Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Dynamic array PIN:A novel approach to secure NFC electronic payment between ATM and smartphone

Samir Chabbi, Rachid Boudour, Fouzi Semchedine & Djalel Chefrour

To cite this article: Samir Chabbi, Rachid Boudour, Fouzi Semchedine & Djalel Chefrour (2020) Dynamic array PIN:A novel approach to secure NFC electronic payment between ATM and smartphone, Information Security Journal: A Global Perspective, 29:6, 327-340, DOI: 10.1080/19393555.2020.1773583

To link to this article: https://doi.org/10.1080/19393555.2020.1773583

Published online: 04 Jun 2020.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2020, VOL. 29, NO. 6, 327–340
https://doi.org/10.1080/19393555.2020.1773583

Dynamic array PIN:A novel approach to secure NFC electronic payment between ATM and smartphone

Samir Chabbi[a], Rachid Boudour[a], Fouzi Semchedine[b], and Djalel Chefrour[c]

[a]Department of Computer Science, Badji Mokhtar University, Annaba, Algeria; [b]Institute of Optics and Precision Mechanic, University of Setif1, Setif, Algeria; [c]Department of Math and Computer Science, University of Souk Ahras, Souk Ahras, Algeria

ABSTRACT

Near Field Communication (NFC) technology has been used recently for electronic payment between an Automated Teller Machine (ATM) and a Smartphone. It is threatened by several attacks that can steal the user personal data like the password or the Personal Identification Number (PIN). In this paper, we present Dynamic Array PIN (DAP), a novel approach for user authentication on a Smartphone that uses NFC electronic payment with an ATM. Our analysis and experimentation prove that this technique protects against thirteen different attacks and is cost-effective in terms of required hardware, authentication time, computing power and storage space.

KEYWORDS

Authentication; automated Teller Machine; confidentiality; electronic payment; NFC; smartphone; secure element

1. Introduction

Near Field Communication (NFC) is a wireless communication technology that enables transactions and messages transfer between two devices at a short distance (Badra & Badra, 2016). It operates at a frequency of 13.56 MHz (Luo et al., 2016). In NFC, the two communicating devices use an electromagnetic induction field to transfer information (Dennis et al., 2018).The NFC is now used in many products to perform proximity payments such as Point of sale (U.S. Payments Forum, 2018), and Automated Teller Machine (Gyamfi et al., 2016). Customers can use NFC bank cards for that purpose. Recently, more customers are using their NFC Smartphone for electronic NFC payments(Merkus, 2018).In recent years, the banking system has replaced bank cards with mobile payment via NFC to secure payment (Wadii et al., 2017).Unfortunately, an attacker can steal banking information stored in a NFC bank card (El Madhoun & Pujolle, 2016).Further, this solution is not effective for any type of attacks as the cloning attack that can be performed on the NFC device(Solat, 2017).Obviously, there are other types of attacks which can steal the PIN code or the password in a Smartphone or an ATM such as: shoulder-surfing(Khan et al., 2018), brute force (Zaidi et al., 2016), side channel(Guerar, 2017), screen recording (Guerar, 2017), Replay(Zaidi et al., 2016), Spyware(Guerar, 2017), camera recording (Shubhra, 2017), smudge(Zaidi et al., 2016), Smartphone or card theft(Shubhra, 2017) and multiple registration (Guerar, 2017).

Customers are involved to secure their Smartphone by a PIN or a pattern lock (Romo, 2014). In the electronic payment with an ATM, the password or the PIN are subject to several attacks (Varalakshmi, 2015).The Card fraud has caused losses estimated at £ 566.0 million in 2017, which represents a decrease of 8% over 2016 (UK Finance, 2018). This shows that attacks on payment remain active.

ATMs can be threatened by physical attacks, logical attacks or frauds (Positive technologies, 2018).

The authentication became today an essential measure to ensure the entity identity that has the access authorization to a system. Recently, several authentication techniques are used such as a Personal Identification Code (PIN), a password, or a biometric feature such as a fingerprint introduced through a reader or the user face introduced through a camera. However, an authentication technique must ensure three main factors: the security, the friendliness of the authentication

CONTACT Fouzi Semchedine fouzi.semcheddine@univ-setif.dz Institute of Optics and Precision Mechanic, Setif, University of Setif1, Setif, Algeria

method and the ease of memorizing the authentication method (Guerar, 2017).

The costs of biometric methods outweighed the benefits in most cases compared to the passwords or PINs (Promontory an IBM Company, 2017). Also, unlike a password or a PIN, if a biometric characteristic is stolen, the user can not change it at the difference of the password or the PIN. In an NFC Smartphone, the technique of password or PIN can be stored in a hardware circuit called Secure Element(SE).The SE is a circuit implemented in the Smartphone which ensures the security of the storage and the execution of sensitive data and programs (e.g. payment application)(GSMA, 2018). Several solutions of user authentication are proposed to secure the electronic payment using ATM, some are based on password or PIN technique, and other are based on biometric technology (Smart payment association, 2018). However, each solution has its limits and inconvenient.

