International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 7(July 2013), PP.01-07
www.irjes.com

Protecting Computer Network with Encryption Technique: A Study

[1]Pavan Kunchur, [2]Veeranna Kotagi, [3]Prasad Kulkarni
[1]MTech(DCN),Bagalkot,Karnataka,
[2]Asst.Prof,LNBCIET,Raigoan,Satara,Maharashtra,
[3]Lecturer,Margadarshan,BCA college,Bagalkot,Karnataka,

ABSTRACT:- *In today's world the networking plays a very important role in our life. Most of the activities occur through the Internet. For the safe and secured exchange of information, we need to have security. The encryption has very wide applications for securing data. Latest authentication deals with biometric application such as fingerprint and retina scan. The different types of encryptions and their strength and standards are discussed.*

Keywords:- *Encryption, Network Security, Authentication, Biometric.*

I. INTRODUCTION

Today‟s global village concept has brought the many unknown people together via electronic media and information technology. Most of the people in today‟s world are familiar with Internet, World Wide Web applications, out of these people 40% [1] of them are still uses the unsafe browsing facility. As we talk about global village, there are many transactions happening each and every second of time, between people. To make sure that they do safe transactions every time, there must be some technology, which assures and safeties of usage. This is known to be Encryption. The concepts of Encryption is very old, as Greek General use to send his message from one place to other place through his messengers using scytale, a thin cylinder made out of wood [2], message will written on the parchment, if someone tries to read the message will appear nonsense. But if the other General receives the parchment he has to wrap it on the similar scytale to read the message. As the day passed the techniques were changed. Now to decode the Encrypted message will take millions of years.

Why we really worry about our transactions? Do we do it in secure way all the time? Because the internet has so many vast connections, as we do not have control over the activities such as hacking, sniffing, breach of conduct, etc. So what is our solution to this problem? For this, we really need to come up with robust system, the system that is difficult to break! The birth of Modern Cryptography has taken place in 1970‟s. "Cryptographic systems are characterized along three independent dimensions, the type of operations used transforming plaintext to cipher-text, the number of keys used and the way in which the plaintext is processed" [3].On the other hand we have two methods to analyze the cryptography, one is Cryptanalysis and second one is Brute-force attack. These are the independent technique to know which cryptography method is adopted.

II. WHAT IS ENCRYPTION?

Encryption refers to set of algorithms, which are used to convert the plain text to code or the unreadable form of text, and provides privacy. To decrypt the text the receiver uses the "key" for the encrypted text. It has been the old method of securing the data, which is very important for the military and the government operations. Now it has stepped into the civilian‟s day-to-day life too. The online transactions of banks, the data transfer via networks, exchange of vital personal information etc. that requires the application of encryption for security reasons.

Whether we really understand what the encryption does in our day-to-day life, but we uses often. As now most of the business completely depended upon the internet for to buy, sell, and transfer money over e-banking system, organize, teleconference, provide various services all need the encryption for safe connection and privacy. Earlier computers didn‟t have the networking facility. As the growth of networking industry the software‟s more readily available for the individuals. The advantage of the business over the internet is realized and to keep the unauthorized people away from the network the encryption is started taking its own importance.

III. BASIC MODEL OF NETWORK SECURITY

It requires the some basic structure like,

a) An algorithm, which transforms the important security, related activity
b) A secret data that is used in the algorithm
c) Building of methods for sharing and distribution of secret data and
d) Define the protocol, which makes use of both algorithm and secret data to have security service.

As we can see in the below model, the network model has basic structure. Opponents will try to surpass the safety barrier to get the required information. The message that is travelling through the information channel is not in the simple format. It got blended with the secret message, which contains the cipher text and keys provided by the trusted 3rd party for encryption. Unless one knows the key to decrypt, they cannot get the message properly. Encryption keeps the message safe and secure, till it reaches the desired recipient. [4]

