Data Encryption

Data Encryption

Data Encryption means converting some easily readable information into a set of texts that appears unintelligible and not readily understandable. This minimises the chance of information leakage while storing and transmitting data. Therefore, data encryption is one of the effective solutions for protecting computer data.

Major Components in Encryption Solution

Data encryption solution includes the following major components:

- Encryption algorithm makes use of a set of mathematical calculation to generate a set of keys for encryption and decryption. The most commonly used encryption algorithm includes RSA, AES, etc.
- Encryption key can be classified as symmetric key and asymmetric key. Symmetric key means using the same encryption key for data encryption and decryption, which can apply to stored data, for example, AES is usually applied to data encryption for portable electronic storage devices. On the other hand, asymmetric key requires the use of a set of key pairs, in which one of the keys is used for encrypting the data. The encrypted data should be decrypted by the other key of the key pairs. Public Key Infrastructure (PKI) is an example using asymmetric key.
- Usually, with the same encryption algorithm, the longer the key length of the encryption key being used, the harder it is to decrypt the data.

How To Choose an Encryption Solution

Nowadays, some application softwares or operating systems come with data encryption features, which allow the document owner to use designated password to restrict other computer users from reading the encrypted document. If the data contains personal or sensitive information, one should choose more advanced encryption software or storage device that supports hardware encryption to encrypt thedata. Advanced software or device usually

employs a stronger encryption algorithm such as AES and fairly long encryption key.

If one needs to connect to the organisation's internal network through the Internet, an "encryptedtunnel" should be established. For example, Virtual Private Network is used to encrypt the data during data transmission.

Advantages of Encryption

Encryption is mainly used to protect data transmission and storage, and to strengthen its confidentiality. Encryption of data transmission can be used in e-commerce, Wi-Fi network security and remote access so as to reduce the risk of data tampering or theft. Encryption of data storage can be used on data, file, email or even the whole hard disk.

With organisations' growing dependency on information technology, the risk of leaking sensitive information in digital form keeps increasing. We should have a deeper understanding of encryption algorithms and adopt appropriate encryption solutions to prevent data leakage.

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk