CluePIN – Secure PIN Entry for Touchscreen Devices Using Indirect Input

Mohammad Irteza Khan
Department of Computer Science
Louisiana Tech University
Ruston, USA
mik004@latech.edu

***Abstract*—In this report, I am presenting CluePIN, a PIN entry system for touchscreen devices that is more secure against shoulder surfing attack and completely eliminates the chance of smudge attack. Inputs are taken using simple touch gesture like left or right and upon successfully entering the PIN through gesture, user will be authenticated. Proposed system is compared against traditional PIN entry system. The result shows it is adequately fast for day to day use where user is concerned about security rather than speed. Moreover, CluePIN is easy to use, learning time is very short, and considerably more secure against shoulder surfing and smudge attack.**

Keywords—PIN; Authentication; Security; Shoulder Surfing

I. INTRODUCTION

Mobile devices nowadays contain a large amount of sensitive personal information. As a result, strong user authentication system on such devices has become mandatory. Though some modern devices are equipped with biometric authentication mechanisms like fingerprint scanners, knowledge based systems is still a dominating system in the field of user authentication. Furthermore, alternative solution like fingerprint scanner or face recognition, uses knowledge based system such as PIN or password as a fallback solution whenever alternative approaches fail.

PIN is the most common means of user authentication that is mainly introduced for ATM machine back in 1960 [1]. This input system is adopted for mobile authentication also. However, the problem with this method is, it is prone to shoulder surfing attack where an adversary could know the PIN by observing over the shoulder or by recording the PIN entry session using a camera. While some systems like ATMs can partially counter this problem by providing privacy shields and regulated environments, such measures cannot be taken for mobile devices as mobile interaction often takes places in uncontrolled semipublic situations. Moreover, touchscreen devices increase the chance of smudge attack where smudge spot of finger left on the screen and by observing the position of those spots an adversary can reduce the number of possible PINs and break the system without even observing the PIN entry session [2].

Recently, possibility of a new attack mode has been discovered. Researchers have shown that PIN code could be guessed just by observing the movement of hand from far away [3]. They have shown that, it is possible to successfully predict the PIN code just by observing one PIN entry session. However, they mentioned that, this mode of attack is not performed in real world yet, but there is a great possibility of seeing this type of attack in near future.

To overcome this issue, a wide range of alternative methods have been proposed. Graphical Password is a strong contender among them [4]. They discussed with several password scheme that are easy to memorable but hard to guess. Déjà vu [5] is a authentication scheme where user has to pick a computer generated abstract image. However, in their study they have found that abstract images are half as memorable as that for photographic images with a clear central subject. But, personal photos are very much predictable and therefore not a good candidate for secure authentication system [6]. Several other different sequential graphical password framework for user authentication has also been proposed [7], but most of those systems takes more than 10 seconds to complete the input taking process. Despite of their long entry time, security does not improve drastically. Design space of graphical passwords and comparative analysis of several graphical password systems has also been studied [8]. They have shown some analysis among different methods in order to achieve password with same strength and compared the time to input password successfully.

Google introduced a graphical authentication methods named as Android patterns [9] back in 2010. Despite of its popularity among Android devices due to its playfulness nature, it is very susceptible to smudge attack [10]. Researchers have shown that, the pattern was partially identifiable in 92% of the time in their tested lighting condition and setup. In order to make this system resistant to smudge attack, multiple methods are proposed in [11]. They have shown comparative analysis of their proposed system about likeability and usability among users. On the other hand, a field study has also done among users about the usability of pattern and PIN based authentication [12].

Password entry using eye gaze have also been proposed [13]. But, this system is heavily error prone and entry time is relatively higher. That will frustrate the user quickly. Besides, detecting eye gaze using camera needs proper lighting condition which is not always obtainable for mobile devices.

