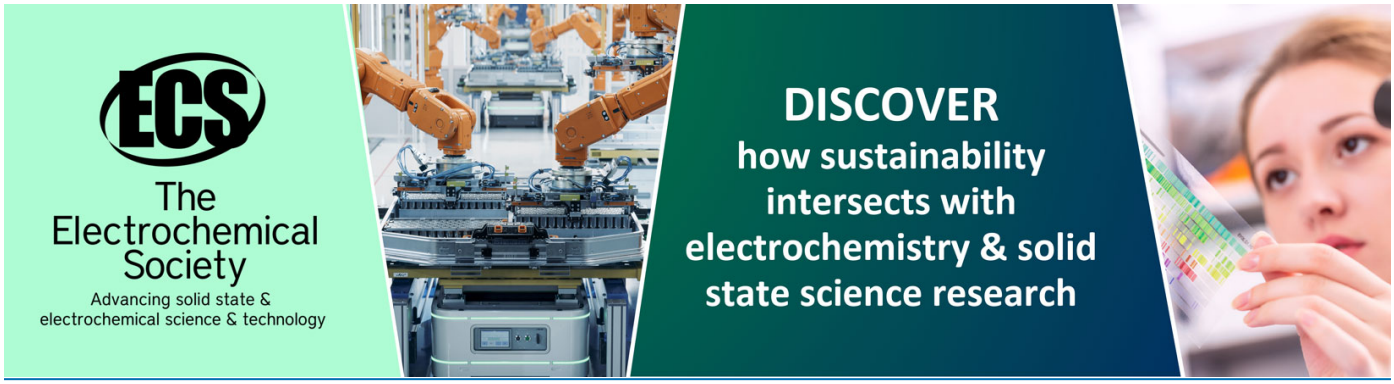
Implementation of incognito method and SHA-3 as an alternative to PIN selection in web login



IOP Conf. Series: Materials Science and Engineering **852** (2020) 012176 doi:10.1088/1757-899X/852/1/012176

Implementation of incognito method and SHA-3 as an alternative to PIN selection in web login

Gesi Deta Hendika Wardani and Yogha Restu Pramadi*
Laboratory of Cryptographic Software Engineering
Sekolah Tinggi Sandi Negara
gesi.deta@stsn-nci.ac.id
yogha.restu@bssn.go.id
* corresponding author

Abstract. Currently, the PIN is still used to verify identity on web-based applications. PIN is widely used because it is easy authentication. However, a PIN has a potential security risk that is vulnerable to shoulder surfing attacks. The way to reduce shoulder surfing attacks is to create an interface that is difficult to attack with shoulder surfing attack techniques. One interface that can be applied is the incognito method. In this research, the application of the incognito method is implemented as a web login application. The application is built based on the web using the SHA3-256 algorithm to hash the PIN. The results of the stufy prove that the application built is resistant to shoulder surfing attack by attackers.

1. Introduction

Personal Identification Number (PIN) is a password in the form of numbers. PIN is used to authenticate someone into a system [1]. PINs are used in virtual and physical environments, such as PassFaces and Gate Access [2]. The PIN is private so it has the potential to pose a security risk, therefore the PIN must be kept secure.

The most common weakness in using a PIN is the user's limitations in remembering the PIN. This limitation results in the user writing down the PIN or using the same PIN for multiple systems [3]. However, the use of PIN as authentication is still chosen because it is the easiest way to authenticate. The main drawback of using a PIN is that it is vulnerable to shoulder surfing attacks [4] because the PIN interface design makes it easy to see user input [2].

Shoulder surfing attack is a type of attack that uses direct observation techniques such as looking behind someone's back to obtain information [4]. This attack is relatively easy and effective to do, especially in crowded places. Attackers can pretend to stand behind someone and see the password or PIN entered, for example entering a PIN on an ATM. Shoulder surfing attacks are sometimes combined with social engineering to trick victims into typing their PIN in front of the attacker [5]. Current shoulder surfing attacks are developed using technology to increase the effectiveness of the attack. Technologies used include optical devices such as cameras, heat-detecting devices, and wearable devices. Although, the user has closed direct access to the entered PIN, this only limits the optical device, not the traces of heat generated from the PIN entry process.

