

Earphones-free Alternative for Shoulder Surfing Safe Login Method

Zhi-Long Tee, Yvonne Hwei-Syn Kam⁺, Ji-Jian Chin

Multimedia University, Selangor, Malaysia

hskam@mmu.edu.my

Abstract. Audio-based authentication methods are commonly more shoulder surfing resistant than purely visual-based methods. However, the user usually must have earphones to use them and they are usually slower than purely visual-based methods. Shoulder Surfing Safe Login (SSSL) is a comparably fast audio-based method. However, the requirement of earphones may impede usability and acceptance. In this work, we propose a modification to SSSL that do not require earphones, by having user-generated challenges. The proposed method has two versions, named Beta and Gamma. Beta and Gamma are like SSSL, but the differences are that Beta version is using a keyboard key to set the challenge, while Gamma version is using knock code. Both versions and the control, which is the SSSL method were implemented and evaluated. At the end of the experiments, the results showed that the Beta version is faster. The login time of the Beta version was 3 seconds on average compared to 8 seconds in the SSSL. Next, the Beta version had a lower error rate than the SSSL, where the number of unsuccessful logins for Beta was 7.69% from a total of 78 attempts from the 12 participants. Moreover, all participants selected the Beta version as preferable, over the SSSL method and Gamma version. The proposed method's Beta version does not rely on earphones and is easy to use. From these results, we show that the proposed method could provide an alternative to audio challenges, which could have higher acceptance.

Keywords: shoulder surfing, observation attack, authentication, PIN, challenge-response

1. Introduction

Authentication is required to protect user information and keep data secured, thus a good authentication method is extremely important. PIN is a traditional authentication method that is used in different types of applications like touch and go, bank applications, Shopee, and so on. The problem with traditional authentication is that when the person inserts their PIN, there is a possibility that a person who stands beside them can observe, understand and remember the number inserted. After that, by using the number, the attacker can authenticate to the account of the victim. This attack is also known as the shoulder-surfing attack (SSA).

In 2021, the authors of (Binbeshr et al., 2021) made a study on shoulder-surfing resistant PIN-entry methods. In it, they mentioned that the methods that were highly resistant to shoulder surfing were in the category of challenge-response methods, which were audio-based or haptic-based. A majority of the highly resistant methods were audio-based methods, such as (Dan & Ku, 2017; Hirakawa et al., 2017; Jang & Park, 2018; Lee et al., 2016; Perković, Čagalj, & Rakić, 2010; Perković, Čagalj, & Saxena, 2010, 2010; Rajarajan et al., 2018). The shoulder surfing safe login (SSSL) method (Perković, Čagalj, & Rakić, 2010) is unique in that it is fast compared to the other methods, where its login time was reported to be 8 seconds.

All these audio-based methods depend on the secrecy of the audio channel to operate, which is de-facto realised by earphones. Aside from method (Dan & Ku, 2017), which utilises the mobile phone speaker at low volume, the other methods require the use of earphones. Thus, these methods are not compatible with the conventional standard PIN-entry method because aside from the visual channel, they require another channel to receive the challenge. This decreases usability as the user has to carry earphones with him/her (Dan & Ku, 2017).

In this paper, considering these drawbacks, we propose alternative techniques to provide challenges in the method SSSL that does not require earphones.

The rest of the paper is organised as the following. Section 2 provides a review of the related works. The details for the design of our proposed system will be in Section 3. We provide the usability and security analysis in Section 4. Finally, we conclude in Section 5.

2. Related Works

The problem statement is that users must bring along the earphone with them to authenticate in audio-based methods. In section 2.1, some relevant methods which are audio-based will be reviewed in terms of this requirement.

In this project, we present the enhanced version of the Shoulder surfing safe login (SSSL) method (Perković, Čagalj, & Rakić, 2010), where the objective of this project is to preserve security and at the same time, provide more convenience where the user does not need to bring along earphones with them. Our system provides different

ways of setup up the challenge number, which enables users to not rely on any external hardware. To achieve this, we have proposed a method to generate the challenges. We have based one of our challenge generating methods on the Knock code system (Jang & Park, 2018) which was originally devised by LG Electronics.

Thus, in section 2.2 we will be describing the existing method which is the Shoulder surfing safe login (SSSL) (Perković, Čagalj, & Rakić, 2010) method and in Section 2.3, the Knock code system (Jang & Park, 2018).

2.1. Audio-based methods

One of the major disadvantages of existing SSA resistant PIN-entry methods that use audio is that the user must have earphones with them. For example, the methods (Hirakawa et al., 2017; Jang & Park, 2018; Lee et al., 2016; Perković, Čagalj, & Rakić, 2010; Perković, Čagalj, & Saxena, 2010; Rajarajan et al., 2018) all require earphones and the screen to operate. This is because one part of the challenges are from audio and another part is displayed onscreen. Even with mobile phones, wherever the display needs to be visible, earphones need to be employed. An exception is method (Dan & Ku, 2017), which is able to use the phone audio receiver because the challenge is fully audio and no part of it is shown onscreen. However, it takes longer than SSSL at 16.7 seconds. It is only applicable to mobile devices and must be placed next to the ear. Thus, that method is not applicable on computers.

