Knowledge-Based User Authentication Associated with Biometrics*

Taekyoung Kwon and Hyeonjoon Moon

Dept. of Computer Engineering, Sejong University, Seoul, 143-747, Korea
tkwon@sejong.ac.kr

Abstract. User authentication is necessary for proving and verifying the claimed identity of users in a distributed environment. Three factors such as user's knowledge, belongings, and biometric traits are usually considered for the purpose. A sort of multi-factor authentication may combine those factors in the way that a user provides the requested multi-factors separately, for improving the accuracy and security of authentication. However, such a combination of distinct factors should require each different human-computer interfaces. In this short paper, rather we introduce our on-going work to associate knowledge-based authentication with biometrics for requiring less interfaces and examine the benefits expected from it in a conceptual level.

1 Introduction

User authentication is necessary for proving and verifying the claimed identity of users in a distributed environment. It has been studied and applied for many years in today's computing environments. For authentication of human beings in those environments, three kinds of factors are usually considered, such as what we know (e.g., passwords, passphrases, or personal identification numbers), what we have (e.g., identification cards, security tokens, or software tokens), and what we are (e.g., fingerprint, retinal patterns, voice patterns, or other biometric identifier). Sometimes a combination of them is used, e.g., a bank card along with a PIN (Personal Identification Number), for producing better security in person authentication. This is called multi-factor authentication in the literature. For such a combination of distinct factors, it should be required to provide each different human-computer interfaces for users. For example, for a combination of password and smart token, the user must be provided with two different interfaces for entering the password and for inserting the smart token device. The knowledge-based authentication appeals to the human memory that may not be accessed readily by another person and may not need any external storage. A password or passphrase authentication system is deployed wide for the reasons. Since the human knowledge can also be used for making a real-time decision by the user in the real world applications, it should be a reasonable attempt to utilize the knowledge for user authentication. For example, the human interactive proofs depending on human knowledge can be applied to interactive authentication

* This study was supported in part by the grant of the Seoul R&BD Program.

C. Stephanidis (Ed.): Universal Access in HCI, Part I, HCII 2007, LNCS 4554, pp. 414–419, 2007.

applications such as CAPTCHAs [1–3]. In addition, the wide-deployed interface such as a keyboard can easily be used for entering the required knowledge into the computing system. However, the knowledge-based authentication accompanies disadvantages as well. The intrinsic problem with this method is a human-memorable secret, associated with each user, has low entropy, so that it is not easy to protect the secret information when it is transmitted over an insecure channel [6]. Besides it is not easy to input the knowledge unless the keyboard-like interfacing device is provided for human users. Specifically in biometric authentication, we use another term, multi-modal authentication, for describing the enhancement to increase the accuracy of authentication systems in five different ways: multiple biometrics, multiple acquisitions of the same biometry, multiple representations for the same biometry, multiple units of the same biometry, and multiple sensors for the same biometry. The multi-modality is accordingly used for describing the multiple treatments of biometric traits associated to a person in the literature [4, 10]. However, multiple human-computer interfaces should be necessary for handling the multi-modal biometrics, while the biometric authentication is expected as a wide spread authentication technology in the future ubiquitous computing environment. Since the human-computer interactions (HCI) is the emerging field of significance in computer science, it should be necessary to study the trade-off of using both multi-factor and multi-modal authentication methods with regard to the human-computer interfacing devices. Our on-going work is to deal with this problem by exploring a method to associate human knowledge with biometrics for requiring less interfaces. In this short paper, we discuss the idea in a conceptual level but we expect more concrete results in our future study. The rest of this paper is organized as follows. In Section 2, we classify the human knowledge for authentication. In Sections 3, we discuss the knowledge-based authentication associated with biometrics in two different ways. In Section 4, we conclude this paper.

2 Human Knowledge for Authentication

In today's computing environment, it is conventional to conduct the human knowledge authentication using the human memorable password or passphrase having low entropy. When we apply Shannon's classic measure of entropy to the human knowledge for authentication, it should be ranging from 20 to 40 bits only. This is because the restricted human memory and alphanumeric characters may limit the space of interactive knowledge. For securing the transmission of such low entropy information, many studies have been done in the context of designing secure and efficient cryptographic protocols, most of which are depending on public key cryptographic technologies. From the perspectives of practical use in interactive authentication, we could classify the human knowledge as follows. In other words, we classify the human knowledge as a shared secret for authentication under the assumption that the knowledge holder, as an authentication client, registers the knowledge or its verifier to the authentication server.

