Distributed Team Cracks Hidden Message in RSA's 56-Bit RC5 Secret-Key Challenge

, Wednesday, October 22, 1997 ð

Distributed Team Cracks Hidden Message in RSA's 56-Bit RC5 Secret-Key Challenge

Fourth Break in Challenge Series Underscores Need for Legislation Allowing Longer Keys

REDWOOD CITY, Calif., October 22, 1997 -- For the fourth time since the launch of RSA's Secret-Key Challenge in early 1997, a team of programmers has cracked a message encrypted with a key length allowed for export by the U.S. government. Armed with an estimated tens of thousands of computers linked over the Internet, more than 4,000 teams, collectively known as the Bovine RC5 Effort, solved the $10,000 56-bit RC5 Challenge sponsored by RSA Data Security, Inc., a wholly-owned subsidiary of Security Dynamics Technologies, Inc. (NASDAQ: SDTI). In June of this year, a team of university students, programmers and scientists solved another RSA Secret-Key Challenge when it cracked a message encrypted with the government's own 56-bit Data Encryption Standard (DES) algorithm.

The Bovine RC5 Effort, led by Adam L. Beberg, Jeff Lawson, and David McNett, used networked CPUs throughout the U.S., Europe, Asia, Australia, and elsewhere to work their way through 72 quadrillion possible keys to solve the challenge and decode a message encrypted with the RC5 algorithm and a 56-bit key. The message discovered was ñIt is time to move to a longer key length.ò

The Bovine RC5 Effort started the project in March of this year, and searched approximately 34,225 trillion keys at a peak rate of over 7 billion keys per second. With over 72 quadrillion possible keys (72,057,594,037,927,936), the winning key was reported to RSA after searching a little more than 47 percent of the total. According to McNett, the success of the project was really due to the thousands of people who banded together and offered their time and their computer's idle processing time to help crack the code.

McNett, along with colleagues Beberg and Lawson, organized the effort and managed the back-end servers that were necessary to distribute and coordinate 268 million key blocks to all of the team participants. The actual computer that found the winning key was a Pentium Pro 200 running MicrosoftÈ Windows NT Workstation.

"RSA congratulates the Bovine RC5 team in cracking the 56-bit RC5 message," said Jim Bidzos, president of RSA. "As with the break in the DES encryption standard achieved earlier this year, the Bovine RC5 team's success again demonstrates that an organized group using ordinary desktop computers can crack encrypted messages in alarmingly brief times where short keys are used.

"This underscores the conclusion that short, 56-bit key lengths and algorithms with fixed key sizes are unacceptable as national standards for use in commercial applications. Fortunately, RC5 was designed to allow software developers to choose longer key lengths to provide great resistance to brute force attacks. RSA has long recommended 128-bit keys for use with RC5."

In the U.S., 128-bit encryption is used in products such as Netscape Communications Navigator and Microsoft Corporation's Internet Explorer to support secure online banking and other applications that require high levels of privacy.

Bidzos added, "This further indicates how the administration is out of step with the real world. RSA intends to continue sponsoring the RSA challenge to demonstrate the flaws in the most recent administration proposal, Bill S.909, "The Secure Public Networks Act of 1997," introduced by Senator John McCain (R-AZ) and Senator Bob Kerrey (D-NE). This bill, if passed, would harm U.S. industry by limiting exports to the 56-bit DES standard."

According to McNett, "This achievement by the team clearly points to the incredible collective computing power that is available. But more importantly, it shows the need for stronger encryption and the need to take a hard look at the government's cryptographic policies. If a loosely organized group can cooperatively break the code using ordinary PCs in their spare time, it certainly supports the need to rethink our current encryption export policies and standards."

Established in 1997, RSA's Secret-Key Challenge is offered to demonstrate the modest level of security in the encryption technology currently allowed to be exported under past and current U.S. government policy. U.S. policy on cryptography currently allows export of only 40-bit encryption technology with exceptions possible for 56-bit algorithms.

About RC5

RC5 is a high-performance, variable key length data encryption algorithm invented by Ron Rivest, a noted cryptographer, co-founder of RSA Data Security, and co-inventor of the well known RSA Public Key Encryption algorithm. RC5 is designed to provide fast, robust encryption for message-oriented data transmission, and offers developers flexibility in tuning the algorithm for maximum performance on various microprocessor and system platforms, as well as the capability to adjust the level of security to meet the needs of the application. RC5 is available for license on a wide variety of platforms from RSA Data Security, Inc.

About RSA Data Security

RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics Technologies, Inc., is the world's brand name for cryptography, with more than 80 million copies of RSA encryption and authentication technologies installed and in use worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, CCITT, ISO, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. RSA develops and markets platform-independent developer's kits and end-user products and provides comprehensive cryptographic consulting services.

Founded in 1982 by the inventors of the RSA Public Key Cryptosystem, the company is headquartered in Redwood City, Calif.

Top of Page
Email to a Friend
Print

É 2005 RSA Security Inc. All rights reserved. | Privacy | Legal

Subscribe: email address
GO