2.2. Shoulder surfing safe login (SSSL)

The shoulder surfing safe login method named SSSL (Perković, Čagalj, & Rakić, 2010) aims to be fast and secure, usable and efficient. The average login time with the SSSL is about 8 seconds in a 5-digit PIN scenario. The user is first issued an audio digit as a challenge. The users do not need to provide any PIN number as a response but rather enter a direction into the system. In terms of authenticating themselves, the user must answer the challenge given by referring to the Orientation of digits (Fig. 1) and arrows keypad (Fig. 2). The user must find the relationship between challenge value and their PIN digit in terms of direction.

The shoulder surfing safe login method named SSSL (Perković, Čagalj, & Rakić, 2010) aims to be fast and secure, usable and efficient. The average login time with the SSSL is about 8 seconds in a 5-digit PIN scenario. The user is first issued an audio digit as a challenge. The users do not need to provide any PIN number as a response but rather enter a direction into the system. In terms of authenticating themselves, the user must answer the challenge given by referring to the Orientation of digits (Fig. 1) and arrows keypad (Fig. 2). The user must find the relationship between challenge value and their PIN digit in terms of direction.

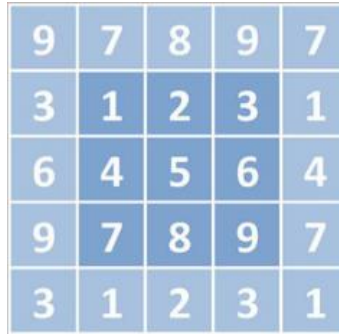


Fig. 1: Orientation of digits (Perković, Čagalj, & Rakić, 2010).

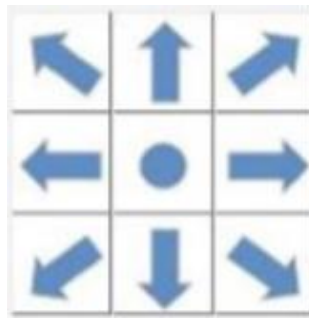







Fig. 2 Arrows Keypad(Perković, Čagalj, & Rakić, 2010).

Suppose the user PIN is 79732, and the corresponding random generated challenge value is 89214. The digit 8 is placed right of the value 7 as shown in Fig. 1. So, the user will press the right arrow button in Fig. 2. When the challenge digit is the same as the PIN digit, the user will press the middle O button to represent the same number. The correct responses are shown in Table 1.

Table 1: User response table of SSSL.

PIN	Challenge	Response
7	8	
9	9	
7	2	
3	1	
2	4	

2.3. Knock Code

Knock Code (Jang & Park, 2018) is the authentication method using touchscreen-based which it was developed by LG Electronics. It has a strong point in which user can unlock their device even the screen is off. The screen is off and divided into (2x2 grid) a total of 4 areas, which are top-left, top-right, bottom-left, and bottom right.

For authentication, the user touches each area in the correct order. Because the scheme can be run off-screen, the shoulder surfing attack is more complicated than the original Android screen lock such as draw pattern, or PIN lock. LG (*KEY LG SMARTPHONES TO GET KNOCK CODE™ UPGRADE / LG NEWSROOM*, n.d.) also points out that a knock code is convenient because the user is not necessarily looking at the screen when tapping. The weakness of this system is a fixed pattern for the password that can be guessed. It is also possible to be observed by the observer if the observer uses any recording instrument (Jang & Park, 2018).

The theory of Knock code is that, suppose the user password is grid sequence $2 \Rightarrow 1 \Rightarrow 3$. Fig. 3 shows the user tapping sequence will start from box 2 to box 1 and then lastly to box 3.

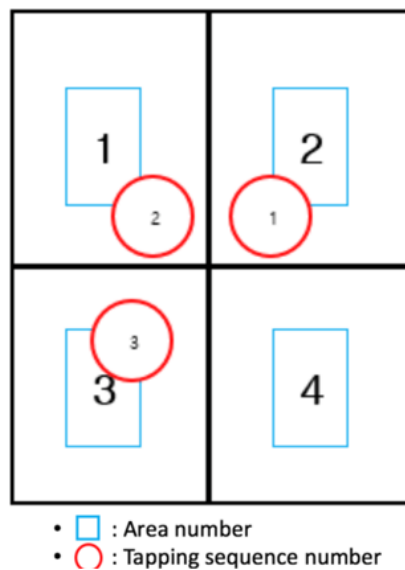


Fig. 3: Knock code (Jang & Park, 2018).

From the listed literature review, SSSL (Perković, Čagalj, & Rakić, 2010) is shoulder surfing resistant. In addition, SSSL (Perković, Čagalj, & Rakić, 2010) is faster and more straightforward compared to methods that need listening through a sequence of digits before reaching the PIN digit, such as (Dan & Ku, 2017) or wait for digit alignment to happen before entering a PIN digit, such as (Rajarajan et al., 2018). The SSSL system (Perković, Čagalj, & Rakić, 2010) is highly secure in terms of that it does not provide any response on screen, it can prevent shoulder surfing attacks, and has a short login time. The challenges are audio-based which necessitates earphones for secrecy. However, this may impede usability and acceptance. Thus, in this research, we develop an alternative way to generate the challenges, which is via the user themselves. Details of our proposed method are described in Section 3.

