THE DATA ENCRYPTION STANDARD: 20 YEARS LATER

Panel Chair
Dorothy E. Denning
Georgetown University, Computer Science Department
225 Reiss Science Building, Washington, DC 20057-1232
202-687-5703, denning@cs.georgetown.edu

Panelists
William J. Caelli
Queensland University of Technology, Information Security Research Center
2 George Street, GPO Box 2434, Brisbane Q 400 Australia
07-864-2752, caelli@fit.qut.edu.au

Stephen T. Kent
BBN Corporation
70 Fawcett Street, Cambridge, MA 02140
617-873-3988, kent@bbn.com

William H. Murray
Deloitte & Touche, Information Systems Security
49 Locust Avenue, Suite 104, New Canaan, CT 06840
203-966-4769, whmurray@ddtus.com

Panel Summary

Adopted as a FIPS in 1977, the Data Encryption Standard celebrates its 20th birthday along with the conference. During its lifetime, DES has stimulated considerable research and become the primary crypto engine in hundreds of products worldwide. It has been adopted by the international banking and finance community and been at the heart of debates over export control policy. Initially suspected of harboring secret trapdoors, it has withstood cryptanalysis by some of the world's best cryptographers. Its 56-bit key size, however, is no longer safe from brute force attack. In June 1997, a DES challenge key was broken after 4 months of trial-and-error testing by tens of thousands of computers on the Internet.

This panel will review the significance of DES to the information security field and to infosec products and practices. Panelists will discuss the impact of DES on academic research, cryptanalysis, algorithm and product development, standards, network security, application-level security, and business practices. The international adoption of DES, particularly for banking and financial transactions, will be discussed. Panelists will be asked to speculate on the impact of DES into the future. What are the implications of the DES challenge cipher being broken? Has DES reached the end of its useful lifetime? Does data stored under DES need to be re-encrypted? How can we migrate to a new standard? Will Triple-DES become the next standard?