In this paper, we propose a novel approach in order to secure the electronic NFC payment between a Smartphone and an ATM. The proposed authentication technique of password, called, Dynamic Array PIN (DAP), which is carried on the ATM screen, verifies the factors mentioned above and guarantees the protection of the user password. Our authentication process protects the payment from thirteen different of attacks. It is characterized by its intuitiveness, resilience, user-friendliness and time reduction. It presents an average authentication time of 5.20 sec. It does not use any complex hardware devices. It does not require the Quick Response (QR) code, numeric keypad or visual keyboard, it only uses two arrays displayed on the screen of the ATM, and so it uses the less degree of difficulties concerning the users of old age. A comparison with some recent well-known solutions is conducted to evaluate the performance and the effectiveness of our solution.

The rest of the paper is organized as follows: in Section 2, we review the related works. In Section 3, we describe our system and proposed protocol. In Section 4, we perform a security analysis of our system to prove its ability to deal with some well-known attacks. In section 5, we present the results of our experiment and evaluation. Section 6 provides a comparison of security and performance between the proposed method and some well-known recent techniques, and finally, we conclude this work in Section 7.

2. Related works

Recently works have been proposed to secure the user password or PIN code and securing the NFC payment. We present in this section the most important recent methods and their limitations.

2.1. FakePIN technique

In this scheme, the password consists of a sequence of alphanumeric characters and a direction. At each authentication session, the order of appearance of the characters or the numbers is changed on a displayed keyboard. To deceive the observer, the user must type a character provided by the combination of this character with the direction of the password to give the exact character of the password. This must be done for all the characters of the password (Kim et al., 2014).

The FakePIN technique proposed to ensure the user authentication by password is vulnerable against recording attack (Guerar, 2017).

2.2. PassWindow method

This method is based on the use of a grid of icons. One icon must be preselected and considered as a password. The position of this icon must be memorized by the user. To ensure the authentication operation, a virtual keyboard with a grid without icons is displayed on the screen. To enter the PIN numbers, the user must enter each digit in the location of the password icon while moving the device and must hide the input by isolating the camera back (Yi et al., 2014).

The PassWindow technique proposed to authenticate the user with a password is weak against the intersection of multiple records (Guerar, 2017).

2.3. Cappcha (Capp) method

This technique provides authentication by entering a PIN code with the operation of tilting the device to a degree displayed on the screen for one second. This degree of inclination can be generated by an

accelerometer integrated into the secure element of the Smartphone (Guerar et al., 2015).

This technique suffers from the Shoulder-surfing attack and a concealed camera that can be hidden on an ATM to record the typed PIN or password. In the case of Smartphone theft, the attacker who steals the PIN code can carry out the payment operation because the Cappcha technique integrated in the secure element displays a random degree of inclination of the Smartphone that it will be simply followed and hence, the restored PIN code will be entered.

2.4. BrightPass technique

In this technique, the SE generates a sequence of 0 and 1 called Lie Overhead. From this sequence, a series of circles of different brightness will be displayed on the Smartphone screen in the area reserved for entering the PIN code. A low-brightness circle (corresponding to the value 0) tells the user to type a random digit that is not a part of the PIN code, while the high-brightness circle (corresponding to the value 1) indicates to the user to type a real number that is a part of the PIN code. This technique is used for fighting the spyware attack that tries to find the PIN code typed by the techniques of screen capture or recording (Guerar et al., 2016).

The BrightPass technique also suffers from the Shoulder-surfing attack and the concealed camera attack.The illustration of a BrightPass authentication session (Guerar, 2017) is a great proof of the possibility of returning the PIN code by an attacker using one of the two attacks.

2.5. Color wheel PIN method (CWPIN)

In this method, the server shares with the user a secret composed of the PIN code and an array of ten colors which is stored in the secure element of the Smartphone. When matching the Smartphone to the ATM, the latter displays a colored wheel divided into 10 portions numbered from 0 to 9, a QR code and a seek bar to rotate the wheel. The user scans the QR code by his Smartphone to receive the color array with a random arrangement of color indices. To authenticate, the user must drag the seek bar to rotate the color wheel so that the color that corresponds to the first digit of the PIN code in the color array on the Smartphone corresponds to the second digit of the PIN code on the wheel of color. After the user raises his seek bar finger, the wheel rotates randomly. Then, the user slides the seek bar so that the color that corresponds to the third digit of the PIN code in the color array on the Smartphone matches the fourth digit of the PIN on the color wheel and so on until the end of the process (Guerar, 2017).The disadvantage of this method compared to ours is that it uses a QR code that must be scanned by the Smartphone. On the other hand, the memorization of the correspondence between the digit and the color seems difficult especially for the older users and especially, when the PIN code exceeds four digits.

2.6. Secure credit card protocol

In (Jensen et al., 2016), the authors proposed a secured credit card protocol (SCCP). It is an authenticate proxied credit card protocol based on pre-computed hashes, indexing and Xor operation. We find in this solution that the protocol is vulnerable against the theft or the loss of the credit card because the owner of the credit card is not authenticated with a Personal Identifier Number (PIN). In the case where a password is used with the protocol, the solution can be vulnerable against recording camera, Spyware, shoulder-surfing and brute force attacks.

