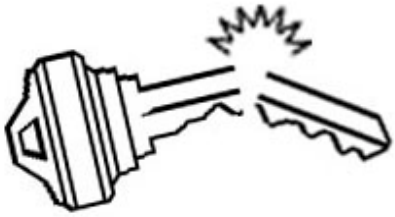
Crypto-World 10/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(31 e-mail výtisků)
Uzávěrka 3.10.99



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.**

Logo z minulého čísla - klíč - bylo po připomínce jednoho z Vás, že klíč značí spíše zvýšenou odolnost proti útokům, ale obsah sešitu spíše poukazuje na bezpečnostní slabiny - změněno (Petře, Je to OK ?). Logo vymyslel můj syn a druhý mi pomohl s jeho realizací a já jim za to slíbil, že to v sešitu napíši. Tedy logo dle návrhu Petra Vondrušky (11 let), grafická úprava Pavel Vondruška (13 let).

A. Microsoft Back Orifice 2000

Z bezpečnostního hlediska se jedná o nové veliké riziko pro počítače připojené na internet. Kusé informace, které se tu a tam objevují , doplníme alespoň úplným oficiálním zněním tiskového prohlášení firmy Microsoft z 31.8.1999 viz www.microsoft.cz, anglická verze je umístěna mezi tiskovými prohlášeními na www.microsoft.com . Pro zájemce jsou připojeny odkazy na www stránky, kde jsou uvedeny rozsáhlejší informace.

Co by měli zákazníci vědět o „BackOrifice 2000“

BackOrifice 2000 (BO2K) je nepřátelský škodlivý program, který měl být uveden do oběhu okolo 10. července t. r. Jeho autoři se jistě pokusí vyvolat okolo něj hysterii. Uživatelé se před ním mohou chránit dodržováním běžných pravidel bezpečné práce s počítačem. Ačkoliv program ještě nebyl do oběhu uveden, společnost Microsoft pečlivě sleduje situaci a vynasnaží se poskytovat informace, které umožní uživatelům pochopit podstatu programu a ochrany proti němu, jakmile se objeví.

Následují odpovědi na nejčastější otázky ohledně programu BO2K.

Co je BO2K za program?
BO2K je program, který po nainstalování na počítač s Windows umožňuje dálkové ovládání počítače jiným uživatelem. Software pro dálkové ovládání počítače není sám o sobě nikterak závadný (škodlivý) a mnoho takových programů se legálně prodává a je využíváno např. správci výpočetních systémů. BO2K se odlišuje tím, že má sloužit k poškozování uživatelů a má utajené funkce, které nemají jiný účel než stížit jeho odhalení.

Jaké nebezpečí od tohoto programu hrozí?
Je-li BO2K instalován na počítači, „útočník“ může s počítačem dělat cokoliv, co může udělat oprávněný uživatel z klávesnice. Může tedy i spouštět programy, tvořit nebo mazat soubory, odesílat a přijímat data apod.

Jak se tento program může dostat do mého počítače?
Jako kterýkoliv jiný program, BO2K musí být na počítač nainstalován. Nelze ho tam jakkoliv nenápadně „vsunout“. Existují pouze dva způsoby, jak může být instalován:
Umožníte-li člověku, který ho chce na váš počítač nainstalovat, fyzický přístup k vašemu počítači (tj. zná-li vaše přihlašovací heslo, nebo pustíte-li ho k zprovozněnému počítači). Pokud vás nějak přiměje, abyste si ho nainstalovali sami. Toto je známo jako tzv. technika Trojského koně. Může vám být např. zaslán e-mail s přílohou, která se tváří jako hra, ale ve skutečnosti nainstaluje na váš počítač BackOrifice.

