ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Approach for Secure Message Transmission through Dynamic key Cryptography with Attack Analysis

Navneet Singh Sikarwar
Computer Science & Engineering
B.S.A. College of Engineeing & Technology
Mathura, India
i_m_navneet@yahoo.co.in

Abstract: This paper introduces an approach for secure message transmission by using the concept of dynamic key cryptography with analysis against attacks. In current security models, cryptography plays a fundamental role in protecting data integrity and confidentiality in information systems. However, cryptography itself is subject to cryptanalysis attacks. To reduce the cryptanalysis attack risk, is presented and analyzed in this paper. The theory can be applied to enhance the security and performance of cryptographic systems, especially those used in wireless networks communication.

Keywords: Authentication, dynamic key cryptography, symmetric cryptography, asymmetric cryptography

I. INTRODUCTION

The widespread use of wireless and wired network services and applications, security becomes a major concern. From security aspects, data integrity and confidentiality are vital issues for information systems. Confidentiality is concerned with resources being only accessed by authorized users while integrity refers to protection against unauthorized modification. Integrity and confidentiality are often related to authentication, authorization and cryptography. In fact, authentication utilizes strong cryptographic systems in order to secure itself. Thus cryptography plays a crucial part of any security system.

There are two basic techniques in cryptography [1] [7]: symmetric and asymmetric cryptography. In symmetric cryptography, encrypted and decrypted keys are the same. In contrast, cryptography using different encrypted keys from decrypted keys is called asymmetric cryptography. Each of them has pros and cons. Because of its characteristics, asymmetric cryptography is more secure than symmetric in key distribution and exchange. However, symmetric cryptography is significantly faster than asymmetric cryptography. Furthermore, as per Blaze [2] the asymmetric cryptography key size must be ten times or more that of a symmetric cryptography key in order to have a similar level of security.

In security systems, based on their advantages, symmetric and asymmetric cryptography are often combined together to protect information systems. In TSL/SSL [3] asymmetric cryptography such as Diffie-Hellman [4], ECC [5] operates key exchange between clients and servers in order to distribute session keys. After that, session keys are used as symmetric cryptographic keys for encrypting all messages in one communication session. Each session key can be used within one session only. However, when the session time is too long, the session key becomes more vulnerable. By capturing communication messages, an adversary might be able to detect patterns in the encrypted messages to crack the ciphers. The compromise of one session key exposes all communication data in the session. Furthermore, key exchange protocols rely on permanent asymmetric keys. The more that asymmetric keys are re-used to create sessions, the more cryptographic systems become vulnerable to cryptanalysis attacks. When these keys are compromised, the whole security system becomes vulnerable to adversaries.[13]

In the past, the major solution for enhancing security and reducing the risk of such cryptanalysis attacks was to increase the key size used in the cryptographic systems. However, increasing the cryptographic key size is not always the best solution, since no matter how large the key is, its cryptography is still ultimately breakable. Every cryptographic key is only secure for a certain amount of time. In 2007, Lenstra [6] stated that the 1024 bit RSA encryption used in most banking and e-commerce systems may only be secure for a few more years. In addition, larger keys often require higher computational resources, especially in asymmetric cryptography. In practice, excessively large keys may admit denial of service possibilities whereby adversaries can cause excessive cryptographic processing. Large keys are also clearly unsuitable for mobile devices having slow processing units and/or limited battery powers.

In this paper, an approach is described for secure message transmission through dynamic key cryptography and mathematically analyzed.

The rest of the paper is structured as follows. In the following section, literature survey related proposed work. Section III explains the proposed work architecture. Section IV describes the analysis of proposed work. Section V illustrate about advantage of proposed work. Section VI gives an idea about its applications. Finally, this paper gives conclusions.

II. LITERATURE SURVAY

The digital message can be categorized into four parts: text, image, audio and video message. So that most of the attack is based on these types of messages and the natures of attack are shown in fig. 1.

