Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 2/2001 12. únor 2001

2/2001

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
(>250 e-mail výtisků)

OBSAH : **Str.**

A. CRYPTREC – japonská obdoba NESSIE (informace)

Jaroslav Pinkava, AEC spol. s r.o. & Norman Data Defense Systems

Úvod

V prosincovém čísle Crypto-Worldu se měli čtenáři možnost seznámit se evropskou inciativou v problematice kryptografie – Cryptonessie. Cílem odpovídajících činností je přinést pro praxi celé portfolio tzv. kryptografických primitivů, které by se následně staly součástí mezinárodních norem. Cryptonessie je připravována v rámci evropských struktur (Evropská Unie).

S obdobnou iniciativou přišla pracovní skupina Information technology Promotion Agency(IPA), sponzorovaná japonským ministerstvem zahraničního obchodu a průmyslu. Formální výzva vyšla 13. června 2000, návrhy byly přijímány do 12.ledna 2001. Předpokládá se, že výsledkem projektu bude určitý seznam (vyhodnocených) kryptografických technik pro použití v e-governmentu jehož infrastruktura bude vytvořena v roce 2003. Webovská stránka inciciativy má adresu :
http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html.

Obsah aktivit CRYPTRECu

Z výše uvedené adresy je převzat následující přehled o diskutovaných návrzích v rámci CRYPTRECu.

Cryptographic Techniques for Detailed Evaluation

Category	Cryptographic Techniques
Asymmetric Cryptographic techniques (Confidentiality)	ACE Encrypt ECAES (Elliptic Curve Augmented Encryption Scheme) in SEC1 EPOC HIME-2 PSEC
Asymmetric Cryptographic techniques (Authentication)	ESIGN-identification
Asymmetric Cryptographic techniques (Signature)	ACE Sign ECDSA (Elliptic Curve Digital Signature Algorithm) in SEC1 ESIGN-signatures MY-ELLTY ECMR-h
Asymmetric Cryptographic techniques (Key-sharing)	ECDHS (Elliptic Curve Diffie-Hellman Scheme) in SEC1 ECMQVS(Elliptic Curve MQV Scheme) in SEC1 HDEF-ECDH HIME-1

Symmetric Ciphers (Stream ciphers)	MULTI-S01 TOYOCRYPT-HS1 CIPHERUNICORN-E
Symmetric Ciphers (64-bit block ciphers)	FEAL-NX Hierocrypt-L1 MISTY1 Camellia CIPHERUNICORN-A
Symmetric Ciphers (128-bit block ciphers)	Hierocrypt-3 MARS RC6 SC2000
Pseudo-Random Number Generators	TOYOCRYPT-HR1

Other Important Cryptographic Techniques to be Evaluated

Category	Cryptographic Techniques
Asymmetric Cryptographic techniques (Confidentiality)	RSA OAEP
Asymmetric Cryptographic techniques (Signature)	DSA RSA PSS
Asymmetric Cryptographic techniques (Key-sharing)	DH Key Exchange
Symmetric Ciphers (64-bit block ciphers)	Triple DES
Symmetric Ciphers (128-bit block ciphers)	Rijndael
Hush Functions	MD5 RIPEMD-160 SHA-1
Pseudo-Random Number Generators	Pseudo-Random Number Generator based on SHA-1 (FIPS186:DIGITAL SIGNATURE STANDARD APPENDIX C)

Z přehledu je zřejmé, že řada z diskutovaných návrhů je již kryptografické veřejnosti známa – např. právě ze zmíněné evropské Cryptonessie. Následující kryptografické primitivy nejsou součástí evropských návrhů (resp. jiných iniciativ jako SECG):
HIME-1, HIME-2, MY-ELLTY ECMR-h, MULTI-S01, CIPHERUNICORN-E, FEAL-NX, CIPHERUNICORN-A, TOYOCRYPT-HR1, HDEF-ECDH, TOYOCRYPT-HS1

Bohužel k těmto posledně zmíněným návrhům zatím ve větší části je dokumentace buď přístupná pouze v japonštině nebo není přístupná vůbec. Nepochybně však bude zajímavé sledovat, jak se bude celý proces evaluace těchto návrhů vyvíjet a srovnávat dosažené výsledky s výsledky Cryptonessie.

B. Připravované normy k EP v rámci Evropské Unie II. (doplnění informace z Crypto-Worldu 1/2001)

Jaroslav Pinkava, AEC spol. s r.o./ Norman Data Defense Systems

CEN/ISSS

V návaznosti na chystané jednání 7.února 2001 v Bruselu skupiny CEN/ISSS WS/E-Sign se na webovských stránkách objevily některé nové dokumenty. Byl schválen pracovní pořádek tohoto jednání (N126). V jeho rámci budou prezentovány resp. schvalovány následující drafty:

CWA Draft on Area D: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures, Farroukh Ahmad **(N129)**

Po rozdělení problematiky (N115 – dole poznámka 2.) v této oblasti je to první verze daného dokumentu. Oproti předešlým verzím (kromě zapracování některých připomínek) byly odstraněny původní přílohy A. a B, jejichž obsah se stane zřejmě základem chystaného nového dokumentu.

CWA Draft on Area F: Secure Signatur-Creation Devices (EAL 4 and EAL 4+), Reinhard Posch (nová verze měla být na serveru dostupná 25.1.2001 – zatím není k dispozici)

CWA Draft on Area G1: Security Requirements for Signature Creation Systems, Robert Willmott (nová verze měla být na serveru dostupná 25.1.2001 – zatím není k dispozici)

CWA Draft on Area G2: Procedures for Electronic Signature Verification; V 1.0.3, 2001-01-25, Denis Pinkas **(N128)**

Dokument popisuje různé stránky verifikačního procesu. Draft nahrazuje starší verzi N102. Struktura dokumentu zůstala shodná, bylo reflektováno na některé připomínky (N113, N127).

CWA Draft on Area V: EESSI Conformity Assessment Guidance; Version 2.0; 2001-01-22, Jan Sauer **(N130)**

Draft nahrazuje starší verzi N120. Je věnován otázkám harmonizace implementací norem pro elektronické podpisy – slouží zejména jako příručka certifikujícím a testujícím laboratořím. Oproti předešlé verzi došlo pouze k některým dílčím úpravám.

Poznámka1.: Pokud je za názvem draftu i číslo (N*), pak uvedený draft je již k dispozici na adrese: http://www.ni.din.de/ (CEN/ISSS Electronic Signatures) a lze si ho stáhnout. Červeně jsou označeny drafty, které již jsou předkládány ke schválení, modře pak první nový draft.

Poznámka 2.: Přestože tak bylo původně ohlášeno (N115), v pořadu jednání (a ani v rámci zveřejněných dokumentů) se zatím neobjevila žádná informace ohledně chystaného draftu ***„Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems“*** (dokonalejší evropský FIPS 140).

ETSI

Co se týče ETSI, tak zde zatím žádný nový dokument (draft) neobjevil, kromě poznámky, že ETSI v roce 2001 chystá vydání zhruba pěti nových dokumentů. K jejich obsahu jsou v současné době známy pouze následující informace.

Policy requirements for CSPs issuing trusted time stamps

Dokument bude vycházet z požadavků na politiku, které již byly v dokumentech ETSI zpracovány. Na službě časových značek je velice zainteresována komerční sféra a stávají se důležitou složkou problematiky elektronických podpisů (dokumentES 201733). Zde zformulovaná minima pro požadavky v oblasti bezpečnosti a kvality jsou nezbytná k zabezpečení důvěryhodného ověření dlouhodobých (long-term) elektronických podpisů.

Policy requirements for CSPs, according to Art. 5.2 of the Directive

Obsahem tohoto materiálu budou otázky řízení bezpečnosti a certifikační politika těch poskytovatelů certifikačních služeb, kteří fungují na bázi principů odlišných od principů pro poskytovatele certifikačních služeb (PCS), kteří vydávají kvalifikované certifikáty. Potřeba existence těchto PCS vyplývá z potřeb trhu (transakce elektronického obchodu střední úrovně – jako například mobilní elektronický obchod). Na základě analýzy provedené STF pro alternativní třídy certifikátů (dle článku 5.2 Směrnice EU o elektronických podpisech) budou stanoveny příslušné specifikace, které se mimo jiné budou odkazovat např. na dokument RFC 2527 a doplní zde potřebné specifické detaily.

XML electronic signatures

Norma se bude zabývat syntaxí a formáty kódování elektronických podpisů v XML na základě dokumentu ES 201733. První studie pro verzi XML je připravována v rámci STF 155 (Specialist Task Force). Současný formát XML podpisů dle W3C bude použit k převzetí formátů vyšších úrovní elektronických podpisů dle ETSI do světa XML. Tato aktivita vznikla v návaznosti na mezinárodní aktivity v dané oblasti, zejména W3C/IETF a práce v EDI. Hlavním důvodem pro toto spojení je uvedení specifikací XML na mezinárodní scénu.

Technical aspects of signature policies

Koncepce podpisové politiky je zde zvažována ve vztahu k ustavení společné základny elektronických podpisů. Dokument ETSI ES 201 733 již sice obsahuje určité specifické nástroje pro definice podpisových politik, avšak neobsahuje všechny takovéto aspekty (např. vícenásobné podpisy). Dokument bude navržen jako experimentální RFC pro IETF a posléze připraven jako norma.

Infrastructure and interoperability requirements for on-line validation of Certification Service Providers

Cílem těchto prací je stanovit doporučení pro podporu akcí spoléhajíci se strany ve směru ověření, že vydavatel došlého certifikátu je v dané době důvěryhodnou stranou transakce. Na základě existujících dokumentů EESSI lze zajistit, že strana spoléhající se na certifikát (například příjemce podepsané smlouvy či objednávky) získá dostatek informací potřebných pro kontrolu platnosti certifikátu. Existují tedy normy podporující takovouto kontrolu. Avšak podstatně obtížnější je ověřit, zda vydávající CSP je v době transakce v pořádku (např. CSP mohla ukončit svoji činnost nebo neprošla posledním auditem atd.). Tento typ informací je dodáván třetí stranou nezávislou jak na straně, která transakci podepsala, tak i na straně vydavatele certifikátu. Důležitost této informace je stěžejní zejména v transakcích překračujících hranice domén a států.

Existující národní schémata pro tuto problematiku nejsou harmonizována, totéž se týká odpovídajících protokolů a formátů dat. Dokument zohlední jak technické tak i akreditační aspekty problematiky a jeho cílem bude identifikace potřebných procedurálních a technických vlastností.

C. K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích

RNDr.Jaroslav Hrubý,CSc., GCUCMP, Praha ,
Ing.Igor MOKOŠ, HPC, Praha

Tato verze je "předpublikační" , touto cestou je předložena k odborné diskusi.

1.Úvod

Význam zákona ČR o elektronickém podpisu č.227/2000 Sb., jeho uvedení do života v celém spektru aplikací , včetně jeho dopadu na ekonomiku , by neměl být podceňován.

Tento zákon otevírá cestu k informační společnosti a jeho správná implementace do naší ekonomiky , a také do všech ostatních oblastí naší činnosti, v níž hrál dosud stvrzovací roli klasický podpis jedince, je nezbytná pro naše přibližování k Evropské Unii (EU).

Se vstupem do 21.století je více než kdykoliv předtím jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů u státní správy, zavést elektronické peníze a v neposlední řadě vytvořit infrastrukturu pro takovéto praktické použití elektronického podpisu (EP), jako jednoho se základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, kulturního a vědeckého je potřeba respektovat daný stav v EU. V případě základních zákonů a právních norem v oblasti informačních technologií (IT) jsme (pokud to míníme s naším vstupem do EU vážně) rovněž povinni slaďovat naše zákony a normy s těmi platnými v EU.

