Two New Mobile Single-Sign-On Systems Against Guessing Attack

Yung-Cheng Lee[1], Jung-Lu Chu[2] and Huan-Cheng Lien[1]
1:Department of Electrical Engineering, WuFeng Institute of Technology.
Email: yclee@mail.wfc.edu.tw
2:The Institute of Opto-Mechatronics and Materials, WuFeng Institute of Technology.

Abstract

Single-sign-on system allows users to login networks for services with only a set of password. Many single-sign-on solutions available today are lack of mobility or even insecure. In this article, we propose two new single-sign-on solutions with the merits of mobility and resisting password guessing attacks. The first system is based on smart cards, and the second one is based on passwords. Both the systems are simple and practical for non-PKI users.

Keywords: single-sign-on, smart card, password authentication, guessing attack.

摘要

單一簽入機制提供使用者僅需輸入一次通行碼，即能簽入各應用系統，方便使用者獲取網路各種服務。迄今許多單一簽入機制缺乏移動性，即使用者僅能在某一特定主機上進行簽入。本文提出二種簡單之單一簽入機制，此機制不僅達到單一簽入之目的並具移動性，能提供使用者在任意一台主機上執行簽入，且可避免通行碼猜測攻擊。

關鍵詞：單一簽入、智慧卡、通行碼認證、猜測攻擊。

1. Introduction

Networks are very important media for people to obtain various kinds of information. Service providers provide users services through networks. In these days, for obtaining various services, people usually have many different network accounts such as web-shops, work accounts, ISP, e-mail, online-banking etc. Each account needs at least one set of password to login, as a result people have to manage a lot of various passwords. Having several passwords for each user will lead to a big trouble on password management. People are probable to write down their passwords or to use the same password for different accounts. Unfortunately, systems with these approaches always security flaw since they can be easily attacked. Therefore, it needs to find better solutions for users to login their accounts [4].

Single-sign-on system allows users to login networks for services with only a set of password. Several researchers have proposed solutions for single-sign-on systems [5,6,9]. Many of the single-sign-on solutions available on the market today are either too expensive or lack of mobility. Pashalidis and Mitchell (2003) proposed a single-sign-on system for GSM [5]. Their scheme

changes the GSM architecture such that it is impractical even though the scheme is secure. Moreover, their scheme cannot prevent smart card stolen-attack. That is the attacker can impersonate the legal user to login system if he/she obtains the smart card.

Short and simple passwords are vulnerable to guessing attacks [1,2,3]. Password guessing attacks include on-line and off-line attacks. An on-line password guessing attack happens when an attacker attempts to guess the password during an on-line transaction, while an off-line password guessing attack occurs when an attacker guesses the password and verifies his/her guess off line. Single-sign-on systems need passwords for users to login, thus how to develop mechanisms that can resist guessing attack is an important issue.

Smart cards, because of their portability and tamper-free features, are convenient and secure devices for remote authentication. Though smart cards have deficiencies in computation and memory, they are widely used in modern networks [7,8]. Using smart cards to login networks is a solution for single-sign-on problem. In order to protect smart card free from thieves to login, it requires PIN or passwords to resist smart card stolen-attack.

In this article, we will provide two new single-sign-on solutions that can resist guessing attack. The preliminaries and notations are presented in next Section. The proposed smart card based mobile single-sign-on system is described in Section 3. The password based single-sign-on is presented in Section 4. Finally, we make some conclusions.

2. Preliminaries and notations

A mobile single-sign-on system denotes a user can login networks for service through any terminals at any place if it connects to the networks. In the mobile single-sign-on systems, suppose that there are users, service providers, and a trusted authentication center in the system. The service providers and authentication center have joined in the public key infrastructure (PKI). A user, even though he/she is not a PKI participant, can also perform symmetric and asymmetric cryptographic computations and send confidential messages to the PKI users. The notations of the paper are as followings:

PW: password.

ID: the identity of the user.

U: user.

SP: service provider.

