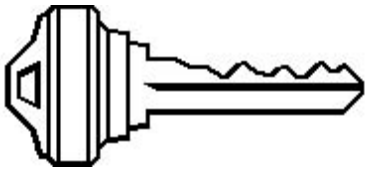
Crypto-World 9/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
Uzávěrka 7.9.99
(25 e-mail výtisků)



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny). Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

A. Nový šifrový standard AES

AES (Advenced Encryption Standard) – algoritmus, který má nahradit dosavadní standard DES . Jaký je vlastně aktuální stav ve vyhledávání nového šifrového standardu?

Historie :
1997 – americká vláda (přesněji NIST) vypisuje „soutěž“ na vytvoření nového komerčního standardu pro symetrické šifrování
1998 , červen – uzávěrka pro podání návrhu, celkem bylo předloženo 15 kandidátů (CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH) , NIST rozhodne vyhodnotit tyto návrhy a přijmout do dalšího kola jen 5 kandidátů
1998, srpen – první konference , kde se hodnotí podané návrhy (Californie, USA)

1999, duben – druhá konference (Řím, Itálie), rozhodnuto, že konec připomínek k jednotlivým algoritmům bude v červnu 1999
1999, srpen – NIST ohlašuje výběr následujících kandidátů:

1) **Mars** – vytvoření rozsáhlým týmem odborníků IBM (reprezentován Nevenko Zunicem)
2) **Rijndael -** připravil vynikající tým belgických kryptologů (Vincent Rijmen, Joan Daemen)
3) **RC6** – od RSA Data Security (Burt Kaliski, podílel se i slavný Ron Rivest)
4) **Serpent** – navržený trojicí velice známých kryptologů - Ross Andrsonem, Eli Bihamem, Lars Knudsenem
5) **Twofish** – návrh firmy Counterpane System (prezident firmy Bruce Schneier)

(Pozn. s většinou uvedených kryptologů - jste se mohli osobně setkat v Praze letos v květnu na konferenci Eurocrypt´ 99 . Barevnou fotku všech účastníků konference si lze u mne zdarma vyzvednout).

NIST publikovalo velice rozsáhlou zprávu (52 stran), ve které zdůvodňuje výběr těchto kandidátů, a proč nebyly přijaty ostatní algoritmy. Tato zpráva je k dispozici na adrese :

http://csrc.nist.gov/encryption/aes/round2/round2.htm#NIST

Dalším krokem bude výběr ze zbývajících kandidátů.

Dohodnutý časový harmonogram:

1) Na „7-th Fast Software Encryption workshopu“ v dubnu roku 2000 budou komentovány vlastnosti uvedených kandidátů.
2) Připomínky bude dále možné na NIST předkládat do 15.května roku 2000 a potom NIST ohlásí, který z algoritmů se stál jediným kandidátem na nový komerční standard.
3) AES dále bude podroben formálnímu vládnímu schvalovacímu procesu a výsledky budou zpracovány ve FIPS (Federal Information Processing Standard).
4) Pokud vše proběhne úspěšně, tak v létě roku 2001 bude ohlášen nový standard šifrového algoritmu pro všechny komerční mezinárodní aplikace.

Připomeňme závěrem, že vybraný standard má být velice flexibilní, lehce implementovatelný, má pracovat s 32-bitovým mikroprocesorem, 64-bitovým procesorem, ale i 8-bitovým (v tzv. režimu smart card). AES má být 128-bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Výběr takového algoritmu, který je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty) není opravdu lehký. Autoři tvrdí , že nově vzniklý standard by snad mohl být standardem pro celé 21-století !