Rozvoj a využití nových oblastí ekonomiky - tzv. digitální ekonomika – nejsou možné bez přechodu na plné využití elektronické komunikace , elektronického obchodu a nejrůznějších elektronických služeb, a to ve všech sférách života společnosti.

Je tedy třeba plně ocenit iniciativu související s návrhem vyhlášky k zákona o EP Úřadu pro ochranu osobních údajů a snahou o její legislativní naplnění. Právě tato vyhláška je nezbytná pro výše zmíněné praktické použití elektronického podpisu a vytvoření potřebné infrastruktury. Vznik této infrastruktury v ČR je zároveň podmíněn úspěšnou integrací nových IT systémů do stávajících při splnění všech bezpečnostních požadavků.

Přestože v současnosti zákon o EP je již v ČR v platnosti, vyhláška však nikoliv, a navíc zůstává celá řada problémů nedořešených.

Jednak chybí vhodné standardy a normy, které by byly platné na území ČR, dále chybí testovací a vyhodnocovací laboratoře a není zatím návaznost na vyhodnocovací laboratoře v zahraničí a jejich uznávání. Není vyřešena otázka křížových certifikací a uznávání zahraničních certifikátů.

Podstatným nedostatkem je neřešení časových značek (součástí klasického podpisu dokumentu je většinou i datum a u EP by to mělo být stejné) , profilů kvalifikovaných certifikátů a dále nastavení požadované bezpečnostní úrovně pro různé typy certifikátů.

Nejsou řešeny rovněž otázky jednotné kořenové struktury v ČR, elektronických formátů a jiné.

Podstatné je, že celý proces vytváření infrastruktury pro praktické použití zákona o EP, jakoby v současnosti ztratil politickou podporu, která byla při samotném vzniku zákona značná.

Je proto nutné, aby všechny zainteresované strany spolupracovaly na řešení těchto otázek, včetně jednotlivých odborníků. I když tito nemohou urychlovat přijetí novely zákona , mohou odborným tlakem na výkonné orgány poukazovat na existující nedostatky , navrhovat jejich řešení a snižovat tak hrozící rizika z nedotažení tohoto procesu do konce.

Cílem tohoto článku je ukázat klíčovou roli bezpečnostního hlediska na tuto problematiku a na několika modelových případech ukázat hrozící rizika v oblasti bankovnictví, elektronického obchodu apod. s neblahým dopadem na celou naší ekonomiku.

Aby hrozící rizika byla snížena na minimum, musí uvedení zákona o elektronickém podpisu do praxe nutně vést ke zvýšení celkového zabezpečení informačních systémů v ČR, a to ve všech organizacích (státních i soukromých) , zejména z hlediska průniku komplexní bezpečnosti a informační bezpečnosti se zákonem o ochraně osobních údajů č.101/1999, zákonem o utajovaných skutečnostech č.148/1998 Sb.(tento zákon se týká organizací, které pracují s utajenými informacemi již od nejnižšího stupně klasifikace „Vyhrazeno“) a souvisejícími normami ČSN, předpisy , včetně platných mezinárodních norem jako jsou ISO 9796, ISO/IEC TR 13335, BS 7799 apod.

To by mělo být sladěno v protiváze stojícím zákonem o dostupnosti informací č.106 Sb. (popřípadě celním, telekomunikačním, obchodním zákonem a jinými relevantními zákony a normami, platnými pro práci ve finančním sektoru. Telekomunikační zákon zmiňujeme z důvodu mobilních finančních portálů, v současnosti populárního tzv.“GSM banking“, a trendům mobilního trhu).

Je nezbytné, aby kompetentní státní orgány vyvinuly v tomto směru kontrolní tlak na všechny subjekty, jelikož nepřesnosti , popřípadě bílá místa v předpisové základně při jeho aplikaci , by mohla mít fatální důsledky pro celou naši ekonomiku.

Relevantním dokumentem EU k zákonu č.227/2000 je finální verze Směrnice Evropského parlamentu a Rady o elektronických podpisech .Tato Směrnice EU byla schválena Evropskou radou dne 30.11.1999 [1].

2. Potřeba průběžné komplexní bezpečnostní analýzy IT systémů

Pojetí bezpečnosti organizace do komplexu všech jejích cílů, strategie a politiky je nedílnou součástí její úspěšné existence ve třetím tisíciletí. Toho je možné dosáhnout pouze zavedením komplexní bezpečnosti organizace. Samozřejmě toto platí pro jakoukoliv organizaci, ale pro finanční organizace obzvláště, jelikož nedostatky u nich mají nejpřímější dopad na naší ekonomiku.

V oblasti finančního sektoru a služeb nemá cenu mluvit o bezpečném elektronickém podpisu, jeho dopadu na ekonomiku, jeho zavádění do státem řízených či jiných finančních organizací jako např. MF ČR, finanční úřady, celnice, ČNB, soukromé banky, pojišťovny atd. …), pokud není v těchto organizacích dobře zpracovaná a prakticky funkční bezpečnostní předpisová základna, včetně té nové pro poskytovatele certifikačních služeb, týkající se certifikační politiky, certifikačních a registračních autorit a všeho, co s infrastrukturou uvedení zákona o EP souvisí.

Rovněž tak ochrana osobních údajů ve smyslu zákona č.101/1999 Sb. a jeho důsledky pro informační systémy (IS) ve finančních institucích bez výše uvedeného je bezpředmětná. Je zřejmé, že pravděpodobnost úniku informace při nedostatcích v oblasti personální bezpečnosti je mnohonásobně vyšší, než její únik např. při kryptoanalytickém útoku na IS.

Komplexní bezpečnost prolíná informační bezpečnost v řadě jejích oblastí, a tedy bezpečnost IT je od komplexní bezpečnosti neoddělitelná. Vytvoření podmínek pro funkčnost jejich vzájemného průniku je nezbytným úkolem každého vedení organizace s vědomím, že útok s cílem získat chráněnou informaci je veden vždy na nejslabším místě.

Vzhledem k dynamickému rozvoji v oblasti informačních systémů, informačních technologií, informační bezpečnosti a kryptologie je nezbytné se vstupem ČR do EU, aby správa informační bezpečnosti v každé organizaci byla v souladu s její komplexní bezpečností a dále se sérií základních mezinárodních dokumentů vydaných v sérii ISO/IEC TR , platných v EU, a to takovým způsobem, aby:

- bezpečnostní opatření byla komplexní,
- systém správy komplexní a informační bezpečnosti byl otevřený pro budoucí změny,
- systém správy komplexní a informační bezpečnosti plně akceptoval zákony v ČR, týkající se této oblasti
- v maximální míře využil stávajících systémů v organizaci, aby jeho realizace byla v optimalizovaném poměru mezi finančními náklady a výsledkem dosažené bezpečnostní úrovně.

Pro splnění výše uvedeného je nezbytné, aby v organizaci byl koncepční přístup k bezpečnosti (nejlépe řízený bezpečnostním orgánem uvnitř organizace, jakým je např. bezpečnostní rada, jakožto poradní orgán vrcholového managamentu realizující zde celkovou bezpečnost a správu informační bezpečnosti. Toto fórum bezpečnosti, zpracovává interdisciplinární témata , doporučuje a schvaluje komplexní bezpečnost organizace , bezpečnost IT a interní standardy IT).

Vývoj v oblasti IT, a také v celém spektru bezpečnostního výzkumu na IT navazujícího, je natolik dynamický, že organizace musí neustále bezpečnostní hlediska aktualizovat, auditovat a svoji bezpečnost koncepčně budovat tak, aby platila v co nejdelším časovém horizontu.

Absolutní bezpečnost neexistuje – i v kvantové kryptografii nelze eliminovat lidský faktor. Avšak lze se jí v limitě přibližovat, a to právě komplexností bezpečnostních řešení IS, minimalizací vlivů lidského faktoru, eliminací jeho nekontrolovatelnosti a sankcionovatelností. Je tudíž nezbytná průběžná bezpečnostní analýza komplexní bezpečnosti v IT, a to především ve všech organizacích finančního sektoru.

Pro průkaznost výše uvedených tvrzení ukážeme současnou zranitelnost EP jeho chybnou integrací do IS, novými fyzikálními a kryptoanalytickými útoky, účinnými i při dobré integraci, i možnou ohrozitelnost samotných matematických principů, na kterých je založen.Abychom toto ukázali, připomeneme v další kapitole základy EP, a to na modelu digitálního podpisu.

3. Základy konstrukce elektronického podpisu z hlediska bezpečnostních rizik

Systém EP je založen na jisté pojmové konstrukci, která tvoří páteř příslušného zákona a která je zobecněním systému tzv. digitálního podpisu. Pojem digitálního podpisu byl zaveden v kryptologii. V současné době je digitální podpis nejčastěji technologicky realizovanou variantou elektronického podpisu. V blízké budoucnosti však mohou přejít do běžného užití i jiné varianty elektronického podpisu, odlišné od podpisu digitálního, a proto bylo účelné přijmout obecnější zákon o EP.

Pro jasné pochopení pojmů diskutovaných uvedeme nyní popis konstrukce digitálního podpisu, která je v současnosti nejužívanější jako model EP.

Digitální podpis využívá určitou matematickou vlastnost tzv. asymetrických šifrových systémů, která byla objevena asi před 20 lety. Bezpečnost je založena na složitosti matematické úlohy faktorizace velkých čísel.

Klíčem se v digitálním podpisu nazývá posloupnost (řetězec) znaků, který umožňuje použít šifrování. Asymetrická šifra obsahuje dva klíče, jeden klíč je určen pro zašifrování

(nazývá se soukromý klíč) a jiný klíč slouží pro odšifrování (veřejný klíč). Přitom platí pravidlo, že ze znalosti veřejného klíče nelze odvodit klíč soukromý.

Zde existuje první bezpečnostní riziko na samotné úrovni složitosti matematické úlohy, která může být principiálně řešitelná. Jednak je klasickými počítači [2] útočeno na bezpečnou délku klíče , což je umocněno ve spojení s novým hardwarovým zařízením typu TWINKLE [3]. Navíc však existuje v kvantovém počítání tzv.Shorův algoritmus [4] , řešící úlohu faktorizovatelnosti a Groverův vyhledávací algoritmus [5], který kvadraticky urychluje vyhledávání v databázích.

I když doposud technická realizace kvantového počítače operujícího s velkým počtem kvantových bitů neexistuje, je nutné i toto kvantové bezpečnostní riziko brát v úvahu již nyní. Je zřejmé, že např. akreditovaná certifikační autorita archivující dle certifikační politiky kvalifikovaný certifikát EP po dobu delší dvaceti let, může být v tomto časovém horizontu kompromitována, jelikož tehdy již mohou kvantové počítače prakticky existovat. Rozbor a možné řešení tohoto problému je v práci [6].

„Černý pátek“ pro EP a infrastrukturu založenou na šifrách s veřejným klíčem bude znamenat den praktické realizace kvantového počítače. Nejenže budou rozbity šifrové systémy stojící na složitosti faktorizace, ale i na složitosti diskrétního logaritmu a eliptických křivek, kterými se v rámci našeho modelového případu nezabýváme. Rovněž budou prediktovatelné pseudonáhodné generátory .

Zhroutí-li se naše bankovnictví a bude-li ČR vskutku komplexně vytunelována záleží jenom na bezpečnostní prevenci. Prevence a příprava může být např. v hledání nových cest jakými je kvantový kryptosystém s veřejným klíčem, tak jak je prezentován v práci [7] .