3. Proposed Method

The proposed method replaces audio challenges of the SSSL(Perković, Čagalj, & Rakić, 2010) with user-generated challenges. Two versions of the proposed method were developed, namely Beta and Gamma. We divide our implementation into three methods, SSSL, Beta, and Gamma methods. The SSSL implementation is similar to the original SSSL (Perković, Čagalj, & Rakić, 2010) system. The Beta and Gamma method are modifications to SSSL. SSSL, Beta, and Gamma methods are using 5-digit PINs for authorization, because the original SSSL system is using 5-digits PINs.

Using the mouse to click on the direction buttons over 5 rounds may not be as convenient or as fast as the keyboard. Thus, our scheme, similar to SSSL, aside from using mouse, also maps the keyboard buttons to the direction buttons. The keypad structure is the combination of 9 buttons, representing the 9 different directions. A red box in Fig. 4 shows the 9 keys which correspond to the 9 direction buttons.

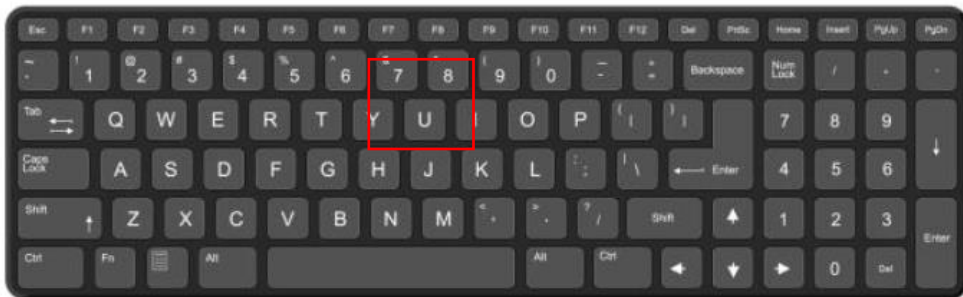


Fig. 4: The 9 keys which correspond to 9 directions.

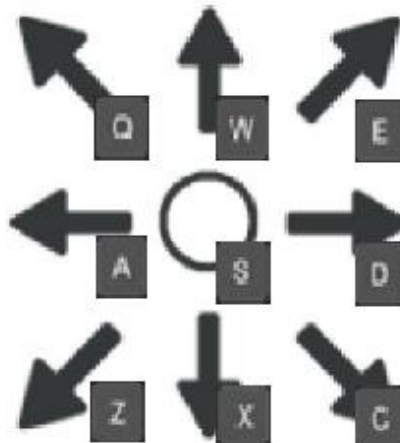


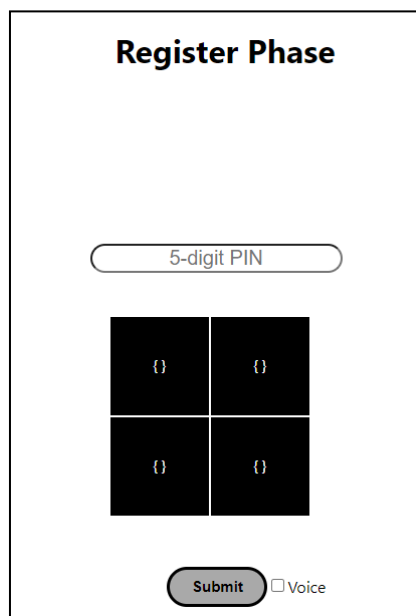
Fig. 5 Each key represents one direction.

Details of using the keyboard as a response button can be seen the Fig. 5. Each key represents one direction. All the direction responses are from the user PIN's digit to the challenge digit. For instance, if the user's first digit PIN is 4 and the challenge

value is 8, from the orientation (Fig. 1), we saw the number 8 is placed down-right from number 4, hence the user response is to either click on the down-right button using the mouse or simply click on the keyboard key “C”.

3.1. Registration

The implementation was designed for user experiments. There are two screens, representing two phases: registration and authentication. Under the registration phase (Fig. 6), the user sets up their user PIN before the authentication phase starts.



The registration interface is titled "Register Phase". It features a rounded rectangular input field labeled "5-digit PIN". Below this is a 2x2 grid of four empty square cells. At the bottom, there is a rounded "Submit" button and an unchecked checkbox labeled "Voice".

Fig. 6: Registration interface.

To begin the experiment with the SSSL method, the user must insert their 5-digit PIN and select the “Voice” checkbox. After clicking on Submit, the system will redirect to the login page of the SSSL implementation. Only the SSSL method is using voice to convey the challenge digit, so we put a voice selection there to redirect to the SSSL method.

If the user wants to begin the experiment with the Beta method, the user inserts their 5-digit PIN only, then proceed to click on submit button, which will redirect to the Beta method. Alternatively, if the user wants to begin the experiment with the Gamma method, the user inserts their 5-digit PIN and sets a grid cell for each of the 5 rounds. This cell sequence is remembered by the user. The user will have to click on the correct cells to set up the challenge digit during login. The user must select the cells in the correct order, which is a feature inspired by knock code.

3.2. SSSL method

Our implemented SSSL method is similar to the original SSSL system (Perković, Čagalj, & Rakić, 2010). After the registration process, the user will be redirected to the login page (Fig. 7). There is a diagram for orientation of digits and the arrow keypad. A 'Challenge' button is to trigger the system to play the audio challenge digit.