Auc: authentication center.

pub_A: public key of A.

pri_A: Private key of A.

K: session key with at least 128-bit length.

$(M)_K$: message M is encrypted or decrypted with session key K by using symmetric cryptosystem.

$\{M\}_{pub\_A}$: message M is encrypted with A's public key by using asymmetric cryptosystem.

$\{M\}_{pri\_A}$: message M is signed with A's private key by using asymmetric cryptosystem.

A→B: *M*: A sends message *M* to B.

3. The smart card based mobile single-sign-on system

Let *x* be the secret of the authentication center. The system includes registration and login phases. All users should register to the authentication center before login the system. The center sends each user a smart card after registration.

3.1 Registration phase

The registration phase is as follows and it is shown in Fig.1.

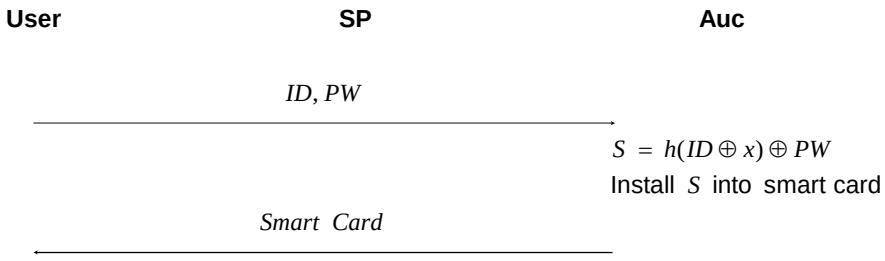

Fig.1. The registration phase of the smart card based mobile single - sign - on system

Step R.1. U→Auc: *ID, PW*

The user forwards his/her identity *ID* and password *PW* to the authentication center personally or through a secure channel.

Step R.2. Auc→U: smart card

The Auc verifies *ID* and *PW* to authenticate user. After the user is authenticated, the center computes $S = h(ID \oplus x) \oplus PW$ and stores it with a secure hash function $h(\cdot)$ into a smart card. Then the center sends the smart card to the user U.

3.2 Login phase

3.2.1 User logins to a service provider

When a user wants to login a service provider for services, he/she inserts smart cart to the cardholder. The login phase is as followings.

Step L.1. U→SP: ID, C_1, C_2, T_1

The user inputs his/her password to the smart card. The smart card generates a random number *R* with at least 128 bit length, and computes $C_1 = S \oplus PW \oplus R$ and $C_2 = h(R, T_1)$, where T_1 is the timestamp. Note that $C_1 = S \oplus PW \oplus R = h(ID \oplus x) \oplus R$. Next, the user forwards (ID, C_1, C_2, T_1) to SP.

Step L.2. SP→Auc: ID, C_1, C_2, T_1

Because secret *x* is unknown, SP cannot authenticate the user with (ID, C_1, C_2, T_1). The SP forwards the message to Auc. Step L.1 and L.2 can be combined to user directly sends (ID, C_1, C_2, T_1) to Auc.

Step L.3. Auc→SP: C_3

After receiving (ID, C_1, C_2, T_1), Auc computes $R' = C_1 \oplus h(ID \oplus x)$. Since

$$\begin{aligned} & C_1 \oplus h(ID \oplus x) \\ &= S \oplus R \oplus PW \oplus h(ID \oplus x) \\ &= h(ID \oplus x) \oplus R \oplus h(ID \oplus x) \\ &= R \quad , \end{aligned}$$

Auc can authenticate the user if $h(R', T_1) = h(R, T_1)$. Next, Auc computes *Token* and sends C_3 to the user. Where T_2 is the timpstamp,

$$Token = \{ID, h(R), Assertion, Auc, T_2\}_{pri\_Auc},$$

and

$C_3 = \{Token, h(R), ID, SP\}_{pub\_SP}$.

Note that other parameters such as serial number, date, version, etc., can also be included in the *Token*. Since *Token* is signed by Auc, everyone even not a PKI user can verify *Token* by using the public-key of Auc.

