International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Verifier Based Prevention for an Offline Password Guessing Attack Using ECC

Radhika L. Bhosale[1], Manoj L. Bangare[2]

[1]University of Pune, SKNCOE, Vadgaon, Pune, Maharashtra, India

[2]University of Pune, SKNCOE, Vadgaon, Pune, Maharashtra, India

Abstract: ***In remote server system, user authentication is an essential requirement. To verify the authenticity of the remote users over insure channel, various authentication methods have been proposed so far. The use of passwords for user authentication is very simple and commonly used method. The password selected by clients may be simple and easy to remember. Hence, it is responsibility of password authentication schemes to securely exchange password related information between server and client over insecure channel. Many password authentication schemes have been published but found susceptible to various attacks. ECC based existing password authentication scheme provides different features and efficient in some way. But it is found that the existing password authentication scheme is vulnerable to offline password guessing attack, stolen verifier attack and denial of service attack. The proposed password authentication scheme is based on ECC and password verifier. ECC is a public key cryptography system better than RSA cryptography because with the same key size, it gives a higher security level than RSA. Proposed scheme allows the client and server to select two random numbers independently and perform computations without exchanging them. Hence the attacker can't guess password from dictionary as he or she is unaware of random numbers selected by the client and server. Proposed password authentication scheme provides prevention scheme for an offline password guessing attack based on ECC. It also helps to securely share id based secret key between client and server.***

Keywords: Offline Password Guessing Attack, Password Verifier, Elliptic Curve Cryptography, Password Authentication, Shared Secret Key.

1. Introduction

Authentication in essence is a process of verifying the authenticity of one's claim about its identity. It is one of the most important aspects of computer security, since other security services all depend upon it. A variety of schemes have been proposed to allow a legitimate user to log into a remote server and access the resources.

Security in the user authentication process is an important and challenging task while the user's program tries to communicate with a server over an insecure communication channel. User authentication is the basic security mechanism for remote login systems. Among the numerous methods for user authentication, the password scheme is the most convenient and widely used method. Password authentication can prove better technique for user authentication if strong password authentication scheme is used. The password authentication scheme can be designed with consideration of four basic approaches based on public key encryption, private key encryption, hash function and their combinations. There are various schemes proposed for password authentication, which are having some advantages and disadvantages.

2. Related Work

Lamport [4] proposed hash based, password authentication scheme. This scheme performs mutual authentication between server and client. The method uses one way hash function for encoding the password. Though Lamport's scheme is immune to eavesdropping on server's data and impersonation attacks, but susceptible to replay attack. Mohammad Peyravian and Nevenko zunic [7] presented a secure method to protect passwords that are transmitted over untrusted networks. The scheme provides a secure method for changing the old password to a new password. The scheme does not have need of the use of additional keys as symmetric keys or public/private keys to protect password interactions. The Peyravian and Zunic's scheme does not make use of any public key or symmetric key cryptosystem. The scheme only employs a collision resistant hash function such as SHA-1.Lin and Hwang showed that the password update protocol in the Hwang-Yeh scheme [2] is not resistant to denial of service attack. Lin and Hwang revealed that the Hwang-Yeh scheme doesn't provide enough forward secrecy when it provides session key distribution. A Lin and Hwang [1] proposed an improved scheme to take away security problems that can accomplish mutual authentication and distribution of the secret key between the server S and the client C. Islam and Biswas [9] analyzed Lin and Hwang's scheme and noticed that the scheme is vulnerable to insider attack, impersonation attack, known session-specific temporary information attack, stolen verifier attack and many logged-in users' attack. The session key distribution of the Lin and Hwang's scheme is costly due to modular exponentiation that is much more expensive than elliptic curve point multiplication. The key distribution protocol of Lin and Hwang's scheme has a high computational cost. After analysis Islam and Biswas proposed a secure remote login scheme for password authentication and password change, distribution of secured session key using ECC.

Various schemes [5, 6, 8, 10, and 12] have been proposed for user authentication, but most of them have security flaws.

3. Implementation Details

The proposed password authentication scheme is based on ECC and used verifier based approach to prevent offline password guessing attack. The scheme also provides an authenticated secret key distribution between client and server. Islam and Biswas proposed [9] password authentication and update scheme based on elliptic curve cryptosystem which overcome security limitations of Lin and Hwang's scheme.

