An Enhanced Opass With Modified Elliptic Curve Cryptography- Based User Authentication Scheme For Grid Computing

M.Victor Jose[1] , V.Seenivasagam[2]

[1]Associate professor, Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India
[2]Professor, Department of CSE, National Engineering College, Kovilpatti, Tamil Nadu, India
Email: mvictorjose@yahoo.com, yespee1094@yahoo.com

ABSTRACT: User authentication to an open server or a system based on username and password is familiar to access the control. Entering the username and password in an untruthful computer is impulse to avert from involuntary exposure through phishing, keyloggers and cross-site password reuse. Since users habitually select weak passwords and reuse the same passwords across diverse websites, trespasser can easily snatch these passwords. Once a trespasser hacks a password of the user, it can be maltreated to gain access to more websites. One time password-oPass protocol can guarantee the blocking of trespassers since it evades long-term password. While oPass make safe passwords, presence of a Cryptography algorithm formulates the password as non–noticeable to intruders. This paper presents a password authentication protocol oPass with modified Elliptic Curve Cryptography algorithm by utilizeing the hash function into account.
[M.Victor Jose, V.Seenivasagam. **An Enhanced Opass With Modified Elliptic Curve Cryptography-Based User Authentication Scheme For Grid Computing.** *Life Sci J* 2013;10(3):1688-1696]. (ISSN:1097-8135). http://www.lifescienceite.com. 254

Keywords: Grid computing, Security, Authentication, Cryptography

I. INTRODUCTION

In individual life, computer security has become a very important role. Among many access control mechanisms, authentication has become a vital problem. Secure networks allow only deliberate recipient to interrupt and read a message addressed to it. Thus security of information is necessary against possible violations that cooperate its confidentiality. The act of confirming the truth of an attribute of a datum or entity is referred to as authentication. To get access to user resources, password authentication is a familiar approach to the system security and it is also a very important practice [Krishna and Chakravarthy 2012].

Usually users log into web sites with usernames and passwords. This is very easy to implement on a server and they allow web sites to easily cooperate with users in different ways. There are lots of problems with these trouble-free approaches, not least of which is that many users will reclaim passwords across different web sites, at which point the cooperation of one web site leads to cooperation of others [Chuan Yue, HainingWang 2009]. For users who might want to memorize diverse passwords, the cognitive trouble makes it unfeasible at scale. In addition, users who face impostor web sites or forms of phishing attacks frequently give up their credentials. It should then come as no surprise that large numbers of users perceive their online accounts accessed by illegitimate parties every day, causing anything from minor annoyances, to financial harm, to very real threats to life and well-being.

Web browsing has become a vital role of life that makes one use browsers to carry out many important tasks such as banking, shopping, and bill-paying. To assist ubiquitous web access, many kiosk environments such as cafes, airport lounges, and hotel business centers afford people with internet connected public computers. These public computers regularly have high-speed network connections [Alexei and Michael 2012]. Since they usually have full-size keyboards and bulky displays, they are also appropriate to employ people who do not hold a computer or take a laptop with them often use these public computers to persue the web.

Since Lamport introduced the first password-based validation scheme in 1981, many passwords based remote user authentication schemes have been projected, where a client remembers a password and the corresponding server holds the password or its verification data that are used to validate the client's knowledge of the password. These passwords which can be easily memerized are called weak passwords, have low entropy and thus are potentially susceptible to a variety of complicated attacks. Particularly offline password guessing attack [Ding Wang and Chun-guang 2012], which is the gravest risk a well intended password authentication scheme, must be able to prevent. A common

characteristic among the published schemes is that computation competence and system safety cannot be achieved at the same time. As the computation capability and battery power of mobile devices (e.g. PDAs, smart cards) are inadequate, the conventional public-key based remote authentication schemes are not appropriate for mobile applications.

A remote password authentication scheme authenticates the authenticity of the remote user over unconfident channel [Eun-Jun and Muhammad 2011]. Key distribution in cryptography has been around and that is the area of research for many years as the key plays a vital role in protection. Once key is compromised, it is not feasible to guard security of IT systems. Generally there are two ways of solving key distribution crisis namely public key cryptography and secret couriers. The public key cryptography relies on mathematically complex keys [Tasleem and Kumaraswamy 2012]. The computational properties which have such public key cryptography are more and occasionally it is inaccessible when long keys are used. The public key cryptography cannot propose unconditional security and its non-polynomial difficulty has not yet been confirmed so far. The other type of key distribution method is known as secret courier which is a known practice since prehistoric times. Quantum key distribution is used to swap secret keys that can grant security to data transmission. The QKD mechanism is unfeasible to break as such because system constantly and arbitrarily generates private keys and shared by parties automatically.

