Encryption 3436

Technology, Computer

The electronic age has brought forth many technological advances. With these

advances came the need for security and tighter control on how we send

information electronically over the Internet or through a network. Date

encryption is, in its simplest terms, the translation of data into a secret

code. In order to read an encrypted file, the receiver of the file must obtain a

secret key that will enable him to decrypt the file. A deeper look into

cryptography, cryptanalysis, and the Data Encryption Standard (DES) will provide

a better understanding of date encryption. Cryptographic Methods There are two

standard methods of cryptography, asymmetric encryption and symmetric

encryption. Data that is in its original form (unscrambled) is called plaintext.

Once the data is scrambled and in its encrypted form it is called ciphertext.

The ciphertext, which should be unintelligible to anyone not holding the

encryption key, is what is stored in the database or transmitted down the

communication line. Asymmetric encryption (also know as public key encryption)

uses two separate keys, a public key and a private key. The private key is available only to the individual receiving the encrypted message. The public key is available to anyone who wishes to send data or communicate to the holder of the private key. Asymmetric encryption is considered very safe but is susceptible to private key theft or breaking of the private key (this is virtually impossible and would constitute trying billions of possible key combinations) (4). Types of public key algorithms include Riverst-Shamir-Adelman (RSA), Diffie-Hellman, Digital Signature Standard (DSS), EIGamal, and LUC (5).

Symmetric encryption uses only one key (a secret key) to encrypt and decrypt the message. No public exchange of the key is required. This method is vulnerable if the key is stolen or if the ciphertext is broken (4). Types of symmetric algorithms include DES, Blowfish, International Data Encryption Algorithm (IDEA), RC4, SAFER, and Enigma (5). Cryptanalysis Cryptanalysis is the art of breaking cryptography. Methods of cryptanalysis include: „ h Ciphertext-only attack ? V the attacker works from ciphertext only. The attacker does not know

anything about the message and is merely guessing about the plaintext (6). „ h

Know-plaintext attack ? V the attacker know the plaintext. Knowing this

information, the attacker can attempt to decrypt the ciphertext (6). „ h Chosen

plaintext attack ? V the attacker can have a message encrypted with the unknown

key. The attacker must then determine the key used for encryption (6). „ h

Man-in-the-middle attack ? V the attacker intercepts the key that is being

exchanged between parties (6). Data Encryption Standard (DES) In 1977 the

National Institute of Standards and Technology (NIST) and IBM developed the Data

Encryption Standard, or DES, to provide a means by which data could be

scrambled, sent electronically to a destination, and then unscrambled by the

receiver. DES was developed to protect data in the federal computer systems

against passive and active attacks (3). Every five years the NIST reviews the

DES and determines whether the cryptographic algorithm should be revised, is

acceptable, or completely withdrawn. DES uses a very complex algorithm, or key,

that has been deemed unbreakable by the U. S. government. There are

72, 000, 000, 000, 000, 000 (72 quadrillion) or more possible encryption keys that

can be used. It applies a 56-bit key to each 64-bit block of data. This process

involves 16 rounds of operations that mix the data and key together using

operations of permutation and substitution. The end result is a completely

scrambled data and key so that every bit of the ciphertext depends on every bit

of the data plus every bit of the key (a 56-bit quantity for DES) (2).

Conclusion Sending secure electronic information is vital for businesses today.

Although the electronic age has made it easier for companies to send and receive

information, it has also increased the need for security. Data encryption in

itself will not assure any business of sending secure information, but understanding it will surely benefit the company. Businesses who understand

cryptography, cryptanalysis, and Data Encryption Standard are on their way to

understanding data encryption.

Bibliography

1. Bay Networks, Inc. (1997). Configuring Software Encryption. www. baynetworks. com

2. Biasci, L. (1999). Cryptology. www. whatis. com.

3. Frazier, R. E., (1999). Data Encryption Techniques. www. softstrategies. com.

4. Litterio, F., (1999). Cryptology: The Study of Encryption. www. world. std. com.

5. SSH Communications Security, (1999). Cryptographic Algorithms. www. ipsec. com.

6. SSH Communications Security, (1999). Introduction to Cryptography.

www. ipsec. com.