Physical Trust-based Persistent Authentication

Masahiro Fujita
Graduate School of Science and Technology
Shizuoka University
Hamamatsu, Japan

Shiori Arimura, Yuki Ikeya
Graduate School of Informatics
Shizuoka University
Hamamatsu, Japan

Christian D. Jensen
Department of Applied Mathematics and Computer Science
Technical University of Denmark
Kgs. Lyngby, Denmark
cdje@dtu.dk

Masakatsu Nishigaki
Graduate School of Science and Technology
Shizuoka University
Hamamatsu, Japan
nisigaki@inf.shizuoka.ac.jp

***Abstract*— Recently companies have applied two-factor user authentication. Persistent Authentication is one of the interesting authentication mechanisms to establish security and usability of two-factor authentication systems. However, there is room to improve its feasibility and usability. In this paper, we propose a new type of persistent authentication, called Persistent Authentication Based On physical Trust (PABOT). PABOT uses a context of "physical trust relationship" that is built by visual contact between users, and thus can offer a persistent authentication mechanism with better usability and higher feasibility.**

***Keywords*— user authentication; persistent authentication; physical trust; visual contact**

I. INTRODUCTION

Recently information security incidents have been increasing dramatically. It forces companies to improve the security of their information systems. A typical solution to the requirement is to apply two-factor user authentication to the systems. By using the second factor (called factor B) in addition to the existing factor (called factor A), the security strength of their system would be improved from "the strength of factor A" to "the strength of factor A plus the strength of factor B". However, this solution naturally leads to worse usability.

Persistent authentication [1] is an effective approach to mitigate the situation. The main idea of persistent authentication is to replace "repetitive re-authentications" with "tracking". In the case where the existing authentication (factor A) is kept unchanged and the idea of persistent authentication is applied to factor B, the authentication works as follows. First, a user, who wants to log into some PC in a company, has to log into the PC by using two-factor authentication. After that the persistent authentication system starts tracking the user by e.g. sensors or cameras. While being tracked by the system, the user can log into any other PC in the company by showing only factor A, or without factor B. This means that the persistent authentication system can provide the user with two advantages; (i) almost the same usability as the existing authentication protected by only factor A and (ii) effectively the same security strength as the two-factor authentication protected by both factor A and factor B.

However, there is room for improvement from the following two perspectives. The first one is a feasibility perspective. The concept of persistent authentication is to combine traditional authentication mechanisms with sensing technologies and tracking capabilities offered by a "smart environment". On the other hand, a smart environment is not always available. If we try to apply persistent authentication to current environments, another tracking mechanism instead of sensors and/or cameras is needed. The second one is a usability perspective. The ideal concept behind persistent authentication is "calm" [4], which means that it should require minimal attention from users [1]. On the other hand, persistent authentication requires users to use conventional authentication mechanisms in the initial authentication. It is preferable if we can reduce the burden of users in the initial authentication.

To respond to these issues in this paper, we propose a new type of persistent authentication, called Persistent Authentication Based On physical Trust (PABOT), which uses a context of "physical trust relationship" that is built by visual contact between users [10]. PABOT introduces "human abilities" into the concept of persistent authentication, allowing it to provide an authentication mechanism with better usability and a tracking mechanism with higher feasibility.

The organization of this paper is as follows. Section II outlines the idea of persistent authentication and its application for two-factor user authentication. Section III introduces our proposal and Section IV discusses the effectiveness of our approach. Section V describes related works. Finally, Section VI presents our conclusions.

II. PERSITENT AUTHENTICATION

A. Persistent Two-Factor Authentication

The main idea of persistent authentication [1] is to replace "repetitive re-authentications" with "tracking". After a user

978-1-4673-7828-4/15/$31.00 ©2015 IEEE

has been authenticated once, this authentication will continue while the persistent system is tracking the user.

As a leading example let us now consider a company's private cloud, in which there are many terminal PCs available for users in the company and each user can access the same computing environment from any PC. In the case of persistent authentication applied to two-factor authentication, the authentication works as follows. In the "initial authentication", a user, who wants to log into some terminal PC in the private cloud, has to log into the PC by using two-factor authentication (factor A and factor B). After that the persistent authentication system starts tracking the user. While being tracked by the system, the user can log into any other terminal PC in the private cloud without re-authentication.

