# Multi-Observed Authentication: A secure and usable authentication based on multi-point observation of a single physical credential

Wataru Hatakeyama[1], Shinnosuke Nozaki[2], Ayumi Serizawa[1], Mizuho Yoshihira[1],
Masahiro Fujita[2], Ayako Yoshimura[2], Tetsushi Ohki[1], Masakatsu Nishigaki[1]
1 Shizuoka University, 3-5-1 Johoku, Chuo, Hamamatsu, Shizuoka, 432-8011, Japan.
2 Mitsubishi Electric Corporation, 5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501, Japan.
E-mail: nisigaki@inf.shizuoka.ac.jp

***Abstract*— Nowadays, it is no longer uncommon for a PC to be infected with malware. User authentication based on only one legitimate credential (such as a password) may be insufficient for judging whether a user is legitimate. A typical solution to this problem is two-factor authentication, which is a method of authentication based on the presentation of two factors by the user. Generally, the first factor is input into a PC and the second into a smartphone. However, this reduces usability by forcing the user to present multiple factors at each authentication. Therefore, we propose multi-observed authentication as a new method based on the concept of "confirmation of the user's intention at the time of authentication, in addition to the validity of the credentials (passwords or authentication tokens)." The proposed method captures the user's physical authentication actions as physical events and simultaneously observes each event at multiple points, ensuring that the credential is not sent by malware residing in the PC but is physically input by a real human.**

## I. INTRODUCTION

In recent years, business systems have been changing to better meet the digital transformation strategy. Correspondingly, the use of malware for stealing user-specific information (hereinafter referred to as credentials) has continued to grow against users (individual and businesses) who are not fully prepared for such changes [1]. In the digital transformation environment, employees log into cloud business systems from their PCs to work. When malware resides on a PC, it is difficult for an authentication server to judge whether the credentials received from the PC are from a legitimate user or the malware. Therefore, inputting only one piece of legitimate user-specific information, such as a password, is often insufficient for judging whether the user is legitimate.

A typical solution to this problem is two-factor authentication. Currently, two-factor authentication is used to prove that a user is legitimate by presenting credentials for two of the following three elements [2].

1. Knowledge factor: based on something the user knows, such as passwords.
2. Possession factor: based on something the user has, such as ID cards, smartphones, etc.
3. Biometric factor: based on something the user is, such as through face recognition, fingerprint recognition, etc.

In general, the user is authenticated by first inputting the credential into the PC and then into a smartphone. In other words, two-factor authentication is a method of strengthening security by multiplexing authentication [3], [4]. However, it reduces usability by forcing the user to present multiple credentials at each authentication. If only improvement in usability is considered, the automatic confirmation of the smartphone's proximity to the PC could be an option for the second factor (possession). However, with this method, if malware fraudulently presents the first credential while a legitimate user is working on a PC, the second factor will also be passed automatically. In terms of security, this is synonymous with single-factor authentication.

Rephrasing it in another way, if the purpose of requiring two-factor authentication is to increase the security of the PC against a malware infection, another credential is not always necessary. Instead, it should be sufficient to verify that a human (not malware) has inputted the legitimate credential. With this method, the user only needs to input a single credential into the PC as before, while maintaining usability and improving security.

Therefore, in this study, a new user authentication method called multi-observed authentication, is proposed based on the concept of confirming that a human (not malware) has inputted the legitimate credential. The proposed method achieves this by simultaneously observing "the input of a single legitimate credential by the user" on both the PC and smartphone. Judging from the fact that both the PC and smartphone have received the legitimate credential from a single input device at the same time, it is deduced that the credential is not sent by malware residing in the PC but physically inputted by a real human. As a result, both PC and smartphone can play a role in authentication factors to verify the user's legitimacy. Thus, the

proposed method achieves authentication equivalent to two-factor authentication with both usability and security.

Depending on the legitimate user model and/or threat model, the information that should be confirmed by the smartphone may be changed to "a human (not malware) has inputted what appears to be a credential" or "a legitimate user has inputted the legitimate credential." This study, in Section V, also proposes a variation of the method for these cases. For the sake of simplicity, the focus is on two-factor authentication, but the proposed method can be extended to multi-factor authentication with a single credential observed at three or more points.

