Reliable Authentication Method by Using Cellular Phones in WBT

Hideyuki Takamizawa and Kenji Kaijiri
Faculty of Engineering, Shinshu University, Japan
jetta@law.hit-u.ac.jp, kaijiri@cs.shinshu-u.ac.jp

Abstract

Institutions of higher education that give the credits by distance learning using WBT have increased recently. In these situations, the authentication model by (ID, password) pair is general. However, this authentication model cannot prevent "Identity theft" effectively. In this paper, we propose a new authentication model to solve this problem by using cellular phones.

Topic B4

1. Introduction

In distance learning, it is difficult to identify students themselves because ordinal distance learning is asynchronous and teachers cannot check students themselves directly. Students who ask other students to do their tasks may lend their (ID password) pair, so authentication by using (ID, password) pair cannot prevent identity theft (other students do the task instead of the specified student) based on the owner's intension effectively. Several papers [1, 2, 3] addressed the problem of secure authentication for Web Based Training (WBT), but their main objective is the security of (ID, password) pair, so they provide no solution for intentional identity theft.

On the other hand, cellular phones become popular. According to the investigation by HAKUHOUDOU [5] 96.3% of university students and 86.6% of high school students have their own cellular phones in Japan. This is the same in the Asian countries, especially, in Korea, Hong Kong, and Singapore. The popularization is very rapid and almost 100% of students will have cellular pones in the near future.

It is very important to make sure that the student accessing the system is whom he/she claims to be if credits will be given based the WBT by using this identification. Cellular phones are personal tools, so lending them in order to ask other student to do their tasks is supposed to be very rare, so we propose a new authentication method based on cellular phones which has the following characteristics: 1) Borrowing and lending the authentication media is very difficult, 2) No additional hardware is needed, 3) The burden is light both for systems and users. Min Wu proposed the usage of cellular phones in authentication [4], but it uses e-mail. E-mail has variable latency, so immediate authentication, which is the major requirement of WBT, may become impossible.

Several authentication methods using cellular phones have been proposed and used [9], but their main target is the services on cellular phones themselves, but our target is WBT. In this paper we propose the authentication method using cellular phones for WBT.

In Chapter 2, we surveyed various authentication technologies and showed the advantage of our method. In Chapter 3, we described the sample implementation of our method and showed the possibility of our method, and in Chapter 4, we described the conclusions and future works.

2. Authentication technology

2.1. Authentication

We define authentication as follows: To identify individuals using attributes which only the identified student knows or has. There are several authentication methods as shown in Figure 1. These methods have some merits and demerits, so an adequate method will be selected based on requirements for authentication.

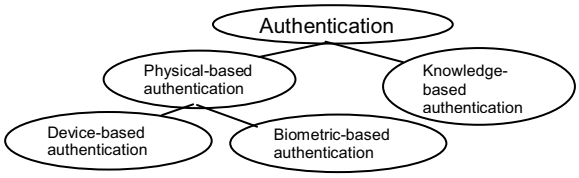

Figure 1 Various Authentication Method

2.2 Traditional Authentication methods and their Problems

Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)
0-7695-2552-0/06 $20.00 © 2006 IEEE

The authentication by using (ID, password) pair is knowledge-based authentication and is the most popular one. The problem of knowledge-based authentication is its dependency on concealment of this pair. If students lend this pair to other student by themselves, its ability will be disappeared, and further easy and permanent lending is possible. Q/A based authentication [10] is a kind of (ID, password) authentication, but lending the Q/A pair to other student is also easy. E-mail based authentication [7,13] is also a variation of (Id, password) authentication, but e-mail lacks the real time property.

The alternative of (ID, password) pair is IC cards, which is a kind of device-based authentication. The copy of IC cards is very difficult, and currently IC cards are used for multiple purposes, for example, student ID cards, or credit cards, so students will hesitate to lend these cards. The main problem of IC cards is the necessity of special input devices, and this requirement diminishes the main advantage of WBT: everywhere and anytime.

The authentication by using biological information [11] is the most adequate method for WBT (it is so for other purposes). The student to be identified must be there in order to authenticate. The most serious obstacle for this method is the cost. It needs special hardware and sampled data for each student. The authentication by using keystroke patterns [8,12] is a kind of biometric-based authentication, but the preciseness is not high.

2.3 The characteristics and requirement for the authentication for WBT

As already mentioned, the authentication in WBT has different characteristics from other applications, in particular when we use WBT as qualifying test. We clarify these characteristics as follows:

- Students intentionally lend authentication keys or media to other student who takes the qualifying test in place of them, so the keys or media need to be difficult to lend.
- No special media or software are not supposed to be installed on client machines, because everywhere and anytime are the main characteristics of WBT.
- Authentication must be done simultaneously.