There are two types of attack: Passive attack are in the nature of eavesdropping on, or monitoring of, transmissions, and Active attacks involve some modification of data stream or the creation of a false stream. Most of the attack based on these two types of attacks.[7]

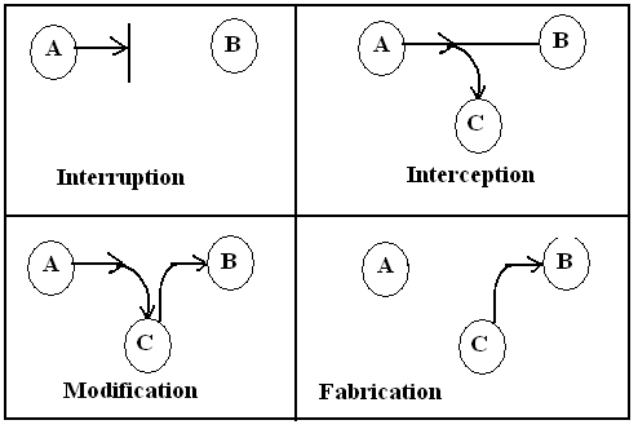


Figure 1: Nature of attacks

Cryptographic Attack Methods: There are six related cryptographic attack methods, including three plaintext based methods and three ciphertext based methods.

a. Known Plaintext: is an attack where a cryptanalyst has access to a plaintext and the corresponding ciphertext, and seeks to discover a correlation between the two.
b. Known Ciphertext: is an attack where a cryptanalyst has access to a ciphertext but does not have access to the corresponding plaintext.
c. Chosen Plaintext: is an attack where a cryptanalyst can encrypt a plaintext of his choosing and study the resulting ciphertext. This is the most common against asymmetric cryptography, where a cryptanalyst has access to a public key.
d. Chosen Ciphertext: is an attack where a cryptanalyst chooses a ciphertext and attempts to find a matching plaintext.
e. Adaptive Chosen Plaintext & Adaptive Chosen Ciphertext Attacks: In both adaptive attacks, a cryptanalyst chooses further plaintexts or ciphertexts (adapts the attack) based on prior results.[10][11]

Some other cryptographic attacks are depends upon the techniques used there are following:

a. Side Channel Attack: leverage additional information based on the physical implementation of a cryptographic algorithm, including the hardware used to encrypt or decrypt data. A side channel attack leverages additional information, such as time taken (or CPU cycles used), to perform a calculation, voltage used and so on.
b. Brute Force Attacks: A brute force attack systematically attempts every possible key.
c. Meet-in-the-Middle Attack: Meet-in-the-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. An example of a successful meet-in-the-middle attack is the attack versus Double DES.
d. Linear Cryptanalysis: Linear cryptanalysis is a known plaintext attack that requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key.
e. Differential Cryptanalysis: Differential cryptanalysis is a chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm.
f. Birthday Attack: The birthday attack is an attack that can discover collisions in hashing algorithms. The birthday attack is often used to attempt discover collisions in hash functions, such as MD5 or SHA1. [11][12]

The major solution for enhancing security and reducing the risk are struggles against all these attacks so we required more trusted solution for secure message transmission.

In Dynamic key cryptotography both party sender and receiver share very few information, basis of these shared information they generate many dynamic key at both end by using some functions. Sender and receiver use one key only for one message transmission. The Dynamic key cryptography is similar the cryptography technique but the Dynamic key cryptography use different key for different message encryption.[8] [9]

III. PROPOSED WORK

This work is based on dynamic key cryptography, the strength of any dynamic key cryptography is depends on two factor: first is secure communication channel by which initial information shared between the parties and other is strength of dynamic key generation algorithm. So the secure message transmission is possible by the combined efforts of both two algorithms.

A. Algorithm for secure communication channel:

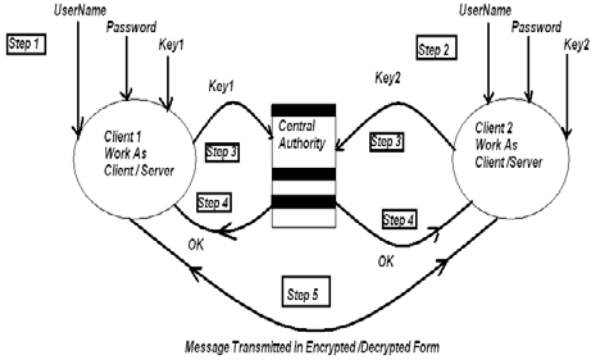


Figure 2: DFD for secure connection establishment

a. Start Central Authority Server (CAS) using username and password for Verification.
b. Now start Client1 (Alice) by using username, password for verification and his secret key authentication.
c. Central Authority check client1 (Alice) secret key, client Address as well as port Address to verify client is valid or not and send ok signal for validation.

Else

It sends No Signal for invalid client and also denies the request of client to start communication.

d. Repeat Step b and c for Client 2 (Bob).
e. If Client 1(Alice) and Client 2 (Bob) are verified by own self and their secret keys are authenticated respectively by Central Authority (i.e. both signals OK) then Communication starts between both Clients they work as Client or Server in Full Duplex mode.