It should be noted here, however, that nowadays password authentication is supported on every single PC as the most commonly used means of authentication. Namely, almost all companies have already implemented an authentication system with factor A. In this situation, companies and users often tend to stay with the existing legacy system. The possible reasons behind it are cost (replacement requires a financial infusion), usability (users get used to it), and/or momentum (once used, security countermeasures will not be uninstalled unless somebody proves that it is absolutely unnecessary). In such a case, we can keep factor A unchanged and apply the idea of persistent authentication to factor B.

In this scenario, the initial authentication is required with both factor A and factor B, but the subsequent authentication can be done by showing only factor A, or without factor B, as long as the user is tracked. This means that the persistent authentication system can provide the user with two advantages; (i) almost the same usability as the existing authentication protected by only factor A and (ii) effectively the same security strength as the two-factor authentication protected by both factor A and factor B. This strategy, while achieving effectively the security strength of two-factor authentication, has almost the same usability as that of conventional systems protected by one factor. This is what we are focusing on in this paper.

B. How to Track Users

The original concept of persistent authentication, called Persistent Authentication In Smart Environments (PAISE) [1][2][3], is to combine traditional authentication mechanisms with sensing technologies and tracking capabilities offered by "smart environment". In other words, PAISE relies on available sensors to track users from the location where they are authenticated to the location where the authentication is thereafter required.

On the other hand, not all companies have a dedicated smart environment at the present time. If we try to apply persistent authentication to current environments (e.g. the company's private cloud which we described in Section II.A), it causes the following problem.

Problem 1: the lack of a smart environment

(i) It costs too much to prepare sensors and/or cameras.

(ii) The accuracy of indoor user localization using sensors and user identification using surveillance cameras is still not enough to track users.

(iii) Users are not used to being tracked by sensors/cameras. Some users may feel psychological resistance to camera tracking.

This suggests that another tracking way is needed instead of sensors and/or cameras. One possible approach to this issue could be to use "observation skills" of surrounding users. A detailed discussion will be made in Section III.C.

C. Calm Authentication

The ideal concept behind persistent authentication is "calm" [4]. On the other hand, persistent authentication requires users to use conventional authentication mechanisms, e.g. passwords or tokens, in the initial authentication. It is preferable if we can address the following problem.

Problem 2: The usability of initial authentication

The initial authentication should require minimal attention from users, or we should reduce the burden of users in the initial authentication as much as possible.

One possible approach to this issue could be to use "chain of trust" between users, such as the system authenticates user U and user U identifies user V, therefore the system can trust user V. A detailed discussion will be made in Section III.B.

III. Persistent Authentication Based On Physical Trust

A. Preliminaries

In this paper, we propose a modification of persistent authentication, called Persistent Authentication Based On physical Trust (PABOT), which uses a context of "physical trust relationship" that is built by the visual contact between users [10]. PABOT introduces "human abilities" into the concept of persistent authentication for solving both of Problem 1 and Problem 2 posed in Section II.B and Section II.C, respectively.

Let us explain our conceptual scenario here with the example of the company's private cloud described in Section II.A. There are many terminal PCs available for users in the company and so far all the PCs have been protected by the authentication using factor A (e.g. user ID and password). The company has now enhanced the security by adding the second authentication factor B (e.g. finger/palm vein). For several reasons the company implemented the idea of persistent authentication to the added authentication mechanism (factor B), while the existing authentication mechanism (factor A) is kept unchanged. The updated authentication system is now: the initial authentication is required with both factor A and factor B, but the subsequent authentication can be done by showing only factor A, as long as the user is being tracked.

PABOT will be used under the following assumptions.

1. Each user in the company has his/her own smartphone, and all company members are listed in an Address Book application in each smartphone.

2. Every single smartphone can detect when it enters/leaves any area. During the stay in an area, each smartphone can find the presence of all smartphones in the area. (A similar mechanism was implemented in i/k-Contact system [10] and hence it is not an inappropriate assumption.)
3. Users' smartphones can contact wirelessly with a persistent authentication server in the company. This server holds the "persistence status flag" for every user. A user, whose persistence status flag is "true", will be authenticated by showing only factor A when he/she uses any terminal PC in the company.
4. Users can check each other by visual contact all over the area.

Hereafter in this paper, we refer to a user who has been authenticated by the initial authentication as a "trusted user".

B. Authentication mechanism by visual contact

PABOT uses context information of "physical trust relationship" between a trusted user and an incomer in an area. This means that by using visual contact, PABOT provides an authentication mechanism to transfer authenticity from trusted users to incomers. In PABOT, "authentication by visual contact" works as follows (also, see Figure 1).