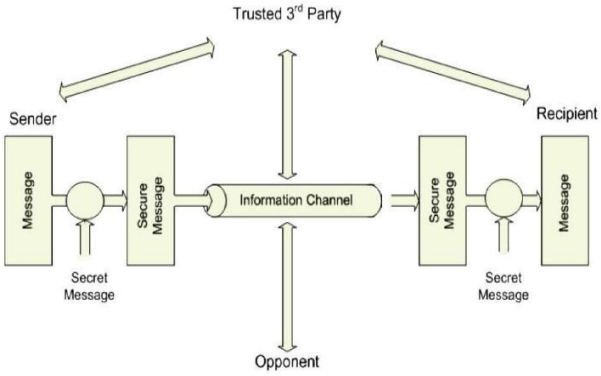

Fig. 1 Block Diagram for Network Security

IV. CLASSIFICATION OF ENCRYPTION

4.1 Symmetric Key

It is also known as single key encryption. It uses the same key for both the encryption and decryption of text. Types of algorithms for Symmetric Key:

Stream Cipher: Here the plain text are encrypted one at a time, each bits of plain text are converted into successive varying digits. Ex. RC4, SEAL
Sample Example:

"We are spartans" is written as "ZH DUE VSDUWDQV"

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fig.2. Caser Cipher

Block Cipher: Here block of plain texts are encrypted, each block has fixed length and unvarying digits.
Ex. Rijndael, IDEA (International Data EncryptionAlgorithm) Sample Example:
"We are spartans" is written as " 25 51 11 24 51 34 53 11 24 44 11 33 34 "

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig.3 Block Cipher

4.2 Asymmetric Key

It uses the two different keys for encryption and decryption, public key is used for the encryption and private key is used for decryption. As the symmetric key encryption does not provide much of the security, the importance of the Asymmetric key is more. It is also known as Public key encryption. It has the combination

of public key and private key, private key is only known by your computer while the public key is given to other computers with which it wants to communicate securely.

As everyone has the public key, but to decode the message one has to use the private key. The combination key is based on the prime numbers, thus it makes highly secure. As many as prime numbers are there, that many keys are available. Pretty Good Privacy (PGP) is one of most public key encryption program.[5]

Public key encryption can be adopted in large scale, such as for web server and the application to be secure. The Digital Certificate or digital signature gives the authentication between the users. These certificates can be obtained by the Certificate Authority, which plays the role as a middleman for both the users.

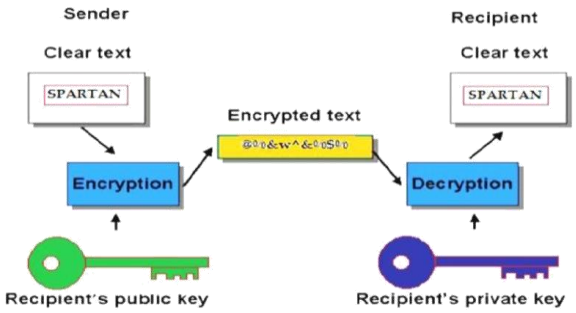

Fig.4 Public Key Encryption Model

4.2.1 Public Key Infrastructure (PKI)

To make most out of the encryption, the public keys must be built to create, maintain, use and distribute, we need the organization known as Public Key Infrastructure.

4.2.2 Certificate Authority (CA)

Without the CA one cannot issue the Digital Certificate, which contains both the public and private key for encrypt and decrypt the data. Depending upon the volume of the identity verification, Certificate Authority can issue Digital Certificate for different level of trust.

CA adopts identifying individual rather going by company. To verify individual CA can ask for Driver License as proof of identity or Notarized letter. This is only applicable for initial level of trust. For high level trust it can go for biometric information like fingerprint, iris scan etc .[6]

4.2.3 Registration Authorities (RAs)

These have similar functionality as the CA has, but RAs are one down to the level of hierarchy. This will work under the CA, mainly to reduce the workload of Certificate Authority. The RA can issue the temporary digital certificates. The temporary digital certificates have limited validity, and not fully trusted, unless CA verifies them completely.[6]

4.2.4 Digital Certificates

These certificates are used to verify the identity of a person or a company through CA. It can also be used to retrieve rights and authority. Some of them have limited access such as encrypt and decrypt. These Digital Certificates can be issued for particular laptops, computers, routers etc. Computers and web browsers have the facility to store these certificates in particular memory. [6]

4.2.5 RSA

It most recognized asymmetric algorithm, the RSA stands for the last names of the inventors Ron Rivest, Adi **S**hamir, and Leonard **A**dleman. They developed this algorithm in 1978, since then it is widely used. There are other algorithms used to generate the asymmetric keys, such as ElGamel and Rabin, but not popular as RSA, because a large corporation RSA Data Security stands behinds it.

