HAL
open science

Security Analysis and Psychological Study of Authentication Methods with PIN Codes

Xavier Bultel, Jannik Dreier, Matthieu Giraud, Marie Izaute, Timothée Kheyrkhah, Pascal Lafourcade, Dounia Lakhzoum, Vincent Marlin, Ladislav Motá

To cite this version:

Xavier Bultel, Jannik Dreier, Matthieu Giraud, Marie Izaute, Timothée Kheyrkhah, et al.. Security Analysis and Psychological Study of Authentication Methods with PIN Codes. RCIS 2018 - IEEE 12th International Conference on Research Challenges in Information Science, May 2018, Nantes, France. pp.1–11, 10.1109/RCIS.2018.8406648 . hal-01777898

HAL Id: hal-01777898

https://hal.science/hal-01777898

Submitted on 25 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Security Analysis and Psychological Study of Authentication Methods with PIN Codes

Xavier Bultel
LIMOS, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Jannik Dreier
LORIA, INRIA, CNRS
Université de Lorraine,
Nancy, France

Matthieu Giraud
LIMOS, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Marie Izaute
LAPSCO, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Timothée Kheyrkhah
LIMOS, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Pascal Lafourcade
LIMOS, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Dounia Lakhzoum
LAPSCO, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Vincent Marlin
LIMOS, CNRS
Université Clermont Auvergne
Clermont-Ferrand, France

Ladislav Motá
PSYCLE
Aix Marseille Université
Aix-en-Provence, France

***Index Terms*—security, authentication, pin code**

***Abstract*—Touch screens have become ubiquitous in the past few years, like for instance in smartphones and tablets. These devices are often the entry door to numerous information systems, hence having a secure and practical authentication mechanism is crucial. In this paper, we examine the complexity of different authentication methods specifically designed for such devices.**

We study the widely spread technology to authenticate a user using a Personal Identifier Number code (PIN code). Entering the code is a critical moment where there are several possibilities for an attacker to discover the secret. We consider the three attack models: a *Bruteforce Attack* (BA) model , a *Smudge Attack* (SA) model, and an *Observation Attack* (OA) model where the attacker sees the user logging in on his device. The aim of the intruder is to learn the secret code.

Our goal is to propose alternative methods to enter a PIN code. We compare such different methods in terms of security. Some methods require more intentional resources than other, this is why we performed a psychological study on the different methods to evaluate the users' perception of the different methods and their usage.

I. Introduction

With the development of technology, more and more personal and sensitive data is stored on our personal devices such as smartphones. More and more companies provide smartphones or tablets to their employees in order to facilitate their work, for instance during business trips or inside the enterprise to facilitate the access to data. In many companies and organizations the digital revolution also starts by changing the way information is collected using such new devices. With the progress of technology and the improvements of batteries capabilities, power of processors and new wireless connections (WiFi, Bluetooth, etc.), smartphones or tablets are devices that are part of this revolution. They allow the users to collect and access to the data in a very practical way. However, these devices have often no or limited authentication mechanisms. Hence, to protect the access to sensitive data on such devices from non-authorized persons, a secure authentication of the user of the device is indispensable. Moreover, authentication methods for tablets and smartphones are essential to protect the data if the devices is lost or stolen, in particular to avoid that some resources are used by non authorized persons, like for example phone credits or even money in the case of a credit card information.

One of the most common authentication methods is the *Personal Identifier Number* (PIN) code usually consisting of four or six digits. The PIN code is used for instance to unlock a smartphone, to withdraw money from an *Automated Teller Machine* (ATM), to activate/deactivate an alarm or to open a door. For these reasons, the security of the PIN code is essential. The PIN authentication method is known to be fast and easy to use for most people, however it can be dangerous to use it under certain circumstances depending on the environment. For instance, an adversary can try to get information on someone's PIN code by direct observation when the user withdraws money from an ATM, by using a camera that records the PIN code, or even by using thermal camera to know the touch used to enter the PIN code [20]. Nowadays, if an adversary knows our PIN code, one has to contact the bank to change the credit card, which implies expenses for credit card owner. On smartphones users should change their PIN code in such a case, but in practice only few users do that (probably because it requires remembering the new code, because of the fear of not remembering the new PIN code and not being able to use the smartphone). Our goal is to see how we can improve the PIN code mechanism in order to be more resistant to such attacks, in the sense of resilience. For this, we consider several scenarios and compare

their security and their acceptability by the users in terms of difficulty.

A. Contributions.

In this paper, we propose different authentication methods. All the studied authentication methods are based on a secret PIN, i.e. we consider neither pattern authentication methods nor graphical or biometric authentication methods. In order to authenticate, a user needs to knows a secret number with n digits. We use 4 digits to test a concrete case with a reasonable difficulty in terms of memory. Then we study the security of the authentication methods given the following three threat models:

1) The *Bruteforce Attack* (BA) model where the adversary has only access to the device and has no other information on the PIN code. For example the adversary stole a credit card and tries to find the correct 4 digit code.
2) The *Smudge Attack with Physical Access* (SA) model where the adversary is in possession of the user's device and has some information on the PIN code. For instance, the adversary stole a smartphone and can see the finger smudge on the locked screen.
3) The *Observation Attack at Distance* (OA) model where the adversary can see the authentication process. This is for example the case, when an adversary looks over the shoulders of the victim while she is withdrawing money at the ATM or unlocking her smart phone in public, e.g. in crowded public transportation.

In addition of this technical consideration, we also study the relation between users and PIN code from a psychological point of view. That means, we study the perceived level of difficulty for the users to use the different authentication methods.