2.7. Nana et al.'s solution

In (Gyamfi et al., 2016), the authors propose an authentication scheme based on an embedded fingerprint biometric for the Automated Teller Machine. We find this solution vulnerable against the attack that uses a default reader to acquire the fingerprint of the user. Even, if the solution also uses a password or a PIN, the attacker can first steal it by Shoulder-Surfing attack or recording camera attack. Then, he can steal the fingerprint by a default reader and by this way; he can perform an electronic payment.

2.8. Payment tokenization

In a credit card payment transaction, a token created with an account number associated to the real account number, is transferred by the issuer.

This token does not constitute the real account number to provide a high level of security for the payment transaction.

If an attacker recovers fraudulently the token, the real account number cannot be generated (Gaddam et al., 2018).

3. Dynamic array PIN

To deal with all the attacks mentioned above, we proposed Dynamic Array PIN: a new method used to improve the authentication mechanism on ATMs, to reinforce the NFC payment security system with the ATM and to facilitate PIN code manipulation especially for older users. Our solution represents a novel approach used for introducing the code PIN in order to authenticate the user before effecting an NFC payment with an ATM using a Smartphone. This technique is used in the following hardware system.

3.1. The hardware system

Our system requires the presence of the following entities: The user, its Smartphone, the bank server and an Automated Teller Machine (ATM) equipped with a small touch pad that has a cover shell (Figure 1). This commodity device is very cheap compared to the cost of the whole ATM, and has a cost smaller than the one of a touch screen.

3.1.1. User

He represents the owner of a Smartphone equipped with the NFC technology and embeds a credit card. To authenticate with the ATM, it must have a PIN code. In our experiment, we propose a PIN code of four digits which is a very common PIN length. Of course, longer PINs can be used in our solution, e.g. 6 or 8 digits, but long PINs constitute a burden for the user as the input phase will be longer.

Figure 1. NFC payment hardware System.

3.1.2. Smartphone

The proposed Smartphone has a non-centric SIM architecture. The Secure Element is implemented with a form of a movable secure support that has a type of memory card (Secure Memory Card: SMC) (Alcime et al., 2013) (Figure 2). The Smartphone is equipped with NFC and is characterized by a movable Secure Element that stores the protocol, the PIN code and the NFC applications (e.g. Payment application), etc.

The use of a non-centric SIM architecture where the Secure Element is a secure memory card (SMC) has the following advantages:

- It offers a high level of security;
- It is conforming with EMV, GlobalPlatform, ISO/IEC 7816 and javacard;
- It has an important capacity of memory;
- It is movable since it can be placed with its contents (NFC applications, protocol, secret keys, PIN code, etc.) in a new Smartphone.

3.1.3. Automated teller machine (ATM)

It has an NFC reader capable to read a credit card embedded in a Smartphone. It communicates with the NFC Smartphone and the bank server. It is equipped with a small touch pad that has a cover shell

3.1.4. Server

It stores in its database the identification information such as the PIN code, the identifier of the Secure Element integrated on the Smartphone, the telephone number and the identifier of the credit

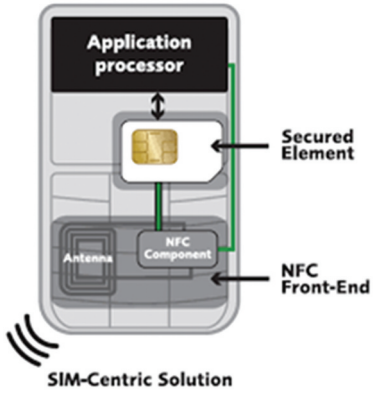

Figure 2. NFC mobile with SMC architecture.

card containing the user affiliation like the bank name, the user account number, its amount, etc. The information is saved during the registration phase by the TSM (Trusted Service Manager).It is updated in the case when the owner changes his Smartphone, or changes his PIN. The storage of the information in the database and the communication of the server with the ATM are considered secure.

After bringing the Smartphone closer to the ATM, an exchange of secure data stored in the Secure Element and the credit card will be performed (Figure 3). The server finally passes to authenticate the user (the owner of the Smartphone) by inviting him to enter the PIN code. In our approach, the ATM displays two arrays of 10 digits each, displayed in a random order (Figure 4).

3.1.5. Objects

The ATM communicates with the Smartphone by a radio frequency communication (NFC) and by an online communication with the Server. The last communication is considered secure (by the use of the TLS protocol). Our goal is to secure the user's intervention with the ATM. The security of the information stored in the server and the information exchanged between the ATM and the server is not addressed in this work and is considered secure. Our principal goal is to ensure the user authentication with a novel approach of PIN code. After authenticating the user, the method provides the payment transactions. To ensure the payment processing system, our method prohibits the payment execution when a PIN is not verified (the case of attack).In the opposite case, the payment processing system is authorized. So, only when the user is authenticated, it is authorized to complete the NFC payment with the ATM. To prove the security, usability and performance of our method, we pursued the following objectives:

Figure 3. Data NFC transmission.

