International Journal of Information and Computation Technology (IJICT)
ISSN 0974-2239 Volume 3, Number 10 (2013)

A Protocol on PicPass Based Key Establishment using Symmetric Key Cryptography

Kiran Kumar[1], Nagendra Nath Dube[2]

[1]CSE Deptt. Lingaya's University
Faridabad, INDIA

[2]CSE Deptt., I.E.T.
Alwar, INDIA

ABSTRACT

In this paper a PicPass algorithm is proposed for the solution of Key Exchange problem using symmetric key cryptography. In 1976, Diffie and Hellman proposed a algorithm for key exchange. But this algorithm suffers from Man-in middle attack. So to overcome this Seo and Sweeny proposed another algorithm that uses text password for the agreement between two parties. But again the password suffers from offline dictionary attack. In this thesis, a PicPass Protocol i.e. picture is used as a password to make an agreement between two parties.

In this protocol 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 picture is shared between sender and receiver. Then the data is encrypted using another shared picture. Then the cipher text is locked with the help of shared picture. When the data will reach to receiver then it will unlock the data with the help of shared picture password and then the decryption process will take place. In between if any person wants to predict the picture password then he cannot guess which part of the picture is going to be shared. So he will take a lot of time to guess this. In between our message transformation will already take place.

Introduction

1.1 Diffie-Hellman Key Exchange/Agreement

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 difficulty of computing discrete logarithms over a finite field. Diffie-Hellman key exchange does not authenticate the participants. Several methods of integrating authentication into the scheme have been proposed.One method involves incorporating certificates (e.g. digital signatures) into the key agreement protocol, thus providing authentication of the session

key. A certificate from a trusted authority is presented to the user along with the public key to certify ownership of the keys. Now an attacker cannot impersonate both Alice and Bob (the participants) and cannot substitute the original public keys with her own because they are signed. A public key system such as RSA can be used for this purpose. One example of this scheme is the authenticated Diffie-Hellman key agreement protocol, or station-to-station (STS) protocol, which was developed by Diffie.

As key exchange schemes with certificates require some trusted authority to verify the integrity of the received messages, the extension to a larger system may be difficult. 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.

1.2 Different protocols o the problem

Another method for achieving an authenticated key agreement protocol which does not require a trusted authority, involves two users (Alice and Bob) who pre-share a secret password. In encrypted key exchange (EKE) a shared password P is used as a key to encrypt a randomly generated number. This scheme defeats man-in-the-middle attacks, as attacker has no method to disguise herself as Alice and Bob without knowing the password P. But this algorithm is complicated and is also patented, obstructing wide usage. Seo and Sweeney proposed the password-based authenticated key agreement scheme, which is a slight modification of the Diffie–Hellman scheme, and based on a pre-shared password method for user authentication. After the scheme of there have been a sequence of works to improve the scheme. Tseng pointed out that Seo and Sweeney's scheme is not secure against the replay attack, in which an adversary can successfully make a honest party compute a wrong session key. Tseng also proposed an improved scheme to remedy this vulnerability. Later, Ku and Wang showed that Tseng's scheme is weak to two attacks, called the backward replay attack and the modification attack, and proposed a new enhancement to eliminate these weak points. However, Hsu et al. showed that Ku and Wang's scheme is weak to the modification attack, in which an adversary fools two communicating parties into sharing a wrong session key, and proposed an improvement to solve this weakness.

2.1 The Proposed Protocol

Laih, Ding and Huang proposed a password-based key establishment protocol such that a user and a server can authenticate each other and generate a strong session key by their shared weak password within a symmetric cipher in an insecure channel. In this protocol, a special function which is a combination of a picture function and a distortion function, is combined to authenticate the user and protect the password from the dictionary attacks that are major threats for most of the weak password-based protocols. They claim that the proposed protocol is secure against some well known attacks. However Tang and Mitchell 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 a protocol with providing practical security against offline attack is still an open problem. In this study, We introduce two password-based authenticated key establishment protocols that provide practical security against offline dictionary attacks by only using symmetric cryptography.

