International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

GROWTH INTERNET SECURITY INVIT ON CRYPHTOGRAPHY

K.PRIYA

Asst.professor.Dept.of.Computer science and Engineering,

Ramanujan Center SASTRA,Kumbakonam.

***ABSTRACT**--In this paper proposed the explosive growth in the Internet, network security has become an inevitable concern for any organization business internal private network is connected to the Organization. Network security is against unauthorized access, alteration, or modification of information, and unauthorized denial of service(DoS). When a network is connected to the network that is valuable to potential in the attacks. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology, which is important for network security. This paper covers the various cipher generation algorithms of cryptography which are helpful in network security.*

Keyword: CipherText, Cryptography

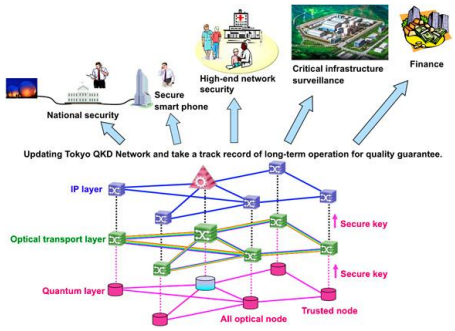
I.INTRODUCTION

The Network Time Protocol (NTP) is widely deployed in the Internet to synchronize computer time to national standards. The current NTP population includes over 230 primary servers and well over 100,000 secondary servers and clients. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the hierarchical network server-client topology and adjust the clock of each participant. It uses redundant servers, diverse network paths and crafted algorithms which cast out incorrect servers and minimize errors due to network latencies and clock frequency variations. The protocol can operate in peer-peer, client-server, and multicast modes, where the identity of the servers can be cryptographically authenticated. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronization source and network paths.,

Computer and network security is a new and fast moving technology and as such, is still being defined. When considering the desired learning outcomes of such a course, one could argue that a network security analyst must be capable of analyzing security from the business perspective in order to adhere to recent security legislation, and from the technical perspective in order to understand and select the most appropriate security solution. Network security [3] originally focused on algorithmic aspects such as encryption and hashing techniques. While these concepts rarely change, these skills alone are insufficient to protect computer

networks. As crackers hacked away at networks and systems, courses arose that emphasized the latest attacks. Currently, many educators believe that to train people to secure networks, they must also learn to think like a cracker [1-2]. The following background information in security helps in making correct decisions: Attack Recognition, Encryption techniques, Network Security Architecture, Protocol analysis, Access control list and vulnerability. For Network security cryptography is present. In cryptography [4] data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption. In cryptography three types of algorithms are present. Symmetric key algorithm, asymmetric key algorithm and hash function.

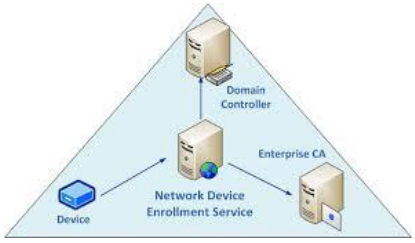
II.CRYPTOGRAPHY PUBLIC PROCESS:



The authentication scheme described in RFC-1305 is designed to support this security model. This scheme has since been augmented to include provisions for the MD5 message digest algorithm , in addition to the DES-CBC,algorithm. The scheme contains provisions to cryptographically authenticate individual servers operating in any mode using a symmetric-key cryptosystem and private keys. It is possible to engineer some interesting and useful security topologies by sharing a single key among a set of servers and clients. For example, a closely cooperating clique of primary servers operating in peer-peer modes can share a single key, in order to provide backup for each other if a radio clock source fails. This avoids having to distribute a different key to every server in the
clique. In another example, a set of servers can operate in multicast mode with a single key, so that a client population can synchronize to any of them without requiring separate keys for each one. While the current NTP security model and authentication scheme have been in use for well over a decade, there are several drawbacks, the most serious being the requirement that keys must be securely distributed in advance for all server-client pairs. There are no provisions in the NTP protocol specification for key distribution or management on the assumption these functions can be provided by standard network security services. Even if such services were available, the large number of associations, well over 250,000 in the current NTP subnet, would make the operations to securely manufacture and distribute keys and enforce their lifetimes very difficult to sustain. In addition, the recent addition of multicast modes raises new issues where the identity of servers is

not known in advance and their credentials must be determined using only public values.

III.CLIENT VERIFIES SIGNATURE:



To verify the signature, the client decrypts the MAC using the server public values, then compares the result with its own message hash. If the two values agree, the message must be authentic, since only the designated server has the corresponding private key. In practice, the public values must be cryptographically bound to the server name and address, as verified by a trusted certificate authority. A certificate including these values is then installed in the public services In principle, the encryption times can be measured in advance and used to correct time values. However, there
is a large variance in running times, depending on the 4 population of one bits in the key and other factors. For example, with random bit strings as keys, the Alpha requires a mean time of 80.4 ms; however the actual times range from 53.3 ms to 104.4 ms. Since time values must be obtained before encryption, these variations translate directly to timekeeping errors. While there are other schemes based on public-key cryptography, all are based on computation-intense algorithms and are likely to behave in a way similar to RSA. For these reasons, the auto key scheme does not require each message to be individually signed.

. IV.CRYPTO PUBLIC KEY :

A public-key cryptosystem requires reliable directory services to obtain the server public values, including the server name, network address, public key, modulus and optional certificates. In principle, these services are required to be synchronized to trusted sources only if they support encryption or decryption operations, since
these operations require keys with enforced lifetimes. Presumably, the availability and authenticity of the public values depend on databases accessible via inband or outband mechanisms; however, the ultimate decision on whether the data are authentic rests with the clients of these services, not the server itself.

CONCLUSION

This paper presents an overview of various block and stream ciphers and their algorithms, which are used in cryptography for Network security purpose. With the help of these cipher's algorithms one can generates its own cipher text algorithms by making modification into existing cipher text algorithms. Also performance evaluation of various ciphers can be done with the help of the cipher's

algorithms discussed about how to get clear security using on Cryptography services and deliver to network services present in this paper.

REFERNCES

[1] Mohamed A.Haleem, Chetan N.Mathur Chandramouli,K.P.Subbalakshmi,"Opportunistic Encryption: A tradeoff between Security and Throughput in Wireless Network" IEEE Transactions on Dependable and secure computing, vol. 4, no. 4.

[2] Dr. James H. Yu & Mr. Tom K. Le, "Internet and Network Security", "Journal of industrial technology",Volume 17, Number 1 - November 2000 to January 2001.

[3] Aameer Nadeem, Dr. M.Younus Javed, "A performance comparison of data Encryption Algorithm", Global Telecommunications Conference Workshops, 2004. GlobeCom Workshops 2004. IEEE

[4]Kyung Jun Choi, John –In Song, "Investigation of feasible cryptographic Algorithm For wireles sensor network", International conference on ICACT Feb 20-22,2006

[5]T.Muthumanickam,"PERFORMANCE ANALYSIS OF CRYPTOGRAPHIC VLSI DATA", IRACST – International Journal of Computer Networks and Wireless

.