New NIST document offers guidance in cryptographic key generation

December 13 2012

NIST's Special Publication 800-133 will help people find the specifics on how to generate cryptographic keys, used in secure data transmission and storage of sensitive information. Credit: Talbott/NIST

(Phys.org)—Protecting sensitive electronic information in different situations requires different types of cryptographic algorithms, but ultimately they all depend on keys, the cryptographic equivalent of a password. A new publication from the National Institute of Standards

and Technology (NIST) aims to help people secure their data with good keys no matter which algorithm they choose.

NIST Special Publication (SP) 800-133 offers guidance on generating the cryptographic keys that are needed to employ algorithms that provide confidentiality and integrity protection for data. Even if adversaries know what algorithm is used, they cannot gain access to the data unless they also have the proper key. SP 800-133 will be helpful to anyone who needs the specifics on how to generate these keys successfully, whether for secure data transmission or storage of sensitive information, to give two examples of their use.

SP 800-133 is primarily a high-level document that refers readers to other documents that contain details on generating the various types of keys. However, it does offer specific details for one type of key generation: the keys used in symmetric-key algorithms, in which the same key is used, for example, to both encrypt and decrypt data. Symmetric-key algorithms operate quickly, and the keys must be kept secret. These algorithms are used to protect sensitive information, including other keys, for which the algorithm is iterated as many times as needed to protect the information.

Another type of algorithm—an asymmetric-key algorithm—uses two keys: a public key that may be known by anyone, and a private key that is known by only one party and must be kept secret. Asymmetric-key algorithms are generally slower than symmetric-key algorithms and are used in cases where only a single operation of the algorithm is required, such as the generation of a digital signature or the encryption of a key to be used later with a symmetric-key algorithm. Details on the generation of keys for asymmetric-key algorithms are not offered in SP 800-133, but the document references others containing the key generation specifications.

The publication is part of a group of documents concerning cryptographic key management, namely SP 800-57 (parts one, two and three), SP 800-130, SP 800-152, and the Federal Information Processing Standard (FIPS) 186 Digital Signature Standard.

More information: csrc.nist.gov/publications/nis … 00-133/sp800_133.pdf

Provided by National Institute of Standards and Technology