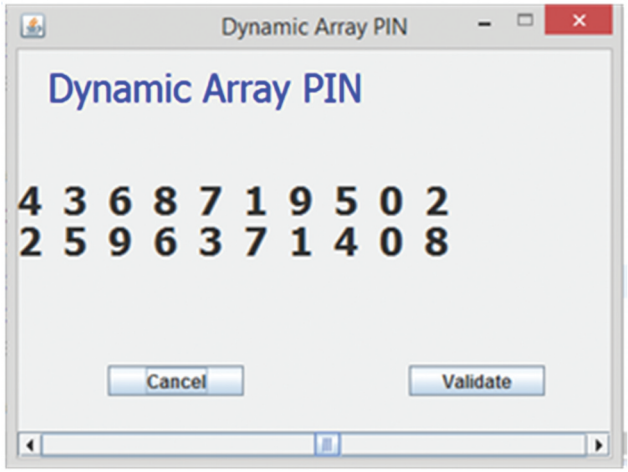

Figure 4. User authentication using DAP.

- Study the resistance of our solution and prove that it is simple and yet protects against the following attacks: Cloning, shoulder-surfing, brute force, side channel, screen recording, replay, Spyware, camera recording, smudge, Smartphone theft, multiple registration, recording camera after theft of Smartphone and Shoulder-surfing after theft of Smartphone.
- Calculate the average time of user authentication time through experimentation and prove that it is efficient.
- Compare our method with several important techniques.

3.2. DAP protocol presentation

In this section, we present our protocol named Dynamic Array PIN (DAP) where the goal is to reinforce the security of entering the PIN code on the ATM. This protocol uses only the PIN code as a shared secret between the user and the banking server. When the user brings his Smartphone closer to the NFC reader of the ATM, the latter displays two arrays, each array contains 10 random digits numbered from 0 to 9. The user can drag the digits in the second array to the digits in the first array.

Our protocol is used to perform an electronic payment with the ATM using a Smartphone. It is characterized by a short authentication time, a small error rate and by protection the NFC payment against thirteen attacks. Our solution allows the user to select a credit card from a list of cards embedded in the Smartphone. The main phases of the solution are as follows:

3.2.1. Registration phase

At the data base of the bank server, the following information is saved:

- The PIN code of the user;
- The Id: the UUID (Universally Unique Identifier) used to identify the Secure Element;
- The phone number;
- The Bank card identifier: it references the name bank, the user affiliation, the user account number, its amount, its transactions' histories, etc.

3.2.2. Authentication phase

The user applies the following steps:

- Memorize the number in the second array that corresponds to the first digit of the PIN code in the first array (see Figure 5). The position of this number in the first array is called the reference.
- For instance, as shown in Figure 5, to introduce the PIN '8642 , the user looks for its first digit 8 in the upper array and finds the digit below it in the lower array. This is digit 4 in this example. Then, he looks for the position of 4 in the first array (which is the third one from the left) and considers it the reference for this time. Then using a small touch pad installed on the ATM and covered with a shell to hide the user's finger, the user slides the second array horizontally to the left or to the right and stops it by releasing his finger each time a PIN digit in the second array matches the reference in the first one. The X-axis scroll bar in Figure 5 is used in our desktop implementation to simulate the ATM touch pad. To indicate the end of entering the PIN, the user presses the 'Validate' button.

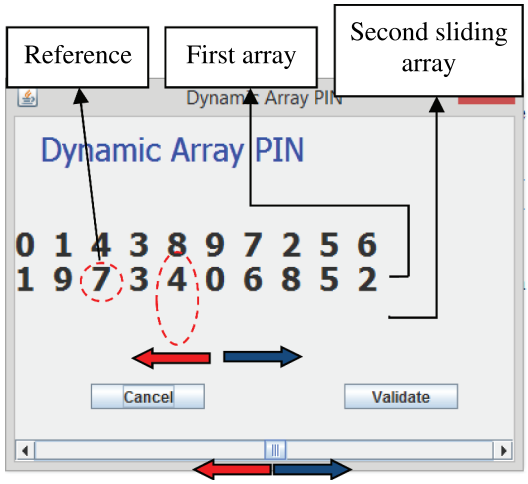

Figure 5. The DAP protocol interface.

The basic idea of this protocol is that the attacker can see the user's input, but he cannot reveal the PIN as he cannot detect the digit that represents the reference referred by the user to enter the digits of the PIN code. This reference which is changeable at each authentication session is obtained from the first digit of the PIN code which is unknown for the attacker.

3.2.3. SMS confirmation phase

When the PIN entry was successful, thepayment transaction is executed. The server sends to the Smartphone a SMS confirmation (considered secure by TLS) indicating the details of the transaction (the user account number, the removed amount, the sold, the date and the time of the transaction, etc.). This message can be used as an intrusion test.

