Key Exchange With Public Key Cryptography

Mrs. Jerina Begum S.
Department of Information Technology, Agni College of Technology, Chennai
jerry.esah@gmail.com

Mr. Vijay M.
Department of Information Technology, Agni College of Technology, Chennai
Vijaymuniyan95@gmail.com

Mr. Vignesh K.
Department of Information Technology, Agni College of Technology, Chennai
Vickeyk95@gmail.com

ABSTRACT: **WHEN USING, AUTHENTICATION BASED ON CRYPTOGRAPHY, AN ATTACKER LISTENING TO THE NETWORK GAIN NO INFORMATION THAT WOULD ENABLE IT TO FALSELY CLAIM ANOTHER'S IDENTITY. KERBEROS IS THE MOST COMMONLY USED EXAMPLE FOR THE TYPE OF AUTHENTICATION TECHNOLOGY. THE AUTHORS CONCENTRATE ON AUTHENTICATION FOR REAL-TIME EXISTING PROBLEMS AND THEN INTERACTS WITH THE SERVICES THAT ARE OFFERED ON COMPUTER NETWORKS. THE USE OF THE TERM REAL-TIME LOOSELY STATES THAT THE CLIENT PROCESS IS WAITING FOR A RESPONSE OR COMMAND. SO, THAT IT WILL DISPLAY THE RESULTS TO THE USER OR OTHERWISE IT WILL CONTINUE PERFORMING ITS OWN INTENDED FUNCTION. THIS TYPE OF SERVICES INCLUDES REMOTE LOGIN, FILE SYSTEM READ AND WRITE, AND INFORMATION RETRIEVAL.**

Keywords: Encryption; key-privacy; anonymity; El Gamal; Cramer-Shoup; RSA; OAEP.

I. INTRODUCTION

To secure communications between two parties, an authenticated encryption key is required to agree. So, far two models have existing for authenticatedkey exchange. One model identifies that someone have shared the information using secrete key or public key to encrypt their information. These keys are random and difficult to remember. Instead the user can maintain it by protecting a password/PIN. Another model is remembering in a human-memory.Bellovin and Merritt [4] were the first to introduce password-based authenticated key exchange (PAKE). where two parties will communicate only through their knowledge of a password. Using the established cryptographic key for exchanging messages.PAKE protocol is used to identify both on-line and off-line dictionary attacks. In off-line dictionary attack the third person tries all possible passwords in a dictionary in order to find the password of the client.In on-line dictionary attack an adversary attempts to login continuously trying each possible password. By cryptographic method. It is difficult to prevent the on-line dictionary attacks. Buton-line attacks can be stopped permanently by providing only certain limitations for login.

A. *SYSTEM ANALYSIS*

It states about the existing system, proposed system and introduction to our technological background, about the system model and the algorithms used in it.

a) Existing System

In the Existing System, all the authenticated users and their passwords are stored in a single client server. If the server is crashed due to any kind of hack or attack. All the passwords stored in that will be disclosed.

For all the time if the user login to his/her account. They will be receiving certain tokens for an authentication purpose. Protocol used in the single client server uses three types of password protection as follows: Password-only PAKE, PKI-based and PAKE ID-based PAKE.

II. DISADVANTAGE OF EXISTING SYSTEM

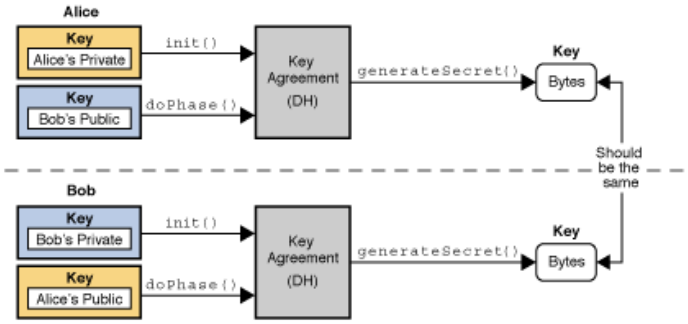
In the Existing System, both the users will share their passwords through the messages. Which is considered as one of the most drawback in it. When the client server gets crashed all the details and the passwords and their information stored in the single client servers does not disclose. This is the major drawback need to be considered.

b) Proposed System

Here, we have proposed a new compiler called ID2S PAKE protocol. Which is used to find identity-based signature scheme (IBS). The client splits the password into two shares and the server keeps one share of the password and the private key using which only the user can sign in. During sign in the server sends the public

key to the user. Using which the user can sign in and access the information contained in it. While decrypting the message the server will send the one-time password. Using which the user can decrypt the information.

c) System Architecture:



B. *LITERATURE SURVEYS* **:**

Encrypted Key exchange : password-Based Protocols Secure Against Dictionary Attacks

M. Merritt, S.M. Bellovin

Cryptographic protocol method help the users to choose their own keys. Which helps them to make their conversation encrypted and secured. During communication both the users will share the public keys to encrypt or decrypt the information shared between them. Keys which are used mainly and plays a vital role are Symmetric key (public key) and Asymmetric key (private key). If the user wants to secure or make their information secure they can encrypt the information and can share to another user along with a public key to decrypt on another side to make the conversation secured. Which also protects the password and their information.

