JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-4, Special Issue-7, Dec 2016 ISSN: 2347-2693

Authentication Mechanism using Encrypted One time Password (EOTP)

Amarjyoti Pathak*
Department of Computer Science Engineering,
Girijananda Chowdhury Institute of Management and
Technology, Guwahati, India
Email:- amar_cse@gimt-guwahati.ac.in

Utpal Barmen
Department of Computer Science Engineering,
Girijananda Chowdhury Institute of Management and
Technology, Guwahati, India
Email:- utpalbelsor@gmail.com

Sanjay Kumar Keot
Department of Computer Science Engineering,
Girijananda Chowdhury Institute of Management and
Technology, Guwahati, India
Email:- sanjaykeot111@gmail.com

Panu Boro
Department of Computer Science Engineering,
Girijananda Chowdhury Institute of Management and
Technology, Guwahati, India.
Email:- Panu606@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—Authentication system is the mechanism of proving the access to authorize users only and to prevent the various security threats. In the various one time passwords based (OTP) systems are third party dependents such as mobile, emails etc. In this paper we will discuss about the problems associated with various authentication techniques and a proposed system which is independent of third party and highly secured.**

Keywords— Network Security, Authentication, Public key, Private key, Cryptography, Encrypted one time password(EOTP)

1. Introduction

Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures. Authentication is the assurance that the communicating entity claims to be genuine. According to Fermi Lab [1], authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network.
The four levels of authentication [2] defined by NIST as follows:
1. Little or no confidence in the asserted identity's validity. There is no need for identity proofing on this level, on this level it is sufficient with a simple password challenge response protocol.
2. Some confidence in the asserted identity's validity. “Level 2 provides single factor remote network authentication”. At this level there is a need for identity proofing and need for a secure authentication protocol to prove the identity.
3. High confidence in the asserted identity's validity. “Level 3 provides multi-factor remote network authentication”. At this level there is need for a proof of possession and a minimum of two authentication factors.
4. Very high confidence in the asserted identity's validity. “Level 4 is intended to provide the highest practical remote network authentication assurance”. At this level there is need for proof of possession through a cryptographic protocol. It is not specified which authentication level can be considered as strong but level 3 with multi-factor authentication is definitely considered as a strong authentication. It is also clear that strong authentication does not have to be multi-factor. According to strong authentication can start with two-factor authentication which combines of the following authentication options:

- Something you know, e.g. Passwords.
- Something you have**,** e.g. One-time password tokens and Digital certificates.
- Something you are, e.g**.** Biometrics.

Most of two-factor authentication solutions combine "something you know" and "something you have". They require the usage of an additional device, which demands administration from the service provider and extra care from the user. Multi-channel communication is another way to further improve the security of an authentication scheme.

2. HOW DOES AUTHENTICATION WORK

A user provides credentials such as a password, smart card, fingerprint, digital certificate which identifies that user as the person who is authorized to access the system. The basic authentication process remains same for all methods. In authentication process, a user must have a valid user account with some authority that specifies the user's rights. User credentials account such as a password, a smart card certificate or a biometric scan must be associated with this account. These credentials are entered into the database against which future data will be compared. When the user wants to log in, he/she provides the credentials or passwords and the system checks the database and compares it with the stored one. If the credentials provided by the user match those in the database, access is granted.

3. AUTHENTICATION METHODS [4]

Various methods for performing authentication are as follows:
(a) Password Authentication
(b) Public Key Cryptography
(c) Biometric Authentication
(d) Out of band

4.1 Password Authentication

The most widely used and oldest form of authentication is password. Users provide an id, a typed in word or name, along with a password. In majority of the systems the passwords are encrypted instead of storing it as a plain text. Password authentication does not require the support of hardware as authentication of this type is simple and does not require much processing power. This method has many drawbacks, some of which are:

1) Passwords are easy to guess.

2) Placing the password in a highly visible area.

3) Unsafe due to malpractice of eavesdropping.

Listening to anyone without permission can be managed by using digests. The connecting party sends a value generally client's IP address or time stamp and any other additional secret information. Because this is unique for each accessed URL, no other documents can be accessed or viewed from other IP address or computers without detection. Because of hashing the password is also not vulnerable to eavesdropping.

4.1.1 One Time Password

To overcome the drawback of password reuse, one-time passwords were developed. A one-time password (OTP) is valid for only a single transaction on a computer system or any other device such as a Smartphone. OTP's are generated using random values and hash functions. Types of one-time passwords are a challenge-response password and a password list [1]. The challenge-response password replies with a challenge value (e.g. a random number chosen by the authentication server) after getting a user identifier. The response is calculated using the response value (using a hardware) or from a table based on that particular challenge. A one-time password list makes use of previous passwords which are sequentially used by the user wanting to access a system. The values are generated such that it is very hard to predict the next value from the previously generated values. The time synchronization is also one of the approaches for generating OTP. In this approach, a security token is used. The clock in the token and authentication server is synchronized as generation of the password depends upon current time.

