An SMS - Based One - Time - Password Scheme with Client - Side Validation

Jing-Jang Hwang[a], Yi-Chang Hsu[b],Gen-Yih Liao[*, a]
[a] Department of Information Management
Chang Gung University, 259 Wen-Hwa 1st Road
Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.
[b] Graduate Institute of Business and Management
Chang Gung University, 259 Wen-Hwa 1st Road
Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.
jjhwang@mail.cgu.edu.tw (Jing-Jang Hwang), m9244107@gmail.com (Yi-Chang Hsu), gyliao@acm.org (Gen-Yih Liao).

Journal of Digital Information Management

ABSTRACT: *Prior to accepting and executing an online transaction, e-commerce systems must allow the consumer to express an informed and deliberate consent to the transaction. Currently, a widely accepted way of letting the consumer express his consent to execute a transaction is the Short Message Service-based One-Time Password (SMS-based OTP) scheme. In this scheme, when the system receives the required and unambiguous information for an on-line transaction from a consumer, it sends a short message containing a one-time password to the consumer's mobile phone. The consumer expresses his consent by entering the password on his client device which then sends the entry back to the system for confirmation. Although the one-time password can prevent the password from unauthorized reuse, an attacker can still launch a series of password guesses that finally leads to either a successful attack or account suspension. This paper presents a system design to improve the SMS-based OTP scheme by enabling the client device to verify the correctness of the OTP entry. In this scheme, a password entry is sent to the system only if it is correct and captured within the permitted time interval. In terms of security, the new feature not only reduces the risk of successful guessing attacks, but also alerts the system to take necessary defensive measures against possible cyber attacks whenever an incorrect or expired OTP entry is received by the system. A quantitative analysis revealed the relative benefit of the proposed scheme.*

Categories and Subject Descriptors
D.4.6 [Security and Protection]; Access Control**: H.2.0 [Database Management]:** Security, integrity, and protection

General Terms: Security, Passwords, Access Control, Short Messaging Service

Keywords: E-Commerce, Transaction Confirmation, One Time Password, Short Message Service, Client-Side Verification on Password Entry

Received: 14 December 2014, Revised 19 January 2015, Accepted 24 January 2015

1. Introduction

E-commerce transactions require confirmation on both of the consumer's intent to execute a given transaction and the content of that transaction. The Organization for Economic Development (OECD) has provided clear guidelines: "*To avoid ambiguity concerning the consumer's intent to make a purchase, the consumer should be able, before concluding the purchase, to identify precisely the goods or services he or she wishes to purchase; identify and correct any errors or modify the order; express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction* [1]."

When the consumer clearly understands the transaction content (e.g., product details, price, payment method, and shipment date and location), he approves the transaction by entering a password that is known to him and can be authenticated on the system side. This is a widely-used and important step in the confirmation process. When the system receives the correct

authentication password, it signifies that the consumer has confirmed the transaction content and agrees to execute the transaction.

The transaction password is chosen by the consumer and recorded on the system side [2]. Generally speaking, the consumer uses his chosen transaction password for a while before changing it, and there is a risk of the password being guessed, overheard or surreptitiously recorded by others [3].

To improve security, many e-commerce systems already use a One Time Password (OTP) transaction confirmation mechanism, especially for transactions with higher financial risks, such as Internet Banking transactions involving changes to client account balances [4]. Lamport presented the concept and the first method for OTP in 1981 [5]. Currently there are two main types of OTP mechanism. In the first type, when a consumer has already provided the unambiguous information required for a transaction and intends to proceed with the transaction, he reads an OTP from a "Password-Generation Token" and, within a set time, enters the OTP into his client-side device and transmits it to the system side. In the second type, when the consumer has confirmed the transaction content and requested the system to process the transaction, the system generates an OTP and then sends it to the client's cell phone via Short Message Service (SMS). The consumer must then, within a set time, enter the OTP into his client-side device and transmit it back to the system.