1. When user U enters an area, his/her smartphone sends an "entering message" to the persistent authentication server.
2. The persistent authentication server sends a "notification request" to each smartphone of all the trusted users in the area. The smartphones popup an alert with vibration/sound toward each owner, displaying "user U enters the area" on the screen.
3. The trusted users check user U by visual contact, and then verify whether he/she is really the same person as the displayed user.
4. If trusted users are suspicious of the entering user, each trusted user sends an NG report to the persistent authentication server. To be more precise, the NG button is also displayed on the screen of each smartphone, and the trusted users are prompted to tap the NG button when something is wrong.
5. If user U is a legitimate user, the persistent authentication server must receive no NG report by all trusted users. Then the server is able to recognize that a user who just entered the area is certainly user U, and then sets the persistence status flag for user U to be "true".
6. After that, when user U is going to use some terminal PC in the company, he/she enters factor A (typically user ID and password) to the PC.
7. If this authentication is confirmed, then the PC sends the persistent authentication server a request to check the persistence status of user U.
8. In the case where user U's flag is "true", he/she can use the PC immediately. Otherwise he/she is required to show factor B in use of the PC.
9. Once user U gets out of the area, his/her smartphone sends a "leaving message" to the persistent authentication server. Then the server sets the persistent status flag for him/her to be "false".

Thus, in this authentication mechanism, the burden for an incomer (user U) in doing his/her initial authentication can be reduced when he/she is confirmed by visual contact. On the other hand, what the trusted users need to do is to take a look at a user who just entered the area and check whether he/she is a legitimate one or not. This behavior is a part of daily behavior between colleagues in a company, so it does not impose a burden on them. For these reasons, it is expected that PABOT will offer better usability to persistent authentication and therefore it solves Problem 2 posed in Section II.C.

It is noted that PABOT can be applicable in the case where more than single trusted users have already stayed in an area. This means that the first user who entered an area needs to do his/her initial authentication by entering factor B (in addition to factor A). When he/she passes the initial authentication, the user is authenticated as a trusted user and his/her persistent status flag is set to be "true" in the persistent authentication server.

C. Tracking mechanism by visual contact

PABOT uses context information of "physical trust relationship" between trusted users in an area in order to provide a tracking mechanism to keep the authenticity of trusted users confirmed in the initial authentication. In PABOT, "tracking by visual contact" works as follows.

1. People often take a casual look around while they are doing something. Hence, in a situation where two or more trusted users are in the same area, they will see each other naturally. That is, a kind of constant visual contact between trusted users is expected, as long as more than single trusted users have stayed in an area.
2. If a trusted user V is suspicious of another trusted user U, the user V sends an NG report to the persistent authentication server. Then the server sets the persistent status flag for user U to be "false"
3. It has not been clarified, but there are reports that an environment under watch by visual contact imparts psychological suppression effect to fraudulently acting users [11].
4. It is quite a normal situation for users to stay with their colleagues in a company. So it is expected that an environment under watch by familiar colleagues has not so much impact on faithfully acting users.

Thus, in this tracking mechanism, the visual contact has the equivalent effect as camera tracking. This mechanism is, so to speak, human eye tracking. Hence a flexible, robust and non-invasive tracking can be achieved without expensive surveillance systems. For these reasons, it is expected that PABOT will offer a better environment to persistent