User's first click on the 'Challenge' button to listen to the challenge digit sent to earphones, and a timer will start. It will then stop when the user presses either a direction button or one of the 9 key buttons on the keyboard. These two steps of obtaining a challenge and inputting a response are repeated 5 times which corresponds to the 5-digit PIN. The time of each round will be added together to make the total login time. After 5 rounds, the user can click on the 'Submit' button or 'Enter' key on the keyboard. Then the system will make a comparison with the expected input. If the result matches, then the user is authorized. At the same time the total login time as well as a success or failure message will show under the Result section, as shown in Fig. 7.

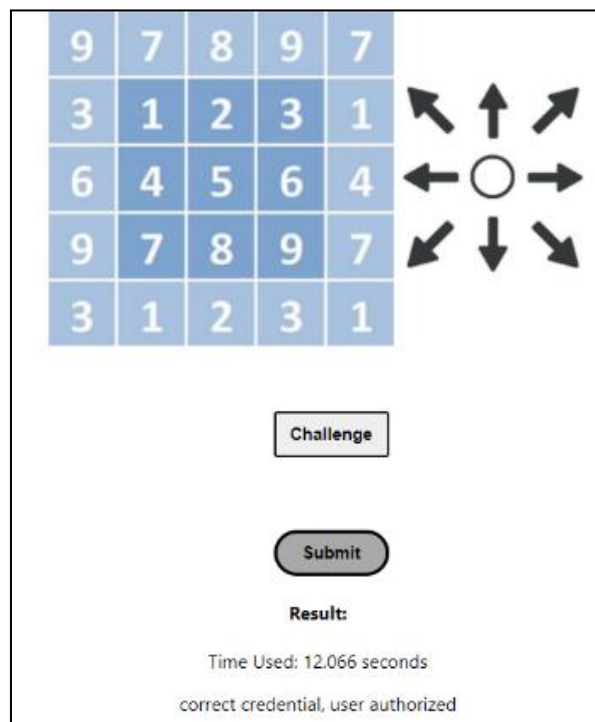


Fig. 7: SSSL authentication interface.

3.3. Beta Method

The Beta Method is a modification of the SSSL method. The Beta method does not need earphones, as the Beta method does not rely on audio to convey the challenge digit. The interface of the Beta method is shown in Fig. 8.

Instead of an audio randomly generated digit, the user presses a keyboard key to set up the challenge digit. The user sets the challenge digit by pressing on the keyboard key 'H' (in the middle of qwerty keyboard) a number of times, where the number of presses is the digit. At the same time, the timer will start. The timer will stop when the user selects a direction button (onscreen or via one of the 9 key buttons on the keyboard). As before, these steps are repeated 5 times which corresponds to the 5-digit PIN. The rest of the steps are similar to the SSSL method.

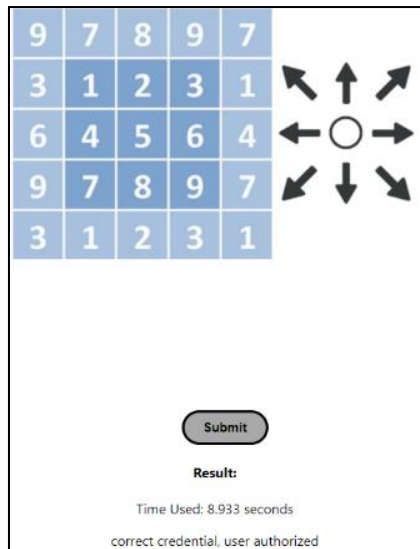


Fig. 8: Beta authentication interface.

3.4. Gamma method

The Gamma method is another version of the proposed method, where the Gamma method also does not need earphones. The way to generate the challenge number is inspired by Knock code (Jang & Park, 2018). The interface of the Gamma method is shown in Fig. 9.

The user recalls the grid cell sequence that was set during registration. The user then clicks on the first grid cell in the sequence to set up the challenge digit for the 1st PIN digit. The challenge digit is the number of mouse clicks. Upon clicking, the timer will start. Like SSSL and Beta, the timer will stop when the user presses either a direction button or one of the 9 key buttons on the keyboard. The steps of inputting a challenge digit and inputting a response are repeated 5 times, which corresponds to the 5-digit PIN. For example, the user clicks on the 2nd grid cell in the registered sequence to set up the challenge digit for the 2nd PIN digit.

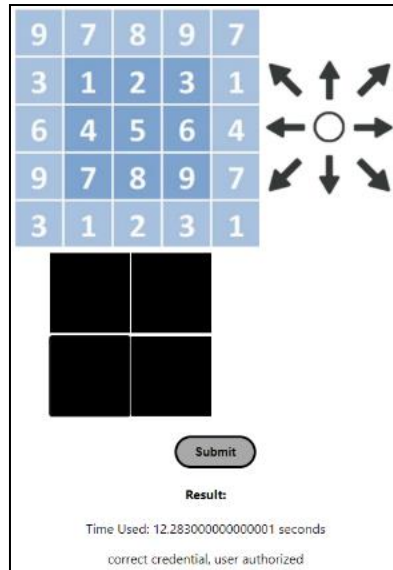


Fig. 9: Gamma authentication interface.

The main difference between the SSSL, Beta, and Gamma methods is that they have different ways of setting up the challenge number. For instance, while SSSL is using audio voice to transmit challenge digits via earphone to the user, Beta is using key presses and Gamma is using grid cells and number of clicks. Table 2 shows the similarities and differences between the SSSL, Beta and Gamma methods implemented.

Table 2: Comparison between SSSL, Beta, and Gamma methods.

