TSPass: A Dynamic User Authentication Scheme Based On Time and Space

Xuguang Ren†, Xin-Wen Wu††, and Kun Tang†††

†College of Information Science and Technology, Jinan University, Guangzhou, China
††Institute for Integrated and Intelligent System, and School of Information and Communication Technology,
Griffith University, Gold Coast, QLD 4222, Australia
†††College of Information Science and Technology, Jinan University, Guangzhou, China

Summary

On-line service providers and their users have suffered from various sophisticated attacks on user authentication. There is a strong desire to develop and implement more secure authentication schemes to protect web services against security threats. Intensive work has been done trying to improve upon traditional password authentication, resulting in two-factor authentication, session key exchanging schemes and time dynamic password schemes. However, these schemes have been proved not effective, due to their security design or additional overheads. In this paper, we proposed a secure dynamic user authentication scheme. Unlike the traditional password authentication (where a static password is used) or two-factor authentication (which requires the user's password and another pieces of time-dynamic authentication information), our proposed authentication scheme will be based on a dynamic one-time password (OTP), which is generated by the user's password, the authenticating time, as well as a unique property that represents the user's location at the moment of authentication (for example, the MAC address of the machine that the user uses for authentication). Compared with traditional OTPs which are only time-dynamic, the proposed scheme is based on both time and space (location). It is thus called TSPass. As we will analyze, our TSPass authentication improves upon two-factor authentication and other currently known authentication schemes, and effectively protect user's account against various attacks (including phishing attack, reply attack, and perfect-man-in-the-middle attack). Our testing and simulation work show that the proposed authentication is efficient and user friendly.

Key words:

Password, Perfect-man-in-the-middle attack, Phishing attack, Reply attack, Dynamic user authentication, Time and space dynamism

1. Introduction

Password authentication has been used, and is still widely used, by on-line businesses for clients to authenticate their identities and access their accounts. In a traditional password authentication scheme, the user is required to enter (directly) an account number (user ID) and a password (PW). The user ID and password then will be compared by the server at the business side, to check whether or not they match those stored in the password file in the database. It has been reported that the password authentication scheme is vulnerable to many attacks, including stolen-verifier attack, man-in-the-middle attack, replay attack, and phishing attack [1], [2], [3], [4], [5].

The stolen-verifier attack works by stealing the password file. People fight stolen-verifier attack by storing hashed or encrypted (rather than plain-text) password in the server [1], [2]. However, this solution is vulnerable to other attacks, as the user is still required to enter a password. The plain-text password traveling through the network can be intercepted by a third party [3], which called the man-in-the-middle attack. A countermeasure against the man-in-the-middle attack is to hash or encrypt the password before it is sent to network. However, this does not prevent the replay attack, which captures the encrypted password and uses it to intrude into the system.

One time password (OTP) scheme has been introduced as a countermeasure against the replay attack. An OTP is a password that is valid for only one login attempt. Algorithms for generating OTPs are critical in this solution, since any unauthorized party should not be able to guess the next password. The S/KEY password scheme presented in [4] is based on OTP technique. However, the scheme has a number of drawbacks, such as heavy hash overhead and password resetting problems. And it has been proved not secure [5].

In [6], the authors present a dynamic password scheme which incorporates time factor into the dynamic password generation. When the user presents his/her static password, an OTP will be generated (by the login page of the system website) by using a hash algorithm. Then, only the user ID and the dynamic OTP are sent to the server. As the OTP is only valid in a very short time (for example, several seconds) and can only be used once, this scheme effectively prevents the replay attack. However, as the authors have already observed, their scheme is vulnerable to the Perfect-Man-In-The-Middle [6] attack, which is a more sophisticated attack where the hacker can intrude into the system by using the intercepted OTP before the OTP expires and before the user gets the access to the account. Moreover, the scheme in [6] is vulnerable to the

Manuscript received October 5, 2012
Manuscript revised October 20, 2012

phishing attack; as the phishing attack can acquire the user's static password by using a fake website.

Actually, any authentication scheme which requires the user to enter the static password into the login web page is vulnerable to the phishing attack. In [7] the authors present an authentication scheme (which is called DPASS) using grid analysis. To use this scheme, each user owns three authentication factors, that is, a user ID, a static password, and a pattern. When authenticating the user has to calculate an OPT based on a matrix. The static password and the pattern are used as OTP generation parameters; the matrix is given by the login page. Then the obtained OTP will be sent to the server. In DPASS scheme, as the user's static password is no longer entered into the login form, it can defend against phishing attack. But DPASS has several drawbacks. First, the user has to remember an extra pattern in addition to the password. Second, the user has to do the calculation. Third, DPASS still cannot defend against the Perfect-Man-In-The-Middle attack. It is obvious that DPASS is not user friendly, as users are required the do a complex OTP generation.

