Design of a Time and Location Based One-Time Password Authentication Scheme

Wen-Bin Hsieh
Department of Electronic Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan
d9802106@mail.ntust.edu.tw

Jenq-Shiou Leu
Department of Electronic Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan
jsleu@mail.ntust.edu.tw

***Abstract*—As the mobile networks are springing up, mobile devices become a must gadget in our daily life. People can easily access Internet application services anytime and anywhere via the hand-carried mobile devices. Most of modern mobile devices are equipped with a GPS module, which can help get the real-time location of the mobile device. In this paper, we propose a novel authentication scheme which exploits volatile passwords − One-Time Passwords (OTPs) based on the time and location information of the mobile device to transparently and securely authenticate users while accessing Internet services, such as online banking services and e-commerce transactions. Compared to a permanent password base scheme, an OTP based one can prevent users from being eavesdropped. In addition to a memoryless feature, the scheme restricts the validness of the OTP password not only in a certain time period but also in a tolerant geometric region to increase the security protection. However, if a legitimate user is not in the anticipated tolerant region, the user may fail to be authenticated. Hence, a Short Message Service (SMS) based mutual authentication mechanism is also proposed in the article to supplement the unexpected misjudgement. The proposed method with a volatile time/location-based password features more secure and more convenient for user authentication.**

Keywords—GPS; One-Time Passwords; Volatile Authentication; Time and Location Based Authentication; Mutual Authentication;

I. INTRODUCTION

Thanks to the development of the mobile technologies, people can access Internet services ubiquitously by the hand-carried mobile devices. Currently, most of modern mobile devices are equipped with a GPS module providing real-time location information. The location prediction technique has made progress with the assistance of the mature GPS technology. A precise location predication can facilitate the geo-encryption or geo-authentication to enhance the security protection. These advantages have been successfully applied to the security control in an ad hoc network environment. On the other hand, the One Time Password (OTP) scheme has been applied to some crucial services, such as online banking services and e-commerce transactions. Such a mechanism of a volatile password can lessen the risk of password being stolen by some malicious users. In this paper, we propose a solution that utilizes a time and location dependent OTP which can prevent permanent passwords from being sniffed for authentication while accessing the Internet application services in a mobile environment. The proposed solution improves the user convenience and authentication security greatly. This scheme can transparently authenticate users in a tolerant geometric region as well so that users do not need to manually type in their passwords. Meanwhile, such a location assisted authentication can reinforce the time-dependent only OTP scheme since the hackers are not easy to get exact time and location information about the users simultaneously. Besides, a Short Message Service (SMS) based mutual authentication mechanism is also proposed to deal with the unexpected misjudgement in case a legal user fails to be authenticated if he or she runs out of the tolerant region.

The rest of this paper is organized as follows. In section II, we briefly introduce the related works about geo-encryption, location prediction, location-based authentication and OTP. Our proposed scheme is depicted in section III. In section IV, we illustrate the analytical characteristics of the proposed scheme. Section V gives a conclusive summary about this paper.

II. RELATED WORK

As the technology of GPS grows mature, many location-based encryption schemes have been proposed recently. D. E. Denning's "Geo-

encryption" [1] takes advantage of GPS technology to conduct GPS-based encryption that integrates the location and time into the process. The decryption is processed in a limited area as well as time. Hsien-Chou Liao's location-dependent data encryption algorithm (LDEA) [2] incorporates a latitude/longitude coordinate with a random key to encrypt data. The encrypted message can only be decrypted when the receiver is in the region centered by the target coordinate within a Toleration Distance (TD).

About the location prediction, an algorithm in [3] based on mobility characteristic can effectively predict the future location of a mobile node in an ad hoc network where nodes use directional antennas to communicate with each other. In [4], Son, Helmy and Krishnamachari identify two problems about location errors, the lost link (LLNK) problem and the loop in packet delivery (LOOP) problem. And then they propose two mobility prediction schemes to mitigate these problems. Neighbor Location Prediction (NLP) can solve LLNK and Destination Location Prediction (DLP) can solve the LOOP respectively.