In real life applications, password based confirmation is debatably the most deployed mean of authentication. The reasons for its extensive use is its user friendliness that makes it a gorgeous selection. Users should keep in mind just a password of their choice and store no other complex data similar to long random keys or certificates. Yet, solutions based on passwords have numerous security drawbacks. First of all, users tend to decide easy, memorable passwords. This gives a potential attacker a non negligible probability of guessing the password and impersonates the user [Mario Di Raimond, and Rosario Gennaro 2003].The most trivial type of this attack (frequently attempt to login until the right password is estimated) can be simply ignored, by gentle protocol implementations steps (like end up an account after a particular number of ineffective login attempts). A further hazardous attack is the so called offline lexicon attack in which the authentication protocol reveals sufficient information to allow competent certification of passwords' guesses.

Numerous schemes using timestamp for isolated authentication have already been projected. To access resources at remote structure, users should have appropriate access privileges and each user should have an identity (ID) and a password (PW). In the existing habitual set up the ID and PW are maintained by the remote scheme in an authentication table. If a user wishes to login to a remote server, user has to present, ID and password PW to the server. The remote server receives the login message and checks the legitimacy of the user by refererring to the verification table. Through information of the password, the remote user can employ it to generate an applicable login message to the authentication server. It checks the validity of the login message and provides access right [Rajaram and Amutha 2012].

Password-based user authentication has a main difficulty that humans are not experts in memorizing text strings. Thus, most users would decide simple to remember passwords (i.e., weak passwords) even if they know the passwords might be dangerous. Another critical problem is that users tend to reclaim passwords across diverse websites. Password reuse causes users to lose perceptive information stored in dissimilar websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack. The above attack are caused by the harmful influence of human factors [Hung-Min and Yao-Hsin Chen 2012]. Consequently, one time password is generated based on a long term password which can be used for all websites.

A number of schemes based on elliptic curve cryptography (ECC) has been projected to diminish computation cost while preserving security power. Nevertheless, the actuality of the condition is that this dilemma is only partly addressed and most of the ECC-based schemes were found harshly damaged soon after they were first put forward, so rigorous further research is essential . The primary benefit that elliptic curve systems have over systems based on either integer factorization or the discrete log dilemma in the multiplicative collection of finite field is the nonexistence of a sub exponential time algorithm (such as those of index calculus type) that could find discrete logs in these groups, provided that the curve and the underlying field are properly chosen. Consequently, one can use an elliptic curve group that is lesser in size while maintaining the same level of security. In many situations the outcome is smaller key sizes, bandwidth savings, and faster implementations, features which are particularly attractive for security applications in devices where computational power and integrated circuit space are restricted, such as smart cards and cell phones [Ann Hibner and Neal Koblitz 2008].

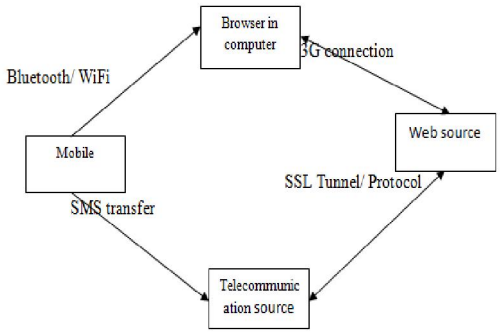

Fig 1: Configuration of proposed Environment

2. oPASS ENVIRONMENT MODEL

This password authentication protocol needs untruthful computer, a web browser, a Telecommunication Source (TS), web source (server) that uses need to contact and user trusted mobile. The user operates the mobile and computer directly. Communication between the mobile and web source through SMS as it is a closed platform and primary service of telecom which belongs to 3GPP standards. Compared with TCP/IP network it increases the difficulty of internal attacks, e.g., tampering and manipulating attacks . Besides the above advantages, this paper slects an SMS channel because of its security advantage.

Users can securely transmit and receive information to the web site through an internet connection. The TS and the web server establish a Secure Sockets Layer (SSL) tunnel for a secure transmission. Through SSL tunnel, the TS can verify the server by its certificate to thwart phishing attacks. TS will participate in the registration and recovery phases. The TS is a bridge between subscribers and web servers. Usually the user connects the mobile with computer browser through secured Bluetooth / WiFi connection. Fig 1 shows the configuration model of the proposed method and Table 1 shows the notations used for designing.