Passwords are the most widely used authentication method although use of them has many well known security weaknesses such that they can be easily guessed by automated programs running dictionary attacks. The scenario in which a user and a server authenticate each other and produce a strong session key through symmetric cryptography from the low entropy password known by the both parties is very practical and convenient in the real world. However, designing a secure protocol for this scenario has been an open problem due to effectiveness of offline dictionary attacks. C.S. 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 proposal is that it does not use public key cryptography to combine a space with password space to form a large enough space to resist 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 $\phi(r, s)=g(p(r, s))$,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 (Yahoo, Microsoft etc.) to avoid too many free account application from machine alone is an example of this function. A sample picture of CAPTCHA is depicted in figure 1. By means of use of such a function, distorted picture can be

easily recognized by a human, while this is a very hard problem for a machine. So according to the authors, the strength of the attacks based on only the power of machine computation can be weakened and with their proposed protocol practical security is provided.

They also analyze the security of the protocol considering the scenario if both human and machine work together to crack the system and claim that such an attack takes about 3.2-month.The basic weakness in the protocol stems from the fact that: A machine can realize the difference between a distorted image pattern and a random image pattern, so when the machine works through all possible passwords, a successful decryption means getting a non-random image pattern. As a result, for 223 password search space, by using a machine which can make one check per millisecond, one can capture the password only about 2.5 hours. In fact, for this attack strategy there is no need of human assistance.

Figure 2.1 an Example Picture of CAPTCHA

2.2 PicPass–Based Key Establishment Protocol with Symmetric Key Cryptography

- User and sever can authenticate each other and generate a strong session key by their shared password with in a symmetric cipher in an insecure channel.
- Used special function which is a combination of picture function and distortion function as password to protect the password from offline dictionary attack.
- CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart) is the example of this type function.
- It will not use the concept of prime numbers like Diffie-Hellman algorithm as the selection of appropriate prime numbers is a tedious job.
- As this protocol will use picture as a password so offline dictionary attack problem permanent vanishes.
- The whole work is done in JAVA language

2.3 Encryption will be done like this:-

The picture is divided into bytes and then for each two rightmost significant bits we will write the two bits of the message. The image will look slighter different.

- The picture will be locked by the picture which we took in first step as the password.
- When the picture will reach to receiver then first he will unlock it with the same picture that we used as a password;
- Then the decryption will occur as the vice versa of step 3.
- The receiver will get the original message.

Table 2.1. The Strength Of the Protocols Against Some Known Attacks

	Reply Attack	Modification Attack	Offline Dictionary Attack	Man-in-middle Attack
Diffie-Hellman Protocol				WEAK
Seo-Sweeney Protocol	WEAK			
Tseng's Protocol	WEAK	WEAK		

3. CONCLUSION

In this paper, a new picture-password based key establishment protocols is presented that use only symmetric cryptography. The proposed protocol provide a practical solution to problem of offline dictionary attack from which Seo and Sweeny protocol suffers. By customizing and scaling the protocol it become very convenient and practical without facing the problem of public key certificates.

4. Literature References

[1] Diffie, W., Hellman, M.E., 1976, New directions in cryptography, *IEEE Trans.*, IT-22, (6), pp.644-654

[2] Diffie, W., Oorschot, P.C.V., Wiener, M.J., 1992, Authentication and authenticated key exchanges, *Des. Codes Cryptography*, 2, pp. 107-125

[3] Bellovin, S., Merritt, M., 1992, Encrypted key exchange: password-based protocols secure against dictionary attacks, in: *IEEE Symposium on Security and Privacy*, pp. 72–84.

[4] Gong, L., Lomas, M., Needham, R., Saltzer, J., 1993, Protecting Poorly Chosen Secrets from Guessing Attacks, *IEEE J. Sel. Areas Communications*., 11, (5), pp. 648-656.

[5]Seo, D.H., Sweeney, P., 1999, Simple authenticated key agreement algorithm, *Electronics. Letters* 35 (13) pp. 1073–1074.

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

[7]William Stalling, Network security and cryptography by PHI publications.

[8] Atul Kahate, Cryptography and network security, second edition, TataMcGraw-Hill