October 24, 1997

Cracked Code Reveals Security Limits

By PETER WAYNER

I n a development that underscores the limits of computer security, RSA Data Security on Wednesday announced that a team of programmers known as the Bovine RC-5 Cooperative broke one of RSA's encryption codes in 250 days and claimed a $10,000 prize.

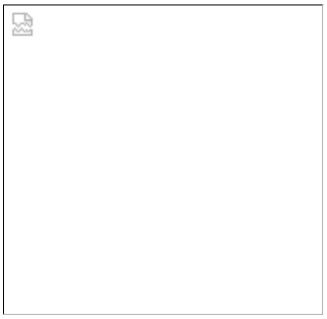

Illustration: Nicole Schooley

While the sport of large scale computing projects may never attract the number of fans that flock to a major sporting event, the team's success offers a vision at how large computing projects will be tackled in the future. The Bovine group won because they attracted tens of thousands of people on the Internet to run their program on their own idle machines — a practice known as distributed computing — by promising them $1,000 of the prize money if they happened to be the lucky one to break the code.

RSA Data Security has long offered prizes to people who attack their codes so they can assess the codes' strength. In this case, the Bovine group — which beat out two other groups, the Infinite Monkeys and Cyberian — was able to crack the 56-bit version of RSA's proprietary cipher, RC-5, in about 250 days, providing a benchmark of its security. Someone who might want to protect data for a day, perhaps a company announcing its quarterly earnings in the next 24 hours, could feel secure. But a company protecting an important secret, like the formula to Coca-Cola, would want a stronger code.

The contest also has political ramifications because the United States government has used key length as one significant measurement that guides its decision of whether a piece of software can be exported. In the past, the government only allowed software that uses 40-bits of key to be exported — a level of code that has been cracked in several hours with a modern machine. Today, software providing 56-bits of encryption strength can be exported if a company takes steps toward implementing the government's planned key-recovery scheme, which would give law enforcement officials the ability to decrypt computer messages.

Today in CyberTimes

ARTICLES AND COLUMNS

Cracked Code Reveals Security Limits
By Peter Wayner

Online Fans and Band Transform Each Other
By Lisa Napoli

Senate Panel Votes to Block Access to Gambling Sites
By Jeri Clausing

In June, a group of computer programmers announced that they had succeeded in cracking the full 56-bit version of the government's Data Encryption Standard, or DES, using distributed computing.

The Bovine's group success gives the software industry additional ammunition to prove that the current export limitations force people to use insecure encryption, endangering their privacy, their industrial secrets and their intellectual property. The industry can argue that even the 56-bit strength technology is not desirable, placing U.S. software companies at a disadvantage when competing against Japanese, Russian, and German corporations that do not face such government limits.

Each additional bit in a key doubles the number of possible keys and thus the length of time that a brute-force attack must spend trying all of them in hope of finding the correct one. A 41-bit key should take twice as long to break, on average, as a 40-bit one.

The Bovine group is already at work on RSA's next challenge, a 64-bit version of its RC-5 cipher. This should take 256 times as much work as the current challenge.

Occasionally, clever mathematical insight can significantly reduce the amount of time spent on the project by eliminating the keys. This was not the case in this attack. Each

Leveraging Government Into New-Media Enterprise
By Jason Chervokas & Tom Watson

INTERNET Q&A
By John C. Freed

TODAY'S SECTION FRONT

SEVEN-DAY INDEX

CYBERTIMES FORUMS

CYBERTIMES NAVIGATOR

key was equally likely to be the right choice, effectively making this a lottery. The software produced by three Bovine group members, Adam L. Beberg, Jeff Lawson and David McNett, simply parceled out blocks of keys to all of the volunteers. Each block contained 268,435,456 keys and there were 268,435,456 blocks to be checked, or over 72 quadrillion total keys.

A 200 MHz Macintosh with a 604e chip could exhaust one block in about 7 minutes and a 200MHz PC with a Pentium Pro chip would take about 9 minutes. A Cray computer may even take much longer because it doesn't include the "rotate left" function and must simulate it with three other functions. Many other popular and otherwise powerful chips also share the same limitation.

In this case, the correct key was found by group led by Jo Hermans, the systems manager at the Computer Science Department (DINF) of the Vrije Universiteit (VUB) in Brussels. He was able to get about 40 people in the lab to run the program on their machines, churning through an average of 10,000 blocks each day. About 47 percent of the entire 72 quadrillion keys had been checked at the end of the 250 days.

The actual key (532B744CC20999 in hexadecimal) was found by Peter Stuer, a researcher at the lab, with his 200 MHz Pentium Pro. This key would decrypt the secret message correctly and reveal the text: "The unknown message is: It's time to move to a longer key length." The researchers knew they were correct because RSA had announced that the right answer began with the phrase "The unknown message is:".