In the study about the location-based authentication, Jarusombat and Kittitornkun in [5] propose a Geo-encryption scheme to generate Digital Signature. In this model, a sign server is used to assist the mobile device in creating a digital signature and receive mobility parameters from mobile devices. It provides authentication, data integrity and non-repudiation services. In [6], the author identifies two aspects — location-based key distribution and run-time location verification — to improve the network access control and proposes Location-Enforced Network Access (LENA) which eliminates the dependence on expensive hardware devices in order to locate the mobile devices. In [7], authors propose a comprehensive definition of location authentication, a review of its threats and possible solutions to help provide a better understanding of this young security requirement.

[8], [9], [10] and [11] are related to the study about OTP. For example, [8] proposes an authentication mechanism integrated with a challenge/response process and an OTP. Many OTP related products, such as [12] and [13], already exist in the market.

III. The Proposed Scheme

Time and location based OTP (abbreviated as TLB OTP) utilizes two physical features to generate an OTP that can reflect the user-related information. With this protocol, server uses login time to calculate the location where user should be. Then it uses these related information as parameters to proceed the authentication. The follows are the detailed explanation.

In our proposed scheme, we assume that the legitimate users have already registered on the application server and all of them are organized under a Public Key Infrastructure (PKI) system [14]. We also assume that the application server and the mobile devices in the network have their clock synchronized.

3.1 Phase A: Time and Location Based OTP Authentication

In Table I, we define notations used in Phase A.

TABLE I. Notations for Phase A.

Notation	Description
PKEY	Public Key
SKEY	Secret Key
IMSI	International mobile Subscriber Identity
L	Location
T	Time
V	Velocity
‖	Concatenation

Step 1: When the mobile device initiates, it sends its IMSI, current time T0 and location L to the server. The application server would record the location L (X0, Y0) and the time T0 in the database as Fig. 1 shows.

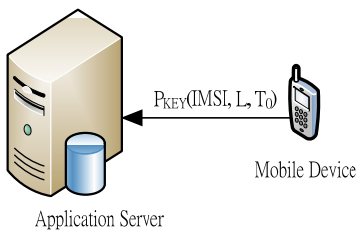

Figure 1. Mobile devise sends its IMSI, location L (X0, Y0) and time T0 encrypted by public key to the server.

Step 2: After a period of time, the mobile device sends its new location L1 (X1, Y1) and new current time T1 to the application server. And the application

server then records the location L1 (X1, Y1) and time T1. (Step 1 and Step 2 can easily be executed at any two consequent time points when the mobile device is moving.)

Step 3: The server subsequently calculates the velocity of the mobile device by the following formula (1).

$$V = \sqrt{\left(\frac{X_1 - X_0}{T_1 - T_0}\right)^2 + \left(\frac{Y_1 - Y_0}{T_1 - T_0}\right)^2} \qquad (1)$$

Step 4: By referring to the statistics in [1], we can predict that the future moving direction and location of the mobile device would be probably is shown in Fig. 2.

Angle(°)	0-30	30-60	60-90	90-120	120-150	150-180
Distribution(%)	93.0	3.9	1.73	0.43	0.43	0.43

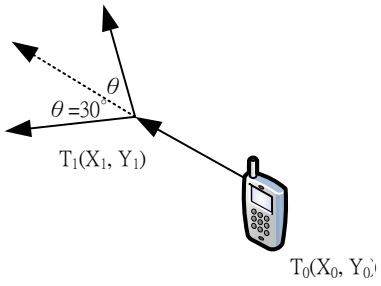

Figure 2. The future moving direction and location of the mobile device

Step 5: From step 3 and 4, we can get the distance d by (2).