These, except the third requirement, are very special requirements, so ordinal authentication methods can not be used for our purpose.

2.4 Authentication by using cellular phone

As described in Section 2.3, an ordinal authentication method has several demerits, so we have proposed the authentication methods by using cellular phones. Authentication by using cellular phone has the following characteristics:

1. Each cellular phone holds much personal information and is used daily, so lending it to other students even for a while supposed to be very rare.
2. Each cellular phone has a variety of peculiar information and this information can be used as authentication data.
3. Almost all of students have cellular phones by themselves, so no additional device is needed. Distance learning with pervasive devices will become popular [6].
4. Cellular phones have mail and web functionalities, so no additional hardware and software are needed except for the authentication software.

So, the authentication by using cellar phones satisfies our requirements.

The following informations and/or data can be used for authentication:

- Telephone number
- Sent and received e-mail data
- Identification number for each cellular phone
- Photo image by using the camera function
- Location information by using GPS function
- Real video by using the video phone function (third generation cellular phones have this capability).

Some of these are already used in several applications, especially in pervasive computing [9], but we have proposed to use these informations in order to make authentication more precise in WBT. Cellular phones hold these informations by themselves, so the combination of these informations is possible and realization is not so difficult.

In order to confirm the effectiveness of authentication by using cellular phones, we performed the questionnaire for 32 college students about "The information that you do not want to lend to other students in WBT".

The first questionnaire is “Which media do you have the most resistance to lend in order to ask other student to do your homework instead of you”.

Figure 2 shows the result of this questionnaire. Notice that the rejection of lending a cellular phone to others is the strongest. On the other hand, there is a little refusal to lending ID-Card to others, so the authentication by the ID-Card is doubtful of effectiveness.

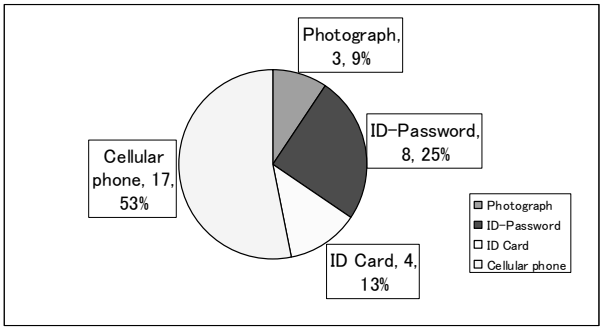

Figure 2 The information that students do not lend to other students in WBT

The next questionnaire is "How often do you use internet?". Figure 3 shows the answer that is classified according to the first questionnaire; for example, the fifth column shows the result by students who resist lending cellular phone. This result shows that students dislike lending cellular phone regardless of the usage of internet.

	Photograph	ID-Password	ID-Card	Cellular phone	Sum
Often	0	1	1	3	5
Sometimes	1	2	3	6	12
Few	2	5	0	7	14
Never	0	0	0	1	1
Sum	**3**	**8**	**4**	**17**	**32**

Figure 3 Relation to ratio of WEB access by cellular phone

The next questionnaire "How do you dislike lend each media in order to ask other student to do you homework". Figure 4 shows the result. In this case, students dislike lending ID-Password, ID-Card, and cellular phone equally. This is because WBT and an E-mail use the same ID-Password in our university. If different accounts are used, refusal of ID-password will be not so high.

	Photograph	ID-Password	ID-Card	Cellular phone
Refusal	8	19	12	19
Registance	3	3	5	4
Unpleasant	8	5	8	5
No Problem	13	5	7	4

Figure 4 The Degree that refuses to lend others each item

I emphasize that there is no resistance in lending others a photograph, so face authentication is not effective if photographs may be used instead of real face images.

3. Implementation

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

3.1 Acquisition of identification number

We can acquire the subscriber ID of a cellular phone by using CGI scripts 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 "a" tag as shown in Figure 5. We show the simple implementation of index.html in Figure5.

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

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

Figure 5 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 6 Sample Implementation of default.asp

As shown in Figure 5, "a" tag augmented with "utn" attribute is described in index.html. The linked CGI as shown in Figure 6 (In this case, WWW server is IIS and CGI is asp) will extract the value of the specified environment variables. When we access this file with a cellular phone of NTT Docomo, we will get the message
"DoCoMo/1.0/D503iS/c10/serNMIUA224231".
"NMIUA224231" in data is subscriber ID.

In authentication, at first these values are stored as personal data for each student, and after that, these values will be checked against the data that is stored beforehand for each student.

3.2 Authentication in WBT

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

1. A student accesses the WBT server.
2. The server demands the input of (ID, Password) pair.
3. The student inputs his/her (ID, Password) pair.
4. The server demands the student to access this server by using his/her own cellular phone.
5. The student accesses the specified URL by using his/her own cellular phone.
6. The server checks the acquired subscriber ID against the store ID. If check succeeds, the server admits the current access for a specified time. If check fails, the server denies the current access. (This action is very similar to that of POP before SMTP).
7. The student starts learning by using this server.