Figure 1 shows examples of the token – a type of off-line devices – used in the first method. When a person needs an OTP, he presses the button on the token, and the token's LCD screen shows a new password for him to use. The principle behind the OTP produced by this type of off-line tokens has already been theoretically verified [6, 7, 8]. The drawbacks to this method are the high cost and the need to carry the token on one's person if it is to be used in different places. Software tokens have been developed which install a software code on the consumer's cell phone [9], and the wide availability of cell phones overcomes the portability problem. However, software tokens are subject to intellectual property licensing which restricts uptake.

The second method is the SMS-based OTP scheme, which avoids the complications Inherent in the off-line synchronization technology required in the token-type approach. Costs are kept low because there is no need for a physical token. In addition, the Short Message Service's transmission route by which the OTP message is transmitted to the cell phone is different from the communication route through the Internet by which the client and the system side exchange messages in an e-commerce process. Using separate communication routes further reduces the risk. As a result, the SMS-based OTP mechanism has come to be seen as an inexpensive and secure option. Oppliger et al. extensively discussed client side

SafeNet eToken Pass

EMC RSA SecurID (USA)

Figure 1. Password Generators

risks and noted that the SMS-based OTP scheme offers some fairly obvious advantages when it comes to protecting the client-side from attack [10].

The SMS-based OTP scheme has potential to become mainstream but there is room for improvement both in terms of user convenience and security. For example, a consumer may enter the OTP incorrectly, either because he misread the SMS containing the OTP or mistakenly pressed a wrong key, or he may be too slow in entering the OTP. Whatever happens, the system side would reject his OTP entry, which would normally require the transaction confirmation process to be repeated. If the transaction confirmation fails a certain number of times, the system side will reject any further confirmation attempts. Most security rules have a threshold for the number of failed attempts allowed to confirm a single transaction and, when this threshold is crossed, the system will suspend the consumer's account privileges, requiring the consumer to verify his identity in person at a service location before the account can be re-activated.

It's worth noting that if this threshold is set to 1, when a consumer times out or enters a wrong OTP the system side will suspend the user's account. This lack of tolerance for user error not only places an unreasonable psychological burden on the consumer, but also increases customer service costs.

Setting the threshold to more than 1 leads to two possible variations. First, when the system determines that that OTP entry is invalid either because the entry is incorrect or late, it will send a new OTP SMS to the consumer's cell phone, requesting the consumer try again using the new OTP. This variation of the mechanism can reduce the risk of system hacks, but is inconvenient for users, especially for users with disabilities which make it difficult for them to read text messages or use a keyboard. The second variation is that the system side only returns an error message indicating that the OTP input was incorrect, and requests the consumer to input the correct OTP. This way, the consumer is not required to obtain a new OTP, but it does provide an opportunity for guessing attacks.

Generally speaking, an incorrectly entered password will by mostly correct, and an attacker can assume that he only needs to change one or two input characters to derive the correct OTP. Given that the transaction conformation has only failed once, the attacker still has [threshold setting – 1] chances to attempt a guessing attack. Under these conditions, the probability of a successful guessing attack is considerably higher than a random guess with no information about the secret.

Given the above, the current SMS-based OTP mechanism has several aspects in need of improvement.

This study proposes an improved SMS-based OTP scheme, which adds a feature allowing the client device to authenticate the consumer's OTP entry locally. The client device can immediately determine whether the inputted OTP entry is valid or invalid (i.e., if correct and captured within the permitted time limit), and thus provides the user with greater convenience. The improved mechanism only transmits the OTP to the system side after it has locally been confirmed to be valid, thus making it impossible for an attacker to intercept or successfully guess the OTP, and ensuring that the consumer's account won't be suspended for entering an incorrect OTP or for taking too long to complete the input, thus improving user convenience. In addition, if the system side receives a late or incorrect OTP entry, the system can deduce that it may be under attack and take appropriate defensive measures, thus providing the system with extra security.

2. The SMS-based OTP Scheme: the State-of-the-art

This section describes the process of implementing the current SMS-based OTP scheme. Functionally, this is a transaction confirmation process; in other words, it allows the consumer to deliberately express his consent to the execution of the transaction.