Research on methods to deal with shoulder surfing attacks is growing. One method to improve security is to use images. It aims to create a safer authentication system. ColorPIN is a method for entering a PIN using color as its input [6]. PassFaces is a graphical password that uses faces instead of PINs. However, the authentication method using images and PIN is still vulnerable to shoulder surfing attacks. To overcome this vulnerability it is needed to create an interface that is difficult to attack. One of this Interface method that can be applied is the incognito.

The incognito method is an interface developed to reduce shoulder surfing attacks on 10-digit keyboards [2]. This method is done by hiding the mouse cursor when passing through the keypad and turning it into a border when selecting keys. Each button can change between active and inactive states. It aims to disguise the number chosen by the user.
This study implements the incognito method as an alternative interface to select a PIN on a web login. To further enhance the security, SHA-3 is selected for hashing the PIN. SHA-3 was chosen because SHA-3 is the latest standard hash function algorithm published by NIST [7]. SHA-3 uses a spongy structure that makes this hash function algorithm different from previous hash function algorithms. This hash function algorithm is resistant to preimage, second preimage, and collision attacks.

2. Method and materials

2.1. Authentication

Authentication is the process of validating a user's identity [8]. The validation process usually uses a username and password. Validated users are granted the right to access a system. The methods for identifying and authenticating users are categorized into three forms including [9]:

1. Something the user possesses is something that user has like a one-time password generator, certificate, or smartcard.
2. Something the user knows is something that the user knows of like a password or an answer to a security question.
3. Something that the user is something that is attached to the user such as fingerprint or iris scan.

The use of usernames and passwords can usually be classified as easily forgotten. There are alternative methods of authentication such as biometrics, graphical passwords, and authentication using public keys. This method has vulnerabilities and cannot replace the use of usernames and passwords even though some function as secondary authentication methods. The following is a classification of secondary authentication methods, including: Token-based authentication; Biometric authentication; and, Knowledge-based authentication.
PIN is an example of a verification process using knowledge authentication, an authentication based on something the user knows [9]. The threat to knowledge authentication is that they are vulnerable to guessing attacks and capturing attacks.

2.2. Incognito method

The incognito method is one of the methods used in selecting a PIN. The incognito method aims to reduce the shoulder surfing attack on the 10 digits keypad [2]. This method combines the use of indirect input and cursor changes. This method requires additional devices, such as a mouse or touchpad to reduce direct interaction with the PIN interface. Each button changes between active and inactive conditions. Active condition is a condition where the border on the button is lit or visible. Inactive condition is a condition where the border on the button is not visible. This condition aims to deceive the attacker in determining the number chosen. This condition changes at certain time intervals which can be seen in Table 1. The following table shows the time interval for active and inactive conditions for each numeric keypad on the keypad. The process of the incognito method can be seen in Figure 1.

Table 1. Time of active and inactive state of each button [2]

Keypad	Active condition (ms)	Inactive condition (ms)
1	1770	6000
2	1300	2500
3	1400	2100
4	970	2200
5	800	2000
6	1800	650
7	1200	2200
8	600	1200
9	500	700
0	900	2400

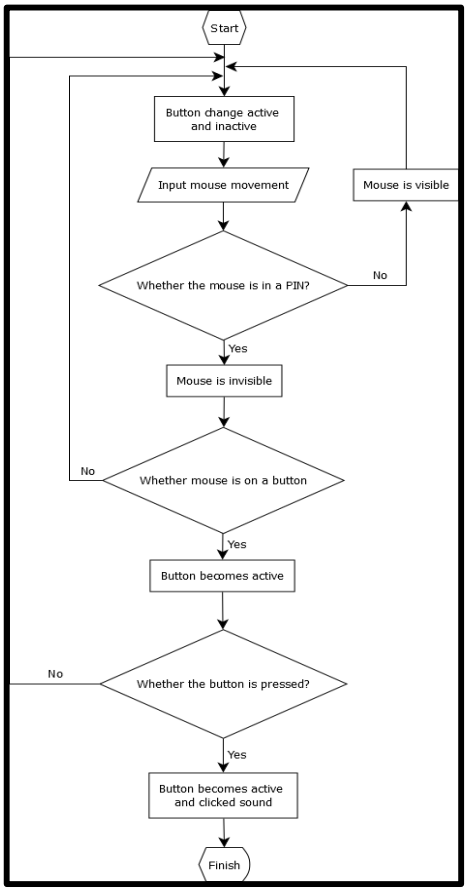


Figure 1. Process of incognito method

This method was originaly implemented using Java for desktop application, in this study we implemented this method for use in a web environment.