Step L.4. SP→U: C_4

After receiving C_3, the service provider obtains *Token* and $h(R)$ by using private key. After *Token* is verified, the service provider generates a partial session key K_1. Next, the service provider computes and forwards $C_4 = (Token, K_1, ID, SP)_{h(R)}$ to the user.

Step L.5. U→SP: C_5

After receiving C_4, the user recovers *Token* and K_1 with $h(R)$. The user generates another partial session key K_2 after *Token* is verified. The user obtains the session key *K* by

$$K = K_1 \oplus K_2$$

Then the user sends C_5 to the service provider, where

$$C_5 = (K_2, h(K))_{pub\_SP}$$

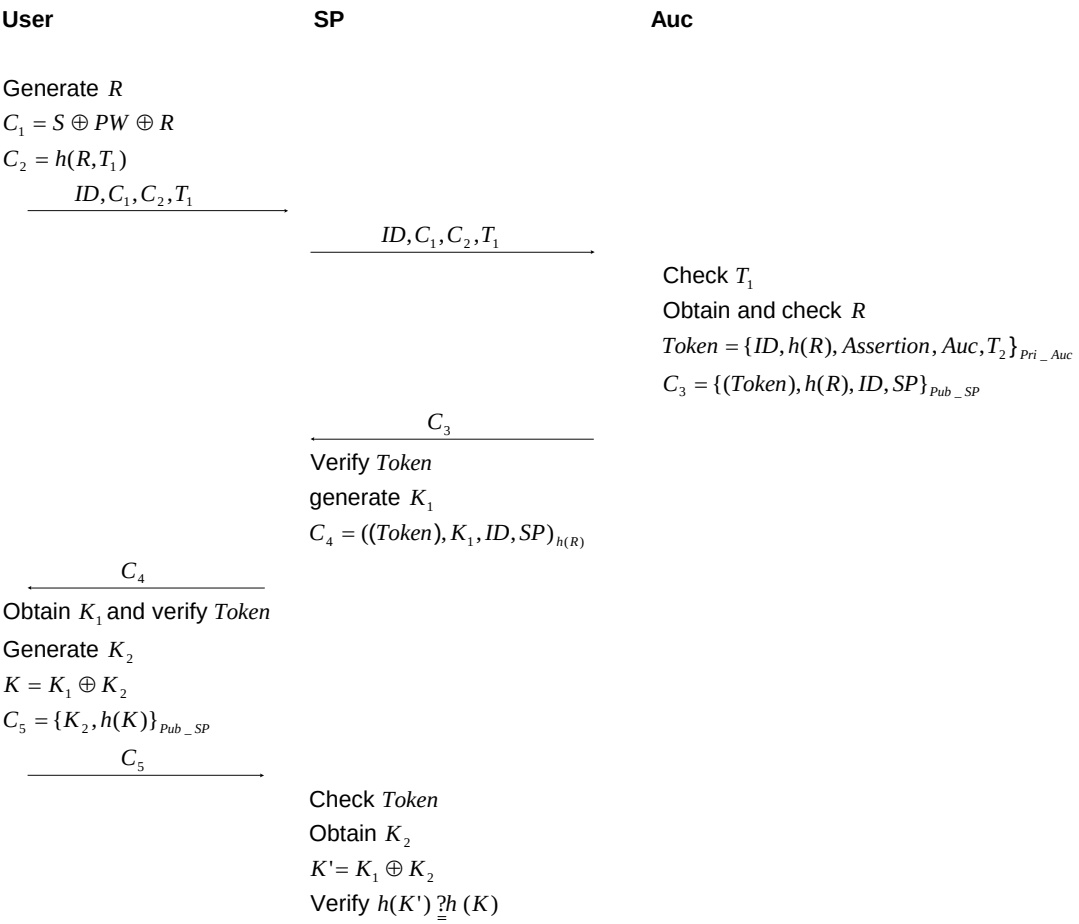

Fig.2. The login steps of the smart card based mobile single - sign - on system

After receiving C_5, the service provider obtains K_2 and the service provider can obtain session key *K*' by

$$K' = K_1 \oplus K_2 .$$

Finally, the user will be authenticated if $h(K) = h(K')$. Hereafter, the user and the service provider can communicate securely with session key *K*. For illustration, the login steps are shown in Fig.2.