Jak předejít instalování BO2K na můj počítač?
Nemusíte podnikat žádná mimořádná opatření. Pouze dodržujte běžné postupy pro bezpečnou práci s počítačem:
nikomu nikdy nesdělujte svoje přístupové heslo a vždy uzamkněte počítač, když od něj odcházíte nikdy nespouštějte software z neověřených zdrojů udržujte neustále aktuální verze vašeho antivirového příp. i jiného bezpečnostního software

Pokud se již BO2K do mého počítače dostal, jak se ho zbavím?
Výrobci antivirového software a utilit pro indikaci nežádoucích aktivit v počítači pozorně očekávají objevení BO2K a jsou připraveni co nejrychleji vyvinout software k jeho detekci a odstranění. Microsoft s nimi úzce spolupracuje a je připraven jim asistovat. Při uvedení

předchůdce BO2K byly obranné prostředky k dispozici během několika dní a stejný termín lze předpokládat i v současné situaci.

Využívá BO2K nějakých mezer v zabezpečení Windows nebo Windows NT?
Nikoliv. Programy jako BO2K mohou být vytvořeny pro jakýkoliv operační systém – tento byl napsán zrovna pro Windows a Windows NT. V jakémkoliv operačním programu můžete spustit program, který může dělat všechno to, co může dělat uživatel přímou obsluhou počítače. A pokud vás někdo lstí přinutí spustit destruktivní program, ten pak může smazat vaše data, pozměnit údaje nebo umožnit někomu dalšímu zadání dalších příkazů.
Software typu Trojského koně nenapadá technologii, ale uživatele. V případě, že by BackOrifice využíval nějaké bezpečnostní mezery ve Windows nebo Windows NT, Microsoft by okamžitě tuto mezeru opravil a zabránil tak funkci programu. Autoři BackOrifice si však uvědomili, že je snazší se zaměřit na lidi a přimět je ke spuštění škodlivého software, než se zaměřit na technologii.

Je BO2K něco jako virus Mellisa?
Jenom v tom smyslu, že oba jsou tzv. Trojské koně a vykonávají „záškodnické“ akce, a ani jeden z nich nevyužívá jakékoliv případné chyby v produktech společnosti Microsoft.

Co v souvislosti s BO2K podniká společnost Microsoft?
Microsoft pečlivě sleduje situaci a cítí se povinen pomoci uživatelům zajistit bezpečnou a radostnou práci s počítačem:
experti společnosti Microsoft na bezpečnost jsou připraveni okamžitě po objevení se software BO2K přesně zjistit jak pracuje a jaké prostředky lze použít k ochraně před jeho účinky
Microsoft spolupracuje s ostatními firmami, zabývajícími se bezpečností počítačů – zejména s výrobci antivirového software, utilit pro detekci nežádoucích aktivit počítače a dalších bezpečnostních produktů – na tom, aby software pro detekci a odstranění BO2K byl dostupný co nejdříve Microsoft poskytne svým zákazníkům maximální množství dostupných informací o tomto programu.

Další informace:
http://www.bo2k.com/
http://www.zdnet.com/zdnn/stories/news/0,4586,2127049,00.html
http://www.infoworld.com/cgi-bin/displayArchive.pl?/99/30/o03-30.36.htm
http://www.microsoft.com/smsmgmt/techdetails/remote.asp
http://www.cultdeadcow.com/news/pr19990719.html

B. Šifrování disku pod Linuxem

To: cypherpunks@algebra.com
From: "Doobee R.Tzeck" <doobee@ccc.de>
Subject: Encrypting your Disks with Linux

Je mnoho možností jak šifrovat data na disku v OS Linux. Šifrování dat na disku potom chrání vaše data proti klasickým útokům, jako přihlášení se vaším jménem, nabootování z jiného volumu a přimontování vašeho disku ke svému, chrání samozřejmě vaše data při ztrátě laptopu. Otázku jakou metodu použít, si položil "Doobee R.Tzeck" <doobee@ccc.de> a shromáždil informace o dostupných šifrovacích programech disku pro

LINUX. Potom se obrátil na diskusní fórum cypherpunks@algebra.com se žádostí, zda může někdo kvalifikovaně k těmto systémům něco říci.