Pokud chcete zaslat nějaké komentáře nebo připomínky k výběru kandidátů , případně ukázat jejich slabost (!), lze je odeslat do NIST dokonce pomocí e-mailu. Přesné instrukce najdete na :
http://www.nist.gov/aes

B. O novém bezpečnostním problému v produktech Microsoftu

1.Historie
Na konferenci CRYPTO v létě roku 1998 oznámil britský kryptolog Nicko van Someran, že při analýze zdrojového kódu Windows - bezpečnostního driveru ADVAPI.DLL, který kontroluje povolení bezpečnostních funkcí včetně Microsoft Cryptographic API (MS-CAPI), objevil, že driver obsahuje dva různé klíče. Jeden slouží Microsoftu ke kontrole (podpisu) použití kryptologických funkcí a ve svém důsledku ke kontrole U.S.exportu silných kryptologických funkcí. Existenci druhého klíče nedokázal objasnit.
Na letošní konferenci CRYPTO ´99 v Santa Barbaře oznámil kanadský matematik Andrew Fernandez, že při analýze service Packu 5.0 pro Windows NT 4.0 získal pomocí odšifrování pomocných debugging informací v souboru _CProvVerifyImage@8 interní označení obou dvou výše jmenovaných klíčů. Jeden z klíčů se jmenuje _KEY a druhý _NSAKEY. Tato skutečnost vyvolala na internetu debatu a spekulace o tom, že Microsoft umožnil NSA pomocí zadních vrátek vstup k právě choulostivému modulu, který slouží k šifrování. Spekulace vycházely především z názvu pro druhý klíč a z nedávno odhalené aféry, kdy známý výrobce šifrových zařízení Crypto AG ve svých výrobcích zadní vrátka pro NSA měl. Microsoft proto 3.9.1999 reagoval oficiální tiskovou zprávou, ve které vysvětluje, že se jedná pouze o záložní klíč, a protože slouží ke kontrole exportu silné kryptografie, která podléhá kontrole vlády, byl "vhodně" nazván _NSAKEY.

2. Odhalení názvu druhého klíče

Uvedený postup provedl Andrew Fernandez z firmy Cryptonym a je popsán např. v dokumetu uloženém na (http://www.cryptonym.com/hottopics/msft-nsa.html)

Před zavedením CSP	v	ADVAPI32.DLL
adresa 0x77DF5530	->	A9 F1 CB 3F DB 97 F5 ... ...
adresa 0x77DF55D0	->	90 C6 5F 68 6B 9B D4 ... ...

Po dešifrování pomocí algoritmu RC4		dostaname
A2 17 9C 98 CA	=>	R S A 1 ... 00 01 00 01 ... (+veřejný klíč)
A0 15 9E 9A CB	=>	R S A 1 ... 00 01 00 01 ... (+veřejný klíč)

Service Pack 5 pro NT4.0		v debugging symbolech v modulu ProvVerifyImage@8"
Adresa 0x77DF5530	<-	mají data označení "_KEY"
Adresa 0x77DF55D0	<-	mají data označení "_NSAKEY"

3. Bezpečnostní problém v systému Windows
Bez ohledu na to, co existence druhého klíče s "podezřelým" názvem znamená, je nutné se podívat, jaké jsou možné důsledky tohoto faktu.
Existence dvou klíčů je prokázána v následujících verzích Win95 SR2, Win98, Win98gold, WinNT4 (všechny verze) a Win2000 (sestavení 2072, RC1). Ve Win2000 byly nalezeny dokonce tři klíče, k tomuto faktu zatím nebylo vydáno žádné oficiální prohlášení.

K čemu vlastně slouží klíč v systému Windows? Microsoft CryptoApi povolí ISVs (Independent Software Vendors) dynamické natažení CSPs (Cryptographic Service Providers) po ověření, že je digitálně podepsán klíčem Microsoft. Pokud CSPs není podepsán nelze použít šifrové rozhraní. Toto bylo zavedeno v souvislosti s kontrolou exportu kryptografie z USA. Jestliže někdo chce nahradit CSPs vlastním rozhraním nebo rozhraním s delšími-silnějšími klíči, musí být toto rozhraní podepsáno digitálním podpisem Microsoftu a to jej udělí jen, je-li použití poveleno v souladu s restrikcemi americké vlády.
Pokusy, které v posledních dnech byly provedeny, ukázaly, že CSPs nemusí být podepsán prvním klíčem (ozanačení KEY), ale k povolení načtení do paměti stačí podpis _NSAKEY. Dále se prokázalo, že veřejný klíč _NSAKEY lze nahradit jiným veřejným klíčem, a pokud je soukromým klíčem podepsán modul CSPs, lze jej provozovat.

