© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Enchancement of security of firewall based cloud server using customized DES

[1]Poonam Verma, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor , Department of CSA, CDLU Sirsa

ABSTRACT: In this dissertation a PicPass algorithm is proposed for the solution of Key Exchange problem using Symmetric and Asymmetric key cryptography. Diffie and Hellman proposed an algorithm for key exchange. But this algorithm suffers from Man-in middle attack. So to overcome this problem Seo proposed another algorithm that uses text password for the agreement between two parties. But again the password suffers from offline dictionary attack. In this, a PicPass Protocol i.e. picture is used as a password to make an agreement between two parties. The protocol contains two function i.e. picture function as well as distortion function is used to make picture in a compact size and then it is sent to receiver. Firstly the sender encrypts the Plain Text using Secret Picture and creates the Cipher Text using Symmetric key cryptography. Then the Secret Picture will be encrypted by covered picture resulting into Encrypted Picture. Now the Cipher Text and Encrypted Picture will be placed into digital envolpe and then the envelope will be send to the receiver. The receiver will receive the digital envelope, open it and then decrypt the Encrypted Picture using his Key Picture.

[1] Introduction

Basics of Cryptography

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

2 Cryptosystem

Encryption is a method of transforming original data, called **plaintext** or **cleartext**, intoa form that appears to be random and unreadable, which is called **ciphertext**. Plaintextis either in a form that can be understood by a person (a document) or by a computer(executable code). Once it is transformed into ciphertext, neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without unauthorized disclosure. When data isstored on a computer, it is usually protected by logical and physical access controls.When this same sensitive information is sent over a network, it can no longer take thesecontrols for granted, and the information is in a much more vulnerable state.

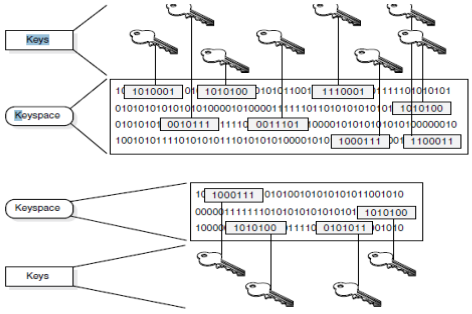

Figure 1. Use Of Key Space In Cryptosystem

[2] LITERATURE SURVEY

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

In 1976 Diffie and Helman introduces a key agreement protocol inwhich two parties can establish a secret session key over insecure channel. It makes use of the difficultyof computing discrete logarithms over a finite field. Diffie-Hellman key exchange does not au thenticate the participants. Several methods of integrating authentication into the scheme have been proposed. They need a large storage for certificates and more bandwidth for the verification of the signature as the number of user increases. Furthermore, if the authority is compromised then the total system would be in danger.The different papers that gave the reference of the above the thesis are as:-

Private Key Cryptography [34][35]the encryption and decryption are done with the help of same key.This is also known as symmetric key cryptography.In a cryptosystem that uses symmetric cryptography, both parties will be using the samekey for encryption and decryption. This provides dual functionality.As we said, symmetric keys are alsocalled secret keys because this type of encryption relies on each user to keep the key a secret and properly protected. If this key got into an intruder's hand, that intruder would have the ability to decrypt any intercepted message encrypted with this key. Each pair of users who want to exchange data using symmetric key encryption musthave their own set of keys. This means if Alice and Bob want to communicate, both need to obtain a copy of the same key.

Diffie et al[33] [34][35] introduces a key agreement protocol inwhich two parties can establish a secret session key over insecure channel. Key can be used only for key agreement ,but not for encryption & decryption of messages.Once the parties are agree on key then the key can be used for encryption as well as decryption. It makes use of the difficulty of computing discrete logarithms over a finite field. Diffie-Hellman key exchange does not authenticate the participants. But it suffers from man-in-middle attack.In practice, man-in-the-middle attacks are often dealt with by designing protocols that protectagainst a list of known attacks; such an approach, however, leaves the protocol vulnerable to newattacks as they are developed. Furthermore, many widely deployed protocols have only heuristicarguments in favor of their security. Such an approach does not engender much confidence, and,unfortunately, many of these protocols have been broken soon after their introduction.

Seo et al[30] proposed a simple authenticated key agreement protocol that Alice and Bob (two users) share a common password *P* before the protocol begins and uses the same public values of gand nas the original Diffie-Hellman. In the Diffie-Hellman key agreement protocol, the system uses public values nand gwhere nis a large prime number and gis a generator with order n-1 in GF(n) .But this protocol also suffers from man-in-middle and replay attack .

[3] Diffie-Hellman, Seo and Tseng Protocol

Devised by Whitefield Diffie and Martin Hellman in 1976.Two parties can agree on a symmetric key using this technique i.e. the same key can be used for encryption as well as decryption.Key can be used only for key agreement ,but not for encryption & decryption of messages.Once the parties are agree on key then the key can be used for encryption as well as decryption.

