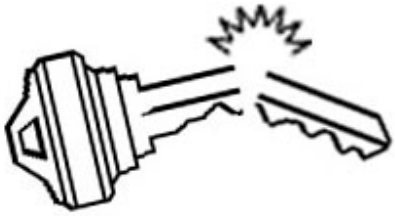
Informační sešit GCUCMP
Crypto-World 3/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz , subject : Crypto-World
(90 e-mail výtisků)
Uzávěrka 15.3.2000



OBSAH : **Str.**

A. Nehledá Vás FBI ?

Mgr. Pavel Vondruška, NBÚ

Začátkem února nastaly problémy s dostupností známých a bohatě navštěvovaných serverů eBay, Amazon, Buy.com, CNN, ETrade a ZDNet. I tyto servery, tak jako již před nimi snad nejznámější vyhledávací server Yahoo, byly napadeny pomocí zcela nového útoku DDS (distributed denial-of-service).

Přibližně čtyři roky již je známa jednodušší varianta výše realizovaného útoku - DOS útok (denial of service). Popíšeme si zjednodušeně tento starší typ útoku, který se dá použít k odříznutí webového serveru. Základem je použití nějakého programu, který bude neustále posílat žádosti na server nabízející danou službu. Po úvodním požadavku na spojení ze sítě se server pokusí navázat kontakt s žádajícím počítačem. Ten se mezitím odpojí a požádá o nové spojení. Než se spojení zrealizuje, je propojení jen "částečné". Pokud k propojení nedojde do předem definované doby, soket realizující polootevřené spojení se uzavře. Počet otevřených soketů s tímto částečným spojením je na každém serveru omezený. DOS útok zpravidla stačí tímto postupem "ucpat" sokety a server je nepřístupný. Jistá obrana proti tomuto útoku existuje a je založena na analýze IP adresy PC, který žádá o připojení. Opět jen velice zjednodušeně platí, že polootevřený soket se při ochraně proti DOS útoku pro stejnou IP adresu již nedá otevřít, tím se zabrání obsazení možných "částečných" propojení.

A tak "samozřejmě" vznikla myšlenka distribuovaného DOS útoku - DDS útok (distributed denial-of-service). Útočník nejprve zaútočí na stovky a tisíce náhodně vybraných, neochráněných počítačů připojených na Internet. Do těchto počítačů nainstaluje speciálně připravený program (v podstatě program pro DOS útok). Takovýto počítač se nazývá "zombie". K tomuto účelu byly použity programy Trin00 and Tribal Flood Network (jejich analýza viz níže uvedené adresy). Útočníkovi potom stačilo pouze zajistit koordinaci útoku a to časovou a místní na jím vybraný server. Připomeňme, že útočník "nevnikl" na vybraný server (jak se někde v novinových článcích uvádělo), ale "pouze" znemožnil ostatním přístup na adresu takto napadeného serveru. Servery byly v těchto případech několik hodin pro žadatele nepřístupné. Žádné trvalé škody nevznikly, ale uživatelům se dočasně znemožnilo jejich použití a provozovatelům napadených serverů vznikly těžko definovatelné škody, jako např. ztráta důvěry nebo i zákazníků, kteří mohli vyhledat jiný server, který jimi požadovanou službu byl schopen ihned poskytnout.

Odborníci se shodují, že proti takto vedenému útoku se v podstatě nedá bránit. Během února proběhly dvě vědecké konference na téma obrana proti DDS. Obě konference se shodly na tom, že úplná obrana není možná, a byly navrženy jen určité patche, které mohou nebezpečí útoku zmírnit. Nejúčinnější obranou tak pravděpodobně bude tvrdý postih útočníků. Mimo FBI, které po útočnících již intenzívně pátrá, se připojilo i Německo, které urychleně vytvořilo speciální oddíl internetové policie s celospolkovou působností. Zákony umožní kvalifikovat takovýto útok jako sabotáž s odpovídajícím postihem.

Mimochodem, nepodílel se také Váš počítač na některém z útoků na výše uvedené servery? Pokud chcete mít jistotu, že nevlastníte "zombie" , nainstalujte si kontrolní program, který Váš počítač prověří a zjistí, zda Tribal Flood Network nebo Trin00 není nainstalován na Vašem počítači. Příslušný program je dostupný např. na adrese :
http://www.nfr.net/updates .

