Multi-Observed Authentication: A secure and usable authentication/authorization based on multi-point observation of physical events

Shinnosuke Nozaki*, Takumi Takaiwa*, Masahiro Fujita†, Ayako Yoshimura†,
Tetsushi Ohki* and Masakatsu Nishigaki*
*Shizuoka University, Hamamatsu, Shizuoka 432-8011, Japan
†Mitsubishi Electric Corporation, Kamakura, Kanagawa, 247-8501, Japan
Email:nisigaki@shizuoka.ac.jp

***Abstract*—As business styles change, the damage from PC malware infections is expanding, and it is becoming increasingly difficult to fully protect against these threats using conventional authentication and authorization methods. Multi-factor authentication is one solution to this problem, but it involves the hassle of presenting multiple credentials every time authentication is required. While putting an expiration date on the authentication token obtained after multi-factor authentication can be an approach to improving the convenience by circumventing the requirement for re-authentication, if the user's PC is infected by malware, information assets can be accessed using this authentication token until expires. What is important is to ensure that the information assets have been accessed by the user and not by malware. In other words, the key is to confirm that the action of access to the information asset is performed by the users themselves. It is not necessary to explicitly ask the user to operate the smartphone. Therefore, we propose multi-observed authentication as a new method based on the concept of "confirmation of the occurrence of physical authentication/authorization actions by the user, in addition to the validity of the credentials (passwords/authentication tokens)."**

I. Introduction

In recent years, individuals and corporations have been struggling to cope with changes in business systems due to DX (Digital Transformation). As a result, damage caused by malware, such as Emotet, which steals credentials, is expanding. It becomes difficult to distinguish whether the credentials received by the authentication server from the PC are from a legitimate user or from malware, as long as the malware that stole the credentials resides on the PC. A typical solution to this problem is multi-factor authentication. This method proves the identity of the user by presenting several types of information (knowledge/possession/biometrics) that only a legitimate user has to the authentication server. This paper focuses on a multi-device multi-factor authentication, particularly a two-factor authentication where the first credential is presented from a PC and the second credential is presented from a smartphone [1][2][3]. Multi-device multi-factor authentication can be said to enhance security through a "multiplication of authentication." However, this multiplication forces users to present multiple credentials, which can lead to a decrease in convenience. When considering only improvements in convenience, it is feasible to use possession information (the fact that the user has a smartphone) as the second credential, and complete the second authentication by automatically confirming the proximity of the smartphone to the PC [4]. However, if malware enters the first credential behind the user's back while the user carrying a smartphone is using his PC for business, the second authentication will pass. In other words, this is synonymous with single-factor authentication. In order to improve convenience in multi-factor authentication, practices that separate authentication and authorization are widely used [5]. Authentication tokens are issued to users who have passed multi-factor authentication (authentication) at the initial access to information assets. These tokens have an expiry date, and within this period, it would be sufficient to present the authentication token (authorization) if the same user wants repeated access. However, in this case, the phase of authorization becomes a single-factor authentication (only the possession of the authentication token is confirmed). In other words, malware on the PC can easily misuse the authentication token without effort by just lurking until the legitimate user obtains it. If the need for multi-factor authentication comes from the need to prevent the misuse of a user's PC by malware, it is considered that it would be sufficient to confirm that the authentication/authorization was performed by the user themselves and not by malware, without the need for an additional separate credential. Therefore, we propose a new user authentication/authorization method (multi-observed authentication), based on the concept of "capturing the user's intention at the time of authentication/authorization as a physical event" and "simultaneously observing the physical event of the user presenting credentials (inputting passwords or using authentication taken) when accessing information assets".

II. Methodology

A. Concept

If we want to confirm that information asset access has been performed not by malware but by the user themselves, it can be sufficient to confirm the action of the information asset access through the legitimate user themselves, but not necessary to explicitly ask the user to operate their smartphone.

Therefore, we propose multi-observed authentication as a new method based on the concept of "confirming the occurrence of physical authentication/authorization actions by the user, in addition to the validity of the credentials (passwords or authentication tokens)". In conventional two-factor authentication/authorization, a smartphone was used as the device to receive the input of the "second factor credentials" from the user and transmit them to the authentication server/file server. In contrast, it should be noted that in multi-observed authentication, a smartphone is used as the second observer to verify the input of the "first factor credentials" of the user. Later, in B and C, we will explain "multi-observed authentication" and "multi-observed authorization" respectively, applying this concept to two-factor authentication and two-factor authorization.

B. Multi-Observed Authentication

The information for multi-observed in this method is the password entered by the user at the beginning of the access to the information assets. In this method, it is assumed that any keyboard input to the PC will be simultaneously input to the smartphone as well. Specifically, the Bluetooth unit of the wireless keyboard is modified to receive inputs from the wireless keyboard on both the PC and smartphone simultaneously. By verifying the credentials entered on the PC on the smartphone as well, both convenience (entering passwords only on the PC) and security (verifying passwords on both the PC and smartphone) can be achieved simultaneously.