Hermans credited his success in motivating the people at the lab to "promising the students a lot of beer" and said that he will spend the $1,000 from the prize for a party in several weeks. The Bovine group will keep $1,000 and donate the other $8000 to the Gutenberg Project, another group on the Internet devoted to creating a electronic collection of some of the most important texts from history.

Related Articles
Surprise Bill Disrupts Encryption Debate
(June 21, 1997)

Distributed Computing: It Takes a Global Village
(May 28, 1997)

Breaking Down the Search for Extraterrestrials With Distributed Computing
(June 4, 1997)

The Bovine group is already at work on their latest version of the software that parcels out work to the machines volunteering to do it. This new version will allow the central machine to place time limits and restrictions on the work. In the future, the group hopes to attack other distributed-computing problems, like playing chess or attacking some of the large computational problems involved in the human genome project.

The success of this problems opens up new avenues for marshaling enough computer resources to accomplish tasks. It is conceivable that a company might run a similar lottery on the Internet instead of buying a powerful supercomputer like a Cray. A drug company could simply offer a prize of $50,000 to the first machine on the Internet to luck upon a solution to their drug design problem instead of investing millions of dollars in a proprietary computer.

Not all problems lend themselves to solutions like this. Brute-force attacks on codes do not require the many machines to do much to coordinate their effort. In this case, several central servers passed out the blocks of keys and checked them off a master list. The thousands of machines did not talk to each other.

Other problems are not so easy to orchestrate. For instance, computerized chess playing is also a fairly crude, brute-force search for the move that seems to be the best, but lack of coordination can lead to much wasted effort. Imagine that one machine is assigned the job of determining the value of moving a pawn and it quickly discovers that the move is essential to prevent checkmate. The other machines in the network would continue examining the value of moving knights, rooks and bishops unless they were stopped and redirected toward solving the most important problem.

One of the most fascinating areas of research today is how the Internet can be used to economically solve these problems. In the 80's, Bernardo Huberman and Tadd Hogg, two researchers at Xerox's Palo Alto Research Center, experimented with allowing projects to bid for work on the different machines in the laboratory. The price to attack a block of work like checking some keys would be set by auction and fluctuate throughout the day as supply and demand ebbed and flowed. Prices would dip as people went to lunch, freeing up their machine to accept outside work and rise again when they returned, to create more jobs competing for the resources. Many other researchers are now looking at similar problems.

A similar bidding war evolved during the course of this contest. Hermans said he chose to devote his machine to running the Bovine group's effort because they were the first to attack the problem.

The effects of competition clearly took hold. At the end, the Infinite Monkey group was promising $8,000 to the

person owning the machine lucky enough to find the right key. They hoped this would make up for a late start -- the Bovine group had already run through 20 percent of the keys when the Infinite Monkeys began. This was not enough to catch up and they only managed to examine less than 2 percent of the entire set of keys by yesterday.

The success in marshaling forces was clearly important. The Infinite Monkeys hit a peak of more than 662 million keys per second, something that was equivalent to about 1,200 Pentium Pro 200s at work. The Bovine group, on the other hand, was churning through keys about 10 times faster at what they estimated was about 14,000 Pentium Pros working simultaneously.

In an interview on Thursday, Dave McNett, the main spokesman for the Bovine Team, downplayed the to find a participant who was in it for the money." he said. "Anyone with the smallest grasp of the mathematics realizes that the chances are slim to nil. Really, I think there is a lot of dedication to our goals of developing distributed computing."

McNett also said that the decision to give so much to charity also inspired people to join the Bovine team. Everyone involved had only a small chance to win the money, but someone who ran the Bovine software increased the chances that Project Gutenberg would be rewarded. His team is currently looking for a worthy charity to reward when they finish attacking the next project.

Steve Curry, a programmer at Unibuilt Technologies in Oklahoma, said his office devoted three Pentium Pro machines to the Cyberian team. He chose to align with them because, "They looked like they were pretty organized and it didn't hurt that they were going to pay $5,000." The extra load did not seem to affect the people using the machines. He said that he was proud that his office ranked 228th although other offices devoted many more machines.

Right now, the Bovine team is producing the third version of its software, called "v3," and planning to attack RSA's challenge to break the 64-bit version of its RC-5 cipher. It is also joining a search for Mersenne primes.

Adam Beberg, the main architect of the system, just announced, "If v3 is everything I'm designing it to be, someday you'll be telling your kids you where there when *the* Net began."

Related Sites

Following are links to the external Web sites mentioned in this article. These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability. When you have finished visiting any of these sites, you will be ableto return to this page by clicking on your Web browser's "Back" button or icon until thispage reappears.

- RSA Data Security
- The Bovine RC-5 Cooperative Home Page
- Jo Herman's HomePage
- The Cyberian Page
- Infinite Monkey Home Page
- Speed Rankings of Various Machines in the Bovine Cooperative
- Project Gutenberg's Home Page

Peter Wayner at pwayner@nytimes.com welcomes your comments and suggestions.