B. Related Work.

To protect the user against an adversary who can directly see the entered PIN code, for example an adversary who is looking over the shoulders of the victim while she is withdrawing money at the ATM, i.e. the OA model (this attack is often also called a *Shoulder Surfing Attack*), several authentication methods are proposed in the literature. Lee proposed in [17] a method using n rounds for a code composed of n digits. The screen displays two horizontal arrays, one composed of digits on the other composed of symbols. At the first round, the first digit of the code is associated with a symbol, then the user will use this symbol to select other digits of her code. Kwon and Na [16] proposed a new pattern lock system called *TinyLock*. The system uses a tiny pattern authentication method and a validation phase to remove smudges from the screen of the user and so to avoid attacks based on these traces. In this paper, we consider only authentication methods based on PIN codes. In [28], Shi et al. proposed an authentication method that for each login, after the user inserts her bank card into the ATM, the machine displays a table where each cell of which contains a number. The assignment of numbers to cells is executed in such a way that some copies of every number are randomly assigned to the cells in the table. After the user input the number corresponding to the first position of her code, the same process is repeated until the user has input all numbers of her code.

Some authentication methods are based on pattern lock authentication systems. They consist in wiping a finger across a specific sequence of nine dots chosen by the user to unlock the device [13]. An analysis of such possible patterns space is done in [27] while the different tradeoffs between usability and security are studied in [19]. In a different way, Zezschwitz et al. [30] proposed an authentication method for smartphones called SwiPIN. This method uses only two simple touch gestures like *up* or *down*. The authors prove that it is secure against a human observer. Another approach was proposed by Roth et al. [26]. The authors proposed two concepts which display digits in distinct sets on the screen. To determine the PIN code, a user repeatedly indicates the respective target set. Then the intersection of these sets is used as the code to authenticate the user. Davis et al. shown in [8] that when the user choose is graphical password drawing a pattern in the screen, the low entropy produces a non-negligible drawback for some shemes. However, Wiedenbeck et al. proposed the Convex Hull Click scheme [31] allows a user to prove knowledge of the graphical password safely in an insecure location because users never have to click directly on their password images.

Other authentication methods based on graphical password have been proposed and are presented by Biddle et al. in the survey [6]. These methods consist in knowing a sequence of unique images selected by the user to make a "story". In [14], Jermyn et al. proposed a authentication method using graphical input devices that enable the user to decouple the position of inputs from the temporal order in which those inputs occur, they shown that this decoupling can be used to generate password schemes with substantially larger and memorable password spaces. With the system "Deja vu", presented in [10], the authors use images instead of PIN code to authenticate users. In [12], Hayashi et al. use modified versions of known images to authenticate users.

In [5], the authors propose a PIN entry system based on audio or touch-sensitive cues. They link movements on a mobile phone touch screen with the display of non-visual cues; a selection of a sequence of these cues composes a password.

Another recent technique, called Illusion PIN (IPIN), is based on some optical illusions [23]. It allows the user, who has to be close to the device, to to see the right keypad to enter her PIN, while an attacker who is looking at the device from a bigger distance sees a fake keypad.

With the development of biometric sensors on smartphones, biometric authentication methods are more and more popular [18]. Evangelin and Fred proposed a method using physical characteristics recognition [11], while Sun et al. proposed an authentication method based on a hand gesture signature [29].

Unlike these authentication methods, we are interested in PIN codes where the user enters a sequence of digits, since this mechanism is easier to put in place. We do not consider authentication methods based on patterns.

In this article, we only aim at analyzing the difficulty for an adversary to guess a PIN code according to his knowledge. We do not aim at breaking the protocols used to verify if the PIN code is correct, as done for instance in [21].

C. Outline.

First, we present in Section II six different authentication methods based on the PIN code. Then we expose three different threat models in Section III and study the security of the presented authentication methods depending on these three threat models in Section IV. Finally, we give a psychological study for the links between the users and the usage of the authentication methods.

II. Authentication Methods with PIN Codes

Different methods of authentication are possible. Some of them require to memorize a numerical code, other a graphic pattern. In the following, we give different authentication methods based on PIN codes. We analyze their security in Section IV in the different attack scenarios. By security, we mean the difficulty for an adversary to guess the PIN code.

A. PIN Code with a Deterministic Placement (PDP)

The *PIN code with a Deterministic Placement* (PDP) is the most commonly used authentication method, and is very popular with smartphones or credit cards. It consists in entering the secret code (usually four digits) on a deterministic numeric pad, in others words where the numbers are always displayed in the same position on the pad. An example of such pad is given in Figure 1. The users, who wants to enter the PIN 1234, has to successively enter the digit 1 then 2 then 3 and 4.

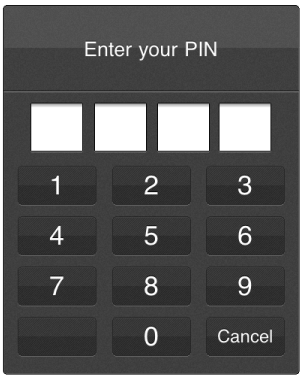

Fig. 1: Example of PDP PIN code.

B. PIN Code with a non Deterministic Placement (PnDP)

The *PIN code with a* non *Deterministic Placement* (PnDP) is, as its name suggests, the authentication method where numbers of the pad are displayed in different positions each time it is used. For example, during the first login, the number 1 is displayed at the top left corner of the screen, but during the second login this same number can be displayed in the right bottom position as in Figure 2. The pad is thus different each time a PIN code is asked for.

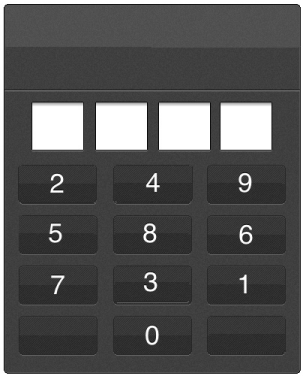

Fig. 2: Example of PnDP PIN code.

C. PIN Code Substring (PS)

The *PIN code Substring* (PS) asks the user for $p \leq n$ specific digits of his PIN code where n the number of digits composing the original PIN code of the user. The p positions of the digits are randomly drawn for each authentication. For instance in Figure 3, if the user's code is 6789, and the authentication terminal asks for positions 1 and 3 of the PIN code, then the code for this session will be 68.

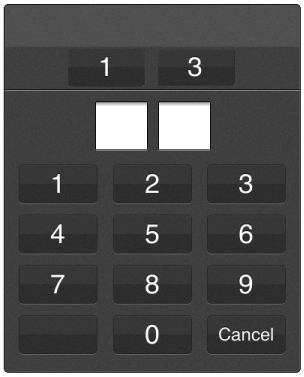

Fig. 3: Example of PS PIN code.

