Press Releases

Team of Universities, Companies and Individual Computer Users Linked Over the Internet Crack RSA's 56-Bit DES Challenge

, Thursday, June 19, 1997 ð

Team of Universities, Companies and Individual Computer Users Linked Over the Internet Crack RSA's 56-Bit DES Challenge

Landmark Breaking of 56-bit Government Encryption Standard Calls Administration Policy Into Question

REDWOOD CITY, Calif., June 19, 1997 -- In a remarkable demonstration of collective computing power, a team of university students, programmers, and scientists linked together thousands of computers over the Internet to solve the $10,000 DES Challenge sponsored by RSA Data Security, Inc., a wholly-owned subsidiary of Security Dynamics Technologies, Inc. (NASDAQ: SDTI).

The DESCHALL effort, led by Loveland, Colorado computer programmer Rocke Verser, used networked CPUs from universities and corporations throughout the U.S. to apply "brute force" computing power to solve RSA's challenge and break a message encrypted with the government's 56-bit Data Encryption Standard (DES) algorithm.

The message discovered by the winning team was "Strong cryptography makes the world a safer place."

According to Mr. Verser, the DESCHALL team started their effort in February of this year, and searched nearly 18 quadrillion keys at rates of up to 601 trillion keys per day. Computers participating in the challenge aimed to try every possible decryption key to crack DES. There are over 72 quadrillion possible keys (72,057,594,037,927,936). At the time the winning key was reported to RSA, according to Mr. Verser, the DESCHALL effort had searched almost 25 percent of the total. Mr. Verser indicated that, at its peak, the DESCHALL effort was testing nearly seven billion keys per second.

According to the DESCHALL team, this effort was equivalent to, "searching for a needle in a haystack, where the haystack is 2.5 miles wide and one

mile high."

The actual computer that found the winning key was a 90 MHz Pentium desktop machine with l6 megabytes of random access memory (RAM).

"RSA congratulates the DESCHALL team for their achievement in cracking the 56-bit DES message," said Jim Bidzos, president of RSA. "This demonstrates that a determined group using easily available desktop computers can crack DES-encrypted messages, making short 56-bit key lengths and unscaleable algorithms unacceptable as national standards for use in commercial applications.

"This event dramatically highlights the fatal 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 severely hamper U.S. industry by limiting export to the 56-bit DES standard."

Bidzos continued, "This is another indication of how the administration is out of step with the real world. We intend to continue sponsoring the RSA challenge to demonstrate that scaleable algorithms and nothing less than 128-bit encryption will provide the security required for commercial applications."

"The government needs to take a hard look at its cryptographic policies," said Verser. "DES was cracked by thousands of users using ordinary PCs working cooperatively over the Internet. DES can no longer be considered secure against a determined adversary."

Widely used by the federal government, the DES algorithm is considered by many scientists and cryptographers to offer only marginal protection against attack, thus making it unsuitable for future commercial use.

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.

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