V. SECURE SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TSL)[7]

The encryption is properly adopted for Secure Sockets Layer, Netscape has first developed it, SSL is basically meant for Internet security protocol used by the web servers and browsers. It became the main part of security known as Transport Layer Security. SSL and TSL make use of CA (Certificate Authority), whenever browser retrieves secure web page there will an additional „s" after the „http".

The browser checks three things while sending the public key and certificate,

1. Is that the certificate is valid
2. Is that the certificate comes from trusted party
3. The certificate has the proper relation with web site, which it is coming from. While initiating a secured connection between the two computers, one will generate thesymmetric key and sends to other using public key encryption. Then the two computers can have safe communication using symmetric key encryption. Once the session is over, each will discard the symmetric key used for that particular session. For next session it requires again fresh keys, and cycle is repeated.

VI. SECURITY ATTACKS [8]

More is the benefits; it‟s more the risk always. As the more people benefits from the Internet, networking the more will be the security attacks too. The attacks may have the proper intention, such as stealing the user names, passwords, credit card details, social security numbers, personal identification numbers, or any others details which can be used and have the benefits and services.

There are mainly two types:

1. Passive attack and
2. Active attack

6.1 Passive attack

It has no harm on system resources, but it tries to learn and makes use of system information. An unauthorized party or a person gain access to the system but eventually cannot modify the content or the data. The pattern of communication is observed and makes use of this information for attack. It is also known as Traffic analysis.

6.2 Active attack

It tries to alter the system resources and also has the adverse effects on their operation. In this attack the unauthorized person successfully gets into the system and has the ability to modify the message, data stream or a file. The attacks may of any kind, replay, masquerading, message modification and denial of service (DoS).

VII. ENCRYPTION STANDARDS [9]

7.1 Data Encryption Standards (DES)

The most commonly used encryption programs are based on the Data Encryption Standard, which is implemented in 1977 by National Bureau of Standards (NBS), now it is known as Institute of Standards and Technology (NIST). The algorithm that is used for the data is known as Data Encryption Algorithm. It has the key length of 56 bit. It takes the 64bit block data and encrypts using the 56bit key. The possible combination for the 2^{56} is over 72,000,000,000,000,000 keys. It is considered as secured, but as the time passed the speed of the computers increased tremendously. To break this key today‟s computer can take very short time. (See Table 1)

Different versions of DES are Federal Information Processing Standard (FIPS PUB 46), FIPS PUB 46-2, and 3. FIPS PUB 46-3 is revised version and introduced in 1997. The strength of DES depends upon the two things, one is the Key Length and second thing is depended on the nature of the algorithm used.

7.2 Advanced Encryption Standards (AES)

Because of the small key length the DES is no longer considered as safe for today‟s applications. AES come up with key length 128bit using the symmetric block cipher. It has also different key size as 192bits and 256bits. Rijndael is the algorithm that is adopted in AES. Vincent Rijmen and Joan Daeman develop this AES algorithm. This is chosen over 15 contestants, the contest is organized by NIST (National Institute of Standards and Technology) in 1997, and it took three years to come-up with final winner, which survived all the tests. The possible key combination for this algorithm will be 2^{128} is over $3.4x10^{38}$ keys, which is much stronger as compared to DES. To crack the code time taken by the computer will be in years.

Table1. Average Time Required for Exhaustive Key Search.