Though, not a new concept but biometric authentication for mobile device gets much attention nowadays. Google

introduced face unlock system from Android 4.0 [14]. But, that system is unreliable [15] as it can be fooled by showing captured image of user. In order to circumvent this issue user liveness check has been introduced [16], which is immediately hacked after its release [17]. After introducing Apple's Touch ID authentication system [18], using fingerprint scanner for mobile authentication becomes very popular [15]. Many other companies such as Samsung, LG followed this trend and release their flagship devices equipped with fingerprint recognition [19], [20]. But, soon after its release, Apple's Touch ID has been hacked by independent hacker group [21]. Moreover, using fingerprint as an authentication system is very unsecure; because if compromised, it can never be changed [15]. Also a survey on multiple users have also been performed about peoples' reaction of these methods [22], where most of the people expressed that they are uncomfortable of sharing their biometric information with mobile devices and after several days, went back to regular PIN based authentication.

In this report, I am proposing a PIN entry system where user will input PIN using gesture instead of typing the PIN on keypad. The proposed system will look very similar to existing keypad based entry system, so that learning curve is easier for new user and input time is adequately faster for practical use. A demo of proposed system is implemented on Android platform and a user test case with 10 different users is performed also. Finally, a comparative analysis about the security and usability with traditional PIN entry system is performed as well as algorithm for breaking the PIN is analyzed also.

II. Related Work

There are actually three different approaches for human authentication [15]. These are, "something you know", "something you have", and "something you are." PIN or password based authentication systems fall on the first category. It forces user to set a password and remember the exact password every time for authentication. Problem with this authentication method is it is susceptible to shoulder surfing attack [23], smudge attack [10], and even hand movement attack [3]. Several works have been done in order to improve the security of existing PIN entry method. A promising approach among them is using indirect input. This means that authentication tokens are taken by some kind of detour instead of direct input. This will make it harder for an adversary to know the password just by observation. Cognitive trapdoor game approach has been proposed in [24]. For each digit, it requires four presses from user. Further analysis and improvement of this system has been proposed in [25]. Several mobile PIN entry concepts which utilize audio and haptic cues have been proposed in [26]. They have claimed that using haptic cues will make system more secure because of its unobservable nature. A system is proposed and implemented in [27] by using haptic cues as a secondary channel. They use color array and number index that has to be matched based on secondary channel cues which is vibration feedback from mobile in their case. Another method is proposed [28] for touchscreen devices where user has to find the letter from a randomized grid and then choose the letter using two interactor. The position of the keys changes in each step, that is why they claim that it will be hard for an observer to reconstruct what has been typed. Another indirect approach is proposed in [29] where user has to set PIN number along with a color among three different colors for each digits. While entering the PIN, three different colored letters is shown under each number. User has to type letter that has correct color for that digit. After every entry, the color and letter is changed. In [30], researchers have proposed and implemented another PIN entry approach where keypad is divided into two groups using two different colors. Each color groups number shows five different swipe gestures. User has to swipe towards that direction inside a box of that color for the current digit of the PIN code. After every session, these directions are changed randomly.

III. Authentication Method

A. CluePIN Concept

CluePIN is a concept of taking PIN entry from user through an indirect medium. While user is setting up the PIN code, along with a PIN number user has to pick a gesture from left and right gestures. The selected gesture will be used for "yes" command and the opposite gesture will be used for "no." During the authentication period, five random digits will be shown to the user. If the current PIN digit is among those shown digits', user will swipe the "yes" gesture, which was selected during PIN setup time. Or if the current PIN digit is not among the shown digits', user will swipe the "no" gesture. After that, five random digits will be shown again for the next digit of the PIN and this process continues until all the digits of the PIN code is entered. Along with this, a face recognition phase is also included in the system. User's face is captured and trained during PIN setup stage. During authentication phase, the system will try to recognize the face of the user at first. If it recognizes the user with more than 80% confidence, then number of shown random digits will be reduced to three. Between 50-80% confidence, this number will be four and for less than 50% confidence, number of random digits will be five. This will reduce an authentic user's burden from scheming through a large amount random numbers.