- Static knowledge: The human knowledge that is held by an individual permanently (or as long as the individual's memory allows) can be used for authentication but provides lower security. The static knowledge is very similar to the biometric traits and is distinguished from the semi-static knowledge in the sense that it is very specific to the individual holder's characteristics and environments, for example, a birth place, a graduated elementary school, and some favourites.

- Semi-static knowledge: The human knowledge that is held by an individual semi-permanently (or as long as the individual does not change it) can be used for authentication. The random selection is recommended for security of the semi-static knowledge but the individual tends to choose his or her preferred one, for example, a reusable password or passphrase that is most widely used.
- Dynamic (responsive) knowledge: The human knowledge that is submitted by an individual dynamically can be used for authentication. It is not specific to the individual holder's characteristics and environments. The knowledge here means rather a key for an interactive proof of human being or an human's answer to dynamic questions, for example, a CAPTCHA.

Since the human knowledge has low entropy, an interactive proof method based on cryptographic techniques is desirable for preventing both active and passive adversaries. In the following section, our on-going work to associate the human knowledge with biometrics will be introduced from the perspectives of this classification.

3 Association of Knowledge and Biometrics

In this section, we introduce our pre-mature work to associate human knowledge with biometrics in very conceptual levels. We are studying two different approaches for requiring less human-computer interfaces. One is to associate biometrics with cryptographic protocols manipulating the low-entropy knowledge such as a password, and the other is to associate biometrics with real-time submission of human knowledge. The former associates static knowledge while the latter does semi-static and dynamic knowledge. Two approaches can be combined for more accuracy and convenience in human authentication.

It is recognized that the entropy determined in the measured sample of biometrics is not as much as required in a cryptographic society [7]. Thus, the tele-biometric authentication is not easy without encrypting the huge amount of measurement with enough randomness for secure transmission. In our first approach, we would aim to apply the well-structured cryptographic protocol for ease of secure transmission. For securing the transmission of such low entropy information, many studies have been done in the context of designing secure and efficient password-based cryptographic protocols, most of which are depending on a public key cryptographic technologies. Recently those protocols have been standardized by IEEE P1363.2 and ISO/IEC 11770-4 [6]. The merit of these protocols is that the shared secrets having extremely low entropy can be handled securely and efficiently in a distributed environment. In that sense, we could utilize these protocols for delivering the biometric information having low entropy. Here we mean by the low entropy biometric information, the reduced set of data that are abstracted and filtered from biometric samples for deterministic decision. The filtering of the biometric sample must be modeled carefully, in the way that the possible errors should be minimized within the range allowable by the numerical property of cryptographic protocols. For example, in our cryptographic protocol designed in a number field, it should be possible to replace the numerical value $y^x \cdot$b (mod p) by $y^x \cdot$ (b + e) (mod p) in feasible computation of a small error distance e and the filtered biometric sample b. We are now studying the filter and helper functions for manipulating the biometric samples in that way. If the distinct decision can be made for biometric traits with both low entropy and extremely low errors, it is further possible to let users remember passwords by deriving it from the filtered sample, for example, pw = f(b), and input pw on a keyboard in the environment that the biometric sensor is not available. The server can then follow the rule in verification. As we have observed, the biometric traits can be associated with static knowledge within the allowable error range. While the static knowledge and the biometric traits are susceptible to replay attacks, we utilize the cryptographic protocols for resolving it in some degree. However, the stronger method can be devised.

In our second approach, we would aim to associate biometric sampling with semi-static and dynamic knowledge, for enhancing the security further against replay attacks. In other words, when the biometric sample is captured, we let the user submit additional information within the context of semi-static or dynamic knowledge. This is based on the human interactive proof of knowledge as well as the multi-modal (or simply multiple treatments of) biometrics. The merit of the knowledge-based interactive proof is the capability of detecting on-line attacks. Thus, a simple forgery of biometric traits works very hard in this approach.

As for the semi-static knowledge, we are able to devise at least two methods. (1) A user may register a sequence (or a variance) of biometric traits and in real time submit his or her biometrics within the sequence (or the variance). The most appropriate biometrics is the fingerprint for this approach. For example, a user registers a sequence of fingerprints using his or her multiple fingers, and repeats the sequence in the verification phase. (2) A user may register biometric traits with a variance (or a sequence) by the help of counter (or a similar tool). The most appropriate biometrics is the face for this approach. For example, a user registers a variance of face expressions with a specific counter value, and repeats the variance of expression when the counter meets the registered value in the verification phase.

