


Chapter 8

Network Security Approaches in Distributed Environment

Keshav Sinha

 <https://orcid.org/0000-0003-1053-3911>
Birla Institute of Technology, India

Partha Paul

Birla Institute of Technology, India

Amritanjali

Birla Institute of Technology, India

ABSTRACT

Distributed computing is one of the thrust areas in the field of computer science, but when we are concerned about security a question arises, “Can it be secure?” From this note, the authors start this chapter. In the distributed environment, when the system is connected to a network, and the operating system firewall is active, it will take care of all the authentication and access control requests. There are several traditional cryptographic approaches which implement authentication and access control. The encryption algorithms such as Rijndael, RSA, A3, and A5 is used for providing data secrecy. Some of the key distribution techniques have been discussed such as Diffie Hellman key exchange for symmetric key, and random key generation (LCG) technique is used in red-black tree traversal which provides the security of the digital contents. The chapter deals with the advanced versions of the network security techniques and cryptographic algorithms for the security of multimedia contents over the internet.

DOI: 10.4018/978-1-5225-7955-7.ch008

INTRODUCTION

Cryptology is defined from Greek word *kryptós* and *lógos* which means hidden word. Cryptography and Cryptanalysis is an amalgamation of cryptology. The art of hiding the readable data (according to the perception of a human being) into a non-readable format is known as cryptography. Cryptanalysis is the opposite of cryptography, where it converts the non-readable data into readable form, without knowing the algorithm of encryption. The word cryptography is originated from the Greek word “*kryptós*”, which means the art of writing or solving codes secretly. The first citation of the cryptography technique was in the form of hieroglyphics, dated back to 1900 B.C, that is during the time of Egyptian. In the year 1799, a French soldier found a black basalt slab, which was inscribed with the ancient script. The stone was in the form of irregular shape which contains three different types of scripts (i) Greek, (ii) Egyptian hieroglyphics, and (iii) Egyptian demotic. In the year 1790-1832, Jean-Francois Champollion was the first person who cracked the hieroglyphics code by using a Greek guide. Since the year 1802, the Rosetta stone has been kept in the British Museum, London. Modern day’s cryptography is very different from ancient cryptography. Now the encryption algorithm is very complicated and require huge computational time. Cryptography algorithm uses the number of shift rounds and XOR operation for decipherment. Due to the advancement in computing power, the future cryptographic algorithm works on quantum computation speed allowing use of large key size. The DNA cryptography is one of the kind of cryptographic technique which uses the perplexing genetic data for hiding and improve the genetic secrecy in the sequencing process. The term cryptology is offend used in the field of data transmission and storage.

Principles of Security

There are several types of security attacks are performed by hackers in real life. To tackle those attacks, there are sets of security principles which will help us to understand and find the possible solutions to those problems which is caused by the attackers. There are six principles of cryptography and security.

1. **Confidentiality:** It specifies that only the sender and the authentic user should be able to access the data. No third party will access the data without authorization.
2. **Authentication:** It is the mechanism to establishing a secure (authentic) connection between sender and receiver. It is mainly used in electronic transactions, and network handshaking.

34 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/network-security-approaches-in-distributed-environment/224449

Related Content

The Impact of Ontology on the Performance of Information Retrieval: A Case of Wordnet

Maria Indrawanand Seng W. Loke (2008). *International Journal of Information Technology and Web Engineering* (pp. 24-37).

www.irma-international.org/article/impact-ontology-performance-information-retrieval/2639

An Adaptive Approach Towards Computation Offloading for Mobile Cloud Computing

Archana Kero, Abhirup Khanna, Devendra Kumarand Amit Agarwal (2019).

International Journal of Information Technology and Web Engineering (pp. 52-73).

www.irma-international.org/article/an-adaptive-approach-towards-computation-offloading-for-mobile-cloud-computing/222720

Semantic Reconciliation of Electronic Health Records Using Semantic Web Technologies

Karim El Guemhiouiand Steven A. Demurjian (2017). *International Journal of Information Technology and Web Engineering* (pp. 26-48).

www.irma-international.org/article/semantic-reconciliation-of-electronic-health-records-using-semantic-web-technologies/176907

Performance Analysis of a Web Server

Lu Jijunand S. Gokhale Swapna (2010). *Web Engineering Advancements and Trends: Building New Dimensions of Information Technology* (pp. 230-242).

www.irma-international.org/chapter/performance-analysis-web-server/40430

A Prediction-Based Flexible Channel Assignment in Wireless Networks Using Road Topology Information

G. Sivaradje, R. Nakkeeranand P. Dananjayan (2006). *International Journal of Information Technology and Web Engineering* (pp. 37-48).

www.irma-international.org/article/prediction-based-flexible-channel-assignment/2617