D. PIN Code Modulo a Random Number (PR)

The *PIN code modulo a Random number* (PR) consists in adding randomness to the user's code at each authentication of the user. To do that, this authentication process displays to the user a random number of the same size of the PIN code. Then, the corresponding code is the addition modulo 10 between the digit of the PIN code (only known by the user) and those of the random number displayed on the screen. For example in Figure 4, if the user's PIN code is 1956 and the displayed random number is 3948 then the user needs to enter the code 4894 since $3 + 1 = 4 \bmod 10$, $9 + 9 = 8 \bmod 10$, $4 + 5 = 9 \bmod 10$ and $8 + 6 = 4 \bmod 10$.

E. PIN Code Modulo a Random Number and Even Numbers (PRE)

The *PIN code modulo a Random number and Even numbers* (PRE) looks like PR but considers only the even numbers

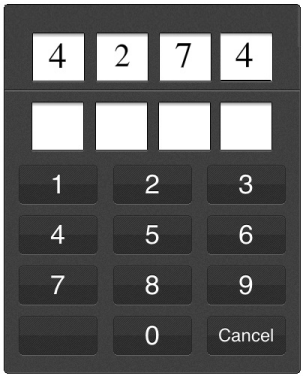

Fig. 4: Example of PR PIN code.

present in the result of the addition modulo 10 between the PIN code of the user and the random number displayed on the screen. For instance as in Figure 5, if the user's PIN code is 1234 and that the random number displayed on the screen is 4274, then after the addition modulo 10, we obtain 5408 since $1 + 4 = 5 \bmod 10$, $2 + 2 = 4 \bmod 10$, $3 + 7 = 0 \bmod 10$, and $4+4 = 8 \bmod 10$. Keeping only the even numbers of the result 5408 in the same order, the resulting code is 408.

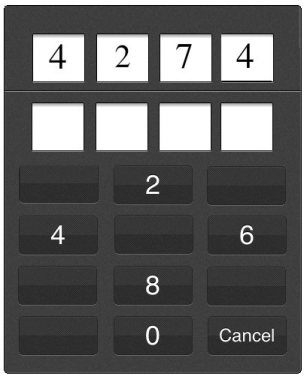

Fig. 5: Example of PRE PIN code.

F. PIN Code Modulo a Random Number and Number of Even Numbers (PRnE)

The *PIN code modulo a Random number and number of Even numbers* (PRnE) looks like (PRE) but instead of constructing the code with the resulting even numbers, the code is the count of even numbers in the addition modulo 10 of the user's PIN code and of the random number displayed on the screen. For example in Figure 6, if user's PIN code is 1234 and that the random number displayed on the screen is 4274, then after the addition modulo 10, we obtain 5408 since $1 + 4 = 5 \bmod 10$, $2 + 2 = 4 \bmod 10$, $3 + 7 = 0 \bmod 10$, and $4 + 4 = 8 \bmod 10$. The code of the user consists in the count the number of even numbers in 5408; hence the code in this example is 3 since 5408 is composed of digits 4, 0 and 8 which are even. Notice that if we consider a PIN code with only 4 digits, the numbers above 4 are useless; 4 corresponds to the case where all digits of the result are even.

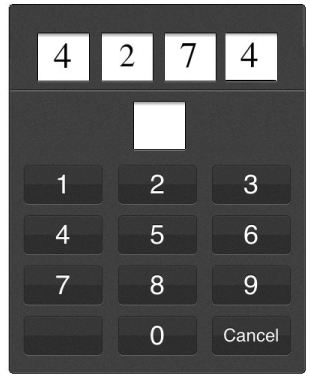

Fig. 6: Example of PRnE PIN code.

III. Threat Models

We present in this section three different threat models where the goal of the adversary is to find the secret PIN code of the user.

A. Bruteforce Attack

The *Bruteforce Attack* (BA) model assumes that an adversary has a physical control of the device, but no other information about the PIN. For instance, the adversary could have confiscated or stolen a smartphone. We stress that in the bruteforce attack, the adversary has no other information, about the PIN code of the user. To find the correct PIN code of the user, the adversary must potentially try all possible combinations.

B. Smudge Attack with Physical Access

The *Smudge Attack with physical access* [3] (SA) model assumes that the adversary, as in the BA, is in possession of the device. But on the contrary to BA, we assume in this threat model that the adversary has auxiliary information on the device's PIN code, like for instance, finger traces, or smudges, on the touch screen surface, or the wear of buttons on the door code. An example of such attack is given in Figure 7. If the numerical pad is deterministic, then the intruder can learn which digits are used in the PIN code of the victim, but there is still the order and or the repetitions of some digits to guess.

C. Observation Attack

The *Observation Attack* (OA) model assumes that the adversary can see the authentication process. For instance, the adversary can look over the shoulders of the victim while she is withdrawing money at the ATM, or looking over the shoulder in the subway while the victim is entering her PIN code on her smartphone, or install a camera that records the authentication process. This attack is also known as "*shoulder surfing attack*" and illustrated in Figure 8.

IV. Security Analysis

We study in this section the security of the six presented authentication methods according to the following three threat models: the Bruteforce Attack, the Smudge Attack with

Fig. 7: Example of a smudge attack.

Fig. 8: Example of a shoulder surfing attack from [23].

Physical Access, and the Observation Attack presented in Section III. We define the security of an authentication method as the number F, where F is the maximal number of codes that an attacker – in the given setting – has to try in the worst case (when only the last PIN he tried is the correct one) to be *sure* to authenticate. For a classical PIN authentication method, this corresponds to the key space, for example for a PIN code composed of four digits, the number F is equal to $10^4 = 10\ 000$. It can also differ from the key space if for example only parts of the PIN are used to authenticate. F depends on the number of digits of the PIN code (denoted by n), on characteristic parameters of the method, and the type of attack.