The process begins when the system obtains the unambiguous information required for a transaction and the consumer has checked the information for accuracy. To initiate the transaction confirmation process, the consumer instructs his client device to send a message to the system to express his intention. Upon receiving the message, the system generates a random number as an OTP. Next, the system transmits the OTP to the consumer's cell phone by SMS, with a prompt on the client device for the consumer to enter the OTP and transmit the OTP back to the system within a time limit for authentication. The system decides if the received OTP is correct and within the time limit. A positive decision implies that the consumer has given the e-commerce merchant a confirmation.

The time limit used here is determined by a tradeoff between consumer convenience and system security. For example, the Standard Chartered Bank's Internet banking service sets its time limit at five minutes [11], while other banks use a longer time limit to allow their consumers greater convenience.

Figure 2 shows an exemplary process using the SMS-based OTP scheme [12]. In the figure, the dashed arrow denotes the SMS "message route". Of course, in SMS, the message route uses the mobile phone as the means of communication, as opposed to e-commerce processes which use the Internet. The current trend is to merge mobile phone communications and computer communications into a single combined infrastructure, and mobile phones are increasingly becoming Internet client-side devices. However, the routes used by SMS and e-commerce message transmission are expected to remain distinct.

The client-side device is usually the consumer's PC, but it could also be the mobile phone on which he received the SMS. The mobile phone number must be known to the system. This number can be provided when the consumer first registers with the system or at any time prior to the initiation of this confirmation process.

The flowchart in Figure 2 shows that, after the system has transmitted the OTP SMS, it immediately transmits to the client device a prompt to inform the consumer to receive the SMS from his mobile phone and return the OTP to the system side via his client device. This prompt message and the return OTP entry are transmitted through an Internet communication route already established between the client side and system side, which is different from the route used to transmit the OTP SMS.

At the client side, the consumer follows the prompt to read the OTP from the SMS, enter the OTP in his client side device and transmit it back to the system side.

If the time limit has not expired when the system receives the returned OTP entry, the system compares the "*received OTP entry*" and the "*previously-generated OTP*". Only if the two values match will the transaction be executed. (Upon the completion of execution, the number of failed confirmation attempts is reset to zero). If the time limit has already expired when the returned OTP is received, or if the received OTP entry and the previously generated OTP do not match, the system will normally prompt the consumer to re-initiate the confirmation process. However, if the number of failed attempts has already exceeded the assigned threshold, the system will refuse to continue the process.

According to the transport protocol for SMS, the SMS message is transmitted in an encrypted manner [13], thus providing additional security. Nevertheless, the main security advantage of the SMS-based OTP scheme is that the password is limited to a single use within a restricted time period, thus preventing the password from unauthorized use.

In the exemplary process shown in Figure 2, the OTP entry time control is carried out on the system side; alternatively, some e-commerce merchants move this step