Section II reviews existing two-factor authentication approaches and presents the corresponding requirements. Section III describes the concept and concrete implementation of multi-observed authentication and presents the usability and security evaluation of the proposed method. User experiment is shown in Section IV. In Section V, a variation and risks of the proposed method are discussed. Section VI concludes the paper.

## II. Two-Factor Authentication

With the spread of COVID-19, working from home has become widespread. Employees work on their PC from home and access the information on the assets of the company's ICT resources, as needed. Each time the employees access an asset, they are required to authenticate. In line with this, malware that infects the employee's PC and steals user authentication credentials is rapidly increasing [1]. This is why user authentication methods must be hardened and two-factor authentication being more widely used across many companies at present. Hereafter, the employee is referred to as the user.

### *A. Single-Factor and Two-Factor Authentication*

In single-factor authentication, the server judges the legitimacy of the user by the presentation of a factor (knowledge/possession/biometric) that can only belong to the legitimate user. The use of possession or biometric factors is recommended from the viewpoint of impersonation. However, single-factor authentication using a knowledge factor has been more common until now due to ease of implementation (input via standard input devices of ICT equipment) and privacy concerns (biometric information being leaked).

When users working with a PC access a company resource using a knowledge factor, e.g., a password (PW), the flow of the single-factor authentication is as follows;

1. The user inputs the PW into the PC.
2. The PC sends the PW to the authentication server.
3. The server authenticates whether the user is legitimate or not based on the PW received from the PC.

In Fig. 1, the PWs in Steps 1 and 2 are written as PW and $PW_{PC}$, respectively, to distinguish them, but actually PW and $PW_{PC}$ are identical.

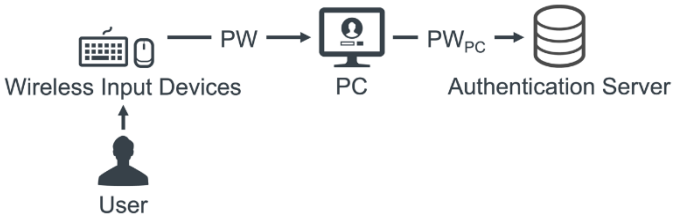


**Fig. 1.** Single-factor Authentication

If a legitimate user's PC is infected by malware, the premise that the credential is possessed by only a legitimate user is broken. Therefore, the server cannot judge if the user is legitimate simply from the input of the PW. A typical solution to this problem is two-factor authentication, which uses two credentials.

A user's PC can be infected with malware and manipulated either autonomously or by the remote control of a rogue actor. Therefore, it is not a good approach to register each user's PC as the second credential to confirm the possession of a legitimate PC. Moreover, the malware can steal a credential inputted into the infected PC. Therefore, it is also not a good idea to send the second credential to the authentication server via the PC[1]. For these reasons, two-factor authentication, in which the smartphone is used as a means to submit the second authentication factor, has become common. By securing a different authentication route from the PC, even if the PC is infected with malware and the first credential (PW) is stolen, impersonation can be prevented as long as an attacker does not break though the authentication of the smartphone.

In the following sections, a two-factor authentication system consisting of a PC and smartphone (Fig. 2) is described, as a concrete example. As shown in Fig. 2, the first credential is a PW and the second is a PIN, but credentials other than knowledge factors may be used. In the actual authentication procedure, the authentication server instructs the smartphone to request the user to input the PIN only when the PW from the PC arrives at the authentication server; however, this is omitted in Fig. 2. In Fig. 2, to distinguish between the credentials inputted by the user and those forwarded to the authentication server, PW, $PW_{PC}$, PIN, and $PIN_{SP}$, are specified, respectively, but actually $PW = PW_{PC}$ and $PIN = PIN_{SP}$.

[1] The exception is when a One-time password (OTP) is used as the second credential. For example, in [4], the user inputs the OTP sent to the smartphone from the authentication server to the authentication server via the PC, which constitutes two-factor authentication.