3. PROPOSED PASSWORD AUTHENTICATION PROTOCOL

The one time passwords are created for multiple times based on an effective authenticated session key established protocol, which is based on the elliptic curve cryptography. Correspondingly, smaller parameters can be used in elliptic curve based system than in the discrete logarithm based system, while sustaining the same level of security. In the proposed protocol an elliptic curve E_C defined over $G_L f(pt)$ with a large group G_L of points on the curve of order o_c and a base point (generator) δ_b of large order o_L (the order of a point g on an elliptic curve is the smallest positive integer o_L such that $o_L \delta_b = p_\infty$, where p_∞ is the point at infinity) is assumed. Let the group G_L has a large embedding degree $E_{\deg}$ (a group is said to have an embedding degree $E_{\deg}$ if the group order o_c divides $pt^{E_{\deg}}$ -1, but does not divide $pt^k - 1$ for all $0 < k < E_{\deg}$, it is believed that A and B share the parameters of the elliptic curve E_C and group G_L and the generator δ_b. The proposed method consists of three primary phases termed as registration phase, authentication phase and recovery phase with oPass curve cryptography protocol. Encryption and decryption with elliptical curves will be discussed in section 5.

Table 1. Notations used in the proposed protocol

	User preferred ID
U_{id}	User preferred Web site URL
S_{id}	Long term password
U_{pwd}	Set of One time passwords
O_{pwd}	generated at β time interval
	One time password given as
$(O_{pwd1}, O_{pwd2}, \ldots O_{pwdn})$	random at i^{th} access
	User phone number
U_{Tnum}	Server phone number
S_{Tnum}	Nonce generated by user
U_{nonce}	Nonce generated by server
S_{nonce}	Nonce generated by cell
C_{nonce}	Secret message between cell
Digest	and server
	Symmetric encryption
{}	Hash function with input 'i'
Hash(i)	Generate Message digest from
SHA-256	SHA-256
	Cipher text from ECC
C_m	Corresponding sequence in
$S_{(u,v)}$	ECC
$\oplus$	Bitwise XOR
$\wedge$	
$\vee$	Bitwise AND
$\urcorner$	Bitwise OR
$+$	
R"	Bitwise complement
S"	Mod 232 addition
	Right shift by n bits
	Right rotation by n bits

REGISTRATION PHASE

Before the system begins, the server S selects a large prime number P_L and two integer elements x and y, where $P_L > 2^{160}$ and $x^3 2^2 + \mathrm{mod}\{PN\} 3^3 y^2 \neq 0$. Then S selects an elliptic curve E_C equation over finite field $f(pt): n^2 = y \bmod\{PN\} + xm + m^3$. Let G_L be a base point of the elliptic curve with a prime order O_C and O be a point at infinite, where $O_C G_L = \mathrm{O}$ and $O_C > 2^{160}$. The server chooses the private key S_{PK} and computes the corresponding public key $S_{vi} = U_{pwd} G_L$. The following operations are involved in the registration phase that is shown in Fig 2. Initially the user executes the oPass program installed on the mobile phone to begin or register with a web server. The user wants to enter Uid and Sid only to the registration form. The oPass sends U_{id} and S_{id} to the TS through a 3G connection to permit the web source.

After receiving the U_{id} and the S_{id} from mobile phone, TS can trace the user's phone number $U_{Tnum,}$ based on their network (GSM). The TS and the web source set up a SSL tunnel for secured communication between them. Then the TS forwards U_{id}, U_{Tnum} to the user preferred web server. Server will generate the corresponding information for this account and reply a response, including server's identity S_{id}, a random seed, and server's phone number S_{Tnum}. The TSP then forwards S_{id}, seed and S_{Tnum} to the user's mobile phone. Once reception of the response is finished, the user will continue to setup a long-term password U_{pwd} with the mobile phone. The mobile phone computes verification by the following operation:

$$U_{vi} = U_{pwd} G_L S_{id}, Seed$$

Then a digest is created based on this computed verification as follows:

$$Digest = hash\{U_{vi}\}$$

To prepare a secure registration SMS, the mobile phone encrypts the computed digest with the key and generates the corresponding SHA

$$\text{Mobile phone} \rightarrow \underset{SHA-256}{S} : U_{id}\{digest, seed\} key$$

Then the mobile phones send the encrypted digest to the server. On receiving the registration message from the n[th] user Un, the server S creates an entry for the following in its database.

$$\{U_{vi}, S_{id,} \mathrm{S}_{\mathrm{Tnum}}, Status\_bit\}$$

Where the status-bit denotes the status of the client, i.e., while the client is logged-in to the server the status-bit is fixed to one, or else it is marked as zero.

LOGIN PHASE AND AUTHENTICATION PHASE

Login phase is shown in Fig 3, in this when the n[th] user Un wants to log-in, the succeeding operations will be operated. The login progression begins when the client sends an access request to the server through an untrusted browser (on a kiosk).The client uses the handset to produce one instant password, e.g., $O_{pwd\ i}$, and distribute indispensable in turn encrypted with $O_{pwd\ i}$ to attendant S via SMS significance.