$$d = V_t \times \triangle T \qquad (2)$$

Based on the algorithm in [1], we make a line passing through the two locations L (X0, Y0) and L1 (X1, Y1). The formula of this line is y = ax + b. We can calculate a and b by the equation (3).

$$\begin{cases} a = \dfrac{Y_1 - Y_0}{X_1 - X_0} \\ b = \dfrac{X_1 Y_0 - X_0 Y_1}{X_1 - X_0} \end{cases}, X_1 \neq X_0 \qquad (3)$$

Then we make an equilateral triangle with one point at (X1, Y1) and its center on line ι as Fig. 3 shows. The edge length of this equilateral triangle is d. The coordinate (X, Y) of the equilateral triangle's center is calculated by (4).

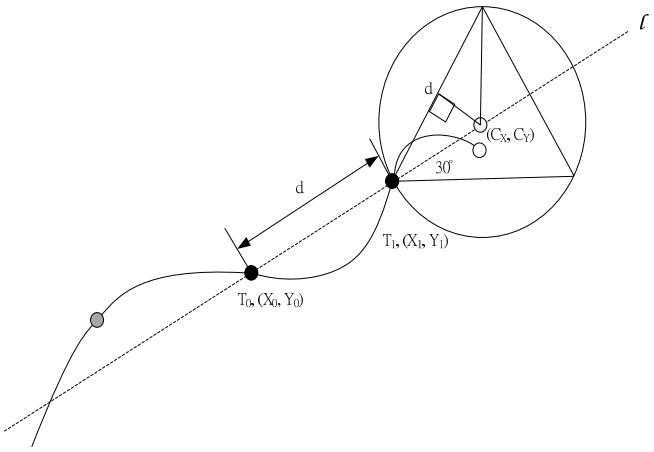

Figure 3. An equilateral triangle with one point at (X1, Y1) and its center on line ι: Y = aX+ b. The radius of the circle is $\sqrt{3}d/3$.

$$\begin{cases} C_X = X_1 + \dfrac{\sqrt{3}d}{3}\dfrac{X_1 - X_0}{|X_1 - X_0|}\cos\left(\arctan\left(|a|\right)\right), \\ C_Y = Y_1 + \dfrac{\sqrt{3}d}{6}\dfrac{Y_1 - Y_0}{|Y_1 - Y_0|}\sin\left(\arctan\left(a\right)\right), \end{cases} \qquad (4)$$
$$X_1 \neq X_0, Y_1 \neq Y_0$$

Finally, we draw a circle containing the equilateral triangle with the smallest radius and the same center (CX, CY). The radius of the circle is shown as (5).

$$r = \frac{\sqrt{3}}{3}d \qquad (5)$$

Then we get the tolerant range of the predicted future location as (6).

$$((X, Y) \mid (X - C_X)^2 + (Y - C_Y)^2) \leq r^2 \qquad (6)$$

Step 6: When a user wants to login the server, the location gotten from the GPS receiver and the current time t would be used to generate an OTP.

Step 7: The concatenation of the IMSI and the OTP would beencrypted by the public key and then sent to the server as Fig. 4 shows.

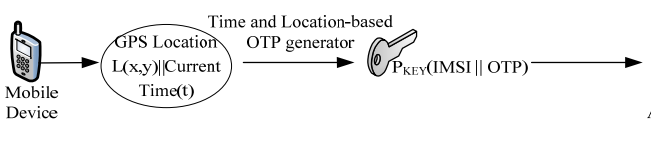

Figure 4. Mobile device sends the authentication message within IMSI, time (t), and Location-based OTP encrypted by a public key.

Step 8: When the server receives the encrypted message, it would decrypt it with a secret key. Then the server extracts the OTP from the message and subsequently retrieves the coordinate L (x, y) and the time t from the OTP by using the inverse function f() of the OTP generator. The procedure of decryption is shown in Figure 5.