C. Multi-Observed Authorization

The information for multi-observed in this method is the mouse operation occurring during the access to the information assets by the user. When the user clicks on the file icon, a dialog box containing an "OK" button is displayed on the PC screen. The user then clicks on the "OK" button via the mouse operation. In this method, it is assumed, as in the multi-observed authentication method, that the mouse operation on the PC is simultaneously input to the smartphone. By verifying the mouse click on both the PC and smartphone, security can be ensured through the confirmation of authorization operations by both devices, while minimizing the decrease in convenience (by adding just one action of clicking the "OK" button when using authentication tokens).

III. Evaluation

To verify the convenience, privacy, and safety of the multi-observed authentication/authorization method proposed in the previous section, we implemented a file management system equipped with four types of security mechanisms: the conventional two-factor authentication/authorization using commonly used PCs and smartphones, and the proposed two- observed authentication/authorization method. We had 20 experiment participants (university students majoring in engineering/information fields) perform comparative experiments. After each experiment participant had experienced the system, we received evaluations. We employed a questionnaire method for evaluation, asked them to rate the method on a 7-point Likert scale ("-3": Support for the conventional method, "0": neither, "3": Support for the proposed method) and to provide reasons for their evaluations.

A. Authentication

In response to the question "Which method do you want to use from the perspectives of convenience and privacy?", the results were "-2" for 5%, "-1" for 30%, "0" for 5%, "1" for 30%, "2" for 20%, and "3" for 10%. The reason the experiment participants evaluated the proposed method favorably was that no operation on a smartphone was needed. The reason the experiment participants appraised the conventional method was their feelings of mistrust towards the transmission of credentials to a terminal different from their own operating PC in the proposed method. From this, it was confirmed that ensuring transparency is essential in multi-observed authentication. Furthermore, when asked how their respective evaluations would change if the frequency of authentication increased, the result was a shift in the evaluation toward the proposed method. From this, it was confirmed that in scenarios where the demand for convenience increases, the evaluation of the proposed method (two-observed authentication) would rise.

B. Authorization

In response to the question "Which method do you want to use from the perspectives of convenience and safety?", the results were "-2" for 5%, "0" for 5%, "1" for 30%, "2" for 25%, and "3" for 35%. The reason the experiment participants evaluated the proposed method favorably was that safety improved with the trivial addition of a single mouse click. The reason the experiment participants appraised the conventional method was that even though it needed only a single click to confirm the user's intention, the conventional method was still more convenient than the proposed one. Furthermore, when asked how their respective evaluations would change if the frequency of file access increased, the results were evenly split. This indicated that even in scenarios where the demand for convenience increased, half the users still supported the benefits of the proposed method (two-observed authorization). Making users aware of the proposed method's merit that "safety is ensured just by a single click" will contribute to enhancing the social acceptability of the proposed method .

References

[1] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y.: Multi-Factor Authentication: A Survey, Cryptography, vol. 2, no. 1, 2018.

[2] "How it works: Microsoft Entra multifactor authentication", https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks, (accessed 2023-11-28).

[3] "Adding MFA to a user pool". https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html (accessed 2023-11-28).

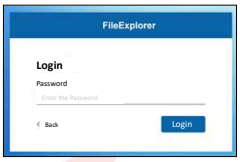
[4] Karapanos, N., Marforio, C., Soriente, C., Capkun, S.: Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound, In 24th USENIX security symposium, USENIX security 15, 2015, p. 483-498.

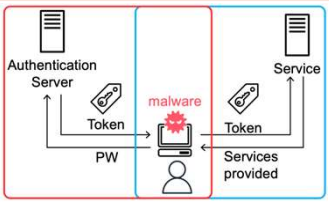
[5] "Kerberos Authentication Overview". https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview,

Multi-Observed Authentication: A secure and usable authentication/authorization based on multi-point observation of physical events

◯Shinnosuke Nozaki † Takumi Takaiwa † Masahiro Fujita ‡ Ayako Yoshimura ‡ Tetsushi Ohki † Masakatsu Nishigaki †
† Shizuoka Univercity ‡ Misitsubishi Electric Corporation nisigaki@inf.shizuoka.ac.jp

Two-factor authentication/authorization issues





Authentication

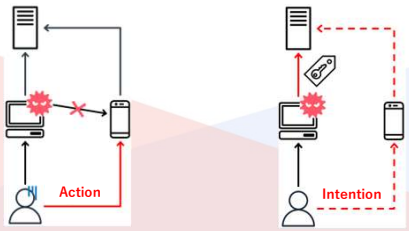
- Advantage
  - Applying two-factor authentication makes authentication difficult for malware lurking inside a PC
- Disadvantage
  - When authentication is frequent, use of smartphones is causing 2-factor authentication to become less convenient