Každá osoba, která chce používat digitální podpis si vytvoří pomocí dodaného softwaru svou vlastní dvojici klíčů – soukromý a veřejný – přičemž soukromý klíč si uloží a veřejný klíč pomocí certifikační autority zveřejní.

Proces podepisování vypadá zhruba takto: podepisující osoba vezme text, který chce podepsat, zašifruje jej pomocí dodaného šifrovacího software s využitím soukromého klíče a výsledek zašifrování připojí k textu jako svůj podpis.

Osoba ověřující digitální podpis postupuje takto: Napřed si z textu zjistí jméno podepsané osoby a pomocí certifikační autority si zjistí, jaký je veřejný klíč podepsané osoby. Pomocí dodaného odšifrovacího software a prostřednictvím získaného veřejného klíče odšifruje digitální podpis (tj. text zašifrovaný pomocí soukromého klíče podepsaného) a získá tak původní tvar textu. Ten pak srovná s otevřeným textem a pokud se oba texty shodují, dojde tím jednak k potvrzení podepsané osoby (jen ten, kdo zná soukromý klíč spojený s daným veřejným klíčem, mohl vyrobit digitální podpis) a zároveň také k potvrzení původnosti textu.

Popsaný postup odpovídá reálné situaci, pouze s jednou změnou. Místo toho, aby digitální podpis vznikl zašifrováním celého textu (tím by vznikl zbytečně dlouhý digitální podpis a také jiné problémy) postupuje se jinak. K danému textu se vytvoří jeho (prakticky) jednoznačná charakteristika – tzv. kryptografický kontrolní součet, který budeme nazývat otisk textu - pomocí dodaného speciálního software a tento otisk textu bude zašifrován soukromým klíčem podepsané osoby. Výsledek bude připojen k textu jako digitální podpis. Ověřující osoba vytvoří (pomocí dodaného software) otisk otevřeného textu, pomocí veřejného klíče pak odšifruje digitální podpis a výsledek odšifrování srovná s otiskem textu. Pokud se shodují, je potvrzena jak správnost veřejného klíče (a tím i podepsané osoby), tak i správnost toho, že text nebyl změněn.

Tento postup má dvě slabá místa. Jednak musí existovat jednoznačná vazba mezi osobou a jejím veřejným klíčem, a to tak, že daný veřejný klíč může náležet nejvýše jedné osobě. To zaručuje certifikační autorita, která potom zaručí společně s registrační autoritou také úplnou identifikaci vlastníka klíče.

Zde si dovolujeme zdůraznit podstatný moment identifikace vlastníka v momentu jeho registrace, což by mělo být bezpečnostně ošetřeno a postup důkladně popsán v certifikační politice dané autority s důrazem na personální bezpečnost. Nejedná se zde pouze o možnost porušení zákona o ochraně osobních údajů 101/1999 Sb., ale možnost personálního selhání pracovníka a identifikace někoho jiného.

Druhým slabým místem je skutečnost, že podepsaná osoba musí dokázat udržet svůj soukromý klíč v tajnosti. Jestliže totiž někdo cizí získá něčí soukromý klíč, pak může bez problémů falšovat digitální podpis této osoby.

Pomineme nedbalostní jednání vlastníka soukromého klíče a soustředíme se na poměrně nové a neustále zdokonalované fyzikální útoky na mikročipy [8]. Ty jsou nedílnou součástí nejrůznějších typů tzv. chytrých karet a útoky na ně mohou být aktivní i pasivní [9] s cílem zisku tajných bitů klíče, popřípadě vytvoření kopie této karty, která je pak používána bez vědomí vlastníka. Pomineme opět ty aktivní, které částečně poškodí mikročip a jsou zjistitelné, minimálně profesionální cestou. Skutečné nebezpečí představují ty pasivní jako jsou tzv. časované útoky [10], útoky založené na momentální změně napětí mikročipu [11] a lineární analýza a diferenční analýza spotřeby energie mikročipu [12].

Jejich aplikace na podepisovací hardware, čipové karty , SIM karty apod. může pro uživatele EP znamenat vážné nebezpečí z hlediska zneužití EP, a ohrozit i celou elektronickou ekonomiku, pokud ostatní bezpečnostní opatření nebudou tato rizika eliminovat. Jednoduchým opatřením je např. nevynášet čipovou kartu pro identifikaci mimo chráněnou oblast (např. režimové pracoviště). To však vede ke značným omezením a ztrátu mnohých výhod plynoucích z rychlosti a okamžité dosažitelnosti elektronických informací. Je to však zcela nemožné u mobilních portálů, které opouští jinak chráněné prostory, např. u mobilních telefonů.

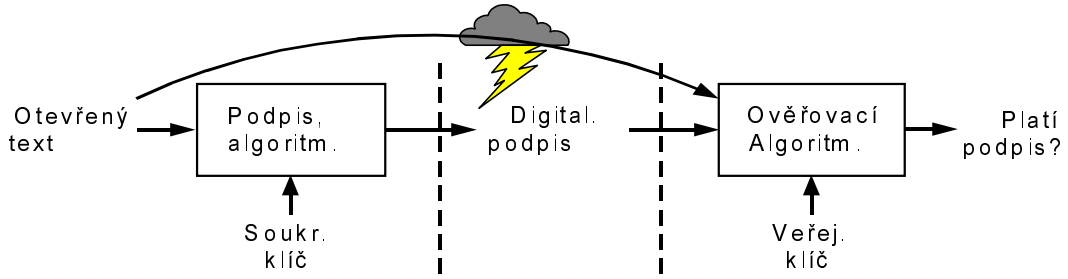
EP funguje podobně jako digitální podpis. Podepisující osoba :

1) si vytvoří dvojici podepisovací data (dříve soukromý klíč) - ověřovací data (dříve veřejný klíč) a ověřovací data uloží u poskytovatele certifikačních služeb (dříve certifikační autorita), který je zpřístupní všem zájemcům.
2) získá od poskytovatele certifikačních služeb podepisovací prostředek (dříve SW pro zašifrování a SW pro vytvoření otisku).

Osoba ověřující elektronický podpis

1) na základě otevřeného textu získá od poskytovatele certifikačních služeb ověřovací data podepsané osoby a dále ověřovací prostředek (dříve veřejný klíč a SW pro odšifrování)
2) použitím ověřovacího prostředku pro otevřený text a s využitím ověřovacích dat získá potvrzení správnosti identity podepsané osoby a původnosti textu.

Každý klient bude mít různou dvojici podepisovací data (utajovaná vlastníkem) - ověřovací data (zveřejněná poskytovatelem) a celý proces EP lze schematicky znázornit následovně:



Certifikační autority se vzorově zpracovanou certifikační politikou a certifikační předpisovou základnou budou muset integrovat nové systémy pro zabezpečení infrastruktury s EP s maximální opatrností do svých existujících IS systémů. Vnořování jakéhokoliv podsystému do systému by mělo být certifikováno na odpovídající bezpečnostní úroveň. Rozhraní jsou nejčastějšími místy vhodné pro průlom do systému . Rovněž odladění a kompatibilita podsystému se systémem nebo dvou systémů bývá častou branou průniku ke chráněné informaci, vede ke snížení celkového bezpečnostního stupně, přestože každý systém zvlášť je bezpečný na stupni vyšším. Bývá proto někdy výhodnější z bezpečnostního a mnohdy i finančního hlediska pořizovat IS jako nový celek, než integrovat systémy, obzvláště není-li přístup ke zdrojovým kódům, vlastní možnosti verifikace v hodnotitelské laboratoři atd. Toto může však končit i požadavkem na vlastní kontrolu při výrobě a programování mikročipů na nejvyšší stupně utajení dle zákona č.148/1998 Sb. Je záhodno dokument podepsat a pak zašifrovat v jednom systému, i když to není podmínka nutná.

Integrátoři konkrétních systémů s EP (např. typu ENTRUST , BALTIMORE a dalších) budou muset provést bezpečnostní analýzu vnoření těchto systémů do IS organizace nikoliv pouze z hlediska funkčnosti a kompatibility, popřípadě předložení certifikátů pro jednotlivé systémy, ale měly by vytvořit vlastní bezpečnostní model v duchu strategie práce [13].

Pouhá prostá integrace těchto systémů do IS organizace, bez certifikace a provedení výše uvedené bezpečnostní analýzy , může rovněž představovat bezpečnostní riziko.

Posledním bezpečnostním rizikem jsou nedostatky při volbě parametrů šifrovacího algoritmu, což si opět ukážeme na modelovém příkladu algoritmu RSA.

RSA (Rivest-Shamir-Adleman) je v současné době asi nejrozšířenější algoritmus s veřejným klíčem. Lze ho použít pro šifrování i pro podpisy. Vhodná délka klíče je odhadnuta v závislosti na možnosti prosté faktorizace útokem hrubou silou. Odhady na nutnou délku klíče v závislosti na vývoji klasické výpočetní techniky vzhledem k exponenciálnímu nárůstu mohutnosti výzkumu v kvantovém počítání se silnou finanční podporou soukromých i státních organizací (např. NSA) není validní. Je třeba vědět, že RSA je zranitelná vůči útokům s volitelným otevřeným textem. Nový typ útoku s měřením času, který jsme již rovněž zmiňovali jako tzv. časový útok, představuje rovněž nebezpečí.

Algoritmus RSA je považován za bezpečný algoritmus, musí se však aplikovat velmi opatrně, aby bylo možné se těmto útokům vyhnout. Je velice důležité mít kvalitní generátor velkých prvočísel**.** Ukazuje se, že pseudonáhodné generátory (např. pseudonáhodný algoritmus v počítači) nejsou tak bezpečné. Počítač je deterministický přístroj a nelze jej naprogramovat tak, aby vygeneroval skutečný chaos. Zde se jeví nutné používat kvalitní fyzikální generátory náhodných čísel založené např. na šumu diod, ale skutečnou nepředvídatelnost a dokonalý chaos může vytvořit pouze generátor kvantový, vyžívající fyzikálního jevu kvantově mechanického indeterminismu.

Přehled známých útoků na RSA je podrobně zpracována v přehledové studii [14]. Zde jsou popsány základní známé klasické útoky jako: faktorizace modulu, použití stejného modulu ve více klíčích, multiplikativní vlastnosti kryptosystému, malé hodnoty veřejného exponentu (Wienerův útok), malá hodnota soukromého exponentu, šifrování stejné zprávy různými klíči, šifrování příbuzných zpráv jedním klíčem, šifrování stejné zprávy s náhodnou vycpávkou, částečné vyzrazení soukromé informace, útoky na vlastnosti implementace a útoky proti PKCS (Public Key Cryptography Standard).

Jako nejnebezpečnější se v současnosti jeví útok pomocí hrubé síly, faktorizace, který se stal počátkem roku 1999 reálný pro klíče délky 512 bitů, a ty se bohužel stále pro některé komerční aplikace používají. Faktorizaci tak velkých čísel lze provést pomocí paralelního prosévacího přístroje TWINKLE, který představil prof. Adi Shamir na konferenci EUROCRYPT 1999 v Praze. Počáteční implementace realizovala propojení zařízení TWINKLE s metodou QS (kvadratického síta) .

Na poslední konferenci EUROCRYPT 2000 byla ukázána faktorizace RSA-155 s délkou klíče 512 bitů [3], pomocí klasických počítačů a byl vysloven jednoznačný závěr, že RSA s touto délkou klíče již není bezpečná [2].

