# A Preventive Security Architecture using Two Factor Password Authentication

**M. Sharmila**
Research Scholar
School of Computer Science and Engineering, Bharathidasan University, Trichy

*Abstract*— The advancement in internet increases the threats over computer networks. Today, the nodes of the network can easily be compromised or intruders have the ability to intervene between the server and the user to observe the transactions or to perform malicious activities. Hence, network security has to be enriched with newer technologies so as to protect the internet users from being attacked by various network threats. This paper proposes a novel architecture that enforces end to end security between the user and server. The security of the user is obtained by proposing a two factor password authentication scheme; where by the security of the server is obtained by implementing elliptic curve. Cryptographic algorithm in both storage and transmission.

***Key words:*** attacks, network security, two factor, elliptic curve

## I. INTRODUCTION

Security incidents are increasing at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center operators, network administrators, and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today.

Effective network security demands an integrated defense-in-depth approach. The first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security. These fundamental security elements form security architecture, creating a strong foundation on which more advanced methods and techniques can subsequently be built. Developing and deploying security architecture can, however, be challenging due to the vast range of features available. The Network Security architecture is designed to assist in this endeavor by outlining those key security elements that should be addressed in the first phase of implementing defense-in-depth. The main focus of Network Security architecture is to secure the network infrastructure itself.

The current security mechanisms and protocols of computer networks are mainly concerned with user authentication, key exchange and key management techniques. User authentication is a process that allows a device to verify the identity of someone who connects to a network resource. There are many technologies currently available to a network administrator to authenticate users. One among the approach is the verification of user login credentials such as user name and password. Most people are not careful about keeping secrets such as passwords and access codes that form the basis for most secure systems.

All security systems rely on a set of measures employed to control access, verify identity and protect disclosure of sensitive information. These measures usually involve one or more "secrets". Should a secret be revealed or stolen then the systems that are protected by these secrets can be compromised.

The non-disclosure of authentication credentials such as usernames and passwords is critical in any system where access is done over non-secure networks, it is important to be concerned about disclosing information that is exchanged between network elements, computers or systems. When a user wishes to avoid data disclosure over a network, encryption methods must be employed that make the transmitted data unreadable to someone who might somehow capture the data as it traverses a network. There are many methods to "encrypt" data.

This paper proposes architecture that encompasses a password scheme for secured user login and ECC encryption method to secure the stored user data. This paper is organized as follows, section II describes the review of literature, section III contains the methodology of the proposed work and section IV elucidates the results and discussion and finally section V presents the conclusion.

## II. REVIEW OF LITERATURE

Yang scrutinized the security requirements of smart-card-based password authentication schemes and proposed a new scheme with a generic construction framework for smart-card-based password authentication. The authors showed that a secure password based key exchange protocol can be efficiently transformed to a smartcard-based password authentication scheme provided that there exist pseudorandom functions and target collision resistant hash functions defined a set of desirable properties for secure smartcard-based password authentication schemes. They constructed a secure two-factor framework smart-card-based password mutual authentication scheme by transforming a proven secure one-factor password based mutual authentication protocol with pseudorandom functions and target collision resistant hash functions.

Gong suggested a novel one-time Password (OTP) mutual authentication scheme based on challenge/response mechanisms. Their scheme used random sub-passwords and their corresponding hashes to be shared between the user and a server vice versa.

Jun-zuo Criticized the weaknesses found in the existing password schemes SUN and LI and suggested some solutions to avoid similar mistakes in future works. The authors also motivated to design more secure enhanced schemes

Bang addressed the vulnerability of login credentials suggested a vulnerability measure of an individual's login credentials and analyzed the vulnerability of current Internet users.

