Remote User Authentication Protocol for Multi-Server Architecture Based on ECC

Vishal Chaugule[1] Ravindrakumar Deshmukh[2] Shreyas Deshpande[3] Prof. Bhate D.V[4] Prof. Sonawane K. P[5]

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]Dnyanganga College of Engineering and Research, Pune, India

Abstract— We have reached an era where desired web services are available over the networks by click of a button. In such a scenario, remote user authentication plays the most important role in identifying the legitimate users of a web service on the Internet. Researchers have proposed a number of password based authentication schemes which rely on single server for authentication. But, with tremendous advancements in technology, it is possible to engage multiple servers in authenticating their clients in order to achieve better security. In this paper, we propose an efficient password based authentication protocol for multiserver architecture. The protocol provides mutual authentication using user system and is based on Elliptic Curve Cryptography, therefore offers best security at a low cost. In 2011, Sood et al. proposed a multi-server architecture protocol using user systems. In this paper, we improve Sood et al. scheme by increasing its security and reducing the computation cost. The protocol is based on the concept of dynamic identity that uses a nonce based system and has no time synchronization problem.

Key words: ECC, CS, Elliptic Curve Cryptography

I. INTRODUCTION

Remote user authentication is the process of identifying a legitimate user of a particular web service on the Internet. Due to their low cost, efficiency and portability, user systems are widely used in e-commerce applications for remote user authentication process. The user of the user system firstly enters his credentials such as identity and password. Based on this information, the authentication server and the user system perform cryptographic operations to authenticate the user of the web service. A number of password based authentication schemes have been developed where only single server is involved in the authentication process. The authentication information stored on a single server becomes highly susceptible to various attacks such as leak of verifier, server spoofing and stolen verifier attack. Nowadays, computing has become very popular where multiple servers are involved in authenticating their users. Therefore, multi-server authentication schemes are required to cater to the needs of modern computing services. Over last few years, researchers have developed password based authentication schemes based on multiple server i.e. (Ford and Kaliski, June 2000; Jablon, 2001; Lee and Chang, 2000; Lin et al., 2003; Brainard et al., 2003; Mackenzie et al., 2006; Juang, 2004; Chang & Lee, 2004; Yang et al., 2005; Hu et al., 2007; Tsai, 2008; Liao and Wang, 2009; Hsiang and Shih, 2009; Sood et al., 2011). Most of the proposed schemes are susceptible to one or more security attacks and involve high computation and communication cost. In this research paper, we propose an authentication scheme which is based on two-server-architecture paradigm. The authentication parameters of the user are distributed among two servers namely the control server and service provider server. The back-end control server is less exposed to the clients and therefore is more secure from various security attacks. The user directly communicates only with the service provider server which in turn communicates with the control server to authenticate the user of the web service.

The system is proposed as follows in the following ways:

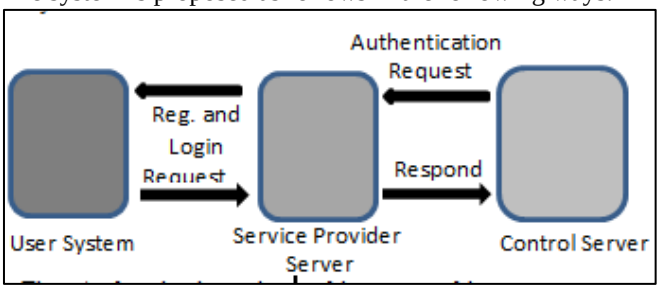

Fig. 1: Authentication Using Multi-Server Architecture

Multiple servers are involved in authenticating their users. Authentication parametres are distributed among two servers namely the control server & service provider server.

II. RELATED WORK

The first multi-server password based authentication scheme was proposed by Ford and Kaliski (2000). The protocol splits the password information among multiple servers and therefore a malicious user cannot compromise the password by launching various attacks. The protocol uses public key systems to achieve authentication and therefore is computationally expensive.