Req: Does not make you aware of smartphone

- Automatic authentication with a smartphone
  - Automatic authentication makes users less aware of their smartphones.
- However...
  - Authentication can be breached if malware sends PW in background while user is at work

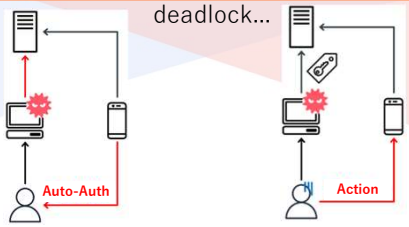
Req: Requires confirmation of intent

Authentication and Authorization



【Req.1】Does not make you aware of smartphone
【Req.2】 Requires confirmation of intent

deadlock...



Authorization

- Advantage
  - Authentication tokens can have an expiration date, eliminating the need for re-authentication
- Disadvantage
  - Single-factor (PC-only) authentication allows malware to exploit authentication tokens

Req: Requires confirmation of intent

- Confirmation of intent via smartphone
  - The intention can be confirmed by the second factor presented to the smartphone
- However...
  - Every time you get authorization, you have to be aware of your smartphone

Req: Does not make you aware of smartphone

Concept：Multi-Observed Authentication

Definition

"Simultaneous observation at multiple points" of **"physical actions"** that occur during user authentication/authorization.

contribution

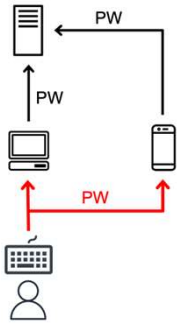
① **Simultaneous observation at multiple points**
→ Simultaneous observation of operations to the PC on the smartphone.
→ Conscious manipulation of the smartphone is eliminated.【Req.1】

② **physical actions**
→ Humans can do it, malware can't. (Like a CAPTCHA)
→ Equivalent to confirming the user's own will.【Req.2】

Multi-Observed Authentication/Multi-Observed Authorization

Multi-Observed Authentication

– Only when entering PW to PC, smartphone also receives keyboard input to PC.
– If both the PWs received by the PC and the smartphone are correct, authentication succeeds (token issued).

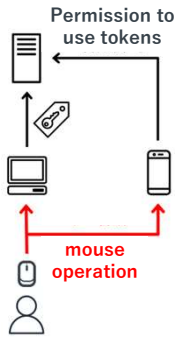


✓Fulfillment of Req.1
- User only needs to enter PW into PC
- Smartphone automatically receives PW

✓Fulfillment of Req.2
- PW input by physical manipulation of keyboard
- Operations not feasible for malware in the PC
- Receipt of a PW on the authentication server is considered to be confirmation of "the user's intention to use the service"

Multi-Observed Authorization

– Only when using authentication tokens, smartphone also receives mouse operation to the PC.
– If both the mouse operations received by the PC and the smartphone are the same, authorization succeeds (token can be used).



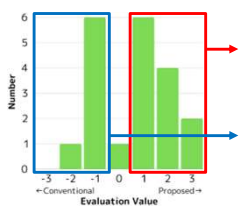
✓Fulfillment of Req.1
- User only needs to operate the mouse on the PC
- Smartphones automatically receive mouse operations

✓Fulfillment of Req.2
- Click input by physical manipulation of the mouse
- Operations not feasible for malware in the PC
- Receipt of a mouse click on the file server is considered to be confirmation of "the user's intention to use the service"

Evaluation

Authentication

- Question
  - "Which method do you want to use from the perspectives of convenience and privacy?"
- Evaluation



☑ No operation on a smartphone was needed.

✘ Distrust for sending credentials to a terminal other than a PC.
→ Transparency is required.

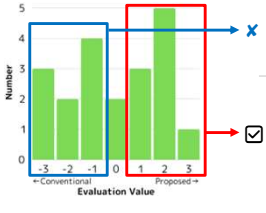
- Implemented the following four methods.
  - Conventional two-factor authentication
  - Double-Observed Authentication
  - Conventional authorization*
  - Double-Observed Authorization*,**

  * : No dialog displayed
  ** : Verify mouse clicks on a confirmation dialog
- Experimental participants
  - Twenty university students
- Evaluation method
  - 7-point Likert scale*** + reasons

  *** : "-3" is support for the conventional method, "0" is neither, and "3" is support for the proposed method

Authorization

- Question
  - "Which method do you want to use from the perspectives of convenience and safety if the frequency of file access increased?"
- Evaluation



✘ Even though it needed only a single click, the conventional method was still more convenient.

☑ Even in scenarios where the demand for convenience increased, half the users still supported the proposed method.
→ Awareness of security is key.