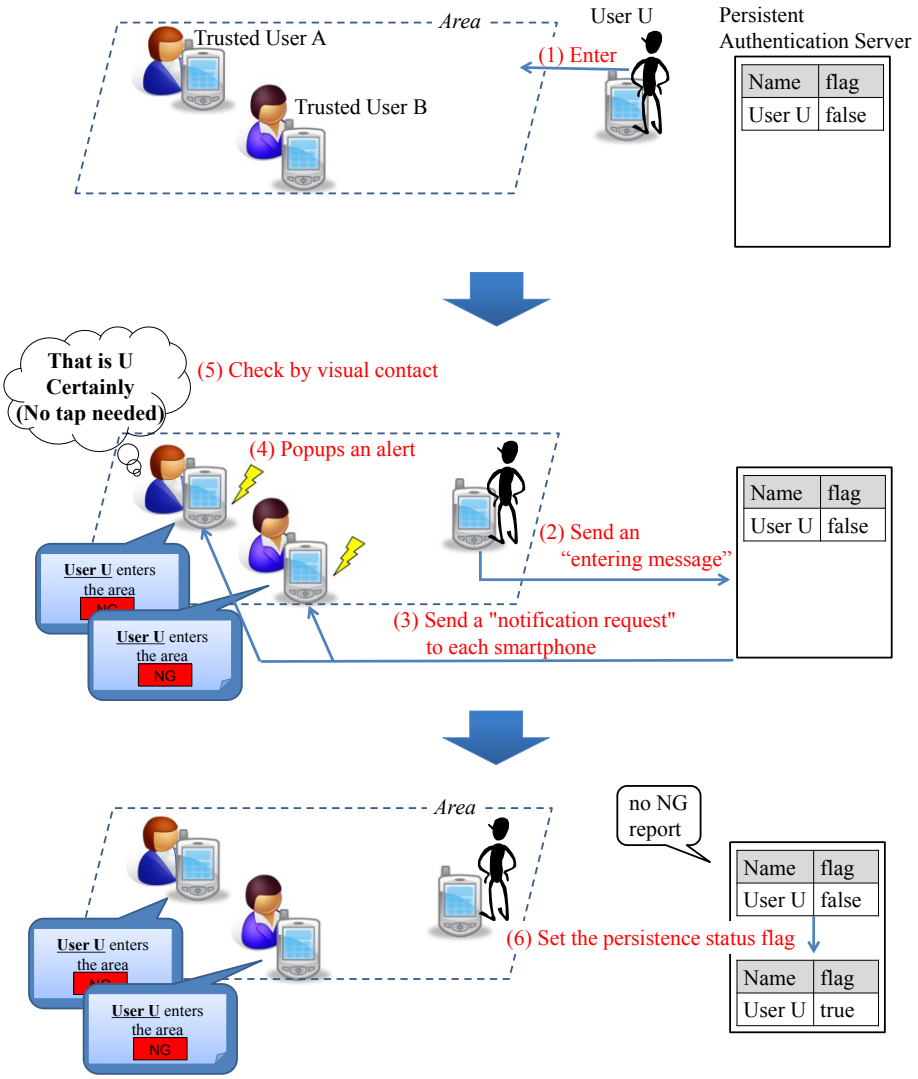

Fig. 1. Authentication mechanism by visual contact

authentication and therefore it solves Problem 1 posed in Section II.B.

It is noted that PABOT can be applicable in the case where more than single trusted users have stayed in an area. In other words, in the case where there is only one user remaining in an area, persistent status flags for the users is not set to be "true" even though he/she is trusted user.

IV. Discussion

A. Security

In this paper, we apply the idea of persistent authentication to the situation described in Section II.A; All terminal PCs in a company have already been protected by the authentication system with factor A. Then, for the purpose of enhancing security, the second factor B is added to the existing authentication system. Here the company wants to keep factor A unchanged and apply the idea of persistent authentication to factor B. In this scenario, the initial authentication is required with both factor A and factor B, but the subsequent authentication can be done by showing only factor A, as long as the user is being tracked.

In this paper, let us consider the case where an illegal outsider who wants to masquerade as user U steals the U's smartphone and gets in front of some terminal PC in the company with it. If no one is in the area, no visual contact occurs and the U's persistence status flag remains "false". So the illegal outsider is required to show both of factor A and factor B. Otherwise, if one or more trusted users are in the area, at least one trusted user will realize that the incomer is different from user U. So the illegal outsider cannot even enter the area. For these reasons, "the strength of factor A plus the strength of factor B" is guaranteed in PABOT.

B. Usability

As described in Step 5 in Section III.B, unless trusted users are suspicious of the entering user, each trusted user does not respond to alert sown in smartphone in Step 2 and no tap is needed in Step.4. Therefore, the burden in doing the persistency check can be almost zero. That is why, PABOT

can provide the user with almost the same level of usability as the existing authentication protected by only factor A, while achieving effectively the same security strength as the two-factor authentication (protected by both factor A and factor B).

The visual contact process that we use to provide an authentication mechanism is feasible because it is part of users' daily behavior. That is why, PABOT does not impose a burden on users.