3.3. The DAP protocol steps

As shown in the diagram of Figure 6, the steps of our protocol are:

- The user brings his Smartphone closer to the NFC reader of the ATM;
- The ATM retrieves the information stored in the bank card on the Smartphone and transmits it to the bank server. This transmission is encrypted using AES encryption algorithm because it is better in confidentiality and integrity factors than the other algorithms like DES, 3DES, AES or BLOWFISH (Wahid et al., 2018).

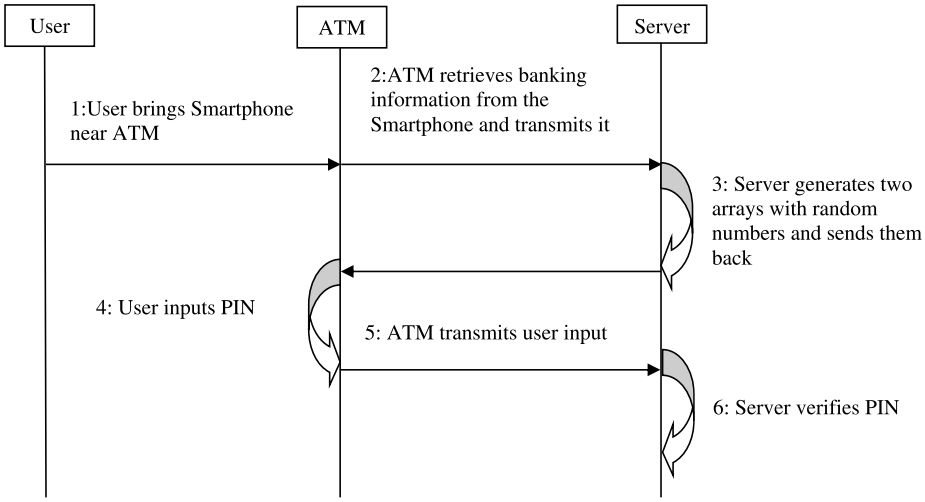

Figure 6. The DAP Protocol.

Concerning the security of the account number (not the PIN), the tokenization process can be used in conjunction with our proposal which is limited to a proven safe technique against multiple attacks, used to enter a PIN code through an ATM. This security is provided at the ATM level. Regarding the secure transfer of the banking information recorded on credit card embedded in the Smartphone (like primary account number), they are transmitted before introducing the PIN with our technique, the primary account number can be transferred from Smartphone to the ATM after applying the tokenization process.

- The server retrieves the user PIN code from its database, generates two arrays of random indices from 0 to 9 and transmits them to the ATM;
- The ATM displays on the screen the two arrays with 'Cancel' and 'Validate' buttons. The second array can be moved by the user to the right or to the left using a touch pad;
- To authenticate, the user must slide the second array and release the finger each time a digit of the PIN code in the second array coincides with the reference number in the first array. Finally, he presses the 'Validate' button to indicate the end of the PIN code input;
- When the 'Validate' button is pressed, the ATM sends the user's input to the server;
- The server compares the entered PIN to the one retrieved from the database.

4. Security analysis

In this section, we analyzed the security of our protocol against thirteen attacks. This analysis shows that our protocol is resilient to the following attacks:

4.1. Brute force attack

The principle of this attack is to try all the possible character combinations until the PIN code is found. In the proposed technique, the randomization of the numbers in the two arrays generated by the server for each authentication session leads the user to release his finger at different times where new values that represent new authentication tests are generated at every attempt of payment. To find the PIN code, there is a probability of 1 in 10 power N*2 (N = number of digits in PIN) since the arrays contain 10 digits each one, which implies that the probability of finding the real PIN is too low. For such attack and by using the DAP technique, it is difficult to iterate through the entire PIN code space. In addition, the ATM may block the payment process after three unsuccessful attempts.

If the attacker applies a shoulder-surfing attack, it is practically impossible to see when the user releases his finger which is hidden by the cover shell and it is also impossible to memorize the screen images corresponding to the digits of the PIN code.

In the case of a screen recording attack by camera, the attacker can't detect the true PIN code for two reasons: the first is that the user can exceed one digit of the password and in this case, he must stop without releasing his finger and scroll in the opposite direction to reach his digit. The second is that the user can do this on purpose (that is slide pass the right digit or slide left and right without releasing his finger) to farther confuse the attacker. For more security, we can add a light source above the ATM to diffuse light in all the directions in front of the cameras which can be installed around the ATM. This light can be an obstacle for the readability of the image recorded by the camera or by an attacker.

4.2. Side channel attack

This type of attack uses spyware that tries to capture the user's keystrokes by using several types of resources such as the accelerometer, the microphone, the camera, etc.

The proposed solution is robust against this type of attack by randomizing the numbers that fill the two arrays generated by the server at each authentication session. Moreover, by releasing his finger under the cover shell, the user gives no opportunity to the attacker to know the digits of the PIN code because the Spyware cannot guess the reference number generated from the first digit of the PIN code and which is known to the user only.

4.3. Cloning attack

In this type of attack, the attacker can install at the ATM, devices that record the user's private data stored in the bank card embedded in the Smartphone, and then clone the stolen information on a new bank card embedded in another Smartphone to use it for an NFC payment. In our system, the cloning attack has no effect because our protocol requires the introduction of the PIN code to perform the payment transaction and the cloning attack does not allow restoring the PIN code which is stored so safe in the Secure Element instead of the bank card.