Else

Connection request denied.

f. Now there is no role of Central authority and Initial message for dynamic key generation are transmitted in Encrypted form using Hash function.

B. Dynamic Key Generation Algorithms:

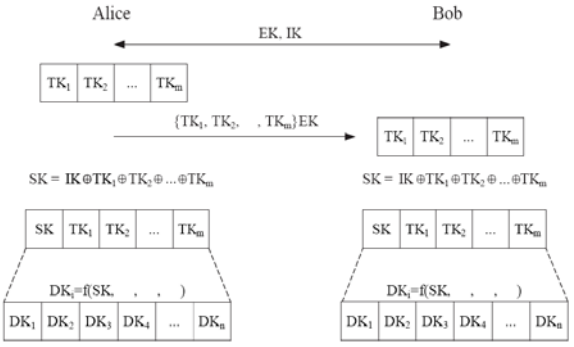
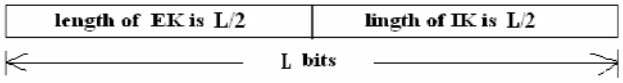


Figure 3: DFD for Dynamic key generation

a. Alice and Bob exchange two keys EK and IK via a secure channel



Here the value of L is power of 2, so that number of dynamic key we want to generate is equals to

$$N = \log2(L)$$

b. Now Alice generate m random (temporary) key in the range of 0 to pow(2,L/2) .

The temporary keys are following.

TK1, TK2, ……. TKm.

Alice encrypt these keys by using EK key and send to Bob.

EK {TK1, TK2, ……. TKm. }

Bob decrypt these keys by using EK key and get keys.

TK1, TK2, ……. TKm.

c. Now Alice and Bob both calculate seed key SK as following.

SK= IK (XOR) TK1 (XOR) TK2 (XOR)……. (XOR) TKm.

Steps for First Dynamic key

Calculate

SK (XOR) TK1 (XOR) TK2 (XOR) …. (XOR) TKm.

The result of it is string of 0 and 1, for example if result is 1010 on the basis of it. We can write an equation of X

$$X^3 + X^1$$

now put X = IK in the above equation, suppose this value is Y

then DK1 = Y mod 65536

Steps for Second Dynamic key

Calculate

SK (XOR) TK2 (XOR) … (XOR) TKm. (XOR) DK1

The result of it is string of 0 and 1, on the basis of it. We can write an equation of X, and put X = DK1 in the above equation, suppose this value is Y

then DK2 = Y mod 65536

Similarly we can write the steps for Nth Dynamic key

Steps for Nth Dynamic key

Calculate

SK (XOR) TKn-m (XOR) ……DKn-3 (XOR) DKn-2 (XOR) DKn-1

The result of it is string of 0 and 1, on the basis of it. We can write a equation of X, and put X = DKn-1 in the above equation, suppose this value is Y

then DKn = Y mod 65536

Both Alice and Bob store all the Dynamic keys in an array DK of N Size. This array is used in for encrypting and decrypting secret message.

IV. ANALYSIS OF PROPOSED WORK

The analysis of this work also depends on the strength of secure channel establishment and dynamic key generation algorithms.

A. Analysis of secure channel:

Let Alice and Bob are authorized user want to communicate over this framework. They want to prevent Oscar (the bad guy or unauthorized user) from listening. There are many ways for Oscar to enter in secure channel and listen to the secret message. All these ways are mentioned in following cases.

a. Oscar tries to find out user name and password of Alice or Bob:

In this case, Oscar tries to find out user name and password of Alice or Bob to run the application because without knowing the user name and password no unauthorized user can run the application software that Alice and Bob used.

But this attack is very weak because it is based on personal analysis of Alice and Bob's life. Today's login system provide limited chance (eg. 3 chance to login) to login so that this attack fails to know user name and password of Alice and Bob. This works provides provision if any user does not enter correct user name and password in

three time's then central authority denied his request for login.

b. Oscar tries to find out secret key of Alice or Bob:

In this work, secret key of Alice or Bob is used for authentication. The central authority checks machine address, port number and secret key, if all the values are correct then only the central authority allows for connection establishment otherwise it will denied the request.

Alice and Bob will try to choose such a secret key which will be more secure from the security point of view. In a survey it is found that if the key length is more then 256 characters, it will be more secure against brute force attack.

