Editor's Note: In distance learning, authentication of student work poses some problems. This solution using cell phones provides an added level of protection. The authors provide a useful analysis of the options available to correctly identify the learner.

Reliable Authentication Method by Using Cellular Phones in Web Based Training

Hideyuki Takamizawa, Kenji Kaijiri

Japan

Abstract

Institutions of higher education that offer credits through distance learning using web based training (WBT) have increased recently. In these situations, an authentication model using the ID-password pair is generally used. However, this authentication model cannot prevent "identity theft" effectively. We propose a new authentication method that solves this problem by using cellular phones as an authentication token. The authentication accuracy is expected to be improved by combining the ID-password pair with the subscriber ID of cellular phones. We realized a prototype system and prepared a questionnaire in order to validate the effectiveness of our proposed method, and as a result, we demonstrated the effectiveness and realizability of our method.

Keywords: authentication, cellular phone, identity theft, WBT, e-learning, ID-password

Introduction

In distance learning, it is difficult to identify students because ordinal distance learning is asynchronous and the teachers themselves cannot monitor the students directly. The students who ask other students to perform their tasks may lend their ID-password pair; therefore, authentication by using this pair cannot effectively prevent intentional identity theft (other students perform a task instead of the specified student). Several papers have addressed the problem of secure authentication for web based training (WBT) (e.g., A design of authentication: E. Suzuki 2004; Security and privacy technologies: Lin et al., 2004; and Securing web-accessible information systems: Lavery and Boldyreff, 2001); however, their main objective is the security of the ID-password pair, and thus they provide no solution for intentional identity theft.

On the other hand, the use of cellular phones has gained popularity. According to an investigation, in Japan, 96.3% of university students and 86.6% of high school students have their own cellular phones (e.g., Cellular-phone use situation: Hakuhoudou 2004). This situation is the same in other Asian countries. Figure 1 shows that the Internet connection infrastructure of cellular phones is particularly advanced in Japan and South Korea (e.g., Information and communications in Japan: Ministry of Internal Affairs and Communications, 2005). The popularization of cellular phones is very rapid, and it is expected that almost 100% of students will have cellular phones in the near future.

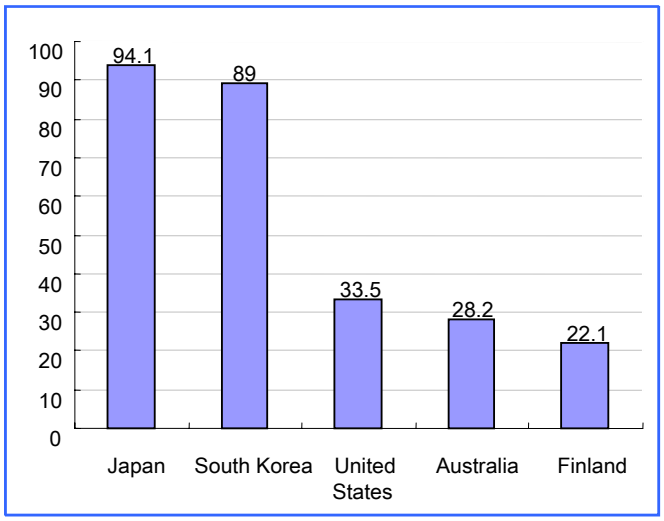

Figure 1. Cellular Phone Internet Compatibility Rates in Leading Countries (September, 2004)

It is very important to ensure that a student accessing the system is who he/she claims to be if the credits are to be given based on the WBT that uses this identification. Cellular phones are personal gadgets and lending them in order to ask other students to do their own tasks is supposed to be very rare; therefore, we propose a new authentication method based on cellular phones that has the following characteristics: (1) borrowing and lending authentication media is very difficult; (2) no additional hardware is needed; and (3) the burden is light both for the systems and users.

Min Wu proposed the cooperation of cellular phones and PCs to control the security of traffic through PCs (e.g., Secure Web Authentication: Min Wu et al., 2003). In this method, a randomly generated message is sent to both the target PC and the cellular phone from a security proxy server. By comparing these messages, users can trust the corresponding server. The purpose of his proposal is the confirmation of secure traffic and not user authentication.