4.4. Screen recording attack

This type of attack is provided by malware that can be installed on the ATM and allows the recording of the entire screen during the authentication session. With our protocol, this attack does not give any result relative to the digit of the PIN code. In fact, at every moment, the screenshot shows only two arrays containing numbers and this image does not give any information on the PIN code number which has been selected by the user only by moving the slide bar.

4.5. Replay attack

This attack assumes that the mobile phone is authenticated with the NFC reader (the ATM in our study) by sending a secret identifier. So, the attacker listens indiscreetly the communication between the phone and the reader, receives the identifier, and returns or replays this identifier from its own phone in another authentication session (Merkus, 2018). Due to the randomization of the two arrays generated by the server, our protocol is resistant against this type of attack since at each authentication session, the reference number in the first array will be changed and the user will memorize a new reference to validate the digits of the PIN code.

4.6. Camera recording attack

The attacker can install a camera on the ATM to record the entry of the PIN. With our protocol, the ATM screen recording by a camera cannot give any information about the digits of the PIN code because the camera can only record two arrays displayed on the ATM screen and a slide bar moving on the left or on the right. The camera recording does not give any information about the digit of the PIN code. Our protocol is therefore secure against this type of attack.

4.7. Shoulder-surfing attack

In this attack, the attacker positions himself behind the user to see and memorize the keystrokes of the user when entering the PIN code. With our solution, an attacker who visualizes

a user entering his PIN cannot have any idea about the numbers of the PIN code as in the case of the camera, because our user does not introduce direct numbers. We can conclude that our protocol is resistant against shoulder-surfing attack.

4.8. Smudge attack

The principle of this attack is to follow the tracks of the fingers of the user left on the screen of the ATM to be able to detect the authentication scheme. Our protocol is protected against this type of attack because there is no drawn authentication scheme and the user does not touch the ATM screen, he only slides his finger on the small touch pad, releases it in the necessary time and finally he presses the 'Validate' button, so he does not give any information on the PIN code.

4.9. Spyware attack

Spyware is a malicious code that captures the coordinates of the user touches on the device (the ATM in our study) screen, or to save the total screen of authentication. By using our protocol, the user does not fear if the spyware captures its coordinates which concern the sliding of the second array and the pressing of the button 'Validate' because through this operation, the spyware can never detect the PIN code digits. The result is the same if the spyware saves the entire authentication screen.

4.10. Multiple registration attack

The attacker can use the intersection of multiple recordings of data, screen, or camera to discover the PIN. However, our protocol is protected against this type of attack because the fact of acquiring several recordings doesn't give any information on the digits of the PIN code because the user makes only two gestures resumed by sliding the second array and pressing the 'Validate' button. On the other hand, the numbers in both arrays change randomly also the reference number at each authentication session, and hence, the multiple recording attacks will have no effect.

4.11. Theft of smartphone attack

Using our technique DAP, the theft of the Smartphone never allows the thief to make an NFC payment with the ATM because DAP requires the introduction of the PIN that is unknown by the attacker and there is no way to know it since it is saved with security in the server database and in the Secure Element of the Smartphone. So, our approach is protected against theft attack of the Smartphone.

4.12. Shoulder-surfing with theft of smartphone attack

If the attacker performs a Shoulder-Surfing attack in first, and later steals the Smartphone, he cannot make payment that requires knowledge of the PIN. Knowing that the Shoulder-Surfing attack does not allow him to know the password by using the proposed protocol, the theft of the Smartphone will have no effect.

4.13. Recording with camera with theft of smartphone attack

If the attacker uses a camera recording and eventually, steals the Smartphone, he cannot make payment that requires knowledge of the PIN code. The camera recording in our case does not allow the attacker to know the PIN code.

5. Experimentation & evaluation

In this section, we evaluate the usability and the memorability because they represent the evaluation factors of any authentication method.

To review the results of our DAP protocol; we designed an application to be installed on the ATM. The development tools were: Eclipse Neon.2 Release (4.6.2) and Java 1.8.0. The development equipment is a Toshiba Core i5 computer that simulates the ATM.

We choose 30 peoples of different ages from 15 years old to 72 years old to test our method. The ages range under 60 years is representative of most of the people who use Smartphone and ATMs in our society. After explaining the principle of the method to participants, everyone must

test the application alone several times to become familiar with it. Then, each participant made nine authentication attempts following the procedure detailed in section III.B, using our Java application on the same computer mentioned above. This means that our experimental results are obtained from 30 * 9 = 270 authentication sessions for each PIN (4, 6 and 8 digits). The authentication time of each session is calculated from the moment when the user starts to move his finger on the touch pad of the ATM for sliding the bar used to move digits of the second table till the moment when he presses the 'Validate' button.

The results obtained from the experiences and represented in Table 1 shows that the average authentication time is equal to 5.20, and the error rate is equal to 4.07%, which means that our protocol is characterized by a fast authentication time and a low error rate.