3.2.2 User logins to another service provider

If the user wants to login another service provider (SP') for service, the procedures are as follows:

Step L.7. U→SP': C_6

The user generates a new partial session key K_1' and sends C_6 to the service provider, where

$$C_6 = (Token, K_1', ID, SP')_{pub\_SP'}$$

Step L.8. SP'→U: C_7

After receving C_6, the service provider recovers $(Token, K_1', ID, SP')$ and checks *Token*. The service provider generates another partial session key K_2' and obtains session key by

$$K' = K_1' \oplus K_2' .$$

SP computes and sends C_7 to the user, where

$$C_7 = (K_2', h(K'))_{h(K_1')} .$$

After receving C_7, the user recovers $(K_2', h(K'))$. The service provider is authenticated if $h(K') = h(K_1' \oplus K_2')$. Thereafter, the user and the service provider can communicate securely with session key *K*'. The login steps for another services are shown in Fig.3

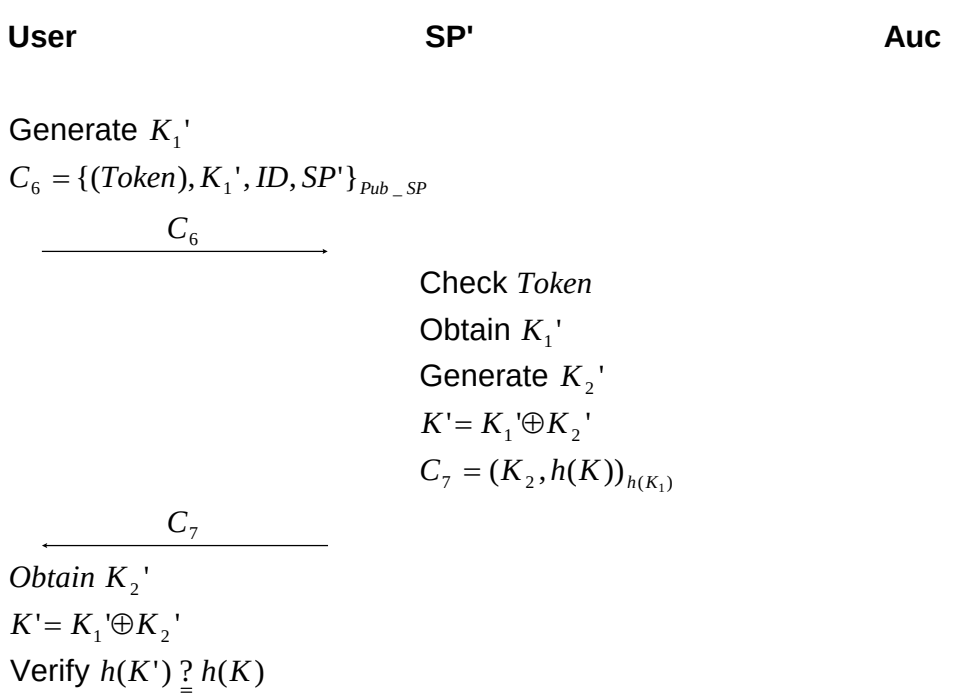

Fig.3. The login steps for other service of the single - sign - on system

3.3 Security analysis

The proposed smart card based single-sign-on system is very simple and has merits as follows:

(1)*Adversary cannot know secret x of Auc*. Since smart card is a tamper-free device, the adversary cannot obtain *x* by reading data out or other means from it. Moreover, because C_1 and C_2 come from *R*, *x*, and T_1 with hash functions, *R* and *x* have at least 128 bit length, therefore, the adversary cannot obtain *x*. If adversary wants to obtain *R* from C_2 and then using *R* to find *x*, it is infeasible due to the long bit length of *R*.