Pro náš sešit jsem přepsal některé základní informace. V případě, že se na diskusním fóru objeví některá informace o slabosti některého z dále předkládaných systémů a já ji zachytím, budu se snažit o ní informovat. Dnes tedy jen základní přehled.

Přehled šifrování v Linuxu :

1. Loopback Encryption http://drt.ailis.de/crypto/linux-disk.html#loopback
2. Encrypted Home Directorys http://drt.ailis.de/crypto/linux-disk.html#ehd
3. CFS - Cryptographic File Systém http://drt.ailis.de/crypto/linux-disk.html#cfs
4. TCFS - Transparent Cryptographic Filesystem
   http://drt.ailis.de/crypto/linux-disk.html#tcfs
5. ppdd - Practical Privacy Disc Driver http://drt.ailis.de/crypto/linux-disk.html#ppdd
6. sfs - Steganographic File System for Linux
   http://drt.ailis.de/crypto/linux-disk.html#sfs
7. StegFS - A Steganographic File System for Linux
   http://drt.ailis.de/crypto/linux-disk.html#stegfs
8. BestCrypt http://drt.ailis.de/crypto/linux-disk.html#bestcrypt

1. The Kernel Loopback Encrypting Block device
Jedná se o klasickou metodu šifrování partitions v Linuxu. Před instalací je nutno použít poslední patch kernelu. Lze jej stáhnout např. z http://www.kerneli.org . Co je podle mne velice zajímavé, že nový patch umožňuje používat následující šifry DFC, MARS, RC6, Serpent, CAST 128, IDEA, Twofish, Blowfish. Jak vidíte většinu tvoří kandidáti na AES - nový šifrový standard (viz. např minulé číslo našeho sešitu Crypto-World 9/99 - Nový šifrový standard AES)..

2. Encrypted Home Directorys Patch
Umožňuje šifrování adresářů užitím loopback encryption, ale pro více uživatelů .Je to výhodné pokud váš počítač je sdílen více uživateli.
Jak to funguje je popsáno v : http://members.home.net/id-est/

3. CFS - Cryptographic File System
CFS byl "zlomen" Matt Blazem. Více o CFS např. ve "A Cryptographic File System for Unix" by Matt Blaze ftp://research.att.com/dist/mab/ .CFS podporuje DES (považovaný již za nepříliš bezpečný), 3DES (který je ovšem pomalý), MacGuffin (ten je již ale rozbit), SAFER-SAK-128 (ovšem v neobvyklém tvaru), Blowfish (který se obecně považuje za bezpečný, ale zde je nějaký problém s uložením P-boxů a S-boxů v systémovém archívu - dokonce tu snad chybí …). Mimo bezpečnosti je zde ještě problém s rychlostí , kopie dat se několikráte vyměňují mezi jádrem a uživatelským prostorem. Při šifrování velkého objemu dat je tato metoda nevhodná.

4. TCFS - Transparent Cryptographic Filesystem
TCFS byl vyvinut na univerzitě v Salerno (Itálie). Je hluboko zaintegrován v systému, šifrové služby a systémová práce se soubory jsou kompletně transparentní pro užití v uživatelských aplikacích. Je nutné mít nainstalovaný poslední patch 2.0.x Kernel. Aplikacemi je zatím málo používán. Nevýhodou je minimální podpora klíčového hospodářství. Je zde jen nějaký

prozatimní " Placebo-key management" dodávaný s TCFS ale ten používá jen přihlašovací heslo a jedno heslo na šifrování.
Některé z možných problémů jsou diskutovány na : http://tcfs.dia.unisa.it/tcfs-faq.html.
Domácí stránka TCFS je umístěna zde :http://tcfs.dia.unisa.it/