Working principle: User receives a password or some value through the SMS and enters that password or value to complete the process of authentication. Real life example: Use of OTP to login online shopping system.

4.2 Public Key Cryptography

Public key cryptography, which is an asymmetric cryptography, is a class of cryptographic protocols. The two keys are mathematically linked. The private key is kept as a secret and is used to decrypt and public key is used to encrypt messages between the clients. Encryption and verification of signature both is completed using public key.

Advantage of public-key cryptography is that the public key is easily available to the public. They are often published on the Internet so that they can be easily retrieved.

It is used to transfer a symmetrical encryption key by which the message is encrypted because of the computational complexity. It is based on simple algorithms and is much faster. A private key is kept by the user, while the corresponding public key is made available in a certificate digitally signed by a respective certification authority. This certificate is made available to users.

Real life example: Updating data of registered voters with the Registration and Electoral Office.

4.3 Biometric Authentication

Biometric is a common approach for the authentication. Many industries are using biometric as authentication mechanisms for accessing bank machines, door access control and general desktop computer access as well as attendance recording systems in various organizations. These systems recognize individuals based on their physical attributes (fingerprint, face, iris, voice) or behavioral attributes such as signature. Because such characteristics are physically associated with a particular user, biometric recognition is a natural and more efficient mechanism for ensuring that only authorized users can access a system.

4.4 Out of Band

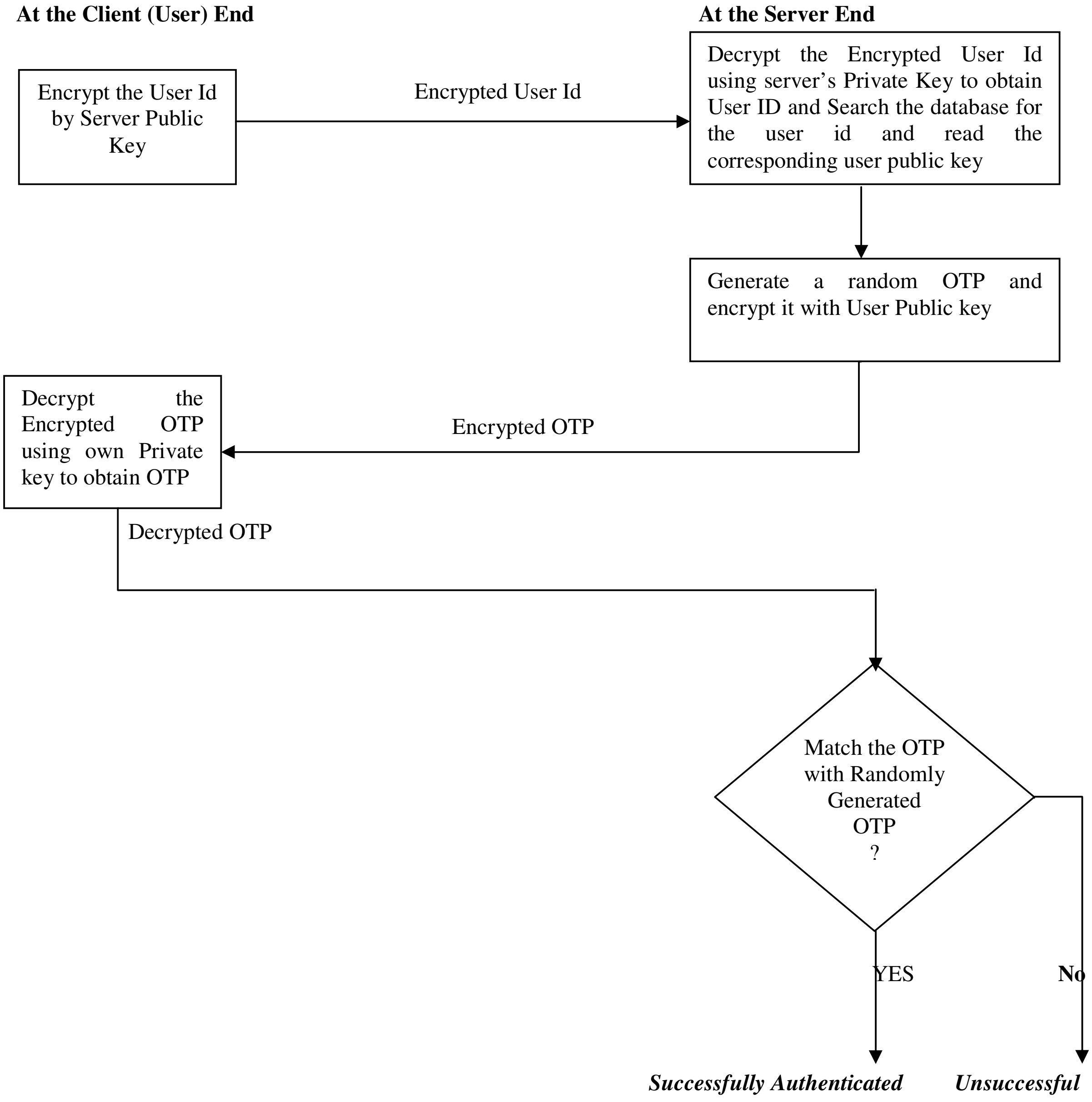
Using an Out-of-band verification for authentication involves the bank organization calling a phone number that has been registered with it before and requesting that user to enter their password over the phone before allowing the user to login [3]. Similar to e-mail or SMS OTPs, this requirement is time consuming and requires that the user must be at the location specified by the registered phone number.