Based on preshared furtive credential process, server S can authenticate user Un based on $O_{pwd\ i}$. Fig 4 shows the feature flows of the login phase. The protocol creates when campaigner U wishes to monitor into the preferred web server S (already registered). Conversely, U begins the login formula by accessing the preferred website via a browser on an untrusted kiosk. The browser launches an instruction S with U's account Uid. Subsequently, server S supplies the Sid and a fresh Nonce S to the browser. The n[th] user U_n keys his identity U_{id} and the password U_{pwd} into the terminal. The client selects a random number n_i from [1,r −1], computes $N_i = n_i . S_{vi}$ and $P_i = \{n_i . U_{pwd}\} . G_L$ .Then encrypts $\{U_{id}, N_i, P_i\}$ using a symmetric key Sx_k, where Sx_k is the x coordinate of $K = U_{pwd} . S_{vi} = \{x_k, y_k\}$. and then decrypts $E_{SX_k} . [U_{id} \| N_i \| P_i]$ using Sx_k . Subsequently S compares decrypted U_{id} with received U_{id} , $\hat{e}[N_i, U_{vi}]$ with $\hat{e}[P_i, S_{vi}]$, respectively. If both conditions are satisfied, S will select a random number Ns and compute $P_s = n_s . S_{vi} = n_s . S_d . G_L$. Provisionally, $P_i + P_s, H(P_s)$ is forwarded to the cell handset through bluetooth or wireless interfaces. User Un retrieves Ps by subtracting Pi from Pi+Ps. If the hashed result of retrieved Ps is equal to the received H(Ps), then Un achieves the hash operation H(Pi||Ps) and sends it to the server the mobile phone inquires associated in progression from its database via Sid, which includes server's phone number ST_{num} and propagate. The next thread is raised with a dialog for its enduring password O_{pwdi} cautious shared documentation digest can be redeveloped by inputting the proper O_{pwdi} on the cell handset. The one-time

password for existing login is recomputed among the following operations:
Digest=hash (Ps||Pi, Sid, seed)
O_{pwd} i=hash N-i(digest)

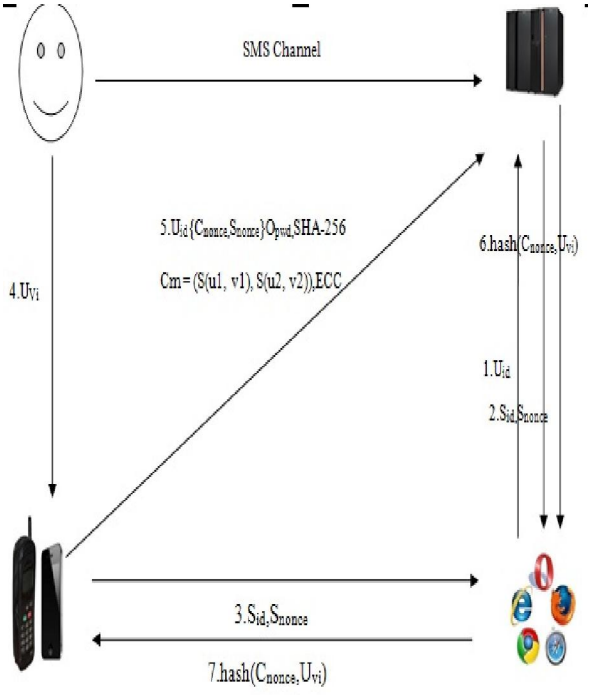

Fig 3 .Login Phase

Fig 4 shows that the main three phases of our proposed method registration, login and recovery process on oPass system. $O_{pwd\ i}$ is solitary pristine for this login (ith login after user registered) and is regard as a secret key with AES-CBC. The cell handset generates a rapid new nonce C_{nonce}. To organize a sheltered login SMS, the cell handset encrypts C_{nonce} and S_{nonce} with and generates the resultant SHA-256. Consequent to receive the login SMS, the server recomputed $O_{pwd\ i}$ (i.e.,) $O_{pwd\ i}$ =hash N-i(digest) to decrypt and validate the dependability of the login SMS. If the expected S_{nonce} equals the formerly generated, the user will be indisputable; unless, the server discards this login appeal. Leading dominant verification, the server sends protract success message through the internet, hash (C_{nonce}, $O_{pwd\ i}$) to the user contrivance. The cell handset will authenticate the expected message to guarantee the achievement of the login method.

RECOVERY PHASE:

Recovery process is chosen for some specific conditions; for example, a user could lose the mobile phone. This protocol is capable of recovering oPass setting on a new mobile phone assuming that user still uses the same phone number (apply a new SIM card with old phone number). When user U installs the oPass program on the new mobile phone, the program can be started to send a recovery request with the account Uid and appeal server Sid to predefine TS over a 3G connection. Such as mentioned before, Sid can be the domain name or URL link of server.