4. Popis bezpečnostního útoku
Útok 1 (neúspěšný):
Použít vlastní CSP podepsané soukromým klíčem.
Přepsat "_KEY" vlastním odpovídajícím veřejným klíčem...
... Windows přestanou pracovat, neboť nemohou ověřit vlastní bezpečnostní podsystém

Útok 2 (úspěšný !) :
Použít vlastní CSP podepsané soukromým klíčem.
Přepsat "_NSAKEY" vlastním odpovídajícím veřejným klíčem...
... Windows pracují dále, neboť k ověření bezpečnostního subsystému je k dispozici _KEY (klíč Microsoftu)

CSP pracuje, protože Windows se pokusily jej verifikovat užitím "_KEY" a protože byly neúspěšné, pokusily se je verifikovat pomocí "_NSAKEY" (obsahuje již náš veřejný klíč).

Výsledek:
Windows CryptoAPI systém je funkční
klíč _NSAKEY je odstraněn
uživatel může použít CSP, bez podpisu klíčem _KEY (Microsoftu) nebo vlastníkem klíče _NSAKEY (Microsoft / NSA ?)

Že uvedený útok je reálný potvrzuje již zveřejněný program na serveru firmy Cryptonym, který si lze pro demonstrační použití dokonce stáhnout. Program je určen pro Windows NT 4.0.

5.Závěr
Vzhledem k uvedenému útoku plyne, že:
- Microsoft ztratil možnost kontrolovat použití silné kryptografie ve svých produktech. Přesněji - uživatel může použít vlastní CryptoApi bez podpisu firmou Microsoft a tedy bez ohledu na exportní omezení a jeho kontrolu americkou vládou.
- Potenciálně je možné ve vašem počítači nahradit _NSAKEY jiným klíčem a nahradit CryptoApi jiným CryptoApi, podepsaným výše zmíněným vnuceným klíčem. Toto nové CryptoApi může mimo předchozích funkcí vykonávat i jiné nedokumentované úkoly, které mohou sloužit útočníkovi k získání cenných informací o datech na vašem počítači

Literatura:

1. Tiskové prohlášení firmy Microsoft 3.9.99
   www.micosoft.com/presspass/press/1999/sept99/rsapr.htm
2. The New York Times, September 4, 1999 , John Markoff, A Mysterious Component Roils Microsoft http://www.nytimes.com/library/tech/99/09/biztech/articles/04soft.html
3. The New York Times, September 4, 1999 , Peter Wayner, Why a Small Software Label Raised Eyebrows , http://www.nytimes.com/library/tech/99/09/cyber/articles/04soft-side.html
4. Duncan Campbell, NSA Builds Security Access Into Windows
5. A. Fernandez, Microsoft, the nSA, and You
   http://www.cryptonym.com/hottopics/msft-nsa.html
6. R. Cooper, Is the NSA in Microsoft - Who killed JFK?
   http://ntbugtraq.ntadvice.com/default.asp?sid=1pid=47&aid=52
7. S. Kettmann, J. Glave, MS Denies Windows "Spy Key"
   http://www.wired.com/news/news/technology/story/21577.html

A další …

C. HPUX a UNIX Crypt Algoritmus

HPUX je šifrový algoritmus implementovaný v operačním systé mu Solaris a Crypt je šifrový algoritmus implementovaný v operačním systé mu UNIX. Ve skutečnosti se jedná o stejné algoritmy. V manuálech k těmto operačním systé mům můžeme najít úplně rozdílné hodnocení těchto systé mů !