5. ppdd - Practical Privacy Disc Driver
ppdd je dobře vystavěný systém na šifrování vašeho disku. Jeho autorem je for Allan Latham. Sám píše, že " … ppdd se užívá k šifrování souborů pod Linuxem. Využívá vysoce kvalitní šifrovací techniky pro velké volumy, lehce se instaluje. …" . Chránit lze např. root tak, že po naběhnutí systému, mohou být různé části chráněny jinými přístupovými právy. Je ideální pro víceuživatelský systém. Práce se zašifrovanými soubory je samozřejmě pomalejší. Např. u Pentia 100 Mhz, 32 MB RAM, IDE řadič je propustnost 50%. Ovšem již na dual PII/266 Mhz, 256 MB RAM, IDE řadič byl sice zápis na zašifrovaném volumu 2x pomalejší, ale čtení zašifrovaných dat již bylo 4x rychlejší …
Další podrobné informace můžete nalézt na :
http://drt.ailis.de/crypto/Specification.txt
http://drt.ailis.de/crypto/ppdd.man.html
http://linux01.gwdg.de/~alatham/ppdd.html
ftp://ftp.gwdg.de/pub/linux/misc/ppdd
http://drt.ailis.de/crypto/ppddhow.txt (podrobnosti k instalaci)

6. sfs - steganographic file system for Linux
Teoretickým východiskem byl článek Ross Anderson, Roger Needham and Adi Shamir "The Steganographic File System" (http://drt.ailis.de/crypto/sfs3.ps.gz) . Prvou implementaci napsal Carl van Schaik and Paul Smeddle. Aby nemohla být data lehce napadnutelná, je zde např. zabudována myšlenka automatického přešifrování (utajení dat) každý den , podle určité skryté informace. Autoři o programu píší, že neručí za případnou ztrátu vašich dat, že se jedná vlastně o experiment Připomínají, že neručí za to jak silnou šifrovou metodu jste použili - s ohledem na platný řád v zemi, kde žijete a kde jsou možná určitá omezení.
Domácí stránka této problematiky je na : http://leg.uct.ac.za/~carl/vs3fs/ (patches pro Linux 2.0 and 2.1). Peter Schneider-Kamp updatoval program pro verzi 2.2. Tento update lze nalézt na adrese: http://www.linux-security.org/sfs/
Problému je také věnována stránka: http://drt.ailis.de/public_html/crypto/sfspatch-2.2.10.tar.gz

7. StegFS - A Steganographic File System for Linux
Andrew McDonald a Markus Kuhn vytvořili vlastní implementaci šifrování dat na základě steganografických metod. Jejich základní myšlenka také vychází z již citovaného článku Anderson, Needhama a Shamira. Tvrdí, že sfs je "vadné". Jejich systém StegFS se zdá být opravdu vypracovaný a zdá se, že je v praxi dobře použitelný a "lepší" než sfs.
StegFS má svoji stránku na http://ban.joh.cam.ac.uk/~adm36/StegFS/

8. BestCrypt
Jedná se o komerční program pro zašifrování disku pod Linuxem. Jeho verze existují též pod operačními systémy MS Windows a MacOS .
Informace na : http://www.jetico.com/

C. Microsoft Point-to-Point Tunneling Protocol (PPTP)

Counterpane Systems and L0pht Heavy Industries Announce Analysis of Microsoft PPTP Version 2 By Bruce Schneier

Plné znění této přednášky lze najít na http://www.counterpane.com/pptpv2-paper.html .
Zde jen některé detaily.

V roce1998, Bruce Schneier and Mudge provedli analýzu protokolu PPTP od firmy Microsoft. My (píše B.Schneier) jsme nalezli vážné chyby v následujících oblastech :

- password hashing -- slabý algoritmus umožňující útočníkovi seznámit se s uživatelskými hesly
- Challenge/Reply Authentication Protocol -- chyba umožňuje útočníkovi tvářit se jako server
- encryption -- chyba v implementaci umožňuje obnovit zašifrovaná data
- encryption key -- obecná hesla poskytují napadnutelné klíče, i když je použito šifrování s klíčem délky 128-bit
- control channel -- neautentizované zprávy umožňují útočníkovi zaútočit na PPTP server

Detaily z analýzy provedené v roce 1998 jsou umístěny v tiskové zprávě na našem serveru (http://www.counterpane.com/) a ve FAQ.