III. PROPOSED METHODOLOGY

In this system, we proposed following phases:

1) Registeration Phase
2) Precomputation Phase
3) Login Phase
4) Authentication Phase
5) Password Change Phase

A. Registration Phase:

User system submits his identity Idi , password Pi and server identity SIDk then CS validates,

$$Fi = H (X | Idi | Yi) \times G$$

Where, Fi = Security Parameter
X = private key of server based on ECC
Idi = User identity
Yi = server secret no. for user Ui
H() = hash function
G=generator point

After generating security parameter US generates,

$$Ei = H (Idi | Pi) \oplus Pi \oplus Ni$$

Where, Ei = Security parameter
Pi = User password
Ni = random no. generaed by US
Then US stores (Fi , Ei)
CS computes,

$$Mk = Sk \oplus H (X | Sidk) \times G$$

Where, Mk = Security parameter
Sk = Kth service provider server
Sidk = Unique identification of Kth SPS
CS stores, (Mk, Sidk).

B. Precomputation Phase:

The user system selects a random number N1 and computes ECC point P1 ¼ N1 _ G. Then it stores P1 in its memory as a communication parameter which is used in the process of authentication.

C. Login Phase:

The user Ui in order to login with the service provider server Sk inserts his smart card into a card reader machine and submits his IDi, password Pi and the identity SIDk of service provider Sk. The authenticity of the user is verified by the smart card which then sends the verification and login information to the destination server Sk.
US computes,

$$Ei^* = H (Idi^* | Pi^*) \oplus Pi^* \oplus N$$

Then checks Ei*? = Ei
US calculates,

$$P11 = N1 \times Fi$$

Where, P11 = ECC
N1 = Nonce generated by US
Sends [P1 , P11] to CS

D. Authentication and Session Key Agreement Phase:

The verification information of user and server Sk is passed to the control server CS by the service provider server Sk. The server Sk and the control server CS mutually authenticate each other and the user Ui. Once authenticated, the user Ui, service provider server Sk and control server CS agree on a common session key for further communication.
SP calculates,

$$P2 = N2 \times G$$
$$P22 = N2 \times Mk$$

Where, P2 & P22 = ECC point
N2 = Nonce generated by SPS
Mk = security parameter computed by CS
CS extracts Yi from Yi ⊕ X,
Calculates point,

$$P'11 = P1 \times H (X | Idi | Yi)$$

E. Password Change Phase:

The user can freely change his password without the interference of the control server CS. Before the system begins, the control server CS selects a large prime number p and two integer elements a and b where p is of high order such that p > 2160 and a and b satisfy the equation (4a3 þ 27b2) mod p s 0. Then the server selects an elliptic curve equation Ep over the finite field p: y2 ¼ (x3 þ ax þ b) mod p. The server selects a generator point G of order n, where n is a large divisor such that n _ G ¼ O. The server also selects X as its private key and publishes (Ep, G, n, p).
US computes,

$$Ei^* = H(Idi^* | Pi^*) \oplus Pi^* \oplus N^*$$

Compare with Ei And calculate new password,

$$Einew = H (Idi | Pinew) \oplus Pinew \oplus Nnew$$

Ui	User i
Sk	Kth service provider server
CS	Control Server
Idi	Unique Identification of User Ui
SIDk	Unique Identity of kth service provider server
Pi	Password of User Ui
X	Private key of Server based on ECC
Yi	Server's secret number for user Ui
Ni	Random number generated by smart card for user Ui
N1	Nonce generated by smart card
N2	Nonce generated by server provider server
N3	Nonce generated by control server
Ep	Elliptic Curve equation over Zp
P	Large prime number
Zp	Algebraic Group over p
H()	Secure public one way hash function
⊕	XOR Operation
|	Concatenation

Table 1:

IV. H/W, S/W REQUIREMENTS

Following are the hardware and software requirements for our system,

1) RAM 256 MB ,
2) 1 GB HDD
3) Apache Tomcat Server,
4) Internet Browser.
5) Ellipse Indigo
6) SQL
7) Java