Kerberos: An Authentication Service for Computer Networks

B.C. Neuman ,T. Ts'o

While using the authentication cryptography method. The online users or third party will look on for the information leakage. So, Kerberos is the common example for this type of authentication technology. The authors consider on authenticating the information in a real-time process using the interactive services that are available on computer networks. The term real-time loosely is used to mean that a client process is waiting for response or command. So, that it will display the results to the user or else continue to perform its own intended function. This process includes remote login, file system read and write and information retrieval.

New Direction in Cryptography

W.Diffie M. Hellman

There are two types of developments used in cryptography. Where Widening applications of teleprocessing have given high place for new types of cryptographic systems. Which is used for minimizing asper the user need for providing secured key distribution channels and to supply the information on a written signature. It helps to solve the current problems. It states that the theories of communication and computation are started to provide set of tools for solving cryptographic problems.

Server-Assisted Generation of a Strong Secret From a Password

W. Ford B.S. Kaliski

Users who are moving instantly are considered as separate group and separate passwords are provided to them to get the continuous access. The server is designed in such a way that it identifies the server attacks and other vulnerable. The protocol is used for securing and generating a strong secret key for secret (password). It helps to communicate and exchange the messages with two or more independent servers. The result can be displayed in various ways. For example: - the strong secret key can be generated to decrypt and encrypt private key or it can be used strongly on authenticating the application server. These methods help the users to safeguard their information from other users or unauthenticated users.

III. SYSTEM CONFIGURATION

1. HARADWARE CONFIGURATION

System : Pentium IV 2.4 GHz.

Hard Disk : 40 GB

Ram : 1 GB.

2. SOFTWARE CONFIGURATION

Operating system : Windows XP/7/8.

Coding Language : JAVA/J2EE

IDE : Eclipse

Database : MYSQL

IV. INPUT DESIGN AND OUTPUT DESIGN

1. INPUT DESIGN:

The input design provides the connection between the information system and the user. It develops certain specification and procedures used for data preparation. There are certain steps used to find for reading the documents and retrieving the required information from the document. It is used to control the size of input, to control the errors, avoid delaying, avoid extra steps and keeping the process simple. Input should be provided in such a way that is must offer high security. Input design contains certain functionalities as the follows:

- What kind of data should be given as input?
- How the data should be arranged?
- How to guide the operating personnel from providing input.
- Methods for providing input validations and their steps as follows:

2. *OBJECTIVS***:**

1.Input Design is used for converting a user input into a computer-based system. This design helps to avoid errors in the input data process and helps to show the correct direction for managing correct information stored in the computerized system.

2. Easy interaction is allowed. Which is used for handling large amount of data. The goal of input is to make the entrance easier and to create error free environment. It also provides record viewing facilities.

3.Once the data is entered it is verified and validated as per its information. Exact and required messages should be provided to the users. Finally, the motive of the input design is to provide the safe and secured communication.

3.*INPUT DESIGN:*

Input design helps to provide the fine quality of output. Which should satisfy the end user requirements and to present the information exactly. In all the system, the results are directly associated with the exact user. The output design helps to clear all the error and to provide correct output. Which helps the users on decision - making?

1. It must be computed in an organized manner and also it needs to provide the results correctly asper the input data.

2.Various methods should be handled for presenting information.

3.Exact documents and reports should be provided.

It can be accessed through the following things:

- Past, Present and Future activity descriptions should be provided.
- Signal important events, opportunities, problems, or warnings.
- Trigger the vulnerable actions.
- Confirm the action need to be performed.

V. FUTURE ENHANCEMENT:

Though we have used limited space in our proposed system. We will look on for extending the space compatibility in future. Also, another vulnerability in the existing system like snatching the information without the knowledge of users performing actions like shoulder surfing, man in the middle attack etc. can also be rectified through the Future Enhancement. It helps on offering high space compatibility and prevents the malicious activities.

VI. CONCLUSION:

Finally, this system deal with the two main activities called two-party PAKE protocol to an ID2S PAKE protocol. It helps to safeguard the message or information exchanged between two users. Our compilers are used to verify and validated the information about the password and the user of the password. Our future goal is to make the process much more efficient.

VII. REFERENCES

[1] Abdallah M. and D. Pointcheval. Simple password-based encrypted key exchange protocols. In Proc. CT-RSA 2005, pages 191-208, 2005.
[2] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt'00, pages 139-155, 2000.
[3] S. M. Bellovin and M. Merritt. Encrypted key exchange: Password based protocol secure against the dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.
[4] J. Bender, M. Fischlin, and D. Kugler. Security analysis of the PACE key-agreement protocol. In Proc. ISC'09, pages 33-48, 2009.
[5] J. Bender, M. Fischlin, and D. Kugler. The PACEjCA protocol for machine readable travel documents. In INTRUST'13, pages 17-35, 2013.
[6] D. Boneh and M. Franklin. Worked on Identity based encryption in theWeil pairing. In Proc., Crypto'01, pages 213-229, 2001.
[7] V. Boyko, P. Mackenzie, and S. Patel. Provably secure password authenticated key exchange using Diffie- Hellman. InProc. Eurocrypt'00, page156-171,200