Security Issues in Password Authentication and Update Scheme based on ECC

Ms. Radhika. L. Bhosale
Department of Information Technology
AISSMS IOIT, Pune, India

Abstract- *The provision of secure remote user authentication system for mobile applications is quite challenging problem. Many password authentication schemes have been published but found susceptible to various attacks. With advances in elliptic curve cryptography, Islam and Biswas proposed a password authentication scheme claimed that their scheme is secure and can resist all related attacks and securely updates user passwords without a problematical process, and also provide explicit session key distribution. Unfortunately, Islam and Biswas's protocol is vulnerable to off-line dictionary attack and denial of service attack, stolen verifier attack. In this paper, we summarize Islam and Biswas's scheme and describe a detailed analysis on the flaws.*

Keywords- Password-authentication, Elliptic Curve Cryptography, cryptanalysis, offline password guessing attack, stolen verifier attack.

I. INTRODUCTION

Security in user's authentication process is an important and challenging task while user's program tries to communicate with server over insecure communication channel. In a password scheme, the password authentication protocol is a procedure to achieve user authentication and the password change protocol is a procedure to allow an authenticated user to change his/her password. To protect the passwords while travelling over public networks, some systems encrypt the passwords with private-key cryptosystems. Password authentication protocols are very subject to password search, replay and stolen verifier attacks.

II. RELATED WORK

Lamport [2] proposed hash based password authentication scheme. The scheme performs mutual authentication between server and client. The user has to identify himself to the server to access remote services. Users can be identified with secret passwords. There are three ways in which attacker can get secret password of users and try impersonation attack:

i. By stealing secret information stored on the system.
ii. By eavesdropping and observing communication link.
iii. By the user's accidental exposure of his password.

Lamport identified hash based solution to tackle first problem. The method used one way hash function for encoding password. The one way function is a mapping M from some set of words into itself such that:
(1) Given a word p, it is easy to compute M (p).
(2) Given a word q, it is not possible to compute a word p such that q= M (p).

In this scheme user's password p is not stored directly in the system but q= M (p) is stored. User identifies himself by sending p to the system and the system authenticates user's identity by computing M (p) and checking that it equals the stored value q.

Though Lamport's scheme is immune to eavesdropping of server's data and impersonation attacks, but susceptible to reply attack.

Mohammad Peyravian and Nevenko Zunic[3] presented a secure method to protect passwords which are transmitted over untrusted networks. Scheme provides secure method for changing an old password to a new password. It does not require the use of additional keys as symmetric keys or public/private keys to protect password interactions. The Peyravian and Zunic's schemes do not use any symmetric-key or public-key cryptosystems. The scheme only employs a collision resistant hash function such as SHA-1.

Lin and Hwang shown that the password update protocol in the Hwang-Yeh scheme [4] 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.

Lin and Hwang [5] proposed an improved scheme to take away above security problems which can achieve mutual authentication and distribution of secret key between the client and the server.

Islam and Biswas[5] analyzed Lin and Hwang's scheme and noticed that the scheme is vulnerable to insider attack, impersonation attack, known session-specific temporary information attack, many logged-in users' attack

and stolen-verifier attack. The session key distribution of the Lin and Hwang's scheme is expensive due to modular exponentiation, which is much more expensive than elliptic curve point multiplication. As a result the key distribution protocol of Lin and Hwang's scheme has high computational cost. After analysis Islam and Biswas proposed a secure remote login scheme for password authentication, password change and distribution of secured session key using ECC.

III. REVIEW OF ISLAM AND BISWAS'S SCHEME

The proposed [6] password authentication and update scheme is based on elliptic curve cryptosystem which provides the omitted security provisions of Lin and Hwang's scheme. Notations used throughout the scheme are as shown in Table 2.

Table 1 Notations used in the Islam and Biswas's scheme [6]

IDA	Identity of the client A
pwA	Secret password of the client A
ds	Secret key of the server S
US	Public key of the server S, where US = dS · G
UA	Password-verifier of the client A, where UA = pwA · G
Kx	Secret key computed either using K = pwA · US = (Kx, Ky) or K = dS · UA = (Kx, Ky)
EKx(•)	Symmetric encryption (AES) with Kx
G	Bases point of the elliptic curve group of order n such that n · G = O, where n is a large prime number
H(•)	A collision-resistant one-way secure hash function
rA/rS	Random numbers chosen by the client/server from [1, n − 1] respectively
+/−	Elliptic curve point addition/subtraction

The proposed scheme consists of four phases—Registration phase, Password authentication phase, Password change phase and Session key distribution phase.

