Password Generation of OTP System using Fingerprint Features

ByungRae Cha, ChulWon Kim
Dept. of Computer Eng., Honam Univ.,
Korea

E-mail: {chabr, cwkim}@honam.ac.kr

Abstract

Security of internet is becoming the latest important concerns along with extensive application of the Internet. All elements that compose security system over maliciously action can display the performance though accomplish harmony of security elements perfectly. Weakness of some a part causes fatal result to whole security system. Therefore, Security systems need elaborate design and mutual coordination in each elements. In this paper, we propose the method of one time password key generation of OTP using fingerprint features. Fingerprint is powerful personal authentication factors, and it can create variable password key for one time using information of fingerprint features. And we performed a simulation for proposed password key generation method.

1. Introduction

Internet security is recently becoming an important issue with the increasingly wide range of Internet applications. However, since the Internet is an open network, it is weak to various attacks such as system intrusion and tapping, etc. Transmitted information level is becoming more important especially as interactions that used to only be carried out offline, such as bank and commercial exchanges are now being carried out online in the form of Internet banking and electronic commercial exchanges, and damages due to such attacks will be greater. User authentication is a necessary security element in the open network environment, and the use of simple authentication information has large problems. There is the problem that it is easy for attackers to guess passwords because users select their ID and password as information that is easy to memorize, or use the same password for many Web sites, and since there is a high risk of being exposed to tapping, attackers with bad intent can use this to their advantage and act as a justified user[1,2]. A authentication method that can overcome these disadvantages is a authentication method that creates one time new password each time[3,4,5]. Such one time passwords were normally used for Internet banking, but recently are also used when purchasing online games, music and videos. The demand for one time passwords is increasing, and they are being used in more diverse fields. National administration is especially strict for the security market, just like the weapons material market. The National Intelligence Service currently administrates cryptography algorithms and security use authentication. Use of foreign security equipment and foreign cryptography algorithms is currently prohibited in the national network and public networks, such as financial networks. Security systems for improper conduct can only perform when all elements of the structure create perfect harmony. A weakness in a single part creates a terminal result for the entire system, so thorough planning and cooperation is needed for each element. This study proposes creating one time passwords based on fingerprint characteristics, and presents a new OTP network model that can adopt this one time password method.

Chapter 2 of this study explains the OTP related study, and chapter 3 presents a password key creation method through extraction of fingerprint characteristics information. Fingerprints are strong authentication elements, but information on characteristics of fingerprints can create temporary one time password keys. Chapter 4 carries out a simulation adopting the presented one time password key algorithm, and lastly, draws a conclusion.

2. Related Works

2.1 Fingerprints

Biometrics is an automated method that recognizes people based on their physical and action characteristics, and is a field that used to authenticate a certain individual's characteristics, recognize a person's character, or study a per-

978-0-7695-3126-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ISA.2008.73

son's measurable characteristics[6,7]. People have unique fingerprints that do not change, and fingerprints consist of ridge and furrow parts of a finger's surface. Fingerprints can be categorized according to many key patterns that include loops, whirl pools and arches[8, 9]. Characteristics of fingerprints are decided by the minutiae point and prominence and depression. Minutiae point refers to the topical characteristic at the end point of the ridge part. The best way to compare fingerprints is to compare all visual information on the fingerprints. However, this is realistically impossible. Comparing all visual information requires too much data, and this is inappropriate to making a commercialized system. Actual commercialized systems do not store the fingerprint itself, but characteristics of the fingerprints, and codes related to the position of these points of characteristics. Since only characteristics are stored, they cannot be revived as fingerprint visuals, and therefore cannot be used as evidence in legal facilities.[6]

2.2 One Time Password

One Time Password(OTP) is a password system where passwords can only be used once, and the user has to be authenticated with a new password key each time. It is a password key creation method that makes it extremely difficult to predict the next password key based on the current password. A new password key is created in its own device constantly after a set period of time and the user has to enter a new password every time he or she uses the system, so it prevents exposure of the user's password due to hacking or the user's mistake. Compared to the existing printed security card where passwords are entered from a set range of 35, OTP has much stronger security because the user has to enter a newly created password key even if his or password is exposed. Most OTPs' password key creation algorithms are based on one-way functions (a function that cannot predict the entered value through the output value). For example, S/Key systems (RFC1760) in almost all UNIX OS use such functions[3,5]. The OTP is standardized by the IETF, and standardized again by verification related companies, and the RSA[10] camp and OATH[11] camp are carrying out the most competitive standardizations.