V posledních letech se zdá, že metoda QS (kvadratického prosívání) je postupně metodou NFS (metoda prosívání číselného tělesa) vytlačována. Obecně se dá říci, že pro malé hodnoty n (řekněme pod n < 100 cifer) je metoda QS rychlejší než NFS. Pro hodnoty n > 130 cifer je lepší síto číselného tělesa. V oblasti čísel od 100 do 130 cifer pak výsledek závisí na druhu použitých počítačů, jemnosti programování a na hledaném tvaru rozkladu. Metoda NFS slaví v posledních letech jednoznačný úspěch při rozkladu velkých těžko rozložitelných čísel. Vzhledem k nesporně lepším výsledkům metody NFS při práci s "velkými" čísly se již celá metoda využití zařízení TWINKLE přepracovala na tuto metodu. Na tomto převodu pracoval vynálezce TWINKELU prof. A.Shamir společně s vynikajícím odborníkem na faktorizaci A.K.Lenstrou. V současnosti je útočeno na faktorizaci čísel větších než 768-bitů v reálném čase.

V této kapitole jsme na modelovém případě se snažili ukázat na možná bezpečnostní rizika související s EP.

Budou-li všechna výše uvedená rizika minimalizována potvrzení správnosti identity podepsané osoby a původnosti textu na konci procesu bude s pravděpodobností v limitě blížící se 1. Klasický počítač nastavený na nějaké bezpečnostní epsilon však vždy rozhodne ano či ne.

V další kapitole se budeme věnovat konkrétnímu případu možného útoku na tzv.“GSM banking“ a potřebě zavedení speciální kontroly v elektronickém bankovnictví.

4. Příklady bezpečnostních rizik ve finančním sektoru ve spojení s EP

Na konferenci Fast Software Encryption Workshop 2000 publikoval Adi Shamir, Alex Biryukov a David Wagner [15] nový útok na silnější verzi šifrového algoritmu A5/1, který se používá ve 130 milionech GSM mobilních telefonů, včetně ČR. Dříve publikovaný útok vyžadoval záznam 2 minut šifrového spojení a následnou analýzou (doba 1 s) byl získán klíč. Nově publikovaný útok umožňuje ze záznamu dvou vteřin spojení získat klíč. Analýza trvá cca 4 minuty a vyžaduje běžné PC (500 Mhz) vybavené 4 pevnými disky, každý o kapacitě 73 GB.

Tato informace v souladu s informací v Intelligence Newsletter dává jednoznačný signál, že telekomunikační bezpečnost GSM je vážně ohrožena. Spojíme-li toto riziko s možností výše zmíněných útoků na čipové karty vzniká značné bezpečnostní riziko pro tzv.“GSM banking“. Uživatelé této služby by měli být o těchto rizicích informováni a minimálně upozorněni na to, že ponechání mobilního telefonu bez dozoru i ve vypnutém stavu je nebezpečné a sdělování klasifikovaných nebo jiných důležitých informací rovněž.

Dalším nebezpečím je možnost tzv. elektronického tunelování pokud není nastaven bezpečnostní mechanismus, který mu zabraňuje. Elektronické peníze jsou virtuální a ve spojení s predikčními programy vývoje kursů akcií, měn apod. lze EP stvrzovat příkazy nákupů a prodejů v takové rychlosti, že peníze zůstávají neustále v elektronické podobě a při zisku je rozšiřováno pouze spektrum transakcí. V konečné fázi jsou pod šifrovou ochranou takto získané virtuální peníze převáděny na účty v zemích s nízkou kontrolou finančního sektoru, či bezcelních oblastí a legalizovány. Investovaný kapitál ze země původu tak mizí, je vykazován jako investiční ztráta , pokud nelze auditem dokázat opak.

5. Závěr

V tomto článku jsme se snažili poukázat na potřebu komplexnosti pohledu na bezpečnost při budování zázemí pro certifikační autoritu a přípravu pro veřejnou akreditaci. Jsme přesvědčeni, že v ČR je co zlepšovat v bezpečnosti z pohledu nových výzkumů u již existujících certifikačních autorit.

Pouze velké firmy v IT s vlastním výzkumem a prostřednictvím svých vysoce kvalifikovaných konzultantů na celém světě disponují hlubokými znalostmi v oblasti PKI (Public Key Infrastructure) a mají rovněž rozsáhlé zkušenosti z reálné implementace těchto systémů ve světě.

Je proto přirozené, že pouze tyto jsou schopny dodávat zcela komplexní dodávku řešení pro komerční certifikační autoritu, zahrnující rovněž přípravu jejího technologického zázemí i celé organizace k procesu žádosti o udělení veřejné akreditace přičemž jsou schopny zabezpečit:

- vstupní audit organizace z hlediska její připravenosti pro realizaci dodávky certifikační autority; tento krok zahrnuje:
  - prověrku bezpečnostní předpisové základny
  - prověrku objektové bezpečnosti
  - prověrku připravenosti pro instalaci technologie CA
  - zpracování kompletní bezpečnostní dokumentace certifikační autority a její harmonické včlenění do celkové bezpečnostní předpisové základny organizace; v rámci tohoto procesu budou m.j. zpracovány**:**
  - certifikační politika,
  - certifikační prováděcí směrnice,
  - havarijní plán včetně plánu obnovy a plánu činnosti po útoku,
  - pracovní postupy pro pracovníky v důvěryhodných funkcích
  - dodávku technologie (HW, SW, kvalifikované služby) pro realizaci IT infrastruktury certifikační autority, umožňující zajistit nepřerušitelný provoz certifikačních služeb (24x365); řešení zahrnuje:
  - vybavení dvou nezávislých výpočetních center certifikační autority (servery, SW, ...),
  - systém pro zálohování a archivaci,
  - systémy pro monitorování provozu a detekci bezpečnostních incidentů,
  - zabezpečení poskytované služby proti narušení z prostředí Internetu,
  - nezbytnou komunikační a jinou infrastrukturu (UPS, ...).
- provozní podporu v požadovaném rozsahu.

Závěrem lze konstatovat, že pokud bezpečnost se nestane klíčovou problematikou integrace v IS ve finančním sektoru v ČR , existují rizika značných ztrát pro naši ekonomiku.

RNDr.Jaroslav Hrubý,CSc. je vědeckým pracovníkem FzÚ AV ČR a řešitelem grantu v oblasti kvantového počítání. Je předsedou odborné skupiny kryptologie při matematické sekci JČMF a byl předsedou kryptologických konferencí PRAGOCRYPT'96 a EUROCRYPT'99. Je členem ISACA a IACR, kde v r.98-99 byl členem předsednictva.
Podílel se v rámci odborné pracovní skupiny SPISu na přípravě zákona o EP a v současnosti je člene pracovní skupiny ÚOOÚ připravující vyhlášku k tomuto zákonu.

Ing.Igor Mokoš, manažer HPC

Literatura

[1] The Directive 1999/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 1999/93/EC, dále dokumentyETSI, http://www.etsi.org/SEC/el- sign.htm,viz. také http://www.uoou.cz.

[2] S. Cavalallar et.al., Factorization of a 512-Bit RSA Modulus, EUROCRYPT 2000, Lecture Notes in Comp.Sci.1807 (2000), p.1.

[3] A.K.Lenstra ,A.Shamir, Analysis and Optimazation of the TWINKLE Factoring Device, EUROCRYPT 2000, Lecture Notes in Comp.Sci.1807 (2000), p.35.

[4] P.Shor,Proc.35th IEEE Symposium on the Foundation of Computers Sci.(1994), p.124; SIAM J.Comp. 26 (1997),p.1484.

[5] L.K.Grover, Proc.28thAnnual Symposium on the Theory of Computing, ACM Press, New York (1996)p.212; Phys.Rev.Lett.78 (1997), p.325; Phys.Rev.Lett.80 (1998), p.4329.

[6] G.Hanaoka et al., Unconditionally Secure Digital Signature Schemes Admitting Transferability,ASIACRYPT 2000, Lecture Notes in Comp.Sci.1876 (2000), p.130.

[7] T.Okamoto et al. Quantum Public-Key Cryptosystems, CRYPTO 2000, Lecture Notes in Comp.Sci.1880 (2000), p.147.

[8] S.H.Weingart, Physical security devices for subsystems: a survey of attack and defenses, Workshop on Cryptographic Hardware and Embedded Systems , Proceedings CHESS 2000 (2000), p.306.

[9] A.Shamir, Protecting smart cards from passive power analysis with detached power supplies, Workshop on Cryptographic Hardware and Embedded Systems , Proceedings CHESS 2000 (2000), p.71.

[10] P.Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, Proceedings of CRYPTO 1996, Springer-Verlag (1996),p104 .

[11]O.Kommerling and M.Kuhn, Design Principles for Tamper Resistant Smart-card Processors, http://www.cl.cam.ac.uk/ mgk25/sc99-tamper[-slides].pdf,Proceedings of USENIX Workshop on Smartcard Technology, USENIX Association (1999), p.9.

[12] P.Kocher, J.Jaffe and B.Jun, Introduction to Differential Power Analysis and Related Attacks, http://www.cryptography.com/dpa/technical/index.html , (1998).

[13]U.Nerurkar,Security Analysis&Design, Dr.Dobb`s Journal,#318 November (2000), p.50.

[14] D. Boneh: Twenty Years of Attacks on the RSA Cryptosystem, Amer.Math.Jour.(1999).

[15] Adi Shamir, Alex Biryukov a David Wagner, http://cryptome.org/a5.ps

[16] Intelligence Newsletter,n.391,12 October (2000).

D. Mobilní telefony (komunikace, bezpečnost)

Jiří Kobelka, student ISŠP Brno

Základní termíny

Terminologie v oblasti mobilních telefonů (mobilních stanic - **MS**) je velice rozsáhlá, ale pro naše potřeby postačí jen krátký přehled některých základních pojmů.

NMT (Nordic Mobile Telephone) analogová síť běžící na 450 Mhz. U nás ji používal Eurotel T!P. NMT je nechráněná a v podstatě k odchytu provozu stačí přijímač na frekvenci 450 Mhz. Tento nedostatek donutil T!P, po vzniku jiných sítí, nabízet své služby velice levně. Výhodou bylo velké pokrytí.

GSM (Groupe Special Mobile) je digitální síť, která funguje na 900 Mhz. Díky šifrování je relativně bezpečný. Data (resp. váš hovor) posílá po paketech (hovor kouskuje na dílky, pakety, a ty pak samostatně posílá příjemci, jeden dílek za asi 4,615 milisekundy), používá se značení rámce (**TDMA** - Time Division Multiple Access).

GSM 1800 má obdobné charakteristiky jako GSM 900. Má trojnásobně zvětšenou kapacitu přenosových kanálů - to dociluje na úkor dosahu (na 1 vysílač GSM 900 připadnou přibližně 4 vysílače GSM 1800).
V tomto článku se budeme zabývat aktuální technologií GSM.

SIM karta

SIM (Subscriber Identification Module - identifikační modul účastníka) je čipová karta. Má obvody i paměť, která obsahuje např. váš telefonní seznam, zabezpečovací algoritmy apod. Bez ní s vámi mobilní telefon odmítne komunikovat. SIM je plně přenositelný na jiný mobilní GSM telefon. SIM karta je pevně svázána s vaším telefonním číslem, a tak si můžete koupit nový mobil, aniž byste byli nuceni měnit číslo.