Table 1. Authentication time of DAP protocol.

	Average authentication time [second]			Error rate PIN (digits)		
Age	PIN 4 digits	PIN 6 digits	PIN 8 digits	4	6	8
19	3.12	6.70	8.92	0/9	0/9	1/9
19	2.40	7.11	8.96	0/9	1/9	0/9
50	5,71	11.36	14.34	1/9	1/9	2/9
20	3.53	7.81	10.26	0/9	0/9	1/9
19	3.76	8.33	11.67	0/9	0/9	0/9
49	5,09	10.14	13.80	1/9	1/9	2/9
20	4.05	6.35	7.77	0/9	0/9	0/9
15	3.19	7.34	10.31	0/9	0/9	1/9
19	4.16	7.22	12.11	0/9	0/9	0/9
38	4.29	8.79	14.18	1/9	1/9	1/9
15	4.35	8.76	11.24	0/9	0/9	0/9
35	4.37	10.78	13.11	0/9	0/9	1/9
25	4.41	7.20	9.26	0/9	1/9	0/9
20	4.52	8.58	12.70	0/9	0/9	0/9
31	4.92	10.59	14.77	0/9	1/9	2/9
28	3.84	8.46	11.75	0/9	0/9	1/9
33	5.15	12.34	15.42	1/9	1/9	1/9
18	3.00	6.37	10.90	0/9	0/9	0/9
47	5.22	11.58	14.91	1/9	0/9	1/9
34	5.22	10.58	13.34	0/9	0/9	0/9
20	3.41	6.33	7.86	0/9	0/9	0/9
32	4.29	8.62	12.25	1/9	0/9	1/9
20	2.31	8.27	10.45	0/9	0/9	0/9
17	3.29	7.06	12.32	0/9	0/9	0/9
41	5.56	9.12	13.86	1/9	1/9	2/9
44	5.87	12.98	15.79	0/9	0/9	0/9
16	7.24	10.48	13.78	0/9	0/9	1/9
15	9.25	11.03	12.58	0/9	1/9	1/9
48	7.72	14.60	19.80	1/9	2/9	2/9
72	21.17	25.67	38.34	3/9	4/9	5/9
Average						
29	5.20	9.69	13.23	4.07	5.56	9.63

6. Security & performance comparison

We can compare our technique with several important methods by performing two types of comparison: security and performance comparison.

6.1. Security comparison

In this section, we compare our solution with several important existing ones. We are checking the attacks which could compromise the methods or the protocols. The results are obtained by the analysis of the attack toward the method or the protocol.

Table 2 below presents the comparison results where 'V' means that the technique is vulnerable to the attack and 'R' is resistant.

Table 2. Security limits of methods.

Attack/Method	FakeP	PassW	Capp	Bpass	DAP
Theft of card or Smartphone	R	R	R	R	R
Shoulder-surfing	R	R	/	/	R
Multiple record	V	V	R	R	R
Auxiliary canal	R	R	R	R	R
Brute force	V	V	R	R	R
Spyware	R	R	R	R	R
Screen record	R	R	R	R	R
Card cloning	R	R	R	R	R
Camera recording	R	R	/	/	R
Smudge	R	R	R	R	R
Replay	R	R	R	R	R
Camera recording with theft of Smartphone	R	R	V	V	R
Shoulder-surfing with theft of Smartphone	R	R	V	V	R

The FakePIN and PassWindow methods use simple passwords despite their resistance against the Shoulder-Surfing attack and the concealed camera attack. To protect these methods against the brute force attack, they must either use long or complicated passwords that require a large number of possible combinations, or they must use in addition to the password, values of motion stored using a secure manner in the SE.

The BrightPass and Cappcha methods are vulnerable to the Shoulder-Surfing or the concealed camera attack with theft of Smartphone attack because an attacker or a camera can use a direct observation by watching or filming the direct entry of the PIN code. In the BrightPass technique, an attacker who knows the operating principle, records in his memory the numbers entered in

the circles having a high luminosity. If thereafter the attacker can steal or borrow the Smartphone, it can carry out a payment transaction with the ATM following the indications of the Secure Element.

According to Table 2, we can calculate for each method, the number of attacks. The results are mentioned in Table 3.We can see from the table that our solution is the safer because it prevents all the listed attacks.

We can present now the security strong points of our solution which are proved:

- The type of the used Secure Element offers a high level of security.
- In the worst case, if a new further attack is discovered and breaks our protocol, a confirmation SMS is sent to the Smartphone of the owner. The SMS represents an alarm message since it informs the user that his account sold is changed. This means that the protocol uses an intrusion detection technique.
- The protocol does not use any biometric method. Thus, the user biometric features are not exposed to the related attacks.

We present in Table 4 the authentication times of the methods FakeP, PassW, Capp, Bpass and CWPIN, as obtained by (Guerar, 2017), and our protocol (DAP) obtained by experimentation, as mentioned earlier. Although, the authentication time of CWPIN is less than DAP, we can say that the estimated authentication time for our protocol is the best. In fact, CWPIN did not consider the older persons (the maximum of age was 58). However, DAP took into account the older persons with age equal to 72. This could influences different metrics such as the authentication time and the error rate.

