ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Efficient Two Server Authentication and Verification Using ECC

Seema P. Nakhate[1], Prof. R. M. Goudar [2]

Department of Computer Engineering, MIT Academy of Engineering, Alandi (D), Pune, India[1]

Department of Computer Engineering, MIT Academy of Engineering, Alandi (D), Pune, India[2]

ABSTRACT: A Password Authenticated Key Exchange(PAKE) protocol is a cryptographic protocol that allows two parties client and server, who share knowledge of a password to mutually authenticate each other and establish a cryptographic keys by exchanging messages and without explicitly revealing the password. Generally storage of allpasswords necessary for authentication of clients is present in single server. But when such a server is compromised, a large number of client's passwords are exposed at once. In such schemes, the capability of verifying a password is split among two or more servers. If any server is compromised, the attacker still cannot pretend to be the client and he/she cannot access the information from the compromised server. Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. In this paper, a symmetric solution for two-server PAKE, where when a user is registered as a client its related information of username & password will be forwarded to web server using web services where it will be encrypted using Diffie-Hellman key exchange and ECC algorithm and a public key is generated which will be notified to client for decryption purpose. The encrypted data is broken & distributed among no. of active servers of system which will be united if & only if trusted user is logged in for system. To maintain the privacy, system is also provided with two steps mobile based verification system by sending a random number to authentic user's mobile.

KEYWORDS: Diffie-Hellman key exchange, Elliptic curve cryptography,Password-authenticated key exchange

I. INTRODUCTION

Passwords are the most common way to prove identity of user when accessing protected data, accounts and user computer itself. The use of strong passwords is therefore essential in order to protect user security and identity. The best security in the world is of no use if a malicious person has a legitimate user name and password. Now-a-day every digital transaction requires the password and it is required to keep track of password in the database. So the security of password is of important concern. Therefore it is highly required to preserve the password from every attacker. Previously password-based authentication systems transmitted a cryptographic hash of the password over a public channel, but there is a possibility of guessing the password by attackers against the true password's hash value. Recent research advances in password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication.

The current solutions for password based authentication follow two strategies. In first strategy, assumes that the client keeps the server's public key in addition to share a password with the server and the client can send the password to the server by public key encryption. The second strategy is called password-only strategy where the password is used as a secret key to encrypt random numbers for key exchange purpose.

Previous protocols for password-based authentication assume a single server stores all the passwords necessary to authenticate clients. So, when the attacker attacks the server, the whole meaningful information regarding password will be available to attacker in encrypted form and with the use of some encryption tool & guessing ,the attacker can decode the required password and can access the system information. So to avoid such a problem the proposed work provides a

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

solution usingefficientserver authentication and verification using ECC.

In this system, user is secured by using two server's password authentication process along with proper mobile verification. When user enters the password, it will be forwarded to web server using SOAP (Simple Object Access Protocol). SOAP is a secure &stateful protocol which is used to hold & sends entered password to web server. At web Server the password is encrypted using Diffie-hellman key exchange protocol and ECC scheme as described below. After encryption at web server the encrypted characters are divided by total no. of servers i.e. if *C* is a cipher text from password plaintext P and N is no. of servers where passwords will be stored then each server (*Si*) will get

$Si=C/N$

It means, If no. of servers where we are storing password is two and the count of cipher text character is 10 then every server will be storing 5 Cipher text characters. For example, if $pwd_1$is a data stored in server1 say S1 &$pwd_2$is a data stored in server2 say S2 then the whole cipher text C is obtained as

$C=pwd_1+pwd_2$

So, when attacker attacks the server, he able to get insufficient encrypted information. Therefore whole password cannot be disclosed.

At the client side, both the encryption and decryption key pairs are generated for the two servers and delivered to the servers via different secure channels during the client registration.Two-server PAKE protocol at client sends two halves of the password to the two servers in secret. In fact, a server should not know the encryption key of another server and is restricted to operate on the encryption of the password on the basis of the holomorphic properties of ECC scheme.

Along with this when data is forwarded to web server from client side, the web server will generate a unique identification number which will be forwarded to user's registered Mobile Number. User can access his data only when entered unique identification number matches with web server's unique identification number for further processing.

