International Journal of Computer Networks and Communications Security

VOL. 2, NO. 4, APRIL 2014, 142–145
Available online at: www.ijcncs.org
ISSN 2308-9830

Secure Mutual Authentication Protocol

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

[1, 2] Department of Computer Engineering, MIT Academy of Engg. Alandi , pune

E-mail: [1]spnakhate@it.maepune.ac.in, [2]rmgoudar@comp.maepune.ac.in

ABSTRACT

In this paper, we have proposed a Secured password based mutual authentication protocol for client-sever computing using elliptic curve cryptography. The proposed framework provides mutual authentication and session key agreement in client-sever environment. It provides secure communication between client and server with help of user email-id and mobile phone as authentication device for mobile hand held device. ECC based mutual authentication protocol is best suited for constrained environments where the resources such as computational power, storage capacity are extremely limited. Devices are such as Mobile phones, PDA's, palmtops, smart cards.

Keywords: *Double Authentication, Password change, Mutual Authentication, Session key agreement, ECC.*

1 INTRODUCTION

Most web services presently use passwords to authenticate the user. However, regardless of the strength of the passwords, this type of authentication is proving to be no longer sufficient, mainly because it can be easily exposed to attacks such as key logging and phishing. Strong electronic authentication is the identification of users based on two or more factors: something the user knows, such as a password; something the user possesses, such as a chip card, device (mobile); or something that characterizes the user, such as a fingerprint. Such strong authentication mechanisms already exist but, unfortunately, most of them have the drawback of being costly. They often use security tokens that are expensive to deploy and quite impractical for users. Hence, there is a need to create stronger authentication mechanisms while still maintaining a good level of usability.

The solution lies in using cryptography and secures authentication protocols that guarantee the confidentiality, authentication and integrity of communications. Most of them are based in RSA public key cryptography. A protocol is developed which is based exclusively on elliptic curve cryptography (ECC), an asymmetric cryptography that performs well in resource constrained platforms and maintain the high security level that one can achieve with the protocols in use today. So experiments have been conducted over various asymmetric cryptographic algorithms to reduce power consumption. Analyses of the power consumption of them are performed to offer users information to produce optimal algorithm for sending information [5]. One way to improve the performance of Conventional ECC cryptosystem is to use an efficient method for point multiplication which is the most time consuming operation. ECC over Window NAF method executes somewhat faster than the conventional ECC. By using ECC over Window NAF, the energy consumption for mobile hand-held devices with no compromization of security.

The rest of the paper is organized as follows. Section II contains related work. Section III expresses the proposed user mutual authentication protocol scheme. In Section IV we discussed security analysis of proposed framework. Finally Section V accounts conclusion.

2 LITERATURE SURVEY

A. Hash-based password authentications

Sanjeet Kumar [1], suggested a hash-based password authentication scheme that mutually authenticates the client and the server successfully,

although it is immune from server's data eavesdropping and impersonation attacks, but vulnerable to reply attack, also its high hash computation and password resetting problem decreases its applicability for practical use. Develop an improved mutual authentication framework with two factor i.e. email-id of registered user but require formal security proofing techniques and techniques for Preserving the privacy of the user's information provided to the server.

B. Password-based authentication scheme

Ding Wang [3] Password-based authentication scheme is vulnerable to various attacks. The offline password guessing attack, stolen-verifier attack and denial of service attack for Islam-Biswas's remote user authentication scheme. Elliptic curve cryptography (ECC) to overcome the drawbacks. It provides the functions of password change, secret number update, revocation and Denial of Service resistant to make protocol much more flexible. Furthermore, the security of scheme is based upon the secure one-way hash function and elliptic curve cryptosystem.

C. Measurement for ECC cryptographic algorithm

The most of the existing authentication protocols are based on RSA asymmetric cryptography are not suitable for such devices due to their confines in computing power, memory capacity, key sizes and cryptographic support. An efficient protocol for resource constrained platforms that attain a level of security similar to the one achieved by the protocols in use today is designed and implemented.

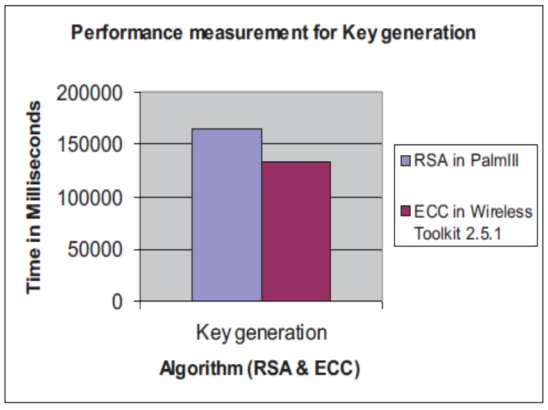

Fig. 1 Measurement for ECC cryptographic algorithm

The Figure 1 shows that performance measurement for RSA and ECC. It is possible to implement the authentication protocol using ECC in resource constrained mobile devices with reasonable performance compared to RSA. Protocols based on this ECC asymmetric cryptography can be directly used in such devices.

3 PROPOSED AUTHENTICATION PROTCOL

The proposed system consists of two main modules. One is client module and second one is server module. Client module is used by user to register and login with server and server module is used to maintain user verification table for user login, if user successfully login with server using mutual authentication protocol, the user can have access to server's services or data. Figure 3.1 show the system design.

1. Server initialization phase

The server chooses an elliptic curve E and P is a generator of order q, where q is large prime number and p = 2q + 1. The server chooses its secret key x keeps it in private.