Similar to registration, TSP can trace the phone number UT_{num} formed on the SIM card and forward the account U_{id} and UT_{num} to server across the SSL tunnel. Once server S gets the request, S will observe the account information in its database to approve if account is entered or not. If account U_{id} develops, the information apply to work out the secret credential will be taken out and be sent back to the user. The server generates a fresh nonce S_{nonce} and answers a message which consists of U_{id}, seed, S_{nonce} and ST_{num}. This message includes all necessary elements for creating the next one-time passwords to the user.

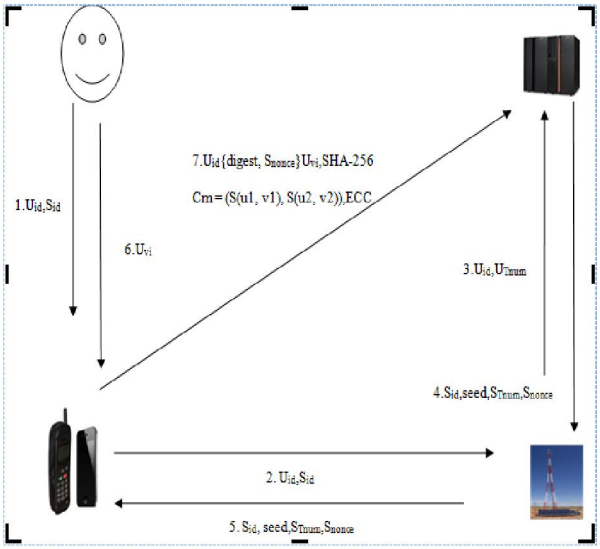

Fig 2: Registration Phase

After the mobile program obtains the message, similar to registration, it powers the user to enter the long-term password to replace the correct one-time password $O_{pwdi+}1$. Throughout the last step, the user's mobile phone transfers the secret credential and server nonce to a cipher text. The recovery SMS message is transported back to the server for testing. Similarly, the server calculates and $O_{pwdi+}1$ decrypts this message to verify that user is already improved. At this point, the new mobile phone is enhanced and ready to achieve further logins. For the later login, one-time password $O_{pwdi+}2$ will be controlled for user authentication. Fig 5 displays the detaiied flows of recovery phase.

4. ELLIPTIC CURVE CRYTOGRAPHY WITH HASH FUNCTION

Encryption is a mechanism through which a message is malformed so that only the sender and recipient can scrutinize. For illustration, suppose to facilitate, user1 wants to send a concealed message to user2. To perform this, user1 first desires user2's public- key. The public key is made public and is distributed widely and freely. User2 can send it over the network. Formerly user1 has user2's public-key; the message has encrypted using user2's public-key and sends it to user2. User2 receives user1's message and decrypts message using its private-key.

ELLIPTIC CURVES OVER FINITE FIELDS

Elliptic curve cryptography encrypts the plain text through points presented in the curves using the following formula.

$v^2=u^3+au+b$

Mod P is $0 < u < p$. Let $p>3$ be an odd prime. An elliptic curve E over F_b is defined by an equation of the form. The constants ' a 'as well as ' b 'are non negative integers lesser than the prime number, P and have to suit the condition

$4a^3+27b^2 \neq 0 \bmod p$

For each value of x, one needs to determine wether it is a quadratic residue or not. If it is the case then there are two values in the elliptical group. If not, then the point is not in the elliptical group, where a, b ε F_b and $4a^3+27b^2 \neq 0 \bmod p$. The set E ($F_b$) consists of all points (u, v), $u \varepsilon F_b$ and $v \varepsilon F_b$ which satisfy the defining equation, together with a special point O called the point at infinity. The two basic point operations are needed for encryption and decryption 1. Point Addition, 2. Point Doubling.