B. Prototype

A prototype of the proposed system is implemented in Android platform. The app that is developed can store multiple users' information. The app will also store the time that was taken by the user for successful or failed authentication in order to analyzed in future. In Fig. 1 a PIN entry session is shown. The digits are highlighted on a regular keypad so that the user can just concentrate on the position of the current PIN digit on traditional keypad. In this way user does not have to scheme through all the random digits. This will make the input process faster. For implementing face recognition, LBPH algorithm from OpenCV for Android has been used. During face recognition phase it waits for five seconds to recognize the face. After the time passes, random digits are highlighted on the keypad based on the confidence of face recognition phase.

IV. Security Evaluation

The password space for CluePIN is as large as regular PIN based system, as it uses same numeric digits that is used by regular PIN entry system. But the way it takes input from user makes it resistant against several attacks. As the highlighted digits are picked randomly, having the information of a single session does not help an adversary to break the PIN. Several attack methods are discussed in this section in order to analyze

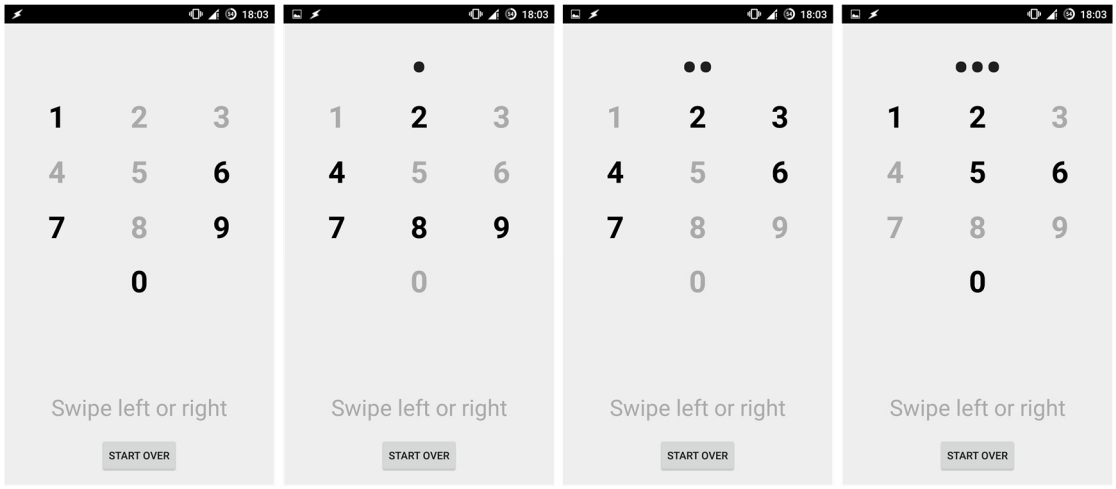

Fig. 1. Different stages for entering a 4-digit PIN is shown. Here, the PIN is "1234" and "yes" gesture is towards right direction. In first stage, user has to swipe towards right direction, as number "1" is highlighted. Same has to be done for the second and third stage. At the final stage; user has to swipe towards left direction, as number "4" is not highlighted.

the security provided by CluePIN approach versus regular PIN entry approach.

A. *Shoulder Surfing Attacck*

CluePIN changes the highlighted digits in each step randomly. That will prevent the adversary from getting much information from a single PIN entry session even s/he could see every action exactly. Moreover, only authentic user knows which swipe direction is used for "yes" command. So, seeing user swipe in a direction gives two probabilities to an adversary; maybe the current PIN digit is among the highlighted digit or maybe not. As a result, this will not compromise the exact digit of the PIN. However, it is possible to decode the exact PIN code by recording several PIN entry sessions. An algorithm for decoding the PIN code is given in Fig 2. To decode a single digit, the given algorithm will need the information of at least three sessions' when all other conditions are met. The probability of decoding a single PIN digit by using the information from three sessions are calculated using the following formula:

$$1/2 \times \left(1/2 \times \binom{5}{4} \Big/ \binom{9}{4}\right) \times \left(1/2 \times \binom{8}{3} \Big/ \binom{9}{4}\right) \quad (1)$$

And the result of (1) is 0.0022. So, the probability of decoding a single PIN digit by using the information of three observations is 0.0022. Thus, by using the information of three observations; probability of decoding all the digits of a four digits PIN is 2.34256×10^{-11}.