Cryptanalysis Of Tseng's Modified Key Agreement Protocol

From Tseng's point of view , with the modified protocol, when Tom(attacker)receives X_1(X_1 =g aQ mod n) from Alice (user), Tom must compute ($X=X_1^{Q\text{^-}1}$mod n =g^amod n)and then sends it to Alice in the verification steps of the session key. However, it is impossible to obtain g^a mod n and Q, since the problem combined with the discrete

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

logarithm and a secret password. Tom cannot therefore compute the correct X from X1. Moreover, in the modified protocol, X and Y computed in the session key establishment phase. Compared with the original protocol, the modified protocol reduces the computational time by two exponentiations. However, Ku and Wang showed that Tseng's scheme is vulnerable to two attacks, called the backward replay attack and the modification attack.

[4] Propose Work

LDH proposed a password-based key establishment protocol such that a two users can authenticate each other and generate a strong session key by their shared password within a symmetric cipher in an insecure medium. In their study, they proposed a special type of function which is a mixture of a picture function and a distortion function, is mixed to authenticate the user and protect the password from the offline dictionary attacks that are major problems for most of the weak password-based protocols.

Figure 2 Snapshot of Symmetric Cryptosystem

Above figure 2 will be the first view of the simulation. In this figure both approach are shown i.e. Symmetric key(Traditional approach) and Picture key(Proposed Protocol).

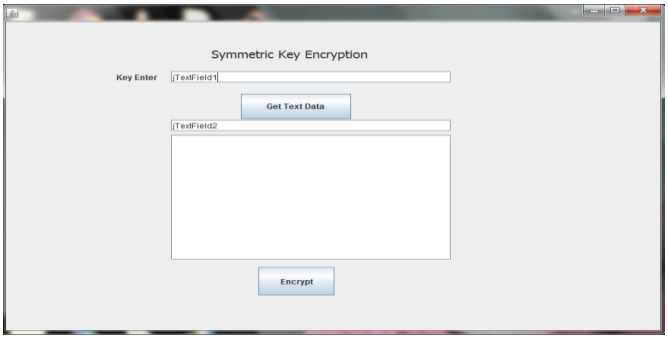

Figure 3 Snapshot of Symmetric Key Encryption

In above figure 3 we will perform symmetric key encryption i.e. traditional approach which will be performed on text message with the help of key.

Figure 4 Snapshot of Message Encrypted

In the above figure 4 we have taken a message **"hello how r u?"** as our plain text and then encrypted the message with a key **"123456"**.

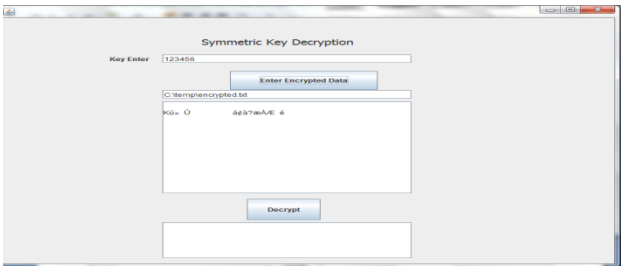

Figure 5 Snapshot of Symmetric Key Decryption

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

In the above figure 5 we are performing decryption process. For that we are taking the same key as used for encryption.Here the key exchange is a big issue more over the intruder can easily attack on the key.

[5] **Simulation, Result and Analysis**

Simulation Environment
The following environment was taken to simulate the proposed protocol.

Hardware used:

- Model : HP Pavilion dv4 Notebook PC
- Pocessor : Intel(R) Core (TM) i3 CPU M 350 @ 2.27 GHz
- Installed Memory : 2.00 GB
- System Type : 32 bit operating System

Size(bytes)	Time(ms)
33776	31
38338	31
39127	31
39552	31
42532	31
46159	31
46167	31
47023	31
48211	
	31
50593	47
52227	47
52613	47
53221	47
65964	47
74207	47
77334	78
111180	78
139864	78
151642	78
160824	93
177543	93
188972	93
199967	96
223456	96
249876	101
270567	101
280908	

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

	115
295408	140
307608	150
322567	160

Table 1 Time(ms) Taken by Text Encryption/Decryption

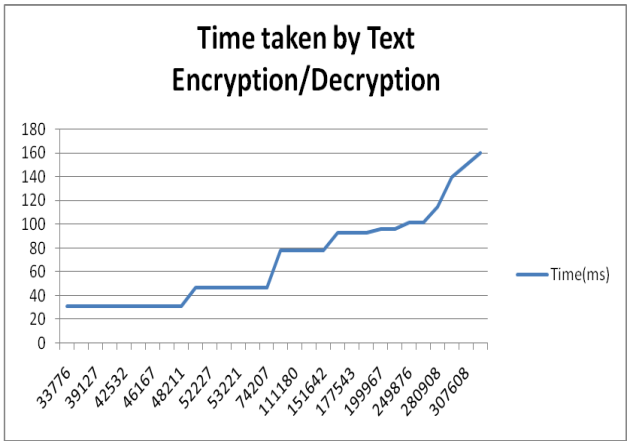

Figure 6 Analysis of Text Encryption/Decryption

Size(bytes)	**Time(ms)**
33776	110
38338	109
39127	124
39552	109
42532	110

46159	109
46167	109
47023	125
48211	110
50593	125
52227	109
52613	93
53221	109
65964	140
74207	109
77334	125
111180	94
139864	109
151642	105
160824	102
177543	99
188972	96
199967	94