However, this method uses SMS (short message service) or e-mail. In Japan, SMS cannot be received directly on PCs (SMS and internet e-mail use different technologies). Further, e-mail has variable latency. Therefore, immediate authentication, which is a major requirement of WBT, may become impossible.

Several authentication methods using cellular phones have been proposed and used (e.g., Enabling Pervasive Computing: George Roussos et al., 2005; Seeing-is-believing: McCune et al., 2005), but their main targets are the services on cellular phones. On the other hand, our target is WBT. In this paper, we propose an authentication method that uses cellular phones for WBT. The cellular phone is not an object of service, but is used as an authentication token.

In the next section we survey various authentication technologies and show the advantage of our method. This is followed by Implementation where we describe the sample implementation of and show the possibility of our method. Then we describe conclusions and future works.

Authentication technology

Authentication

We define authentication as follows: it is the identification of individuals using attributes that only the identified student knows or has. There are several authentication methods, as shown in Figure 2. All these methods have some merits and demerits; therefore, an adequate method will be selected based on the requirements for authentication.

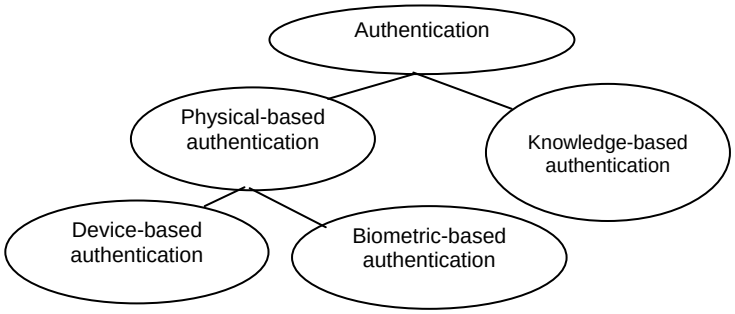

Figure 2. Various Authentication Methods

Traditional Authentication methods and their Problems

Authentication by using the ID-password pair is knowledge based authentication and is the most popular authentication technique. The problem with knowledge based authentication is its dependency on the concealment of this pair. If students lend this pair to other students voluntarily, authentication can no longer be assured; further, easy and permanent lending is also possible. Q/A based authentication is a kind of ID-password authentication, but lending the Q/A pair to other students is also easy (e.g. Challenge-Question Systems: Mike Just, 2005).

E-mail based authentication using the e-mail account-password pair is also a variation of the ID-password authentication (e.g., Mobile technologies in the lecture room: Christian et al., 2005; and E-mail-based identification: Garfinkel et al., 2003). Illegal use of the ID-password pair can be controlled through e-mail to some degree and lending this pair is rare; however, e-mail lacks the real-time property.

Sharing the frequently used e-mail ID-password pair with the WBT ID-password pair is effective in the improvement of authentication accuracy. Typically, this sharing will be possible by using Lightweight Directory Access Protocol (LDAP), but this method includes some problems concerning platform dependent implementation architecture.

The alternative to using the ID-password pair is the use of IC cards, which is a kind of device-based authentication. It is very difficult to copy the contents from IC cards, and currently these cards are used for multiple purposes such as student ID cards and credit cards; therefore, students will hesitate to lend these cards. The main problem with IC cards is that special input devices are required, and this requirement tends to negate the main advantage of WBT: it is accessible anywhere and anytime.

Authentication by using biological information (e.g., User Authentication through Biometrics: Vaclav et al., 2003) is the most appropriate method for WBT (it is so for other purposes). The student to be identified must be present for the authentication. The most serious obstacle to this method is the cost. Special hardware and sampled data for each student are required. Authentication by using keystroke patterns is a kind of biometric based authentication, but the preciseness is not high (e.g., Learning to identify a typist: Nisenson et al., 2003; and A key to User Identification: Allen et al., 2004).