3 Creation of Password keys using Fingerprint Characteristics

Normally when a user requests authentication, even after first contact, certain important services confirm passwords again. However, as explained above, the existing password system has many weaknesses, and a solution for this is one time password mechanism. The elements of one time password mechanism are a token included in a security/password algorithm or one time password key creating

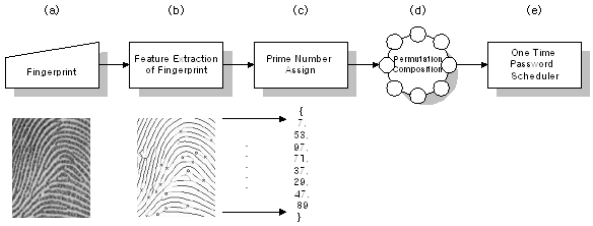

Figure 1. Password key Creation process of OTP

device(OTP token), a authentication server and a authentication client. Since the one time password mechanism is also a program, it is programmed to be random, but the randomness breaks after a certain period of time and passwords become predictable so one time password mechanisms have the disadvantage of having to exchange OTP token modules after a certain period of time. In order to overcome such weaknesses, this study presents a method of creating one time password keys in OTP Clients using fingerprint characteristics, and figure 1 shows the password key creation process. On characteristics of this study that should be focused on is that the OTP token is not positioned in the OTP Server, but on the side of the OTP Client for reduceing OTP Server's overhead.

The password key creation process starts with the user scanning his or her fingerprint, as shown in (a) of figure 1. The scanned fingerprint is not used for authentication. The range of this study starts after the authentication process is over, and is not related to authentication. However, another advantage is that it can be used together with another authentication system. Existing authentication systems can be added to this study to create a strong new OTP token. As shown in (b) of figure 1, the OTP Client can use the user's fingerprint to extract information on its characteristics. (c) of figure 1 shows the process of randomly prime number selecting characteristics points through the extracted fingerprint characteristics information. (d) of figure 1 shows the process of creating a combination of permutation using the selected prime number by order, and (e) of figure 1 shows creation of an OTP keys using the cyclic permutation. (d) of figure 1 creates temporary infinite OTP password keys for one session. Infinite temporary OTP passwords can be created because it uses the characteristics of cyclic permutation, and figure 5 shows this in more detail.

3.1 Extraction of Characteristic Points Using Fingerprints

If an OTP key is created using fingerprint characteristics, the same fingerprints will have the same characteristics each time, and the password key will always be the same. How-

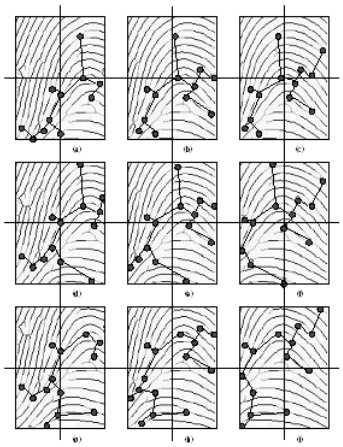

Figure 2. Characteristic Points Variation for Changed Location of Same Fingerprints

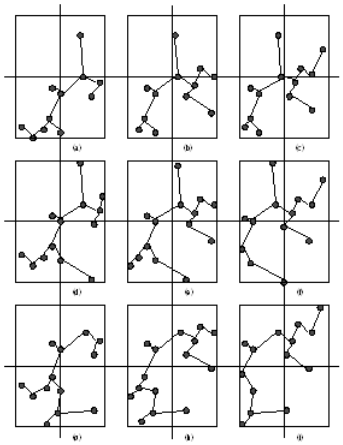

Figure 3. Variation of Characteristic Points Graph that eliminates the fingerprints

ever, this study reversely used this disadvantage and made it an advantage. Once created, person's fingerprints permanently do not change. For this reason, many authentication systems use Biometric informations such as fingerprints for authentication. In the past in the orient, when a authentication system using handwriting was not developed, stamps were used to sign most document instead of a signature. However, if you use a stamp instead of a signature, you will find that the same stamp is a little different each time. There is a slight change in location and angle of the imprinting of the stamp.

