International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015
ISSN 2091-2730

A NOVEL APPROACH TO INCREASE CONFIDENTIALITY OF DATA USING PICTURE KEY ENCRYPTION

1Ishu Saini, 2Rajiv Mishra

1M. tech. student, CBS group of institution, Jhajjar, Haryana; isstranger77@gmail.com

2A.P. in CSE deptt, CBS group of institution, Jhajjar, Haryana; mishrarajiv99@gmail.com

Abstract— Diffie and Hellman first formulated key exchange algorithm. Man in the middle attack is major weakness of this algorithm. In this paper we propose PicPass protocol, picture is used as a password to make an agreement between two parties. The PicPass protocol having 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. In this paper, a new technique is used i.e. picture is used as a password instead of text to authenticate key exchange between two parties so that they can communicate confidentially. It also gives practical solution against offline dictionary attacks by using both private and public key cryptography.

Keywords— Key Exchange, Protocol, Cryptography, Authentication, Confidential, Secret Picture , Covered Picture, Key Picture.

Introduction

Symmetric key cryptography is also called as secret key cryptography or private key cryptography.in this a single key is used for both encryption and decryption of messages between sender and receiver. It is also known as secret key as there is only single key between two of them and it must be kept secret to maintain the security of communication. Both parties must decide a single key and carry out transmission and it must not be known to others. At sender end the plain text get converted to cipher text using this key and reverse action is performed at another end. In this way original message is received by the receiver.[7]

But this algorithm suffers from a major problem of key exchange under the practical environment which is the agreement of key between the two parties? Two conventional solutions are handing over physically and over the courier. But these methods are totally irrelevant as the person could exchange message too via this and they are highly prone to attacks. A third way is to transmit the key over the same network along with acknowledgement from other side. But then, if it is intercepted by any intruder then the security breach occurs. Second problem is in case of broadcast we require a lot of key pairs and key ring gets very large. Also this problem is equally difficult as the same key is used for encryption and decryption per party.[1,4]

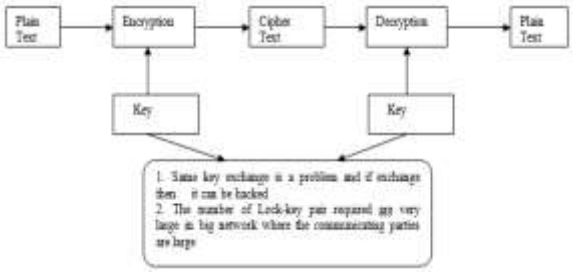

Figure 1 Key Exchange Problem [2]

Previous work: LDH proposed a key exchange protocol which is password based in which sender and receiver can authenticate one another to generate a very strong session key using a shared password over a medium which is not secure. A special function is used by having distortion and picture subroutines used as password in order to save password from offline dictionary attack. We used picture as password in place of text making it less exposed to attacks and hence more secure. Diffie and Hellman [6] first formulated

key exchange algorithm. Man in the middle attack is major weakness of this algorithm. In order to tackle this problem, another algorithm that uses text password for the agreement between two parties is proposed by Seo. [3] But again this algorithm (password) suffers another problem i.e. Offline dictionary attack. Secure protocol designing is still a major problem due to availability of offline dictionary attacks. Laih et. Al. suggested a key establishment protocol which is based on password in order to resolve the problem. The protocol is different from several others proposed protocols as it doesn't use public key and it uses special function $\varphi(r, s)=g(p(r, s))$,where g stands for distortion function, s is input argument which is random and p stands for picture function . In PicPass protocol, picture is used as a password to make an agreement between two parties. The PicPass protocol having two functions 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.

II. Pic Pass Protocol

Encryption Steps:-

- Encryption of plain text that is to be send by the sender using encryption from secret picture which is actually sender's private key and thus generating cipher text using DES.
- Further, it will carry out the process on secret picture by the use of covered picture which is receiver's public key and thus encrypting with Rivers Shamir Adleman algorithm i.e. RSA.
- A digital envelope is sent to receiver having cipher text and picture so encrypted.