Characteristics and Requirement for Authentication in WBT

As previously mentioned, authentication in WBT has different characteristics from that in other applications, particularly when WBT is used as a qualifying test. We clarify these characteristics as follows:

- Students intentionally lend authentication keys or media to other students who take the qualifying test in their place; thus, it should be difficult to lend the keys or the media.
- The main characteristic of WBT is that it should be accessible anytime and anywhere; therefore, it should not be essential to install any special media or software on the client machines.
- Authentication must be done simultaneously.

With the exception of the third one, the above mentioned characteristics are very special requirements for WBT; therefore, ordinal authentication methods cannot be used for our purpose.

Authentication by Using Cellular Phones

As described in foregoing paragraph, ordinary authentication methods have several demerits; thus, we have proposed an authentication method that uses cellular phones. Authentication by using cellular phones has the following characteristics:

1. Each cellular phone contains a large amount of personal information and is used daily; therefore, lending it to other students, even for a while, is supposed to be rare.
2. Each cellular phone has a variety of distinctive information that can be used as authentication data.
3. Almost all students own cellular phones; therefore, no additional device is needed, and it is believed that distance learning with pervasive devices will become popular (e.g., Enhancing Synchronous Distance Education: Martin et al., 2001).
4. As current cellular phones have mail and web functionalities, no additional hardware and software, with the exception of authentication software, is required.

Therefore, authentication by using cellular phones satisfies our requirements.

The following information and/or data can be used for authentication: (a) telephone number, (b) sent and received e-mail data, (c) identification number for each cellular phone, (d) photo images by using the camera function, (e) location information by using the GPS function, and (f) real video by using the video phone function (the third generation cellular phones have this capability).

Some of these are already used in several applications, especially in pervasive computing (e.g., Enabling Pervasive Computing: George et al., 2005); however, we have proposed the use of this information in order to increase the preciseness of the authentication in WBT. Since this information is already contained in cellular phones, some combinations of this information are possible and its realization is not so difficult.

In order to confirm the effectiveness of the authentication by using cellular phones, we conducted questionnaire survey among 75 Japanese college students on “The information that you do not want to lend to other students in WBT.”

The first question is “Which media do you have the most resistance to lend in order to ask other student to do your homework instead of you?” Students are requested to select one of four choices: portrait, ID-password (for study portal sites including the ones for WBT), ID-card (student’s identification card), and cellular phone. Figure 3 shows the result of this questionnaire.

Portraits are used in face authentication, ID-cards in device-based authentication, the ID-password pair in knowledge-based authentication, and cellular phones in our proposed authentication method.

It is noteworthy that the percentage of students who have stated that they would not like to lend their cellular phones to others is the highest. On the other hand, a lower percentage would refuse to lend their ID-cards to others; therefore, the authentication by ID-cards is not effective in the prevention of identity theft.

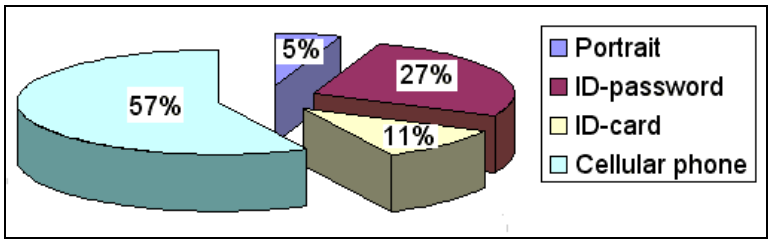

Figure 3. Information that students do not lend to other students in WBT

The next question is "How often do you use Internet?" Table 1 shows the answers that are classified according to the first question; for example, the fifth column shows the results of students who resist lending their cellular phones. This result reveals that the students dislike lending their cellular phones regardless of their Internet usage.

