Simultaneous Authentication System for Cooperation Verification

Kenta Soneda, Akane Ito, and Manabu Okamoto

***Abstract*—Various situations exist in which enhanced security procedures require that two or more people work together and authenticate at the same time. For example, police personnel or security guards carrying cash must always work in pairs so that if one of them is incapacitated, the other person can complete the mission. In principle, this also enables one partner to stop the other from carrying out any illegal act. However, the question remains as to how a manager can verify that two people are actually working together. We propose a simultaneous authentication system that utilizes smartphones, Twitter, and a cross-password technique to verify whether two persons are really at the same place at the same time; that is, working together cooperatively.**

***Index Terms*—Cross-password technique, enhanced security, simultaneous authentication, Twitter.**

I. Introduction

Many organizations utilize enhanced security procedures that require multiple individuals to work cooperatively and authenticate simultaneously. For example, banks may have a secret safe or strong box that can only be opened by two persons working in concert. As shown in Fig. 1, such a safe may have a locked door that requires that a pair of keys, A and B, be inserted and turned at exactly the same time in order to open. If the time at which the keys are turned is out of sync by more than a specified fraction, the door does not open. Further, the distance m between A and B is longer than the reach of a person's open arms, such that one person with two keys cannot open the door.

We call this kind of authentication system "simultaneous authentication." The concept underlying this system can be applied to other scenarios. For example, police personnel or security guards carrying cash must work together at all times because it is safer than one person working alone, and they can also check on each other. However, a manager who wants to verify that personnel in the field are actually working cooperatively may find it difficult to verify this condition. Such a manager could make a phone call to one of them and, after carrying out proper identification procedures, tell him/her to "Please keep this telephone online and pass it to your partner." The manager could thereby confirm that they are indeed working cooperatively, but this method would be burdensome.

We propose a simultaneous authentication system that easily enables confirmation as to whether two persons are at the same place at the same time via the Internet. In this scenario, we assume that all users have an information and communications technology (ICT) device such as a notebook PC or smartphone to perform authentication. Fig. 2 depicts our simultaneous authentication scenario. All persons with an ICT device authenticate at the same place and at the same time.

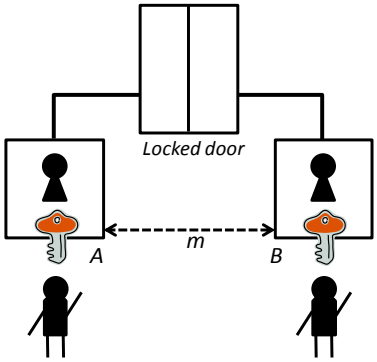

Fig. 1. Secure box in bank.

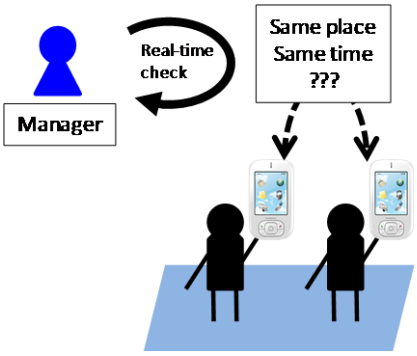

Fig. 2. Simultaneous authentication scenario.

II. Related Work

Location-based authentication [1]-[7] and monitoring and tracking systems [8] are broadly related to our proposed system,

All parents want to keep their children safe. GPS tracking and monitoring systems designed for child tracking provide parents the assurance that their children's location can be accessed at any time. Such systems usually provide the following:

- Ease locating children
- Knowledge of where a child is at all times
- A movement log

GPS tracking systems are designed to be compact and portable. Thus, GPS devices can easily be clipped onto children's belts, or simply placed in their backpacks, pants, or jacket pockets. Live-streaming tracking system data are easily

Manuscript received November 3, 2014; revised March 6, 2015.

The authors are with Kanagawa Institute of Technology, Japan (e-mail: gaku.kamoto@gmail.com, gintonic@sea.plala.or.jp, manabu@nw.kanagawa-it.ac.jp).

DOI: 10.7763/IJIEE.2015.V5.576

accessible from a computer to view everywhere a child has been and their exact location in real-time. However, these monitoring and tracking systems cannot be used for simultaneous authentication. Two persons can have separate GPS devices that a manager can check to verify that they are at the same place with the same GPS data. However, one individual can give his/her GPS device to the other and they will still appear to be at the same place at the same time on a GPS system, as illustrated in Fig. 3.