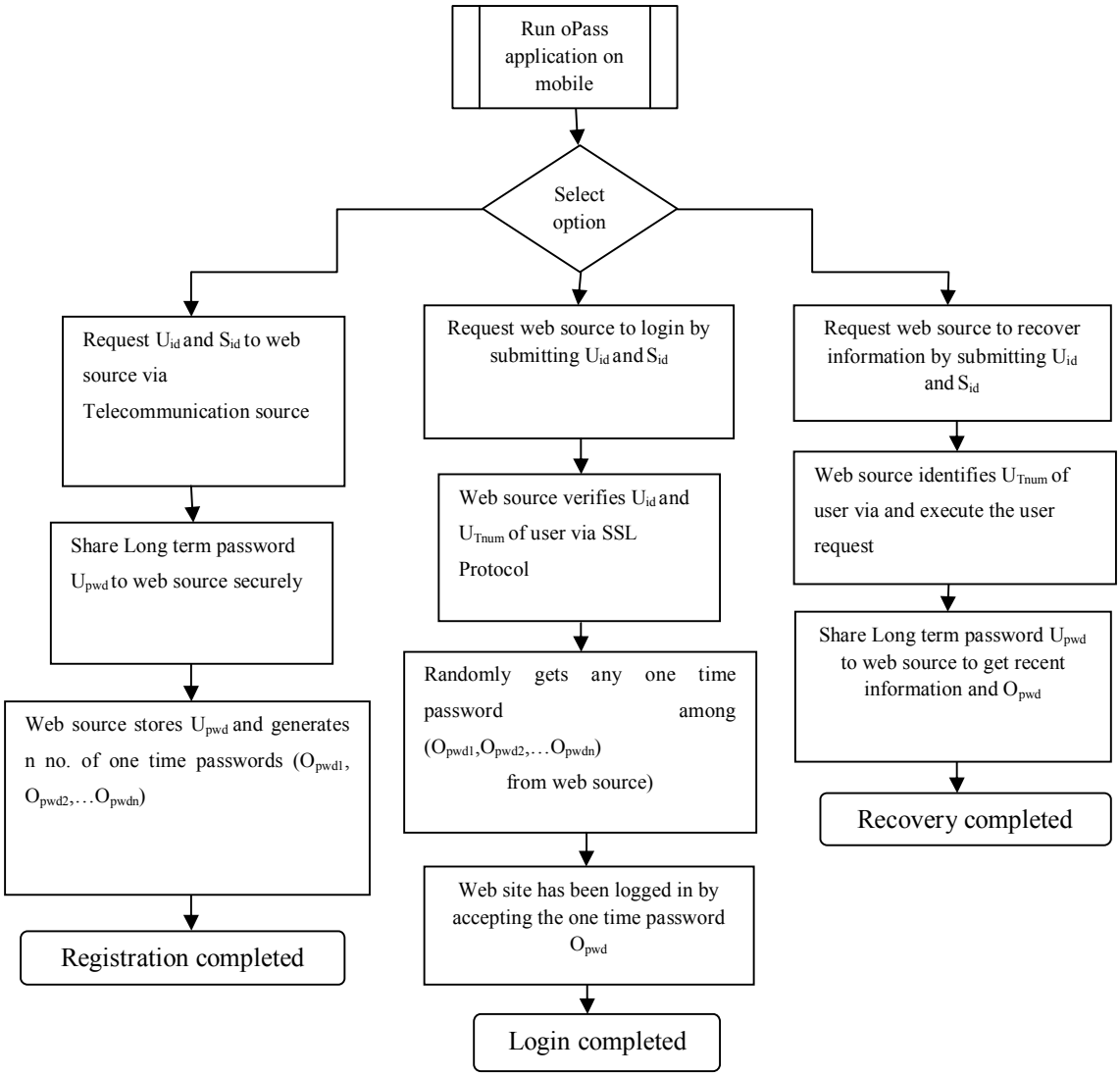

Fig 4. Proposed method flow Diagram

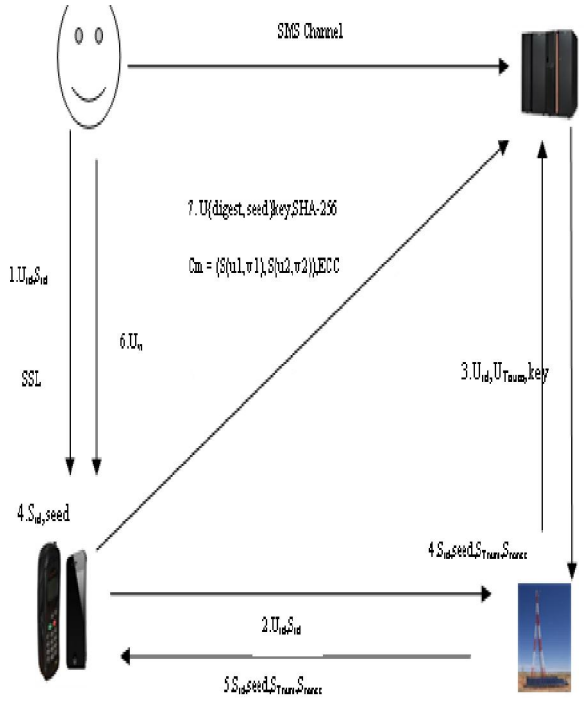

Fig 5: Recovery Phase

POINT ADDITION

Adding two points with different *x*-coordinates: Let $(u1, v1) \varepsilon E(F2m)$ and $(u2,v2) \varepsilon E(F2m)$ be two points such that $u1 \neq u2$. Then $(u1, v1) + (u2, v2) = (u3,v3)$, where:

Let $(u_1, v_1) \in E(F_m)$ and $(u_2, v_2) \in E(F_m)$ be two points such that $u_1 \neq u_2$ .then

$(u_1, v_1) + (u_2, v_2) = (u_3, v_3)$, where

$$u_3 \equiv \lambda^2 - u_1 - u_2 (\text{mod } p)$$

,

$$v_3 \equiv \lambda(u_1 - u_3) - v_1 (\text{mod } p)$$

And $$\lambda \equiv \frac{v_2 - v_1}{u_2 - u_1} (\text{mod } p)$$

ENCRYPTION ALGORITHM

Generate message digest from SHA-256 cryptographic hash function.

1. Pad the message in the normal way: Assume the length of the message M, in bits, is l. Attach the bit "1" to the end of the message, and then k zero bits, where k is the smallest non-negative solution to the equation l+1+k = 448 mod 512. To this affix the 64-bit block which is equal to the number l record in binary.
2. Parse the message into N 512-bit blocks $M^{(1)}$, $M^{(2)}$……, $M^{(N)}$.
3. Initially assign the hash values to the registers h_0, h_1, h_2, h_3.then update the register using the logical functions.
   Ch (u, v, z) = (u ^ v) ⊕ (¬u ^ z)
   Maj (u, v, z) = (u ^ v) ⊕(u ^ z) ⊕ (v ^ z)
   $\omega_0(u) = S^2(u) \oplus S^{13}(u) \oplus S^{22}(u)$
   $\omega_1(u) = S^6(u) \oplus S^{11}(u) \oplus S^{25}(u)$
   $\mu_0(u) = S^7(u) \oplus S^{18}(u) \oplus R^3(u)$
   $\mu_1(u) = S^{17}(u) \oplus S^{19}(u) \oplus R^{10}(u)$
4. Adding the initialized hash value with updated register value and concatenates the each hash value which is called message digest.
5. The message digest is encrypted by ECC. Initially, receiver picks a random integer a, and proclaims the point CR (while C remains secret).
6. Sender selects their own random integer l and calculate the pair of points:
   R1 (u1, v1) = lR
   R2 (u2, v2) = Ri + l(CR)
7. Calculate S (u1, v1) and S (u2, v2) with S is a corresponding sequence.

Then, the cipher text is as following:

Cm = (S (u1, v1), S (u2, v2))

8. Sender converts Cm to binary form with: 0 → 00, 1 → 01, 2 → 10 and send to receiver a series of bits.

DECRYPTION ALGORITHM

1. Converts a binary form to series of digits as well as: 00 → 0, 01 → 1, 10 → 2
2. Transforms C_m into groups of 2m.
3. Haul out a group of m digits in sequence of step2.
4. Circularly shifting this order of m digits by one element to the left
5. Exchange an order to decimal form, and store a value in k
   For example: 0100 will in the form: $0 *3^3 + 1 *3^2 + 0 * 3^1 + 0 *3^0 = 9$, so k=9
6. Acquire (k+1) P from pre-computed and stored point (k+1) R=(x1, y1).
7. The approach is repeated for the next element of the sequence of step 3 for the recovery of S (u2, v2).
8. The procedure is frequent for the next groups of step 2, which is not visited former. Recall that lR is represented by (u1,v1) and Ri + l(CR) is represented by S(u2, v2) In order to pull out Pi from Ri +l(CR), user applies his secret key a and calculates C(lR) from the first part of the pair, then subtracts it from the second part to obtain:

Ri + l(CR) - C(lR) = Ri + lCR - lCR = Ri,

and then reverses the embedding to get back the message.

5. RESULTS AND DISCUSSION

IMPLEMENTATION MODEL

This paper has implemented the protocol of oPass with curve cryptography based on its three phases namely registration, login and recovery. The function of our protocol depends on three components: a mobile program running on Android Smartphones (Android OS v2. 1); a web browser and a web source or web server. The communication interface between the phone and the browser extension is based on a client/server model over the TCP/IP network. Mobile phones utilize their WiFi or 3G to connect the TCP server built by the extension. Other mediums, such as Bluetooth and cable line, can substitute for current communication interface. The efficiency comparison of the proposed protocol and the existing protocols are done with the computation cost of pre-computation phase(E1), execution phase for a client(E2), execution phase for a server(E3), number of messages exchanged(E4), execution phase(E5) are shown in Table 2. In this table following abbrivations are also used.

Exp: exponential operation,

Emul: elliptic curve multiplication operation,

Hash: hashing operation,

Sym: symmetric encryption or decryption.

The comparison of the proposed oPass with ECC protocol and the existing oPass protocol are shown in Table 3 .

