P－14

Development of an Authentication System Employing Method of "a Question to an User and the Answer from Him/Her"

Kiyofumi Haneda*, Tadashi Koyama*,
Tokuo Umeda**, Hajime Harauchi***, Kiyonari Inamura***

* Department of Radiological Sciences & Technology,
Hiroshima Prefectural College of Health and Welfare
** School of Allied Health Sciences , Kitasato University
***School of Allied Health Sciences, Faculty of Medicine, Osaka University

1. PURPOSE

In case a computer is connected to a network by telephone, we must have the risk that someone could break into our system. Messages could be intercepted, missorted, and forged. Communication lines connecting computers to each other, or connecting terminals to a central computer, could be tapped or physically damaged by a cracker.*1

The first way in which a system provides computer security is by controlling access to that system: Who's allowed to log in? How does the system decide whether an user is legitimate ? How does the system keep track of who's doing what in the system ? [1]

In order to authenticate an user as the authorized person who could access to the system, a new method of authentication is strongly required because conventional password method has limitation to the level of accuracy and security. Consequently we devised an authentication system employing the method of "a question to an user and the answer from him/her "which can be applied to any environment of computers and communications, and we evaluated the degree of accuracy, security and operability of our system.

2. METHOD

2-1 The Methods of Authentication

Authentication is way you prove to the system that you are who you say you are. In just about any system, you must identify yourself and the system must authenticate your identity, before you can use the system.

2-1-1 Comparison of Other Authorized Methods

There are three general methods in which you can prove yourself [2] :

a) Password (Conventional)

The theory is that if you know the secret password for an account, you must be the owner of that account. The advantage of this method is that it runs without any special equipment (such as card readers or fingerprint scanners). The disadvantage of conventional passwords is that they are easily foiled. You might give your password away or have it stolen from you. If you write it down, someone might read it. If you tell someone, that person might tell someone else. If you have a simple, easy-to-guess password, someone might guess it or systematically crack it.

b) Challenge-response (or One-Time Pad)

The theory is password which can be used only once. To log in, the user contacts the remote machine, which displays a number as a challenge. The user types the challenge number into the card, along with its personal identification number (PIN). The key calculates a response and displays it. The user then types the response into the remote computer as user's one-time password.

Electronic keys, badges, and smart cards are gaining acceptance as authentication devices and as access devices for information system and computer rooms. People are becoming increasingly familiar with this type of authentication. The disadvantage of these methods is that they require either the installation or the purchase of additional hardware (such as card readers) . You might lose the key or equivalent, it might be stolen from you, or someone might borrow it and duplicate it.

---

*1 The word "cracker" has been firmly defined as a person exceptionally talented with computers who often misuses that skill.

c) Biometrics

The theory is the use of user's characteristics to provide positive personal identification. Examples are physiological or behavioral traits, such as your fingerprint, handprint, retina pattern, voice, signature, or keystroke pattern. Biometric systems compare your particular trait against the one stored for you and determine whether you are who you claim to be. Although biometric systems occasionally reject valid users and accept invalid ones, they are generally quite accurate. The disadvantage of these methods is that they require either the installation of special programs or the purchase of additional hardware (such as fingerprint scanners etc). Many people just don't like being measured, there is quit a bit of personal resistance to using them. These methods can't change the identification number.

2-1-2 Our Authorized Method

a) Method

Our system employs a method of " Challenge-response " where identification numbers are changed every time of required authentication. The system uses "Question and Answers" instead of identification number. The question is simple, and it is based on "private life or past private events", but the answer is different each other from an individual by a difference of "memory and experience". (see examples in Table 1)

Table 1 Example of Question and Answers

1. **Question**	How long did it take to walk to your elemental school ?
Answers	less than 5 min, 5~10 min, 11~15 min, 16~20 min 21~25 min, 26~30 min, 31~35 min, more than 36 min
2. **Question**	How long did it take to your high school ?
Answers	less than 15 min, 15~30 min, 30~45 min, 46~60 min 61~75 min, 76~90 min, 91~120 min, more than 121 min
3. **Question**	How many desks have you bought ?
Answers	None, 1, 2, 3, 4, 5, 6, more than 7
4. **Question**	How many bags have you bought ?
Answers	None, 1, 2, 3, 4, 5, 6, more than 7
5. **Question**	How long have you swum at a time ?
Answers	can't swim, 0~25 m, 26~50 m, 51~100 m 100~200 m, 200~500 m, 500~1000 m, more than 1001 m
6. **Question**	What area do you want to live most in Japan?
Answers	Hokkaido, Tohoku Kanto, Cyuubu Kinki, Chugoku, Shikoku, Kyushu
7. **Question**	What country do you want to visit most ?
Answers	U.S.A, Americas (expect U.S.A), Australia & NZ, Europe Japan, Asias (expect Japan), Africa, other
8. **Question**	How many films do you watch in movie theater in a year ?
Answers	None, 1, 2, 3 , 4, 5, 6, more than 7

2-2 Trust in Identifying Number

Trust in identifying number is based on probability and statistics (permutations and combinations). [3] If we set X, Y and Z as

X : Total number of questions , Y : Number of prepared questions and Z : Number of possible selections of answer, where questions are independent and orthogonal each other and selections are also independent and orthogonal,

The probability of getting one success in Y independent trials is

$$p=(1/Z)^Y \qquad (1)$$

The number of ways in which Y objects can be selected from a set of X distinct objects is

$$xC_Y = X!/Y!(X-Y)! \quad (2)$$

The number of permutations of Y objects selected from a set of X distinct objects is

$$xP_Y = X!/(X-Y)! \quad (3)$$

(1) and (2) are trusted for masquerade*2, and (3) is trusted for playback*3

3 Our System Designed

We designed a system on the basis of method described in 2-2 and practical operation as shown in Figure 1

3-1 System Environment

The system's flow is: 1) authorized software must be implemented to a server computer beforehand, 2) the server computer sends an user a question which could be answered only by the user reflecting his/her private life or past private events, 3)the user answers to the question, 4) the server computer authenticate

The user require any special hardware nor software to be implemented, because our system apply world wide web of internet technology. Our system employs only a browser software on a popular operating system (examples : windows95, MacOS, etc), and authorizing side employs a world wide web application and data base (question and answers) .