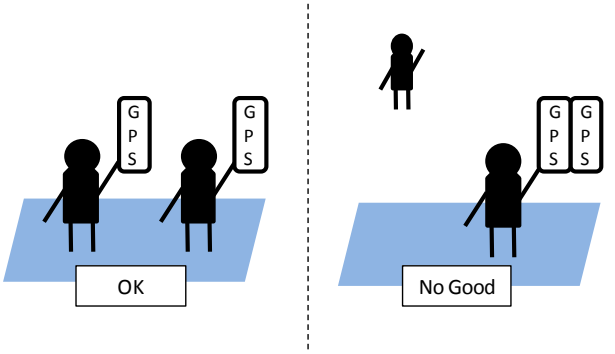

Fig. 3. "No Good" situation.

Instead of a GPS device, a mobile phone can be used for more reliable checking. A mobile phone cannot be passed to other persons easily because it is a very "personal" device that usually has much secret and personal information. However, there is still a problem with this scenario. A mobile phone can be password-locked and loaned to another person temporarily. In addition, GPS and mobile phones cannot be used underground and inside some buildings.

In this paper, we propose a simultaneous authentication system that uses not only GPS but also cross-password and Twitter [9]. Using Twitter makes the system more reliable because a Twitter account cannot be passed to another person as a mobile phone can.

III. Proposed Method

"Simultaneous authentication" is accomplished as follows:

- We assume that smartphones are being used. A smartphone is very personal device that can use GPS and the Internet. Most people will not lend their smartphone to anyone.
- A "cross-password" system is utilized to ensure simultaneity.
- Twitter is utilized because, in addition to a Twitter account being a personal possession, real-time tweets can ensure simultaneity and Twitter can add GPS data to tweets.

We assume that two persons *P* and *Q* have their own smartphones and Twitter accounts that are registered in the simultaneous authentication system. Twitter [9] is a micro-blogging network with real-time posts that are limited to 140 characters.

We implemented the simultaneous authentication system (SAS) as a website that users can access via PC or smartphone (Fig. 4). Fig. 5 shows the sequence of actions that take place in our proposed system. We describe the system in detail from the point of view of user P (but both P and Q need to carry out the same action at the same time) below.

1) P accesses SAS with his/her smartphone to perform simultaneous authentication. Q also accesses the same SAS site at the same time. P logs in to his/her SAS account with his/her password. Fig. 4 shows the login form for SAS.

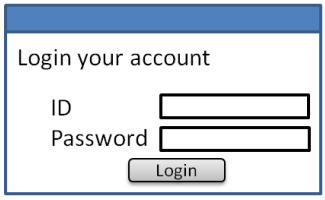

Fig. 4. SAS login form.

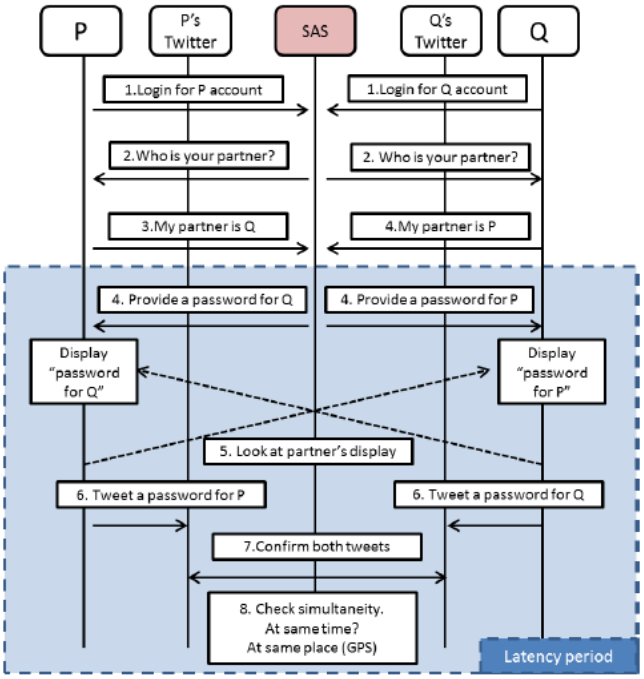

Fig. 5. Sequence of actions in our proposed system.

