International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 464 - 465

Study of Network Security Using Cryptographic Techniques

Sanket Kadu
2nd Sem M.E., Department of CSE
PRMIT&R, Badnera

Prof. K.H. Hole
Asst. Professor, Department of CSE
PRMIT&R, Badnera

Prof. A.P. Ambarkhane
Asst. Professor, Department of CSE
PRMIT&R, Badnera

Prof. F. M. Shelke
Asst. Professor, Department of CSE
PRPCE&T, Amravati

***Abstract*—** In information security network security is one of the most important element because it is responsible for providing security to all information passed through network devices. Network Security refers to all hardware and software functions, characteristics, features, events, responsibility, measures, access control, and administrative and management strategy required to provide an acceptable level of protection & security for Hardware & Software and information in a network. merely one particular element underlies more of the protection mechanisms in use: Cryptographic technique hence focus is on this area Cryptography. It is an rising technology which is more important for network security.

***Keywords*—** *Network Security, access control, cryptography. management policy.*

*****

I. INTRODUCTION

Network Security & Cryptography is a term to protect network and data transmission over wireless network. Data Security is the main term of secure data transmission over unreliable network. Data Security is a challenging issue of data communications this days that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The fast development in information technology, the secure transmission of confidential data herewith gets a vast deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized person for malicious purpose. Therefore, it is necessary to apply effective encryption or decryption methods to enhance data security. It involves the access to data in a network, which is controlled by the network administrator. Users choose or are assigned an USER ID and password or other authenticating information that allows them access to information and programs within their authority.It covers a lot of computer networks, both public and private, that are used in everyday life for conducting transactions and communications among various businesses, government agencies and individuals. Networks can be private, such as within a organization, or others which might be open to public access. It does as its title explains: It secures the network, as well as protecting & overseeing operations being done. The most common and simple way of protecting a network resource is by giving it a unique name and a strong password [1].

II. . RELATED SURVEY

Sanchez-Avila et.al[4] analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and limitations with DES and T-DES. [4]. A. Murat Fiskiran et.al[5] showed some cryptographic algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, [5]. Aameer Nadeem et.al [6]presented, performance of 4 secret key algorithms (DES, 3DES, AES, Blowfish) were compared by encrypting input files of various contents and sized on different hardware program. [6]. Kyung Jun Choi et.al[7] investigated various cryptographic algorithms suitable for used in wireless sensor network utilizing MICA z-type motes & Tiny OS is investigated. [7]. Susan et.al [8]concluded that the Security field is a new, fast moving career. A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students the skills necessary to become security analysts. [8]. Neetu Settia et. al [9]discussed the security and attack aspects of cryptographic techniques and also discussed the issues of security and various attacks. [9].

III. . CONCLUSIONS

Network Security is the delegant element in information security because it is responsible for securing all information passed through various networked computers. Network security consists of the provisions made in an underlying computer network infrastructure(CNI), policies adopted by the network administrator to protect the network and the network-accessible resources are from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have discussed various cryptographic techniques to increase the security of network.

IV. REFERENCES

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.
[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.
[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.
[4] Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.
[5] Murat Fiskiran, Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE

International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[6] Aameer Nadeem, Dr. M.Younus Javed, ―A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.

[7] Elkamchouchi, H.M; Emarah, A.-A.M; Hagras, E.A.A, ―A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes‖, the 23rd National Radio Science Conference (NRSC 2006).

[8] Like Zhang, Gregory B. White, ―Anomaly Detection for Application Level Network Attacks Using Payload Keywords‖**,** Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007).

[9] Suhaila Orner Sharif, S.P. Mansoor, ―Performance analysis of Stream and Block cipher algorithms‖, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[10] Punita Mellu & Sitender Mali, ―AES: Asymmetric key cryptographic System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[11] YudhvirSingh, YogeshChaba, ―Information Theory test based Performance Evaluation of Cryptographic Techniques‖ , International Journal of Information Technology and Knowledge Management, Vol 1,No.2,2008 , pp. 475-483.

[12] YanWang, Ming Hu, ―Timing Evaluation of known cryptographic Algorithm‖, International Conference on Computational Intelligence and security, 2009.