Základy GSM sítě

GSM síť má Mezinárodní telekomunikační konfederací určena 2 pásma. A sice pásmo 890-915 MHz (pro kontakt od mobilu k BTS; o BTS blíže v sekci "Spojení hovoru"), a pásmo 935-960 MHz (pro spojení od BTS k mobilu). Omezená šířka pásma GSM se dělí na několik rádiových kanálů za pomocí časového a frekvenčního dělení přístupu - **T/FDMA** (Time and Frequency Division Multiple Access). Pomocí frekvenčního dělení se pásmo rozdělí po 200 kHz do 124 přenosových kanálů, z toho jeden i více připadne na jednu BTS. Následně je pomocí časového dělení, každý ze 124 kanálů rozdělen na 8 menších kanálů, tzv. **timeslotů**. Timeslot trvá 0,577 milisekundy. Proto jeden TDMA rámec trvá 4,615 ms (8*0,577). Jestliže má jeden timeslot dorazit k BTS a zpět, je potřeba polovina (0,577/2) a nějaký ten čas pro samotnou techniku přenosu, tedy 0,233 ms. Při znalosti rychlosti šíření rádiového signálu se dá spočítat, že dosah signálu je 70 km. Takže poloměr dosahu BTS je maximálně 35 km. I kdyby byl signál z BTS dostatečný a vy od něj byli 35,8 km, nebudete moci služeb BTS využívat jednoduše proto, že k ní určená data včas nedorazí ("ztratí se..."). V servisním menu mobilu lze nalézt hodnoty time advance (viz. sekce "Lokalizace MS"), které když vynásobíme 547ms, dostaneme vzdálenost od BTS na metry.

Co se děje, když zapnu mobil?

Především začne autentizace MS (k tomu se využívá šifra **A38**, někdy se jí také říká **COMP128**) pro vstup do sítě operátora. Autentizace má za hlavní účel bránit jiné osobě

vydávat se za vás, tedy např. telefonovat na váš účet, někomu z něj sprostě vynadat, vyhrožovat apod. Šifra A38 se používá k označení dvou šifer **A3** a **A8**. Tyto šifry jsou však často implementovány jako jeden modul. Při autentizaci se používá jedinečný tajný klíč, tzv. **K[i]**. Ten se nalézá v SIM kartě, která je proti přečtení K[i] částečně chráněna a dovolí s K[i] pouze právě operace A3/A8. Každý operátor má tzv. autentizační centrum (**AUC**), které také vlastní váš K[i] .
Celý proces vstupu do sítě probíhá následovně: MS požádá o vstup do sítě (login). Síť chce po AUC autentizační triplet (**AT**), což je trojice:
[- náhodné číslo - A3(náhodné číslo, K[i]) - A8(náhodné číslo, K[i])].
Náhodné číslo AUC zašle mobilu (MS), mobil poskytne náhodné číslo SIM kartě, která vytvoří AT' . AT' je opět trojice, tentokráte to je:
[- náhodné číslo - A3(náhodné číslo, K[i])' - A8(náhodné číslo, K[i])'].
MS uloží A8 do SIM karty a odešle výsledek A38 do sítě. Síť porovná AT a AT'. Jestliže nastane situace AT=AT', proběhlo přihlášení do sítě úspěšně. Neúspěšné může být např. v případě, kdy je váš **IMEI** na blacklistu apod. (IMEI – je jedinečné identifikační číslo mobilu; International Mobile Equipment Indentity; na většině mobilů zjistíte IMEI volbou *#06#).
Tím autentizace končí. Pro samotné volání se pak probíhá šifrování spojení pomocí šifry **A5** s klíčem A8, který je při autentizaci uložen do SIM karty.

Spojení hovoru
Síť mobilního operátora (celulární, resp. buňková síť) obsahuje několik aktivních prvků. Tvoří ji mobilní telefon, který si udržuje rádiový (900 Mhz) kontakt s **BTS** (Base Transceiver Station). Tyto základní stanice se umisťují na objektech, stožárech a v budovách (indoor). Dají se dělit dále také podle způsobu vyzařování signálu na všesměrové, směrové a indoor.
Dalšími prvky sítě jsou **BSS** (Base Station Subsystem - subsystém základních stanic) v roli řídícího centra a **NSS** (Network Switching Subsystem - síťový přepínací subsystém) obstarávající přepojování účastníků, ať už vlastních, nebo jiného operátora.
Jakmile vytočíte číslo, je signál předán bráně GSM sítě. Ta si ověří číslo volaného mobilního telefonu, provede vyhledání existence, polohy a stavu. Jestliže je volaný účastník na příjmu, BTS s ním zahájí komunikaci, proběhne zabezpečovací fáze, pokud skončí úspěchem nastane spojení hovoru.

Nyní se podíváme na některé detaily tohoto procesu. Po potvrzení volaného čísla se prověří **IMSI číslo** (International Mobile Subscriber Identity - mezinárodní) v tzv. domovském lokačním registru - **HLR** (Home Location Register, tedy tam, kde jste MS pořídili - pravděpodobně ČR.). Dále si HLR zjistí od návštěvnického lokačního registru - **VLR** (Visitor Location Register, náleží k BTS, při přechodu do dosahu jiné BTS maže údaje o účastníku, návštěvníkovi, ze své databáze), zda číslo existuje a MSR číslo (**MSRN** - Mobile Station Roaming Number). Spojení proběhne přes mobilní spínací ústřednu (**MSC**). VLR dostane požadavek o lokalizaci a stavu MS. Jestliže je MS v dosahu a zapnutá, nastává část spojení. MSC zaktivuje veškeré BSS (subsystémy základních stanic) spadající pod oblast VLR. Volaná MS začne komunikovat s BTS. Proběhne zabezpečení a v případě kladného pořízení, dostává MSC od VLR signál OK. Volaný mobil začne vyzvánět.
Při přetížení sítě mobilního operátora dokáže MS pomocí funkce **frequency hopping** přepínat na méně vytížené kanály, a to až 217x za sekundu. Leckdy při hovoru dochází k tzv. **overhandu**. Ten nastává v okamžiku, kdy MS s aktuální BTS ztrácí signál a přepíná na jinou (pokud je ;-)) BTS se silnějším signálem, tedy provede overhand.

SMS (Short Message Service)
Po odeslání obdrží SMSku nejbližší BTS. Ten ji odešle na **SMSC** (SMS Centrum), které se pokouší ji doručit příjemci pomocí vyhledané jemu blízké BTS. Když toto nelze provést (vypnutý mobil, mimo dosah apod.), pokouší se ji doručit do časového limitu. Časové omezení na doručení lze nastavit, standardně je navoleno 72 hod.

Lokalizace MS
Někteří odborníci tvrdí, že kdyby se zapisovaly polohy všech mobilních telefonů v ČR v intervalu 1O minut, byla by velikost výsledné databáze pouhých 500 GB (současné pevné disky PC mají 30 GB). To by následně mohlo jít využít k onomu pověstnému: kdo, kdy, kde, komu, s kým,....
V důsledku mobility MS je vždy potřeba zjišťovat její pozici. To se zajišťuje buňkovým systémem (jedna buňka =1 BTS). BTS v časových intervalech kontroluje dostupnost MS a vyhodnocuje časovou prodlevu signálu, následně funkcí **time advance** zjistí vzdálenost od vysílající BTS. A protože mobilní telefon při každém požadavku obnovení informací o poloze (**refresh request**) zkouší i sílu signálu vůči ostatním BTS v akčním radiusu, nabízí se možnost porovnání time advance (minimálně 3 BTS - triangulační kvóta). V ČR je něco okolo 2000 vysílačů. To umožňuje na volném neosídleném, ale pokrytém GSM signálem, uzemí lokalizovat MS s přesností přibližně 500 m. Ve městě (oblasti hustě pokryté vysílači) pak na desítky metrů.

Odposlech
Odposlouchávání hovorů není momentálně (nejspíš) v reálném čase možné. Nicméně lze dešifrovat hovor již po nasbírání asi 120 sekund záznamu (takže pro jistotu tak 90 sekund :-) ?). Tato časová délka je nezávislá na výkonnosti počítače, který bude kód lámat. Těch 120 sekund je prostě třeba pro nasbírání potřebného množství vzorků. PC se 128 MB RAM a 2x73 GB harddisky tuto činnost vyřeší za 1 sekundu! Takže přibližně po dobu 90 sekund jste chráněni proti útokům na vaše soukromí. Připomínám, že píši o útoku při odchytu signálu ze vzduchu, nikoliv o možnostech příslušného operátora. Pro nás obyčejné účastníky tak prozatím nehrozí odposlech a sledování, nějakým útočníkem, který nemá možnosti operátorů a snaží se získat informace pouze odposlechem provozu vašeho mobilu. Tohoto útočníka navíc nepotěší měnění frekvence (frequency hopping), které vzniká při vytížení sítě.
Situace se také výrazně mění v případě směrování hovoru na pevnou linku (u nás jedině SPT Telecom), kde poslední článek (klasický telefon) je nezabezpečen a odposlouchávat jej dokáže kdejaký domácí kutil.

Závěr
Česká republika se vyrovnává ve využívání mobilních telefonů vyvinutým zemím. Osobně se domnívám, že za to mohou drahé klasické telefonní poplatky a naopak ceny mobilního vybavení, které v porovnání se světem je poměrně levné.
Osobně vlastním Paegas a musím říci, že operátorky mají docela nízké odborné znalosti problematiky. Na dotaz často odpoví absolutní "pitomost".
Operátoři (EuroTel, RadioMobil, Oskar) také nezcela přesně tvrdí, že pokrývají spoustu procent oblastí, ale v tomto údaji se nepočítá s tím, že byste byli za kopcem či snad ve stíněné budově. Proto při výběru příslušného operátora si nejdříve zjistěte jak je to s jeho signálem v místě vašeho bydliště - jen tak máte zaručený kvalitní příjem signálu.

Prosím o zaslání případných připomínek, dotazů a námětů na e-mail "jksoft@post.cz".

S přáním co nejlepšího signálu, Jiří Kobelka, student ISŠP Brno.

E. NIST software pro statistické testování náhodných a pseudonáhodných generátorů pro kryptografické účely (rozšířená recenze)

Jaroslav Pinkava (AEC spol. s r.o. / Norman Czech Republic)

1. Úvod

V rámci edice „Special Publications“ se v loňském roce (2000 - hlavní dokument byl ještě modifikován 8.prosince 2000) objevil velice zajímavý balík statistických testů v návaznosti na dokument

NIST Special Publication (SP) 800-22: *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*

Význam náhodných a pseudonáhodných čísel v kryptografii je známý a dalo by se říci zásadní. Kritickou informaci kryptografických postupů (z hlediska ochrany dat) tvoří hodnoty klíčů a to platí jak pro symetrickou tak i asymetrickou kryptografii. Aby používání těchto klíčů bylo dostatečně bezpečné, je třeba zajistit vysokou kvalitu metod používaných ke generování hodnot těchto klíčů, tj. vysokou kvalitu příslušných zdrojů náhodných (pseudonáhodných) posloupností. Obdobně je třeba zabezpečovat kvalitní zdroj náhodné posloupnosti pro správnou a především bezpečnou funkčnost celé řady kryptografickcých protokolů.

V současné době je známa celá řada postupů pro testování statistických kvalit RNG (random number generator, česky - generátor náhodných znaků, někdy se užívá také zkratka GNZ) používaných v kryptografii (viz literatura). Přesto zde chyběl jakýsi oficiální reprezentant, norma, tj. definovaný postup, který by umožňoval poskytovat srovnatelné výsledky. Publikace **SP 800-22** tuto mezeru vyplňuje a to na základě komplexního balíku testů zahrnujícího v podstatě veškeré významné současné statistické metody testování vhodné pro kryptografické účely. Nedílnou součástí je i softwarový balík **NIST Statistical Test Suite**, který obsahuje implementace všech popsaných testů (6,5 MB základní software + dalších 43,8 MB dat).