Most currently used two-factor authentication systems are quite user friendly. In a two-factor authentication system, the user will be provided the OTP by certain secure means, which can be a password scratch sheet, a security Token [8], or a mobile phone based software [10]. Many organizations generate the OTP and send it to the user through SMS [9] [13]. However, for most existing two factor authentication schemes, apart from the overhead, the user has to bring an extra token or mobile phone for the authentication. More importantly, two-factor authentication schemes are still vulnerable to the Perfect-Man-In-The-Middle attack.

To summarize, the currently known authentication schemes are not effective due to the following problems:

Being vulnerable to the Perfect-Man-In-The-Middle attack.

Requiring a high overhead (such as involvement of telephone system or external token) and/or user's effort to generate OTPs.

In this paper, we present a dynamic authentication scheme. The core of our authentication scheme is a dynamic OTP which is generated by the user's password, the authenticating time, as well as a unique property that represents the user's location at the moment of authentication, for instance, the MAC address of the machine that the user uses for authentication. Unlike traditional OTPs which are only time-dynamic, the proposed scheme is based on both time and space (location). We thus call it TSPass. The TSPass authentication improves upon two-factor authentication and other currently available authentication schemes. As we will analyze, it can effectively protect user's account against various attacks including the Perfect-Man-In-The-Middle attack (thus it solves the first problems mentioned above). Furthermore, the authentication procedure is efficient, and the rest two problems are eliminated in our scheme.

The rest of the paper is organized as follows. Section 2 presents basic concepts used in our scheme. Problem definition and an authentication framework are given in section 3. Section 4 presents the detailed design of our scheme. Scheme analysis is presented in section 5. Simulation test are given in section 6. Section 7 concludes the paper.

2. Preliminaries

A. Basic Concepts

Authentication is the act of confirming that the communicating entity is the one claimed. Commonly, three types of techniques for authentication on internet: what you know (e.g. passwords), what you have (e.g. unique ATM card or unique tokens), and what you are (e.g. unique biometrics). As the expensive overhead and complexity of biometrics, the using of first two types is more widespread.

The Perfect-Man-In-The-Middle [6] attack is a kind of attack conducted by some hackers with advanced skills, who can implement authentication in a very short period of time and before the user does if they intercepted the user's one time password and account number.

A cryptographic hash function, denoted as H, is a hash function, that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string. It is computationally infeasible to find any pair *a* and *b*, such that $H(a) = H(b)$.

Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. Commonly, one machine only has one MAC address.

A one-time password (OTP) is a password that is valid for only one login session or transaction. In this paper, we treat OTP as a kind of dynamic password which can be changing with the time or some other factors.

Network Time Protocol (NTP) is a networking protocol for synchronizing the clocks of computer systems over packets-witched, variable-latency data networks.

B. Time Dynamism

Time dynamism is an OTP generation principle widely utilized in current dynamic password authentication schemes and two factor authentication schemes. By incorporation of the time factor into OTP generation, the OTP can be changing with the time. Different password is needed for different time at which the user is launching authentication. Due to reality consideration, time dynamism always means that the OTP keeps static in a very short period of time while appears dynamic in different time periods. The static time period is designed for user to input the OTP into the login form upon receipt of the dynamic password, and the length of which can always be customized by the client.

C. Space Dynamism

Most of current methods used to generate OTP are Time-synchronized or Mathematical algorithms. Time-synchronized method keeps the OTP changing with the time and never repeats. Mathematical algorithms based on the previous password or a challenge also generate non-repeat OTP each time. Some hackers, in Perfect-Man-In-The-Middle attack, being capable of conducting authentication in a very short period of time and before the user does makes authentication schemes simply based on above OTP generation methods vulnerable.

Space dynamism is a new OTP generation concept requiring the generated OTP can only be valid in a particular space. The space can be a user specified city or country, and also can be a particular computer. In our system, we limit the valid space of OTP to a computer by using which the user is launching authentication. Hence, a particular OTP can only be used to login at a particular machine. In this way, even if the hackers get the OTP and account number, they still cannot login successfully at any time using their own computers. Thus, Perfect-Man-In-The-Middle attack can be countered effectively.