In this work, Alice and Bob use key of length 256 and this work uses Unicode value. In Unicode system, each character is represented by 65536 combinations. So if Alice and Bob use the key of 256 lengths, Oscar will try to break it. If Oscar applies brute force attack, it requires

65536 x 65536…….256 times = 6.844E+1237 steps to break this key for 256 length. So this step will not easily broken by Oscar.

Table I. Estimated brute force resistance of symmetric algorithms

Key length	Security estimation
56-64 bits	short term (a few hours or days)
112-128 bits	Long term (several decades in the absence of quantum computers)
256 bits	Long term (several decades, even with quantum computers (QC) which run the currently known brute force QC algorithms)

c. Oscar tries to access port number of Alice or Bob:

In this work, central authority checks machine address, port number and secret key of Alice and Bob. The aim of Oscar is to listen to the secret message that Alice and Bob is communicating.

In a machine total number of ports is 65536, in which 1024 are reserved ports and remaining is free ports. In this framework Alice, Bob and central authority run on fixed port therefore if Alice and Bob communicating each other then it is not possible (or impossible) for Oscar run his application on same port. The central authority does not allow Oscar for communication until he does not run his application on right machine, right port and with right key.

d. Oscar tries to find out encryption decryption algorithm between Alice/Bob & central authority and between Alice & Bob

This work uses two different encryption decryption algorithms. First use when Alice/ Bob send his key to central authority and second use when Alice and Bob communicate each other. Both algorithm use linear mathematical equation for encryption and decryption.

So that it is not easy for Oscar to break these algorithms, because one client uses different linear mathematical equation for different client.

B. Dynamic key generation complexity:

The complexity of dynamic key generation are depends on the no. of operation required to execution, as well as it also indicate the randomness of dynamic key.