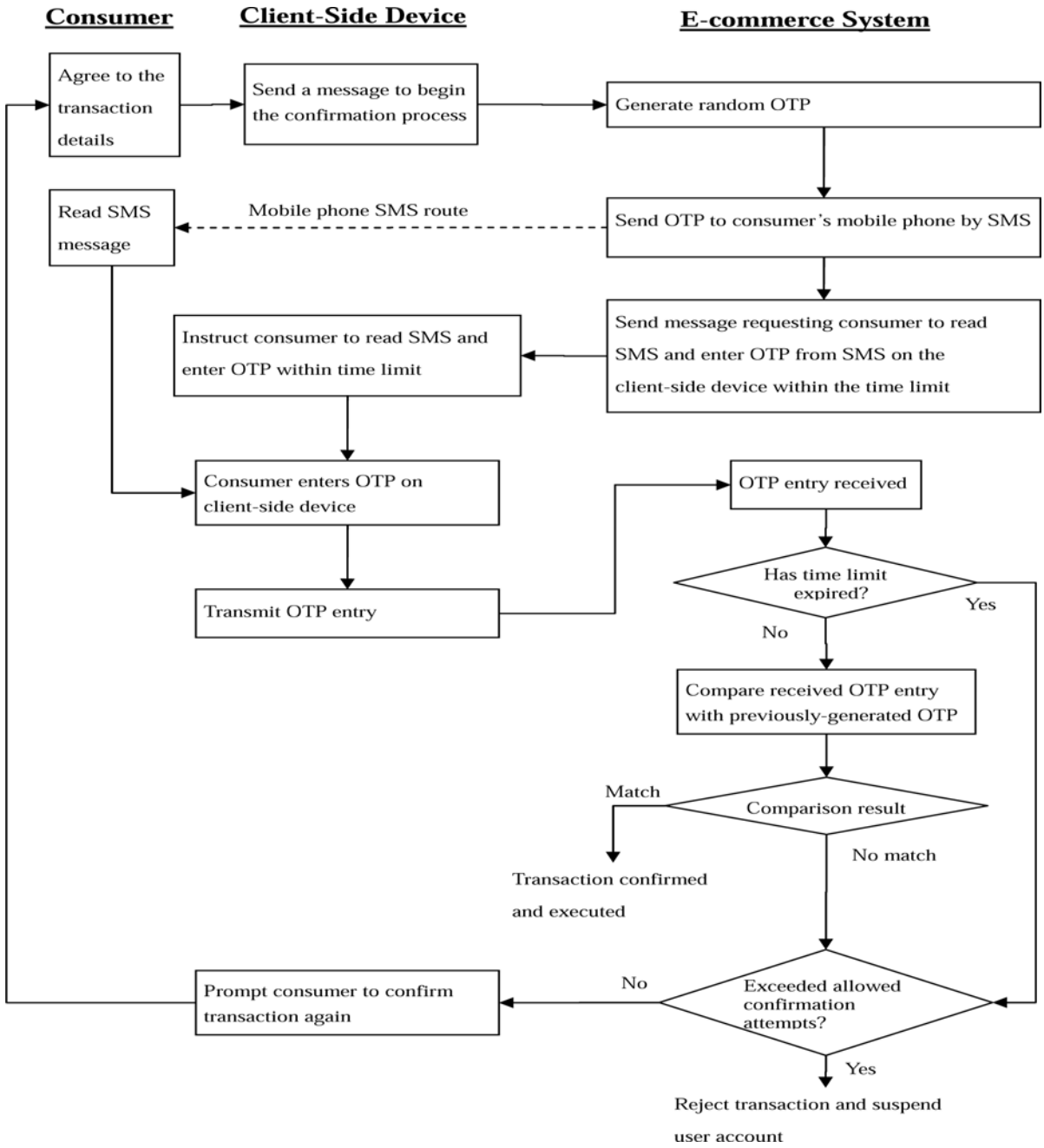

Figure 2. Process using the SMS-OTP scheme

to the client side. In contrast, the state-of-the-art only allows the correctness of the OTP to be validated on the system side. No client-side methods have been published in the relevant literature.

This research is primarily concerned with the design of an instantaneous client side method for ensuring the correctness of the OTP entry, and also recommends that time control be moved to the client side. The improved design offers users greater convenience and improves security.

3. Client-side Validation

Our improved scheme adds an OTP Transformation step on both the system and client sides. On the system side, the input to the OTP Transformation is the randomly generated OTP, and the output of the transformation becomes a "*substitute of the system-side OTP*". This output is transmitted to the client device via the Internet route already established in the present e-commerce process. On the client device, the input to the OTP transformation is the inputted OTP entry, and the output becomes a "*substitute of the client-side OTP entry*". The client device compares these two substitutes. If they match, the OTP entry is correct and can be transmitted to the system. Otherwise, the consumer is prompted to enter the OTP again.

For the sake of security, the OTP Transformation must meet the following conditions: (1) Disclosure of the "*substitute of the system-side OTP*" must not reveal clues to the actual OTP and, (2) with different inputs, the OTP Transformation's output must not be repeated.