Decryption Steps:-

- Digital envelope will reach receiver's side.
- Digital envelope will be opened to get encrypted picture and decrypt using its own private key with RSA algorithm and receiver get secret picture.
- IP Filter would be applied to enable only authentic system to Decrypt the cipher text

  Jave code to validate IP would be as follow:

```
int flag=0;
try
{
Enumeration e = NetworkInterface. getNetworkInterfaces();
while(e.hasMoreElements())
{
NetworkInterface n = (NetworkInterface) e.nextElement();
   Enumeration ee = n.getInetAddresses();
   while (ee.hasMoreElements())
```

```
{

InetAddress i = (InetAddress) ee. nextElement();

// System.out.println(i.getHostAddress());

if(i.getHostAddress().equals("1.0.0.1"))

flag=1;

}}}

catch(Exception e)

{}

if (flag==1)

{

//Decryption would be implemented

}

else

{

System.out.print("Invalid Ip");

}}
```

- Cipher text will be changed using plane text using secret picture applying DES.
- Thus receiver will get the plain text.

III **ASSESSMENT BENEFITS**

The proposed protocol when implemented using java language is found to be protected from the above different attacks in the manner as:-

- **Offline Dictionary attack:-**The proposed protocol is safe from offline dictionary attack as we have not used any text or number key to encrypt and lock the plain text. We are using PNG images for our algorithm to take place and predicting of plain text from picture makes the life of a hacker uneasy as compared to let approach.[5]
- **Modification Attack:-** The protocol is safe from active attack because according to algorithm we have encrypted the data using picture and picture encryption increases the confidentiality of the original message a lot. The increase in confidentiality normally reduces the chance of modification attack.
- **Man-in Middle attack: -** The above protocol is safe from the man-in-middle attack as after the encryption. While comparing our Pic-Pass algorithm with other algorithm proposed earlier against various attacks the result is as displayed in the table 1.

	Replay Attack	Modification Attack	Offline Dictionary attack	Man-in middle attack
Diffie-Hellman Protocol	No	Yes	No	Yes
Seo-Sweeney Protocol	Yes	No	Yes	No
Tseng's Protocol	Yes	Yes	No	No
PicPass Protocol	No	No	No	No

Table 1 the Strength of the Protocols Against Some Known Attacks

IV Simulation results

When simulated in java programming language the proposed methodology i.e. Pic-Pass algorithm gives the following results (text encryption results for the similar simulation environment I also shown):

Size in bytes	Time1(Text Encryption)	Time2(Picture Encryption)
33776	31	110
39127	31	124
50593	47	125
65964	47	140
77334	78	125
139864	78	109
151642	78	105
160824	93	102
177543	93	99
188972	93	96
249876	101	96
280908	115	95
295408	140	93
307608	150	90
322567	160	88

Table 2 Time (ms) Taken by Text Encryption vs PicPass Encryption

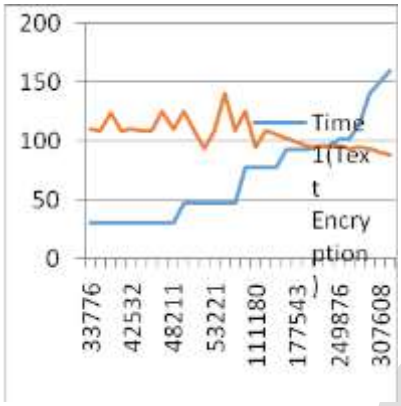

Figure 2 Analysis of Text Encryption vs PicPass Encryption

V. CONCLUSION AND FUTURE SCOPE

In this paper we proposed a new technique for authentication i.e. picture-password based key exchange algorithm instead of text password using both private and public key cryptography. This proposed protocols overcome the problem of offline dictionary attack from which Seo and Sweeny protocol suffers. After a certain calculation we can conclude 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 integrity i.e. the main attack is Man-in-Middle attack. But our proposed algorithm PicPass provides the solution of many attacks. 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 protocol solve the problem but not fully satisfactory.

REFERENCES:

1. David Pointcheval, *Password-based Authenticated Key Exchange.* (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.
2. 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.
3. Seo, D.H., Sweeney, P., 1999, Simple authenticated key agreement algorithm, *Electronics. Letters* 35 (13) pp. 1073–1074.
4. [31] Diffie, W., Oorschot, P.C.V., Wiener, M.J., 1992, Authentication and authenticated key exchanges, *Des. Codes Cryptography*, 2, pp. 107-125
5. [32] 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.
6. [33] Diffie, W., Hellman, M.E., 1976, New directions in cryptography, *IEEE Trans.*, IT-22, (6), pp.644-654.
7. Crptography concepts, URL: http://en.wikipedia.org/wiki/private key crptography