3. AUTHENTICATION FRAMEWORK

In this section, we take various security threats into consideration and develop a novel dynamic password authentication framework based on time dynamism and space dynamism.

A. Problem Definition

1) Text password is the most widely used authentication method with quite a lot of disadvantages, the most detrimental of which is weak password. Users tend to select relatively weak passwords for easy memorization [14]. Therefore, a novel authentication scheme should have the ability to assign the users with strong passwords or put some limits on selection when users are choosing passwords.
2) The server is difficult to be provided absolute security to prevent the steal of the password table, in which case the passwords of the clients should be hashed before being saved into the database. Moreover, it should be computationally impossible to reveal the password on the server side only with the hashed password table in hands.
3) It is a nightmare for an authentication scheme that cannot work without external real entity. The involvement of telephone system will lead to extra time delay and service unavailability when there is no telephone signals. Endeavour should be done to cut off the extra overhead and to provide the best performance and convenience.
4) Unlike DPASS [7], the OTP generation should be user friendly, in other words, the complex calculation of OTP should be completed automatically with the least help from the user.
5) Time dynamism of the OTP could ensure that the dynamic password is only valid in a short period of time. Space dynamism of OTP could achieve that the OTP is valueless in any other machine apart from the machine by using which the user generates the OTP. One situation can make it certain necessity to implement time dynamism, which is that the adversary launches login at the same machine by using which the user generated the OTP. Only the OTP being different at different time can counter this same-machine attack. Therefore, it requires the combination of time dynamism and space dynamism to ensure that the OTP only be used to login on one particular machine and at a particular short period of time.

B. Authentication Framework

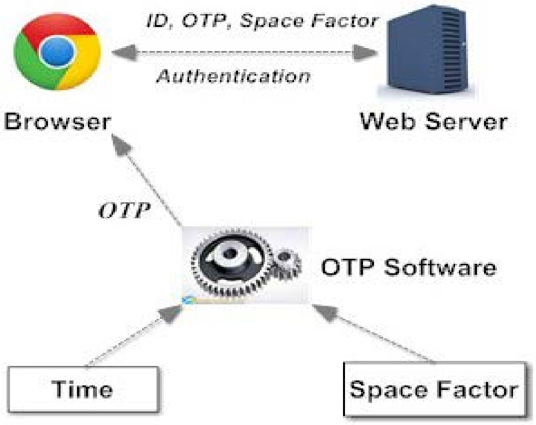


Fig.1. Authentication Framework

Fig.1. presents the framework of an authentication scheme based on time factor and space factor, which is the overview of TSPass. The space factor can be some specific unique elements, such as the MAC address of a machine in TSPass. As can be seen from Fig. 1, apart from the traditional client who is a browser and the central server, there is extra software aimed to generate the OTP. The software takes the time and space factors as input, and combines them together to generate a dual dynamic OTP. The dual dynamic OTP has both time dynamism and space dynamism. The browser sends he user’s ID, dynamic OTP input by the user, and the used space factor to the server. The server then will make a similar OTP calculation and compare all the authentication details to decide whether the client is a legitimate user.

4. TSPASS

In this section, the detailed structure of TSPass has been presented, which is designed based on the problems discussed before. Some critical techniques are also listed. All the notations used are explained in table I.

TABLE I NOTATIONS

Name	Description
IDu	User's account number
Pu	User's strong password
PD	The digest of user's password
⊕	Exclusive or
Tu	Time used on user side
Ts	Time used on server side
MKs	Server's master key
MPD	The value of PD exclusive XORed by MKs
U_OTP	OTP generated on user side
S_OTP	OTP generated on server side
HMAC	The digest of MAC address of user's machine

A. Authentication Procedure

We decomposed the authentication procedure into four steps: sign-up period, OTP generation, passing authentication details to server and verification.

1) *Sign Up*:

The server owns a master key (MK_s) which should be kept secret. In the sign-up period, the user is issued an account number (ID_u) and a static password (P_u) which is a strong password to counter the brute force attack. Then the static password is hashed to PD=H(P_u). PD is short for password digest. The user's account number with the corresponding PD will be saved in the database of the server.

2) *OTP Generation:*

User's static password is used to generate the OTP. The OTP generation is designed as a tiny software which can be downloaded from our website for free, anytime and anywhere, if the user has a internet connected PC or mobile phone. The software is not unique for a particular user and can also be incorporated into the ATM machines. The mechanism of the software is shown in the Fig. 2.

