DES 81: An Update

Miles E. Smid

National Bureau of Standards

Since the Data Encryption Standard (DES) was published in January 1977 as a Federal Information Processing Standard (FIPS), it has become the basis for several additional standards. Five DES related standards have already been approved, and at least eleven others are in progress. These will be produced by five standards standards-making organizations: the American Bankers Association (ABA), the American National Standards Institute (ANSI), the General Services Administration (GSA), the International Standards Organization (ISO), and the National Bureau of Standards (NBS).

The ABA has recommended that DES be used whenever encryption is needed to protect Personal Identification Numbers (PINs). The ABA is also in the process of producing a DES key management standard.

ANSI has adopted DES in a standard called the Data Encryption Algorithm (DEA). The DEA differs from the DES in that the DES permits only hardware implementations while the DEA allows both hardware and software implementations. The encryption algorithms of the two standards are identical. ANSI has several DEA standards under development in X3T1 (Encryption), X9A3 (PIN Security), and X9E8 (Financial Institution Message Authentication). These standards include a DEA Modes of Operation Standard, a Removable Storage Media Encryption Standard, a PIN Management and Security Standard, and a Financial Institution Message Authentication Standard. In Addition, there are efforts to produce encryption standards for layers 1, 2, 4, and 6 of the ISO Open Systems Interconnection - Basic Reference Model.

GSA is in the process of developing DES related standards through the Federal Telecommunications Standards Committee (FTSC). This committee of government representatives is in the process of producing GSA Federal Standards 1025, 1026, and 1027. 1025 deals with encryption at the Network and Transport layers of the Open System Interconnection - Basic Reference Model while 1026 covers the Physical and Link layers. 1027 will present the general security requirements for equipments using the DES.

In ISO there are plans to make DEA an ISO standard developed under Technical Committee 97. It has also been proposed that ISO TC68/SC2/WG2 adopt DES as a test key (financial message authentication) standard.

NBS published the original DES standard (FIPS PUB 46), a Guideline for Implementing and Using the DES (FIPS PUB 74), and the DES Modes of Operation Standard (FIPS PUB 81). The Bureau will continue to publish DES related ADP standards as the need arises. NBS has implemented DES in its Experimental Computer Facility to perform encryption, decryption, authentication, key and initialization vector generation, and key management. The knowledge gained in these projects will be useful in future standards efforts.

The activity of standards making bodies in developing DES related standards indicates a belief that encryption will play a significant role in the protection of sensitive data, and that standard techniques are needed to attain interoperability and security objectives.