SRENGHTENING THE IMMUNE SYSTEM OF A NETWORK

AUTHOR

Dr. Sriram A L
A.P.(III), Dept. of ICT.,
Sastra University,
Thirumalaisamudram,
Tanjavor.

CO- AUTHOR

Subramanian A L
Project Manager,
Mistral Solutions,
Banglore.

***ABSTRACT**:*

A strong immune system for a network system is very important and highly required need in data security as it reflects in the overall protection of the whole of the data and information that is traversed through the network. Here to achieve this both the software and hardware functions their attributes, functional way, features, accountability, quantity, data transfer control and administrational and managerial procedures need to furnish a minimum implementable level of securing both hardware and software, and the data contained inside a network. The most of the above mentioned need can only be satisfied and fulfilled through the application of different ciphering methods. The availability and apt usage of different ciphering methods is the latest available and widely applied in the latest research world for securing data.

Keywords---- Ciphering, data security, data transfer control, managerial skills.

1. INTRODUCTION

Improvising network immune system through ciphering methods is a concept to protect data in a network of both wired and wireless type. This is done to protect data that travel through unreliable network. In the communication part the security of the data is of prime importance as it covers many domains like highly protected communication channel, apt and appropriate use of ciphering methods and reliable source that maintain the information or data base. As with the high advancement of technical and information development and transfer there is a great emphasis on the protection and security of information. This can be realised only through the appropriate use of cryptography. There is always a great possibility of unauthorised and unwanted access of data so the only way out of this situation is the application of ciphering and deciphering methods which can effectively make the information immune system strong and secured. With the involvement of network administrator the security of the network can be achieved to some extend. With the proper id and password regulations the access and entry can be restricted and regulated. Both the pubic and private domains like those having everyday transactions and those involving businesses, those involving public enterprises are covered in this aspect of strengthening the immune system through encryption method. There are networks implemented in a private domain basis and can be accessed even by the publics. So this concept of strengthening the immune system is applicable to almost all the areas of network. The proposed system not only secures the data but strengthens the immune system as a whole by overseeing and watching the whole of the communication system.[1] The most effective and basic way of protecting a resource involved in a network is by assigning a unique name and password to it. The authentication is the first and the prime way to strengthen the immune system of a network. A token and another device like the ATM card the two factor authentication

and with an additional of finger print or retinal scan a three factor authentication is also implemented[2]. Even these two and three factor authentications utterly fail before viruses and other worms that are present in networks. An effective use of antivirus software and other intrusion prevention systems help in such situations. There are some other specialised dedicated intrusion detection systems that monitor the network and traffic toward untoward and unexpected encounters like the Denial of service or illegal and unauthorised access of data, and act in a wiser way to protect the resources. The entire privacy and protection between two communicating parties can be ensured only through the process of encryption.

a) RSA

RSA cryptosystems was put forwarded by Ron Rivest, Adi Shamir, and Len Adleman. Privacy and ensuring authenticity of digital data are the main factors provided by RSA.[9]

b) DH/DSA

An Entirely new type of cryptography called public key Digital Signature Algorithm was invented by Diffie and Hellman are based on the discrete log problem in a prime field Fp. The US government's National Institute of standards and Technology proposed a digital signature standard using DSA in 1991.

c) ECDH/ ECDSA

A new system called RSA was suggested by Rivest, Shamir, and Adleman in 1978 on the basis that it is difficult to factoring large integers. In 1976 a system based on public key called Diffie-Hellman key exchange was put forward by Whitfield Diffie and Martin Hellman.[10]In 1985 Elliptic curve groups was put forward that can be used in place for the multiplicative groups modulo p in either the DH or DSA protocols. In

