normou při certifikaci kryptografických prostředků.

NIST byl založen kongresem 3. března 1901 jako první federální výzkumná laboratoř orientovaná do fyzikální problematiky. Mezi jeho počáteční úkoly patřilo vytvoření norem pro různé typy fyzikálních měření. NIST funguje dnes jako vládní agentura podřízená ministerstvu obchodu. Náplň jeho činnosti je dnes velmi bohatá a rozvětvená (celkový přehled produktů a služeb, které NIST nabízí, najdete zde – http://www.nist.gov/public_affairs/products.htm).

Do problematiky informační bezpečnosti zasahují především následující oblastí činnosti NIST:

- akreditace laboratoří – program NVLAP (National Voluntary Laboratory Accreditation Program)
- publikace NIST (zejména série NIST Special Publication 800)
- normy a související dokumenty k IT bezpečnosti.

Představení obsahu činnosti, kterou se NIST v IT bezpečnosti zabývá, bude proto věnována pozornost tohoto článku (který má víceméně úvodní charakter) a několika jeho dalších pokračování.

2. Program NVLAP (akreditace laboratoří)

Na základě programu National Voluntary Laboratory Accreditation Program (NVLAP) je prováděna akreditace testovacích a kalibračních laboratoří. Tento program funguje plně ve shodě s mezinárodními normami ISO (International Organization for Standardization) a IEC (International Electrotechnical Commission) včetně podmínek z norem ISO/IEC 17025 a ISO/IEC 17011.

NIST Handbook 150: 2001, NVLAP Procedures and General Requirements (http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf) - tato příručka popisuje základní procedury, s kterými program NVLAP pracuje a obecné požadavky pro akreditaci testovacích a kalibračních laboratoří (netýká se jen bezpečnosti IT).

Na základě tohoto programu pracuje již celá řada akreditovaných laboratoří. Bezpečnosti informačních technologií se dotýkají problematiky

- testování ve smyslu dokumentu Common Criteria
- testování kryptografických modulů

Common Criteria

Akreditace provedená ve smyslu tohoto programu umožňuje naplnit požadavky jak vládních organizací, tak i soukromého sektoru ve vztahu k testování bezpečnosti informačních technologií. Příručka NIST Handbook 150-20 definuje technické požadavky na prováděné vyhodnocování a ověřování shody dle norem ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation* (Common Criteria) a *Common Methodology for Information Technology Security Evaluation* (CEM). Samotný program (označovaný jako NIAP Common Criteria Evaluation and Validation Scheme - CCEVS - for Information Technology Security) byl vytvořen na základě spolupráce NIST a NSA (National Security Agency). Závěry hodnocení takto validovaných produktů jsou pak uznávány i v celé řadě dalších zemí. V současné době je v USA akreditováno pro hodnocení dle CC celkem deset takovýchto laboratoří (http://ts.nist.gov/ts/htdocs/210/214/scopes/cct.htm).

Kryptografické moduly

Program Cryptographic Module Testing LAP (CMT) je zaměřen na akreditaci laboratoří, které provádí validaci kryptografických modulů (ve smyslu testování na shodu).
Příručka NIST Handbook 150-17 definuje technické požadavky na prováděné testování kryptografických modulů (ve smyslu publikace FIPS 140-1, nyní již FIPS 140-2).
Program CMT LAP byl vytvořen na základě požadavku laboratoře NIST (Information Technology Laboratory) pro akreditaci laboratoří, které testují kryptografické moduly na shodu na bázi programu CMV (Cryptographic Module Validation). NIST zde spolupracuje s kanadskou institucí CSE (Communications Security Establishment) obdobného zaměření. V současné době je pro tuto činnost akreditováno v USA celkem sedm laboratoří (http://ts.nist.gov/ts/htdocs/210/214/scopes/crypt.htm). Dále jsou akreditovány dvě laboratoře v Kanadě, jedna v Německu - TUV Informationstechnik GmbH (TUViT), http://www.tuvit.de. Další dvě akreditované laboratoře jsou ve Velké Britanii - BT Cryptographic Module Testing Laboratory (http://www.bt.com/consulting) a LogicaCMG FIPS Laboratory (http://www.logicaCMG.com).

Seznam evaluovaných produktů lze nalézt na adrese
http://csrc.nist.gov/cryptval/140-1/1401val.htm.

3. Publikace NIST

NIST provozuje rozsáhlou databázi publikací, základní údaje lze nalézt na adrese http://www.nist.gov/public_affairs/pubs.htm. Existuje rozsáhlá řada publikací NIST, které se dotýkají problematiky IT bezpečnosti, některým z nich bude věnováno pokračování tohoto článku. Zde lze zmínit například sérii Special Publication 800 (http://csrc.nist.gov/publications/nistpubs/index.html) a možná nejčastěji citovaný dokument této série - An Introduction to Computer Security: The NIST Handbook, SP 800-12.