Další informace k tomuto tématu najdete např. na adresách :
Discussion of DDS attacks: http://staff.washington.edu/dittrich/talks/cert
CERT Advisory: http://www.cert.org/incident_notes/IN-99-07.html
Popis DOS útoku:
http://www.hackernews.com/bufferoverflow/00/dosattack/dosattack.html
Trin00 Analysis: http://staff.washington.edu/dittrich/misc/trinoo.analysis
Tribal Flood Network Analysis: http://staff.washington.edu/dittrich/misc/tfn.analysis
Stacheldraht Analysis: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
Článek o DDS: http://www.wired.com/news/politics/0,1283,34294,00.html

B. Aktuality z problematiky eliptických křivek v kryptografii

Ing. Jaroslav Pinkava, CSc., AEC Brno

I. Faktorizační metody opírající se o využití aparátu eliptických křivek

Jednou z klasických faktorizačních metod je Pollardova metoda (lit [1]). Předpokládejme, že chceme rozložit složené číslo n, a že p je (zatím neznámý) faktor n. Pollardova metoda je využitelná, pokud p je takové číslo, že p-1 nemá velké prvočíselné dělitele, tj. metoda nepracuje pokud všechny prvočíselné faktory p čísla n jsou takové, že p-1 obsahují velká prvočísla.

Základní myšlenkou Lenstrovy metody pracující eliptickými křivkami nad tělesem F_p = Z/pZ, je využitelnost podstatně většího souboru grup a hledání mezi nimi takové, jejíž řád není dělitelný velkým prvočíslem nebo mocninou prvočísla.

Je dáno složené liché číslo n a chceme nalézt jeho faktor p, $1 < p < n$. Nejprve vezmeme nějakou eliptickou křivku E : $y^2 = x^3 + ax + b$ s celočíselnými koeficienty spolu s bodem P = (x,y) na této křivce. Dvojice (E,P) je obvykle generována náhodně. Jestliže máme dvojici (E,P), zvolíme číslo k, které je dělitelné mocninami malých prvočísel a menší než nějaká mez C. Dále se pokoušíme spočítat kP, přitom celou dobu počítáme modulo n. Pokud při výpočtu inverzní hodnoty x_2-x_1 či inverse $2y_1$ spočteme číslo, které není vzájemným prvočíslem s n, pak máme nějaký násobek k_1P (částečný součet spočtený během našeho výpočtu kP), který pro nějaké $q < n$ v grupě E mod q má řád dělící k_1. Eukleidovým algoritmu (počítáme inversi modulo n jmenovatele, který je dělitelný q), najdeme největší společný dělitel n a tohoto jmenovatele. Tento NSD je vlastním faktorem n, nebo je n samotným, nebo je jmenovatel dělitelný n. Pokud se nám náš pokus nepodaří vezmeme jinou dvojici (E,P) a tak pokračujeme do té doby než najdeme faktor $p < n$.

Lenstrova metoda má několik výhod :

(1) Je to jediná metoda, která je podstatně rychlejší než jiné metody, pokud n je dělitelné prvočíslem mnohem menším než je n.
(2) Z tohoto důvodu ji lze používat i současně s jinými faktorizačními metodami (v situacích, kdy je požadována faktorizace dalších čísel potřebných k práci těchto jiných algoritmů).
(3) Metoda nemá velké požadavky na paměť.

Je třeba říci, že po objevení se Lenstrova článku (lit. [3]) byla v tuto metodu vkládána velká důvěra. Dokonce se věřilo, že se stane nejúspěšnější faktorizační metodou. Vývoj však

ukázal, že použitelnost metody má skutečně své logická omezení a je vhodná zejména při hledání malých faktorů.

Metoda je však v praxi používána a na adrese:
ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt
lze nalézt výsledky experimentů, které charakterizují současné možnosti této metody. Použitím algoritmu GMP-ECM autorů Nik Lygeros a Michael Mizony byl získán faktor 4840612542768783681257268707891802319959648700949169 37
(dělitel čísla : (6^43-1)^42+1)). Tento výsledek byl dosažen na konci koncem minulého roku (26.12.1999).
Největší činitel takto nalezený má v současnosti tedy 54 dekadických míst.