V. COST ANALYSIS

An efficient authentication protocol must consider computation and communication cost while authenticating a remote user. Elliptic Curve Cryptography is a public key cryptography that provides maximum strength per bit in terms of security. For the same level of security, the length of cryptographic keys in ECC is comparatively much smaller than any other public key systems. Table 1 shows the comparison of key sizes among various cryptographic techniques. Moreover, our protocol uses only XOR operations and one-way hash functions, both of which are very inexpensive operations in cryptography. Our protocol is very secure and efficient as it is based on random nonce values and has no time synchronization problem as the protocol does not use timestamps. The remote user authentication protocols based on timestamps are subjected to time synchronization problems if the server's and client's

clock in not synchronized. While calculating the cost of the protocol, the identity IDi, password Pi, X, Yi and nonce values (N1, N2, N3) all are assumed to be 128 bits long. Also, the output of the one way hash function is 128 bits and elliptic curve cryptosystem is ECC e 224 bits. Let TH, TE, TECM, TS be the time for one hashing operation, one exponential operation and time for one multiplication of a number over elliptic curve, time to carry out symmetric encryption/decryption respectively. The comparison of the time complexity associated with these operations can be expressed as TS >> TE >> TECM > TH. The time taken to perform an exponential operation is much more (approx. 8 times) than the time taken to perform one elliptic point multiplication. Let (E1) be the memory needed in smart card to store the security parameters. In the proposed protocol, the parameters stored in the smart card are Ei and Fi is (352) bits Let (E2) be the cost of communication parameters involved in the authentication process.

VI. CONCLUSION

Password based authentication schemes make an ideal choice for e-commerce applications over cooperate networks as they provide multifactor authentication between the user and server. With a low computational and communication cost it prevents all well-known attacks by the malicious users of the network. We have proposed an efficient multi server authentication protocol using smart cards based on Elliptic Curve Cryptography (ECC). The use of ECC provides all the benefit of using an asymmetric crypto system even for a constrained environment of a typical smart card. With a low computational and communication cost it prevents all well-known attacks by the malicious users of the network.

REFERENCES

[1] Chien HY, Chen CH. A remote authentication scheme preserving user anonymity. In: Proceedings of the advanced information networking and applications 2005. p. 245e8.
[2] Das ML, Saxena A, Gulati VP. A dynamic id-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 2004;50(2):629e31.
[3] Chang CC, Lee JS. An efficient and secure multi-server password authentication scheme using smart cards. In: Proceedings of the international conference on cyber worlds November 2004.
[4] Jablon DP. Password authentication using multiple servers. In: Proceedings of the RSA security conference April 2001. p. 344e60
[5] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proceedings CRYPTO 99 1999. p. 388e97.
[6] Lee WB, Chang CC. User identification and key distribution maintaining anonymity for distributed computer networks. Computer System Science 2000;15(4):211e4.
[7] Liao YP, Wang SS. A secure dynamic id-based remote user authentication scheme for multi-server environment. Computer Standard & Interface 2009;31(1):24e9.
[8] Liao IE, Lee CC, Hwang MS. Security enhancements for a dynamic id-based remote user authentication scheme. In: Proceedings of the conference on next generation web services practice July 2005. p. 437e40.
[9] Lin IC, Hwang MS, Li LH. A new remote user authentication scheme for multi-server architecture. Future Generation Computer System 2003;19(1):13e22.
[10] Mackenzie P, Shrimptom T, Jakobsson M. Threshold password authenticated key exchange. Journal of Cryptography 2006;19(1):27e66.
[11] Messerges TS, Dabbish EA, Sloan RH. Examining smart card security under the threat of power analysis attacks. IEEE Transactions on Computers 2002;51(5):541e52.
[12] Sood SK. Secure dynamic identity-based authentication scheme using smart cards. Information Security Journal: A Global Perspective 2011;20:1e11.
[13] Sood SK, Sarje AK, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Application 2011;34:609e18.
[14] Tsai JL. Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers & Security 2008;27(3e4):115e21.
[15] Wang RC, Juang WQ, Lei CL. Robust authentication and key agreement scheme preserving the privacy of secret key. Computer Communications 2011;34:274e80.
[16] Yang JH, Chang CC. An Id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computer & Security 2009;28:138e43.