V manuálu Solaris 2.6 Crypt můžeme číst : „ crypt je implementací jedno-rotorové ho zař ízení založené ho na bázi německé ho př ístroje Enigma, ale s 256-elementy rotoru. Metody útoku na takový to algoritmus jsou obecně známy, crypt poskytuje jen minimální bezpečnost.“
V manuálu HPUX 10.20 můžeme číst : „ crypt je implementací jedno-rotorové ho zař ízení založené ho na bázi německé ho př ístroje Enigma, ale s 256-elementy rotoru. Metody útoku na takový to algoritmus jsou známé , práce, které je tř eba vzít do úvahy s těmito útoky, jsou však velmi rozsáhlé .“
Čteme-li manuál HPUX dále , najdeme vyjádř ení, že crypt chrání adekvátním způsobem vaše soubory. Je smutné , když šifrový algoritmus, který umí „breaknout“ (rozluštit) každý student kryptografie za domácí úkol, je doporučen dodavatelem operačního systé mu k ochraně dat!
http://www.counterpane.com

D. Letem "šifrový m" světem

1) Na adrese
http://www.ntsecurity.net/forums/2cents/news.asp?IDF=118&TB=news
je uvedeno tvrzení, že šifrový algoritmus EFS (Encrypting File Systé m) vestavěný do Microsoft Windows 2000 byl „rozbit“. Microsoft ve své odpovědi tvrdí, že systé m samotný nebyl „rozbit“, ale bylo využito toho, že uživatelé systé m špatně používají (jedná se o možnost využití EFS recovery key) …
http://www.microsoft.com/security/bulletins/win2kefs.asp

2) Objevila se nová verze známého viru Melisa. K šíření využívá slabin Microsoft Outlook. Vir ničí operační systém Windows. Na internetu najdeme jízlivé komentáře, které dodávají, že práce, kterou Melisa provádí je "chytrá a aktuální ".
http://www.computerworld.com/home/print.nsf/all/990719B50A

3) V Kalifornii byla přijata nová verze zákona o digitálním podpisu. Digitální podpis je nyní uznáván jako podpis, který lze právně použít k podpisu obchodních kontraktů .
http://www.computerworld.com/home/news.nsf/all/9907294dig

4) Útok "hrubou silou" (totální zkoušky klíčů) na soubor zašifrovaný pomocí programu ZIP je samozřejmě možný (odmyslíme-li otázku strojového času) a jednoduchý (na internetu je spousta programů, které lze úspěšně použít. Na níže uvedené adrese se však objevila novinka, která využívá možnosti útoku ze znalosti otevřeného textu (known-plaintext attack). Velice zajímavé je, že k útoku stačí znalost 13-ti bytů ! Zájemci mohou navštívit adresu :
http://www.unix-ag.uni-kl.de/~conrad/krypto/pkcrack.html a pokud vlastníte 30 ecash (digitálních peněz) můžete si stáhnout verzi pro UNIX nebo DOS.

5) Po úspěšném útoku hackerů na poštovní server Microsoftu koncem minulého měsíce se řada lidí ohlíží po jiném "bezpečném" poštovním serveru. Vzhledem k tomu, že hackeři stáhli úplný seznam všech uživatelů včetně hesel a vzhledem k tomu, že pro zapomnětlivé je na Hotmailu přímo vestavěná možnost jak heslo (při znalosti jistých údajů o majiteli účtu) získat, rozhodl jsem se tuto adresu vyškrtnout ze seznamu mnou používaných adres. Současně doporučuji používat pro důvěrnou poštu následující server : "Hushmail".
Hushmail je typu serveru Hotmail, ale používá šifrování. Pro komunikaci je implementován protokol SSL (z prohlížeče) na server a následně šifrování zpráv pomocí kvalitního programu Blowfish . RSA v SSL používá klíč délky 1024 bitů ! Zdrojový kód lze také získat a stáhnout z níže uvedeného serveru (poslední verze je 1.04) a vytvořit si vlastní silnou kryto-aplikaci (nepodléhá výrobním restrikcím !).
http://www.wired.com/news/news/email/explodeinfobeat/technology/story/19804.html
Hushmail homepage: **http://www.hushmail.com/**
Technická podpora: **https://www.hushmail.com/tech_description.htm**
Zdrojový kód: **http://www.cypherpunks.ai/~hush/**