Method	SSSL	Beta	Gamma
Similarity	They share the same digit orientation and the arrow keypad They use direction as the response		
Challenge transmission	Audio voice from computer	The challenge is inputted via keyboard	The challenge is inputted via mouse on a grid
Challenge value	Generated by the system randomly	set by the user using number of key presses	set by the user using grid cells and number of clicks
Secret	PIN	PIN	PIN and grid cell order.

4. Results and Discussion

After the system implementation, we performed user testing to study the usability and security of the proposed method's two versions, Beta and Gamma and that of the

control method: SSSL. In this section, we present how we conducted the evaluation procedure as well as discuss the results obtained.

4.1. Evaluation procedure

A total of 12 participants participated in our evaluation experiment with most of the participants being in the age group of 20 to 29, and only 2 participants being above 40. In the experiment, each participant was asked to log in using all 3 methods to make the comparison at the end of the experiment. The participants were given a tutorial on all 3 methods before the experiment began. Each of the participants had to set their 5-digit PIN during the registration phase, before beginning their authentication procedure.

To make the experiment scalable as well as easier for data collection, our scheme was developed as a web application, so that the user can use our scheme on a computer or mobile phone. For each participant, we recorded information such as response time, the sum of response time as the login time, as well as the number of unsuccessful logins. Every participant made 6 attempts for SSSL, Beta and Gamma methods each. This resulted in a total of 216 logins recorded for each method, along with the timings for successful attempts.

For the second experiment, we performed an observer experiment where the purpose was to evaluate the resistance of the method to shoulder surfing. In this setting, one person acts as a shoulder surfer who observes the challenge digit and the responses inserted by the user. We collect the user's challenge number, and the observation given by the shoulder surfer at the end of each round. The results for this experiment are presented in Section 4.3.

Finally, we provided a short questionnaire to all participants about the SSSL, Beta, and Gamma methods. The results are presented in Section 4.4.

4.2. Data presentation

Authentication experiments were carried out to measure login time and error rate. During the first experiment, after participants successfully logged in using the SSSL, Beta, or Gamma methods, we collected their login time. If a participant fails to authenticate, we increment the number of unsuccessful logins for the method they are using to measure the error rate.

4.2.1. Login time

In the login experiments, we restricted the participants from using simple PINs such as the repetition of numbers e.g. 1111.

For login time, we collected a total of 216 records with a successful login: 72 records each from SSSL, Beta and Gamma methods respectively. Each of the 12 participants contributed to 6 successful logins for each method. We then compiled the data into graphs to observe the average login time.

We plotted a graph of the login duration in seconds versus the number of logins. We only recorded the login times during successful logins.

From the graph, we can see that the login time decreases when the number of logins increases. This is possibly because participants were getting familiar with the system, so their response times improved.

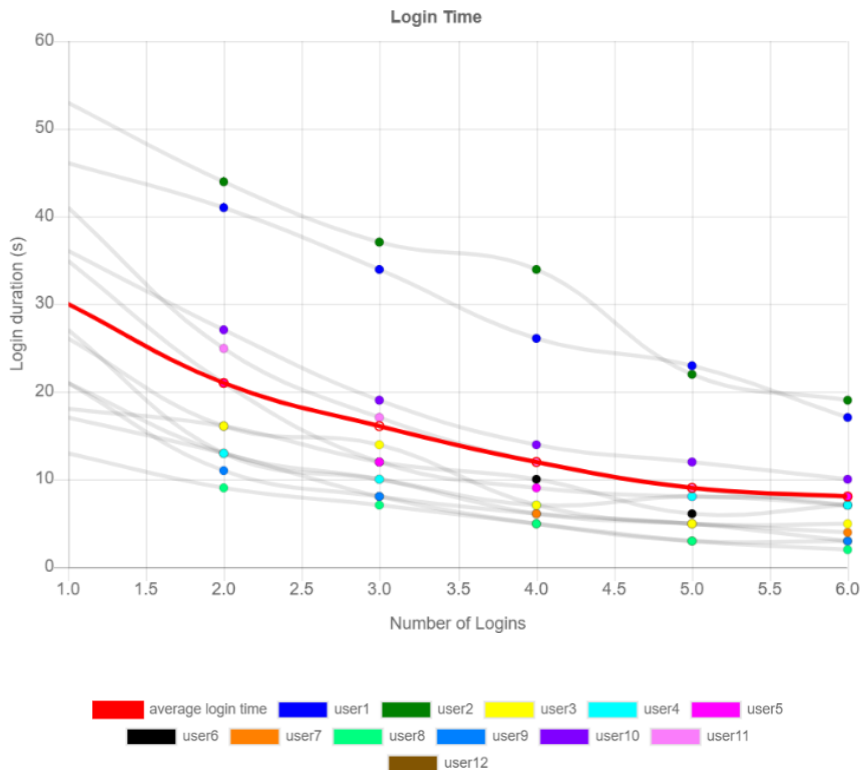


Fig. 10: SSSL methods' login time.

Fig. 10 shows the graph of login time for the SSSL method. From the graph we can observe the login duration for the first time is very high. This then decreases with time as the users get familiar with the system. The red line in the graph represents the average login time for 12 participants. On the 6th login, the login time has become very short, only 7.7 seconds on average. The fastest login duration is only 3 seconds. Comparing between our results and the results stated in the original SSSL (Perković, Čagalj, & Rakić, 2010), the average login time is almost the same, which shows consistency with their findings. Users 1 and 2 who were participants aged above 40 were also able to successfully login below 20 seconds. This is also consistent with the simplicity of SSSL which does not need any mathematical operations, therefore showing it is user-friendly.