Literatura:

[1] Koblitz, Neil:
[2] P.L. Montgomery's, ``Speeding up the Pollard and Elliptic Curve Methods of Factorization," Mathematics of Computation 48 (1987), pp. 243-264.
[3] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Mathematics* (2) 126 (1987), 649-673.

II. ECC – charakterizace současného stavu

Na adrese http://www.certicom.ca/ecc/wpaper.htm se objevil nový článek Don Johnson: Advances in Cryptography – ECC, Future Resiliency, and High Security Systems. Zájemcům o praktické aplikace eliptické kryptografie ho vřele doporučuji.

Na adrese http://cacr.math.uwaterloo.ca/~ajmeneze/misc/cryptogram-article.html
uveřejnil Alfred Menezes určité porovnání RSA a kryptosystémů na bázi eliptických křivek (leden 2000).

III. Elliptic Curve Crypto Conference, NatWest premises behind Bank of England, 27 Jan 2000

Tato jednodenní konference měla za cíl pomoci připravit příslušná rozhodnutí v bankovnictví a průmyslu.
(zastoupeny:NatWest, Mondex, platform7, HSBC, Barclays, Abbey National, APACS, Keycorp, Lloyds TSB, Hewlett-Packard a PwC)
Vystoupili zde: Allen Chilver, *NatWest Card Services*, Nigel Smart, *Hewlett-Pacard Laboratories*, Dimitrios Markakis, *Keycorp*, Duncan Garret, *Mondex International.*
Byla projednávána chystaná opatření k zavedení kryptografie na bázi eliptických křivek na základě dnes již jednoznačně ustavených jejích výhod: menší klíče, rychlejší zpracování, menší nároky na spotřebu energie, menší nároky na paměť atd.
Další informace lze na vyžádání získat od Kima Wagnera (Kim.Wagner@uk.pwcglobal.com).

C. Hrajeme si s mobilním telefonem Nokia

(anonym)

Nokia 5110, Nokia 6110, Nokia 6150, Nokia 7110 a další Nokie (nutno ozkoušet)

Toto funguje pouze pro starší firmware 5110 !!!
Zapnutí zablokovaného telefonu - po vložení SIM karty telefon zapněte, poté stiskněte na 3 sec ^šipku nahoru, dále stiskněte C, poté stiskněte * a počkejte až naskočí na displeji, znovu hvězdičku a poté kód 04*PIN*PIN*PIN#

*#06# - vypíše na display IMEI telefonu (International Mobile Equipment Identity). Toto číslo je jedinečné na světě a neexistují 2 telefony se stejným číslem.
(platí pro většinu značek mobilních telefonů tedy nejen Nokie - ozkoušejte si !)

*#0000# - vypíše verzi software telefonu
Telefon vypíše například toto:
V 5.02
02-02-99
NSM-1
První řádek je verze firmware, druhý je datum firmware a třetí je typ telefonu (NSE-1 pro 5110, NSE-3 pro 6110 a NSM-1 pro 6150, NSE-5 pro Nokia 7110)

*#746025625# - dá se také zapamatovat jako *#sim0clock#, zjistí jestli může být SIM Clock zastaven. Některé verze 5110 se SIM Paegas strašně vybíjely baterii telefonu. Zadáním tohoto kódu se můžete přesvědčit, zdali to není Váš případ. Telefon musí vypsat SIM Clock stop allowed. Pokud vypíše not allowed, nechejte si vyměnit kartu (vymění Vám ji zdarma)!

*#92702689# - dá se také zapamatovat jako *#war0anty#. Jedná se o výpis záručních informací o telefonu. První stránka je IMEI, druhá je datum výroby telefony, třetí je kdy byl telefon zakoupen (můžete jednou editovat), čtvrtá je kolikrát byl telefon opravován (doporučuji zkontrolovat před koupí) a poslední slouží k přenosu(zazálohování) uživatelských dat do počítače.