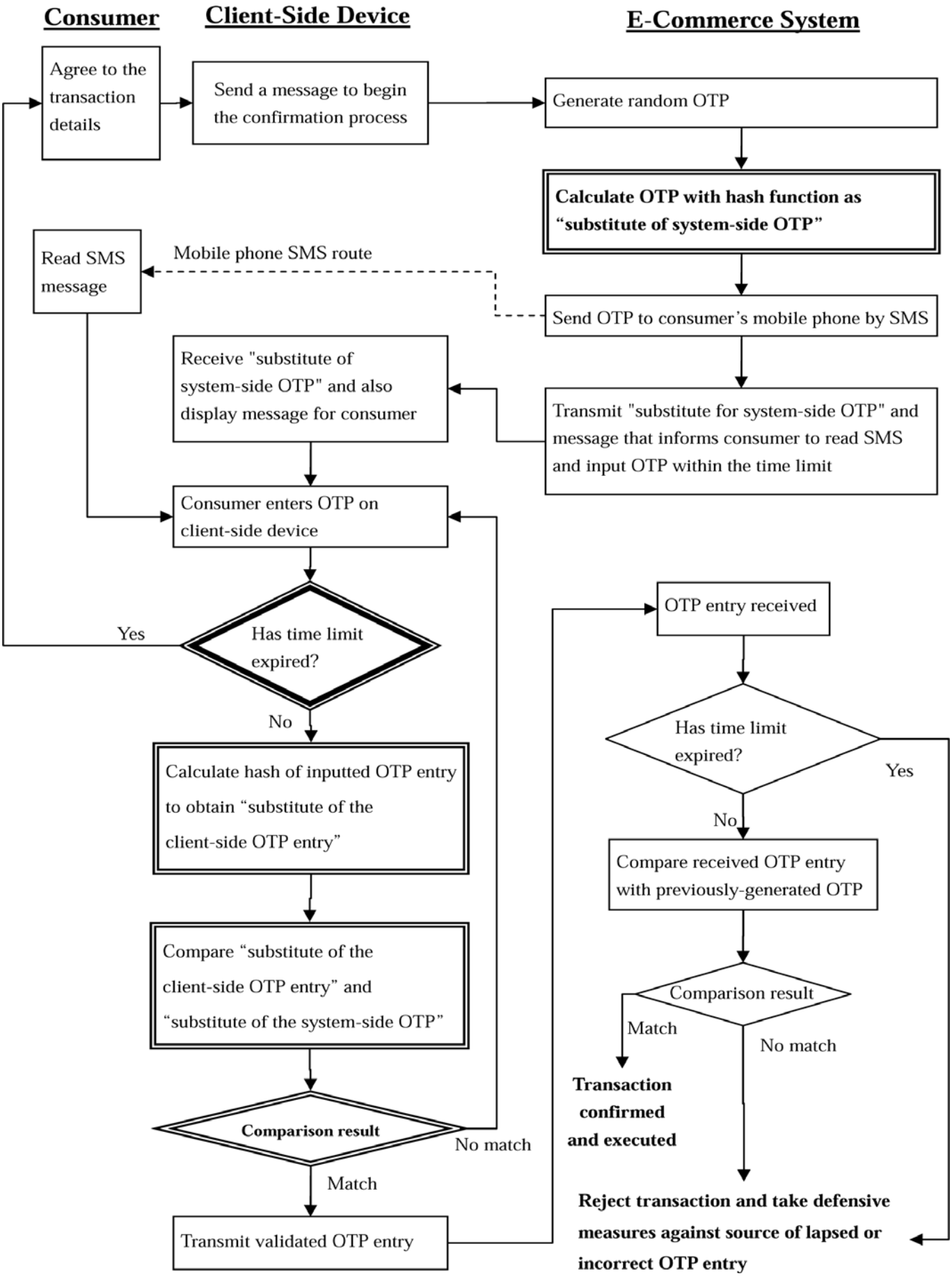

Figure 3. Adding Client-Side Device OTP Entry Check To The SMS-Based OTP Transaction Confirmation Procedure

The OTP Transformation can be implemented with a hash function.

Hash functions are deterministic (i.e., non-probabilistic), meaning that the output is completely determined by the input. The hash function of implementing the OTP Transformation should be collision-resistant, meaning that it is extremely difficult to find two distinct inputs that could produce the same output. A collision-resistant hash function also has the desired property of being one-way; this means that, given an output, it is very difficult to find an input whose hash value is the specified output).