V. Related Works

Corner and Noble [5][6][7] define a transient authentication mechanism, where all data in the system is encrypted and a small authentication token, worn by the user, is needed to provide access to the encrypted data, thus ensuring that access can only be granted when the token is in close proximity to the system. The token stores the cryptographic keys and the proximity mechanism is based on short range wireless communication. The definition of transient authentication by Corner and Noble is device centric, and authentication sticks to the device as long as the user is present, so restrictions are put on the users, e.g., they have to wear the authentication token. This creates problems when authentication tokens are forgotten, borrowed or lost. PABOT also uses a smartphone, but it is confirmed by visual contact between users that the smartphone is possessed by a legitimate user. Thus it is difficult for illegal users to steal or borrow a token.

Bardram et al. [8] define a context-aware user authentication mechanism, where users need a smart card to identify themselves to the system and an RFID based tracking system that is used to authenticate the user. This adds complexity to the users, by requiring them to carry two tokens, without offering significantly improved convenience, i.e., the user still has to insert the smart card into the system whenever authentication is required. In comparison, PABOT removes the need to perform repeated authentication actions, by conducting visual contact which is a part of daily behavior between users.

Klosterman and Ganger [9] define a continuous biometric-enhanced authentication mechanism, which uses a biometric authentication module, based on face recognition, to periodically re-authenticate users who are logged into the system. If, at some point, the biometrics of the user sitting in front of the monitor does not correspond to the biometrics of the authenticated user, re-authentication is required. This means that continuous authentication is achieved without additional requirements placed on the user, but their system authenticates a specific user at a specific location, whereas PABOT transfers the authentication from user to user using visual contact. It is an interesting similarity that face recognition is part of the process of visual contact.

VI. Conclusions

In this paper, we proposed a new type of persistent authentication, called Persistent Authentication Based On physical Trust (PABOT), which uses a context of "physical trust relationship" that is built by visual contact between users. PABOT has an authentication mechanism with better usability and a tracking mechanism with higher feasibility. We applied PABOT to a specific two-factor authentication and showed the effectiveness of the method. PABOT is still in the phase of its conceptual design. We need to implement an experimental system for PABOT and evaluate the system.

Acknowledgment

We wish to acknowledge valuable discussions with Ichiro Iida, Akira Shiba, Kazuaki Nimura, Yosuke Nakamura and Junya Kani of Fujitsu Laboratories Ltd. We are also grateful to the reviewers for their constructive comments and careful proofreading.

References

[1] M.S. Hansen el al., "Persistent Authentication in Smart Environment", in *Proc. 2nd Int. Workshop on Combining Context with Trust, Security and Privacy*, Trondheim, 2008, pp.31-44.

[2] H.I. Akram et al., "Identity Metasystem in Location Based Persistent Authentication", in *Proc. 3rd European Workshop on Combining Context with Trust, Security and Privacy*, Pisa, 2009.

[3] M.I. Ingwar and C.D. Jensen, "Remote Biometrics for Robust Persistent Authentication", in *Proc. 18th European Symp. on Research in Computer Security*, Egham, 2014, pp. 250-267.

[4] M. Weiser and J.S. Brown, "Designing calm technology", *PowerGrid Journal 1.01*, 1996.

[5] M.D. Corner and B.D. Noble, "Zero-interaction authentication", in *Proc. 8th Annu. Int. Conf. on Mobile Computing and Networking*, Atlanta, 2012, pp. 1-11.

[6] B.D. Noble and M.D. Corner, "The case for transient authentication", in *Proc. 10th ACM SIGOPS European Workshop*, New York, 2002, pp.24-29.

[7] M.D. Corner and B.D. Noble, "Protecting applications with transient authentication", in *Proc. 1st Int. Conf. on Mobile Systems, Applications and Services*, San Francisco, 2003, pp.57-70.

[8] J.E. Bardram et al., "Context-aware user authentication – supporting proximity-based login in pervasive computing", in *Proc. 5th Int. Conf. on Ubiquitous Computing*, Seattle, 2003, pp. 107-123.

[9] A.J. Klosterman and G.R. Ganger, "Secure continuous biometric-enhanced authentication", Tech. Rep. CMU-CS-00-134, May 2000.

[10] S. Arimura et al., "i/k-Contact: A context-aware user authentication using physical social trust", in *Proc. 12th Annu. Conf. on Privacy, Security, and Trust*, Tront, 2014, pp. 407-413.

[11] Gill, Martin and Angela Spriggs. *Assessing the impact of CCTV. London: Home Office Research*, Development and Statistics Directorate, 2005.