V rámci Serie 800 Special Publications jsou zveřejňovány dokumenty obecného zájmu (http://csrc.ncsl.nist.gov/publications/nistpubs/index.html) pro odborníky z oblasti informační bezpečnosti . Série byla založena v roce 1990 a její aktivity jsou prováděny ve spolupráci s průmyslovými, vládními a akademickými institucemi.

2. Publikace SP 800-22

Výše zmíněný dokument NIST Special Publication 800-22 je poměrně rozsáhlý - zahrnuje celkem 162 stran textu. Obsahuje celkem pět kapitol a třináct příloh (A-M). Práce na přípravě tohoto materiálu se zúčastnilo dvanáct autorů (Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo). Provedeme čtenáře stručně obsahem tohoto dokumentu.

2.1 Úvod do testování náhodných čísel

Autoři nejprve analyzují dva pojmy, které mají pro diskutovanou oblast zásadní význam. Jsou jimi náhodnost a nepredikovatelnost. Odsud a z existující praxe jsou vyvozeny pojmy generátoru náhodných čísel (na bázi fyzikálních zdrojů) a generátoru pseudonáhodných čísel

(používá vstupní data - tzv. seed, která jsou následně transformována deterministickou funkcí). Uvedeny jsou rovněž základní pojmy z problematiky statistického testování (nulová hypotéza, hladina významnosti, zamítnutí hypotézy atd.).

Každý statistický test je založen na vypočtené hodnotě nějaké statistiky, která je funkcí vstupních dat. Statistika je použita k výpočtu tzv. **P**-hodnoty (dle terminologie dokumentu), která shrnuje hodnotu výsledků ve vztahu k nulové hypotéze. V testech, které popisuje daný dokument je každá **P**-hodnota pravděpodobnost, že dokonalý náhodný generátor může vyprodukovat posloupnost méně náhodnou než je testovaná posloupnost. Je volena hladina významnosti α. Pokud je **P**-hodnota větší než toto α, pak je přijata nulová hypotéza (tj. posloupnost se jeví jako náhodná). Pokud **P**-hodnota je menší než dané α, pak nulová hypotéza je zamítnuta (posloupnost se jeví jako nenáhodná). Parametr α označuje také tzv. pravděpodobnost chyby I. druhu (pravděpodobnost, že zamítnu nulovou hypotézu za podmínky, že nulová hypotéza platí).

Vzhledem k testovaným náhodným posloupnostem jsou učiněny tři základní předpoklady:

- *rovnoměrnost* (pravděpodobnost **0** či **1** je právě ½)
- *nezávislost měřítka* (každý test aplikovatelný na posloupnost lze aplikovat i na její libovolnou náhodnou podposloupnost)
- *konzistence* (chování generátoru nezávisí na vstupní hodnotě - seed).

V závěru kapitoly l. je proveden rozsáhlejší přehled použitých pojmů a symbolů.

2.2 Testy generovaných náhodných čísel

Příručka popisuje a přiložený softwarový balík obsahuje následujících 16 základních testů:

1. The Frequency (Monobit) Test,
2. Frequency Test within a Block,
3. The Runs Test,
4. Test for the Longest-Run-of-Ones in a Block,
5. The Binary Matrix Rank Test,
6. The Discrete Fourier Transform (Spectral) Test,
7. The Non-overlapping Template Matching Test,
8. The Overlapping Template Matching Test,
9. Maurer's "Universal Statistical" Test,
10. The Lempel-Ziv Compression Test,
11. The Linear Complexity Test,
12. The Serial Test,
13. The Approximate Entropy Test,
14. The Cumulative Sums (Cusums) Test,
15. The Random Excursions Test, and
16. The Random Excursions Variant Test.

Kapitola 2 obsahuje přitom popis postupu provádění jednotlivých testů (viz následující odstavec).

2.3. Technický popis jednotlivých statistických testů

V návaznosti na 2. kapitolu dále poskytuje kapitola 3. nezbytný matematicko-statistický teoretický fundament k jednotlivým testům a to včetně odkazů na příslušnou literaturu. Uvedeme některé poznámky k jednotlivým testům:

Test 1. Test četností (jednotlivých bitů)

Tento test spočítá četnost **0** a **1** v posloupnosti délky n. Přitom nuly posloupnosti jsou konvertovány na hodnotu **-1**. Je pak spočtena statistika

$$S_n = X_1 + X_2 + ... + X_n ,$$

přitom

$$X_i = 2E_i - 1$$

a E_i je původní posloupnost nula jedniček. Následně je spočtena statistika

$$S = | S_n | / \sqrt{(n)}$$

a **P**-hodnota, která je rovna **erfc (S /√2).** Pokud je tato hodnota menší než α (při statistickém testu na α-procentní hladině významnosti) - přijatý závěr říká, že daná posloupnost není náhodná. V opačném případě má daná posloupnost náhodný charakter (vzhledem k výsledkům daného testu).

Tento test se opírá o klasickou Moivre-Laplaceovu větu o asymptotické normalitě posloupnosti S_n. Funkce erfc je přitom tzv. (komplementární) funkce chyb - určitý integrál od hodnoty **z** do $+\infty$ funkce $(2/\sqrt{\pi}) \exp(-u^2)$.

Test 2. Test četnosti bloků (znaků)

V tomto statistickém testu je vstupní **0-1** posloupnost délky **n** rozdělena na **N** bloků délky **M**. Přitom zde **N** je celá část podílu **n/M**, poslední bity, které již nevytvoří blok délky **M** jsou z výpočtů vyňaty.

V každém **i**-tém bloku délky **M** se spočte počet jedniček π_i **(i=1,...N).** Následně se spočte statisitika chí-kvadrát:

$$\chi^2 = 4M \sum_{i=1}^{N} (\pi_i - ½)^2.$$

Příslušná P-hodnota je spočtena jako **igamc (N/2,** χ^2 **/2),** kde **igamc** je neúplná gama funkce.

Statistika χ^2 má za platnosti nulové hypotézy χ^2 -rozdělení s **N** stupni volnosti. Materiál obsahuje doporučení k volbě hodnoty **M** (předpokládá se, že hodnota **n** je minimálně **100**).. Velikost bloku **M** by měla být volena tak, aby $M \geq 20$, $M > 0.01n$ a $N < 100$.

Test 3. Test serií

Serii je v **0-1** posloupnosti délky n nazýván nepřerušený úsek identických hodnot - maximální velikosti, tj. např. serii nul předchází jednička a následuje rovněž jednička.

V tomto testu je spočtena statistika V, která je rovna počtu serií v **0-1** posloupnosti délky **n**. Poznámka: Pokud nevyšel test četností, není nutné daný test provádět, příslušná **P**-hodnota je položena rovna nule.

Symbolem π označíme počet jedniček v dané posloupnosti. Potom spočteme příslušnou **P**-hodnotu jako

$$\text{erfc}[\, | V - 2n\pi(1-\pi) | / (2\sqrt{((2n\pi(1-\pi)))}\,]$$

Test je založen na chování statistiky **V** (počtu serií). Při daném π má tato statistika asymptoticky normální rozdělení.

Je doporučováno, aby každá testovaná posloupnost měla délku nejméně **100** bitů.

Test 4. Nejdelší serie jedniček v bloku

V tomoto testu zkoumáme nejdelší serie jedniček v **M**-bitových blocích. Posloupnost délky **n** je rozdělena opět jako v testu 2. na **M**-bitové bloky. Následně se spočtou četnosti $\mathbf{v_i}$ nejdelších serií a statistika

$$\chi^2 = \sum_{i=1}^{K} (v_i - N\pi_i)^2 / N\pi_i$$

Hodnoty **K** a **N** mohou být (z hlediska přiložené softwarové realizace množiny testů) následující:

M	K	N
8	3	16
128	5	49
10000	6	75

Test 5. Test hodnosti binární matice

Smyslem testu je objevit lineární závislosti v testované posloupnosti. Opět analyzujeme posloupnost nula jedniček délky **n**. Symbolem **M** označíme počet řádků každé matice, symbolem **Q** označíme počet sloupců každé matice (v softwaru je M=**Q**=32). Pro test je použito celkem **N** bloků délky **MQ** (zbylé bity jsou odstraněny).

Pro každou matici $\mathbf{A_j}$, (**j=l,...,N**) je spočtena hodnost této matice $\mathbf{R_j}$. Symboly $\mathbf{F_M}$ je označena četnost matic s plnou hodností M, symbolem $\mathbf{F_{M-1}}$ je označena četnost matic s hodností **M-1**. Potom $\mathbf{N - F_M - F_{M-1}}$ je počet zbývajících matic.

Následně se spočte statistika

$$\chi^2 = (F_M - 0.2888N)^2 / 0.2888N + (F_{M-1} - 0{,}5776N)^2 / 0.5776N + (N - F_M - F_{M-1} - 0{,}1336N)^2 / 0{,}1336N$$

Výsledná **P**-hodnota je rovna $\exp(-\chi^2/2)$. Je doporučováno aplikovat test na posloupnosti délky minimálně **38MQ** (**38912** v přiloženém softwaru), tj. musí být vytvořeno minimálně **38** matic.

Test 6. Diskrétní Fourierova transformace

Smyslem testu je nalézt potenciální periodicity v analyzované posloupnosti. Je detekován počet vrcholů nad 95% prahem. Postup výpočtu sledované statistiky **d** je následující:

(1) **0-1** posloupnost se transformací **X = 2E -1** převede na posloupnost obsahující hodnoty **1** a **-1**.
(2) Aplikací diskrétní Fourierovy transformace získáme **S = DFT (X).**
(3) Spočteme **M = modulus (S´),** kde **S´** je podposloupnost **S** obsahující prvních **n/2** prvků z **S** a funkce modulus produkuje posloupnost výšek vrcholů.
(4) Spočteme výšku vrcholu pro 95% práh $\mathbf{T} = \sqrt{(3n)}$.
(5) Spočteme $\mathbf{N_0 = 0.95n/2}$ což je teoretický očekávaný počet vrcholů (za předpokladu náhodné výchozí posloupnosti), které jsou pod úrovní **T.**
(6) Spočteme $\mathbf{N_1}$ - aktuální počet vrcholů nižších než **T**.
(7) Spočteme statistiku

$$d = (N_1 - N_0) / \sqrt{(n.(0.95)(0.05)/2)}$$

(8) Spočteme **P**-hodnotu jako $\mathbf{erfc}(|d|/\sqrt{2})$.

Pro aplikování tohoto testu je doporučována minimální délka výchozí posloupnosti 1000.

Test 7. Test shody s nepřekrývající se šablonou

Smyslem tohoto testu je analyzovat počet výskytů určitých předem definovaných bitových řetězců., tj. detekovat generátory vytvářející příliš často určitý (neperiodický) obrazec.

Předpokládáme opět, že pracujeme s **n**-bitovou vstupní **0-1** posloupností, symbolem **m** označíme délku šablony **B**. Dále - **M** označuje délku testované podposloupnosti (v softwaru **M = 2^{17} = 131 072**) a **N** je počet nezávislých bloků (**N=8** v softwaru).

K popisu testu:

(1) rozdělíme posloupnost na **N** nezávislých bloků délky **M**.

(2) Nechť W_j je počet realizací šablony **B** v bloku **j (j=1,...,N).**

(3) Teoretický průměr a teoretický rozptyl jsou dány vzorci:

$$\mu = (M-m+1) / 2^m \qquad \sigma^2 = M [1/2^m - (2m-1) / 2^{2m}]$$

(4) Spočte se statistika

$$\chi^2 = \sum_{i=1}^{N} (W_j - \mu)^2 / \sigma^2$$

(5) **P**-hodnota je dána jako **igamc (N/2, χ^2 /2) -** neúplná gama funkce.