### *A. Findings on Login Credentials*

1) The number of subscribing account is larger
2) Same user id and password used for multiple accounts

 

3) Limited portion of possible user id, password combinations is used
4) Usage patterns of login credentials are highly skewed

Nelson conducted an experiment where Participants in this study were assigned to select one of three password generation groups: PPC (Proactive Password Checking) restrictions alone, image-based mnemonic, or text-based mnemonic to assess the vulnerability of password cracking. All participants were individually tested by

1) By assigning to the image-based mnemonic group
2) Verbally informed mnemonic group
3) Assigned PPC passwords

*B. The Results Were Then Analyzed and Discussed In This Paper*

Cheong presented a secure two-factor authentication Near Field Communication smartphone access control system using digital key. The proposed Encrypted Steganography Graphical Password (ESGP) validated the user perception and behavioral intention to use NFC ESGP smart phone access control system through an experiment and user evaluation survey. Their goal is to propose a new system to enhance the security of access control system without imposing undue technological efforts and inconvenience.

Vu evaluated the time and number of attempts needed to generate unique passwords satisfying different restrictions for multiple accounts, as well as the login time and accuracy for recalling those passwords

*C. Recommendations For Enhancing Password Security And Memorability*

1) There should be minimum length restriction
2) Inclusion of special characters and increase the security of passwords
3) Avoid using simple patterns
4) First letter sentence generation technique improve memory of passwords
5) Administrators should use a lock-out procedures after a certain number of attempts
6) Engaging user to login multiple times after generating the password will increase the memorability

Duggan designed security policy, task models of password behavior for different user groups—Computer Scientists, Administrative Staff and Students. Modeling revealed Computer Scientists viewed information security as part of their tasks and passwords provided away of completing their work. By contrast, Admin and Student groups viewed passwords as a cost incurred when accessing the primary task.

Wang paper investigated two recent proposals in the area of smart-card-based password authentication for security-critical real-time data access applications in hierarchical wireless sensor networks (HWSN). The two schemes were equipped with a claimed proof of security. They proposed lightweight operations, such as one-way hash functions and exclusive OR operations. They also pointed out that both protocols have various security flaws being overlooked.

Huang proposed TSOTP (Time Stamp One Time Password) a new effective simple OTP method that generates a unique pass code for each use, since One-Time Passwords can provide complete protection of the login-time authentication mechanism against replay attacks. The calculation used both time stamps and sequence numbers.

## III. METHODOLOGY

This paper proposes a secure architecture that can be incorporated at two phases of generic networking such as authentication and data protection. Fig. 1depicts the proposed secured architecture.

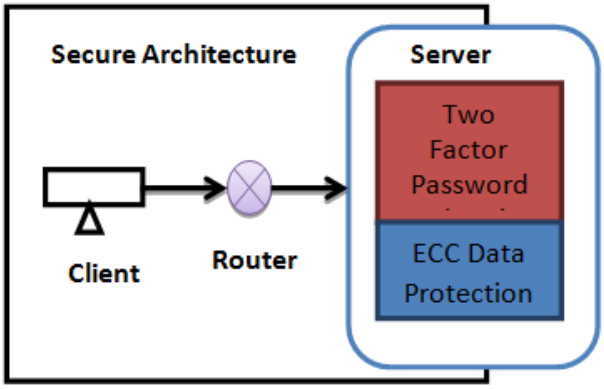


Fig. 1: Proposed Architecture

The proposed password authentication scheme consists of two passwords, where the first one is the generic alphanumeric password and the second one is the random personal password. Users are thrown number of personal questions during the registration along with user id and traditional password system. When the user prompts for login, the users are expected to enter their user id, password and the answer for a random question thrown to the user from the personal data stored in the database. When all three submissions are matched with the database the user is authenticated as valid. Otherwise, the users have to reprocess the login request. Along with the password mechanism Elliptic Curve Encryption is implemented to secure user data over the transmission medium.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

An elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

$$y2 = x3 + ax + b,$$

along with a distinguished point at infinity, denoted ∞. Where $4a3+ 27b2\neq0$ . Each value of the ‘a’ and ‘b’ gives a different elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters ‘a’ and ‘b’, together with few more constants constitutes the domain parameter of ECC.

The equation of the elliptic curve on a prime field Fp is $y2 \bmod p = x3 + ax + b \bmod p$, where $4a3 + 27b2 \bmod p\neq0$. Here the elements of the finite field are integers between 0 and

 

p –1. All the operations such as addition, substation, division, multiplication involves integers between 0 and p – 1. The prime number p is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure.