① an user requests for log in, and input user's name
② request of Question and Answers being responsed to the name
③ response of Qustion and Answers. Qustions are selected at random.
④ send only questions to user side
⑤ exhibit of questions and change order of questions
⑥ answer to questions and the user's answers
⑦ replay of answers to authorizing side
⑧ verification compare registration answer A and user's answer A*

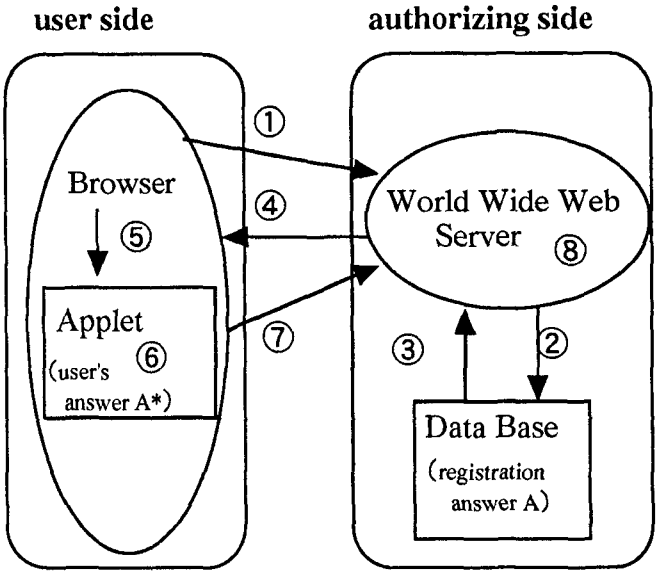

Fig. 1 Practical Operation and Data Flow in Our System

3-2 Trust in Our system

Our system registration: ;Total number of questions : X=200 , Number of prepared questions : Y=8 and Number of possible selections of answers : Z=8.

The probability of getting 1 success in 8 independent trials is

$$(1/8)^8 = 4.9 \times 10^{-4},$$

*2 Posing as an authorized user, usually in an attempt to gain access to a system.
*3 The recording of a legitimate message and the later, unauthorized resending of the message.

The number of ways in which 8 objects can be selected from 200 set of n distinct objects is

$_{200}C_8 = 5.5 \times 10^{13}$

The number of permutations of 8 objects selected from a set of 200 distinct objects is

$_{200}P_8 = 2.2 \times 10^{18}$

3-3 Speed of The Authentication

We measured speed of the authentication procedure between user entry and the end of authentication.

The system's operation is ; preparation of question and answers(a) + transmission of application software(b) + user's answers to the question(c) + transmission of answers(d) + certification judgment(e)

(a), (d), and (e) have few seconds, (c) depends on responses of user, (b) have long time, because our application software is large (about 2 MB). Consequently the speed of the authentication can be defined as an approximation to the transmission speed of application software(b).

Time of the authentication = Size of application software / Speed of transmission (4)

Our system uses two media : ethernet cable (transit speed was 1MB/sec) and telephone line (transit speed was 4kB/sec) . Time of the authentication by the ethernet cable and telephone line were about 3 seconds and about 500 seconds respectively.

4. DISCUSSION

The probability that cracker who doesn't know an answer answers it accidentally is 4.9×10^{-4}, and there are total 5.5×10^{13} different ways of preparation of question . The number of 4.9×10^{-4} is small compared with other crypt systems [4] . Other popular crypt systems use the same identification number (key) every time, but our system uses one of identification number of 5.5×10^{13}. It is difficult for a cracker to pretend to be an authorized user.

There are altogether 2.2×10^{18} permutations of the preparation of questions in total questions. It is difficult for cracker to doing playback . If a system increases total number of questions, preparation number of questions and selection number of answers, the system's trust is improved. But labor for preceding registration of question and answers increases, and time for user's answers to the question increases, too. Optimized setting becomes necessary in user's environment.

It is not necessary for users to remember precise passwords and changing passwords. It is not necessary for users to have special operation to be conscious of encoding nor decoding keys, and it is not necessary for users to require any special hardware nor software to be implemented.

But speed of the authentication depended on the data transfer capability between computers. The system employing a small transfer capacity is slow.

5. CONCLUSION

We devised a new method of authentication. The point of enhancing system performance was to keep age independence of users and time independence of historical experience by the users when we select assemblies of " question and answer " to users. The practicability of our system were verified and the next step to improve system performance and robustics was clarified. Speed of the authentication mainly depended on the size of the application software and the speed of transmission.

REFERENCES

1. Garfinkel, Simon and Spafford, PRACTICAL UNIX & INTERNET SECURITY 2nd Ed, O'Reilly & Associates Sebastopol (CA),1996
2. Deborah Russell, G.T. Gangemi Sr., COMPUTER SECURITY BASICS, O'Reilly & Associates Sebastopol (CA),1991
3. John E.Freund, Gary A. Simon, MODERN ELEMENTARY STATISTICS 8th Ed, PRENTICE HALL(NJ),1992
4. Simson Garfinkel, Pretty Good Privacy,O'Reilly & Associates Sebastopol (CA), 1995