#pw+123456789+1# - tímto kódem zjistíte, zdali je Váš telefon blokován pro určitého operátora

*3370# - aktivace EFR (Enhanced Full Rate), neboli u EuroTelu SuperSOUND
#3370# - deaktivace EFR (Enhanced Full Rate), neboli u EuroTelu SuperSOUND

*4720# - aktivace HR (Half Rate), baterie déle vydrží na úkor kvality hovoru
#4720# - deaktivace HR (Half Rate)

Menu v hovoru - v pohotovostním stavu podržte na 3 sec tlačítko MENU a dostanete se do menu, které je přístupné pouze při aktivním hovoru. (Pouze u NOKIA 61xx!)

Melodie pro Nokii 3210
Macarena Tempo = 180

4f2	8f2	8f2	4f2	8f2	8f2	8f2	8f2	8f2	8f2	8f2	8a2	8c2	8c2	4f2
8f2	8f2	4f2	8f2	8f2	8f2	8f2	8f2	8f2	8d2	8c2	4-	4f2	8f2	8f2
4f2	8f2	8f2	8f2	8f2	8f2	8f2	8f2	8a2	4-	2.c3	4a2	8c3	8a2	8f2 4- 2-

D. Tisková informace (Zákon o elektronickém podpisu)

Zařazuji následující oficiální tiskovou informaci o pozměňovacím návrhu k zákonu o elektronickém podpisu, protože ve zmiňované "expertní pracovní skupině" pracovala i skupina odborníků GCUCMP (RNDr. Jiří Souček DrSc., Ing.Jaroslav Pinkava, CSc., RNDr. Petr Tesař, Mgr. Pavel Vondruška)..

Zástupci SPISU, ÚSISU a expertní pracovní skupina se sešli na víkendovém pracovním shromáždění v Třešti (26.2. - 27.2.) a potom dále v následujících dnech pracovali na úpravě znění zákona o elektronickém podpisu. Diskuse nad zákonem měla za cíl odstranit hrubé chyby a nedostatky, které se ještě v sedmé předložené verzi SPISU vyskytovaly a dále měla za úkol zapracovat obsah direktivy EU o elektronickém podpisu. Internetové diskuse před a po tomto setkání se zúčastnila ještě celá řada dalších členů GCUCMP a odborníků z celé ČR (nutno vyzdvihnout práci silné brněnské skupiny, která demonstrovala skvělou znalost této problematiky) . Všem těm, kteří ve svém volném čase a zcela zdarma se podíleli na této aktivitě, patří poděkování.

Konečný produkt (návrh zákona o elektronickém podpisu) předala paní Bosáková 7.3. panu Mlynářovi, který jej předložil hospodářskému výboru parlamentu.
(Pro úplnost uvádím složení expertní skupiny z Třešti - pánové Budiš, Cvrček, Felix, Hanáček, Peterka, Pinkava, Souček, Staudek, Tesař, Vondruška, Zápotocký, všichni pod vynikající taktovkou paní Bosákové z ÚSIS).

POZMĚŇOVACÍ NÁVRHY K ZÁKONU O ELEKTRONICKÉM PODPISU BUDE PROJEDNÁVAT HOSPODÁŘSKÝ VÝBOR PARLAMENTU

Praha, 28. února 2000 - Zákon o elektronickém podpisu je jedním z nutných kroků na cestě k budování informační společnosti a rozvoji elektronického obchodu. Na tom se shodli zástupci Sdružení pro informační společnost a Úřadu pro státní informační systém. V lednu tohoto roku se obě strany dohodly na společném postupu při prosazování přijetí zákona o elektronickém podpisu, který předložili poslanci Vladimír Mlynář (US), Ivan Langer (ODS), Stanislav Gross (ČSSD) a Cyril Svoboda (KDU-ČSL). Dne 26. ledna 2000 byl pak návrh zákona drtivou většinou poslaneckých hlasů postoupen do druhého čtení.

Dohodu mezi SPIS a ÚSIS přivítal také ministr Pavel Mertlík, který Sdružení pro informační společnost dopisem sdělil, že Ministerstvo financí již pracuje na několika projektech, k jejichž realizaci potřebuje elektronický podpis a tedy zmíněný zákon. Jedná se například o možnost podávání daňového přiznání či přiznání silniční daně po Internetu.