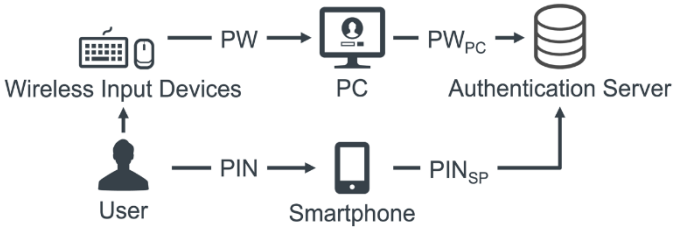


**Fig. 2.** Two-factor Authentication

*B. Issue of Two-Factor Authentication*

Figure 2 simply shows only two credentials (PW and PIN). However, in practice, the actual operation of the user is to input the PW after logging in to the PC, and to input the PIN after activating the smartphone. To note this precisely, Fig. 2 is reconfigured as shown in Fig. 3. Notations are provided below.

- $AC_{PC}$: The activation credential that the user inputs to the PC when using the PC.
- PW: The first credential that the user inputs into the PC when accessing the information asset. The PC sends the first credential to the authentication server.
- $AC_{SP}$: The activation credential that the user inputs into the smartphone when using the smartphone.
- PIN: The second credential that the user inputs into the smartphone when accessing the information asset. The smartphone sends the second credential to the authentication server.

In Fig. 3, just like in Fig. 2, PW = $PW_{PC}$ and PIN = $PIN_{SP}$.

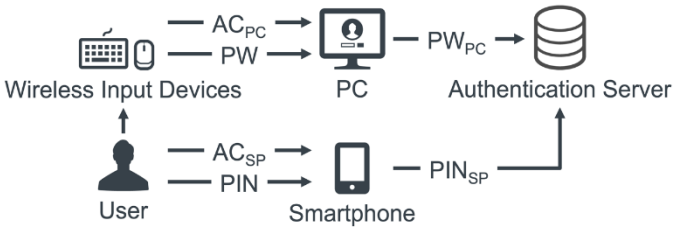


**Fig. 3.** Details of Two-factor Authentication

While the users (employee at their job) are working on their computer, the user is in front of the PC and the user's PC is always activated. In other words, there is no need to input the $AC_{PC}$ to the PC again when the user accesses company's internal data. Thus, the PW ($PW_{PC}$) is an important security factor on the PC side. In general, it is not unusual at all, even for the legitimate user, to be prompted for the password before accessing confidential data. Therefore, inputting the PW into the PC is not a significant burden to the user. In contrast, as the user is unlikely to utilize the smartphone while working on the PC, the smartphone is not activated. Thus, the $AC_{SP}$ must be input into the smartphone each time the user accesses company's resources. In practice, it is possible to keep the PIN in the smartphone and have the smartphone automatically send the PIN ($PIN_{SP}$) to the authentication server only when the $AC_{SP}$ input from the user has been confirmed. Thus, the $AC_{SP}$ is an important security factor on the smartphone side.

As a result, the tedious part of the procedure in Fig. 3 is inputting the $AC_{SP}$. Each time the user must be authenticated, the user must be aware of the smartphone, which has nothing to do with the user's work. With the widespread practice of working from home, company's internal data are being accessed from outside more frequently. Current two-factor authentication requires activation of the smartphone for each authentication. This significantly increases user effort and reduces work efficiency. Therefore, in terms of usability, there is a need for two-factor authentication that can avoid making the legitimate user aware of the smartphone (referred to as "Requirement 1").

*C. Existing Research on Improving the Usability of Two-Factor Authentication*

Bardram et al. proposed the idea of context-aware authentication in which the authentication method dynamically changes according to the user's situation [5]. This method confirms whether a client to be authenticated is in close proximity to a smart card held by a user. If the client and the smart card are in close proximity, user authentication is performed automatically. If proximity cannot be confirmed, the user is asked to input a password. By using context-aware authentication, the second factor can be employed automatically. When the PW ($PW_{PC}$) arrives at the authentication server, the server sends the second factor request to the smartphone. If the smartphone confirms its proximity to the PC, the PIN ($PIN_{SP}$) is sent automatically from the smartphone to the authentication server.