It is important to note that we assume that the attacker can try to authenticate as often as he wishes, which is usually the case if he is in possession of the device. We do not consider a limitation of the number of guesses, for example the limit of three tries as used for credit cards, which often is an efficient counter measure.

A. Security of PIN Code with a Deterministic Placement (PDP)

a) BA Analysis: The maximal number of codes to be tested depends on the length of the code, i.e. the number of digits composing the PIN code of the user. Assume the code is a digital code of length n, then the number of arrangement with repetitions is naturally $F(n) = 10^n$.

b) SA Analysis: As shown in [20], if a user has withdrawn money at the ATM then an attacker equipped with a thermal camera can retrieve the t digits used for the user's code. The problem of the adversary is then to find the correct order of the digits since the thermal camera gives to the adversary only digits used by the user but does not inform on their order. In other terms, the problem is to find the number of surjective functions from 10 elements (the set of digits) to a set of t elements[1], which corresponds to $S(n,t)$ the Stirling number of second kind [1], [24], [15], where

$$S(n,t) = \sum_{k=0}^{t} (-1)^{t-k} \cdot \binom{k}{t} \cdot k^n \ .$$

We then obtain that $F(n,t) = S(n,t)$.

c) OA Analysis: In the OA model, the adversary can watch the victim when she is authenticating. In the case of the PIN code with deterministic placement, the adversary retrieves directly the secret code of the victim. Hence, $F(n) = 1$.

B. Security of PIN Code with a non Deterministic Placement (PnDP)

a) BA Analysis: As for PDP, the maximal number of codes to be tested depends on the length of the code. Assuming that the code is a digital code of length n, then the number of possible codes is also $F(n) = 10^n$. In the bruteforce model, the randomness does not provide additional security since the space of secret code stays the same.

b) SA Analysis: We still assume that the PIN code is a digit code of length t. In this case, the adversary knows the t buttons that the user has used for the authentication. The number of the combinations of these t touch is given by the Stirling number which is equal to $\sum_{k=0}^{t} (-1)^{t-k} \cdot \binom{t}{k} \cdot k^n$. However, the PnDP authentication consists to place digits in a random order on the screen. Hence, the number of arrangements with repetitions is equals to

$$F(n,t) = \binom{10}{t} \cdot \sum_{k=0}^{t} (-1)^{t-k} \cdot \binom{k}{t} \cdot k^n \ .$$

c) OA Analysis: As for PDP, if an adversary can watch the authentication screen of the victim, the adversary retrieves directly the secret code of the victim, i.e. $F(n) = 1$.

C. Security of PIN Code Substring (PS)

a) BA Analysis: In this situation, the authentication method asks to the user $1 \leq p \leq n$ digits of its PIN code where n is the length of the original secret PIN code of the user. Hence, the number of possibilities for an adversary to find the correct p digits is $F(p) = 10^p$.

[1]https://oeis.org/A019538

b) SA Analysis: Assume that an adversary sees $t \leq p$ smudges of fingers on the screen, where p is the number of positions asked to the user. These residues give information on the p wanted digits. On p positions, we are in the same situation that the SA analysis of the PDP authentication method. Hence, there are $S(p,t)$ possible sequences, and as the indications of p positions are not known, the adversary tests p among n combinations of positions. Finally, the adversary has to test all the arrangements with repetitions for $n-p$ digits on which he has no information. Hence, the number of configurations is:

$$F(n,p,t) = 10^{n-p} \cdot \binom{n}{p} \cdot S(p,t) \ .$$

c) OA Analysis: In the case where the adversary has the total vision, he learns directly the p elements of the PIN code during an authentication of the user. Since the length of the PIN code is n, it remains 10^{n-p} combinations to be tested.

Remark: We can wonder how many times the adversary needs to see a user authenticating on average before knowing the entire PIN code of the user.

To simplify, we first study the case where $p = 1$, then we propose an upper bound. Let T_i be the number of authentications to know i digits from $i-1$ known digits. Then, the required total number of authentications to obtain n known digits is equal to:

$$T = \sum_{i=1}^{n} T_i$$

Assume that the adversary has already obtained $i-1$ different digits and he is watching the user authentication until he obtains a new digit. If the length of the PIN code is n, then the probability for the adversary to know a new digit equals to:

$$P_i = \frac{n-i+1}{n}$$

In this situation, T_i follows a geometrical law of parameter P_i. Hence,

$$\mathbb{E}[T_i] = \frac{n}{n-i+1}$$

Finally, the average total number of authentications for $p = 1$ is

$$\mathbb{E}[T] = \sum_{i=1}^{n} \frac{n}{n-i+1}$$

By generalization and without taking into account the constraint to have two wanted digits at different positions, we obtain for $1 \leq p \leq n$:

$$\mathbb{E}[T] < \frac{n}{p} \cdot \left[\sum_{i=1}^{n} \frac{1}{n-i+1} \right] \ .$$

D. Security of PIN Code Modulo a Random Number (PR)

a) BA Analysis: As for PDP and PnDP, the bruteforce analysis to find the secret code with PR authentication gives a number of arrangements with repetitions equal to $F(n) = 10^n$.

b) SA Analysis: With the added random number to the secret PIN code, the adversary cannot take information from the t buttons used by the user. Hence, the adversary is in the same case that the bruteforce analysis and the number of codes is equal to $F(n) = 10^n$.

c) OA Analysis: In this case, we assume that an adversary sees the random number that the user adds to its PIN code, and the code that the user inputs to the screen. Then, the adversary can compute directly the secret PIN code of the user from these two numbers by subtracting modulo 10 the code given by the user to the random number displayed to the screen $F(n) = 1$.

E. Security of PIN Code Modulo a Random Number and Even Numbers (PRE)

a) BA Analysis: Although there are $\sum_{i=0}^{n} 5^i$ possible entries for a user, it is nevertheless necessary to test $F(n) = 10^n$ PIN codes since the adversary must apply them the PRE method to be sure to be able to authenticate.

b) SA Analysis: As well as for the BA analysis, we have inevitably 10^n tests to be made by the adversary. In fact, the random number used in every authentication prevents from having more information. Thus the authentication requires the explicit search of the PIN code.

