Week 3 Case Study -

ABC Institute Encryption

Anthony Meunier

DeVry University

SEC 280

Week 3 Case Study – ABC Institute Encryption

There are two basic techniques for encrypting information: symmetric encryption and asymmetric encryption. The decision about which to use for purposes of securing data largely comes down to what the information is and how it is intended to be accessed. In a scenario in which information needs to be sent over the Internet, there is even merit to using facets of both encryption types in the exchange of information. Let’s explore how each of these encryptions types work, and then we can determine which use of them is best for our exchange of information at hand with XYZ Inc.

Symmetric encryption is the oldest and best-known technique when it comes to these two encryption methods. Symmetric algorithms (also known as “secret key”) use the same key both for encryption and decryption of data. This secret key, which can be a word, number or string of random letters, is applied to the message itself in a manner that changes the content in a particular way. An example of this change could be a shifting each letter contained in the message by a certain amount of alphabet places.

In symmetric encryption, the original message is plaintext while the encrypted message is called ciphertext. The ciphertext is what is sent out to the intended recipient, and by applying the private key and the correct/same symmetric cipher, the recipient can then decrypt and access the message. If the same key is always used for communication, then a presumed attacker would have access to all information exchanged with that key. To combat this, a session key can be generated which allows a key to be randomly generated and valid only for the one session; in this case, only the data exchanged in the session is tied to that key.

The alternative, and other, method of encryption is asymmetric encryption. This method is thought of to be more secure than traditional symmetric encryption. Asymmetric encryption (also called “public key”) uses different keys for encryption and decryption, rather than sharing the same key for both. In this sense, you can already begin to see how it can be more secure. Asymmetric encryption functions by using a key-pair, one private and one public. The public key is available for “everyone” but the private key is known only by the owner. If a message is encrypted with the public key, only the associated private key can decrypt it; any message encrypted with the private key can only be decrypted by using the matching public key. What makes this functioning and secure is the fact that the private key cannot be learned from the public one.

With symmetric encryption, anyone who knows the one and only secret key can then decrypt the message. In this type of encryption, there is always an inherent problem of the key needing to be managed. Because of the way key-pairs function, as described above, asymmetric cipher essentially solves the “problem” of secure key distribution and management. While asymmetric is typically much slower of an encryption process because of the complexity of the algorithm and how it operates, when secure distribution of keys (particularly when information is exchanged over a large network) is at the utmost priority, it is undeniable that asymmetric encryption is the go-to method. It is for this reason that I believe asymmetric encryption is the best encryption method for ABC Institute of Research to use in its collaboration with XYZ Inc.

References

Czagan, D. (2013, October 23). Symmetric and Asymmetric Encryption. Retrieved November 12, 2014, from <http://resources.infosecinstitute.com/symmetric-asymmetric-encryption/>

Young, B. *Lecture 44: Symmetric vs. Asymmetric Encryption*[PowerPoint slides]. Retrieved November 12, 2014 from University of Texas Computer Science Department <https://www.cs.utexas.edu/~byoung/cs361/lecture44.pdf>