CNN Custom News logo

October 24, 1997 8:10 pm GMT

Custom News Title

Ad Space

Word Theme

Home
World
U.S.
Weather
Sports
Business
Sci-Tech
Showbiz
Lifestyle
alt
On Target

Customiz Profile

Help
Feedback
Switch User

InfoSeel

Link of the Day

Video Pick of the Day

The story below was selected from CNN Custom News - a new personalized service that delivers only the news that's important to YOU.

Sign up now to receive your personal news stories, weather, sports scores, and stock quotes from over 100 different sources - all for FREE. If you're already a user, please login.

Custom News

Programmers Crack 56-Bit Rc5 Encryption

Ziff Davis Wire Highlights
23-OCT-97

ZDNet News (October 23, 1997) - The fourth of RSA Data Security Inc.'s 13 crypto-cracking contests, launched in January, is over. A team of some 4,000 programmers from across the globe, calling themselves the "Bovine RC5 Effort," has claimed the $10,000 prize for decoding a message encrypted in 56-bit RC5 code.

The massive endeavor, which involved tens of thousands of computers working since March to work through 72 quadrillion possible decoding keys, was completed this week after the group, led by programmers Adam Beberg, Jeff Lawson and David McNett, searched through 47 percent of the possible keys to find the one that revealed the message: "It is time to move to a longer key length."

Encryption software maker RSA is sponsoring the contest to prove its point that 128-bit encryption must become the standard. Under current U.S. policy, software makers can sell only 40-bit key encryption overseas, with some exceptions available for 56-bit algorithms.

The remaining challenges use progressively stronger versions of the variable key length RC5 encryption algorithm invented by RSA co-founder Ron Rivest. They increase in 8-bit increments, with every single bit increase doubling the strength of the key.

The first of the challenges, to decode a 40-bit key, was successfully met in 3 hours. The second challenge, a 48-bit key, took 13 days. The third challenge, to decode a message encrypted with a 56-bit DES algorithm, was overcome in June after five months of effort. The DES standard is considered weaker than RC5, according to RSA officials.

The team's success in breaking the 56-bit RC5 message "demonstrates that an organized group using ordinary desktop computers can crack encrypted messages in alarmingly brief times where short keys are used," said RSA President Jim Bidzos. "This underscores the conclusion that short, 56-bit key lengths are unacceptable as national standards for use in commercial applications."

RSA, in Redwood City, Calif., can be reached at (415) 595-8782 or www.rsa.com.

By Maria Seminerio Copyright (c) 1997 Ziff-Davis Publishing Company. All rights reserved. For additional Ziff-Davis online information, access Ziff-Davis on Compuserve (GO ZIFFNET) or ZD Net on the Internet (http://www.zd.com)

Search the net:
Seek [Help]
Ad Space

Copyright © 1997 Cable News Network, Inc. A Time Warner Company
ALL RIGHTS RESERVED.
Terms under which this information is provided to you.