International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

An Implementation of Picpass Algorithm for the Solution of Key Exchange Problem

Er.Krishan Kumar[1], Nidhi singla[2]

[1]Assistant Professor, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India
[2]M.Tech. Scholar, Department of CSE, JCDM College of Engineering, Sirsa, Haryana, India

Article Info
Volume 7, Issue 6
Page Number: 76-79

Publication Issue :
November-December-2021

Article History
Accepted : 05 Nov 2021
Published : 20 Nov 2021

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 envelope 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. This will result the receiver to get the Secret Picture. Now the receiver will open the Cipher Text using the Secret Picture and get the Plain Text. In between if any person wants to predict the Encrypted Picture then he cannot guess as the picture will only be decrypted using the Secret Key which will be only with the receiver. So in this dissertation, a picture is used as a password to authenticate key exchange is that gives practical solution against offline dictionary attacks only by using both private and public key cryptography.

Keywords : Key Exchange, Protocol, Cryptography, Authentication, Secret Picture(Sender's Private Key), Covered Picture(Receiver's Public Key) , Key Picture(Receiver's Private Key), Plain Text

I. INTRODUCTION

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, In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

II. LITERATURE SURVEY

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.

Seo and Sweeney (Seo and Sweeny 1999) proposed a simple authenticated key agreement protocol that is based on a pre-shared password method and modifies the Diffie-Hellman scheme to provide user authentication. They claimed that established session key between two users is also verified. However, Tseng (Tseng 2005) pointed out that verification of the session key cannot be achieved in their protocol. If an opponent replies to the received message after receiving the honest user’s message, the honest user cannot determine the invalidity of the session key. That is, verification of the session key cannot be achieved in the Seo-Seweeney protocol (Seo and Sweeny 1999).

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.

Tseng [14]By using a pre-shared password technique, Seo and Sweeney (Seo and Sweeny 1999) proposed a simple key agreement protocol which was intended to act as a Diffie-Hellman scheme (Diffie and Hellman 1976) with user authentication. In the Seo-Sweeney protocol, two parties who have shared a common password can establish a session key by exchanging two messages. The authors also claimed that key validation can be achieved by exchanging two more messages. Later, Tseng (Tseng 2005) addressed a weakness in the key validation steps of the Seo-Sweeney protocol. By replying to the message sent from the honest party, the adversary can fool the honest party into believing a wrong session key. Tseng modified the key validation steps of the Seo-Sweeney protocol and claimed that key validation can be achieved in the modified protocol.

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.

3.1.1 Steps of the Algorithm

Let us assume that Alice & Bob want to agree upon a key to be used for encrypting /decrypting messages that would be exchanged between them. So the steps are as :-Firstly Alice and Bob agree on the two large prime numbers, n & g. These two numbers need not be secret. They can use some insecure channel to agree on them.

- Alice choose another large random number x, and calculate A such that
- A=g^x mod n
- Alice sends the number A to Bob.
- Bob independently choose another large random integer y and calculates B such that:

  B=g^y mod n
- Bob sends the number B to Alice.
- A now computes the secret key K1 as follows:

  KI=B^x mod n
- B now computes the secret key K2 as follows:

  K2=A^y mod n

  At last K1=K 2 (Both will agree on same key)

4. The Proposed Protocol

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. They gave the idea that proposed protocol is secure against some predefined attacks. However Tang shows that the protocol suffers from an offline dictionary attack requiring a machine based search of size 223 which takes only about 2.3 hours. So designing such type of protocol which provides the practical security solution against offline attack is still a challenge . In this study, we introduce picture password-based key establishment protocols that provide practical security solution against offline dictionary attacks by only using private key cryptography.

Passwords are the most commonly used authentication method although use of them has many well known security problems such that they can be easily guessed by automated programs running offline dictionary attacks. The scenario in which two users authenticate each other and produce a strong session key through private key cryptography from the low strength password known by the both parties is very practical and convenient way in the real world. However, designing a secure solution potocol for this problem is still an open problem due to effectiveness of offline dictionary attacks.Laih et. al. proposed a password-based authenticated key establishment protocol to resolve this problem. Actually, the major difference of the protocol from some well-known protocol is that it does not use public key cryptography to combine a large space with password space to form a large enough space to potect from the offline dictionary attack. The key idea behind this protocol is use of a special function which is consisted of a picture function and a distortion function. This function is defined as φ(r, s)=g(p(r, s)) ,where g is a distortion function, p is a picture function which takes random string of characters/digits r and a random number s as input arguments. The CAPTCHA which is used by several companies to avoid lot of free account application from machine alone is an example of this type function.

III. CONCLUSION AND FUTURE SCOPE

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.
Figure 5.17 shows 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.
After a certain calculation we can say that the PicPass algorithm is 55% better as compared to Text

encryption.Moreover the simple text encryption/decryption suffers from the problems such as confidentiality, authentication and intergrity i.e. the main attack is Man-in-Middle attack. On the another hand the protocol such as the PicPass is protected from the attacks.

IV. FUTURE SCOPE

The problem of key agreement is not fully solved. In particular, it has not yet been solved for two new users who want to communicate electronically.Some of the existing potocol solve the problem but not fully statisfactory.

V. 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.

Cite this article as :

Er. Krishan Kumar, Nidhi Singla, "An Implementation of Picpass Algorithm for the Solution of Key Exchange Problem", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 76-79, November-December 2021.
Journal URL : https://ijsrcseit.com/CSEIT217621