Network Security Encryption

Charles Kanakan

Curry College

Network Security Encryption

The advancement of technology solves and causes new problems. In the world of networking this is very much the case. As Networks continue to get larger, security becomes a larger issue. This is where encryption comes into play. According to a study by Nie, Zhou, and Lu (2014) an encryption is defined as an algorithm that encrypts plain text into code that you need a key or a password to gain access to. Narayanan et Durai(2016) say the field of encryption is a very important subject today. The reason being that security attacks can cause serious damage to anyone that is the target. Encryption is used in several different applications. Narayanan et Durai(2016) says that some examples of application that uses encryption are medical imaging, internet communication, military communication, multimedia systems, telemedicine.

There are two types of encryption algorithms. They are called symmetric key encryption and asymmetric key encryption. Narayanan et Durai(2016) says that symmetric key encryption only needs one key or password to decrypt code used for security. The strength of this kind of encryption is based on how long the key is. The longer it is the better. The encryption key must be made and distributed before the transmission among entities. Another name for this encryption is secret key encryption.

According to an article written by Margaret Rouse titled A*symmetric Cryptography (Public Key Cryptography)* says that asymmetric encryption uses both public and private keys. The public key can be shared with any person. This is reaffirmed by Narayanan et Durai(2016) which also says that public keys are used for encryption, while private keys are used for decryption. This type of encryption uses mathematics, which makes it much slower than symmetric encryption which doesn’t. This creates a need for more processing power. Another name for this is public key encryption.

An example of encryption comes from a study by Chen, Jia, Huang, Lan, and Yan(2016) titled *A Secure Network Coding Based on Broadcast Encryption in SDN* along with a recurring issue concerning security encryption. Chen et al(2016) says that with the emergence of transmission applications, a major problem with the current transport mode is highlighted. The problem is that it is inflexible and it hinders development of networks. The reason is that it is not capable or structured to handle the requirements of the up and coming transmission applications.

A method that is being proposed that is called secure switch network coding(SSNC). Chen et al(2016) says that in SNCC intermediate nodes are allowed to encode packets that are received to improve the capacity for multicast groups. SNCC uses multiple multicast groups and turns it into a single multicast group. This allows for stronger encryption on applications.

In conclusion, I found out how important network security encryption is. There are many applications that use encryption. The reason is that they do not want to be subjected to a security attack. However, due the fact that networks aren't developing as fast as new transmission applications. It means that developing encryption methods for these newer applications is becoming difficult.

Citations

Chen, Y., Jia, H., Huang, K., Lan, J., & Yan, X. (2016). A Secure Network Coding Based on Broadcast Encryption in SDN. *Mathematical Problems In Engineering*, 1-8. doi:10.1155/2016/7145138

Narayanan, C. S., & Durai, S. A. (2016). A critical study on encryption based compression techniques. *Journal of Computers*, *11*(5), 380+. Retrieved from <http://libraries.state.ma.us/login?gwurl=http://go.galegroup.com/ps/i.do>

Rouse, M. (2016). *Asymmetric Cryptography (Public Key Cryptography)*. Retrieved from URL:<http://searchsecurity.techtarget.com/definition/asymmetric-cryptography>

Tingyuan, N., Lijian, Z., & Zhe-Ming, L. (2014). Power evaluation methods for data encryption algorithms. *IET Software*, *8*(1), 12-18. doi:10.1049/iet-sen.2012.0137