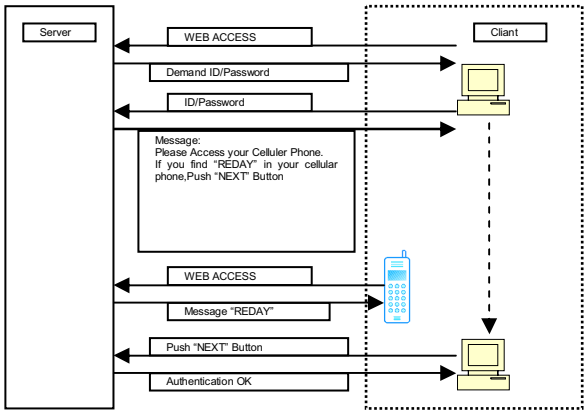

Figure 7 Authentication Flow in WBT

3.3 Evaluations

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

Several students used our tools and they took about 15-20 seconds in order to complete the authentication process. It is a little longer than the method by using (ID, password) pair. But in this method, students think that the system remands more personal informations, so our method is valuable for the prevention of "Identity theft" from the psychological point of view.

Authentication procedure becomes a little complicated comparing with the ordinary (ID, password) authentication, so if frequent authentication request is needed, our method is cumbersome. This problem can be resolved by lengthening the effective period of authentication by using cookie. The authentication method becomes as follows when we use cookie.

1. A student accesses the WBT Server.
2. The server demands the input of (ID, Password) pair.
3. The student inputs his/her (ID, Password) pair.
4. The server requests the browser to look for the cookie.
5. When the cookie is found, the server doesn't request authentication by using cellular phones.
6. Otherwise, the server requests authentication by using cellular phones, and the server writes subscriber ID, user ID, and the expiration date (Several hours from time now after) in the cookie.
7. The student starts learning.

4. Conclusion

In this paper, we have proposed the new authentication method by using cellular phones and have shown the realizability by prototype implementation. Authentication accuracy will be improved and the advantage of WBT, that is, "everywhere" will be preserved. The combination of several individual informations is possible in order to increase the accuracy of authentication.

One important problem that cannot be resolved yet is to make sure that the student takes an examination alone without any support from other students. If a student and his/her support person coexist and identical student does authentication, our method makes no effect. It is difficult to solve this problem. However integration of our method and the usage of camera can improve this situation.

The usage of video function of cellular phones may suggest some possibilities for this problem. Several authentication systems by recognition of the face image are realized, but these systems cannot distinguish between the real image and the photo image, but if identification numbers of cellular phones are used at the same time, it is expected to improve this problem. We are advancing research on the method of identification by using photographs and/or genuine articles using cellular phones.

5. References

[1] E. Suzuki: A design of authentication system for distributed education, ITHET 2004

[2] Nigel H. Lin, et al: Security and Privacy Technologies for Distance Education Applications, AINA 2004

[3] Janet Lavery, et al.: Securing Web-accessible Information Systems within Higher Education Institutions, WETICE 2001

[4] Min Wu, et al.: Secure Web Authentication with Mobile Phones. Student Oxygen Workshop 2003

[5] Cellular-phone use situation investigation from teen-ager to 30-something in http://www.hakuhodo.co.jp/news/pdf/20040319.pdf 2004 (in Japanese)

[6] Martin Mauve, et al.: Enhancing Synchronous Distance Education with Pervasive Devices, Proc. Informatik 2001

[7] Cristian Wattinger, et al.: Mobile Technologies in the Lecture Room: Techniques and Case Study, Proceedings 6th ICNEE 2004

[8] Mordechai Nisenson, et al.: Towards Behaviometric Security Systems: Learning to Identify a Typist, 7th European Conference on Principles and Practice of Knowledge Discovery in Databases 2003 LNCS 2838

[9] George Roussos, et al.: Enabling Pervasive Computing with Smart Phones, Pervasive Computing, April-June 2005

[10] Mike Just: Designing and Evaluating Challenge-Question Systems, IEEE Security & Privacy, Sep. 2004

[11] Vaclav Matyas Jr, et al: Towards Reliable User Authentication through Biometrics, IEEE Security & Privacy, May/June 2003

[12] Allen Peacock, et al: Typing Patterns: A Key to User Identification, IEEE Security & Privacy, Sep. 2004

[13] Simson L. Garfinkel: Email-Based Identification and Authentication: An Alternative to PKI, IEEE Security & Privacy, Nov. 2003

Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)
0-7695-2552-0/06 $20.00 © 2006 IEEE