Remark: There is a probabilistic method allowing on average to authenticate more quickly than using bruteforce. If we systematically type the same sequence of even numbers, we have a certain probability of succeeding because of the random character of the method. Indeed, if we note k the number of even digits in the result of the addition modulo 10, there is a probability $P(n,k)$ that the result of the addition contains a sequence of k even digits defined at first:

$$P(n,k) = \frac{\binom{n}{k}}{2^n \cdot 5^k}$$

If we study the continuation of Bernoulli experiment of parameter $P(n,k)$, by noting X the random variable representing the average number of necessary tests to succeed by seizing a sequence fixed of k even digits, the expected value of X value is equal to:

$$\mathbb{E}[X] = \frac{2^n \cdot 5^k}{\binom{n}{k}}$$

c) OA Analysis: We estimate here the complexity of the bruteforce knowing that the user entered $p \in [\![1, n-1]\!]$ even digits during the authentication. The fact is that we have no control over the value p. We ignore what are the digits of the random number which gave these p even numbers during their modulo 10 addition with those of the PIN code, we must then test all the combinations of p elements among n and complete with all the arrangements with repetitions of odd digits for $n-p$ unknown digits. Thus, we have a complexity of

$$F(n,p) = \binom{n}{p} \cdot 5^{n-p}$$

We can also propose a probabilistic method that uses the information obtained after each authentication of the user. We can estimate the probability for a number $a \in [\![0, 9]\!]$ to

be at the position $b \in [\![1, n]\!]$ in the PIN code by testing every combination of the input in the PIN code. With the frequency of occurrence of numbers at each position, we can compute how many authentications in average are needed and the maximum frequencies giving the correct PIN code.

F. Security of PIN Code Modulo a Random Number and Number of Even Numbers (PRnE)

a) BA Analysis: In the case of the PRnE authentication method, classic bruteforce in 10^n is not necessary. Indeed only the knowledge of the parities of the digits of the PIN code comes into the play, consequently we can restrict us to all the arrangements with repetitions of 0 and 1. This means counting binary and thus testing $F(n) = 2^n$ sequences.

b) SA Analysis: We have the same situation as for the bruteforce attack, because no information can be learned without the value of the random number. We thus have $F(n) = 2^n$.

c) OA Analysis: Knowing that the user entered a number $p \in [\![1, n]\!]$ during his authentication, which always represents the number of present even digits in the result of the addition modulo 10 of the random number with the PIN code. It means that there are p digits of the random number which are the same parity that those of the PIN code. From the parities of the random number, we can determine the parities of the PIN code by testing all the combinations (of p among n sequences of 0 and 1), which gives a complexity of $F(n, p) = \binom{n}{p}$.

Remark: Again, there is a probabilistic method allowing on average to authenticate more quickly than using bruteforce. If we enter systematically the same sequence of number of even numbers, we have a certain probability to succeed in logging in thanks to the random character of the method. Indeed, if we note k the number of even digits in the result of the addition modulo 10, there is a probability P_k that the result of the addition contains k even digits, i.e.

$$P_k = \frac{\binom{n}{p}}{2^n}$$

If we study the continuation of the experiments of Bernoulli of parameter P_k by noting X the random variable representing the average number of necessary tests to succeed in becoming identified by seizing a number fixes k of even digits, the expected value of X costs then

$$\mathbb{E}[X] = \frac{2^n}{\binom{n}{p}}$$

Hence, in order to minimize $\mathbb{E}[X]$, we observe that k must be close to $n/2$.

G. Summary

In Figure 9, we recall all the results obtained for all our authentication methods. We can see the following:

BA: All the methods have similar results with a maximal security, except PRnE and PS. PRnE has the lowest security and PS has a security that depends on the number of digits that are required for the authentication.

SA: For a fixed value of n, we choose the average security for the methods that depend on multiple variables. Then we obtain the following order:

$$PR = PRE \geq PnDP \geq PS \geq PDP \geq PRnE$$

OA: For this attack, we can easily classify methods by algebraic comparison:

$$PS \geq PRE \geq PRnE \geq PR = PnDP = PDP$$

V. Acceptability of Methods

From a psychological point of view, our authentication methods can be divided into two categories regarding primer and computation. Concerning the primer, we have authentication methods that require a primer – such as the presence of a random number – and the ones that require no primer. Similarly, there are methods that require computation and the ones that do not. These distinctions are important because they are known to have an influence on individual's (participant's) cognitive load. The main structure in humans for processing and storing information, namely working memory, has limited capacity in terms of processing speed and the amount of information that can be stored [4]. According to the model devised by Cowan [7], only few elements can be processed and held in memory at once. Therefore the two following categories were introduced:

- Authentication methods requiring neither addition nor primer: PDP, PnDP and PS.
- Authentication methods requiring addition and a primer: PR, PRE and PRnE.

Two studies aimed to evaluate *a priori* the acceptability of our different authentication methods, for instance during the unlocking of a smartphone. The first was an exploratory and a qualitative study including 8 participants. The second was a quantitative study including 88 participants.

A. Exploratory Study

On the one hand, the first experiment aimed to assess the influence of the random placement of digits on the screen. On the other hand, it aimed to collect data concerning the usability of authentication mechanisms.

In this exploratory study, participants were presented with the five authentication methods as an authentication mechanism for unlocking a smartphone. After having tested the different authentications methods, the participants evaluated all methods based on several criteria such as *a priori* representation, feeling of safety/security, usability, and were asked to choose their preferred method.

More precisely, in this experiment eight participants evaluated all five authentication methods. Four participants were female and four were male. These eight participants are between 24 and 45 years old. Four participants have evaluated these methods with a traditional touch screen on which digits were displayed in numerical order while the other 4 participants evaluated the methods with a random touch screen on which numbers were displayed in a random order.