Figure 2 and 3 show the change in a graph that displays characteristic points extracted from the same fingerprints when the fingerprint is moved 3mm to the right and 3mm down. Figure 3 is a graph that eliminates the fingerprints in

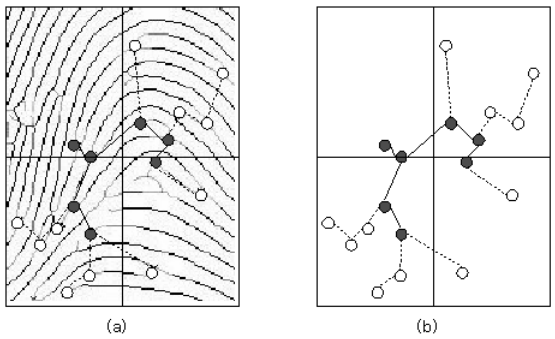

Figure 4. Variation of Graph Nodes

figure 2, to show the change of the graph more clearly. The characteristic points graph creation process starts from the closest node to the middle of the scanned screen, and creates an MST (Minimum spanning tree) graph with Prim's Algorithm.[12] Figures 2 and 3 show that even the same fingerprint has slight differences every time it is scanned. Thus, even the same fingerprint shows changes in the extracted characteristic points graph due to a change in location and angle, and create a homomorphic graph. Using this characteristic points, even the same fingerprint can be used to create different password keys each time through changes in the characteristic points graph for each scan.

(a) of figure 4 shows the extracted characteristic points graph made with 9 images from figure 2. (b) of figure 4 is (a) of figure 4 without the fingerprint images. The black node of the characteristic points graph is the part that does not change in the characteristic points graphs, and the white node expresses the node that shows node elimination or additional changes due to change in location.

3.2 Password Keys Creation using Cyclic Permutation

Random prime numbers are selected from the fingerprints characteristic points graph, and the order relation is structured as a permutation according to the MST graph search order. The password key creation of the permutation starts from the MST graph's start node and creates a password key using the graph's search order and selected points, and is expressed as in figure 5. Which permutation's element comes first is not important, order of the permutation is important.[12] If you use the randomly selected prime number list, there is a lack of password keys for the many packets that relay between the client and server that make up one session. In order to solve this disadvantage, the permutation characteristic is used and the a password key list is switched to a permutation, so a continuous cycle can create temporary infinite password keys. When one session ends, the permutation that creates pass-

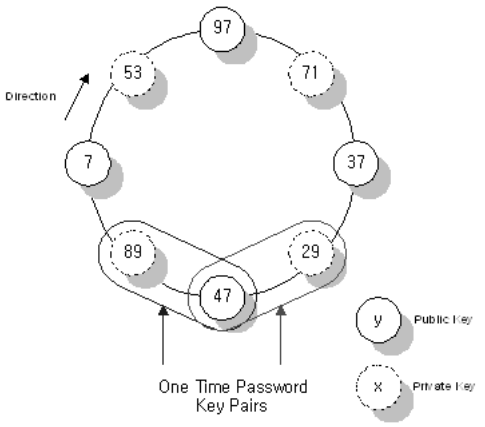

Figure 5. Cyclic Permutation for Password Keys Generation

word keys is terminated, and a new permutation is created in the next session, strengthening security. Also permutations can be expressed as a multiplication of cyclic permutations through disjoints, and this characteristic of cyclic permutations can create multiple times as many one time password couples as cyclic permutations. Password key lists that make up permutations do not have a relationship of odd or even numbers, and if the Password key couples according to permutations are divided as public keys and private keys, Public-Key Cryptography System(PKCS) characteristics can be adopted.