Fathy et al. investigated the usefulness of fully automatic face recognition system using videos recorded by the front camera of a smartphone [6]. Fully automatic face recognition can be used to automate receipt of the second factor for authentication. When the PW ($PW_{PC}$) arrives at the authentication server, the server sends the second factor request to the smartphone. If the smartphone is able to confirm the user's presence by means of a fully automatic facial recognition system, the PIN ($PIN_{SP}$) is sent from the smartphone to the authentication server.

As in these existing studies, if the smartphone automatically authenticates the user, meaning it remains active, it is possible to mitigate the usability degradation in two-factor authentication. However, in situations where the user's PC is infected by malware, such automated measures are insufficient.

If malware sends the PW ($PW_{PC}$) to the authentication server in the background while the user (twiddling with their smartphone) is working on the PC, the smartphone will confirm the legitimate user and automatically send the PIN ($PIN_{SP}$) to the server. In other words, malware can easily break through the two-factor authentication while the user is working on their PC. Even when the second factor authentication is automated, it is still necessary to confirm the intention of the user to authenticate. Therefore, in terms of security, there is a need for two-factor authentication to confirm the intention of a legitimate user to authenticate (referred to as "Requirement 2").

## III. Multi-Observed Authentication

### A. Concept

The requirements explained in the previous section for two-factor authentication are summarized below.

(Requirement 1) The legitimate user is not made aware of the smartphone.

(Requirement 2) The intention of the legitimate user to authenticate can be confirmed.

The key point of two-factor authentication is to establish a different authentication route from that of the PC. Therefore, we propose a new user authentication method called multi-observed authentication in which a single legitimate credential physically entered by the user into the PC is observed simultaneously on the smartphone. While the user inputs a credential into the PC, the legitimacy is authenticated via two routes (the PC and smartphone). Thus, Requirement 1 is satisfied. Judging from the fact that both the PC and smartphone have received the legitimate credential from a single input device at the same time, it is expected that the credential is not sent by malware residing in the PC but physically inputted by a real human. Thus, Requirement 2 is also satisfied. As a result, the proposed method achieves authentication equivalent to two-factor authentication with both usability and security.

### B. Authentication Procedure

This section describes the specific authentication procedure of the proposed method (Fig. 4). A variation of the authentication procedure are also described in Section V. The authentication procedure discussed in this section is referred to as Method A, and the variation in Section V.A as Methods B, respectively.

The basic flow of the proposed Method A is outlined below (Fig. 4). The credential used in the example is a password. To realize Method A, it is assumed that keyboard and mouse inputs to the PC are simultaneously input to the smartphone. Specifically, it is assumed that the wireless keyboard and wireless mouse (referred to as wireless input devices in this paper) are connected to the PC, and that the keyboard and mouse operations are modified so that they can also be received by the smartphone.

1. The user is working with the PC (i.e., the PC is already in activated state).
2. The user requests the authentication server to access information assets via the PC.
3. The authentication server instructs the smartphone to start listening to input from wireless input devices to the PC.
4. The smartphone starts receiving signals from the wireless input devices.
5. The authentication server instructs the PC to display a login page.
6. The PC displays the login page.
7. The user inputs the PW into the PC by using the wireless input devices.
8. The PC sends the PW to the authentication server.
9. The PW inputted by the user in Step 7 is simultaneously received by the smartphone. The smartphone also sends the PW to the authentication server.
10. The authentication server confirms the legitimacy of the PW received from the PC.
11. The authentication server confirms the legitimacy of the PW received from the smartphone.
12. If both Steps 10 and 11 are verified, the user is determined to be legitimate.
13. The authentication server instructs the smartphone to stop listening to input from wireless input devices to the PC.
14. The smartphone finishes receiving signals from the wireless input devices.