Na základě naší analýzy Microsoft realizoval upgrade protokolu. Tento upgrade je použitelný pro Windows 95, Windows98, a Windows NT jako DUN 1.3. Microsoft tak zvýšil upgradem bezpečnost svého protokolu.

O analýze nového upraveného protokolu vzhledem k přesnosti již původní originální text :

The weaker LAN Manager hash is no longer sent along with the stronger Windows NT hash. This is to prevent automatic password crackers like L0phtcrack (http://www.l0pht.com/l0phtcrack)
from first breaking the weaker LAN Manager hash and then using that information to break the stronger NT hash. An authentication scheme for the server has been introduced. This is to prevent malicious servers from asquerading as legitimate servers.
The change password packets from MS-CHAPv1 have been replaced by a single change password packet in MS-CHAPv2. This is to prevent the active attack of spoofing MS-CHAP failure packets. MPPE uses unique keys in each direction. This is to prevent the trivial cryptanalytic attack of XORing the text stream in each direction to remove the effects of the encryption.

The software is more robust against denial-of-service attacks, and does not leak as much information about its status.

These changes address most of the major security weaknesses of the orginal protocol. However, the revised protocol is still vulnerable to offline password-guessing attacks from hacker tools such as L0phtcrack**. At this point we still do not recommend Microsoft PPTP for applications where security is a factor.**

D. Letem "šifrovým" světem

1) Několik lidí se pozastavilo nad tím, že v čísle 9/99 jsem tak rezolutně vystoupil proti poštovnímu serveru HOTMAIL a zrušil jsem svoji adresu na tomto serveru.
Můj postoj snad osvětlí následující krátký komentář. Z článků, které se objevily během tohoto měsíce na internetu vyplývá, že chyba na serveru HOTMAIL dovolila číst bez hesla všechny e-mailové zprávy po delší dobu a nejednalo se o náhodný průnik na poštovní server. Je více jak pravděpodobné, že hackerské společenství o chybě na serveru vědělo a umělo ji využívat již dávno před tím, než byla tato chyba odhalena.
http://207.82.250.251/cgi-bin/start?curmbox=ACTIVE&js=no&login=username
http://www.wired.com/news/news/technology/story/21503.html
http://www.msnbc.com/news/306093.asp
http://www.zdnet.com.au/zdnn/stories/zdnn_display/0,3440,2324361,00.html
http://news.excite.com/news/zd/990901/10/the-bug-syndrome
http://news.excite.com/news/zd/990901/06/how-hotmail-blew
http://www.salon.com/tech/log/1999/09/02/hotmail_hack/print.html

2) Firma Microsoft vyvinula k zajištění digitální hudby speciální bezpečnostní formát - Windows Media Audio (WMA), zabezpečenou alternativu MP3. O tom, že právě bezpečnost není doménou firmy Microsoft svědčí to, že byl do dvou dnů po jeho uveřejnění již rozbit.
http://www.wired.com/news/news/technology/story/21325.html
http://www.news.com/News/Item/0,4,0-40672,00.html?st.ne.lh..ni
http://www.msnbc.com/news/302195.asp

3) Bezpečnost NT.
Bruce Schneier v článku o Microsoft Orifice 2000 (časopis "Crypto-Gram 8/99")se zmínil, že aby byl operační systém Windows NT opravdu bezpečný, bylo by potřeba provést více jak 300 úprav. Na svém webu (http://www.counterpane.com) Bruce Schneier píše :

"Mnoho lidí se pozastavilo nad mou poznámkou o bezpečnosti grafického operačního systému NT a potřebě nastavit více jak 300 bezpečnostních změn. Předložil jsem tedy tento odhad diskusní skupině na Usenetu (comp.os.ms-windows.nt.admin.security) a ptal se kolik tedy je potřeba nastavit bezpečnostních opatření. Diskusní skupina se ujednotila, že počet změn je kdesi mezi 50 a 3000, a tedy můj odhad 300 nebyl nerozumný . Pokud si to chce někdo ověřit, doporučuji
http://people.hp.se/stnor/ nebo http://www.trustedsystems.com/NSAGuide.htm "
- konec citace .