Na základě této dohody Úřad pro státní informační systém a SPIS iniciovali vznik expertní skupiny nezávislých odborníků a požádali ji o zpracování odborných připomínek k textu poslaneckého návrhu zákona formou pozměňovacích návrhů tak, aby byl uveden do souladu s direktivou Evropské unie o elektronických podpisech schválenou 30.listopadu 1999.

Expertní pracovní skupina se sešla společně se zástupci ÚSIS a SPIS na víkendovém setkání v Třešti, aby zde uzavřela svoji dlouhodobou práci na formulaci připomínek a dopracovala zde pozměňovací návrhy do konečné podoby tak, aby mohly být předány hospodářskému výboru Parlamentu. Ten bude v průběhu března přepracovanou verzi projednávat a výsledky svého jednání pak předloží poslancům při druhém čtení plánovaném na květnovou schůzi Parlamentu.

Kontakt: Jitka Pavlonová, SPIS, Blanická 16, 120 00 Praha 2, telefon 02/21503481-3, telefax 02/21503482, e-mail jitkap@spis.cz, http://www.spis.cz.

E. Digital Signature Standard (DSS)

Vzhledem k aktivitám části členů GCUCMP v oblasti zákona o digitálním podpisu zařazuji aktuální zprávu o standardu NIST (platný od 27.6.2000). Překlad by textu spíše uškodil, a proto jej zařazuji v originále.

15 February 2000
Source: http://www.access.gpo.gov/su_docs/aces/fr-cont.html

[Federal Register: February 15, 2000 (Volume 65, Number 31)]
[Notices]
[Page 7507-7508]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr15fe00-37]

DEPARTMENT OF COMMERCE

National Institute of Standareds and Technology

[Docket No. 981028268-9247-02]
RIN No. 0693-ZA-23
Announcing Approval of Federal Information Processing Standard
(FIPS) 186-2, Digital Signature Standard (DSS)
AGENCY: National Institute of Standards and Technology (NIST),
Commerce.
ACTION: Notice.

SUMMARY: The Secretary of Commerce approved Federal Information Processing Standard 186-2, Digital Signature Standard (DSS), which supersedes Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard (DSS), FIPSs 186-2 expands FIPS 186-1 by
[[Page 7508]]
specifying an additional voluntary industry standard for generating and verifying digital signatures. This action will enable Federal agencies to use the Digital Signature Algorithm (DSA), which was originally the single approved technique for digital signatures, as well as two new ANSI standards that were developed for the financial community. These new standards are ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

EFFECTIVE DATE: This standard is effective June 27, 2000.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker (301) 975-2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930.

Specifications for FIPS 186-2 are available on NIST Web page: http://csrc.nist.gov/encryption>.

Copies of ANSI X9.31, Digital Signatures Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA) are available from the American Bankers Assoc./DC, X9 Customer Service Dept. P.O. Box 79064, Baltimore, MD 21279-0064; telephone 1-800-338-0626.

SUPPLEMENTARY INFORMATION: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems. In May 1994, the Secretary of Commerce approved FIPS 186, Digital Signature Standard (DSS), which specified the Digital Signature Algorithm (DSA) as the single technique for the generation and verification of digital signatures. In 1997 NIST solicited comments on augmenting FIPS 186 with other digital signature techniques including the Rivest-Shamir-Adleman (RSA) and the elliptic curve technique. The comments received by NIST supported adding both techniques to FIPS 186. Both techniques were being considered by the financial services industry as voluntary industry standards.

On December 15, 1998, (FR Vol. 63, No. 240, pp 69049-51) NIST announced that the Secretary of Commerce had approved FIPS 186-1, Digital Signature Standard (DSS) as an interim final standard. FIPS 186-1 added the RSA digital signature technique, which had been approved as an industry standard (X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry). The elliptic curve technique was not included in the interim final standard since it had not yet been approved by the American National Standards Institute (ANSI) as a voluntary industry standard.