Table 1

Relation to ratio of WEB access media and its frequency

	Portrait	ID-password	ID-card	Cellular phone	Sum
Often	0	3	4	13	20
Sometimes	1	8	3	17	29
Few	2	9	1	11	23
Never	1	0	0	2	3
Sum	4	20	8	43	75

The next question is "How much do you dislike lending each media in order to ask other students to do your homework?" Table 2 shows the results of this question. In this case, the refusal rate of ID-password is as high as that of cellular phones. This is because the ID-password pairs are shared between WBT and e-mail in our university. If different accounts are used, the refusal rate of ID-password will not be so high.

Table 2

The Degree of which students refuse to lend others each item (%)

	Portrait	ID-password	ID-card	Cellular phone
Refusal	20	51	29	59
Resistance	16	17	24	20
Unpleasant	24	20	28	16
No problem	40	12	19	5

Table 2 also shows that students strongly dislike lending their own cellular phones to others. This is confirmed by the fact that "Refusal" has the highest percentage while "No Problem" has the lowest percentage.

Moreover, I emphasize that there is no resistance in lending others a portrait. Therefore, face authentication is not effective if portraits are used instead of real face images.

A large number of students stated that a reason for refusing to lend their own cellular phone is that personal mailing information, addresses, etc., are preserved in the phone.

This answer can be further classified into the following two categories.

- Because a large amount of their **own personal information** is included
- Because a large amount of personal **information of their friends** is included

The students who believe that the personal information preserved in cellular phones includes information about their friends show stronger rejection. We introduce other answers in order to show how students think about cellular phones

- Students feel uneasy about situations in which they are without their cellular phones.
- Students do not like that others use their own cellular phones inappropriately.
- While students have lent others their cellular phones, it will be a problem if they receive a telephone call.

These reasons confirm the fact that it is difficult for students to lend their cellular phones to others.

Cellular phones contain a lot of personal information. This personal information is not protected as in the case of the data in IC cards within cellular phones. This is one of the main reasons why students dislike lending others their own cellular phones. Therefore, cellular phones are suitable for use as an authentication token.

Implementation

There are several possibilities in our method, and as a first step, we have implemented the authentication tool by using the identification numbers of cellular phones (subscriber ID) in order to validate the realizability and effectiveness of our method.

Acquisition of identification number

We can acquire the subscriber ID of a cellular phone by using the active server pages (ASP) in a WWW server. In the case of Docomo and Vodafone in Japan, we can acquire the subscriber ID as the value of an environment variable "HTTP_USER_AGENT" by adding a "utn" attribute in the "a" tag, as shown in Figure 4.

```
<html>
<head>
<title>Authentication</title>
<head>

<body>
<p><a href="default.asp" utn>Click Here!</a>
</p>
</body>
</html>
```

Figure 4. Sample Implementation of index.html

```
<html>
<head>
<title>Results</title>
<head>

<body>
<p>
<%
Response.Write(Request.ServerVariables("HTTP_X_UP_SUBNO"))
Response.Write(Request.ServerVariables("HTTP_USER_AGENT"))
%>
</p>
</body>
</html>
```

Figure 5. Sample Implementation of default.asp

As shown in Figure 4, the "a" tag augmented with the "utn" attribute is described in index.html. By using the linked ASP, as shown in Figure 5 (in this case, the WWW server is Microsoft IIS), we can extract the value of the specified environment variables. When we access this file with a cellular phone using the NTT Docomo service, we will get the message

"DoCoMo/1.0/D503iS/c10/serNMIUA224231"

The string "serNMIUA224231" is the subscriber ID.

During authentication, these values are first stored as personal data for each student, and after that, these values will be checked against the data that is stored previously for each student. However, the user is able to prevent his/her own subscriber ID from being sent. If the system cannot obtain the subscriber ID, the system needs to ask the users to send their subscriber IDs.

Authentication in WBT

First, it is necessary to register the subscriber ID in the server in order to use the cellular phone for authentication. The registration flow of our method is as follows (Figure 6). The student accesses the web page for registration with the cellular phone.

1. The server asks for the student's (ID, password) pair.
2. The student inputs his/her (ID, password) pair.
3. If the (ID, password) pair is correct, the server collates and stores the subscriber ID of the cellular phone in the authentication database.
4. If the ID is new, the system stores it in the database.