Key Size (Bits)	Number of Alternative Keys	Time Required at 1 Encryption / µs	Time required at 106 Encryptions / µs
56 (DES)	256 =7.2X 1016	255µs = 1141 years	10.01 hours
128(AES)	2128=3.4X	2127µs = 5.4 X	X 1018 years

	1038	1024 years	

VIII. HOW THE ENCRYPTED TEXT LOOK LIKE?

Below is the sample of encrypted text:

OT8Hj8uA7inuG2tq5YjID5mESlm2F7exsc0X3fnZRFZhk8YCEpbnDLtOfSAGdK9+cO7/D
b3MFlPJwCcAzlCJMElczhvsf2qVAcTDmsMEt3TVQFqolayND7cj4ldksCL3JDu83wup6wu
YZnw05QekQ3MGd3heMpqk4Yx3211yfV7SEQQoUAlz3Y6TwyzC5UWehb0a2dIWils1v6
ZGZ1aVzih3AmrK53+JVQ0pBMj6wbRq/LRtZvoPNA2qLUZE4o4UTKH5G9ElnqrnxBvt3
WukDcm1BxdwEtTCY9K/7Qq6X8=

Actual Plain Text:

"Encryption refers to set of algorithms which are used to convert the plain text to code or the unreadable form of text and provides privacy. To decrypt the text the receiver uses the "key" for the encrypted text". [10]

IX. APPLICATIONS OF ENCRYPTION

9.1 Data Protection

The wide application of encryption is in the field of data protection. The data that is there in the computers is invaluable for the person or the company that owns it. Encryption is necessary for safeguarding the data or the information. The common application of encryption is such as files and email encryption. Encryption protects the stored data on hard disk; the situation like theft of a computer or the attacker successfully hacks in into a system. The managing the encryption becomes more difficult as the access to the system increases. If the people working in a particular company are more the sharing of the key will be more, hence it reduces the effectiveness of encryption.

9.2 Authentication

It means the proof of identification. As the user wants to login or sign-in, to the system using the user name or ID and password, the details are sent over network using the encryption. This can be verified as soon as the login page appears on the browser; an additional „**s**" will appear next the http. It means it"s secured. Whenever we use the online banking for transactions we need to confirm, whether we secured or not by looking into the address bar and a padlock sign at the bottom or in the same address bar of the browser. (See fig. 5)

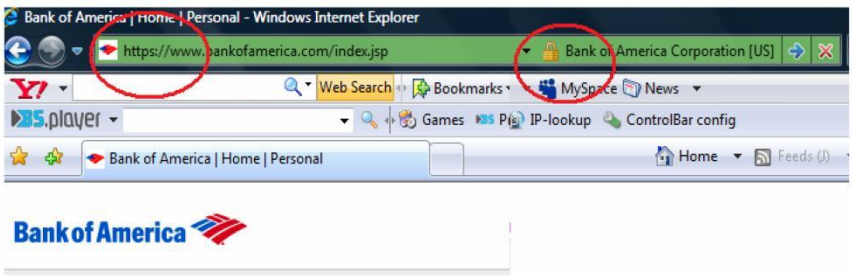

Fig. 5 HTTPS and PAD LOCK in Address Bar

X. BIOMETRIC AUTHENTICATION [11]

Some of the advanced systems require the biometric authentication. For log in into the very sophisticated laptops it may have face recognition system or the fingerprint scanning. Some of the biometric authentications include,

1. Iris scan (Retina scan)
2. Face recognition
3. Voice recognition
4. Finger print

10.1 Biometric Encryption (BE)

Biometric encryption is the process that binds the PIN or key to biometric. It is not possible to get key or biometric from the stored master file / template. The key can be re-recreated only by producing the live biometric sample on the verification.

The digital key is randomly generated up on sign up; the user will not have the clue about it. The key is completely independent of the biometrics. Once the biometric is obtained the biometric algorithm will attach the key to the biometric securely, and stores as the private template. Once the registration is over both key and

biometrics are discarded. On verification applicant will provide a fresh biometric to retrieve the PIN when it is applied over a legitimate BE template. If the biometric is not correct, then they will not get the PIN for the further application or use. The BE algorithm itself provides the decryption key. Advantages of Biometric Encryption:

1. No storage of personal data required. No retention of biometric information or the template.
2. Multiple/ cancelable / revocable Identifier
3. No tempering
4. No substitution attacks
5. Improved authentication security

XI. FUTURE SCOPE OF ENCRYPTION

In today‟s world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information. As a result cryptography is emerging as the foundation for enterprise data security and compliance, and quickly becoming the foundation of security best practice. Cryptography, once seen as a specialized, esoteric discipline of information security ,is finally coming of age.