The December 1998 Notice from NIST invited comments from public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations concerning the specification of two techniques (DSA and ANSI X9.31- 1998) for the generation and verification of digital signatures. That Notice also referred to the elliptic curve technique, which NIST had expected to be approved by ANSI as a voluntary industry standard. In addition to being published in the Federal Register, the Notice was posted on the NIST Web pages; information was provided for submission of electronic comments. NIST received comments from 15 private sector organizations and individuals, and from two federal government organizations. The comments supported the addition of the ANSI X9.31 standard, as well as the addition of the elliptic curve technique to the Digital Signature Standard (DSS). NIST recommended that the Secretary of Commerce approve FIPS 186-2, which includes the DSA, ANSI X9.31, and the elliptic curve technique, which has now been approved as ECDSA, under ANSI X9.62, Elliptic Curve Digital Signature Algorithm. Other comments supported the continued use of another RSA signature algorithm that is specified by PKCS#1. The algorithm specified in PKCS#1 does not interoperate with the algorithm specified in ANSI X9.31. FIPS 186-2 allows for the continued acquisition of implementations of PKCS#1 for a transition period of eighteen months from the date of approval of this standard, which will enable federal agencies to plan for the acquisition of implementations of the algorithms promulgated by FIPS 186-2.

Dated: February 8, 2000.
Karen H. Brown, Deputy Director, NIST.
[FR Doc. 00-3450 Filed 2-14-00; 8:45 am]
BILLING CODE 3510-CN-M

F. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

Pozvání pro členy GCUCMP a další zájemce o problematiku informační bezpečnosti. I v tomto semestru se přednášky, semináře konají každé úterý. Přednáška je dvouhodinová a je v seminární místnosti KSI MFF UK na Malé straně (druhé poschodí, katedra systémového inženýrství). Seminář bude věnován matematickým analytickým principům, bude definována a analyzována matematická podstata zabezpečení informací. Seminář bude vycházet z praktických úloh, na semináři budou přednášet přední odborníci v dané oblasti. Seminář je vhodný pro studenty a bude probírat danou problematiku od počátku. Na seminář je volný přístup pro členy GCUCMP a další zájemce o konkrétní témata.

Identifikace: MAT069
Zajišťuje: MUKU
Vyučující: Jiří Souček, Tonda Beneš
Rozsah: 0/2 Z, 0/2 Z
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)
Konkrétní témata přednášek budou vyhlašovány v průběhu semestru.

Program:

22 2.	Jiří Souček:	Elektronický podpis
7.3.	Jiří Souček:	Protokol SET
14.3.	Pavel Kaňkovský :	RSA
21.3.	Pavel Vondruška :	Možné slabiny implementace RSA
28.3.	Tonda Beneš:	Přehled používaných protokolů

G. Letem šifrovým světem

1. Skupina Distributed.net rozluštila text, který firma CS Communications & Systems umístila na svůj web. Firma doporučuje přechod na šifru CS-Cipher s délkou klíče 128 bitů. Text byl ovšem zašifrován verzí s délkou klíče 56 bitů. Na dešifraci se podílelo 38,107 počítačů a během 62 dnů bylo prověřeno 98% všech možných klíčů. Skupina získala vypsanou odměnu 10000 Euro. http://www.wired.com/news/print/0,1294,33695,00.html

2. Vzhledem ke změně regulačních pravidel US exportu lze nyní získat podrobné zdrojové kódy kandidátů na AES. Twofish si např. můžete od února stáhnout z adresy : http://www.counterpane.com/blowfish.html#source

3. Firma Cylink Corporation vyrábí a vyváží kryptografické prostředky pro sítě více jak 16-let. Jejich produkty jsou používány po celém světě - v obchodní, bankovní a státní sféře. Na adrese :. http://cryptome.org/cylinked.htm se objevil 3.3.2000 článek, který naznačuje jisté podezřelé styky této firmy.