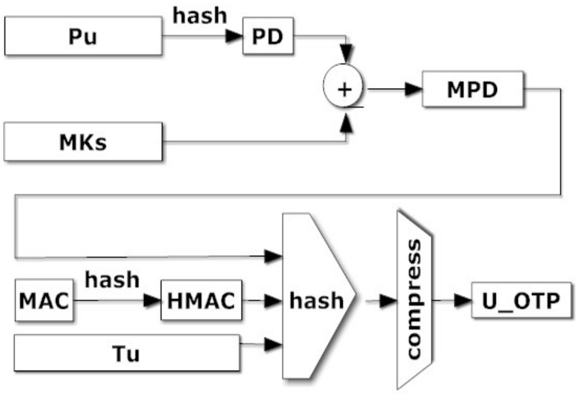


Fig.2. OTP Generation

To achieve time dynamism property of the OTP, the time factor is incorporated into the generation procedure. MAC address of the machine on which the user performs OTP generation is used to achieve space dynamism. The password, input by the user, first will be hashed to get the PD which then will be XORed with the master key (embedded in the OTP generation software) of the server to generate the MPD(Master key and Password Digest). The MAC address of the user's machine will be obtained and hashed to HMAC which is designed to protect the user's privacy. MPD combining with time and HMAC composes the message, which then will be hashed to generate the OTP. A compressing procedure is an optional procedure which can be used to compress the long OTP to a short one. It depends on the balance of the security and convenient requirements. The output OTP can be regarded as the user's signature at a particular time and on a particular machine. We denote the user side OTP as U_OTP in the figures.

3) *Passing Authentication Details To server:*

This process mainly involves the user's inputting by hand or copying the generated U_OTP into the login form on the web page. One more thing should be considered, which is that the HMAC hashed from MAC address should be sent along with other authentication information to the server. User's MAC address can be automatically grabbed by the web page by using JavaScript technique. In our system, we only support the situation in which the user implements authentication and OTP generation on the same machine. This process can be shown in Fig. 3.

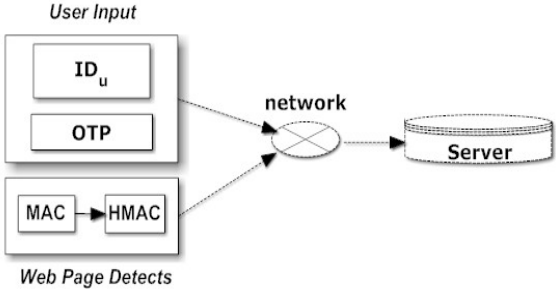


Fig.3. Passing Authentication Details To server

1) *Verification:*
Upon receipt of the authentication details, the server will implement the verification which consists of extracting the HMAC, generating the OTP and comparing the authentication details. The server uses a similar process to generate the OTP. User's PD can be retrieved from the database. User's corresponding HMAC is easily available as well. In terms of the time, multiple strategies are given in the next subsection to achieve synchronization between server and the user. The server side OTP is denoted as S_OTP. Intuitively, if server generated S_OTP matches the user generated U_OTP; the user will be verified as a legitimate user. The verification on the sever side can be shown in Fig. 4.

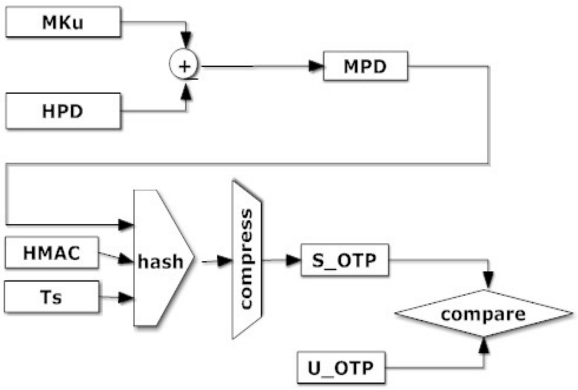


Fig.4. Verification

B. Critical Techniques

- *Time Synchronization*

As can be known, the server needs to implement OTP generation by using the same time factor as the user does, in order to generate the identical OTP. We proposed two strategies which can be used to achieve time synchronization.

1) Add Time Factor To OTP
The simple solution to time synchronization is to add the time information to the OTP. Thus the final dynamic password consists of two parts: U_OTP and time information, as shown by Fig.5.

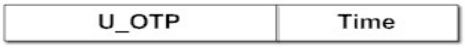


Fig.5. Dynamic password structure

In this manner, the server can get the time information from the received dynamic password. But adding information increases the length of the OTP, which will add more inconvenience for the user to input. If the time information needs to be encrypted due to security requirements, the length of final dynamic password may be longer.