6) Francie změnila svoji politiku restrikcí na poli šifrování. Ministerský předseda Lionel Jospin oznámil, že Francie obrací svoji dlouhotrvající tradiční domácí restriktivní politiku směrem k volnému používání silných šifer až do délky klíče 128 bitů. Do té doby Francie umožňovala na domácím poli používat volně jen šifry do 40 bitů klíče. Jedná se pravděpodobně o rozhodnutí, které bylo provedeno na základě informací o existenci a využívání špionážního systému ECHELON.
http://jya.com/jospin-coup.htm

7) Na základě zprávy odborného orgánu EP (Evropského parlamentu) STOA, která byla publikována v dubnu 1999 (zpráva se krátce nazývá "Interception Capabilities 2000", nebo jen IC2000 , **http://www.iptvreports.mcmail.com/stoa_cover.htm**), byla přehodnocena německá vládní politika v oblasti kryptologie a ochrany dat. Německá vláda přijala zásadní dokument o principech šifrové politiky "Eckpunkte der deutschen Kryptopolitik", který je svým obsahem ve světě zcela ojedinělý (**http://www.bmwi.de/presse/1999/0602.html**). Tento dokument zásadně mění vládní postoj k silné kryptografii. Některé základní informace lze nalézt např . v V.Klíma : "Velký bratr všechno slyší", CHIP 8/99 nebo mohu přeedat svůj pracovní překlad kompletního vládního prohlášení.

8) Švédsko. Podle časopisu Datateknik (10/99, http://www.datateknik.se) švédské ministerstvo studuje zprávu STOA IC2000 a švédská vláda pověřila tajnou polici SAPO, aby vyšetřila průmyslovou špionáž, která je vedena proti švédským národním a průmyslovým zájmům. Zahrnuje to systém ECHELON a dohodu UKUSA.
Snad již reakcí na výsledky tohoto šetření je liberalizace švédského exportu šifrových zařízení (z 23.7.1999) a obecně povolení exportu silné kryptologie s klíči do 128 bitů (mimo vyjmenované státy).
http://www.ud.se/pressinf/pressmed/1999/juni/990623_5.htm

9) CGHQ britský ekvivalent NSA se bude stěhovat. Nová budova má plánovanou kapacitu pro 4500 lidí (v originále for 4,500 eavesdroppers and code-breakers) a bude dokončena v roce 2002. V areálu bude místo pro 1750 služebních aut a náklady jsou stanoveny na 300 miliónů liber šterlinků.
http://www.guardianunlimited.co.uk/Archive/Article/0,4273,3862710,00.html

10) INVEX Computer Brno´99 se již tradičně uskuteční v týdnu od 4.10 do 8.10.1999. Ve stánku DSM se konají každý den od 13.00 hod. do 16.00 hod. neformální odborná setkání, která budou koncipována jako odborné přednášky zástupců jednotlivých firem. Mottem setkání je slogan "O informační bezpečnosti - netradičně". Na akci je nutné se předem registrovat u DSM.

E. e-mailové spojení (aktuální přehled)

hruby@gcucmp.cz (Union of Czech Mathematicians and Physicists)
- oficiální adresa kryptologické sekce JČMF (Group of Cryptology …)
- jako člen výboru této sekce poštu na této adrese pravidelně zpracovávám
- vzhledem k velkému objemu pošty je vhodné do subjectu umístit jméno Vondruška
- odesílat a přijímat lze libovolný počet příloh
- upřednostňuji pro přenos většího objemu dat

pavel.vondruska@post.cz
- hlavní osobní stránka, o příchodu e-mailu jsem informován na mobil
- k e-mailu lze přiložit jen jedna příloha !
- někdy je tato adresa přetížena
- odeslat lze jen jedna příloha, jsou problémy s některými typy příloh (obsah je konvertován do textu e-mailu) např . *.rtf .
- ozkoušeny a vhodné jsou přílohy *.doc a *.zip

pavel_vondruska@hotmail.com ZRUŠENA !!! (obsah do konce listopadu vybírán)

pavel.vondruska@sms.paegas.cz
- slouží k přímému odeslání e-mailu na můj mobilní telefon
- nelze přidat přílohu
- celková délka textu je omezena cca 160 znaky
- zobrazí se adresa e-mailu odesílatele, subject, a zpráva

Pozn. Všechny výše uvedené články jsou k dispozici v elektronické formě.