2.3. Shoulder surfing attack

Shoulder surfing attack is an attack where the attacker observes the login process by looking over the user's shoulder and trying to get the password used by that user [10]. Shoulder surfing attacks, including attacks that are difficult to overcome [11]. Shoulder surfing attacks can be carried out using binoculars and a camera, acoustic keyboard, or electromagnetic emission from the display. Shoulder surfing attacks are common in real life [12]. Shoulder surfing attacks take the private information from the authentication process such as PINs, passwords, and patterns. This study validates the implemented method by conducting shoulder surfing attacks. Shoulder surfing attacks threat model are illustrated in Figure 2. The shoulder surfing attack process is done using a camera that records the user's process of logging in. Attackers guess the PIN used by the user.

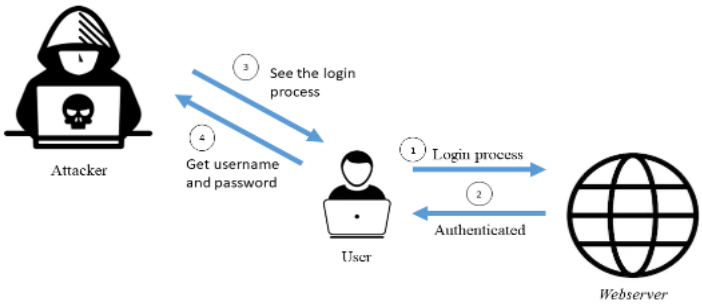


Figure 2. Shoulder surfing attack threat model

2.4. SHA-3

SHA-3 is a hash function algorithm that aims to complete SHA-2 as an approved standard for various applications. SHA-3 is set as a standard published by the National Institute of Standards and Technology (NIST). SHA-3 is an algorithm that is different from the previous SHA algorithm because SHA-3 uses a sponge construction. This hash function algorithm is resistant to the collision, preimage, and second preimage. SHA-3 has several output sizes including SHA-3 224, SHA-3 256, SHA-3 348, and SHA-3 512.

This study will be using SHA-3 256 which has a security level of 128 bits. The selected PIN from the incognito application will be hashed using the SHA-3 256 algorithm and then stored in the database.

3. Designing the Incognito Web Login Interface

3.1. PIN Display

The PIN is used as a parameter to login. The PIN applies the incognito method. The PIN is built using Javascript and CSS. PIN is chosen using mouse or touchpad. The PIN display can be seen in Figure 3.

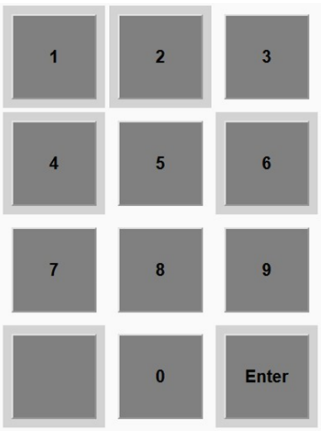


Figure 3. Display PIN

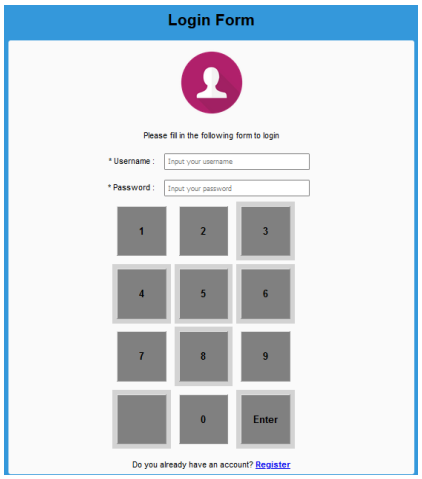


Figure 4. Display the login page

PIN consists of 10 digits. 3x4 PIN. Each PIN button is 100px X 100px. CSS is used to make the appearance of a PIN, among others, make a keypad, button, and border. Javascript is used to make the PIN conditions as expected.