2) Server Guesses Method
The other strategy that we can use is to let the server guess the time when user generates the OTP. This method involves the OTP generation software as well. Given the length of OTP's valid time is *VT*, at *UT* time the user is performing the OTP generation. Then the time factor used by the OTP generation software is *UT-UT mod (VT/2)*. If the server side receives the authentication at time ST, the server will have two guesses. First time the server will use *ST-ST mod (VT/2)* as time factor to generate the OTP. If the first guessing OTP matches the user's OTP, guessing process will be terminated and authentication success for the user. If the first guessing failed matching, then the server will use *ST-ST mod (VT/2)-VT/2* to implement the second OTP generation, the second comparison will be applied accordingly.

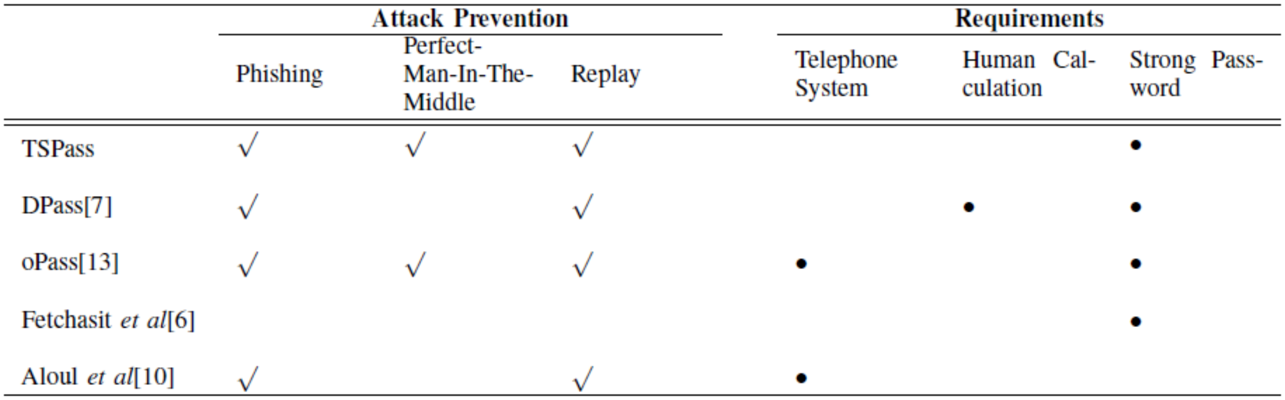
Example 1: If *the valid time period has been set as 10 minutes. The user is generating the OTP at 18:12. Then 18:10 will be used by the software as the time factor. If the server receives the authentication details at 18:17, then both 18:15 and 18:10 will be guessed to calculate the OTP. And the 18:10 will hit the target.*

3) Method Comparison
Both the above two methods can achieve the time synchronization. The simply adding method is simple to apply and more efficient than the server guessing method. But consider the average guessing times is 1.5, which is also acceptable, and the adding method will add the dynamic password length, we prefer the server guessing method. We tested both the methods in our tests.

It is worth noting that the time of the user's PC should be consistent with that of the server. However, it is difficult due to different time zones or wrong time of the user's PC, in this situation, the NTP protocol is needed to achieve the consistency between the server and the user. The OTP generation software will use NTP to grab the internet time instead of the system time of the user's PC.

- *Space Dynamism*

TABLE II
COMPARISON OF RELATED AUTHENTICATION SCHEMES



	Attack Prevention			Requirements		
	Phishing	Perfect-Man-In-The-Middle	Replay	Telephone System	Human Calculation	Strong Password
TSPass	√	√	√			•
DPass[7]	√		√		•	•
oPass[13]	√	√	√	•		•
Fetchasit *et al*[6]						•
Aloul *et al*[10]	√		√	•		

In addition to time dynamism, we added space dynamism implemented by using MAC address. Each machine has a unique MAC address. By incorporating the MAC address into the OTP generation, the OTP will be only valid for the user's machine. In this manner, even at the same time the hacker using the user's OTP to login, he still cannot authenticate successfully, because the MAC address of the hacker's PC is different from that of user's PC.

- *Encoding*

As the output of the hash function is a binary string. The Radix 64 encoding technique has been used in order to present a readable and type-able OTP to the user.

