New authentication code urged for digital data

June 3 2005

The National Institute of Standards and Technology (NIST) is recommending a new algorithm for authenticating digital data for federal agencies. Called CMAC (cipher-based message authentication code), the algorithm can authenticate the source of digital data, such as messages sent over the Internet, and thus provide assurance that the data have not been modified either intentionally or accidentally.

The main component of CMAC is a block cipher. Within encryption algorithms, block ciphers are used to scramble the data after they are broken down into blocks. In CMAC, the block cipher creates a digital tag that authorized parties can use to verify that the received message has not been altered.

Other authentication mechanisms, such as the hash function message authentication code (HMAC) and digital signatures, have long been available. CMAC is a new option, intended especially for devices in which a block cipher is more readily available than the components of these other mechanisms.

CMAC was submitted to NIST as part of an ongoing public effort to develop and update block cipher-based algorithms, called modes of operation. A team of Japanese scientists, Tetsu Iwata and Kaoru Kurosawa of Ibaraki University, developed CMAC based on an earlier proposal by a team of American scientists, John Black of the University of Nevada, Reno, and Philip Rogaway of the University of California at Davis.

Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication (NIST Special Publication 800-38B) is available at csrc.nist.gov/publications/nis … index.html#sp800-38B . It is the third of a series of publications recommending modes of operation to provide confidentiality or authentication for digital data. For more information, see csrc.nist.gov/CryptoToolkit/modes/ .

Source: NIST