4) Microsoft se snaží zvýšit svoji vážnost na poli bezpečnosti například i následující akcí. Microsoft umístil beta verzi svého nového grafického operačního systém Windows 2000 a vyzval hackery, aby se do něj pokusily "vloupat". Útok hackerů byl neúspěšný. (Možnost útoku byla ovšem časově omezena).
http://www.zdnet.com/zdnn/stories/news/0,4586,2309474,00.html?chkpt=hpqs014
http://www.windows2000test.com/

5) Oficiální bezpečnostní politika firmy Microsoft je popsána ve sděleních "white paper" na serveru microsoftu. Mezi tato sdělení přibyla dvě následující:
Základy bezpečnosti: http://www.microsoft.com/security/resources/security101wp.asp
Microsoft Office 2000 Macro Security White Paper :
http://officeupdate.microsoft.com/2000/downloadDetails/o2ksec.htm

6) Za jediný měsíc, kdy je na tuzemském trhu k dispozici sada kancelářského softwaru Office 2000 v české verzi, se prodal rekordní počet 31 000 licencí (mimochodem instalační sada nyní již obsahuje 4 plná CD)! http://www.microsoft.cz/

7) Skupina českých hackerů CzERT pozměnila (již potřetí) www stránku banky UNION. Tentokráte přejmenovali banku na RUIN banku a umístili zde fotografii nahé ženy, která strká ruku do zadnice koně, s nadpisem "Ředitelka ústavu" a textem : "Tady lovím vaše investice a úspory ! " . Pokud se chcete pokochat jak vypadaly stránky před útokem a po útoku této skupiny, doporučuji navštívit archiv průniků této skupiny (jsou zde informace i útoku na servery policie, ministerstva zdravotnictví apod.). Archiv je umístěn na http://www.hysteria.sk .

8) Těsně před uzávěrkou jsem dostal upozornění od J.Pinkavy na velice zajímavou informaci, která se týká odolnosti eliptických křivek. Celý text je uveden v závěru jako samostatná příloha :
"INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"

9) Ještě jednou připomínám INVEX Computer Brno´99 začíná dnes tj. 4.10 a trvá 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 pro veliký zájem předem registrovat u DSM a nebo se na místě vnutit.

10) Problém Y2K (přechod na rok 2000) a Windows. Těm, kteří to neví, připomínám že je potřeba doinstalovat patche do jednotlivých verzí Windows, aby (v případě, že váš BIOS je OK) jste mohli v roce 2000 dále bez potíží používat svůj oblíbený operační systém. Tentokráte musím firmu Microsoft pochválit. Na serveru http://www.microsoft.com/year2000 jsou k dispozici všechny patche pro jednotlivé verze Windows. Nejsou nijak malé (až několik megabyte). Nicméně konec roku se blíží, a tak doporučuji stáhnout a nainstalovat.

11) A tuhle znáte …
Z oficiálního sdělení firmy Microsoft... Pokud nebude verze Windows 2000 v prodeji do konce tohoto roku 1999 , bude v prodeji v lednu roku 1900.

E. e-mailové spojení (aktuální přehled)

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

pavel.vondruska@post.cz - osobní stránka
pavel_vondruska@hotmail.com - ZRUŠENA !!!
pavel.vondruska@sms.paegas.cz - jen 160 znaků !

Příloha č.1

http://www.inria.fr/Actualites/pre55-eng.html

INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom

Paris, September 28. 1999 - A new code-cracking challenge set by Certicom has been successfully overcome using 740 computers in 20 countries over a period of 40 days. The code, ECC2-97, is based on a technique known as elliptic curves.

Led by Robert Harley, a member of the Cristal project at INRIA, France's National Institute for Research in Computer Science and Control, the 195 researchers involved showed that a 97-bit encryption system based on elliptic curves is more difficult to crack than a 512-bit system based on integers such as RSA-155.