No one would argue that cryptography and encryption are new technologies. It was true decades ago and it is still true today – encryption is the most reliable way to secure data. National security agencies and major financial institutions have long protected their sensitive data using cryptography and encryption. Today the use of encryption is growing rapidly, being deployed in a much wider set of industry sectors and across an increasing range of applications and platforms. Put simply, cryptography and encryption have become one of the hottest technologies in the IT security industry – the challenge now is to ensure that IT organizations are equipped to handle this shift and are laying the groundwork today to satisfy their future needs [12].

XII. CONCLUSION

The advantages of the networking is tremendous, the applications are vast. It saves the lot of time and energy. It has touched almost all fields, where you cannot say we don‟t need network anymore. Education, commercial to life saving telemedicine application everything is dependent on networking. To make it happen the services should be reliable and secured. The Encryption serves the purpose all time and every time.

XIII. GLOSSARY

Authentication A process used to verify the integrity of transmitted data, mainly messages

Block Cipher It is a type of symmetric encryption algorithm, which takes a large block of plain text bits and converts into a whole cipher text block of the same equal length. The size of the block is 64 bit.

Cipher It is usually replace the plain text with another object mainly to cover the meaning; the replacement is controlled by key.

Cipher text The form of encrypted text; an output from the encryption algorithm.

Code The replacement of original data to some other data with or without fixed rules. **Cryptanalysis** A branch of cryptography deals with decode of cipher to recover the data.

Cryptography The branch of cryptology dealing with formation of algorithms for encryption and decryption, indented to secure the data or the message.

Decryption The process of transformation of encrypted text to the original readable text.
It‟s also known as deciphering.

Encryption The process of conversion of plain text into unreadable form, it‟s also known as enciphering.

Key The value by which the algorithm does its encryption or the decryption of text. **Private Key** The key which is known by the creator, and used in asymmetric encryption.

Public Key It is one of the key which is used in asymmetric encryption for securing the data.
Secret This key is same for both the user for encrypt and to decrypt the data, used in symmetric Encryption method.

REFERENCES

[1] Brian Krebs, The Washington Post,"Forty Percent of Web Users Surf with Unsafe Browsers" July 1, 2008.
[2] Jeff Tyson „How Encryption works: Introduction to How Encryption works‟
[3] William Stallings Cryptography and Network Security: Principles and Practices, 3rd ed. USA: Pearson Education, Inc and Dorling Kindersley Publishing Inc. p.45, 2006.
[4] William Stallings Cryptography and Network Security: Principles and Practices, 3rd ed. USA: Pearson Education, Inc and Dorling Kindersley Publishing Inc. p.32-33, 2006.
[5] Jon Callas, „An Introduction to Cryptography‟, Sept.2006.
[6] Chey Cobb, „ Cryptography For Dummies The PKIPrimer‟, John Wiley and Sons, 2004.
[7] Jeff Tyson, „How Encryption works: SSL and TSL‟,How stuff works website.
[8] William Stallings, „Cryptography and NetworkSecurity: Principles and Practices‟, 3rd ed. USA: Pearson Education, Inc and Dorling Kindersley Publishing Inc. p.29, 2006.
[9] William Stallings, „Cryptography and NetworkSecurity: Principles and Practices‟, 3rd ed. USA: PearsonEducation, Inc and Dorling Kindersley Publishing Inc. pp. 90,150. 2006.
[10] Online encryption software, Available HTTP: http://infoencrypt.com/
[11] Ann Cavoukian and Alex Stoianov, „Biometric Encryption: A Positive-Sum Technology that AczievesStrong Authentication, Security and Privacy‟, p.15, March2006.
[12] Richard Moulds, „The Future of Encryption‟, nCipher website ,2008