The one-way characteristic of hash functions can ensure that disclosure of the "*substitute of the system-side OTP*" will not lead back to the actual OTP. The collision-resistance implies that a match between the "*substitute of the system-side OTP*" and the "*substitute of the client-side OTP entry*" indicates that the OTP entry inputted by the consumer is correct.

Figure 3 illustrates the application of hash functions to improve the current SMS-based OTP transaction confirmation procedure.

To clearly illustrate the differences between the improved mechanism and the current scheme (as described in Section 2 and illustrated in Figure 2), Figure 3 uses double-line frames to show the added steps, including (1) a system-side step to calculate the "substitute of the system-side OTP, (2) client-side check for the time-validity of the OTP entry where a late entry prompts the consumer to re-initiate the process, and (3) assuming timely consumer OTP entry, steps for client-side calculation of the "*substitute of the client-side OTP entry*" and OTP entry verification.

Our improved scheme compares two substitute values to authenticate the user entry on the client-side device. These substitute values are designed with consideration of security. As for the timeout check, timekeeping techniques commonly found in web applications can be adopted here. As a result of our design, the client-side device is only able to transmit correct and valid OTP entries to the system. If the system receives an expired OTP entry, or if the received OTP entry is incorrect, the system can infer that it is under attack and can take appropriate countermeasures. The remaining steps of our scheme are described in Section Two and illustrated in Figure 3, and are therefore not repeated here.

4. Benefit, Cost, and Security Enhancement

This section provides an analysis on the advantages and cost of the proposed method. In terms of security, this improved scheme avoids giving hackers an opportunity to mount an attack based on guessing the OTP, because the communication between the client-side device and the e-commerce system need not be repeated as a result of user error. Furthermore, this OTP entry verification on the client side provides another security advantage in that, if the system fails to re-validate the user's OTP entry, it can infer that it is under attack and can take appropriate counter measures. To quantitatively compare the likelihood of a successful attack in our design with that in existing systems, we provide an analysis as follows:

(1) The likelihood of a successful attack in existing systems is $O(E \times G)$, where E represents the number of error inputs by a user and G stands for the number of guesses that an attacker can issue in a unit time. That is, the longer a user makes erratic inputs, the more time in which an attacker can issue guesses; these two factors determine how likely the attack can succeed (without considering the usual security policy of limiting the number of user inputs).

(2) The likelihood of a successful attack in our proposed design is constant (i.e., $O(1)$); if an attacker fails in the first attempt, the server will recognize an attacking state and stop processing.

In addition to the advantages with regard to security, the improved scheme offers obvious advantages in terms of ease of use. The user can immediately see if his OTP entry is late or incorrect without involving system-side determination. This ensures that the user won't have to deal with the potential inconvenience of account suspension due to inadvertent input errors or timeouts.

One question that could be raised is this: is it possible that the consumer inputs a correct OTP entry, but the entry is unable to pass through the validation process on the client-side device? Given the transmission quality of today's TCP/IP-based Internet, the probability of data packet loss or transmission error is already very low. Moreover, e-commerce sites all use Secure Sockets Layer (SSL) and other means for secure communication to ensure data integrity. Thus, failure caused by transmission errors can be ruled out. If, in fact, a correct OTP entry cannot pass, the consumer can be notified that his client side device may be experiencing a hardware or software failure and thus requires repair.

This improved scheme adds a hash function to both the system-side and client-side implementations. Not only are hash functions a well-understood information security technique, but they are a computational efficiency algorithm with open source code available. For example, the system and client sides of the above-mentioned SSL can be each equipped with a hash function [14, 15], and so can the general password login process [16]. Therefore, given current data security practices, the cost of adding the hash function is negligible. However, selection of a secure hash function is essential, and those hash functions in which weaknesses have been found must be avoided. Also, security professionals should monitor the SHA-3 (Secure Hash Algorithm-3) competition presently being held by the US's National Institute of Standard and Technology (NIST) and update their understanding of hash

functions accordingly [17].