A. 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 Ep over finite field Fp: $y2 = x3 + ax + b \bmod p$. G is a base point of the elliptic curve with a prime order n and O is a point at infinity, where $n \cdot G = O$ and $n > 2^{160}$. Server selects the private key ds and computes the public key Vs =PWi · G. The registration phase involves the following steps:

S1. Ui selects his identity IDi and password PWi, then computes Vi = PWi ·G .

S2. Ui --> S: {IDi, Vi}.

S3. Server S receives the registration message from Ui creates an entry (IDi, Vi, status-bit) in server database

B. Authentication phase

As soon as Ui wants to login to S, the following operations are performed:

S1. Ui keys his identity IDi and the password PWi into the terminal. The client selects a random number ri from [1, n −1], computes Ri = ri *Vs and Wi =(ri * PWi) * G. Then encrypts (IDi, Ri, Wi) using a symmetric key Kx, where Kx is the x coordinate of K = PWi *Vs = (Kx ,Ky) .

S2. Ui → S: {IDi, EKx (IDi || Ri ||Wi) }.

S3. S computes the decryption key Kx by calculating K = ds * Vi = (Kx ,Ky) and then decrypts EKx (IDi || Ri || Wi) using Kx. then S compares decrypted IDi with received IDi, eˆ(Ri ,Vi) with eˆ(Wi ,Vs) , respectively. If both conditions are satisfied, S selects a random number rs and computes Ws = rs*Vs = rs *ds *G .

S4. S→Ui: {Wi +Ws, H (Ws)}.

S5. Ui retrieves Ws by subtracting Wi from Wi +Ws. If the hashed result of retrieved Ws is equal to the received H(Ws) , then Ui performs the hash operation H(Wi ||Ws) and sends it to the server.

S6. Ui→ S: {H (Wi ||Ws)}.

S7. The server S computes the hash value with its own copies of Ws and Wi and compares it with the received H (Wi ||Ws), to accept or denied the login request.

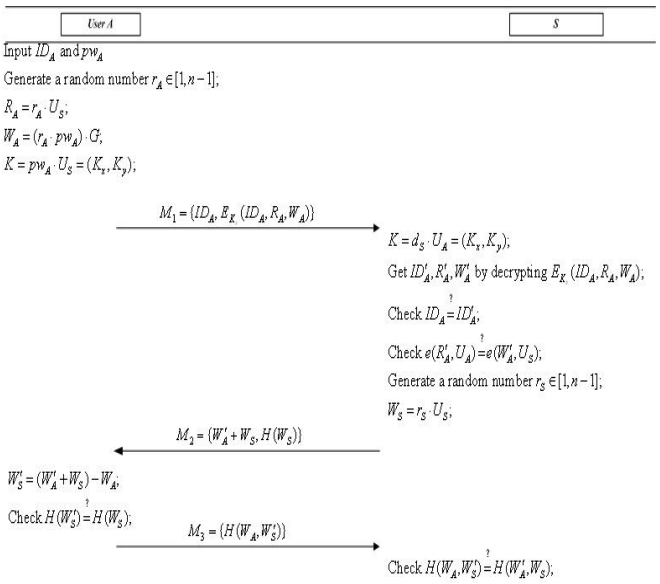

Fig. 1. Password Authentication phase [8]

C. Session Key Distribution Phase and Password Change Phase

As both the session key distribution phase and password change phase have less relevance with this security analysis, so these phases are not considered here.

IV. CRYPTANALYSIS OF ISLAM AND BISWAS SCHEME

Islam-Biswas's scheme looks desirable at first glimpse. They claim that their scheme is secure against various attacks. However Wang et al [7] shown that Islam-Biswas's scheme is secure in specific-attack scenario and without some degree of rigorousness, and thus it is not fully persuasive. Islam-Biswas's scheme still fails to supply its purposes and has security flaws as described below.

A. Offline Password Guessing Attack

A remote user authentication scheme is vulnerable to the offline password guessing attack should satisfy the following two conditions: (i) the password is weak; (2) there exists a password-related information used as a comparison target for password guessing.

A user is allowed to choose his own password at during the registration and password change phases; the user usually tends to select a password, which is easily remembered for his convenience. These weak passwords are potentially vulnerable to offline password guessing attack.