4. Třetí evropské čtyřdenní setkání nazvané : "Cryptographic security aspects of smartcards & Internet" se uskuteční od 25.4. do 28.4.2000 v Amsterdamu. Workshop je organizován ve spolupráci s IBM Finance Services. Přihlášky na e-mailu : akl@euroforum.nl

5. Zajímavý článek na téma - jak jednoduché je se nabourat do webovských stránek - můžete nalézt na adrese : http://www.pcworld.com/current_issue/article/0,1212,14415,00.html

6. Přestože se ostrá verze Windows 2000 začala prodávat v minulých dnech, šíří se již také první virus, který byl vyvinut speciálně pro prostředí Windows 2000. Více informací lze najít na http://www.computerworld.com/home/print.nsf/all/000113DD52
   Na internetu jsou dostupné informace o prvních bezpečnostních problémech Windows 2000 (PTPP) : http://dailynews.yahoo.com/h/zd/20000130/tc/20000130748.html

7. (13.2.2000 , RSA) Cílem útoku hackerů se stala i hlavní webovská stránka legendární firmy RSA Security (www.rsa.com). Úvodní strana byla pozměněna , výsledek je možno najít na diskutovaném serveru

   http://www.2600.com/hacked_pages/2000/02/www.rsa.com .
   Hackeři označili písmenem L osoby na vstupním pohyblivém panelu. Nově (proti originálu) se zde objevil text "Big things are coming" a další komentáře typu : "Trust us with your data! Praise Allah! ". "Zpřetrhány" byly také linky na úvodní stránce a nasměrovány jinam. Nově se objevila např. linka s nadpisem:"Girls are stupids and easy ".

8. I naši (nebo slovenští ?) hackeři se v únoru činili. Některé jejich "úspěchy" můžete najít na stránce http://hysteria.sk/czert . Za měsíc únor jsou zde zdokumentovány útoky na servery http://www.tinysoftware.cz (které vyústily v masový útok na desítky adres spravované firmou tinysoftware, všechny takto postižené adresy jsou pečlivě vypsány v "zoznamu", který je zde k dispozici). Skupina nazývající se binary division pak pozměnila úvodní webovské stránky firem www.winroute.cz (stránka po změně zadokumentována na http://dump.hysteria.sk/hacked/www.winroute.cz) , a www.isdn.cz (stránka po změně zadokumentována na http://dump.hysteria.sk/hacked/www.isdn.cz).
   Jiné skupině se podařilo dostat na prezentační server českého mobilu. Výsledek je dostupný na http://dump.hysteria.sk/hacked/www.ceskymobil.cz .

9. Psát o CeBITu je asi celkem zbytečné - ve všech našich sdělovacích médiích se objevilo nebo se objeví na toto téma ještě dost článků. Takže jen připomenu, že proběhl netradičně o měsíc dříve a to v termínu od 24.2.2000 do 1.3.2000. Osobně mne zaujala nejvíce výborná práce organizátorů a podmínky, které zde přímo na výstavišti byly nabízeny programatorům a pracovníkům InfoSecu z východní Evropy v případě jejich práce v Německu. Není mi jasné, co naše kompetentní orgány provedou, aby zabránily odchodu schopným, odborným pracovníkům do Německa (odhadováno na jeden tisíc osob).

10. (18.2.2000) Na internetu se objevily články, které tvrdí, že v Microsoftu pracovali tajní agenti USA. Zdrojem těchto článků je francouzská výzvědná služba.
    http://www.intelligenceonline.fr
    http://www.theage.com.au/breaking/0002/19/A27800-2000Feb19.shtml

H. Závěrečné informace

Omlouvám se všem čtenářům za zpoždění tohoto čísla. Během měsíce jsem strávil týden na dovolené, týden v Německu, týden prací na zákoně o elektronickém podpisu a také jsem musel pracovat pro svého zaměstnavatele…Takže jsem to opravdu při sebelepší vůli dříve nestihl dopsat.

URL adresa, 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, mé články a další související témata :

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

Stránku lze již také najít pomocí funkce hledej na www.seznam.cz (klíčové slovo GCUCMP). Stránka je umístěna v oddíle www.seznam.cz , věda, informatika .

Spojení :

hruby@gcucmp.cz (Group of Cryptology Union of Czech Mathematicians and Physicists)
- oficiální e-mail adresa kryptologické sekce JČMF

p.vondruska@nbu.cz - osobní poštovní stránka , zasílání příspěvků, běžná komunikace

pavel.vondruska@post.cz - náhradní osobní poštovní stránka, registrace odběratelů

pavel.vondruska@sms.paegas.cz - jen 160 znaků !
mobil : Mgr.Pavel Vondruška 0603 436 341

Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má kdokoliv zájem o zasílání tohoto sešitu, stačí se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět : Crypto-World). Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu.

Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.