2) To perform simultaneous authentication, SAS asks P about his/her partner, at which point P selects or inputs his/her partner in the form on the SAS site and presses "together now" if P is with Q. Figure 6 shows this form.

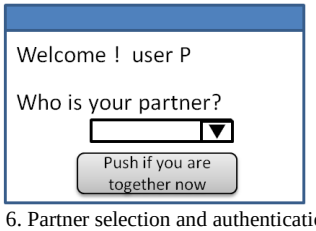

Fig. 6. Partner selection and authentication.

3) P and Q need to be side by side and press the button at the same time. SAS then starts to count the latency period, with P and Q needing to complete all of the following steps to conduct simultaneous authentication in a limited time period.
4) SAS then provides cross-passwords for users in their smartphone display. In fact, SAS provides P with a password for Q and Q with a password for P. Fig. 7 shows

P's display, which indicates Q's password.

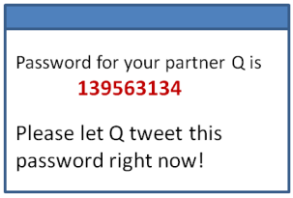

Fig. 7. Cross-password.

5) P and Q both look at each other's smartphone in order to obtain their respective password.
6) P and Q launch their Twitter application on their smartphones and tweet with their respective password. They can also add GPS information to their tweets if they so desire. Fig. 8 shows an example of Q's tweet.

Fig. 8. Cross-password tweet.

7) SAS receives both P's and Q's tweets with their passwords.
8) SAS checks the time lag, the difference between the time of P's tweet and that of Q. If both passwords on their tweets are correct and the time lag is almost zero, SAS confirms that P and Q are at the same place at the same time. If both P and Q add their GPS information to their tweets, SAS can also check the latitude and longitude they provide when they make a tweet and confirm that they are at the same place.

IV. Advantages and Security Analysis

Our proposed system has the following advantages:

- GPS information can be used as in existing systems.
- A smartphone is a very personal belonging and is seldom loaned to another person by the owner.
- The cross-password technique makes it difficult for users to be deceptive; they need to look at each other's display side by side.
- A Twitter account is personal and is seldom loaned (if ever) to another person by the owner.
- Twitter can add GPS data; thus, a separate GPS application is not needed.

Obviously, P could reveal his/her password to Q on the telephone or via email or network messenger. However, they would need more time than that required just to mutually check each other's screen. Consequently, the limited time is very important. If the allotted time is long, they can easily cheat. However, when the time is short, they would have to look at the password on the screen, launch the telephone or messenger application, connect to the partner, and reveal the password within this short time.

We have three kinds of restriction time, as shown in Fig. 9.

1) Request time: We assume that both user P and Q push the request button to display the cross-password at the same time. The request time is the difference between P's push time and Q's push time. We assume that this time is almost zero because they push the button side by side, looking at each other and saying, "Ready? 1-2-3-Go!"
2) Tweet time: This is the same as Request time, but for tweets. We assume that both user P and Q tweet at same time, side by side and looking at each other. We assume that this time is also close to zero.
3) Total time: Total time is the time between request time and tweet time. This is the most important time and must be chosen appropriately. Within this time, both users have to view each other's display and tweet that password.

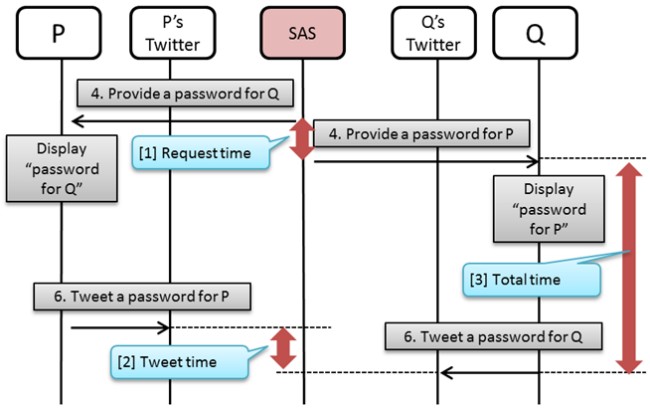

Fig. 9. Time period.

To determine the value for this time, we conducted a user test. In this test, we used browsers on a tablet PC. All testers were university students.