4. Normy v informačních technologiích

NIST, jak již vyplývá z jeho základního zaměření, se problematikou normalizační činnosti zabývá ve značné šíři. Dopady této činnosti směřují jak na vnitřní trh USA, tak i např. na

pomoc americkým vývozcům při nezbytnosti dosahování shody s požadavky cílových zemí dovozu (příkladem zde může být Evropská Unie).

Normy pro oblast informačních technologií (hardware, software, sítě) jsou svým obsahem kritické pro fungování celého oboru. NIST spolupracuje s jednotlivými průmyslovými skupinami při vývoji těchto norem. Řadu činností v tomto směru vykonává Information Technology Laboratory (http://www.itl.nist.gov/index.html). Jednou z ústředních kompetencí této laboratoře je pak počítačová bezpečnost. Odpovídající činnosti (normy, produkty, výzkum) se koncentrují v rámci Computer Security Resource Center (CSRC - http://csrc.nist.gov/).

Dalšími důležitými stránkami, která se týkají problematiky norem ve vztahu k IT bezpečnosti jsou:

- Common Criteria (http://niap.nist.gov/cc-scheme/index.html), mj. je zde v současné době k dispozici draft třetí verze dokumentu CC. Samotný dokument (ve starší verzi) se stal normou ISO/IEC 15408 používanou v širokém mezinárodním měřítku.
- Federal Information Processing Standards (FIPS - http://www.itl.nist.gov/fipspubs/), NIST vydává normy a příručky, které mají za cíl specifikovat požadavky federální vlády (ve smyslu bezpečnost a interoperabilita).
- Standards and Conformance Testing Group (http://www.itl.nist.gov/div897/ctg/), tato skupina vyvíjí testy na shodu a další nástroje, které jsou používány pro dosažení shody s normami z IT.

5. Shrnutí

Úvodní článek se věnoval celkovému pohledu na aktivity amerického NIST ve vztahu k problematikám IT bezpečnosti. NIST – jako v tomto směru jedna z nejvýznamnějších světových institucí – má díky svým aktivitám a své bohaté dokumentační a normalizační základně široký dopad na řešení výzkumných i praktických otázek IT bezpečnosti, a proto si zaslouží pozornost odborníků. Některým těmto aktivitám a dokumentům budou věnována pokračování tohoto článku.

D. E-Mudžahedínové, virtuální strana štěstí a e-sprejeři ….

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

Muslimy po celém světě rozhněvaly karikatury proroka Mohameda, které už loni v září otiskl dánský deník Jyllands-Posten. Mezinárodní krize však naplno vypukla až poté, co je přetiskla norská a následně i další evropská média. Co následovalo, můžeme průběžně sledovat v různých médiích – masové demonstrace, útoky radikálních muslimů na dánská velvyslanectví (Sýrie, Indonésie, ..), odchod dánských diplomatů z muslimských zemí, omluvy některých evropských států, dohadování na téma svoboda projevu, vyhlášení soutěže o nejlepší comiks na téma holocaust a útok „elektronických“ Mudžahedínů na www servery v Dánsku a posléze v celé Evropě.

Nutno říci, že boží bojovníci se opravdu činili a denně za nimi zůstávaly stovky pokořených serverů. Pokud vás zajímají statistiky z této elektronické svaté války (počty podle dnů, podle domén, podle útočníků, podle systémů), doporučuji server http://www.zone-h.org/en/defacements . Zde také můžete zjistit, že za poslední měsíc bylo pozměněno kolem 260 webů v doméně cz. V případě evidovaných českých serverů, jde o útoky muslimů jen zřídka… Ostatně je otázkou, zda za sestřelené stovky serverů v Dánsku a Evropě mohou opravdu výlučně hackeři - muslimové anebo zda se nepřidala k této nové zábavě řada nevěřících hackerů a obě skupiny pak na stránky umísťují výkřiky typu Alláh Akbar.

Nedávno jsem si zavedl pro svoji potřebu nový pojem – elektronický sprejer. Je to v mém pojetí útočník, který se snaží pozměnit cizí www stránku za jediným účelem – ponechat zde svůj „podpis“ a případně doplnit něco vtipného. Dělá to samozřejmě pro adrenalínový pocit a pro „prchavou“ slávu zasvěceného okolí. Mimo obdobné motivace se mezi ním a sprejerem najde celá řada dalších shodných znaků. Netvrdím zde, že je to jediný nebo hlavní důvod, proč se útočníci snaží stránky pozměnit. Ve svém dvoudílném článku z roku 2004 Hackeři,

Crackeři, Rhybáři a Lamy jsem se pokusil popsat motivace útočníků a jejich „typologii“ detailněji.