But Wang et al. [11] explained that ECC based password authentication proposed by Islam and Biswas is vulnerable to Offline password guessing attack. Once the login request message $\{ID_c, E_{B_x}(ID_c \| R_c \| W_c)\}$ in any authentication process is intercepted by attacker A, an offline password guessing attack can be carried as follows [11]:

Firstly Adv guesses the value of PW_c to be PW_c^* from dictionary space D and then computes

$$B^* = PW_c^* \cdot V_s = (B_x^*, B_y^*) \quad \ldots\ldots (1)$$

as V_s is the public key of the server. Adv then decrypts previously intercepted $E_{B_x}(ID_c \| R_c \| W_c)$ using B_x^* to obtain ID_c^*. In the next step Adv verifies correctness of PW_c^* by comparing intercepted ID_c with computed ID_c^*. Adv repeats this procedure of guessing till he/she finds the correct value. After guessing the correct value PW_c Adv can compute valid symmetric key

$$B = PW_c \cdot V_s = (B_x, B_y) \quad \ldots\ldots (2)$$

Proposed system improves existing ECC based password authentication [9]. Table 1 shows notations used throughout the scheme.

Table1: Notations Used in the proposed scheme [9]

ID_i	Identity of the client U_i
PW_i	Secret password of the client U_i
d_s	Secret key of the server S
H(•)	A collision-resistant one-way secure hash function
G	Elliptic curve group base point of order n such that n ·G = O
V_s	Public key of the server S, where $V_s = d_s \cdot G$
+/−	Elliptic curve point addition /subtraction
V_i	Password-verifier of the client I, where $V_i = PW_i \cdot G$
K_x	Secret key computed either using $K = PW_i \cdot U_s = (K_x, K_y)$ or $K = d_s \cdot V_i = (K_x, K_y)$
$E_{K_x}(\bullet)$	Symmetric encryption (AES) with K_x
r_A/r_S	Random numbers chosen by the client/server from [1, n – 1]

The proposed scheme consists of three phases-Registration stage, Password authentication stage, id based key exchange.

3.1 Registration Phase

The server selects a large prime number p and two integer numbers a and b, where $p > 2^{160}$ and $4a^3 + 27b^2 \bmod p \neq 0$. After that the server selects an elliptic curve equation E_p over finite field

$$Fp: y^2 = x^3 + ax + b \bmod p \quad \ldots\ldots\ldots\ldots (3).$$

G is an elliptic curve base point of the prime order n and O is a point at infinity, where $n \cdot G = O$ and $n > 2^{160}$. The server selects the private key d_s and generates the public key $V_s = d_s \cdot G$. The registration phase involves the following steps:

1) U_i gets his user id ID_i and password PW_i, then computes $V_i = PW_i \cdot G$.
2) $U_i \rightarrow S$: $\{ID_i, V_i\}$.
3) Server S receives the registration message from U_i creates an entry (ID_i, V_i, status-bit) in the server database.

3.2 Authentication Phase

The authentication phase of the existing system is modified with the help of a verifier based approach as follows during login:

1) U_i sends ID_i and PW_i into the terminal. The client selects a random number r_i from [1, n −1], calculates $R_i = r_i * V_s$ and W_i

$$= (r_i * PW_i) * G \quad \ldots\ldots\ldots\ldots (4)$$

Then encrypts (ID_i, R_i, W_i) using a symmetric key K_x, where K_x is the x coordinate of K.
The generation of K is modified. The verifier based password authentication [3] can be used for variable K generation as mentioned below to prevent the attack. Verifier is same as computed in existing system. 1. The client chooses a random number a

$$\epsilon Z_q^*, \text{ computes } X_A = a \cdot G + H(V_i) \quad \ldots\ldots (5)$$

Next, the client sends $A \| X_A$ to the server.
2) After receiving $A \| X_A$, the server takes out the client's verifier V, and then computes μ, d, e, k and sends $\mu \| d \| k$ to the client.
3) The client computes $k' = H_1(A, S, X_A, \mu, \sigma, d, k)$ and sends k′ to the server. Next, the client calculates the shared session key $K_A = H_1(A, S, X_A, \mu, \sigma, V)$.
4) After receiving k′, the server checks whether k′ is equal to $H_1(A, S, X_A, \mu, \sigma, d, k)$. If $k' = H_1(A, S, X_A, \mu, \sigma, d, k)$, the server computes the shared session key

$$K = H_1(A, S, X_A, \mu, \sigma, V) \quad \ldots\ldots\ldots\ldots (6)$$

This value of K is then converted into point on elliptic curve. Its x coordinate is used to encrypt