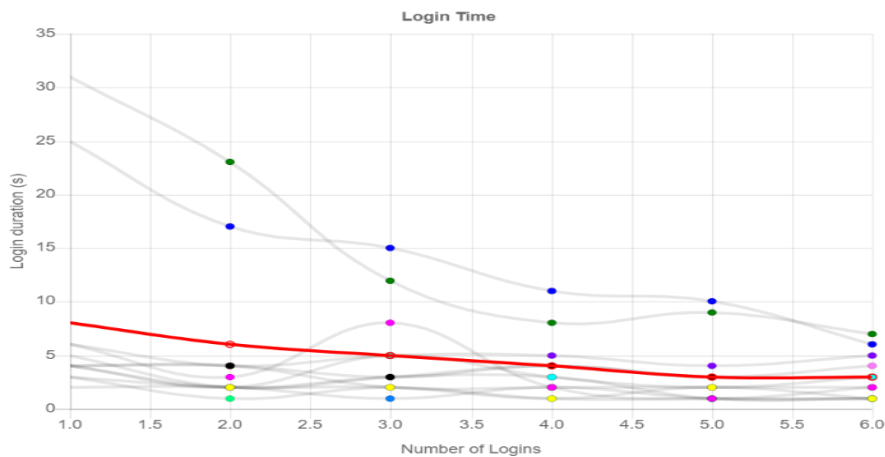


Fig. 11: Beta method login time.

Fig. 11 shows the graph of login time for the Beta method. In this experiment, the challenge digits (number of button presses) are chosen by the user. However, participants are restricted from using 1 or 2 for the number of presses. From the graph, the login duration is faster than the SSSL method. Similarly to SSSL, the login duration also declined after users had gotten familiar with the system. The red line in the graph represents the average login time. We observed that in the 6th attempt, the overall login time is shorter than the SSSL methods at only 3 seconds on average. This could be because in the Beta method, users do not need to listen for the audio as compared to the SSSL method.

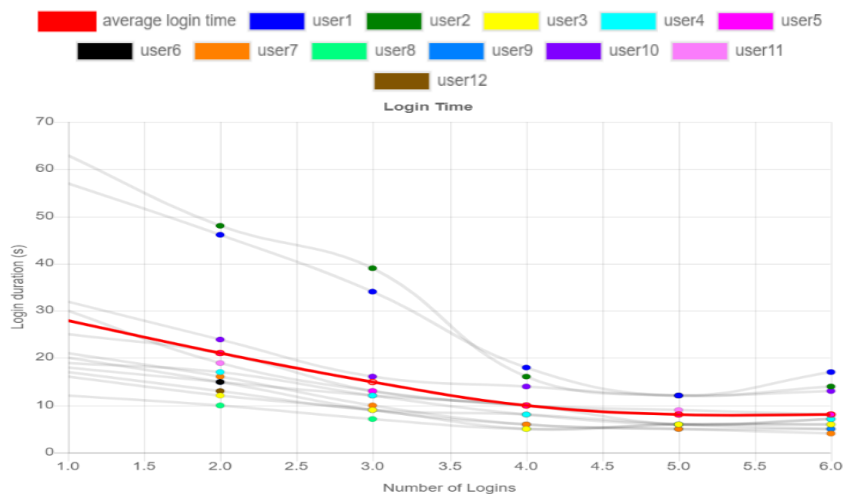




Fig. 12: Gamma method login time.

Lastly, Fig. 12 shows the graph of the login time for the Gamma method. Unlike SSSL and Beta, it has features inspired by the knock code (Jang & Park, 2018), so it is slightly more complex than the previous two. From the graph we can observe the login duration for the first time is higher than the previous two methods and only after the user gets familiar with the system, the login duration begins to decline. Moreover, at the end of the experiment, the overall login time is almost the same as the SSSL method with 8.3 seconds on average. The fastest login duration is 4 seconds. Once again, for Users 1 and 2 (aged above 40), they were also able to successfully login in below 20 seconds. This shows that although the Gamma method is more complex than the other two methods, overall the login time is still acceptable.

4.2.2. Error rate

In this subsection, we discuss the error rate calculated in our experiment. We counted the number of unsuccessful logins for all 3 methods.

At the end of the experiment, we collected a total of 39 unsuccessful logins - 16 from SSSL, 6 from Beta, and another 17 from Gamma.

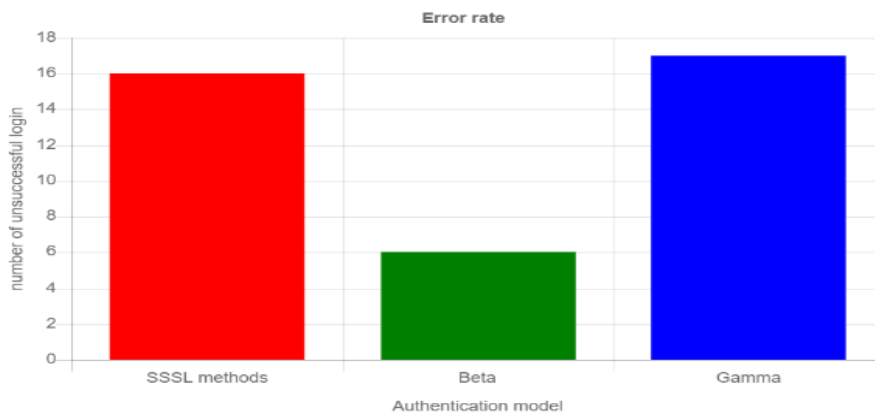


Fig. 13: Error rate.