In Fig. 4, the PWs in Steps 7, 8, and 9 are shown as PW, $PW_{PC}$, and $PW_{SP}$, respectively, to distinguish them. However, in fact, PW, $PW_{PC}$, and $PW_{SP}$ are identical. $AC_{PC}$ is a credential for PC activation. By the time the user starts to work on the PC (prior to Step 1), the user has inputted $AC_{PC}$ and logged into the PC. As explained in Section III.C, $AC_{SP}$ (for smartphone activation) is not required in Method A.

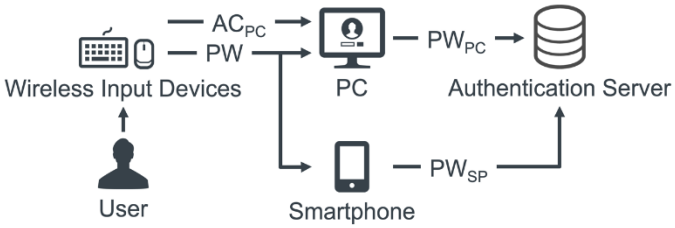


**Fig. 4.** Two-observed Two-factor Authentication

### C. Evaluation

Here, Method A is evaluated in terms of usability (Requirement 1) and security (Requirement 2).

In Method A, all that is required of the user is to input the PW into the PC (in step 7). Thus, Method A satisfies

Requirement 1. The user can use Method A in the same way as one-factor authentication (password authentication). As password authentication is familiar to the user, there are no mental barriers to the introduction of Method A. In contrast, the fact that the input to the PC is also sent to the smartphone may be a concern in terms of privacy. However, Method A is expected to limit the user's psychological burden, as the smartphone listens to the user's key input to the PC only during the period of credential input (from Step 4 to Step 14).

Notably, malware lurking in the PC can illegally send PW in Step 8. However, malware cannot physically manipulate the wireless input devices, so Step 7 cannot be performed. Therefore, the PW received by the smartphone in Step 9 can be determined as the PW inputted by the user in Step 7. In other words, the receipt of the PW from the smartphone in Step 9 is the basis for the assumption that the user intended to input the credential. Therefore, Method A also satisfies Requirement 2.

In existing two-factor authentication (Fig. 3), $AC_{SP}$, the credential for activating the smartphone, is required to confirm the user's intention for authentication using the smartphone. In contrast, Method A does not need to request $AC_{SP}$ from the user, because the intention to authenticate is confirmed in Step 9. In other words, Method A can omit the confirmation of $AC_{SP}$ for activating the smartphone (for this reason, the $AC_{SP}$ is not shown in Fig. 4). This fulfills Requirement 2 (the legitimate user is not made aware of the smartphone) while satisfying Requirement 1 (the intention of the legitimate user to authenticate can be confirmed).

### *D. Authorization Procedure*

To enhance convenience in multi-factor authentication, practices that separate authentication and authorization are widely adopted [7]. Authentication tokens are issued to users who have successfully completed multi-factor authentication upon initial access to information assets. These tokens have an expiry date, and within this period, presenting the authentication token (authorization) is sufficient for repeated access by the same user. However, this approach effectively reduces the authorization phase to single-factor authentication (only confirming possession of the authentication token). Consequently, malware on the PC can easily misuse the authentication token by simply waiting until the legitimate user obtains it.

This means that it is crucial to confirm the user's intention at the time of not only authentication but also authorization. This suggests that the concept and procedures of the proposed multi-observed authentication can be directly applied into authorization to enhance both usability and security of authorization. The flow of multi-observed authorization is similar to that of Method A, but due to space constraints, the details are omitted.

## IV. User Experiment

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/informatics) perform comparative experiments. After each participant had experienced the system, we conducted subjective assessments. We employed a questionnaire method for the assessment, 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 assessments.

### *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 assessments would change if the frequency of authentication increased, the result was a shift in the assessment toward the proposed method. From this, it was confirmed that in scenarios where the demand for convenience increases, the assessment 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 assessments 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.