5. PROPOSED SYSTEM

In the proposed system we use public key cryptography. In the proposed system the user will generate a public and private key pair using any asymmetric key cryptography algorithm such as RSA or Elliptic curve cryptography algorithms. During the registration process the user will provide the system public key which will stored in the database along with User Id.

And after the registration the user will also get the public key of server. And when the user need to login he will asked to enter the his user id and encrypt it by public key of server send it to server now the server will decrypt the Encrypted User Id using servers Private key to obtain User ID and search the database if the user id exists then he will generate a random password and encrypt it with the public key of user (stored in database) and send the encrypted one time password (EOTP) to sender and the Sender will decrypt it with his private key. Now the user will send the decrypted OTP to the server. The server will match it with the random generated OTP. If it matches the user will be authenticated.

A diagrammatic representation of proposed system:-


At the Client (User) End
At the Server End
Encrypt the User Id by Server Public Key
Encrypted User Id
Decrypt the Encrypted User Id using server's Private Key to obtain User ID and Search the database for the user id and read the corresponding user public key
Generate a random OTP and encrypt it with User Public key
Encrypted OTP
Decrypt the Encrypted OTP using own Private key to obtain OTP
Decrypted OTP
Match the OTP with Randomly Generated OTP ?
YES
No
Successfully Authenticated
Unsuccessful

6. ADVANTAGE OF PROPOSED SYSTEM OVER EXISTING SYSTEMS

Following are the advantages of proposed system are:-

1. The proposed system is independent of third party such as email of mobile phone.
2. In the proposed system user doesn't require any token or smartcard.
3. The proposed system is highly secure.
4. The proposed system verifies both client and server.

7. CONCLUSION

This paper has suggested a way to employ the public key cryptography to design a secure authentication system. The above proposed system is one time password based. Public key cryptography is highly secure cryptography. The above proposed system secure authenticate the user and it is independent of any third party and so it also less time consuming one.

REFERENCES

[1]. R . L. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public Key Cryptosystems", Technical Memo 82, Laboratory for Computer Science, Massachusetts Institute of Technology, April 1970.

[2]. National Institute of Standards and Technology (NIST) U.S.Department of Commerce: Electronic Authentication Guideline-Information Security, Special Publication 800-63-1, December 8,

[3]. W. E. Burr, D. F. Dodson, W. T. Polk. ElectronicAuthentication Guideline. Technical Report 800-63, National Institute of Standards andTechnology,2008.<http://csrc.nist.gov/publications/nistpubs/800SP800-63V1_0_2.pdf>.

[4]. CA.Managing strong Authentication: A Guide to Creating an Effective Management System, 2007. Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar,Tanvi Madhekar nad B.S. Thakare, "An Overview of Various Authentication Methods and Protocols" in International Journal of Computer Applications (0975 – 8887) Volume 131 – No.9, December2015.

[5]. Geetanjali Choudhury and Jainul Abudin, "Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password" International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4077-4080.

[6]. Jainul Abudin, Sanjay Kumar Keot, Geetanjali Malakar, Nita Moni Borah and Mustafizur Rahman, "Modified RSA Public Key Cryptosystem Using Two Key Pairs" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3548-3550.

Author Profile

Amarjyoti Pathak is currently working as Asst.Professor at Department of Computer Science Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, India. He is author of various journel papers in national and international journels. His research interests include cryptography and network security,Computer Network,etc .

Utpal Barmen is currently working as Asst.Professor at Department of Computer Science Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, India. He is author of various journel papers in national and international journels. His research interests include computer networks, image processing etc.

Sanjay Kumar Keot is currently pursuing M.tech(CSE) at Department of Computer Science Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, India. He is author of one research paper "Modified RSA Public Key Cryptosystem Using Two Key Pairs"in (IJCSIT) International Journal of Computer Science and Information Technologies. His research interests include cryptography and network security,Computer Network,etc .

Panu Boro is currently pursuing M.tech(CSE) at Department of Computer Science Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati.