Press Releases

Swiss-based Ph.D. Student Solves 48-bit Key in RSA Data Security's Secret-Key Challenge

, Friday, February 14, 1997 ð

Swiss-based Ph.D. Student Solves 48-bit Key in RSA Data Security's Secret-Key Challenge

Search rate by 3,500 computers reaches 1.5 trillion keys per hour

REDWOOD CITY, Calif., February 14, 1997 -- RSA Data Security, Inc., a wholly-owned subsidiary of Security Dynamics Technologies, Inc. (NASDAQ: SDTI), today announced that the 48-bit encryption challenge, posted on RSA's World-Wide Web site on January 28, was solved February 10 by a cryptographer in Switzerland. More than 3,500 host computers were linked over the Internet to find the key, with a peak key search rate of 1.5 trillion keys per hour.

As expected, the key search was solved after exhausting approximately 57 percent of the total available key space, close to the 50 percent statistical average.

RSA's Secret-Key Challenge is being 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. The 48-bit codebreaking effort was headed by Germano Caronni, a student at the Swiss Federal Institute of Technology who is working on a Ph.D. in communication security. Caronni, using his own workstation and an extended client/server program he wrote in 1992, solicited help via newsgroups and mailing lists on the Internet. Starting with a group of 800 computers and working up to 3,520 computers donating their idle time, the program parceled out blocks of keys to test. Using a "brute force" technique, the correct key was found after 312 hours of processing. The winners will receive $5,000 from RSA for their effort, and the funds will be donated to Project Gutenberg at http://www.promo.net/pg/.

The solved message was encrypted with RSA's RC5 encryption algorithm. Although the key for the particular message was found, the algorithm itself remains valid, since a comparable effort would be required to break any other similarly encrypted message. However, RSA believes this event

demonstrates the need for longer keys.

"You don't want to use keys that are so short that anyone on the Internet could simply harness the idle processing time of other people's computers, with their cooperation, to reveal private and personal information," said Jim Bidzos, president of RSA. "With the Internet and today's desktop and workstation computers, it is entirely reasonable to crack Data Encryption Standard (DES)-encrypted and other 56-bit encrypted messages in such a short time that it makes the algorithms very questionable for use in commercial applications."

In fact, the same group that solved the 48-bit key is already planning an assault on the 56-bit key, also part of RSA's contest. "I am aware that the effort is much higher, but the computing power we saw during the last two weeks is so strong that we imagine that there could be enough power collected to solve 56-bit DES in several months," Caronni said.

Currently, U.S. policy on cryptography allows export of only 40-bit encryption technology with exceptions possible for 56-bit algorithms. "We believe the policy should be uniform worldwide," Bidzos said. "In our opinion, 40-bit encryption is completely unacceptable for commercial use and therefore, the government policy is untenable. It is also our opinion that 56-bit DES, even though it's much stronger than a 48-bit key length, is still not acceptable because it is still practical for someone to crack open a message using borrowed processing time. We aim to prove that in this challenge."

The implication, Bidzos stated, is that baseline encryption for commercial purposes needs to be raised to a much higher level. "We at RSA believe that the standard for encryption key lengths should be 128 bits, which is the currently-supported maximum key length for RSA's RC4 and RC5 algorithms and other symmetric algorithms that RSA provides," he said. Several scientific panels have recommended key lengths no shorter than 90 bits as the minimum acceptable length to assure long-term message security.

RSA Data Security, Inc.

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. The company 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