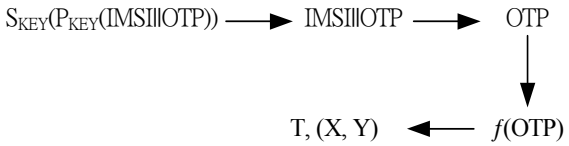

Figure 5. The procedure of decryption at the application server

Step 9: The server checks if the coordinate (X, Y) is in the tolerant distance of the expected destination. If it is, the user would pass the authentication. If not, the login request would be rejected.

3.2 Phase B: Supplementary SMS-based mutual authentication

In case the coordination of the mobile device is out of the tolerant range or the first method fails to work, a user still needs a supplementary method to login to the server. Hence, we propose a backup solution - SMS-based mutual authentication by referring to [14], [15] and [16]. A general method is to insert a smart card into a user's mobile device to generate the OTP.

We define the notations used in Table II for Phase B.

Table II—Notations for Phase B

Notation	Description
h( )	secure one-way hash function
A	account
PW	password
$\oplus$	exclusive-or operation
g	a primitive element in $GF(p)$
p	a large prime number
b	a random number in the smart card
R	h(IMSI) $\oplus$ h(b$\oplus$PW)

The authentication system selects two large prime numbers p and q, such that q divides p–1. A primitive element g with order q in the Galois field GF(p)[14], where GF(p) is the set of integers {0, 1,…, p-1} with arithmetic operations defined modulo p. We assume that the user has registered on the server prior to asking to login the server. Hence, the user already has an account A, a password PW, and a smart card.

When the user wants to login to the server, he inserts the card into its mobile device first and inputs A, PW and a large random integer x less than p-1. Then the following sub-phases for mutual authentication are executed.

3.2.1. Preparing the authentication message at the mobile device

Step. 1 Calculate $C = g^x \oplus R \oplus h(b \oplus PW)$.

Step. 2 Acquire current time stamp Tu.

Step. 3 The device sends the message (Tu , A, C) via a SMS to the server.

3.2.2. Checking the authentication request and generating an OTP at the server

Step 1. Check if Tu has already been used, the server rejects the user's request and terminates the authentication. Otherwise, the authentication process continues.

Step 2. The server uses A to query its authentication database and find the corresponding IMSI.

Step 3. The server gets g^x by computing $g^x = C \oplus h(IMSI)$ and acquires the current time Ts.

Step 4. The server selects a large random integer y less than p-1 to get $g^y \pmod p$.

After all parameters are gotten, the server would calculate $g^{xy} \pmod p = (g^x)^y = (g^y)^x = g^{xy}$.

Step 5. The server generates $C' = g^y \oplus h(IMSI)$ and $C'' = g^{xy} \oplus OTP$.

Step 6. The server sends the message (Ts, Tu, ,C' , C'') to the mobile device via a SMS.

3.2.3. Authenticating the server and replying back from the mobile device

Step 1. Check if the received Tu is equal to the stored Tu. If not, the mobile responses a failure message to the server.

Step 2. Compute $g^y = C' \oplus h(IMSI)$ and derive $g^{xy} \pmod p$.

Next, the mobile device retrieves the OTP by computing $OTP = C'' \oplus g^{xy}$.

Step 3. The mobile device computes $C''' = OTP \oplus g^y$ and sends the message (Ts, Tu, C''') back to the server.

3.2.4. Checking the replied message from the mobile device at the server

Step 1. Retrieve OTP by computing OTP = $C''' \oplus g^{y}$.

Step 2. Check if the received Ts and OTP are equal to the stored Ts and OTP. If not, the server rejects the user's login request. Otherwise, the user is permitted to login.

IV. Analytical Characteristics of the Proposed Scheme

4.1 The advantages and security improvement of our proposed scheme

In this sub-section, we discuss the advantages and security improvement of our proposed scheme.

4.1.1 An OTP based mechanism is not easy to be fabricated since the generated passwords are volatile. Therefore, the malicious hacker is hard to guess the one-time-used passwords.