Encryption systems based on elliptic curves have been known since the mid-1980s, but have only recently been adopted by leading encryption companies such as RSA Security Inc. Certicom issued its "ECC Challenge" in November 1997, specifying a series of challenges of increasing difficulty. The company offers prizes up to US$100,000. The aim of the challenge is to encourage research in the field of elliptic curves and their applications in encryption, and to strengthen arguments in favor of using elliptic curve cryptography instead of systems based on integer factorization.

The challenge dubbed "ECC2-97" took place in a set of about 10^29 points on an elliptic curve chosen by Certicom. To solve the problem, participants first computed 119,248,522,782,547 (more than 10^14) using open-source software developed by Harley. Among these points, they screened 127,492 "distinctive" points and collected them on a Alpha Linux workstation at INRIA where further processing revealed two twin points. Finally Harley computed the solution using information associated with these two points, thus nailing the problem.

The solution was found after less than one third of the predicted computation. The probability of finding the answer so quickly was less than one in ten. Two other twins were detected a few hours after the first - a less than one in 100 probability! Nevertheless the computing power used, around 16,000 MIPS/years, was twice as much as that used for the factorization of RSA-155 announced by Herman Te Riele of CWI (Amsterdam) and his colleagues on 26 August 1999.

"These results strengthen our confidence in codes based on properly-chosen elliptic curves," said Harley. "This needs to be taken into account in standards for security and confidentiality on the Internet."

According to Andrew Odlyzko, Head of Mathematics and Cryptography Research, at AT&T Labs, the code-cracking operation was "a great achievement that demonstrates the value of fruitfully harnessing some of the huge computational power of the Internet that is idle most of the time". He added: "It validates theoretical security predictions, and demonstrates the need to keep increasing cryptographic key sizes to protect against growing threats."

Arjen K. Lenstra, Vice President at Citibanks's Corporate Technology Office in New York and one of the main contributors to the recent successful attack on the RSA-155 challenge, compared the two computational efforts and noted that the present result makes 160-bit ECC keys look even better compared to 1024-bit RSA keys, from a security point of view. "Ideally we would like new theoretical advances to further reinforce these practical results, although such advances appear out of reach for the moment."

Out of the $5000 prize money, the team members will give $4,000 to the Free Software Foundation to encourage the creation of new free software. The remaining $1,000 go to the team members who identified the twin points. Both were in fact found by Paul Bourke using a network of Alpha workstations, mainly used for studying pulsars at the Centre of Astrophysics at Swinburne University in Australia.

The most active teams in the project were:

Astrophysics & Supercomputing	Australia
INRIA	France
University of New South Wales	Australia
"Friends of Rohit Khare"	USA and France
Ecole Polytechnique	France
Compaq	USA and Italy
Technischen Universitat Wien	Autriche
University of Vermont	USA
"WinTeam"	International
British Telecom Labs	UK
Internet Security Systems	UK
Rupture Dot Net	USA
"Jabberwocky"	USA
Ecole Normale Superieure de Paris	France

For a complete list of participants consult the project's Web pages.

Further information:
The ECDL Project
http://cristal.inria.fr/~harley/ecdl/

The Certicom ECC Challenge
http://www.certicom.com/chal/

Technical contact:
Robert Harley, INRIA :
33 1 39 63 51 57 - Robert.Harley@inria.fr

Media contacts:
Christine Genest, INRIA :
33 1 39 63 55 18 - Christine.Genest@inria.fr
Sylvie Baranger, Andrew Lloyd & Associates :
33 1 43 22 79 56 - sylvie@ala.com

Data k příloze poskytl :
Ing.Jaroslav Pinkava, CSc. (člen IACR, GCUCMP)
AEC Ltd.
Bayerova 30 tel./fax: +420 (0)5 4123 5466-7 / 41235038
602 00 Brno mobil: 0602 845 027
Czech Republic HotLine: +420 (0)5 4123 5468

INTERNET: e-mail : jaroslav.pinkava@aec.cz