

Note: this topic was not fully addressed due to time limitations and the complexity of the issues involved.

Definition

Security is understood to include protection of the privacy of information, protection of information against unauthorized modification, protection of systems against denial of service, and protection of systems against unauthorized access. Network security addresses these issues in a networked environment.

Standards

The development of network security standards facilitates the interoperability between security service implementations.

RSA

"RSA is a public-key cryptosystem for both encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It works as follows: take two large primes, p and q , and find their product $n = pq$; n is called the modulus. Choose a number, e , less than n and relatively prime to $(p-1)(q-1)$, and find its inverse, d , mod $(p-1)(q-1)$, which means that $ed = 1 \text{ mod } (p-1)(q-1)$; e and d are called the public and private exponents, respectively. The public key is the pair (n,e) ; the private key is d . The factors p and q must be kept secret, or destroyed." (<http://www.qualix.com/html/rsa.html>)

DES

"DES is the Data Encryption Standard, an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard; the details can be found in the official FIPS publication. It was originally developed at IBM. DES has been extensively studied over the last 15 years and is the most well-known and widely used cryptosystem in the world.

DES is a secret-key, symmetric cryptosystem: when used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography was invented to solve this problem." (<http://www.qualix.com/html/des.html>)

Capstone

"Capstone is the U.S. government's long-term project to develop a set of standards for publicly-available cryptography, as authorized by the Computer Security Act of 1987. The primary agencies responsible for Capstone are NIST and the NSA (see above). The plan calls for the elements of Capstone to become official U.S. government standards, in which case both the government itself and all private companies doing business with the government would be required to use Capstone." (<http://www.qualix.com/html/cstone.html>)

Clipper

"Clipper is an encryption chip developed and sponsored by the U.S. government as part of the Capstone project. Announced by the White House in April, 1993, Clipper was designed to balance the competing concerns of federal law-enforcement agencies with those of private citizens and industry. The law-enforcement agencies wish to have access to the communications of suspected criminals, for example by wire-tapping; these needs are threatened by secure cryptography. Industry and individual citizens, however, want secure communications, and look to cryptography to provide it." (<http://www.qualix.com/html/cstone.html>)

Skipjack

"Skipjack is the encryption algorithm contained in the Clipper chip; it was designed by the NSA. It uses an 80-bit key to encrypt 64-bit blocks of data; the same key is used for the decryption. Skipjack can be used in the same

modes as DES, and may be more secure than DES, since it uses 80-bit keys and scrambles the data for 32 steps, or "rounds"; by contrast, DES uses 56-bit keys and scrambles the data for only 16 rounds." (<http://www.qualix.com/html/cstone.html>)

DSS

"DSS is the proposed Digital Signature Standard, which specifies a Digital Signature Algorithm (DSA), and is a part of the U.S. government's Capstone project. It was selected by NIST, in cooperation with the NSA, to be the digital authentication standard of the U.S. government; whether the government should in fact adopt it as the official standard is still under debate. DSS is based on the discrete log problem and derives from cryptosystems proposed by Schnorr and ElGamal. It is for authentication only." (<http://www.qualix.com/html/cstone.html>)

Other Related Standards

NIST, NSA, MD2, MD4, MD5 (MD stands for Message Digest), SHS, Kerberos, RC2, RC4, PEM, RIPEM, PKCS, RSAREF.

Best Practices

The following security guidelines address the entire Internet community, consisting of users, hosts, local, regional, domestic and international backbone networks, and vendors who supply operating systems, routers, network management tools, workstations and other network components.

1. Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.
2. Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.
3. Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.
4. Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.
5. Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.
6. Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

Five areas should be addressed in improving local security:

1. There must be a clear statement of the local security policy, and this policy must be communicated to the users and other relevant parties. The policy should be on file and available to users at all times, and should be communicated to users as part of providing access to the system.
2. Adequate security controls must be implemented. At a minimum, this means controlling access to systems via passwords, instituting sound password management, and configuring the system to protect itself and the information within it.
3. There must be a capability to monitor security compliance and respond to incidents involving violation of security. Logs of logins, attempted logins, and other security-relevant events are strongly advised, as well as regular audit of these logs.
4. Up-to-date security information is a pre-requisite for sound decision-making and this information must be actively sought on an ongoing basis. The CERT Coordination Center (<http://www.cert.org>) is an excellent source for information relating to security issues on the Internet.
5. There must be an established chain of communication and control to handle security matters. A responsible person should be identified as the security contact. The means for reaching the security contact should be made known to all users and should be registered in public directories, and it should be easy for computer emergency response centers to find contact information at any time.
6. Sites and networks which are notified of security incidents should respond in a timely and effective manner. In the case of penetrations or other violations, sites and networks should allocate resources and capabilities to identify the nature of the incident and limit the damage.

Policies

On January 9, 1997, the Governor's Task Force On Information Resource Management released 'Technology Policy 97-1 Information Security Policy.' It states that "This document is designed to provide State agencies with recommended minimum security policies for protection of assets inclusive of information, computers, and networks." It provides physical access security guidances on Secure Locations, Location Selection, Review of New Collections to Outside Sources, Review of Installation, Platform-specific Physical Security, External Network Access to Agency Information, Transaction Controls and Database Security, Downloading Software, Non-Agency Owned IT Components, Agency Owned IT Components and Logging.