1) $ID_i \| R_i \| W_i$ and send to the server.
2) $U_i \rightarrow S$: $\{ID_i, E_{K_x}(ID_i \| R_i \| W_i)\}$.
3) S calculates the decryption key K_x by computing

$$K = ds * V_i = (K_x, K_y) \quad \ldots\ldots (7)$$

and then $E_{K_x}(ID_i \| R_i \| W_i)$ is decrypted using K_x. Server S compares decrypted ID_i with received ID_i, $e\hat{}(R_i, V_i)$ with $e\hat{}(W_i, V_s)$, respectively. As both conditions are satisfied, S selects random number r_s and calculates

$$W_s = r_s * V_s = r_s * d_s * G \quad \ldots\ldots\ldots (8)$$

4) $S \rightarrow U_i$: $\{W_i + W_s, H(W_s)\}$.
5) U_i extracts W_s by subtracting W_i from $W_i + W_s$. U_i calculates the hash of $(W_i \| W_s)$ and sends it to the server.
6) $U_i \rightarrow S$: $\{H(W_i \| W_s)\}$.
7) The server calculates the hash of its own copies of W_s and W_i and compares that value with the received $H(W_i \| W_s)$, to allow or deny the login appeal. If values are equal, the server grants the user's login request, else rejects the request.

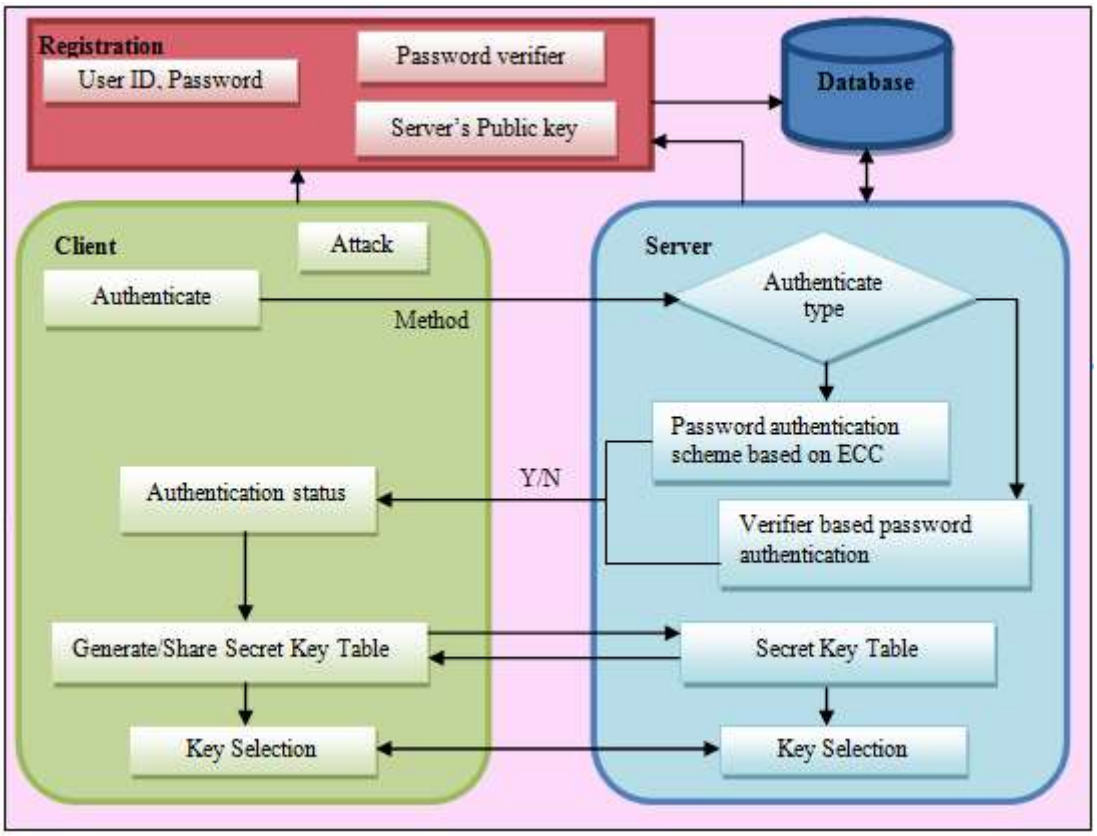

Figure 1: Architecture of Proposed System [13]

This improved approach provides secure mutual authentication between the client and server as well as prevents offline password guessing attack and securely authenticates passwords.