(2)*Adversary cannot masquerade as a legal user to login the system.* Since $C_1 = h(ID \oplus x) \oplus R$ and $C_2 = h(R, T_1)$, without knowing *x*, the adversary cannot forge C_1 and C_2 consistently for a successful login. Similarly, due to $K = K_1 \oplus K_2$ and K_1 cannot be obtained from C_4, the adversary cannot forge C_5 for authentication. Thus the adversary cannot login the system.

(3)*It can resist on-line password guessing attacks*. If the adversary uses a stolen smart card to login, the probability for a successful login is $p = 2^{-|PW|}$ which is quite low, where $|PW|$ denotes bit length of the password. If the attacker continues to guess the password, the server will reject the illegal attempt by limiting the number of fail trials. If the adversary has no smart card, as described in (2), he/she cannot forge C_1 and C_2 to login the system.

(4)*It can resist off-line password guessing attacks and protect the smart card*. In general, the off-line guessing attack can be avoided if there are no enough messages for the attacker to verify his/her guessing. The attack falls into either of the following cases:

(a) *The attacker has no smart card*. Since *R* and *x* are unknown, an attacker cannot generate C_1 and C_2 consistently to masquerade a legal user. That is, the scheme can withstand off-line guessing attacks when attackers have no smart card.

(b) *The attacker has stolen or somehow obtained a smart card*. If an adversary obtains smart card, he/she tries to guess password off-line. Because *R* is a random number changed on each login session, C_1 and C_2 are renewed on each session even if the timestamp remains the same. If an attacker obtains the smart card and knows C_1 and C_2 at a previous successful login, he/she still cannot verify his/her guess because C_1 and C_2 are changed on each trial. That is the adversary cannot know his guessing is right or wrong. Thus our new scheme can resist off-line password guessing attacks and protect the cardholder even if the smart card is lost.

(5)*It can resist replay attacks*. Since both C_2 and *Token* include timestamps, the server can detect replay attacks if an attacker resubmits an intercepted message. The nonce can also be used to resist the replay attack.

(6)*It does not require any password verification table*. For an authentication system with a verification table, a hacker usually attacks the system by obtaining or modifying the verification table. The proposed scheme can resist such attacks since there is no verification table at the server end.

(7)*It can resist service provider impersonate attack.*

In the system, *Token* is signed by Auc and only known by Auc, SP, and the user, the adversary cannot forge C_6 for a successful login. Moreover, since *ID* is included in the *Token*, the service provider cannot impersonate a legal user to login other SPs even though he knows user's *Token*.

4. The passwords-based mobile single-sign-on system

In the proposed password based mobile single-sign-on system, users need no smart cards and it provides users to login networks only by passwords. There is a password verification table in Auc. The registration phase and login phase are as follows.

4.1 Registration phase

In this system, the user should also register to Auc beforehand. The user sends his/her ID and password to Auc for registration. After registration, the user and the authentication center share the common password *PW*.

4.2 Login phase

4.2.1 User login to some service provider

When user asks for services from a service provider, the login phase is as followings.

Step L.1. U→SP: C_1

The user inputs password, and generates a random number *R*. Next, he/she computes C_1 by

$$C_1 = \{ID, SP, PW, R, T_1\}_{pub\_Auc}$$

Note that the random number *R* is updated on each login session. Next, the user sends C_1 to the service provider.

Step L.2. SP→Auc: C_1

The service provider cannot decrypt C_1, and he/she can only forward the message to Auc. Step L.1 and L.2 can be combined to one step that user directly sends C_1 to Auc.