The Performance comparison of various previous research scheme with proposed scheme are represented in Table 4.

Table 2. Efficiency comparison of the proposed protocol and the existing protocols

Proto col	**E1**	**E2**	**E3**	**E4**	**E5 in** bits
PP-TAKE	2Exp	5Hash+1 Sym	4Hash+1Sym + 1Exp	4	1664
Juang et al.	2 Exp	5Hash+1 Sym	Not specified	3	1696
Lee et al.	2 Exp	5Hash+1 Sym	4Hash+1Sym+1Exp	2	1856
ECC proto col	2Emul	5Hash+1 Sym	4Hash+1Sym+1Emul	3	960
Pro posed	1Emul	2Sash+1Emul			

Table 3. Comparison of the proposed oPass with ECC protocol and the existing oPass protocol

oPass	**oPass with ECC**
Suffers from computation cost	Reduced Computation cost
Ensures security for long term password	Provides additional security strength
Requires more running time	Reduced running time, which mainly depends on the smallest prime factor size
Suffers from sms overhead of about 41 %	Sms overhead is reduced to 31%

Table 4: Comparing oPass with previous research

Protocols	**Attack Prevention**		
	Phishing	**Key logger**	**Password Reuse**
Proposed	✓	✓	✓
MP-Auth	✓	✓	
Chuan Yue et al. [2]	✓	✓	
Tasleem et al. [6]	✓	✓	
Eun-Jun Yoon et al. [4]		✓	
Nivedita et al. [9]		✓	
Zi-Yao Cheng et al. [10]		✓	

6. CONCLUSION

In this paper, a modified Elliptic Curve Cryptography algorithm is proposed for user password protection against password stealing and reuses attacks. Initially our research environment was assumed as an untrusted kiosk with 3G connections with web server and secured bluetooth or WiFi connection with user mobile phone; telecommunication source with SSL tunnel has employed as bridge for mobile and web server. The adoption attitude of oPass on mobile phones was to eliminate intruders or hackers as much as possible. By utilizing this, user only needs to consider a long-term password in all the scenarios presented here. Based on the long-term password our protocol generates the one time passwords for every access which is transferred through curve points. To make our protocol more efficient, password recovery phase was also discussed in the case of user lost the mobile phone. Experimental result shows that the proposed protocol with the utilization of elliptic curves is more efficient than the existing methods.

REFERENCES

[1] P.E.S.N. Krishna Prasasd, A.S.N. Chakravarthy, B. D. C. N. Prasad," Performance Evaluation of Password Authentication using Associative Neural Memory Models", International Journal of Advanced Information Technology (IJAIT) Vol. 2, No.1, February 2012.

[2] Chuan Yue, HainingWang," Session Magnifier: A Simple Approach to Secure and Convenient Kiosk Browsing", ACM, 2009.

[3] Alexei Czeskis, Michael Dietz, Tadayoshi Kohno, Dan Wallach, Dirk Balfanz," Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions", ACM, October 16–18, 2012.

[4] Eun-Jun Yoon, Muhammad Khurram Khan, Kee-Young Yoo," New Robust Protocols For Remote User Authentication And Password", International Journal of Innovative Computing, Information and Control (ICIC International), Vol. 7, Number 9, September 2011.

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

[6] Tasleem, P. Kumaraswamy, Dr.C.V. Guru Rao, "Hybrid Approach: Combining Classical Cryptography and QKD for Password Authentication", International Journal of Computer Science & Communication Networks, Vol 2(4), 512-515, September 2012.

[7] Mario Di Raimond, Rosario Gennaro,"Provably Secure Threshold Password-Authenticated Key Exchange", IBM T.J.Watson Research Center, July 25, 2003.

[8] Rajaram Ramasamy, Amutha Prabakar Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", International Journal of Network Security, Vol.14, No.3, PP. 180-186, May 2012.

[9] Nivedita Datta,"Zero Knowledge Password Authentication Protocol", International Journal of Communication Network Security ISSN: 2231 – 1882, Vol.1, Issue-4, 2012 .

[10] Zi-Yao Cheng, Yun Liu, Chin-Chen Chang, Shih-Chang Chang, "An Improved Protocol for Password Authentication Using Smart Cards", 2011.

[11] Hung-Min Sun, Yao-Hsin Chen, Yue-Hsun Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", IEEE Transactions On Information Forensics And Security, Vol 7, No. 2, April 2012 .

[12] Ann Hibner Koblitz, Neal Koblitz, Alfred Menezes, "Elliptic Curve Cryptography:The Serpentine Course Of A ParadigmShift", 2008.

[13] K R Chandrasekhara Pillai, 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), Vol.2, No.3, July 2010.

8/30/2013