3.3 Key Exchange phase

If the client is authenticated successfully, secret key for secure communication will be shared between client and server as follows:

1. The pool of secret keys is generated using pool management algorithm which is shared between client and server. It is stored on the client and server.
2. The client selects randomly a number from 1 – 100 which points to a key to be used for an initial conversation from the pool (say r_4). The client will choose this random number in such a way that no 'n' consecutive session will repeat same key.
3. The client selects one more random number (say r_1) that points to the secret key used for the secure communication with the server.
4. The client encrypts its unique identifier ID_c along with a random value r1 and sends cipher text along with r_4.
5. Server on the receiving side will get the cipher text along with r_4. Firstly the server will verify whether the r_4 received is not repeated for n sessions. If it is repeated, then it is considered as a request from an attacker. Otherwise the server will first discover the secret key which is used for r_4, and then decrypts the cipher text to get ID_c and r_1.
6. The server encrypts its unique identifier ID_s along with a random number r_1 with a secret key pointed by r_1 and sends it to the client.
7. The client will decrypt the cipher text and retrieve the IDs along with r_1 and then it will verify r1. It will use the authentic secret key for the session.

Thus, the verifier based password authentication will help to prevent offline password guessing attack.

4. Result Analysis

A detailed performance evaluation of the proposed system and existing system is demonstrated in table and bar charts. The arithmetic and cryptographic operations performed on both the client side and the server side are considered for calculating computation cost.

4.1 Number of message exchanges

For achieving network resource efficiency nd minimum latency and setup time, the number of message exchanges between the client and the server should be kept as minimum as possible.

The Existing system requires three-message exchanges and proposed system requires eleven-message exchanges. It is worth having more number of messages exchanged in a proposed system because it prevents password guessing and hence provides security.

4.2 Computation cost

Computation cost is calculated on the basis of number of elliptic curve point multiplications and hash value computations of authentication phase of existing system and proposed system. The proposed protocol includes nine elliptic curve point multiplication operations and eight hash

operations at client and server in the authentication phase. In an efficient and optimized elliptic curve cryptography implementation having minimum computation time and code size requirements, 160 bits elliptic curve point multiplication is less complex than 1024 bits exponential operation. Hence, the computational load of the proposed protocol is lower than the computational load of the existing relevant protocols.

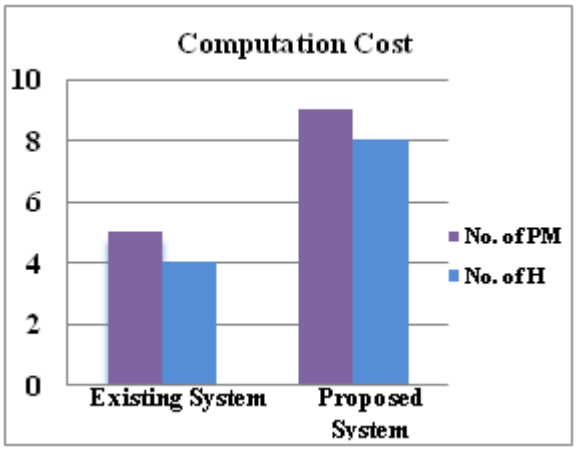

Figure 3: Computation cost comparison
PM: Elliptic curve point multiplication H: Hash calculation

Table 2: Security and Efficiency analysis

Sr. No	Parameter	Existing System	Proposed System
1.	Offline password guessing attack	NP	P
2.	All variables shared between client and server	Yes	No
3.	Server spoofing attack handled	Yes	Yes
4.	ECC used	Yes	Yes
5.	Provision of id based shared secret key	No	Yes
6.	Computation cost	5PM+4H	9PM+8H

NP: Not prevented P: Prevented

From the table2 investigation, we can state that the proposed password authentication scheme provides strong security against offline password guessing attack. The main reasons for this strength are the random numbers selected by client and server is kept secret. Proposed scheme provides id based shared secret key that can be used for secure communication session between client and server.