Fig. 13 shows the total number of unsuccessful logins from 12 participants in the 3 methods. For SSSL, we collected 6 attempts from 12 participants, totaling 72 successful logins with 16 unsuccessful logins. So the total number of attempts using the SSSL methods is the sum of 72 and 16, which is 88. The error rate of the SSSL methods can be calculated using the total number of unsuccessful logins divided by a total number of attempts, which is 16 over 88, which is 18.18%. This result is higher

than the original SSSL result stated in (Perković, Čagalj, & Rakić, 2010) that had an 8% error rate. We conjecture this could possibly be caused by the duration of our experiment being shorter where the participants may not have had as much time to practice. Perković, Čagalj, & Rakić, (2010) carried out the experiments for a longer period (4 weeks) and collected more logins (≥ 28).

In the Beta method, there were only 6 erroneous attempts from 12 participants with a total of 72 successful logins. Thus, the total number of attempts using the Beta method is the sum of 72 and 6, which equals 78. Therefore, the error rate of the Beta method is 6 over 78, which is 7.69%. This lower error rate showed that the Beta method was possibly more convenient, simpler, and easier to use compared to SSSL.

Lastly for the Gamma method, there were 17 unsuccessful login attempts from 12 participants in addition to 72 successful logins. So the total number of attempts using the Gamma method is the sum of 72 and 17, which equals 89. The error rate of the Gamma method is 17 over 89, which is 19.1%. Gamma method is the enhanced version of the SSSL methods with the addition of knock code. We conjecture the error rate of the Gamma method is slightly higher than the SSSL methods because the complexity of the Gamma method is higher as the user must think of the correct order of the grid.

In the nutshell, from the results we presented under Section 4.2, we can conclude the Beta method has the shortest average login time and lowest error rate amongst all 3 methods.

4.2.3. Security

To find out the shoulder surfing resistance of our proposed methods, we conducted an experiment. In this experiment, we have a shoulder surfer to observe the challenge number inserted by the user.

In this subsection, we will discuss the security of all three methods. We invited 4 participants, that were randomly selected, to join our shoulder surfing experiment. The participants are paired, where one person acts as the system user and another person acts as the shoulder surfing observer and vice-versa. When the user is using the system, the observer is sitting beside the user and observes the response inserted by the user.

Without earphones, the only way users can avoid the adversary hearing the challenge digit is by lowering the speaker volume, which also impedes the user. In the experiment, the volume was first set low (32%) and increased gradually (36, 38, 40%) until the user could hear clearly. Two observers and the user wrote down their guesses of the audio number played at the intervals. Their answers were identical, even mishearing identically. SSSL method (Perković, Čagalj, & Rakić, 2010) relies on the earphone to keep challenge digit secret. Thus, without earphones it is not shoulder surfing resistant at all.

The Beta method has the user set up the challenge number, so the advantage of this method is that users are able to think of the challenge digits and the responses they want to insert before starting to press the key. Possibly due to this reason, the login time using the Beta method is the fastest. However, the security of the Beta method is not as high as the SSSL method as it relies on only the user's fast keypress speed to avoid being observed. If the user's keypress speed is slow, the observer can guess the range of the digit within ± 4 . Data was collected from three pairings of user and observer. Three users pressed their challenge number, which is 5 digits long. From a total of 15 challenge digits, 1 digit or 6.7% was guessed correctly. Some keyboards have a clicking sound when the key is pressed, which may leak information about a challenge digit. Key presses may be visible unless the user uses fast keyboard press speeds to obfuscate the adversary's vision. Possibly, the Beta method can be used on mobile phones or ATM machines in the bank. One of the unused keys on the keypad (e.g. 0,# or*) can serve to input the challenge or possibly have a foot switch/pedal for that purpose.

The Gamma method uses the knock code method where the user must use the mouse to set up the challenge digits. The advantage of this method includes higher security, as to the knock code system will become the second layer of security. However, the physical sound of a mouse click may also leak information, allowing an observer to guess the range of challenge digit in ± 2 , no matter how fast the user presses, unless the user manages to utilize a silent mouse. Data was collected from three pairings of user and observer. From a total of 15 challenge digits, 4 digits or 26.7% was guessed correctly. Hence, the percentage of matches is higher than the Beta scheme. Possibly the Gamma method can be deployed on mobile phones which do not have keypress sounds. Most of the observers have the same vantage point when the user is using the mouse to click on the grid.

Lastly, we consider the randomness issue on the challenge digit. The audio challenge used in the SSSL method is more random as the challenge digit is chosen by the computer, while the randomness used in the Beta and Gamma is dependent upon the user. However, our new methods improved the timing as the users do not need to wait for the audio to play before making their entry.