In Fig. 3 average number of observation needed to decode three, four, five, and six digits PIN are given. This test is done by randomly generating a different PIN and then emulate the successful PIN swipe pattern for a session which is termed as an observation. After that, the algorithm tries to decode the digit using the information of this observation. If it cannot decode the digit, another successful observation is provided. This process continues until it decodes all the digits. For each case, 25,000 different PINs are used. From Fig. 3 we see that the algorithm takes a large number of observations when only three random digits are shown. This happens because when only three digits are shown, probability of rejecting a number as a candidate reduces. As the algorithm depends on changing the swipe direction between two sessions when same number shown on the screen, it increases the required number of observations greatly.

B. *Smudge Attack*

It is not possible to perform smudge attack to break the PIN in CluePIN system. Because, smudge spot does not reveal any information about the random shown digits or the actual PIN code. User has to swipe based on the random digits that are shown in each step. And the smudge spot will always be at the

```
boolean candidate_arr[10] = TRUE
int direction_arr[10] = 0

getDigit(shown_digits[], direction){

    For i in shown_digits {
        If candidate_arr[i] == true and
          direction_arr[i] == 0
            set direction_arr[i] = direction

        Else if direction_arr[i] != direction
            set candidate_arr[i] = false
    }

    count = 0
    pin_digit = -1

    For (i = 0; i < 10; i++) {
        If candidate_arr[i] == true
            If count == 0
                pin_digit = i

        count = count + 1
    }

    If count == 1
        return pin_digit
    Else
        return -1

}
```

Fig. 2. Algorithm for decoding the PIN

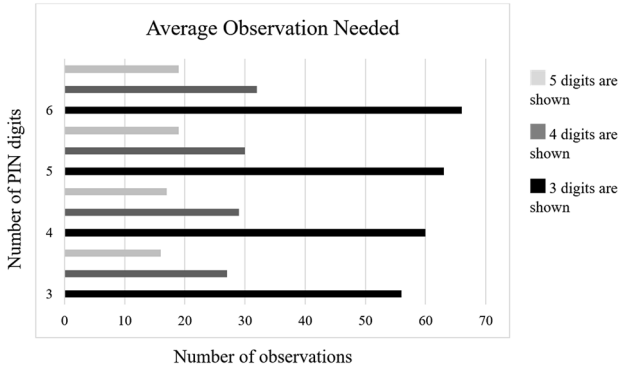

Fig. 4. Comparison of average number of observations needed for different length of PIN. For all cases when 3 digits are shown it requires a large number of observations.

same place for every case of input. So, the proposed system is completely safe against smudge attack.

C. *Hand Movement Attack*

Capturing hand movement also cannot be used to break or guess the PIN. Similar as smudge spot; the hand movement does not reveal any information about the PIN code. In order to break the PIN hand movement along with the random digits that are shown in the screen has to be recorded. Only then it is possible to employ the given algorithm to break the PIN. Although, it will require information from multiple successful authentication sessions to decode the PIN as shown in Fig. 3.

V. Usability Analysis

A. *Procedure and Participants*

Evaluation of the proposed system was conducted using the developed Android app installed in a Samsung Galaxy S4 mobile phone. 10 peoples are participated in the study where all of them are familiar with touchscreen phone and use those in a regular basis. Participants are divided into five groups where each group has two members. First, one participant is asked to set a four-digit PIN code. Then the participant tries to login to the system when face recognition confidence is higher than 80%. Another member then observes all the five sessions and at the end tries to guess the PIN code. Then the user changes his PIN code and repeat the same procedure by deforming the face so that the face recognition confidence is between 50-80%. And finally same procedure repeats with face recognition confidence of less than 50%. After finishing all three stages, participant try to login using traditional keypad based PIN entry method and the other participant performs as adversary again. In this time, adversary tries to guess the PIN after finishing every session. Then the participants change their role and repeats the same process. Time taken for every stages recorded for future analysis. Before recording the data, participants are allowed to test the CluePIN system in order to familiarize with the system.