Methods \ Intruder	BA	SA	OA
PDP	10^n	$S(n,t)$	1
PnDP	10^n	$\binom{10}{t} \cdot S(n,t)$	1
PS	10^p	$10^{n-p} \cdot \binom{n}{p} \cdot S(p,t)$	10^{n-p}
PR	10^n	10^n	1
PRE	10^n	10^n	$\binom{n}{p} 5^{n-p}$
PRnE	2^n	2^n	$\binom{n}{p}$

Fig. 9: Summary of security analysis for each method, where we use the following notations: BA for Bruteforce Attack, SA for Smudge Attack, OA for Observation Attack, PDP for PIN code with a Deterministic Placement, PnDP for PIN Code with a *non* Deterministic Placement, PS for PIN code Substring, PRE for PIN Code Modulo a Random Number and Even Numbers, PRnE for PIN Code Modulo a Random Number and Number of Even Numbers.

For each authentication method, the following points were assessed:

- Attitudes, *a priori* representations
  - Preliminary knowledge and use of PIN codes, feeling of invulnerability, usability, awareness of the need to protect personal data, etc.
    - Do you lock your phone?
    - Which authentication method do you use to unlock it?
    - How would you benefit from switching authentication methods?
- Perception of the authentication methods
  - Order them:
    - According to order of preference.
    - According to safety level.
  - Debriefing.
    - Why these choices?
    - What do you think of this particular authentication method?
- Conclusion questions
  - Frequency of use.
  - Knowledge of new technologies.

B. Results of the Exploratory Study

a) Influence of the digit order of display: The use of traditional touch screen or random touch screen had no influence on the participants' answers. This account seems satisfactory as according to Nielsen's work on usability [22], 75% of problems can be detected between 3 and 5 subjects. Henceforth, in the quantitative study, only the traditional touch screen was used for all authentication methods, and PnDP was not considered.

b) Attitudes and a priori Representations: We analyzed the results as follows:

- For some people, locking is not usual as the following comment shows: "*I do not want to use any authentication method, I have too much to codes to remember and moreover, my phone was never stolen*".

TABLE I: Preference orders.

Meth. \ Ord.	1	2	3	4	5
PDP	4	2	0	0	2
PS	3	3	1	1	0
PR	1	1	3	0	3
PRE	0	1	1	5	1
PRnE	0	1	3	2	2

- Moreover, participants may have a feeling of control: "*I do not need an authentication method, I pay attention*".
- When the lock option is set up, securing data seems unnecessary due to the frequent number of calls.
- Locking the phone is not always perceived as a secure solution "*I slide my finger on the screen, I do not see the use of the PIN code*".
- Nevertheless, some users express more concerns: "*I want to block the access for my child and to my colleagues*" or "*I want to lock my phone today because the confidentiality and the sensitivity of transported data have increased*".
- And users are at least aware of advanced methods of authentication: "*I use fingerprint and the PIN code, there could be retinal check, smart cards, etc.*" or "*I lock my phone with four digits but there is also the fingerprint and voice recognition*".
- Finally, we would like to stress that the "*mathematical*" authentication methods are not mentioned except for the fact that PIN codes sometimes use 8 digits instead of 4.

c) Perception of Authentication Methods: Table I introduces participants' preferences of the authentication methods. Table II introduces the rankings of feeling of security and Table III introduces rankings of usability. For each table, the values displayed in cells correspond to the number of participants who chose a particular order and method. Hence, each column displays a total of 8 (as for 8 participants). Each participant had to rank the 5 methods on a scale from 1 to 5 (1 being the least preferred method and 5 most preferred one).

We remark:

- The security perception is inversely proportional to the ease of handling for the presented method.

TABLE II: Security feeling order.

Meth. \ Ord.	1	2	3	4	5
PDP	4	1	1	0	1
PS	0	4	1	1	1
PR	0	0	4	2	1
PRE	0	1	0	3	4
PRnE	3	1	1	1	1

TABLE III: Ease of handling order.

Meth. \ Ord.	1	2	3	4	5
PDP	5	0	1	0	1
PS	0	4	1	1	1
PR	0	1	5	1	0
PRE	0	1	0	3	3
PRnE	2	1	0	2	2

- The preference of the different authentication methods seems to be more linked to the ease of handling rather than to the safety of the solutions as it has been shown in the previous section.

These results also show that:

1) participants perceive different levels of security generated by the different proposed authentication methods;
2) but the overall preferences for a given authentication methods are less influenced by the perceived security of data than by the ease with which a particular method is handled.

We expose below participant's comments for each method according to this first experiment, where participants are represented by their number to respect their anonymity.

PDP. The traditional method, not necessary secure but the most simple in the cognitive sense.

#1: "*It is the method that I usually use.*"
#3: "*Easy to use.*"
#4: "*Basic, easy to hack.*"
#5: "*Technically outdated.*"
#6 and #7: "*I do not particularly care, but compared to other methods, it is the fastest / the one that require the least efforts.*"

PS. The ideal trade-off.

#2: "*One my favorites in terms of security.*"
#3: "*Simple.*"
#4: "*Remains simple but is still more secure.*"
#6: "*There is not addition and the random feature is nice.*"
#7: "*New, simple and fast.*"

PR and PRE.

Problems of learning, memorizing, and efficiency.

#1: "*It is a difficult method to use, loss of time, and too much thinking.*"
#2: "*It is expensive, and we can easily block the phone in case of emergency due to the number of trials.*"
#3: "*Great chance to find by chance by anyone.*"
#4: "*Anxiety, there are people who are going to have trouble.*"
#6: "*Complicated to do all these calculations, in addition with possibility to be wrong.*"
#7: "*Playable, but for the random code, it would be necessary to put small numbers, not to exceed the tens.*"

PRnE. Feeling of security.

#3: "*Great chance to find by chance by anyone.*"
#5: "*Too complicated while the chance to find the solution is* 66%."

Based on the data from these 8 participants, the PS and PRE solutions appear as the best ones in terms of security. However, although these two solutions are considered secure, they are not deemed user friendly and are perceived as too complex to implement.

C. Quantitative Study

Eighty-eight participants responded to a questionnaire containing different theoretical items (intentions of use, attitudes, perceived control, etc.) for authentication methods PS ($n = 31$), PR ($n = 27$), and PRE ($n = 30$). These authentication methods were chosen based on the results of the qualitative study above, and following the theoretical concepts borrowed from the theory of planned behavior (TPB) [2] and the technology acceptance model (TAM) [9].