Once the login request message {IDi, EKx (IDi || Ri ||Wi) } during any authentication process is intercepted by adversary A , an offline password guessing attack can be carried as follows:

S1.A Guesses the value of PWi to be PWi* from a dictionary space D.

S2. Then Computes K* = PWi* ·Vs = (Kx*,Ky*) , as Vs is the public key of server S.

S3. Then Decrypts the previous intercepted EKx (IDi ||Ri || Wi) using Kx* to obtain IDi*.

S4. Then Verifies the correctness of PWi* by checking if the computed IDi* is equal to the captured IDi .

S5**.** A Repeats Steps1, 2, 3, and 4 of this procedure until the correct value of PWi is found.

After guessing the correct value of PWi , A can compute the valid symmetric key K = PWi ·Vs = (Kx ,Ky) . After that the attacker can impersonate Ui to send a valid login request message {IDi, {EKx(IDi||Ri||Wi)} to the service server S, since Ui's identity IDi can be intercepted. After receiving the fabricated login request, S will find no anomaly and responds with {Wi +Ws, H (Ws)}. Then A can compute the valid Ws since he knows Wi. Hence the attacker A can successfully pretend as a legal user Ui to server S. The attacker may also impersonate the server S to Ui successfully in a similar way.

B. Stolen Verifier Attack

If the verifier table in the database of the server S is leaked out or stolen by an adversary A . With the obtained entry (IDi, Vi, status-bit) corresponding to Ui, he can guess out the password PWi of Ui using the steps as follows:

S1. A Guesses the value of PWi to be PWi* from a uniformly distributed dictionary.

S2. Computes Vi* = PWi* ·G, as G is public point.

S3. Verifies the correctness of PWi* by checking if the computed Vi* is equal to the somehow obtained Vi.

S4. Repeats Steps1, 2, and 3 of this procedure until the correct value of PWi is found.

As the password dictionary size is very limited, the above attack procedure can be completed in polynomial time.

V. COMPARISON & ANALYSIS

In this section, the security analysis of the different password authentication scheme is given. The comparison of the Islam and Biswas's scheme with other related schemes is as given in table 1 for the performance study.

Table 2: Security Analysis and Performance Analysis

Scheme / Parameter	[1]	[2]	[3]	[4]	[5]
Operations used	Hash	Hash, XOR	Hash, XOR	Hash, XOR, MEXP	Hash, EPM,EAD
Overall computation cost	low	low	high	high	low
Encryption Decryption	Not used	Not used	public	public	Symmetric
ECC is used	No	No	No	No	Yes
Replay attack handled	Yes	Yes	No	yes	yes
Server spoofing attack handled	No	No	Yes	Yes	Yes
Offline password guessing attack handled	No	No	No	No	No

VI. CHALLENGES & FUTURE DIRECTIONS

Ding Wang et al performed cryptanalysis of Islam and Biswas scheme and shown the password authentication scheme is vulnerable to various attacks like offline password guessing attack, stolen verifier attack and denial of service attack as well as fails to preserve user anonymity.

In future we will work on Islam and Biswas scheme to eliminate above mentioned attacks and to make the scheme more efficient. More secure and efficient password authentication and update scheme can be provided using elliptic curve cryptography.

VII. CONCLUSION

Islam and Biswas's 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 is not fit for practical applications. Various smart card based password authentication schemes have been proposed. Issues related to smart card must be considered before the scheme is deployed for security critical applications.

REFERENCES

[1] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, New York, USA, 2004.

[2] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770–772.

[3] M. Peyravian, N. Zunic, Methods for protecting password transmission, Computers and Security 19 (5) (2000) 466–469.

[4] J.J. Hwang, T.C. Yeh, Improvement on Peyravian–Zunic's password authentication schemes, IEICE Transactions on Communications E85-B (4) (2002) 823–825.

[5] C.L. Lin, T. Hwang, A password authentication scheme with secure password updating, Computers and Security 22 (1) (2003) 68–72.

[6] S.H. Islam, G.P. Biswas: Design of improved password authentication and update scheme based on elliptic curve cryptography, Mathematical and Computer Modelling. http://dx.doi.org/10.1016/j.mcm.2011.07.001.

[7] 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,2012, 181-188.

[8] He, D.B.: Comments on a password authentication and update scheme based on elliptic curve cryptography. Cryptology ePrint Archive, Report 2011/411 (2011),http://eprintH.iacr.org/2011/411.pdf.