*A. Point Addition*

Consider two distinct points J and K such that
J = (xJ, yJ) and K = (xK, yK)
Let L = J + K where L = (xL, yL), then
xL = s2 - xJ – xK mod p
yL = -yJ + s (xJ – xL) mod p
s = (yJ – yK) / (xJ – xK) mod p, s is the slope of the line throughJ and K.

*B. Point Subtraction*

Consider two distinct points J and K such that
J = (xJ, yJ) and K = ($x_K$, $y_K$)
Then J - K = J + (-K) where -K = (xk, -yk mod p)
Point subtraction is used in certain implementation of point multiplication such as NAF.

*C. Point Doubling*

Consider a point J such that J = (xJ, yJ),
Where yJ ≠ 0
Let L = 2J where L = (x,y)Then
xL = s2 – 2xJ mod p
yL = -yJ + s(xJ - xL) mod p
s = (3xJ2 + a) / (2yJ) mod p

*D. Working Principles of ECC*

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit ( This should be a prime number )

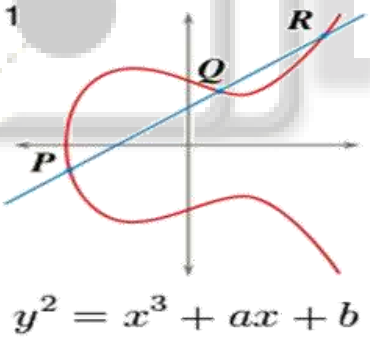


Fig. 2: Elliptic Curve Cryptography Model

*1) Key Generation*

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd' within the range of 'n'.

Using the following equation we can generate the public key
Q = d * P
d = the random number that we have selected within the range of (1 to n-1). P is the point on the curve.
'Q' is the public key and'd' is the private key.

*2) Encryption*

- Let 'm' be the message that we are sending. We have to represent this message on the curve. These have in-depth implementation details.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].
Two cipher texts will be generated let it be C1 and C2.
C1 = k*P
C2 = M + k*Q
C1 and C2 will be sent

## IV. PROPOSED SYSTEM

The proposed system is implemented in a social networking website using jsp programming. The users of the social networking are asked to enter their preference user id, full name, gender, email, mobile number, password and date of birth as an initial progress of registration.


Fig. 3: Initial Process of Registration

As a second level of registration the users are asked several personal questions which are going to be used as a random password question in the login phase. Fig. 4 represents the second phase of registration.


Fig. 4: Creation of Random Personal Password

These questions will be randomly thrown for every login prompted by the user to be authenticated by the server. The server authenticates by verifying the user id, password and random personal password for granting access to the services of the social networks. Fig. 5 and Fig.6 depicts the login phase and the home page of the proposed work.

 


Fig. 5: Login page of the proposed work

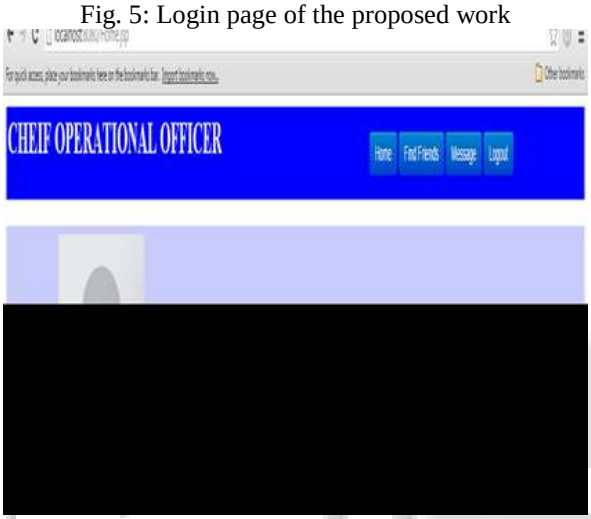


Fig. 6: Home page of the proposed work

Moreover, the database stores the user data in the encrypted form using ECC and AES. Since, ECC in asymmetric public key infrastructure it can be applied only for transmission. On the other hand, the AES can be used for data storage since, because it is symmetric cryptographic algorithm. Fig.7 shows the encrypted data storage of the proposed architecture in the server.