5. Analysis of Scheme

A. *Security Analysis*

- *Proper Use Of Hash Functions*

The user's password is saved in the database in a cipher manner, implemented by using a hash function. In this way, the hacker cannot get the user's password through stolen-verifier attack. The use of server's master key makes it difficult to implement OTP generation manually even if the hacker gets the hashed password table. The OTP sending in the network is the result of a hash function of HMAC, time and MPD. Hackers cannot get any information about the user's static password from the OTP.

- *Time Factor*

Time factor has been incorporated into the generation of OTP to achieve time dynamism property. OTP will be changed in a short period of time. The length of valid time can be set according to the user's preference. NTP ensure the consistency of the time between server and the client.

- *MAC Address*

The participation of MAC in the generation of OTP is an example of utilizing space factor which addressed the space dynamism problem. The MAC address is unique for each machine (only consider one machine with one MAC address), thus MAC address can be seen the utilization of "what you have" in authentication technique. Even a hacker gets all the authentication details(account, OTP) input into the authentication form, and implements authentication in the valid time of OTP, there is no way for him to authenticate successfully. As at the server side, the hacker's MAC will be used to generate the OTP which is totally different from the users. Space dynamism and time dynamism together guarantee the scheme is secure against replay attack, same-machine attack and Perfect-Man-In-The-Middle attack.

- *OTP generation software*

Compared with most of two-factor authentication, our scheme uses software to generate the OTP, which is much more economic and easier to apply. The advantage of our scheme over DPASS is the user friendly property which does not let the user do the calculation of OTP. In terms of phishing attacks, as our scheme not letting the user input the static password in the login form, which can counter phishing attacks effectively.

B. *Performance Comparison*

Compared with other existing authentication schemes, TSPass comes with its advantages. Table II gives a summary of comparison of TSPass and previous systems. We use '√' to indicates the system prevents against this kind of attack. The symbol ' • ' represents the special requirement needed. TSpass achieves a good performance on most of security attacks with the least requirements. Any authentication scheme needs the static password input into the login form, like Fetchasit et al, is subject to phishing attack. To counter phishing attack, most of current systems are relying on the telephone system to play as a trusted third party. oPass and Aloul's two-factor authentication are all using SMS service provided by telephone system which also incurs longer time delay than the internet. By requiring the user to do some calculation based on an extra grid pattern, DPass can prevent phishing attack but is still vulnerable to Perfect-Man-In-The-Middle attack.

C. System Flexibility

1) Parameter Flexibility

In our system, we put most of our attention on the authentications of internet area. A pure MAC address can be used to uniquely identify each PC. For some security considerations, more techniques, such as check bits can be integrated with MAC address to achieve a higher security level. If this scheme is needed to be implemented in the mobile phone systems, the IMEI (International Mobile Equipment Identity) number can replace the role of MAC.

2) Security Services Flexibility

As known in the authentication procedure, the server has to know the HMAC from the user's machine. If the legacy system has already applied secure mechanisms to defend against fake packets attack, in which situation the hacker manually puts the user's HMAC in the package and send to server, nothing needs to be done specially for MAC transformation. If no such secure mechanisms existing in legacy system, only an external encryption algorithm is needed to protect HMAC. The server is he only one can encrypt and decrypt the HMAC. In his manner, the insecure legacy system can also achieve advanced security level without lots of painful work.

3) Implementation Flexibility

In our scheme, we assume that the user has to use the same machine to launch login and OTP generation, because the server grabs the user's MAC address and hashes it by using the login page, and the HMAC used in OTP generations of both server side and user side should be the same. However, the OTP software can also easily be embedded into mobile phones or portable devices by adding dependent running and self-detect ability to them. When to login, the user only needs to insert the mobile devices into the PC and lets it detect the PC's MAC address by itself. Moreover, consider most of current smart phones have Wi-Fi been installed, the MAC address can be sent to the mobile phone through wireless interface, which will be more convenient to use. This separating OTP generation strategy is much safer because of the potential malwares in an untrusted computer. Running the OTP generation software in a mobile phone or on a relatively dependent portable platform will raise security level of the system. In this manner, our scheme can fit more users' requirements and achieve a higher secure performance.

6. Tests

A. TSPass Implementation

As discussed before, TSPass is composed of three parts: OTP generation software, a login page displayed in a browser and a central server dealing with authentication requests. All the involved hash functions are implemented as MD5. The detailed simulation work is given as follows.