According to TPB, the intention of adopting or not adopting a given behavior is the result of three determinants: 1) behavioral beliefs, which may be defined as a general feeling (favorable or unfavorable) towards behavior; 2) normative beliefs, which correspond to an individuals perception of the normative expectation of others and the motivation to comply with it; and 3) control beliefs, which refer to an individuals perception of any constraints (internal or external) on performing behavior.

With TAM, intention is determined by: 1) perceived ease of use, in other words "the degree to which the user expects the target system to be free of efforts" in using the technology [9, p. 985]; and 2) the users perception of usefulness, in other words his or her "subjective probability that using a specific application system will increase his or her job performance" [9, p. 985].

Among the most salient results, we can observe that:

- Participants consider themselves to be the most in control, i.e. they perceive the most ease of use, when using the authentication method PS ($\bar{x} = 3.6$ out of 5) compared to the authentication methods PR and PRE ($\bar{x} = 2.9$ out of 5 and 2.5 out of 5, respectively), where $F = 7.94, p = 0.001$. We recall that F is the F-statistic and p is the probability of obtaining the same (or even more extreme) value of the test if the null hypothesis were true.
- Participants consider that even other users will be more likely to use the authentication method PS, i.e., feel more comfortable using it even for "social" reasons ($\bar{x} = 3.45$ out of 5, and 2.82 out of 5 and 2.48 out of 5 for

authentication methods PR and PRE, respectively), where $F = 6.81, p < 0.01$.

- And finally, in line with the qualitative study (see above), the perceived risks for authentication method PS (M = 3.13 out of 5 points maximum) are higher than the perceived risks for solutions PR and PRE ($\bar{x} = 2.63$ and 2.50 out of 5, respectively), where $F = 3.80, p < 0.05$.

In line with the qualitative study, it is observed that solution PS seems to be the most accessible to the participants, with a perceived level of security lower than for solutions PR and PRE. The quantitative study did not reveal more intentions for the use of solution PS ($\bar{x} = 2.68$ out of 5 maximum) compare with solutions PR and PRE ($\bar{x} = 2.33$ and 2.11, respectively).

At first glance, data concerning intentions of use seem to confirm the hypothesis of a better acceptability of the PS solution as compared to the other solutions

This would also be consistent with the diffusion theory of innovation [25], according to which the norm of "continuity" determines the acceptability of novelty; and the latter is certainly more important for the solution PS (close to the 4-digit codes, solution PDP) than for the solutions PR and PRE (or even PRnE).

D. Summary

Using Figure 9 and Table I, we graphically represent the different authentication methods with respect to two parameters: the participant's preference and the security.

Figure 12 shows the user's preference and the security for each proposed authentication method. The horizontal axis represents the participant's preference and the vertical axis represents the security of the method in the Bruteforce Attack (OA) model. The more a method is on the right side of the graphical representation, the more the method is prefered by participants. In the same way, the more a method is on the top of the graphical representation, the more the method is secure in the OA model.

Figure 11 shows the user's preference and the security for each proposed authentication method in the Smudge Attack with Physical Access (SA) model.

Figure 12 shows the user's preference and the security for each proposed authentication method in the Observation Attack at Distance (OA)model. Hence, in the OA model, the best authentication method is PS. In fact, it is the best solution in the participant's preference point of view and also the best solution in the security point of view.

VI. Conclusion

We have shown that different authentication methods are available for modern devices that are more and more used in the company of the future. We analyzed the security of these methods against different types of attacks:

- Bruteforce Attacks,
- Smudge Attacks,
- Observation Attacks.

Some of these methods are very simple to use and are widely accepted by the public as for example the traditional PIN

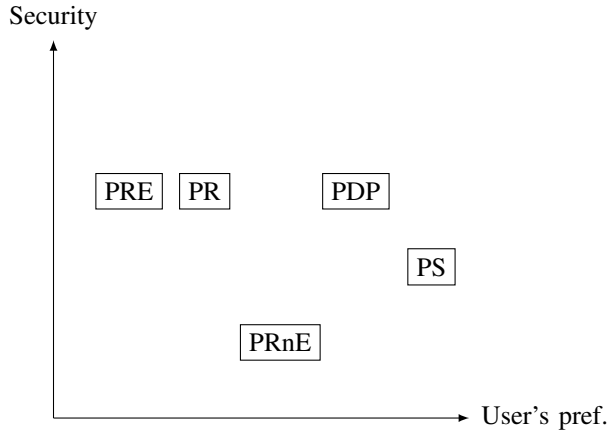

Fig. 10: User's preference vs Security in the Bruteforce Attack (BA) model.

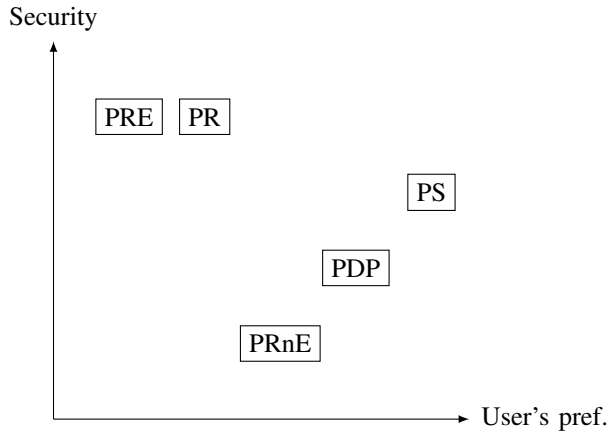

Fig. 11: User's preference vs Security in the Smudge Attack with Physical Access (SA) model.