Step L.3. Auc→SP: C_2

After receiving C_1, Auc obtains (ID, SP, PW, R, T_1). Then Auc generates a *Token* and sends C_2 to the service provider if password (ID, SP, PW, T_1) is verified, where

$$Token = \{ID, h(R), Assertion, Auc, T_1\}_{pri\_Auc},$$

and

$$C_2 = \{Token, h(R), ID, SP\}_{pub\_SP}.$$

Step L.4. SP→U: C_3

After receiving C_2, the service provider will obtain $(Token, h(R), ID, SP)$. Then the service provider generates a partial session key K_1 after *Token* is verified. The service provider computes and forwards $C_3 = (Token, K_1, ID, SP)_{h(R)}$ to the user.

Step L.5. U→SP: C_4

After receiving C_3, the user recovers *Token* and K_1 with $h(R)$. Then the user generates another partial session key K_2 after *Token* is verified. The user obtains the session key *K* by

$$K = K_1 \oplus K_2$$

Then the user sends C_4 to the service

provider, where

$$C_4 = (K_2, h(K))_{pub\_SP}$$

After receiving C_4, the service provider obtains K_2. With the partial session key K_1 generated previously and the received partial key K_2, the service provider will obtain session key *K*' by $K' = K_1 \oplus K_2$.

Finally, the service will be provided if $h(K) = h(K')$. Thereafter, the user and the service provider can communicate securely with session key *K*. For illustration, the login steps are shown in Fig.4.

4.2.2 User logins to another service provider

If the user asks for another service provider SP' for service, the procedures are the same as the smart card based system.

4.3 Discussions

Like the smart card based single-sign-on system, the proposed password based mobile single-sign-on system also has the advantages as follows:

(1)*It can resist on-line password guessing attacks*.

Since $C_1 = \{ID, SP, PW, R, T_1\}_{pub\_Auc}$, the attacker should guess password *PW* to obtain C_1 for a successful login. The probability to guess password is only $p = 2^{-|PW|}$. If an attacker continues to guess the password, the Auc will