5. Conclusion and Future Work

Existing password authentication and update scheme based on ECC provides various features and is efficient as well. The scheme is not secure because it is vulnerable to various attacks like offline password guessing attack, stolen verifier attack, denial of service attack. Hence the scheme doesn't fit for practical applications. The proposed password authentication scheme improves the existing scheme by combining verifier based approach with ECC based approach. Hence it can prevent password guessing effectively.

The proposed system uses the performance metrics such as computational cost, number of messages exchanged to judge the efficiency of password authentication. Even though, the existing system is more efficient as compared to proposed system, the effectiveness of proposed system better than that of the existing system.

In future, efficiency can be improved against computational overhead, communication cost and throughput. Other attacks like stolen verifier attack, denial of service attack and failure to preserve user anonymity may be considered for future enhancements.

References

[1] C.L. Lin, T. Hwang, “A password authentication scheme with secure password updating”, Computers and Security 22 (1), pp. 68–72, 2003.
[2] J. J. Hwang, T.C. Yeh, “Improvement on Peyravian Zunic’s password authentication schemes”, IEICE Transactions on Communications E85-B (4) pp. 823–825, 2002.
[3] Junhan YANG, Tianjie CAO, ”A Verifier-based Password-Authenticated Key Exchange Protocol via Elliptic Curves”, Journal of Computational Information Systems 7:2 ,pp. 548-553, 2011.
[4] L. Lamport, “Password authentication with insecure communication”, Communications in the ACM 24 (11), pp. 770–772, 1981.
[5] Li, Xuelei, Fengtong Wen, and Shenjun Cui, “A strong password-based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem for portable devices.” Journal Appl. Math 6.2, pp. 217-222, 2012.
[6] Lo, Jung-Wen, et al., “A secure and efficient ECC-based AKA protocol for wireless mobile communications.” International Journal of Innovative Computing, Information and Control 6.11 , pp. 5249-5258, 2010.
[7] M. Peyravian, N. Zunic, “Methods for protecting password transmission”, Computers and Security conference 19 (5) ,pp. 466–469, 2000.
[8] Ramasamy, Rajaram, and Amutha Prabakar Muniyandi, “An Efficient Password Authentication Scheme for Smart Card.” IJ Network Security 14.3, pp. 180-186, 2012.
[9] S.H. Islam, G.P. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography”, journal of Mathematical and Computer Modeling, Elsevier Science Direct, pp. 1-15, July 2011.
[10] Tang, Hong-Bin, Xin-Song Liu, and Lei Jiang, “A Robust and Efficient Timestamp-based Remote User Authentication Scheme with Smart Card Lost Attack Resistance.” International Journal of Network Security 15.6, pp. 360-368, 2013.
[11] Wang, D., Ma, C. G., Shi, L., & Wang, Y. H, “On the security of an improved password authentication scheme based on ECC”, Information Computing and Applications, Springer, pp. 181-188 , 2012.
[12] Yoon, E., S. Choi, and K. Yoo, "A secure and efficiency ID-based authenticated key agreement scheme based on elliptic curve cryptosystem for mobile devices."

International Journal of Innovative Computing Information Control 8.4, pp. 2637-2653, 2012.

[13] Radhika Bhosale, Prof Manoj L. Bangare, "Prevention scheme for offline password guessing attack based on ECC", Post Graduate Conference for Information Technology (iPGCON 2014), SKNCOE in association with Cyber Times International Journal of Technology and Management, Volume 7, Issue 1, pp. 385-390, 2014.

Author Profile

Mr. Manoj L. Bangare received M.Tech.(Comp.) from the Computer Science Department of COEP, Pune, (2005) and received B.E.(comp.) from government college of engineering Amarvati, (2003) Currently he is doing research from Pune university and he is working as an Assistant Professor in the Department of Information Technology, in STES's Smt. Kashibai Navale College of Engineering, Vadgaon, Pune. His area of interest is Computer security, cloud computing and network security.

Radhika L. Bhosale received B.E. in Computer Engineering from Computer Department of Bharati Vidyapeeth's College of Engineering for Women, from Pune University, Pune. (2009). Currently she is pursuing M.E. In Information Technology from STES's Smt. Kashibai Navale College of Engineering, Vadgaon, Pune. Her area of interest is Network security and data mining.