Software obsahuje šablony délek m= 2,3,...,10. Je doporučováno použít hodnotu N≤100.

V programu je předpokládána délka posloupnosti $n=10^6$ a M = 131072.

Test 8. Test shody s překrývající se šablonou

Opět i tento test je zaměřen na vyhledávání určitých stanovených bitových řetězců. Je použito **m**-bitové okno k vyhledávání m-bitových obrazců. K značení: **M** je délka testovaného podřetězce (**M=1032** v softwaru), **N** je počet nezávislých bloků posloupnosti délky **n** (**N=968** v softwaru), **B** je **m**-bitová šablona. K vlastnímu testu:

(1) Výchozí posloupnost rozdělíme na **N** nezávislých bloků délky **M**.

(2) Spočteme počet realizací **B** v každém z **N** bloků.

(3) Spočteme následující teoretické parametry

$$\lambda = (M-m+1) / 2^m \qquad \eta = \lambda /2$$

a s jejich pomocí teoretické pravděpodobnosti π_i **(**i=0,...,5).

(4) Spočteme

$$\chi^2 = \sum_{i=0}^{5} (v_i - N \pi_i)^2 / N \pi_i$$

(5) Spočteme P-hodnotu jako **igamc (5/2, χ^2 /2).**

Každá testovaná posloupnost by měla být nejméně 10^6 bitů dlouhá, hodnota **m** je doporučována **m=9** či **m=10**.

Test 9. Maurerův univerzální statistický test

Smyslem testu je detekce skutečnosti zda výchozí posloupnost může či nemůže být význačně zkomprimována bez ztráty informace. Posloupnost, kterou lze takto zkomprimovat nelze považovat za náhodnou. K parametrům testu: **L** je délka jednotlivých bloků, **Q** je počet bloků v inicializační posloupnosti. V rámci testu je konstruována statistika $\mathbf{f_n}$ (součet dvojkových logaritmů mezi souhlasícími **L**-bitovými šablonami). Výpočet probíhá trochu komplikovaněji a proto odkazujeme čtenáře na samotný článek. Z hodnoty $\mathbf{f_n}$ je pak příslušná **P**-hodnota počítána následovně:

$$= \mathbf{erfc} [| f_n - E(L)) / \sqrt{2}\, \sigma |],$$

kde **E(L)** je střední (očekávána) hodnota při daném **L**, σ je směrodatná odchylka. Tyto dvě hodnoty jsou předpočítány pro **L = 6,...,16**.

Test 10. Lempel-Zivův kompresní test

Smyslem tohoto testu je stanovit jak dalece může být daná posloupnost komprimována. Za tímto účelem je spočten počet různých obrazců v posloupnosti (kumulativně). Posloupnost, kteroulze vyznamně komprimovat považujeme za nenáhodnou. Náhodná posloupnost má přitom určitý charakteristický počet obrazců.

Při délce posloupnosti n je sledovanou statistikou $\mathbf{W_{obs}}$, která je rovna počtu disjunktních a kumulativně různých slov v posloupnosti. **P**-hodnota je počítána následovně:

$$= \tfrac{1}{2}\ \mathbf{erfc}\ [(\mu - W_{obs})/\sqrt{(2)}\,\sigma]$$

Přitom $\mu = 69586.25$ a $\sigma = \sqrt{(70{,}448718)}$. Pokud **P**-hodnota je menší než **0,01**, je činěn závěr, že daná posloupnost nemá náhodný charakter. Je doporučováno, aby testovaná posloupnost měla minimální délku 1 000 000 bitů.

Test 11. Testování lineární složitosti

Smyslem tohoto testu je určit zda daná posloupnost je či není dostatečně složitá (tak, aby mohla být považována za náhodnou). Test je orientován na otázku délky lineárního registru se zpětnou vaznou. Náhodné posloupnosti jsou charakterizovány delšími lineárními registry. Příliš krátký registr indikuje nenáhodnost. Posloupost délky n je rozdělena do bloků délky **M**. Je pevně zvolen počet stupňů volnosti **K= 6** (v softwaru). Sledovanou statistikou je

$$\chi^2\ \mathbf{(obs)}\ ,$$

která charakterizuje, jak se počet pozorovaných shod s lineárním registrem pevné délky shoduje s teoretickým odhadem tohoto počtu, který byl učiněn za předpokladu náhodnosti dané posloupnosti.

Test využívá Berlekamp-Masseyho algoritmus k určení lineární složitosti každého z bloků. Spočtení **P**-hodnoty probíhá dle vzorce $\mathbf{igamc\ (K/2,\ \chi^2\ (obs)/2)}$. Pokud P-hodnota je menší než **0,01**, je činěn závěr, že daná posloupnost nemá náhodný charakter. Je doporučována opět minimální délka analyzované posloupnosti 1 000 000 bitů a hodnota **M** musí splňovat nerovnost $\mathbf{500 \le M \le 5000}$.

Test 12. Test překrývajících se m-znaků

Obsahem testu je stanovení počtu všech překrývajících se obrazců délky **m** v průběhu celé posloupnosti. Následně je pak tento počet porovnáván s teoretickou hodnotou získanou za předpokladu náhodné výchozí posloupnosti – zde každý obrazec má stejnou pravděpodobnost (při **m=1** dostáváme test četností – Test 1).

Pro posloupnost délky **n** zkoumáme hodnotu statistik

$$\nabla\psi^2_m\mathbf{(obs)} \quad \text{a} \quad \nabla^2\psi^2_m\ \mathbf{(obs)},$$

to jsou míry shody pozorovaných a teoretických četností, tyto míry mají χ^2 –rozdělení. Na jejich základě jsou opět konstruovány příslušné **P**-hodnoty a test je prováděn na jednoprocentní hladině významnosti. Tj. pokud obě **P**-hodnoty jsou větší než **0,01**, pak je činěn závěr, že daná posloupnost je náhodná.

Z hlediska volby parametrů je stanoveno doporučení, že **m** by mělo být menší než číslo **L-2**, kde **L** je největší celé číslo menší než dvojkový logaritmus **n** (tj. celá část tohoto čísla).

Test 13. Testování přiblížení entropie

Stejně jako u předcházejícího testu obsahem testu je stanovení počtu všech překrývajících se obrazců délky **m** v průběhu celé posloupnosti. Zde je testována četnost překrývajících se bloků dvou sousedních délek (**m** a **m+1**) ve vztahu k očekávané četnosti – při předpokladu náhodnosti výchozí posloupnosti. Sledovanou statistikou je

$$\chi^2\ \mathbf{(obs)}\ ,$$

tato charakterizuje tuto shodu. P-hodnotu spočteme jako **igamc (2^{m-1}, χ^2 (obs)/2).** Pokud získaná hodnota je menší než 0,01, činíme závěr o nenáhodnosti dané posloupnosti. Z hlediska volby délky bloků platí shodné omezení jako v předešlém testu.

Test 14. Test kumulativních součtů

V rámci tohoto testu ověřujeme zda maximální odchylka (od nuly) v průběhu náhodné procházky definované jako kumulativní součet hodnot **–1** a **+1** posloupnosti (poznámka – nula jedničkovou posloupnost převádíme na posloupnost hodnot **–1** a **+1** zjevným způsobem).
Testovanou statistikou je tedy **z** – ona maximální odchylka. Test lze provádět ve dvou módech – a to buď vzhledem k výchozí náhodné posloupnosti nebo vzhledem k jejímu zrcadlovému odrazu, tj. fakticky pozpátku od posledního bitu. Test lze aplikovat na posloupnosti již od délky 100 bitů.

Test 15. Náhodná procházka

Tento a následující test zkoumají vlastnosti náhodné procházky (konstruované shodným způsobem jako v testu 14). Počítáme počet cyklů, které mají právě **K** návštěv v průběhu získané náhodné procházky. Cyklem přitom je rozuměn úsek náhodné procházky začínající a končící nulovým stavem, mezilehlé stavy jsou nenulové. Testujeme zda získaný výsledek odpovídá situaci, kdy vstupní posloupnost má náhodný charakter. Sledují se počty návratů do osmi nenulových stavů : **-4, -3, -2, -1** a **1, 2, 3, 4**. Celkem máme zde tedy vlastně osm různých testů.
Sledovanou statistikou je

$$\chi^2 \text{ (obs)},$$

(pro daný stav) tato charakterizuje shodu teoretických a experimentálních hodnot – statistika má χ^2 –rozdělení. Potom pro každý ze stavů x spočteme **P**-hodnotu jako
igamc (5/2, χ^2 (obs)/2), testujeme opět na jednoprocentní hladině významnosti. Pro tento test je doporučována minimální délka posloupnosti 1 000 000 bitů.

Test 16. Náhodná procházka - test variant

V rámci tohoto testu sledujeme kolikrát byl jeden určitý stav navštíven během náhodné procházky (výše popsané). Přitom toto sledujeme a statistické závěry konáme vždy pro jeden určitý stav **x**. Sledovanými stavy jsou **-9, -8, …, -2, -1** a **1, 2, …, 8, 9**. Celkem se tedy jedná o osmnáct testů. Při daném stavu **x** je sledována statistika

$\xi(x)$

mající tzv. polonormální rozdělení (pokud náhodná veličina **Y** má normální rozdělení, pak **|Y|** má polonormální rozdělení – terminologie je v různých knihách různá). **P**-hodnoty jsou počítány následovně:

$$= \text{erfc}\left[|\xi(x) - J| / \sqrt{(2J(4|x| - 2))}\right]$$

Opět je doporučována minimální délka posloupnosti 1 000 000 bitů.

2.4. Strategie testování a interpretace získaných výsledků

V rámci kapitoly 4 jsou diskutovány tyto tři základní okruhy otázek:
- strategie statistické analýzy generátoru náhodných čísel,
- interpretace empirických výsledků získaných použitím NIST Statistical Test Suite (NSTS),

obecná doporučení.

K prvnímu bodu. Strategie testování je rozdělena do pěti základních bodů:
1. Volba generátoru (jako příklad jsou zde uváděny generátory z ANSI X9.17 a FIPS 186 - doporučuji však věnovat pozornost generátoru Yarrow Bruce Schneiera)
2. Vygenerování binární posloupnosti (generujeme m binárních posloupností délky n)

3. Aplikace NSTS na soubory z bodu 2 (jsou vybrány statistické testy a vstupní parametry těchto testů - jako jsou např. délky bloků atd.)
4. Výpočet P-hodnot pro každý statistický test
5. Zhodnocení získaných výsledků

K bodu dva - interpretace empirických výsledků. Typické jsou následující tři situace po provedení konkrétních testovacích postupů:
A. Analýza P-hodnot neindikuje žádné odchylky od jejich náhodného charakteru
B. Tato analýza zřetelně indikuje nenáhodnou odchylku
C. Výsledkem není zřetelná situace.

Třetí bod - obecná doporučení obsahuje přehled možných objasnění situací, ve kterých statistické testy neproběhly úspěšně (nesprávně naprogramovaný software, nesprávně užitý statistický test, nesprávná implementace GNZ, nesprávně napsaný software pro sběr dat z GNZ a špatné rutiny pro výpočet **P**-hodnot, nesprávná volba vstupních hodnot - délka posloupnosti, velikost výběru, velikost bloku a volba vhodných šablon).

V závěru kapitoly se autoři zabývají možnými závislostmi mezi jednotlivými testy. Na základě provedené analýzy autoři dovozují charakter závislosti určitých testů v NSTS (obsahující celkem 161 dílčích testů!). Metodami faktorové statistické analýzy - jak autoři tvrdí - bylo prokázáno, že existuje celkem 161 faktorů ovlivňujících výsledky testů. Toto číslo je rovno počtu dílčích testů. Autoři tak dovozují, že duplikace mezi testy jsou velmi malé.