5. The server sends the cellular phone URL on the web page for authentication.

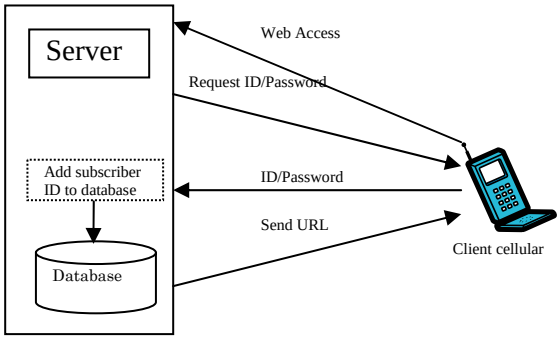

Figure 6. Registration Flow for authentication

The authentication flow of our method is as follows (Figure 7).

1. The student accesses the web page of a WBT server.
2. The server asks for the student's (ID, password) pair.
3. The student accesses the specified URL by using his/her own cellular phone. (Sequences 1–2 and 3–4 may not be in this order.)
4. The server checks the acquired subscriber ID against the stored ID. If the check is successful, the server sends the message "OK" to cellular phone and admits the current access for a specified time. (This action is very similar to that of POP before SMTP.)
5. During this specified time, the student inputs his/her ID-password pair.
6. If the ID-password pair is correct, a target web page is displayed.
7. The student starts learning by using this server.
8. After the authentication is completed, the session management or the cookie may use this authentication.

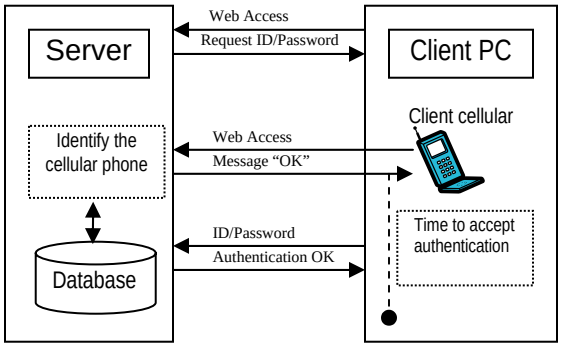

Figure 7. Authentication Flow in WBT

Evaluations

We have implemented the authentication tool based on the above mentioned flow in order to validate the reliability of our method.

Several students used our tools, and they took about 15–20 s to complete the authentication process. This is a little longer than the time taken in the method using ID-password pair. However, students believe that the system that uses the ID-password pair demands more personal information; therefore, our method is valuable for the prevention of identity theft from a psychological point of view.

The authentication procedure becomes a little complicated when compared to the ordinary ID-password authentication method; therefore, if frequent authentication requests are needed, our method becomes cumbersome. This problem can be resolved by increasing the effective period of authentication by using cookies. For instance, when the student first uses the cellular phone for authentication, the authentication information is stored in a cookie on the PC. The server does not demand authentication from the cellular phone for the period during which the cookie is effective.

Conclusion

In this paper, we have proposed a new authentication method by using cellular phones and have shown its realizability by prototype implementation. The authentication accuracy will be improved, and the advantage of WBT, that is, it can be used everywhere, will be preserved. The results of the questionnaire suggest the possibility of preventing spoofing by using the token value of cellular phones. It is possible to use a combination of the information on several individuals to increase the accuracy of authentication.

One important problem that cannot be resolved yet is how to ensure that a student takes an examination alone without any support from other students. If a student and his/her support person coexist and the same student performs the authentication, our method will have no effect. It is difficult to solve this problem. However, the integration of our method and the usage of cameras can improve this situation.

The second problem is the possibility that a user buys a cellular phone for an illegal attestation. It is possible to solve this problem by recording the position when attesting it by using the GPS function of the cellular phone. We are advancing our research on the method of identification by using photographs and the GPS function.

Nevertheless, the current version of this method has proven to be effective based on the results of the questionnaire. The authentication that combines the cellular phone with the ID-password pair is notable.