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

223456	94
249876	96
270567	93
280908	95
295408	93
307608	90
322567	88

Table 2 Time (ms) Taken by Picture Encryption

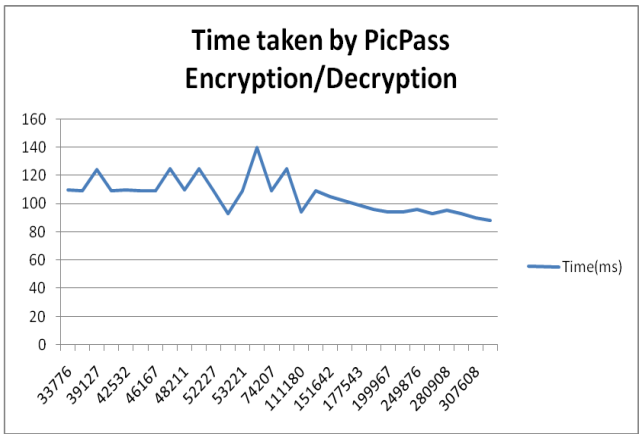

Figure 7 Analysis of PicPass Encryption/Decryption

[6] Conclusion

In this dissertation, a new picture-password based key establishment algorithm is presented that use both private and public key cryptography..The proposed protocols provide a practical solution to problem of offline dictionary attack from which Seo and Sweeny protocol suffers. By customizition of the protocol it become very convenient and practical.the analysis of time with same size of text and same size of picture.From the graph it is concluded that though the Pic-Pass protocol takes more time at the starting of the encryption but after meeting a certain point with Text encryption it takes a lesser time and text encryption takes more time with same amount of data.

References

[1]David Pointcheval, Olivier Blazy, *New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange*(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, *Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages*(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, *Password-based Authenticated Key Exchange.* (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, *Contributory Password-Authenticated Group Key Exchange with Join Capability*, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, *Strong Cryptography from Weak Secrets*, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, *Flexible Group Key Exchange with On-DemandComputation of Subgroup Keys*, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, *Distributed Public-Key Cryptography from Weak Secrets*, (18_20 march 2009, Irvine, CA, USA), S. Jarecki and G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

[8] David Pointcheval, Michel Abdalla, *Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness*, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, *Analysis and design of a secure key exchange scheme*, Information Sciences 179 (2009) , Elsevier

[10] David Pointcheval, Michel Abdalla, *Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange* , December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui and D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.

[11] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, *Provably-Secure Authenticated Group Diffie-Hellman Key Exchange*, ACM Transactions on Information and System Security, Vol. 10, No. 3. August 2007.

[12] Kumar Mangipudi, Rajendra Katti, *A Secure Identification and Key agreement protocol with user Anonymity (SIKA)*, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 420 – 425.

[13] Chin-Chen Chang, Jung-San Lee, An anonymous voting mechanism based on the key exchange protocol, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 307– 314.

[14] Tseng, Y.M., 2005, Weakness in simple authenticated key agreement scheme, *Electronics. Letters* 36 (1) pp. 48–49.

[15] *Cryptologye Print* Tang, Q., Mitchell, C., 2005, Enhanced Password-based Key Establishment Protocol, *Achive*, Report 2005/141

[16] Laih, C. S., Ding, L., Huang, Y. M., 2005, Password-only Authenticated Key Establishment Protocol without Public Key Cryptography, *Electronics Letters*, 41 (4), pp. 185-186.

[17] S.W. Lee, H.S. Kim, K.Y. Yoo, 2005, Improvement of Lee and Lee's authenticated key agreement scheme, *Applied Mathematics Computation*, 162, pp. 1049-1053.

[18] Lee, N.Y., Lee, M.F., 2004, Further improvement on the modified authenticated key agreement scheme, *Applied Mathematics Computation* 157 pp. 729–733.

[19] Moy, G., Jones, N., Harkless, C., Potter, R., 2004, Distortion estimation techniques in solvingvisual CAPTCHAs, *In Proceedings of 2004 IEEE Computer Society Conference onComputer Vision and Pattern Recognition, IEEE Computer Society*, pages 23–28.

[20] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, *New Security Results on Encrypted Key Exchange*, 7th International Workshop on Theory and Practice in Public Key Cryptography { PKC 2004 (1-4 march 2004, Singapore) F. Bao, R. Deng and J. Zhou Eds. Springer-Verlag, LNCS 2947, pages 145-158.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in