http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271893_bezpecnost

http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271894_bezpecnost

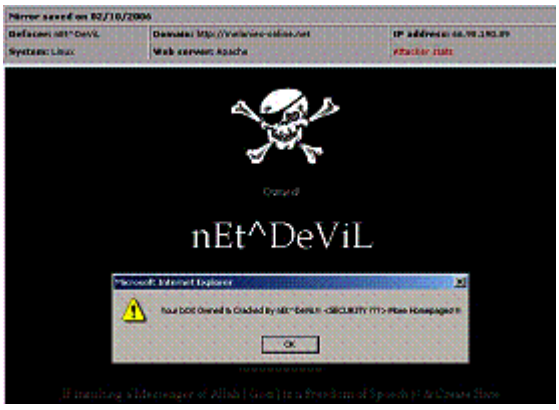
Psal jsem zde i o hacktivismu, což je politicky motivované napadání internetových stránek. Měl jsem tehdy poměrně málo příkladů. Prakticky to bylo jen pár odkazů, které souvisely s předvolebním bojem a šlo vesměs o pozměňování stránek politickým stranám. Na závěr jsem se však zmínil, že: *V posledních letech se stále více a více rozvíjí. Je pravděpodobné, že mimo jednotlivce a organizované skupiny se do této činnosti zapojují i profesionálové ze speciálních služeb.* Materiálu, který by to dokazoval, jsem však příliš neměl. Nyní se situace zcela změnila, příkladů je k dispozici nepřeberné množství. Připravil jsem proto malou ukázku v podobě screenshotů, které tento drobný fejeton doprovází.

Musíme si začít zvykat na to, že politický boj se vede již nejen diplomatickou a mediální cestou, ale že začíná využívat více a více moderních prostředků. Mezi tyto prostředky patří i zbraně, které umožňují vést e-válku. Když jsem v roce 2003 uveřejnil na rootu článek *E-válka v zálivu (a okolí?)*, bylo to ve skutečnosti povídání spíše o jednotlivých e-sabotážích, skutečná válka vedená na celé frontě kyberprostoru teprve začíná a teprve nás čeká.

Velmi mne překvapuje úspěšnost elektronických útočníků, kteří ve jménu Alláha táhnou Evropou. Dovolím si proto vyslovit dvě kacířské hypotézy. Jedna zde již v úvodu zazněla, útočí i skupiny nemuslimských hackerů. Jejich motivem může být spletitá směs důvodů – být IN, být přitom, podpora islámských států – nenávist Bushe, zábava, atd. atd.…

Druhá hypotéza pak souvisí s možností přípravy na e-válku. Zjednodušeně řečeno, co takhle nenápadně otestovat své zbraně v reálné situaci?

Když jsem si v roce 2003 dovolil vyslovit obdobné myšlenky o e-válce v zálivu, byl jsem v diskusi k článku napadán pro svůj politický a neobjektivní názor. V poslední době jsem



přemýšlel, jaký můj názor opravdu je, které straně dát přednost. Blíží se volby, a tak tato otázka bude stále více a více aktuální. Se svým bratrem jsme vedli řadu „pivně politických diskusí“. Mnou prosazované vytvoření virtuální strany, která zcela nevšedními postupy převálcuje ve volbách všechny stávající politické skupiny, vyústilo místo její skutečné realizace v knihu, kterou bratr napsal a vydal. Máte-li zájem se před volbami trochu zasmát (a doufejme, že snad ještě i po nich), dovoluji si zde na úplný závěr dát na toto dílko malou upoutávku:

V.Vondruška, Strana štěstí, MOBA, 2005,

http://www.royal-glassworks.cz/vondruska/beletrie.php

Pokud si myslíte, že vás naše politika už nemůže ničím překvapit, přečtěte si příběh o Straně štěstí. V malém motorestu na Vysočině se sejde několik lidí – neschopný syn bohatého podnikatele, vyhozený vysokoškolský pedagog, propuštěný podvodník, ambiciózní řezník, znuděná kráska a rozšafný údržbář. Založí novou politickou stranu, která přijde s převratným nápadem – obsazovat místa v parlamentu po vítězných volbách losováním. Losy Strany štěstí se začnou neuvěřitelně dobře prodávat a každý, kdo si los koupí, ve volbách tuto stranu podpoří. Co kdyby padlo štěstí i na něj? A Strana štěstí volby skutečně s drtivou převahou vyhraje. Pak proběhne slosování a vylosovaní šťastlivci začnou řídit chod této země. Zdá se vám tenhle nápad šílený? Autor se vás pokusí ve skvělém satirickém románu přesvědčit, že i nejnesmyslnější šílenosti nakonec nemusí být tak nesmyslné.

E. O čem jsme psali v únoru 1999 – 2005

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 P.Vondrušky a 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 sešity GCUCMP, 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:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf

NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška

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@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.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/