1) OTP Generation Software

We implemented the OTP generation software by using pure Java under J2EE. The software is very easy to use, which only contains a window interface to let user input the static password and to print out the generated OTP. For testing the implementation flexibility of TSPass, besides the PC version, we also created the corresponding OTP software for smart phones. As the OTP software was implemented in Java and very small, which is supported by most of the smart phones no matter what the underlying operating system is. Currently, we built a functional extension for Chrome browser which can automatically set up a TCP server socket. When needs to generate the OTP on a phone, a connection can be established for the extension to pass the MAC address to the OTP software installed on the phone via Wi-Fi.

2) Login Page

The login page is implemented by using simple HTML statements. JavaScript technique was utilized to obtain the MAC address of local machine. As the MAC address is personal privacy which needs some particular browser settings to make it visible. The MAC address was hashed before being sent to the network to protect user's privacy.

3) Central Server

We developed a central server system which was running on Tomcat and used Java Spring as underlying framework. The entire user's information was saved in database (MYSQL). The server system was designed to be running on a computer with Intel Pentium CPU, 2G RAM.

TABLE III DEMOGRAPHIC CHARACTERISTICS (N = 20)

	Characteristics	**Mean**
1	Age	25
2	Computer Experience(years)	4
3	How often need to login to website(times/day)	7.5

B. Usability Test

The primary purpose of the test was to assess the usability of TSPass authentication scheme. Our test was carried out with 20 persons whose overall characteristics are given in Table III. We conducted the usability test by using "Dialog Design [15]" method, which consists of three individual steps: Interview, Solving test tasks and Debriefing.

- *Interview*

In this phase, each participant was issued an account number and a static password. We also gave the participants a brief introduction of TSPass authentication system to let them know what they can and need to do.

- *Solving tests tasks*

For TSPass system, there was only one task needs to be done, which was to generate the OTP and to launch login on our website.

- *Debriefing*

All the participants have succeeded to use both mobile and PC-based software to generate OTP. And all the logins were launched smoothly as expected. It demonstrated that TSPass system was friendly enough for user to use. And mobile-based software provides a more secure choice when needs to launch the authentication on an untrusted PC. However, as it is much more convenient to directly generate the OTP on a computer, and consider many times of logging into websites everyday in modern life, most of participants admitted that they preferred to use PC-based OTP software unless they need to login some financial websites.

C. Performance Test

1) Effectiveness

It can be demonstrated from the usability test that TSPass worked very well on legitimate user's authentication. We also conducted several negative tests based on security attacks discussed before, especially for Man-In-The-Middle attack and Perfect-Man-In-The-Middle attack. Due to the difficulties to break a hash function, like MD5, it is computationally impossible to reveal the static password only by captured OTP even with full knowledge of time and MAC address. Regarding Perfect-Man-In-The-Middle attack, as analyzed in the previous sections, attempts to login during the OTP's valid time on other computers had no success in all tests.

TABLE IV
TIME AUDIT

#	Max	Mean	Min
OTP Generation(s)	12	5.5	3
Input Authentication Details(s)	12.5	6	4
Web Page Response (ms)	70.4	46.2	37.7

TABLE V
OTP SOFTWARE INTERNAL RUNNING TIME

Test Number	Response Time (ms)
1	15
2	17
3	15
4	31
5	15
6	15

2) Efficiency

Compared with other authentication schemes involving telephone service or two-factor authentication schemes using an external token, time efficiency can be another advantage of TSPass apart from the lower overhead. Table IV is a snapshot of time audit in different phases recorded from the usability test. As the table shows, most of the time is consumed by OTP generation and inputting the authentication details into the login form. Regarding OTP generation, time is mostly taken by typing in the user's password rather than OTP software's internal working, which can be demonstrated by Table V. It can be seen that the response time of the OTP generation software is pretty fast, which is because the information to be hashed is very short. In terms of the web page response, the performance will be mostly affected by the time of server retrieving the account number and PD from the database instead of by the time of OTP generation and authentication details comparison.

And we also compared the performances of different time synchronization methods. The server guessing method had shown a good performance without affecting the length of OTP.

7. Conclusion

Overcoming the limitations of currently available user authentication schemes, and solving the problems that they suffered from, we have proposed a dynamic authentication scheme, TSPass. It employs both the time factor and the space factor (such as MAC address), to provide a secure and efficient authentication means. It is robust against attacks including the Perfect-Man-In-The-Middle attack. And it is flexible to meet different requirements. The testing and simulation work shows that the TSPass is effective, efficient and user friendly.