In this test, we had seven test groups. Groups A–E were normal groups. Each group consisted of two persons who performed the authentication correctly.

Groups F and G were attack groups. Group F consisted of only one person who operated two PCs by him/herself. Group G consisted of two persons in separate locations who exchanged messages using Internet messenger software.

Each group performed the simultaneous authentication five times while we measured the time. In particular, we recorded the three kinds of restriction time as test data and, moreover, we recorded the longest ("worst") value. We show these times in Table I.

Almost all groups achieved times of almost 0 s for Request and Tweet times. Attack groups F and G can also authenticate at the same time and achieve times of less than 2 s. Using messenger software does disadvantage the attackers with respect to time. One person must say "I got it" on the messenger and the other person must push the button or tweet. However, they can achieve times of less than 2 s.

It is difficult to decide a limit for the Total time. However, less than 10 s is reasonable for correct authentication. Authenticators sometimes fail, but when they do so, they must try again.

Attack groups F and G require more time. Especially for group F, it required serious coordination for one person to operate two PCs simultaneously and input two passwords. In addition, group G required time to reveal the password in the display to each other by messenger software and then tweet. However, the shortest time is 10 s. Over that time, we may be tricked. When an attacker uses a single smartphone, attack is

difficult. However, with two smartphones, it is easier.

The GPS information embedded in tweets effectively thwarts this situation because the latitude and longitude can be obtained from the tweet. If the latitude and longitude of the tweets are not the same, then SAS will not validate their claim.

TABLE I: USER TEST (S)

	Request time	Tweet Time	Total Time
A	< 1	< 1	7
B	< 1	< 1	14
C	< 1	1	6
D	1	< 1	8
E	< 1	< 1	7
F	< 1	< 1	18
G	1	2	16

V. CONCLUSION

In this paper, we proposed a simultaneous authentication system that uses smartphones, cross-password, and Twitter to verify whether two persons are at the same place at the same time and working cooperatively.

In future work, we plan to evaluate this system through extended user tests. In particular, we need to determine the time-up value: In our current test, 30 s is the time limit. When the time is less than 30 s, even in the right situation, the system fails. Conversely, a time limit longer than 30 s gives attackers enough time to easily tell their partner the cross-password. Thus, we need to set an appropriate time for real use.

REFERENCES

[1] D. E. Denning and D. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 2, pp. 12-16, 1996.

[2] A. I. G.-T. Ferreres, B. R. Álvarez, and A. R. Garnacho, "Guaranteeing the authenticity of location information," *Pervasive Computing, IEEE*, vol. 7, no. 3, pp. 72-80, 2008.

[3] G. T. Becker, S. C. Lo, D. S. De Lorenzo, P. K. Enge, and C. Paar, "Secure location verification," *Data and Applications Security and Privacy XXIV*, Springer Berlin Heidelberg, 2010, pp. 366-373.

[4] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. the 10th workshop on Mobile Computing Systems and Applications*, ACM, 2009, p. 3.

[5] W. Luo and U. Hengartner, "Veriplace: A privacy-aware location proof architecture," in *Proc. the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*, ACM, 2010, pp. 23-32.

[6] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," in *Proc. 2011 IEEE INFOCOM*, 2011, pp. 1889-1897.

[7] H. Takamizawa and K. Kaijiri, "A web authentication system using location information from mobile telephones," in *Proc. the IASTED International Conference Web-Based Education (WBE 2009)*, 2009.

[8] GPS Tracking Children. [Online]. Available: http://www.tracking-system.com/for-consumers/gps-tracking-children.html.

[9] Twitter. [Online]. Available: http://twitter.com

Kenta Soneda is a student at the Kanagawa Institute of Technology. His research interests include web application security, anti-phishing, single sign-on, authentication methods, attribute exchange, password authentication, cloud computing, portable computing, and portable security.

Akane Ito is a student at the Kanagawa Institute of Technology. Her research interests include web application security, anti-phishing, single sign-on, authentication methods, attribute exchange, password authentication, cloud computing, portable computing, and portable security.

Manabu Okamoto received B.S. and M.S. degrees in mathematics from Waseda University in 1995 and 1997, respectively. In 2010, he received a doctoral degree in the field of global information and telecommunication from Waseda University. He is currently an associate professor at Kanagawa Institute of Technology.