This system can be applied in distributed systems where multiple servers exist.The objectives of this proposed work are to design and implement minimum two server password authentication system where we store encrypted password on different servers & the data will be decrypted for authentic user only. The system should be robust & safe in case of malfunctioning attacks. In order to prevent unauthorized person from taking access of system & database by providing two step mobile verification.

II. LITERATURE SURVEY

In 2005, Katz et al. [2] proposed the first two-server password-only authenticated key exchange protocol with a proof of security in the standard model. Their protocol extended and built upon the Katz-Ostrovsky-Yung PAKE protocol [3] called KOY protocol.The advantage ofthis protocol is the structure which supports two servers to compute in parallel and disadvantage is inefficiency for practical use. Built on Brainard et al.[4] work in 2005, Yang et al. [5] suggested an asymmetric setting, where a front-end server, called service server (SS), interacts with the client, while a Back-end server, called control server (CS), helps SS with the authentication, and only SS and the client agree on a secret session key in the end. They proposed a PKI-based asymmetric two-server PAKE protocol in 2005 [5] and several asymmetric password-only two-server PAKE protocols [6,7] in 2006. The security of Yang et al.'s protocol is based on an assumption that the back-end server cannot be compromised by an active adversary. This assumption was later removed at the cost of more computation and communication rounds. The advantage is its efficiency for practical use. Yang et al.'s protocols are more efficient than Katz et al.'s protocols in terms of communication and computation complexities and disadvantage is its protocol structure which requires two servers to compute in series and needs more communication rounds.Jin further improved Yang et al.'s [8] protocol and proposed a two-server PAKE protocol with less communication rounds.The advantage is it needs less communication rounds than Yang et al.'s protocol without introducing additional computation complexity and its disadvantage is its protocol structure which requires two servers to compute in series.

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem. Firewalls and proxy servers will normally block this kind of traffic. A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this which provides a way to

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

communicate between applications running on different operating systems, with different technologies and programming languages.

III. PRILIMINARY ALGORITHM

Diffie–Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. To implement Diffie-Hellman[12], the two end users Alice and Bob, while communicating over a channel they mutually agree on two positive whole numbers *q* and *g*, such that *q* is a prime number and *g* is a generator of *q*. The generator *g* is a number that, when raised to positive whole-number powers less than *q*, never produces the same result for any two such whole numbers. The value of *q* may be large but the value of *g* is usually small.Once Alice and Bob have agreed on *q* and *g* in private, they choose random positive whole-number *m* and *n*, Next, Alice and Bob compute public keys *A* and *B* based on their personal keys according to the formulas

$A = g^m \bmod q$
$B = g^n \bmod q$
The two users can share their public keys *A* and *B* over a communications medium assumed to be insecure, such as the Internet or a corporate wide area network (WAN). From these public keys, a number *x* can be generated by either user on the basis of their own personal keys. Alice computes K_1 using the formula
$K_1 = (B)^m \bmod q$
Bob computes K_2using the formula
K_2 = (A) n mod q
Obviously$K_1 = K_2$.So this will be shared secret key among Alice and Bob.Elliptic Curve Cryptography (ECC) fits well for efficient and secure encryption method. ECC utilizes lesser key sizes for correspondent security. This facet of ECC enables it to be applied to wireless networks where there are constraints related to memory and computational power.

Mathematical Concept of Encryption and decryption

Consider a Prime Number p, another number m and e where e<pand m<p.Then,
m*e=c (mod p) (1)
where c is the remainder obtained by multiplying m & e and withrespect to prime p.We find number d , such that :
e*d =1(mod p) (2)
The above operation is accomplished using Extended EuclideanAlgorithm. Finally m is recovered as follows:
d*c= m (mod p) (3)
So the actual operation
c=(m*e) mod (p)
d*c (mod p)= d*(m*e)=(m*1)=m (mod p)

m is recovered in this way. d is computed using Extended
Euclidean Algorithm.(1) is the Encryption Operation and (3) is the DecryptionOperation.
The elliptic curve cryptographic scheme requires the point andscalar multiplication defined as follows:
Q=kP=P+P+P+…+P (k times)
where P denotes a point on the elliptic curve and k is arandom integer. Point addition and point doubling play a keyrole in scalar multiplication algorithm for scalar multiplicationas shown in below:

Key Initialization and processing

We compute SK as SK=rQ. SK has two components that are the x-co-ordinate and the y-co-ordinate. SK represents the session key that represents the Key, with which data is actually encrypted.

