Free computer system and data security essay example

Law, Security

The symmetric and asymmetric key encryptions are different operations, which functions in different circumstances, for different applications and different attack models. Therefore, it is not sensible enough to say that either symmetric or asymmetric is better than the other in terms of computer system and data security. If some measurable security could be available, then it could have been easy to tell which key is better. However, this measure is not simple to describe (Sudha, 2012).

The encryption key length or size defines the number of bits of the given security key that is employed in the algorithm of cryptography. This algorithm can either be a code or secret message. The cryptographic security is different from key length of an algorithm. The cryptographic security is determined by the measure of the logarithm of the fastest computational attack that is recognized which might be smaller. For instance, a key length of 168 bits for the case of Triple DES but, which offers a maximum of 112 bits has an attack level of complexity which is equivalent to 2 raised to the power of 112. This, in fact, is not a weakness as far as the characteristics of Triple DES is concerned as long as 112 bits is enough for the secret message application. The majority of symmetric key algorithms has security equivalent to their key length unlike asymmetric key algorithm with elliptic curve cryptography which possess an efficient security that is approximately half of its key size (Sudha, 2012).

If the user needs involves the use of protocol for data exchange with any other party that he/she do not trust like in the case of ABC Institute of Research collaborating with XYZ inc, than symmetric key cryptography on its own can not accomplish the security issue. As some ways of sharing, the

keys might be required. On the other hand, asymmetric cryptography like RSA is better suitable in this case if both ABC institute and XYZ Inc exchange public keys in advance. Nevertheless, there are also other possibilities of implementing this security issue apart from this option suggested. The process will, therefore, involve deciding whether RSA key length bears the correct strength the application (Sudha, 2012).

Each one of these two encryption methods has their strengths and limitations. For example, the disadvantage of asymmetric key is that it is exceedingly demanding. This is because it involves implementing encryption. Also, it can publish the ways for encrypting public key devoid of showing the ways of decrypting private key. The asymmetric key implementation also involves a lot of mathematical computations for algorithms hence harder to understand as compared to symmetric key encryption. In addition, the asymmetric method is quite slow in terms of execution and more so easy to mess up with due to its complexity. Symmetric encryption is also disadvantageous to use because it involves a lot of scrambling things which makes it hard to carry out an excellent job. The advantage of symmetric method is that it is simpler to understand than the asymmetric one. The symmetric algorithm is also faster in terms of execution speed. It is, therefore, not easy to mess up with symmetric key algorithm. Symmetric encryption is in addition, less expensive since it requires less processing than asymmetric encryption, that is, they are easy to decrypt as compared to the latter. The asymmetric key method is also advantageous. This is because it gives a higher level of security than the symmetric method when the key length is set longer in most circumstances.

Asymmetric key encryption is also best suited when a significant number of groups of people will be able to share information (Sudha, 2012, Babu, Abraham., & Borasia, 2013).

Given that the information must be kept top secret at any cost and none of the method seems to be perfect on its own, the best idea is to combine the two methods of key encryptions. This will ensure that the user maximizes security level by enjoying the strengths of the two key encryptions. As a result, it is now clear that the security strength is not dependent on either symmetric or asymmetric key encryption. The asymmetric encryption and decryption amid any two peers in the course of a given transaction only takes place during the initial handshake. After both the peers decide upon a private key, the symmetric encryption will be used for the rest of the communication. This means that the only costly operation is at the initial stage of handshake after when symmetric encryption is used which requires few resources (Sudha, 2012, Babu, Abraham. & Borasia, 2013).

References

Sudha, M. (2012). Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography. Advances in Computer Science and its Applications, 1(1), 32-37.

Babu, R., Abraham, G., & Borasia, K. (2013). A Review on Securing Distributed Systems Using Symmetric Key Cryptography. arXiv preprint arXiv: 1303. 0351.