To calculate the possibility of guessing attack on the methods, in the first case we consider an attacker being able to see the response inserted by the user, but the challenge value remains unknown. In this case, no information is revealed by the attacker obtaining the response alone. There are 9 possible challenge digits for every response inserted by the user, so that is not the most efficient way to do a guessing attack. Instead, the attacker will try to guess the entry itself. There are 95 or 59049 possible outcomes to guess 5-digit entry. Another thing is that the Gamma method has extra security from the knock code. In addition to the attacker guessing the right responses, each of the rounds must have clicks in the correct cell out of the 4-cell grid. So, there are $(9 \times 4)^5$ or 60466176 possible outcomes.

Table 3: Comparison of results

Methods	SSSL1 (Perković, Čagalj, & Rakić, 2010)	SSSL2 method	Beta method	Gamma method
Average login time/ s	8	7.7	3	8.3
Error rate/ %	7	18.18	7.69	19.1
Possible outcomes	59049	59049	59049	60466176

Table 3 shows the comparison results between the data from the original SSSL paper (SSSL 1) and the data we calculated from our experiment. Our implemented SSSL method (SSSL 2) has similar login time to the original paper (Perković, Čagalj, & Rakić, 2010). We found that the Beta method was the fastest, and had less error rate.

4.2.4. Questionnaire

At the end of the experiment, all participants were asked to complete a short questionnaire about all three authentication methods. First, the participants were asked to rate the authentication time for the SSSL, Beta, and Gamma method from 1 – 5 where 1 is fast and 5 is slow. Second, participants were asked whether using a mouse or keyboard to insert a response is preferable. Lastly, the participants were asked whether SSSL, Beta, or Gamma is the most preferable in high-security situations. Tables 4 to 6 show the results for all the 3 questions by the 12 participants.

Table 4: Rating for authentication time.

Time to enter 5-digit PIN					
Grades	1	2	3	4	5
SSSL	4	6	2	0	0
Beta	11	1	0	0	0
Gamma	5	4	2	0	1

Table 5: Rate your preferred tool.

Which tool is preferable to insert response		
Tools	mouse	keyboard
Number of Participants	2	10

Table 6: Rate the best system.

Which method in the experiment is the best			
Methods	SSSL	Beta	Gamma
Number of participants	0	12	0

Table 6 shows the rating for the best system that is tested in the experiment, with 12 out of 12 participants preferring the Beta method. Beta does not require earphones to keep challenge digit secret, so the user does not need to bring earphones with them. Likewise, the Beta method is easy to be used as it does not require listening, resulting in the lowest average login time and lowest error rate.

5. Conclusion

In this work, we experimented on both security and usability aspects of 3 methods of authentication. SSSL is the existing audio-based method which we implemented. Beta and Gamma are the two versions of the proposed method, which is based on SSSL but does not have the audio challenges, replacing them with user-generated challenges. Experiments were conducted by 12 participants with their login times and error rates measured. One of the limitations is that the sample size was not large. Although our sample size was sufficient for this exploratory study, a higher number of participants would be informative. A future work would be to conduct experiments with a larger number of participants.

We conducted a shoulder surfing experiment on all three methods. Without earphones, the SSSL method was observed to not be shoulder surfing resistant. The Beta method had the highest shoulder surfing resistance among the three methods.

The Beta method was the most preferred as it has the lowest login time and error rate, as well as not needing additional earphones, resulting in all participants preferring Beta over SSSL and Gamma methods. This suggests that the Beta method is a viable alternative to SSSL, especially when earphones are not available.

Acknowledgements

This work was supported by the Multimedia University IR Fund [grant number MMUI/210071 - IR Fund].

References

- Binbeshr, F., Mat Kiah, M. L., Por, L. Y., & Zaidan, A. A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. *Computers & Security*, 101, 102116. DOI:10.1016/j.cose.2020.102116.
- Dan, Y.-X. & Ku, W.-C. (2017). A simple observation attacks resistant PIN-entry scheme employing audios. *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, 1410–1413. DOI:10.1109/ICCSN.2017.8230341.
- Hirakawa, Y., Kurihara, K., & Ohzeki, K. (2017). borderless interface for user authentication method tolerant against multiple video-recording attacks. *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, 1144–1148. DOI:10.1109/ICCSEC.2017.8446913.

Jang, Y. -H. & Park, Y. (2018). Enhanced knock code authentication with high security and improved convenience. *KSII Transactions on Internet and Information Systems*, 12(9), 4560–4575.

Key Lg Smartphones To Get Knock Code™ Upgrade | Lg Newsroom. (n.d.). Retrieved August 8, 2022, from <https://www.lgnewsroom.com/2014/03/key-lg-smartphones-to-get-knock-code-upgrade/>.

Lee, M. -K., Nam, H. & Kim, D. K. (2016). Secure bimodal PIN-entry method using audio signals. *Computers & Security*, 56, 140–150.

Perković, T., Čagalj, M., & Rakić, N. (2010). SSSL: Shoulder surfing safe login. *Journal of Communications Software and Systems*, 6(2), 65–73. DOI:10.24138/jcomss.v6i2.191.

Perković, T., Čagalj, M., & Saxena, N. (2010). Shoulder-surfing safe login in a partially observable attacker model. In R. Sion (Ed.), *Financial Cryptography and Data Security, Springer*, 351–358. DOI:10.1007/978-3-642-14577-3_29.

Rajarajan, S., Kalita, R., Gayatri, T., & Priyadarsini, PLK. (2018). SpinPad: A secured PIN number based user authentication scheme. *2018 International Conference on Recent Trends in Advance Computing (ICRTAC)*, 53–59. DOI:10.1109/ICRTAC.2018.8679257.