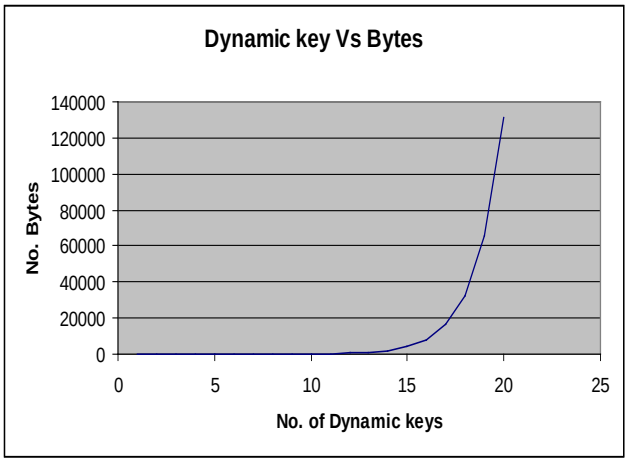


Figure 4: Dynamic key Vs No. Bytes required to shared

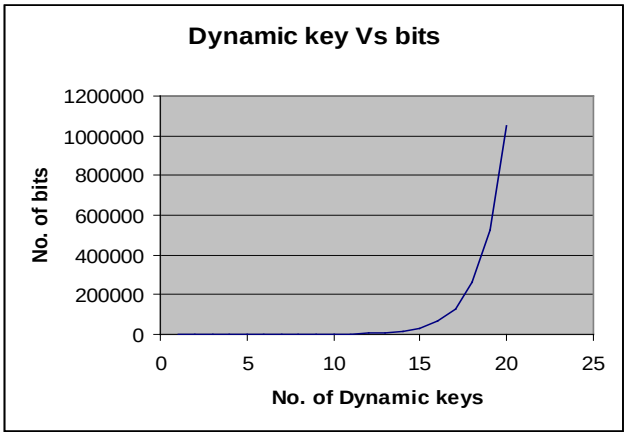


Figure 5: Dynamic key Vs No. bit required to shared

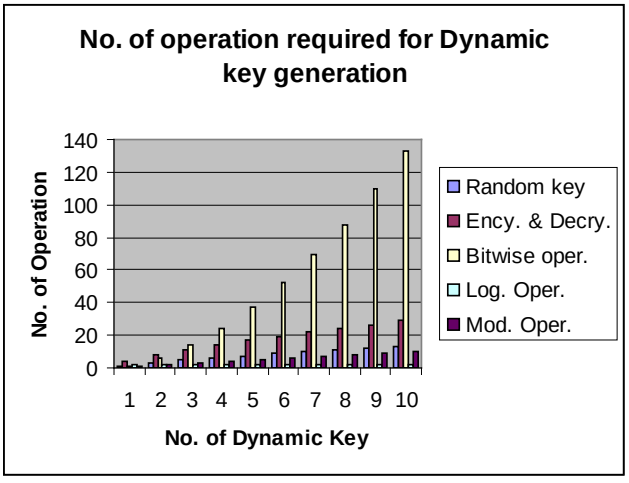


Figure 6: No. of Dynamic key Vs No. of Operation

Table II. Operation required generating dynamic key

No. of Dynamic key	Random Temporary key	No. of Encryption & Decryption	No. of Bitwise operation	No. of Modules operation	No. of logarithm operation
1	1	4	1	1	2
2	3	8	6	2	2
3	5	11	14	3	2
4	6	14	24	4	2
5	7	17	37	5	2
6	9	19	52	6	2
7	10	22	69	7	2
8	11	24	88	8	2
9	12	26	110	9	2
10	13	29	133	10	2

V. ADVANTAGE OF PROPOSED WORK

This proposed work has many advantages over the symmetric key cryptography and asymmetric key cryptography and this work has more strength over all the attack those are based on symmetric and asymmetric key cryptography, apart form it has more strength compare to session key cryptography. The comparisons are listed in table 3.

Table III. Comparison between session key and dynamic key

Issues	Dynamic key	Session Key
Key Exchange	Once	Every Session
Life time	Within a message	Within a session
Key Reusable	No	Yes
Vulnerable under man in middle Attack	No	Yes
From a compromised cryptographic key, adversary can	Decrypt a message	Decrypt all messages in the session
From a compromised pair of public and private keys of the key exchange protocol	Cryptographic system is still safe	Cryptographic system and session are vulnerable

VI. CONCLUSION

This paper gives an idea about how we will get secure message transmission with help of dynamic key cryptography. In dynamic key cryptography can become secure until we don't have a secure communication channel for initial information sharing, this paper also included the secure communication channel. This paper also includes the analysis of this approach against attacks, strengths of the work as well as advantage of it.

VII. ACKNOWLEDGMENTS

The author is grateful to the anonymous reviewers for valuable comments

VIII. REFERENCE

[1]. B. Schneier, Applied Cryptography, John Wiley & Sons, 1996.

[2]. M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T.Shimomura, E. Thompson, and M. Wiener, Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, Report of Ad Hoc Panel of Cryptographers and Computer Scientists, Jan. 1996. (http://www.crypto.com/papers/)

[3]. J. C. Mitchell, V. Shmatikov, and U. Stern, "Finite state analysis of SSL 3.0," Proceeding of the 7th Conference on USENIX Security Symposium, pp. 201- 206, San Antonio, Texas, 1998.

[4]. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

[5]. D. Hankerson, A. J. Menezes, and S Vanstone, Guide to Elliptic Curve Cryptography, Springer, Jan. 2004.

[6]. J. Kirk, \Researcher: RSA 1024-bit encryption not enough", PC World, IDG News Service, 2007. (http://www.pcworld.com/article/132184/researcherrsa1024bit encryption not enough.html)

[7]. D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.

[8]. R. Divya & T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks", International Journal of Scientific & Engineering Research Volume 2, Issue 5, May- 2011,ISSN 2229-5518

[9]. Xukai Zou, Yogesh Karandikar and Elisa Bertino, "A Dynamic key management solution to access hierarchy", International Journal of Network Management 2007; 17: 437- 450

[10]. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3rd ed.,Prentice-Hall, 2003.

[11]. W. Stallings, Cryptography and Network Security, 4th ed., Prentice-Hall, 2005.

[12]. B. A. Forouzan, Data Communications and Networking, 4th ed., McGraw-Hill, 2007.

[13]. G. Blelloch, Introduction to Cryptography, online: http://www.2.cs.cmu.edu/afs/cs/project/pscicoguyb/realworld/crypto.ps, 2000

Short Bio Data for the Author

Navneet Singh Sikarwar is Asst. Prof. & HOD, Department of Computer Science & Engineering at B.S.A. College of Engineering & Technology, Mathura. He did B.E. in Computer Science & Engineering from M.P.C.T., Gwalior (M.P.). He obtained M.Tech. in Computer Science & Engineering from T.I.T., Bhopal (M.P.).He is pursuing PhD. in Computer Science & Engineering from Bhagwant University, Ajmer (Raj.). He published 15 research papers in International, National journals and conferences. He has eight years of teaching experience. His area of specialization includes network security, data base management system, artificial intelligence and data structure. He is member of Computer Society of India, The Institution of Electronic and Telecommunication Engineers and International Association of Engineers. He is also reviewer of IJCNS, IJCIIS, IJNS and IJCA.