4.1.2 The proposed scheme can provide a not only time-dependent but also location-dependent OTP that is volatile and not reusable. That means even if an attacker intercepts the message it is hard to disguise a legitimate user's location in terms of time and location factors.

4.1.3 If a user moves steadily, the user does not need to input his account and password. It is convenient for a user to transparently login the server without an explicit manipulation, such as manually typing in the username and password.

4.1.4 To enhance the precision of the location prediction, our scheme is developed based on the statistics of the recently movement and moving direction of the mobile device.

Even though the supplementary authentication scheme which is based on [14], [15] and [16] is believed infeasible to execute in polynomial time, the backup solution with a mutual authentication provides a high security protection in case the GPS malfunctions or an unexpected behavior of the user happens.

4.2 A brief comparison between the proposed scheme and the traditional one

In this sub-section, we make a brief comparison between the traditional scheme and our proposed one as the Table III shows.

Table III Comparison between the traditional scheme and our proposed one

	Traditional Authentication Scheme	**Our Time/Location based OTP**
Inputting Account and Password	Required	Unnecessary
User Behavior Dependent	No	Yes
Password Life Time	Permanent	Volatile
Vulnerability for being Attacked	High	Low

First, a traditional authentication scheme normally requires a user to input the account and password for authentication. Our proposed scheme would authenticate a user by referring to the location information of a mobile device within a certain life time. Second, the traditional authentication system cannot identify a malicious user who tries to login by a pair of stolen account and password. However, we may recognize a user based on the user behavior like the past movement information. Third, a permanent or rarely-changed password in the traditional authentication scheme is vulnerable to be attacked whereas our time/location dependent OTP can effectively prevent the password from being stolen.

4.3 Analysis from the viewpoint of different OTP mechanisms Typical OTP mechanisms are classified into the following types [17]:

4.3.1 Time based mechanism: one generated OTP stays valid for a certain period of time.

4.3.2 Event based mechanism: the generated OTP stays valid only when the met condition satisfies.

4.3.3 Time and Event driven mechanism: combines the advantages of the above.

Our proposal belongs to the 3rd one. The event condition is the future tolerant region of the user. It is harder for an attacker to mimic the velocity and the moving direction of the user so that it is hard to counterfeit the OTP.

Table IV shows a comparison of our proposed protocol with other existing security protocols on the basis of their security properties. Our protocol's security features are mentioned in the final column.

Table IV Security Properties – Comparison

Protocol	KERBEROS	S/KEY OTP	Our Protocol
Replay Attack	√	√	√
Eavesdropping attack	⌂	√	√
Dictionary attack	×	√	√
Brute Force Attack	×	⌂	√
Man-in-the-middle attack	×	×	√
User Impersonation attack	⌂	√	√

Notation: √ Satisfied ⌂ Partially Satisfied × Not Satisfied

V. Conclusion

Even though mobile applications are all the rage, the security issue is still a major concern for most of users. Nowadays the use of OTP becomes a trend for user authentication since OTP is volatile and not reusable. The specifications such as Europay MasterCard Visa Chip Authentication Program (EMV/CAP) detail the use of such a technology. Many OTP authentication schemes have been proposed for one-time use. Most of them are time constrained. There is still room for improvement if we can add the location information into consideration in the mobile world. After studying some related researches about the location prediction [18, 19], location-based encryption and signatures, and mutual authentication [20, 21], we propose a time and location based OTP to authenticate users while accessing the application server in this paper. A time and location constrained OTP scheme can lessen the risk of passwords being stolen so that it can make an attacker harder to break through. Meanwhile, if a user moves steadily, the user can get transparently authenticated without remembering the password. To supplement the possible mistakes brought by the proposed scheme, a SMS based mutual authentication mechanism is also proposed in the article to make up for the unexpected misjudgement.