5. Conclusion

According to a 2010 survey by the International Telecommunication Union (ITU), there were 4.6 billion mobile phone users globally at the end of 2009, and 90% of the world's population live within range of a mobile network [18]. A similar survey by Goode Intelligence suggests that products and services related to SMS-based OTP schemes will experience quick growth [19].

This study makes a fundamental improvement to the current SMS-based OTP scheme. The improvement inherits benefits from the current scheme including: transaction risks are reduced through the use of two different data channels, OTP generation and authentication are simplified, consumers do not require an off-line hardware token, and e-commerce providers are able to serve a broader clientele. The proposed client-side validation builds on these advantages by providing consumers with greater convenience while simultaneously strengthening security for the transaction system.

Acknowledgement

We are grateful for the support of the National Science Council of Taiwan Government (Project Number NSC 99-2410-H-182 -025 -MY2)

References

[1] Organisation for Economic Co-operation and Development (OECD). Recommendation of the OECD council concerning guidelines for consumer protection in the context of electronic commerce, http://www.oecd.org/dataoecd/18/13/34023235.pdf, accessed March 2011

[2] Claessens, J., Dem, V., Cock, D., Preneel, B., Vandewalle, J. (2002). On the security of today's online electronic banking systems, *Computers & Security*, 21, (3) 257-269

[3] Clarke, N. L., Furnell, S. M. (2005). Authentication of users on mobile telephones - a survey of attitudes and practices, *Computers & Security*, 24 (7), 519-527

[4] Alzomai, M., Alfayyadh, B., Jøsang, A., Mccullagh, A. (2008). An experimental investigation of the usability of transaction authorization in online bank security systems'. Proceedings of the sixth *Australasian conference on information security* (AISC 2008), p. 65-74

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

[6] Weiss, K. P. (1989). Method and apparatus for synchronizing generation of separate, free running, time-dependent equipment'. US Patent 4885778, December.

[7] Weiss, K. P. (1997). Method and apparatus for utilizing a token for resource access'. US Patent 5657388, August

[8] Margalit, Y., Margalit, D. (2004). User-computer interaction method for use by a population of flexibly connectable computer systems', US Patent 6748541, June

[9] Aloul, F., Zahidi, S., El-Hajj, W. (2009). Two factor authentication using mobile phones, *In*: Proceedings of the IEEE/ACS international conference on *computer systems and applications* (AICCSA 2009), 2009, p. 641-644.

[10] Oppliger, R., Rytz, R., Holderegger, T. (2009). Internet banking: client-side attacks and protection mechanisms, *Computer,* 42, (6) 27-33

[11] Standard Chartered Bank. Frequently asked questions - is it safe to use the personal online banking service?, http:// http://www.standardchartered.com.tw/en/etc/cs_fq.asp?Page=2#Q5, accessed March 2011

[12] Alzomai, M., Alfayyadh, B., Josang, A. (2010). Display security for online transactions: SMS-based authentication scheme'. Proceedings of the international conference for Internet technology and secured transactions 2010 (ICITST 2010), p. 1-7

[13] Lo, J. L., Bishop, J., Eloff J, H, P. (2008). SMSSec: an end-to-end protocol for secure SMS, *Computers & Security,* 27, (5-6) 154-167

[14] Rescorla, E.: 'SSL and TLS: designing and building secure systems' (Addison-Wesley, 2001, 1st edn.)

[15] Shoriak, T.G. (2000). SSL/TLS protocol enablement for key recovery', *Computers & Security,* 19 (1) 100-104

[16] Simpson, W. (1996). PPP Challenge handshake authentication protocol (CHAP), RFC 1994, 1996

[17] http://csrc.nist.gov/groups/ST/hash/sha-3/index.html, accessed March 2011

[18] http://www.itu.int/ITU-D/ict/material/

Facts Figures2010.pdf, accessed March 2011

[19] http://www.goodeintelligence.com/pdfs/The Mobile Phone As An Authentication Device Analys Report_Release.pdf, accessed March 2011