2.5. Příručka pro uživatele

Tato kapitola popisuje jak správně používat statistické testy implementované v přiloženém softwaru.

Balík je určen především k testování (pseudo)náhodných generátorů (P)RNG z hlediska charakteru dosažené náhodnosti. Lze ji používat:
- k identifikaci (P)RNG, které produkují slabou binární posloupnost (z hlediska náhodnosti)
- k návrhu nové (P)RNG
- k verifikaci, že implementace (P)RNG je správná
- k analýze (P)RNG z norem
- k analýze stupně náhodnosti v současné době používaných (P)RNG

Zdrojový kód byl napsán v ANSI C (nezávislost na platformě, je však možné, že bude nutné provést některé modifikace ve vztahu ke konkrétní platformě a kompilátoru). Uživatel může používat vlastní matematické moduly. Lze zavést i nové statistické testy. Soubor testů lze použít jak pro PRNG, tak i RNG a šifrovacím algoritmům. Z hlediska časové náročnosti by měly být jednotlivé algoritmy dostatečně efektivní.

V další části kapitoly je popisován přesný postup pro instalaci softwaru na pracovní stanici. Data mohou vstupovat dvěma základními cestami. Uživatel může na základě výstupu z RNG vytvářet soubory libovolných délek v libovolném množství. Soubory mohou obsahovat binární posloupnost uloženou jako znaky ASCII (nuly a jedničky) nebo jako hexadecimální znaky uložené v binárním tvaru. Na tyto soubory lze pak aplikovat softwarový balík testů.

Pokud vznikne problém s ukládáním dat, lze referenční implementaci modifikovat. Bitový řetězec lze pak uložit přímo v „epsilon“ datové struktuře obsahující binární posloupnost.

Výstup výsledků je uložen v dvou souborech *stats* a *results* (první obsahuje informaci o použitých statistikách, parametrech testů atd., druhý pak o získaných P-hodnotách pro každý aplikovaný test).

K balíku je přiloženo pět testovacích souborů dat. Čtyři z nich byly vygenerovány programem *Mathematica* jako binární rozvoj několika klasických čísel.

Ve zbývající části této kapitoly jsou popsány některé další vlastnosti softwaru (struktura modulů, vlastnosti některých parametrů softwaru, implementované matematické funkce, komunikace se softwarem a interpretace výsledků).

2.6. Přílohy

V přílohách jsou obsaženy další potřebné technické detaily:

A.Výpočet hodnosti binární matice (zde je uveden použitý algoritmus).
B. Podrobnosti k zdrojovému kódu (pomůcky při ladění)
C. Empirické výsledky dosažené z přiložených dat (výsledky testování pěti přiložených souborů dat - P-hodnoty)
D. Konstrukce neperiodických šablon
(pro **m=2,...,21** byly předpočítány všechny neperiodické šablony - k testu 8).
E. Generování rozvoje iracionálních čísel v binárním tvaru (program pro *Mathematicu*)
F. Některé numerické algoritmy (výpočty hodnot speciálních funkcí jako neúplná gama funkce)
G. Hierarchie struktury adresářů (popsána struktura adresářů NIST Statistical Suite)
H. Vizualizační postupy (pro diskrétní Fourierovu tansformaci, přibližnou entropii a profil lineární složitosti)
I. Postupy pro přidání dalších testů (jak přidat další testy do balíku)
J. Postupy pro včlenění dalších GNZ (jak přidat další RNG)
K. Uživatelské grafické rozhraní (GUI obsažené v zdrojovém kódu rng-gui.tcl)
L. Popis referenčních pseudo GNZ (v této příloze je uvedeno devět obsažených PRNG:
- generátor na bázi lineární kongruence
- generátor na bázi kvadratické kongruence I+II
- generátor na bázi kubické kongruence
- exclusive OR generátor (lineární registr délky 127 bitů)
- modulární umocňování - využit DSS
- generátor na bázi SHA-1
- Blum-Blum-Shubův generátor
- generátor Micali-Schnorra

k těmto generátorům jsou pak v tabulce shrnuty výsledky jejich testování)
M. Odkazy na literaturu (třináct titulů)

3. Závěrečné poznámky

Pokud se týká konkrétního výběru testů pro *NIST Statistical Test Suite*, pak z hlediska současných poznatků v této oblasti je možné konstatovat, že tento výběr zahrnuje prakticky všechny důležité používané metody testování významné z hlediska kryptografické praxe. Jeden z dalších možných přístupů (zde neobsažených) lze zkonstruovat na bázi prediktoru následujícího bitu posloupnosti - viz Cryptonessie, prosincové číslo Crypto-Worldu.

Vzhledem k oblasti samotných RNG - zde v dnešní době neexistuje exaktní norma pro vytváření (P)RNG, i když věřím, že něco takového se v dohledné době objeví. V současnosti jsou zkušenosti s některými modely RNG, jako jsou algoritmy zmíněné v příloze L. Pro konstrukci komplexního RNG to však nestačí. Je třeba řešit i otázku vzniku vstupních parametrů těchto generátorů, jejich dynamické modifikace atd. Zatím nejdále v tomto směru postoupila asi konstrukce B. Schneiera a jeho spolupracovníků - generátor Yarrow.

Opublikováním SP 800-22 se dostal široké veřejnosti do rukou vysoce kvalitní nástroj statistického testování. Jeho velkou výhodou je i zmíněná možnost jednotného přístupu k statistickým metodám Možná se někdo i v ČR ujme praktického ověření vlastností tohoto balíku a své zkušenosti sdělí zainteresované veřejnosti.

Literatura:
[1] Schneier, Bruce: RNG Yarrow (http.//www.counterpane.com)
[2] Knuth, D.: The Art of Computer Programming, Vol 1-3,
Addison-Wesley Reading, Massachusetts, 1997, 1998
[3] Tesař, Petr: Přednáška na semináři Vojenská kryptografie, listopad 2000
[4] G. Marsaglia: DIEHARD Statistical Tests
http://stat.fsu.edu/~geo/diehard.html

F. Letem šifrovým světem

Informace pro odběratele e-zinu. Prosím nepřehlédněte změnu e-mail spojení!
Mé nové adresy jsou pavel.vondruska@uoou.cz nebo vondruskap@uoou.cz .
Adresa pavel.vondruska@post.cz zůstala zachována.

1. (Reuters, 7.2.2001) Papež Jan Pavel II. zvažuje vyhlášení svatého patrona pro Internet. Mohl by se jím stát svatý Isidor ze Sevilly. Tento svatý muž žil v sedmém století našeho letopočtu. Napsal první encyklopedii (Ethymologies), v níž shrnul veškeré tehdejší poznatky z medicíny, matematiky, historie a teologie.

2. (USA Today, 6.2.2001) V naší soutěži (9/2000 - 12/2000) jsme vás seznámili i se steganografií. Tohoto systému použili i extrémisté ze skupiny známého teroristy Usáma bin Ládina k předávání zakódovaných zpráv. Zasílání e-mailů mezi členy skupiny z pochopitelných důvodů nebylo možné (řada členů byla hledána). Šifrování v takovém případě také není vhodné - sice pomůže utajit obsah komunikace, ale současně upozorňuje, že subjekty komunikace se snaží obsah své komunikace utajit. Toto může vést ke "kontrole" , kdo se za šifrovou komunikací na internetu skrývá. Skupina Usáma bin Ládina postupovala proto jinak. Informaci (zprávy, mapy, pokyny) zašifrovali přímo do obrázku (zpravidla pornografického obsahu). Tento obrázek pak umístili na některou z populárních pornografických www stránek. Odtud si informaci příjemce jednoduše stáhl a obsah dekódoval. Vzhledem k tomu, že tyto stránky jsou denně navštěvovány i desítkami tisíc návštěvníků - dařilo se utajit kontakt příjemce a "odesílatele". Celý systém odhalila zpravodajská služba CIA. Další detaily lze získat ze zápisů soudního líčení s Usámem bin Ládinem. Tyto zápisy jsou dostupné na http://www.cryptome.org

3. Známý mladý kryptolog Daniel Bleichenbacher - Bell Labs - (o jeho útoku na PKCS #1 jsme psali v minulém čísle) našel díru v náhodném generátoru pro DSA (dle FIPS 186-2, Appendix 3). Podle jeho závěrů takto sestrojený generátor neprodukuje náhodná čísla se stejnou pravděpodobností! Z jedné oblasti (range) je dvakrát pravděpodobnější získat náhodné číslo než z jiné oblasti (bohužel zdrojem je jen článek obsahující pouze výše uvedenou nepřesnou charakteristiku):
http://www.infoworld.com/articles/hn/xml/01/02/05/010205hndsa.xml?p=br&s=6

Nedostatek představuje ohrožení bezpečnosti pouze za předpokladu, že bude využit veliký výpočetní potenciál. NIST přesto ohlásilo opravu normy. Tato oprava má být publikována do konce února.

4. Začátkem tohoto měsíce proběhla několika médii neuvěřitelná zpráva : RSA je rozbito !
   http://www.zdnetasia.com/news/dailynews/story/0,2000010021,20178050,00.htm
   Jenže pak se objevily další články, které se kriticky vyjadřovaly k metodě mladého Filipínce van Lopeze. Diskusi ukončilo zveřejnění korespondence mezi Rivestem (jeden ze tří tvůrců RSA) a Lopezem. Z této korespondence plyne, že metoda je použitelná pouze pro malá čísla. Ve skutečnosti je zveřejněná metoda pomalejší než faktorizace modulu pomocí pokusů s postupným dělením (viz. teorie složitosti).

5. Pokud máte zájem o elektronické vydání známé knihy : "Underground: tales of hacking, madness and obsession on the electronic frontier" , stačí si ji jednoduše stáhnout z adresy http://rubberhose.sourceforge.net/underground

6. Ve čtvrtek 15.2.2001 proběhne tisková konference, kterou pořádá Národní bezpečnostní úřad a Microsoft. Veřejnosti na ní bude poprvé oficiálně představen kryptografický prostředek CSP-I MicroCzech. Využívání tohoto prostředku je vyhrazeno pro potřeby orgánů státu. Je určen pro začlenění do subsystému CryptoAPI v prostředí Windows NT 4.0. Bude používán pro ochranu informací na stupeň utajení „Vyhrazené“. Jeho nasazení bylo otestováno s aplikacemi MS Outlook a MS Internet Explorer. Předpokládá se také produkce vlastních aplikací, které budou tento produkt využívat. Tento modul by mohl tvořit i základ bezpečného prostředku pro vytváření a ověřování elektronických podpisů. Jako jeden z těch, kteří se na vývoji modulu podíleli, vám tento produkt představím v příštím čísle Crypto-Worldu.

7. O čem jsme psali před rokem ?
   Crypto -World 2/2000
   http://www.mujweb.cz/veda/gcucmp/casop2/Crypto2_00.html

   A.Dokumenty ve formátu PDF (M.Kaláb)
   B.Kevin Mitnick na svobodě (P.Vondruška)
   C.Velká Fermatova věta (historické poznámky) (P.Vondruška)
   D.Fermat Last Theorem (V.Sorokin)
   E.Zákon o elektronickém podpisu otevírá cestu do Evropy ?
   (Souček,Hrubý,Beneš,Vondruška)

G. 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

Pokud máte zájem o zasílání tohoto sešitu, můžete se 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, informace

pavel.vondruska@uoou.cz alias **vondruskap@uoou.cz**

pavel.vondruska@post.cz