3.2. Login

To log in, the user enters the username that has been registered and the PIN used. The user chooses by pressing the PIN used using a mouse or touchpad device. The PIN on the application is built using the incognito.

The user who has filled in the data pressing the enter system key processes the data. The first process is calculating the hash value of the PIN used. Then check the username used by the username stored. If the username is not available, the system displays a notification that the username has not been registered and the user is asked to repeat the login process. If the username is in the database the system will compare the PIN hash value stored with the hash value of the PIN used. If appropriate, the system will create a session for users so they can enter the application. If it does not match, the system will display an incorrect password notification and the user can repeat the login process. The login page display can be seen in Figure 4.

4. Implementation

In the scenario of an attack carried out, the attacker sees the user login process. The scenario of an attack carried out can be seen in the following image. This process aims to get the username and PIN used by the user. The username and password obtained are used to log into the application. The system checks whether the username and the hash value of the PIN entered is by the data stored in the database. If appropriate, the attacker can be authenticated with the application, as in the threat model seen in Figure 2.

In this validation process, the scenario carried out is to use a video that displays the PIN selection process using the incognito method. This video is scanned as a login process carried out by the user. The scenario involved 20 respondents who acted as attackers. Respondents view the video login process without limits. Then the respondent writes down or guesses the chosen PIN 3 times. The selected PIN has no special number relationship with the user.

Based on the attacks carried out there were 60 guesses produced. The results of the attacks carried out can be seen in the following table. From all of these guesses, there is only one correct PIN guess. The results of attacks can be seen in Table 2.

Table 2. Results of shoulder surfing attack

Succeed	Failed
1 guess	59 guess
1,66%	98,33%

The percentage of shoulder surf attack resilience from built applications is 98.33%. Based on this, the validation process that has been done, found that the incognito method that was built already meets the desired criteria and can be implemented as an alternative to selecting a PIN that is resistant to shoulder surfing attacks.

5. Conclusion

In this paper we implemented the incognito PIN selection method paired with SHA-3 in a login form using web technology. Technology such as CSS and Javascript made the specified method

posible to implement. And based on the results of the shoulder attack validation of the study that has been done it can be the concluded that the implemented incognito method in a web login application is resistant to shoulder surfing attacks. The incognito method to be implemented as an alternative to choosing a PIN on a web login that is resistant to shoulder surfing attacks still needs to be tested from a user expirience point of view which is open for further research.

6. References

[1] A. D. Luca, M. Denzel dan H. Hussmann, “Look into my Eyes! Can you guess my Password?,” dalam *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009.

[2] J. D. Still and J. Bell, "Incognito: Shoulder-surfing Resistant Selection Method," *Journal of Information Security and Applications,* pp. 1-8, 2018.

[3] R. Dhamija and A. Perrig, "Deja Vu-A User Study: Using Images for Authentication," in *USENIX Security Symposium*, 2000.

[4] S. A. Alsuhibany and S. G. Almutairi, "Making PIN and Password Entry Secure Against Shoulder Surfing Using Camouflage Characters," *International Journal of Computer Science and Information Security*, pp. 328-335, 2016.

[5] A. D. Luca, B. Frauendienst, S. Boring and H. Hussmann, "My Phone is my Keypad: Privacy-Enhanced PIN-Entry on Public Terminals," in *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group*, Melbourne, 2009.

[6] A. D. Luca, K. Hertzschuch and H. Hussmann, "ColorPIN-Securing PIN Entry through Indirect Input," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Georgia, 2010.

[7] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-otput functions," 2015. [Online].

[8] N. A. Lal, S. Prasad and M. Farik, "A Review of Authentication Methods," *International Journal of Scientific & Technology Research,* pp. 246-249, 2016.

[9] R. G. Rittenhouse and J. A. Chaudhry, "A Survey of Alternative Authentication Methods," in *International Conference on Recent Advances in Computer Systems*, 2015.

[10] M. K. Lee, "Security Notions and Advanced Method for Human Shoulder-surfing Resistant PIN-entry," *IEEE Transactions on Information Forensics and Security,* pp. 695-708, 2014.

[11] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry," in *Proceedings of the 3rd symposium on Usable privacy and security* , 2007.

[12] M. Eiband, M. Khamis, E. v. Zezschwitz, H. Hussmann and F. Alt, "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.