Encryption

Let the Bit Size of the key be n .The Block Size of the Message to be encrypted will be of size n. The Block of message is represented as an n-bit number by simply concatenating the Base 2 representation of each character in the message.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Step 1
We choose a message block m of Size n. The x-co-ordinate of SK becomes the Encryption Key and in this step, we accomplish the modular operation with respect to the Private-Key k. The remainder generated is tempc.
m * (SK.x) =tempc (mod k)

Step 2

Here we multiply tempc generated in step1 with the corresponding y-co-ordinate of Session Key,SK with which Encryption was performed with it's x-co-ordinate in Step1. This operation is done with respect to the Field Prime p. The remainder obtained in this step forms the final Cipher Text. This is denoted by c.

tempc * (SK.y)=c (mod p)

Reason for using k is that, we don't introduce a new variable into the Encryption process and so the overhead in transferring Secret components reduces, since the Private Key is directly involved in Key Generation and in Encryption, Decryption Processes. Finally, R is appended to the Cipher Text.

Decryption

We have used the El-Gamal Scheme for Session Key Generation. After receiving the secret-key, we perform scalar multiplication to compute D=kR, where R is retrieved from the Cipher Text, to which it was appended during encryption.
But R=rP.
So, D=krP.
During Encryption, we computed SK as SK=rQ, where Q is the public-key. But Q=kP.
So , SK=rkP=krP=D.
So, SK is recomputed as D here and the same is used for decryption.

Step 1
The Size of the Block remains the same, n. Represent this block of data as a n-bit number, c and Multiply it with the corresponding Decryption key d1 , where d1*D.y 1(mod p) since this operation was performed last during Encryption Operation. This is done with respect to the Field Prime p. The remainder generated is tempc.
c*d1 =tempc (mod p)

Step 2
Here we multiply tempc generated in step1 with thecorresponding decryption key for step2 ,d2 , where

d2*D.x=1(mod p)

This operation is done with respect to the Secret-Key k. The Remainder obtained is the original message. Thus the original mis recovered.If private Key, k<p

tempc* d2 =c (mod k)
If private Key, k>p
(tempc+p)* d2 =c (mod k)
The Remainder obtained is the original message. Thus the originalm is recovered.

Algorithm

Input: P, a , k
Output: Q=kP
Q=0;
for i=k–1 to 0
if k[i]=1

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Q<=2Q (Point doubling);
If i=! 0
Q<=P+Q (Point addition);
end if
end if
end for
return Q;

The flow chart of the scalar multiplication is shown in Fig.2

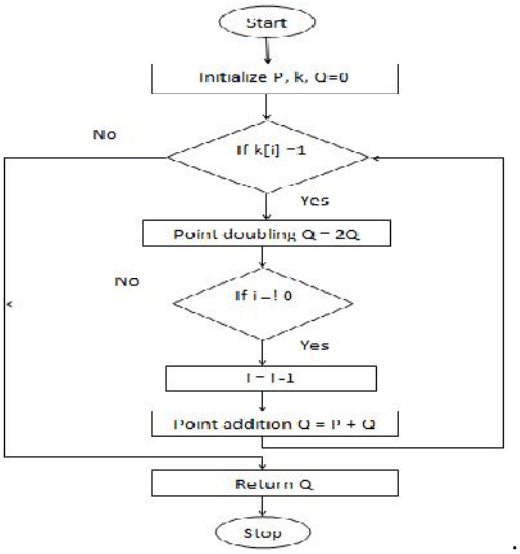

Fig 2: Flow chart of the scalar multiplication

IV. SYSTEM IMPLEMENTATION

According to paper, we are implemented the secure two server password authentication system. The basic flow of system is shown in following figure 3.The target system consist of following modules namely Client registration module, Web Service Operations, two server modules to store password and a two-step mobile verification module.