As for the dynamic knowledge, we could apply the interactive verification method used in CAPTCHAs [2]. In other words, we could exploit the experience of passing the U.S. border control as a foreign visitor [9]. When the verification system asks us a specific request, we could response with biometrics associated with our dynamic knowledge. For example, the verification system may ask us by sending messages such as left finger, right finger, the first right finger, or smile, turn right, turn left, and something like that. We then can follow the dynamic question for submitting our biometric traits in the verification phase. If we utilize a CAPTCHA's one-time gimpy-like image that is hard to be read by a machine, we may further be able to apply the image to processing and scrambling the biometric samples in the interactive proofs [2, 5]. The methods described in this section can prevent replay attacks and on-line forgery attacks on biometrics by associating it with human knowledge.

4 Conclusion

In this short paper, we introduce our on-going work on knowledge-based authentication associated with biometrics for improving accuracy and security of user authentication with requiring less human-computer interaction devices. The goal of this study is to consider two different authentication factors without requiring multiple hardware interfaces. Specifically two different schemes are considered for the purpose, while both requiring only biometrics devices as a human-computer interface. One is to derive a low-entropy value from biometrics and apply it to cryptographic protocols using the low-entropy secrets, while the other is to apply human knowledge to the decision of biometrics. Both methods require biometrics devices only but human-knowledge can be associated with biometrics for more accuracy and security. Besides the first method can be applied to the classical computing environment having a keyboard only. Finally, such a combination can be extended more flexibly to accommodate access control features. In our future study, we will investigate more concrete details of the two proposed approaches. Our first implementation is on a PDA having a fingerprint sensor and we expect a comparable result with the related work such as [8].

Acknowledgement. This research was also supported in part by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0028).

References

1. von Ahn, L., Blum, M., Hopper, N., Langford, J.: The CAPTCHA Web Page (2000), http://www.captcha.net
2. von Ahn, L., Blum, M., Hopper, N., Langford, J.: CAPTCHA: Using Hard AI Problems For Security. In: Biham, E. (ed.) Advances in Cryptology – EUROCRPYT 2003. LNCS, vol. 2656, pp. 294–311. Springer, Heidelberg (2003)
3. Baird, H., Popat, K.: Human Interactive Proofs and Document Image Analysis. In: Lopresti, D.P., Hu, J., Kashi, R.S. (eds.) DAS 2002. LNCS, vol. 2423, Springer, Heidelberg (2002)
4. Bign, J., Duc, B., Smeraldi, F., Fischer, S., Makarov, A.: Multi-modal person authentication. In: Proc. of Face Recognition: From Theory to Applications (NATO-ASI Workshop) (1997)
5. Hopper, N., Blum, M.: Secure human identification protocols. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 52–66. Springer, Heidelberg (2001)
6. IEEE P1363-2, Standard specifications for password-based public key cryptographic techniques (December 2002), available from http://grouper.ieee.org/groups/1363
7. Juels, A., Sudan, M.: A Fuzzy Vault Scheme. In: One-page abstract appeared in the Proceedings of IEEE Internation Symposium on Information Theory, p. 408. IEEE Press, Lausanne, Switzerland (2002), Also available at http://www.rsasecurity.com/rsalabs/staff/
8. Koreman, J., Morris, A.C., Jassim, S., Sellahewa, H., Chollet, G., Aversano, G., Salicetti, S., Allano, L.: Multi-modal biometric authentication on the SecurePhone PDA. In: Proc. of MMUA workshop on Mult-Modal User Authentication (May 2006)

9. Kwon, T., Moon, H.: Multi-modal Biometrics with PKI technologies for border control applications. In: Berthold, M.R., Glen, R.C., Diederichs, K., Kohlbacher, O., Fischer, I. (eds.) CompLife 2005. LNCS (LNBI), vol. 3695, p. 99–114. Springer, Heidelberg (2005)
10. Thian, N., Bengio, S.: Why Do Multi-Stream, Multi-Band and Multi-Modal Approaches Work on Biometric User Authentication Tasks? IDIAP research report. In: Proceeding of 2004 Internation Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2004) vol. 5, pp. 893–896 (2004)