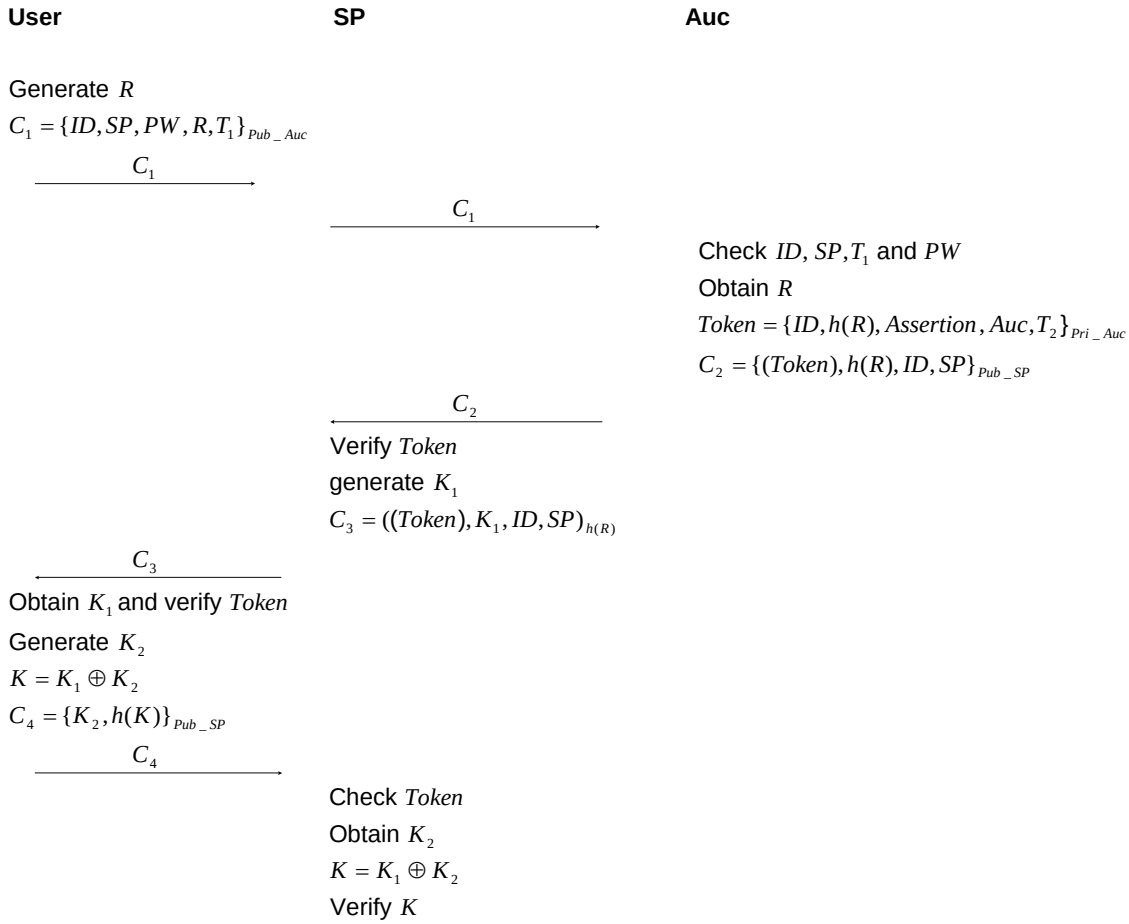

Fig.4. The password based mobile single - sign - on system

reject the illegal attempt by limiting the number of fail trials.

(2)*It can resist off-line password guessing attacks*. Since *R* is renewed and thereby C_1 is changed in each login session, the attacker cannot verify his/her guess even he/she intercepts message at the previous login session. Thus our new scheme can resist off-line password guessing attacks.

(3)*It can resist replay attacks*. Since both C_1 and *Token* include timestamps, the server can detect replay attacks if an attacker resubmits an intercepted message. The timestamp can be replaced with nonce to resist the replay attack.

(4)*It can resist service provider impersonate attack.* Since *ID* is included in the *Token*, the service provider cannot impersonate a legal user to login other SP though he knows user's *Token* after a successful login.

(5) *No smart card is needed in the system*. The proposed system only uses password for authentication, it is simple and low cost for single-sign-on systems.

5. Conclusions

We have proposed two new single-sign-on systems with the merits of mobility and resisting password guessing attack. The first system uses smart cards, and the second one uses passwords. The smart card based system doesn't need password verification table and can resist smart stolen attack, the password based system is both simple and easy to use for users.

Acknowledgements

This work was supported in part by the National Science Council of the Republic of China under the contract number NSC 95 - 2221 - E - 274 - 012

References

[1] H.Y. Chien, J.K. Jan, and Y.M. Tseng, "An efficient solution to remote authentication: smart card", Computers & Security, Vol.21, No.4, 2002, pp.372-375.

[2] M.S. Hwang, C.C. Lee, and Y.L. Tang, "A simple remote user authentication scheme", Mathematical and Computer Modeling, Vol.36, 2002, pp.103-107.

[3] T. Kwon and J. Song, "Efficient and secure password-based authentication protocols against guessing attack", Computer Communications, Vol.21, 1998, pp.853-861.

[4] C.J. Mitchell and A. Pashalidis," A taxonomy of single sign-on systems", ACISP 2003, LNCS 2727, pp.249-264.

[5] A. Pashalidis and C. Mitchell, "Using GSM/UMTS for Single Sign-On", Joint First Workshop on Mobile Future and Symposium on Trends in Communications, 2003. SympoTIC '03. Oct. 2003, pp.138-145.

[6] M. Peyravian and N. Zunic, "Methods for protecting password transmission", Computer & Security, Vol.19, No.5, 2000, pp.466-469.

[7] H.M. Sun, "An efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, Vol.46, No.4, 2000, pp.958-961.

[8] W.H. Yang, and S.P. Shieh, "Password authentication schemes with smart card", Computer & Security, Vol.18, No. 8, 1999, pp. 727-733.

[9] G. Zhao, D. Zheng, and K. Chen, "Design of Single Sign-On,", IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), pp. 253-256, 2004.