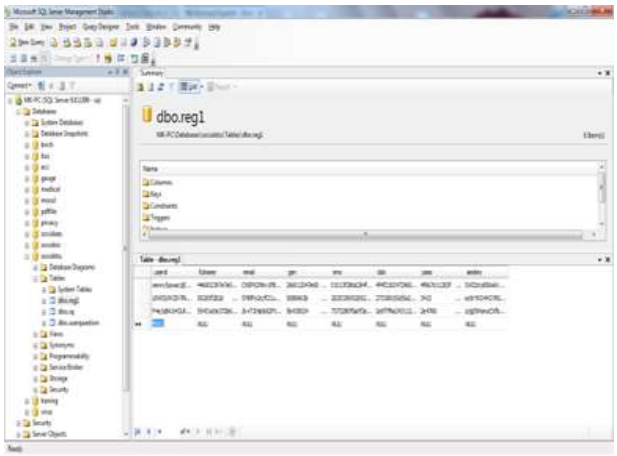


Fig. 7: Encrypted Storage of User Data

## V. CONCLUSION

With the increased number of threats to networks such as worms, viruses and clever hackers, security cannot longer be viewed as an option, even within social networks. Securing user information is critical to maintaining uptime and seamless access to services. Providing and maintaining security across social networking typically means increased administration. Historically, this has been the largest barrier to broad implementations of security. The secure architecture presented in this paper could address certain network attacks such as eave's dropping, identity theft, man-in-the middle and brute force attacks as the person should know one's life history to crack the password. Moreover, ECC cryptography is highly challengeable for the attackers to decryption user data. Hence, the architecture proposed in this paper effectively protects the user from network threats.

## REFERENCES

[1] Guomin yang , duncan s. Wong , huaxiong wang , xiaotie deg .[1]"Two-factor mutual authentication based on smart cards and passwords" JournalofComputerandSystemSciences74(2008)1160–1172

[2] Longyan Gong , Jingxin Pan , Beibei Liu , Shengmei,[2] "Zhao A novel onetime password mutual authentication scheme on sharingrenewed finite random sub-passwords" Journal of Computer and System Sciences79(2013)122–130.June 2012, 19(Suppl. 1): 137–141.

[3] Jun-zuo1, WANG Yong-jian, QIAN Hai-feng, zhou yuan JUN-ZUO [3]" On the security of two password authenticated key agreement scheme using smart cards" June 2012, 19(Suppl. 1): 137–141.

[4] YoungsokBanga , Dong-JooLee b,Yoon SooBaec, ,Jae-HyeonAhnc, [4] "Improving information security management : Ananalysis of ID–password usage and a new login vulnerability measure" InternationalJournalofInformationManagement32 (2012) 409–418.

[5] DeborahNelsona ,Kim-PhuongL.Vub, [5]" Effectiveness of image-based mnemonic techniques for enhancing theme morability and security of user-generated passwords" Articlehistory:Availableonline9February2010

[6] Soon-NyeanCheonga,Huo-ChongLinga,Pei-LeeTehb,[6]"SecureEncrypted Steganography Graphical Password scheme for Near Field Communication smart phone access control system" ExpertSystemswithApplications41(2014)3561–3568

[7] KimPhuongL.Vua, RobertW.Proctorb, AbhilashaBhargav-Spantzelb,Bik-Lam(Belin)Taib,JoshuaCookb,E.EugeneSchultzc [7], Improving password security and memorability to protect personal and organizational information" Int.J.Human-ComputerStudies65(2007)744–757

[8] PingWang, DingWang[8]" Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks" AdHocNetworks20(2014)1–15

[9] Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai Huang[9]" A new One-time Password Method" IERI Procedia 4 ( 2013 ) 32 – 37

 