References

E, Suzuki. (2004). A design of authentication system for distributed education, *in Proceeding of 5th ITHET International Conference, May-June 2004,66-71*.

Hakuhodo. (2004). Cellular-phone use situation investigation from teen-ager to 30-something in *http://www.hakuhodo.co.jp/news/pdf/20040319.pdf* (in Japanese, retrieved November 12, 2005)

Just, Mike. (2004). Designing and evaluating challenge-question systems. *IEEE Security & Privacy, September–October 2004, 2,* (5), 32–39.

Lavery, J, & Boldyreff, C. (2001). Securing Web-accessible Information Systems within higher education institutions. *Proceeding of WETICE*, Cambridge, MA, USA.

Lin, N. H., Korba, L., Yee, G., Shih, T. K., Lin, H. W., Nigel, H. L. (2004). Security and privacy technologies for distance education applications. *AINA 18th International Conference 580-585 Vol. 1*

Matyas, V, Jr., & Rish, Z. (2003). Towards reliable user authentication through biometrics, *IEEE Security & Privacy, May–June 2003, 1,* (3), 45–49.

Mauve, M., Schelle, N., &Geyer, W. (2001). Enhancing synchronous distance education with pervasive devices, *Proceedings of Informatik,* Wien.

McCune, J. M., Perring, A.Reiter, &M. K. (2005). Seeing-is-believing: Using camera phones for human-verifiable authentication. *Security & Privacy IEEE Symposium, May 2005, 110–124.*

Ministry of Internal Affairs and Communications. (2005). *Japan: Information and Communications in Japan*, 2005, *http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2005/2005-index.html* (retrieved February 5, 2006)

Mordechai, N., Ido, Y., Ran, E., & Ron, M. (2003). Towards behaviometric security systems: Learning to identify a typist. *Proceeding of 7th European Conference on Principles and Practice of Knowledge Discovery in Databases* , Cavtat-Dubrovnik, Croatie 2838, 363–374.

Peacock, A, Ke, Xian, &Wilkerson, M. (2004). Typing patterns: A key to user identification, *IEEE Security & Privacy, September–October 2004, 2(5),40–47.*

Roussos, G, Marsh A. J. &Maglavera, S. (2005). Enabling pervasive computing with smart phones, *IEEE Pervasive Computing, April–June 2005, 4, (2), 20–27*.

Simson, Garfinkel, L. (2003). Email-based identification and authentication: An alternative to PKI, *IEEE Security & Privacy Magazine, November–December 2003, 1, (6), 20–26.*

Wattinger, C, Kern, C, Guggisberg, M, & Burkhart, H. (2004). Mobile technologies in the lecture room: Techniques and case study, *in Proceeding of 6th ICNEE,* Neuchatel, Switzerland.

Wu, M., Garfinkel, S., &Miller, R. (2003). Secure Web authentication with mobile phones. *Proceedings of Student Oxygen Workshop*, Cambridge, MA, USA.

About the Authors

Hideyuki Takamizawa

Hideyuki Takamizawa is a graduate student and Ph.D. Candidate at the Shinshu University in Japan and an IT engineer with the Graduate School of Law at Hitotsubashi University in Japan. His areas of research interest are authentication and distance learning.

Hideyuki Takamizawa
Graduate School of Science &Technology, Shinshu University
4-17-1 Wakasato, Nagano, 380-8553
JAPAN

E-mail: jetta@law.hit-u.ac.jp

Kenji Kaijiri

Kenji Kaijiri was received the B.E., M.E., and Dr. Eng. Degrees from Osaka University, Japan, in 1972, 1974, and 1977 respectively. He Joined Shinshu University in 1977, and is currently Professor of Faculty of Engineering. His areas of research interest are software engineering and distance learning. He is a member of the IPSJ Japan, IEEE, and ACM.

Kenji Kaijiri
Graduate School of Science & Technology, Shinshu University
4-17-1 Wakasato, Nagano, 380-8553
JAPAN

E-mail: kaijiri@cs.shinshu-u.ac.jp