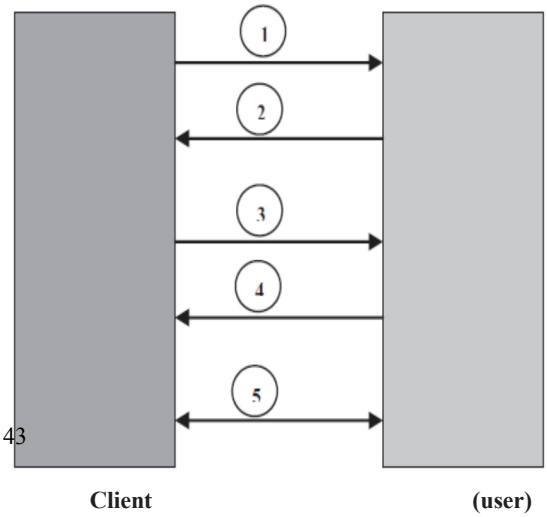

Fig. 2 Mutual authentication proposed protocol using ECC

2. Registration Phase

The user first registered with server with user id, email-id and mobile number. The server generates a dynamic token and sends this to user's email id via text message. This step provides double authentication in registration phase.

The user enters that token by checking his registered email-id and his password to confirm his registration.

Server computes authentication information and sent it to user's registered email-id and keeps in the

registration table user id, email-id and mobile number, in private with encrypted form.

1. Login and Authentication Phase

The user enters his id and password in the login interface of his system. Then, the user's system computes the secret value using the stored value which was already sent by server in registration phase.
The user's system generates a nonce (random number used once) and then sends to the authentication server the encrypted message using ECC algorithm.
Server decrypts the message and extracts user's nonce.
The server generates a nonce and sends encrypted message to user.
Upon receiving the server message, user's system decrypts it and verifies that the received is equal to the sent.
Upon receiving the message, server decrypts and extracts server nonce. Server verifies that server nonce received is equal to server nonce sent.
If both are equal, the server trusts the user and allows him to communicate and sent dynamic One Time Password on user's email-id.
User's check email-id and re-login to server.

2. Password Change phase

This phase is used when the users want to change his password from old password to new password.
User enters his id and old password in his system and request message for password change to Server.
Server checks this with the stored password in the database and if both are matched then the server sent a dynamic token to his registered email-id.
Upon receiving the token the user inputs that token as session password.
Server sent alert of successful password changed to the user's email-id or mobile phone.

5 SECURITY ANALYSIS

The efficiency of authentication protocol can be measure with respect to following factors over the unreliable networks. The certain cryptographic security attributes of the proposed scheme and some relevant schemes is in table 1.

Table 1: Functionality Comparisons of Different Remote Login Schemes with Proposed Scheme

Scheme	Sanjeet Kumar [1]	Chandra se-khara[2]	Xuel ei L[4]	Prasan na Ganesa n [5]	Propos ed Scheme
Session Key management	Yes	Yes	Yes	Yes	Yes
Mutual authentication	Yes	No	No	Yes	Yes
Password change	Yes	No	No	Yes	Yes
Clock synchronization Problem	No	No	No	No	NO
Extra Hardware device	No	No	No	No	NO
Band Width Requirement	High	Low	Low	Low	Low

6 CONCLUSION

The static passwords based and two-factor authentication scheme don't satisfy the needs for security, flexibility and cost. The best cryptographic algorithm ECC is used for safety and fast speed. The proposed mutual authentication scheme that uses OTP authentication for the login procedure, a very secure registration system and with all traffic transmissions encrypted with ECC.

The implementation provides high security for the users while it is still easy to use. The big difference from solutions with static passwords is that the password in this solution is only valid for one time only, which is big advantage in security.

7 REFERENCES

[1] Sanjeet Kumar, Nayak, Subasish Mohapatra, Banshidhar Majhi "An Improved Mutual Authentication Framework for Cloud Computing" International Journal of Computer Applications, Volume-5, August 2012.

[2] K R Chandrasekhara Pillai, Sebastian and M P Sebastian" Elliptic Curve based Authenticated Session Key Establishment Protocol for High Security Applications in Constrained Network Environment" International Journal of Network Security & Its Applications (IJNSA), July 2010.

[3] Ding Wang, Chun-guang Ma, and Yu-heng Wang" On the Security of an Improved Password Authentication Scheme Based on ECC", LNCS, Springer–Verlag , 2012.

[4] Xuelei Li, Fengtong Wen and Shenjun Cui"A strong password-based remote mutual authentication with key agreement scheme on

elliptic curve cryptosystem for portable devices" An International Journal 2012.

[5] Mrs. S. Prasanna Ganesan" An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography" 2010 IEEE.

[6] SK Hafizul Islam , G.P. Biswas "Design of improved password authentication and update scheme based on elliptic curve cryptography ",Science Direct 2011.

[7] Aqeel Khalique ,Kuldip Singh, Sandeep Sood "A Password-Authenticated Key Agreement Scheme Based on ECC Using Smart Cards" International Journal of Computer Applications ,Volume 2 – No.3, May 2010.

[8] Rajaram Ramasamy and Amutha Prabakar Muniyandi" An Efficient Password Authentication Scheme for Smart Card" International Journal of Network Security, Vol.14, No.3, 2010.

[9] Amutha Prabakar , Muniyandi Rajaram , Ramasamy Indrani" Password Based Remote Authentication Scheme using ECC for Smart Card" ACM, 2011.

[10] Shanmugapriya S, Gulzar Begam J" Two Factor Authentication on Cloud" Journal of Computer Applications, Volume-5, Issue EICA2012-5, February 10, 2012.