We would like to point out that the scheme can be improved in the future, considering that attacks are evolving. Phishing attacks typically lead the user to a fake authentication web site which is seemingly identical to legitimate one. We assume the software used by the user is legitimate. If the future phishing attack uses fake software, our scheme will be vulnerable to the evolved attack. Although it is more difficult to deceive a user to use phishing software than just a fake web site, it can happen in some special environments. As a future research work, we will investigate effective methods to counter software-based phishing attacks.

References

[1] A. Evans Jr., W. Kantrowitz, E. Weiss, "A user authentication scheme not requiring secrecy in the computer", Common. ACM, 17(1974), pp.437-442.

[2] G. B. Purdy, "A high security log-in procedure", Commun. ACM, 17(1974), pp. 442-445.

[3] K. Kwon, S.J. Ahn, J.W. Chung, "Network Security Management Using ARP Spoofing", ICCSA, 2004, pp.142-149.

[4] N. M. Haller, "The S/Key one-time password system." Proc. Internet Society Symposium on Network and Distrbuted System Security, pp. 151-158, 1994.

[5] C.J. Mitchell, L. Chen, Comments on the S/KEY user authentication scheme, ACM Operating Syst. Rev. 30 (1996) 1216.

[6] D.Pansa, T.Chomsiri, "Web Security Improving by using Dynamic Password Authentication", International Conference on Network and Electronics Engineering, vol.11, pp. 32-36, 2011.

[7] Balaji. R, Roopak. V, "DPASS: Dynamic password authentication and security system using grid analysis", Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.2, no., pp.250-253, 8-10 April 20111216.

[8] D.Pansa, T.Chomsiri, "Web Security Improving by using Dynamic Password Authentication", International Conference on Network and Electronics Engineering, vol.11, pp. 32-36, 2011.

[9] Balaji. R, Roopak. V, "DPASS: Dynamic password authentication and security system using grid analysis", Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.2, no., pp.250-253, 8-10 April 2011

[10] "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005. Available at http://www.rsa.com/ press release.aspx?id=6092 (06-Aug-2012)

[11] Jong-Won Seo, Je-Gyeong Jo, Hyung-Woo Lee, "SMS(Short Message Service) based Secure Authentication and Accounting Mechanism in Wireless Network," Hybrid Information Technology, 2006.ICHIT '06. International Conference vol.2, pp.736-744, 9-11 Nov. 2006

[12] Aloul. F,Zahidi S., El-Hajj W., "Two-factor authentication using mobile phones," Computer Systems and Applications, 2009. AICCSA 2009.IEEE/ACS International Conference, pp. 641-644, 10-13 May 2009

[13] Scratch And Weep Attack, Available, At http://www.globaltrust.it/html popup/phishing swedish/images/mail.pdf

[14] Ziqing Mao, Florencio D., Herley C., "Painless migration from passwords to two factor authentication," Information Forensics and Security (WIFS), 2011 IEEE International Workshop, pp.1-6, Nov. 29 2011-Dec.2 2011

[15] Huang-Min S.,Yao-hsin C., Yue-Hsun L.,"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.

[16] S. Gar and E. W. Feltem, "Password management strategies for online accounts", in SOUPS '06: Proc. 2nd Symp. Usable Privacy. Security, New York, 2007, pp. 657-666, ACM.

[17] DialogDesign ved Rolf Molich, DialogDesign(online), Available: <http://www.dialogdesign.dk/Usability testing.htm>(15-Sept-2012)

Xuguang Ren, is a bachelor student of Jinan University, Guangzhou, China. He was sent to study at Griffith University from 27-July-2011 to 27-Aug-2012 as an Exchange Student. He is a member of 'Top Student Training Plan' of Jinan University. His researching interests were information security and encrypted database.

Xin-Wen Wu received the Ph.D. degree from the Chinese Academy of Sciences. He was with the Institute of Mathematics, Chinese Academy of Sciences, the University of Louisiana (as a visiting researcher), the University of California, San Diego (as a post-doctoral researcher), and the University of Melbourne (holding a research fellowship). He was a faculty member of the School of Information Technology and Mathematical Science, University of Ballarat, Australia, before joining Griffith University. Since April 2010 he has been a faculty member of the School of Information and Communication Technology, Griffith University, Australia. His research interests include coding and information theory, applied cryptography, and the applications. He has published over 40 research papers, two book chapters and two books in these areas. He is a member of IEEE.

Kun Tang is a bachelor student of Jinan University, Guangzhou, China. She was sent to study at State University of New York from 27-July-2011 to 27-Aug-2012 as an Exchange Student. She is a member of 'Top Student Training Plan' of Jinan University. Her researching interest was security of wireless sensor network.