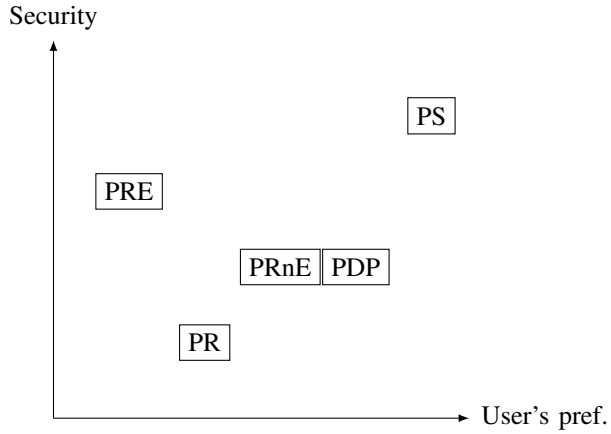

Fig. 12: User's preference vs Security in the Observation Attack at Distance (OA) model.

code with four digits. However, the security of such methods is questionable. Indeed, it is fairly easy for someone to see the PIN code being entered and to later steal and use the credit card. Therefore, innovative authentication methods such as randomized PIN codes and modulo PIN codes offer a better level of security. Indeed, even if someone sees the PIN code being entered they will not be able to reproduce the code and use the stolen credit card for their own benefit. The acceptable trade off seems to be PS method, which consists to ask only a subset of the digit of the PIN code. This method is already used in practice, for example by some banks to authenticate their users online. However, the present study has shown that such an authentication method is still generally perceived as difficult to implement. That is why, future research needs to be done to explore the possibility of a secure authentication method that is much more user friendly, and to compare the acceptability of biometrics authentications to the PIN codes.

Acknowledgments

This research was conducted with the support of the FEDER program of 2014-2020, the region council of Auvergne-Rhône-Alpes, the Indo-French Centre for the Promotion of Advanced Research (IFCPAR) and the Center Franco-Indien Pour La Promotion De La Recherche Avancée (CEFIPRA) through the project DST/CNRS 2015-03 under DST-INRIA-CNRS Targeted Programme.

References

[1] M. Abramowitz and I. Stegun. *Stirling Numbers of the Second Kind. In Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. Dover Publications, 1972.

[2] I. Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179 – 211, 1991. Theories of Cognitive Self-Regulation.

[3] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In *4th USENIX Workshop on Offensive Technologies, WOOT '10, Washington, D.C., USA, August 9, 2010*, 2010.

[4] A. Baddeley. Working memory: theories, models, and controversies. *Annual Review of Psychology*, 63:1–29, 2012.

[5] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon. The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction*, TEI '11, pages 197–200, New York, NY, USA, 2011. ACM.

[6] R. Biddle, S. Chiasson, and P. C. van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, 2012.

[7] N. Cowan. The magical mystery four how is working memory capacity limited, and why? *Current Directions in Psychological Science*, 19:51–57, 2010.

[8] D. Davis, F. Monrose, and M. K. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA*, pages 151–164, 2004.

[9] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.*, 13(3):319–340, Sept. 1989.

[10] R. Dhamija and A. Perrig. Deja vu-a user study: Using images for authentication. In *9th USENIX Security Symposium, Denver, Colorado, USA, August 14-17, 2000*, 2000.

[11] L. N. Evangelin and A. L. Fred. Biometric authentication of physical characteristics recognition using artificial neural network with PSO algorithm. *IJCAT*, 56(3):219–229, 2017.

[12] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig. Use your illusion: Secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, pages 35–45, New York, NY, USA, 2008. ACM.

[13] S. Higashikawa, T. Kosugi, S. Kitajima, and M. Mambo. Shoulder-surfing resistant authentication using pass pattern of pattern lock. *IEICE Transactions*, 101-D(1):45–52, 2018.

[14] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

[15] D. E. Knuth. Two notes on notation. *The American Mathematical Monthly*, 99(5):403–422, 1992.

[16] T. Kwon and S. Na. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42:137–150, 2014.

[17] M. Lee. Security notions and advanced method for human shoulder-surfing resistant pin-entry. *IEEE Trans. Information Forensics and Security*, 9(4):695–708, 2014.

[18] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin. A survey on behavioral biometric authentication on smartphones. *J. Inf. Sec. Appl.*, 37:28–37, 2017.

[19] N. Malkin, M. Harbach, A. De Luca, and S. Egelman. The anatomy of smartphone unlocking: Why and how android users around the world lock their phones. *GetMobile: Mobile Comp. and Comm.*, 20(3):42–46, Jan. 2017.

[20] K. Mowery, S. Meiklejohn, and S. Savage. Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. In D. Brumley and M. Zalewski, editors, *5th USENIX Workshop on Offensive Technologies, WOOT'11, August 8, 2011, San Francisco, CA, USA, Proceedings*, pages 46–53. USENIX Association, 2011.

[21] S. J. Murdoch, S. Drimer, R. J. Anderson, and M. Bond. Chip and PIN is broken. In *31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA*, pages 433–446. IEEE Computer Society, 2010.

[22] Nielsen. *Usability Engineering*. Academic Press, Boston, USA, 1993.

[23] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon. Illusionpin: Shoulder-surfing resistant authentication using hybrid images. *IEEE Transactions on Information Forensics and Security*, 12(12):2875–2889, Dec 2017.

[24] J. Riordan. *Combinatorial Identities*. Wiley, 1979.

[25] M. Rogers Everett. Diffusion of innovations. *New York*, 12, 1995.

[26] 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 2004, Washington, DC, USA, October 25-29, 2004*, pages 236–245, 2004.

[27] 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, pages 11:1–11:14, New York, NY, USA, 2013. ACM.

[28] P. Shi, B. Zhu, and A. Youssef. A pin entry scheme resistant to recording-based shoulder-surfing. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pages 237–241, June 2009.

[29] Z. Sun, Y. Wang, G. Qu, and Z. Zhou. A 3-d hand gesture signature based biometric authentication system for smartphones. *Security and Communication Networks*, 9(11):1359–1373, 2016.

[30] E. von Zezschwitz, A. D. Luca, B. Brunkow, and H. Hussmann. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI 2015, Seoul, Republic of Korea, April 18-23, 2015*, pages 1403–1406, 2015.

[31] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces, AVI 2006, Venezia, Italy, May 23-26, 2006*, pages 177–184, 2006.