B. *Comparison between CluePIN and Regular PIN Entry*

A comparison between the CluePIN and regular PIN entry method is given in Fig. 4. Here, regular PIN entry method takes

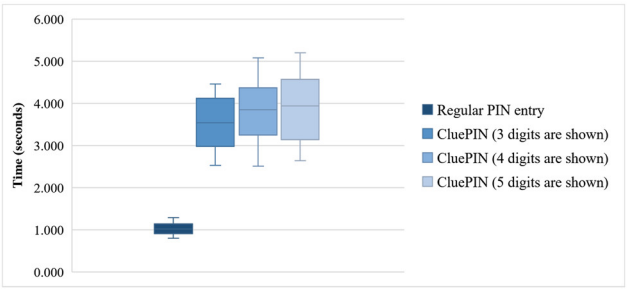

Fig. 3. Distribution of successful login attempts for each system

around 1s to complete which is undoubtedly superior than CluePIN entry time. On average, CluePIN entry method takes around 3.7 seconds. An important fact is that time does not vary greatly due to the change of the number of random digits. This is because of highlighting the numbers in traditional keypad. As the participants are familiar with the traditional keypad, they tend to look for the digit in its particular position. If it is highlighted, then user swipe the “yes” gesture or else the “no” gesture. This relieves the user from scheming all the digits, but does not help an adversary in any way; as adversary has no idea where the user is looking at.

After finishing the five sessions the participant who was performing as an adversary tries to guess the PIN which was inputted using CluePIN. No one can successfully guess the PIN for any cases. In case of regular PIN entry, 7 out of 10 participants correctly guess the PIN just after one session. Rest of the 3 participants correctly guess the PIN after second sessions.

VI. Conclusion and Future Work

The evaluation showed that CluePIN is notably more secure against shoulder surfing attack compared with standard PIN entry, due to its process of indirect entry. However, as the process of input taking creates an extra cognitive load to the user, it takes a little longer to finish the session than standard PIN entry system. But, the security it provides against several attacks are far more awarding than the extra time it takes. Also, the average time it needs to complete a session is 3.7s, which is arguably acceptable compared with other proposed system [24], [27], [31]. Moreover, CluePIN relies on “something you know” strategy, on which users are very much comfortable, as it has been shown in [22] that peoples are not very comfortable of sharing their biometric information. Another strong point of CluePIN is that it requires no extra hardware. Any phone or ATM machine equipped with touchscreen display can implement this very easily.

Now, there are some scope of improvement that could make the proposed system much more secure. Instead of using only left and right gesture as input signal, up and left gesture could also be used along with a haptic feedback cue. Using haptic feedback cue will make the shoulder surfing or camera attack even more harder. As in that case only the information from visible observation will not be sufficient to decode the PIN code. Therefore, this approaches surely deserves further assessment.

REFERENCES

[1] "Royal honour for inventor of Pin," *BBC*, Jun-2006.

[2] S. Sinofsky, "Signing in with a picture password - Building Windows 8 - Site Home - MSDN Blogs," Dec-2011. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx. [Accessed: 29-Jul-2015].

[3] D. Shukla, R. Kumar, A. Serwadda, and V. V. Phoha, "Beware , Your Hands Reveal Your Secrets !," in *CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 904–917.

[4] W. Moncur and G. LePlâtre, "Pictures at the ATM: Exploring the usability of multiple graphical passwords.," 2007.

[5] R. Dhamija and A. Perrig, "Deja vu: A User Study Using Images for Authentication," *Proc. 9th USENIX Secur. Symp. Denver, CO Usenix, 2000.*, no. 102590, pp. 45–58, 2000.

[6] T. S. Tullis and D. P. Tedesco, "Using Personal Photos As Pictorial Passwords," in *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, 2005, pp. 1841–1844.

[7] L. T. Hui, H. K. Bashier, L. S. Hoe, W. K. Kwee, M. Fikri, and A. Abdullah, "Sequential Graphical Password Framework for Mobile Devices," in *2014 Fourth World Congress on Information and Communication Technologies (WICT)*, 2014, pp. 194–198.