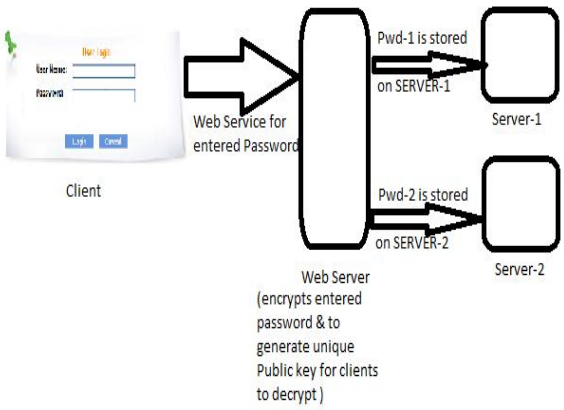

Fig 3: Block Diagram of System

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A) Client Registration Module
In this module client is registering himself as an authentic user by entering username, password, personal mobile number & other necessary information. The entered data will be directed towards web server using SOAP protocol for further processing.

B) Web Service Operations
In this module the incoming password information is encrypted using Diffie-Hellman Key Exchange Protocol &ECC Scheme. After encryption encrypted password is broken into two sub passwords on the basis of length of total password i.e. if length of encrypted password is 10 characters then each sub password contain 5 characters. All the sub passwords will be directed & stored in two different servers.

C) Server Modules (Two Server)
This module will store the password coming from web server & will be retrieved only at the time of authentication to maintain the securities in the system.

D) Two step mobile verification system
This module is used to enhance the security of system by involving mobile verification process. In this module, when user registers for the system, web server will generate and send a unique random verification code to client's mobile for verification purpose. If user enters the correct verification code then only he/she will get an access to further processing & data access. The said module is similar to Google verification system. To complete two step verification process, we use android mobile API interface.

V. CONCLUSION

Overall, the project design will achieve its objectives. The project will provide an efficient, meaningful and secure two server password authentication system along with mobile based validation system for only authentic user access.
To insert user's precise information such as password we use SOAP protocol. To configure the SOAP we use web services.

REFERENCES

[1] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.
[2] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "Two-ServerPassword-Only Authenticated Key Exchange," Proc. Applied Cryptography and Network Security (ACNS '05), pp. 1-16, 2005.
[3] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords,"Proc. Int'l Conf. Theory and Application of CryptographicTechniques: Advances in Cryptology (Eurocrypt '01), pp. 457-494,2001.
[4] J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two- Server Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.
[5] Y. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise," Proc. 20th IFIP Int'l Information Security Conf. (SEC '05), pp. 95-111, 2005.
[6] Y. Yang, R.H. Deng, and F. Bao, "A Practical Password-Based Two-Server Authentication and key Exchange System," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 105-114, Apr.-June 2006.
[7] Y. Yang, R.H. Deng, and F. Bao, "A Practical Password-Based Two-Server Authentication and key Exchange System," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 105-114, Apr.-June 2006.
[8] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two- Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.
[9] M. Abdalla, O. Chevassut, and D. Pointcheval, "One-Time Verifier-Based Encrypted Key Exchange," Proc. Eighth Int'l Conf. Theory and Practice in Public Key Cryptography (PKC '05), pp. 47-64, 2005.
[10] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure against Dictionary Attacks," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 139-155, 2000.
[11] http://www.schneier.com/blog/archives/2006/12/realworld_passw.html, 2013.
[12] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, IT-22, no. 6, pp. 644-654, Nov. 1976
[13] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
[14] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.
[15] Y. Tsiounis and M. Yung, "On the Security of ElGamal based Encryption," Proc. First Int'l Workshop Practice and Theory in Public Key Cryptography: Public Key Cryptography (PKC '98), pp. 117-134, 1998.
[16] "Design For a Patient-Centric Medical Information System Using XML Web Services" International Conference on Information Technology (ITNG'07) 0-7695-2776-0/07, 2007