Press Releases

RSA's Secret-Key Challenge Solved by Distributed Team in Record Time

, Thursday, February 26, 1998 ð

RSAôs Secret-Key Challenge Solved by Distributed Team in Record Time

Team of Computer Enthusiasts Cracks Government-Endorsed DES Algorithm in Less Than Half the Time of Previous Challenge

REDWOOD CITY, Calif., February 26, 1998 -- Armed with tens of thousands of computers linked over the Internet, a coordinated team of computer programmers and enthusiasts known as distributed.net, this week solved the DES Challenge II sponsored by RSA Data Security, Inc. The distributed.net team met the challenge in 39 days, less than half the 90 days of computing time it took the original challenge to be solved by a university team.

RSA launched the original DES Challenge in January 1997 to demonstrate that 56-bit security, such as that offered by the governmentôs Data Encryption Standard (DES), offers inadequate protection against hackers. This vulnerability was confirmed when the secret key for encryption was recovered on June 17, 1997. The goal of subsequent challenges, such as DES Challenge II, is not only to recover the secret key used to DES-encrypt a message, but to do so in less time.

The distributed.net organization utilized the idle time of computers throughout the world to solve particularly arduous computing tasks. For the DES Challenge II, the team managed to coordinate the efforts of 22,000 participants throughout the world, linking together over 50,000 CPUs to power through 72 quadrillion possible keys. One by one, the computers crunched through all possible combinations until the winning key was found to decode the message encrypted with the DES algorithm. The message discovered read "Many hands make light work."

The distributed.net team started the project immediately after the DES Challenge II was announced on January 13, 1998 at RSAôs Data Security Conference in San Francisco. The team searched over 61 quadrillion, 254 trillion keys at a peak rate of 26 trillion keys per second. The winning key

was found by a U.S.-based machine powered by an Alpha CPU after searching 85 percent of the total.

"We're very appreciative of all the volunteers who offered their time and their computers's idle processing time to help crack the code," said David McNett, distributed.net co-founder and logistics coordinator. "Not only have we once again shown the collective computing power that can be applied to security technology with ordinary PCs's, but we've shown that it can be done even faster, in this case, less than half the time of the original DES challenge. We look forward to future RSA-sponsored challenges that will assist in exposing the need for stronger government-backed encryption standards."

"RSA congratulates the distributed.net team in meeting the second DES Challenge, and in stepping up to the time-oriented goals of the project," said Jim Bidzos, president of RSA. "RSA intends to continue sponsoring the RSA challenge to demonstrate the dire need to rethink our current encryption export policies and standards for use in commercial applications."

The Data Encryption Standard (DES) algorithm, adopted by the U.S. government in 1977, is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. The DES algorithm is widely used and is still considered reasonably secure.

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. (NASDAQ: SDTI), is a leading supplier of software components that secure electronic data, with more than 300 million copies of RSA encryption and authentication technologies installed worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ISO, ITU-T, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. RSA develops and markets platform-independent security components and related developer kits and provides comprehensive cryptographic consulting services. RSA can be reached at http://www.rsa.com.

Top of Page
Email to a Friend
Print

É 2005 RSA Security Inc. All rights reserved. | Privacy | Legal
Subscribe: email address
GO