## V. Discussion

### A. Modified Method with Keystroke Recognition (Method B)

Consider the case where a malicious user in collusion with the malware can physically access the legitimate user's PC. In that case, the malicious user can directly input the PW stolen by the malware into the PC while the legitimate user is away from the PC. In such an environment, it is not sufficient to simply confirm that a legitimate credential (PW) was inputted into the PC. It becomes necessary to confirm that the PW, which is a legitimate credential, was inputted by a legitimate user (not by malware nor a malicious user). In such a case, in addition to confirming the legitimacy of the PW, another credential is needed to verify that the user who inputted the PW is legitimate.

To address the problem of requiring another credential, we propose a modification to Method A (Section III.B) by adding keystroke dynamics. Specifically, keystroke recognition is added to Step 11 of Method A using the characteristics of the keystroke operations when inputting the PW. This allows the authentication server to simultaneously achieve confirmation of the legitimacy of the PW (whether the input PW is legitimate) and legitimacy of the user (whether the user who input the PW is legitimate) in Step 11 while the legitimate user is still requested to simply input a single credential into the PC in Step 7. This enhances the password inspection in Step 11 of Method A. In this study, this was referred to as Method B.

### B. Authentication

The proposed methods (Methods A and B) are authentication methods that assume the use of wireless input devices connected to both the PC and smartphone. As Bluetooth pairing is based on a one-to-one connection, a remodeling of the wireless communication protocol is required to implement the proposed method. Therefore, from the viewpoint of feasibility, the barriers to introducing the proposed method cannot be ignored.

In addition, vulnerabilities in wireless communication protocols pose a risk to the proposed method. Bad USB is a typical example of such a vulnerability, whereby the device drivers to be exploited are tampered with by malware without permission [8]. Under normal conditions, wireless input device communication is unidirectional (wireless input devices to PC). However, if malware replaces these with bidirectional device drivers, it is possible for malware residing in the PC to manipulate the wireless input devices. The solution will be discussed in a future study.

## VI. Conclusions

In this paper, we proposed multi-observed authentication was proposed as a solution to the problem of reduced usability caused by the introduction of two-factor authentication. This was based on the concept of verifying a legitimate credential inputted by a human. After presenting the specific procedures of the proposed method (Method A), we evaluated Method A in terms of usability and security. Also, we implemented the proposed method (two-observed authentication/authorization) and carried out user experiments with 20 participants. With regards to future research directions, we plan to investigate ways to ensure transparency in the multi-observed authentication method and ways to increase users' awareness of the advantages of the multi-observed authorization method.

## VII. Acknowledgment

This study was supported in part by JST Moonshot-type R&D project JPMJMS2215 and JSPS KAKENHI Grant Number JP23K28084.

## References

[1] Kaspersky Emotet modules and recent attacks, SECURELIST, Kaspersky (online), https://securelist.com/emotet-modules-and-recent-attacks/106290/ (accessed 2022-4-21).

[2] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y. "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, 2018. https://doi.org/10.3390/cryptography2010001.

[3] Microsoft: How it works: Azure AD Multi-Factor Authentication, Microsoft (online), https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks (accessed 2021-12-23).

[4] Amazon: Adding MFA to a user pool, Amazon (online), https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html (accessed 2021-12-23).

[5] Bardram, J. E., Kjær, R.E., Pedersen, M. Ø.: Context-aware user authentication- supporting proximity-based login in pervasive computing. International Conference on Ubiquitous Computing. Springer, Berlin, Heidelberg, 2003.

[6] Fathy, M. E., Patel, V. M., Chellappa, R.: Face-based Active Authentication on mobile devices. 2015 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2015, pp. 1687–1691, doi: 10.1109/ICASSP.2015.7178258.

[7] "Kerberos Authentication Overview". https://learn.microsoft.com/enus/windowsserver/security/kerberos/kerberos-authentication-overview, (accessed 2023-11-28)

[8] Choi, B., Suh, T.: A Security Program to Protect against Keyboard-Emulating BadUSB. Journal of the Korea Institute of Information Security & Cryptology, vol. 26, no. 6, pp. 1483–1492, Dec. 2016.