2004 a group of researchers *Paul Kocher, Ruby Lee, Gary McGraw , Anand Raghunathan and Srivaths Ravi* did a study on the security aspects of embedded systems**.** In this paper the challenges involved in designing secure embedded systems has been introduced to the designers of embedded systems and design tool developers as such. An unified view of embedded system security by primarily analyzing the typical functional security requirements for embedded systems from an end user angle of view, then identify the implied challenges for embedded system architects, as well as hardware and software designers i.e., tamper resistant design, processing requirements for security, impact of security of physical factors such as battery life of such battery powered systems has been attempted to provide a solution through this paper. Another group of researchers in 2009 have implemented Elliptic Curve Cryptography (ECC) on an embedded multicore system, and tried to do an intense study on the task scheduling methods in different levels. An instruction scheduling method that utilizes all the cores to perform one modular operation in parallel has been proposed. Then multiple modular operations with multiple cores in parallel are performed. A scheduling method combining these two types of parallelism is proposed after doing a comparison study on the above. Then *Rahat Afreen and S.C. Mehrotra* (2011) proposed a study on public key cryptography (PKC) systems. In PKC system, to encode and decode the data we use separate keys. As one of the keys is distributed publicly, the strength of security depends on large key size in a PKC system. Previously the mathematical problems of prime factorization and discrete logarithm are used in PKC systems. After that R.L. Rivest, A. Shamir, and L. Adleman proposed a method for obtaining digital signatures and public-key cryptosystems.

2. SECURITY ASPECTS

The secure data falls in different categories requiring different levels of security.[40] Thus based on the user's classification for whom the data need to be protected the data type can be classified as first user's personal/private data and user's restricted data. The users private data are those data which when its security is compromised has a direct effect on the user are termed as personal or private data.[11] A user's internet banking password hacking can be viewed as a simple example of compromising on such security. If we compromise on the data or content's security then rather than the end user the author or the data provider fatally suffers the loss. Multimedia content that are digitalized such as digital photos, audio and video contents having copyright are examples of such data. The security of data is not only taken into account during data transfer through public network but also at most security concerns need to be stressed at the end user devices. Certain security breaches like secret keys that are used for encryption and decryption of data if at all goes into wrong hand then the entire security arrangements can go in vein. Same techniques are being followed by the protocols involved for the secure transmission of either of the data mentioned above through a public network. The way the user restricted data at the data source side involves very much care to ensure data safety even from the user itself. Thus every embedded system should implement methods or protocol to secure data transfer and it is a must to implement security methods so as to defeat attempts of unauthorized access of secure data from the system. The basic security requirements can be classified into two:

− Data transfer security and

− Device level security.

a) Data transfer Security

In a public network data need to travel through a n number of unreliable intermediate points. So data must be secured in such a way that the data hacked in between the source and correct destination will be in a confusing, useless or beyond the reach of other's intelligence. Thich can be realized with the aid of number of cryptographic methods like Encryption/Decryption, Key Agreement, Digital Signatures and Digital Certificates.

Data Encryption

Encryption is the process of scrambling or encrypting a portion or whole of the data by applying a secret key so as to make only the desired recipient with the corresponding key to receive and decrypt or descramble the data on the other side.

Among the available n number of publicly available cryptographic algorithm like DES, 3DES or AES or any algorithm invented by the device manufacturer to suite a particular demand any one can be applied for this purpose.[40] Only the end users i.e. the communicating ends will know the keys and can be even of length 100s of bits. The keys used for encryption and decryption should be kept highly secured and secret if we are using any publicly available algorithms. Distributing and maintaining the keys in a secret way between the end users involved without any unauthorized hackers getting the information regarding the keys is very important and vital for a successful and foolproof data communication. It is also possible to embed the keys within the device prior to the communication, i.e. they are exchanged offline in a secured way or using any key agreement algorithm to get established online.

b) Device level security

The main fore point in the security aspect is that the security of the data lies in the fact that it solely depends in the secrecy of the keys whether it is the private-key of any

public-key algorithm or it is any previously negotiated shared secret between the devices. To reinforce additional security, few cryptographic algorithms also specify a set of constant values that need not be disclosed from the device. The secret keys and secret values that are kept in the device that requires to be protected from unauthorized exposure are often referred as 'secret keys' in this document. The secret keys are kept inside the device, and some may even last for the lifetime of the device. The security measures that are embedded and implemented on the Hardware and software side of the device must defeat any attempts of unauthorized access to trace out these secret keys. Also, there are few data such as the Root CA Certificate in the device that can be shared with the outside world but need be prevented from unauthorized modification or deletion. If Root CA certificate was allowed to be modified, then the attacker can easily tamper and make the device to accept any certificate by substituting a fake root CA certificate and thus misleading and defeating the purpose certificate and secured communication. It is therefore of at most important that the security within the device is such that the data such as Root CA Certificates inside the device is not allowed to unauthorized modification.

