Open access Journal International Journal of Emerging Trends in Science and Technology

Network Security and Cryptography

Author

Dr Daruri Venugopal

M. Tech; Ph.D; Ph.D (Post.Doc.)
Professor in Dept. of Computer Science & Engineering
Siddhartha Institute Of Technology And Sciences
Narapally, Ghatkesar, R.R. Dist.
Email: *Profdarurivg.edu@gmail.com*

Abstract

Network Security & Cryptography is a complicated and Historically only tackled by Well-trained and experienced experts. However as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. This research was written with the basic computer user and information system manager in mind, explaining the concepts needed to read through the hype in the marketplace. The hackers and virus writers try to attack the internet and computers connected to the Internet. The Network Security and Cryptography application is rapidly becoming crucial to the development of the internet. The open systems interconnection security architecture provides a systematic framework for defining security attacks, mechanisms, and services

Keywords: *Historical; experienced; wired; framework; hackers; crucial; architecture.*

Introduction

In the Last decade, the number of computers in use has exploded. The growth of this industry has been driven by two separate forces which until recently have had different goals. The first factor has been research interests and laboratories, these groups have always needed to share files, emails and other information across wide areas. Many research labs developed several protocols and methods for this data transfer, most notably TCP/IP. Business interests are the second factor in network growth. For unite sometime, businesses were primarily interested in sharing data within an office or campusenvironment. In the study of techniques for ensuring the secrecy and authenticity of information can be gathered from cryptology.

The combination of space, time and strength that must be considered as the basic elements of Network Security and Cryptography theory. Security attacks are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis; and active attacks, such as modification of messages or files, and denial of service. Security services include authentication, access control data confidentiality, nonrepudiation, and availability. The security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer.

Importence of Network Security and Cryptography

Peer entity authentication provides for the corroboration of the identity of a peer entity in an association. It is provided for use at the establishment of or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection. Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. When a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. As with confidentiality, data integrity can apply to a stream of messages, a single message, or selected fields within a message and it is most useful and straightforward approach with stream protection. In Banking sector Visual Cryptography is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveal the secret image.

We can make a distinction between the service with and without recovery. Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message. Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. With Routing Control enables selection of particulars physically secure routers for certain data and allows routing changes, especially when a breach of security is suspected. The different type of attacks such as Cipher text , Known plaintext, chosen plaintext, chosen cipher text, chosen text on Encrypted Messages can be controlled with the help of Cryptographic system

Problem Statement

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits then substitution involves replacing plaintext bit patterns with cipher text bit patterns. When letters are involved the following conventions are used. Plaintext is always in lowercase; cipher text is in uppercase; key values are in italicized lowercase. In the Substitution process of cipher The Caesar cipher involved replacing each letter of the alphabet with the letter standing three placed further down the alphabet. Example:

Plain: meet me after the toga party
Cipher: PHHW PH DIWHU WKH WRJD SDUWB

We can define the transformations by listing all possibilities plain: a b c ………………………x y z
Cipher D E F G ………………………… A B C

If we consider a=0, b=1 …….z=25
By substitution C=E(3,p)=(p+3) mod 26
A shift may be of any amount, so that the general Caesar algorithm is C=E(k,p)=(p+k) mod 26
Where ktakes on a value in the range 1 to 25. Then the decryption algorithm is simply
P=D(k,C) =(C-k) mod 26
In this process there are only 25 keys to try.

Objectives

Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building lock for computer security. The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information. The purpose of this Research provide a practical survey of both the principles and practice of cryptography and network security. In this process of Research the basic issues to be addressed by a network security capability are explored by providing a knowledge and survey of cryptography and network security technology. The major objective of this Research survey is a detailed examination of conventional encryption algorithms and design principles, including a discussion of the use of conventional encryption for confidentiality. Public-key Encryption and Hash Functions, Network security practices and system security.

Conclusion & Recommendations

In this Research paper I presented a comparative study of Substitution techniques for ensuring the secrecy and authenticity of information gathered from cryptology. This research topic provides an absorbing account of a probable – word attack. Majorly we can identify the role of Security services include authentication, access control data confidentiality, nonrepudiation, and availability. In this paper we can Recall that differential crypt analysis of DES requires Selective plaintext. If all you have to work with is known plaintext, then you must sort through a large quantify of known plaintext-ciphertext pairs looking for the useful once. A potential for violation of security, which exists when there is a circumstances, capability, action, or even that could breach security and cause harm. That is, a threat is possible danger that might exploit a vulnerability. This research paper focuses on internet security, which consists of measures to deter, prevent, detect and correct security, violations that involve the transmission of information.

References

1. Barker, W.Introduction to the Analysis of the Data Encryptionstandard (DES) Laguna Hills CA: Aegean Park Press,1991
2. Stinson, D.Cryptography: Theory and Practice, Boca Raton, FL: CRC Press,2002
3. Wayner, P.Disappearing, Cryptography. Boston: AP Professional Books,1996.
4. Sinkov, A. Elementary Cryptanalysis: A Mathematical Approach, Washington, DC: The Mathematical Association of America, 1966.
5. C.Security in Computing. Upper Saddle River, NJ : Prentice Hall,2005
6. Schneier, B.Secrets and Lies: Digital Security in a Networked World. New York: Wiley 2000.
7. G.R Blakley. Safeguarding Cryptographic keys.Proceedings of AFIPS Conference, 1970.

Other Recommendations

The following Websites are of general interest related to cryptography and network security:

COAST: Comprehensive set of links related to cryptography and network security.

IETF Security Area: Material related to Internet security standardization efforts.

Author Profile

Prof. Daruri Venugopal received the Bachelors and M.Sc. degrees in Mathematics from Osmania University in 1995 and 1997, respectively. He done his M.Phil Mathematics from Algappa University in the year 2003. He done his Doctorate from NITK, Surathakal in the year 2006 in Computer Science Engineering. He done his M.Tech Computer Science Engineering from JRN Deemed University in 2007. Presentpursuing the Post. Doctorate in Computer Science Engineering. He is a recognized Ph.D Supervisor in Rayalaseema University, A.P. and also, Three Other Technical Universities in southern part of India In Mathematics & Computer Science Engineering. He is Editorial Board Member and Reviewer for Three International Journals in Mathematics & Computer Science Engineering. Currently he is working as Professor &Academic Dean of Siddhartha Group of Institutions, Ghatkesar, Hyderabad.