[8] F. Schaub, M. Walch, B. Könings, and M. Weber, "Exploring the design space of graphical passwords on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 2013, p. 1.

[9] J. B. Miller and J. M. Trivi, "Touch Gesture Actions From A Device's Lock Screen." Google Patents, 2011.

[10] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," *USENIX Conf. Offensive Technol.*, pp. 1–7, 2010.

[11] E. von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making Graphic-Based Authentication Secure against Smudge Attacks," in *Proceedings of the 2013 international conference on Intelligent user interfaces (IUI '13)*, 2013, pp. 277–286.

[12] E. Von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," in *Proceedings of Mobile HCI 2013 – Security And Privacy*, 2013, pp. 261–270.

[13] A. De Luca, M. Denzel, and H. Hussmann, "Look into my eyes!: can you guess my password?," in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 2009, p. 1.

[14] "Ice Cream Sandwich | Android Developers." [Online]. Available: http://developer.android.com/about/versions/android-4.0-highlights.html. [Accessed: 29-Jul-2015].

[15] A. De Luca and L. München, "Is Secure and Usable Smartphone Authentication Asking Too Much?," *Computer (Volume:48 , Issue: 5)*, pp. 64 – 68, 2015.

[16] C. Velazco, "Google Pumps Up Jelly Bean's Face Unlock Feature With A New 'Liveness Check' | TechCrunch," Jun-2012. [Online]. Available: http://techcrunch.com/2012/06/29/google-pumps-up-jelly-beans-face-unlock-feature-with-a-new-liveness-check/. [Accessed: 29-Jul-2015].

[17] A. Racoma, "Android Jelly Bean Face Unlock 'liveness' check easily hacked with photo editing | AndroidAuthority," Aug-2012. [Online]. Available: http://www.androidauthority.com/android-jelly-bean-face-unlock-blink-hacking-105556/. [Accessed: 29-Jul-2015].

[18] "Apple - iPhone 5s - Technical Specifications." [Online]. Available: http://www.apple.com/iphone-5s/specs/. [Accessed: 29-Jul-2015].

[19] "Samsung GALAXY S5." [Online]. Available: http://www.samsung.com/global/microsite/galaxys5/features.html. [Accessed: 29-Jul-2015].

[20] "Discover the LG G4 – Release Date, Specs & Where to Buy | LG USA." [Online]. Available: http://www.lg.com/us/mobile-phones/g4. [Accessed: 29-Jul-2015].

[21] "CCC | Chaos Computer Club breaks Apple TouchID," Sep-2013. [Online]. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid. [Accessed: 29-Jul-2015].

[22] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I Feel Like I ' m Taking Selfies All Day ! Towards Understanding Biometric Authentication on Smartphones," in *CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 1411–1414.

[23] 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 SOUPS 07*, 2007, vol. 229, p. 13.

[24] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM conference on Computer and communications security - CCS '04*, 2004, p. 236.

[25] T. Kwon and J. Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 2, pp. 278–292, 2015.

[26] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry," *Interact. Comput.*, vol. 24, no. 5, pp. 409–422, Sep. 2012.

[27] A. Aratani and A. Kanai, "Authentication Method against Shoulder-Surfing Attacks using Secondary Channel," in *2015 IEEE International Conference on Consumer Electronics (ICCE)*, 2015, no. c, pp. 430–431.

[28] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-Resistant Keyboard : Towards More Secure Password Entry on Publicly Observable Touch Screens," in *OZCHI 2005*, 2005.

[29] A. DeLuca, K. Hertzschuch, and H. Hussmann, "ColorPIN – Securing PIN Entry through Indirect Input," in *In Proceedings of the 28th international conference on Human factors in computing systems*, 2010, pp. 1103–1106.

[30] E. Von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "SwiPIN - Fast and Secure PIN-Entry on Smartphones," in *CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 1403–1406.

[31] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, "Multi-Touch Authentication on Tabletops," in *ACM Conference on Human Factors in Computing Systems (CHI)*, 2010, pp. 1093–1102.