REFERENCES

[1] L. Scott and D. Denning, "Geo-encryption: using GPS to enhance data security." GPS World, pp. 40-49, 2003.

[2] Hsien-Chou Liao, Yun-Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users," Information Technology Journal, Vol. 7, Issue 1, pp. 63-69, 2008.

[3] Xiaofeng Lu Wicker, F. Leung, I. Lio, P. Zhang Xiong, "A Location Prediction Algorithm for Directional Communicaiton," Wireless Communications and Mobile Computing Conference, pp. 159-164, 2008.

[4] D. Son, A. Helmy, B. Krishnamachari, "The Effect of Mobility-induced Location Errors on Geographic Routing in Ad Hoc and Sensor Networks: Analysis and Improvement using Mobility Prediction," IEEE Transactions on Mobile Computing, Vol. 3, Issue 3, pp. 233-245, July 2004.

[5] Jarusombat, Santi Kittitornkun, Surin, "Digital Signature on Mobile Devices based on Location," International Symposium on Communications and Information Technologies, pp. 866-870, 2006.

[6] Lichun Bao, "Location Authentication Methods for Wireless Network Access Control," Performance, Computing and Communications Conference, pp. 160-167, 2008.

[7] Ferreres, A.I.G.-T. Alvarez, B.R. Garnacho, A.R., "Guaranteeing the authenticity of Location Information," IEEE Pervasive Computing , Vol. 7, Issue 3, pp. 72-80, July-Sept. 2008.

[8] Me, Gianluigi Pirro, Daniele Sarrecchia, Roberto, "A mobile based approach to strong authentication on web," International Multi-Conference on Computing in the Global Inoformation Technology, pp. 67-67, 2006.

[9] Alghathbar, K.; Mahmoud, H.A., "Noisy Password Scheme: A New One Time Password System," Canadian Conference on Electrical and Computer Engineering, 2009.

[10] ByungRae Cha, ChulWon Kim, "Password Generation of OTP System using Fingerprint Features," 8th IEEE International Conference on Computer and Information Technology, pp. 420-425, 2008.

[11] Vipul Goyal, Ajith Abraham, Sugata Sanyal, Sang Yong Han, "The N/R one time password system," International Conference on Information Technology: Coding and Computing, Vol. 1, pp. 733-738, 2005.

[12] "One Time Password" http://us.zyxel.com/

[13] "UKey" http://ukey.com.tw/site/ukey.html/

[14] Whitefield Diffie, Martin Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, Issue 6, pp. 644-654, Nov. 1976.

[15] Fadi Aloul , Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones," 2009 IEEE/ACS International Conference on Computer Systems and application, pp. 641-644, 2009.

[16] Han-Cheng Hsiang, Wei-Kuan Shih, "Improvement of Efficient Remote Authentication and Key Agreement," International Conference on Future Generation Communication and Networking, 2008.

[17] Philip Hoyer, "OTP and Challenge/Response algorithms for financial and e-government identity assurance: current landscape and trends," ISSE, 2008.

[18] Lei Mu, Geng-Sheng Kuo, Ningning Tao, "A Novel Location Algorithm Based on Dynamic Compensation Using Linear Location Prediction in NLOS Situations," Vehicular Technology Conference, Vol. 2, pp. 594-598, 2006.

[19] William Su, Sung-Ju Lee, Mario Geria, "Mobility prediction in wireless networks," 21st Century Military Communications Conference Proceeding, Vol. 1, pp. 491-495, 2000.

[20] Huixia Jia, Li Tu, Gelan Yang, Yatao Yang, "An Improved Mutual Authentication Scheme in Multi-Hop WiMax Network," International Conference on Computer and Electrical Engineering, pp. 296-299, 2008.

[21] Joaquin Torres, Jose M. Sierra, Antonio Izquierdo, "A Realistic Approach on Password-Based Mutual Remote Authentication Schemes with Smart-Cards," Digital EcoSystems and Technology Conference , pp. 334-338, 2007.