3. A COMPARATIVE STUDY

Rijndeal cipher or new AES's design and structure was thoroughly analyzed by C.Sanchez-Avila categorizing its advantages and limitations and also he did a comparative study using the DES and T-DES and formulated its similarities and dissimilarities.[4] He also did a thorough comparative study taking the different algorithms like AES,DES and T-Des implemented upon different microcontrollers and concluded that AES consumes the cost factor as compared with the T-DES.A. Murat

Fiskiran proved by the application of some cryptographic algorithms that are applicable for systems with constrained and limited resources and environments like mobile information applications, where one has to retain the computation resources and the power availability that with an apt and appropriate usage and selection even ordinary processors can be used. The workload of systems with a set of key sets, symmetric key and hash algorithms that are applicable for an environment are being studied.

Algorithm	Data	Time(Seconds)	Average MB/sec	Performance
DES	256 MB	11	21	low
T-DES	256 MB	13	14	better
BLOWFISH	256 MB	4-4.5	64	high

Here with the application of different algorithms Diffie Hellman key exchange, AES, Hash and the instructions needed by them are studied and a comparison is done with simple RISC style processor with ALU and shifter. By these the work load characteristics are found out.[5] Aameer Nadeen also did a thorough study of four private key algorithms like DES, AES, Triple DES and Blowfish were compared by encrypting input files of various contents and sized on various hardware programs.

FACTORS	DES	T-DES
KET LENGTH	K1,k2 and k3—>168 bits K1 = k2=112 bits	56 bits
CIPHER TYPE	Symmetric block cipher	Symmetric block cipher
CRYPT ANALYSIS RESISTENCE	Vulnerable to differential brute force attacker could analyse plain text using differential cryptography	Vulnerable to differential and linear cryptanalysis weak substitution tables.
SECURITY	Only one weak which is exit in DES	Proven inadequate
POSSIBLE KEYS	2^{112} ,2^{168}	2^{56}
POSSIBLE ASCII PORTABLE CHARACTER KEYS	95^{16},95^{21}	95^{7}

TIME REQUIRED CHECKING ALL POSSIBLE KEYS AT 50 BILLIONS KEYS PER SECOND.	For a 112 bit keys 800 days	For a 56-bit key 400 days

For a uniform and unbiased comparison all the implementations are done on the same language following the standards applicable. The algorithms that are taken for study are being encrypted in Pentium-2 having 266MHZ and Pentium-4 with 2.4 Mhz so that the standard and time of execution is almost same and one can do a fair comparison study. The results of the study on the basis of their performance have been tabulated and analysed a trade off between performance and security and a conclusion has been presented. For the studies java has been taken and it has been found that blowfish was the faster algorithm as compared to other cryptographic algorithms and the results have been given in ECB mode for the block ciphers and in the CFB for the stream ciphers and has been concluded that an algorithm having much more complex rounds and a larger number of number of rounds is generally considered to be very strong immune wise.[6] Thus it has been concluded that Blowfish is the strongest and secured one.Kyung Jun Choi did a detailed study on the application of various cipher algorithms used in wireless sensor network utilizing MICA ztype motes and tiny operating system. Then with an intensive experimental anaysis he tabulated the usage of resources like space, time for computing and the power associated with each cipher methods are being characterised experimentally. In his study he concluded that the MD5 and RC4 are better than others in term of power dissipation and in the processing time aspect.[7]

4. CONCLUSION

Strengthening the immune system of a network through ciphering algorithm is the most important and only solution to protect data/ information in a network. The

strengthening of the immune system involves the features lying in the apt application and usage of the infrastructure, policies that are formulated and updated time to time by the administrator and protection of the data with the appropriate application of the ciphering algorithm by doing a comparative study of the cipher algorithm for all the particular set of systems and also based on the context.

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] D. AGRAWAL, B. ARCHAMBEAULT, J. RAO, AND P. ROHATGI.(2002) The EM sidechannel(s). *Cryptographic Hardware and Embedded Systems—CHES 2002* (LNCS 2523) [238], 29–45.

[9] R. ANDERSON. *Security Engineering, A Guide to Building Dependable Distributed Systems*. Wiley. *(* 2001)

[10] D. AUCSMITH, editor. *Information Hiding—IH '98*, volume 1525 of *Lecture Notes in Computer Science*. Second InternationalWorkshop, IH'98, Portland, Oregon, April 1998, Springer-Verlag.1998

[11] E. BACH AND J. SHALLIT. *Algorithmic Number Theory, Volume I: Efficient Algorithms*. MIT Press, (1996)