4 Simulation : Comparison of Distance according to Change in a Fingerprint Location

Using the 9 homomorphic graphs created with fingerprint characteristic points, 3-digit random numbers were allocated to the each node and shown in a dendogram, and the dedogram used the JMSL[13] library. Figures 6 and 7 show through the dendogram that the same fingerprint can have randomness through creation of a homomorphic graph, and shows expansion of randomness through allocation of random numbers. There is also the advantage that infinite password keys can be created for one session using a cyclic permutation structure.

5 Conclusion

Internet security is a recent important point of interest with the wide use of the Internet. Security systems against improper actions only perform well when all the parts consisted create perfect harmony. A weakness in one part can

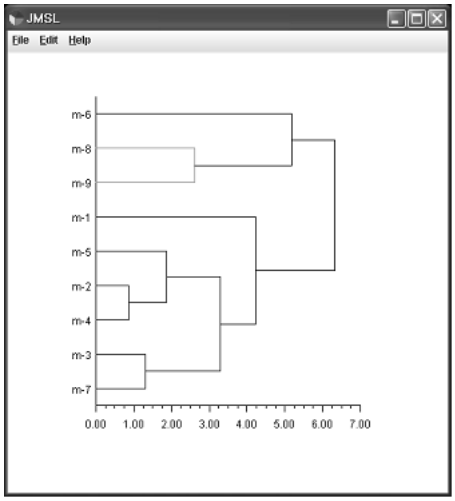

Figure 6. Dendrogram for 9 Fingerprints

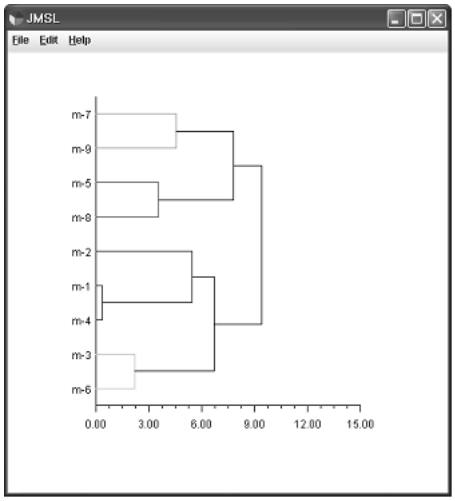

Figure 7. Dendrogram of Expansed Randomness

be terminal for the entire system, and therefore, thorough planning and cooperation is needed for each element. This study presented an OTP model with a password key creating method using fingerprint characteristics information, and an OTP model that can adopt a password key creating algorithm. The one time password key creation method created a homomorphic characteristics point graph with the same fingerprint each time, showing inconvenience of a password key. In addition, an OTP model that has the characteristic of creating password keys through OTP clients was presented, and the validity of the method was simulated.

References

[1] Ed Tittel, Mike Chapple, James Michael Stewart, "CISSP : Certified Information Systems Security Professional", Sybex , 2003.

[2] Rolf Oppliger, "Security Technologies for the World Wide Web", Artech House, 2000.

[3] Neil Haller, "The S/KEY One-Time Password System", Proceedings of the Symposium on Network and Distributed System Security, 1994.

[4] A.D. Rubin, Independent One-Time Passwords, Proc. 5th UNIX Security Symposium, USENIX Association, June 1995.

[5] N. Haller, C. Matz, P. Nesser, M. Straw, "A One-Time Password System", RFC 2289, IETF, 1998.

[6] Introduction to Biometrics, http://ics1.mk.co.kr/file/cd104/biometrics1.pdf

[7] Pankanti, S., Bolle, R. M., and Jain, A., Biometrics: The Future of Identification. IEEE Computer magazine, February, 2000.

[8] L. Hong, A. K. Jain, "Classification of Fingerprint Images", MSU Technical Report, MSU Technical Report MSUCPS:TR98-18, June 1998.

[9] Jain, A., and Pankanti, S., Fingerprint Classification and Matching. Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, April 2000.

[10] RSA, http://www.rsa.com

[11] OATH, http://www.openauthentication.org

[12] Park Bonggu, Han Sangeun, Cha Byungrae, Discrete Matematics using Computer, KyungMoon Publishing Company, 2003.

[13] JMSL, http://www.vni.com/products/imsl/jmsl.html