Table 5 gives a comparison between DAP and CWPIN, which is the most secure and recent among all the mentioned solutions. CWPIN error rate is obtained by (Guerar, 2017). The analysis shows that DAP is more economic.

Table 6 shows the difficulty that the older users can find during the authentication operation with an ATM using one of the five methods (FakePIN, Passwindow, Cappcha, BrightPass and CWPIN) and our solution. We assume each difficulty has a score of one point.

6.2. Performance comparison

The object of this comparison is to show that the proposed solution is economic in terms of hardware and authentication time and, it is efficient.

The time measurements obtained with 6 and 8 digits PIN code are slightly higher than the times required for the users to enter 4 digits PIN codes. The time duration of our method is linearly scalable with the number of digits in the PIN code. The other proposals like (Guerar, 2017) have only considered 4 digits PINs.

The Figure 7 presents a result of an authentication session using DAP protocol

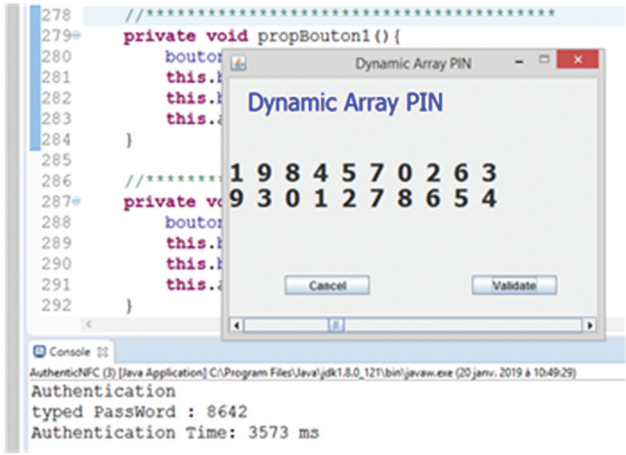

Figure 7. Authentication session with DAP protocol.

Table 3. Number of attacks comparison.

Method	Number of attacks
FakeP	2
PassW	2
Capp	2
Bpass	2
DAP	0

Table 4. Authentication time comparison.

Method	Authentication time (s)
FakeP	10.90
PassW	18.12
Capp	4.12
Bpass	8.20
CWPIN	4.55
DAP	5.20

Table 5. DAP vs. CWPIN.

CWPIN	DAP
Uses QR code	Does not use QR code
Time for scanning QR code	No time for scanning QR code
Storage PIN & color array in Secure Element	Only storage of PIN in the Secure Element
Two applications: One on the Smartphone and another on the ATM	Only one application installed on the ATM
Not usable for PIN codes that contain an odd number of digits	Usable in the case of the even or odd number of digits that make up the PIN code.
The end of entering the PIN code is not indicated	The end of entering the PIN code is indicated by pressing the 'Validate' button

The results shown in Table 6 indicate that the proposed method DAP presents fewer difficulties for older users.

Table 7 shows a comparison between DAP and the Secure Credit Card Protocol (SCCP), with important characteristics in favor of our proposal.

The comparison of our solution to the Nana et al.'s solution one, shown in Table 8, indicates that our solution is safer and economic.

7. Conclusion

In this paper, we have proposed a novel technique of user authentication for securing NFC payment in a system consisting of: a server, an ATM and an NFC Smartphone. This technique is a novel secure method for introducing a PIN code. This method represents a protocol that enables or disables the NFC payment. We have evaluated the proposed protocol by analysis and we have proved that it is efficient. We have proposed an intrusion test in order to indicate to the user that his account sold is changed after each transaction. Further, we have compared our solution with several important existing security protocols and methods. We have proved that it is the best one and it is resistant against thirteen attacks. Also, we have proved that it is not expensive because it did not require complex hardware devices.

Further, the proposed solution presents the following interesting features:

- The use of Smartphone that replaces the bank card or the credit card which can be selected by the user.

Table 6. Degree of difficulties comparison.

Method	Difficulties	Degree of difficulties
FakeP	-Memorize two passwords: one is alphanumeric and the other is a direction. -Virtual keyboard that can be modified with each authentication attempt. -The letter to press is the combination of the letter of the password and the direction.	4
PassW	-Memorize two passwords: PIN code and a preselected icon. -Memorize the location of the preselected icon in an editable grid for each authentication operation and containing other random icons. -Display a virtual keyboard and a grid without icons. - Incline the phone to move the grid on the virtual keyboard to enter the PIN digit in the location of the preselected icon. -Hide the lens of the camera.	6
Capp	-Store the PIN code. -Incline the mobile phone to a specific degree displayed on the screen and hold it in such position for one second to have access to the PIN code.	2
Bpass	-Store the PIN code. -Display a set of small circles that take the positions of the password numbers. In a circle of low light, the user enters a false number. In high brightness, he enters a real number.	2
CWPIN	-Store the PIN code. - Scan the QR code - Display a Color wheel and slip a seek bar following the principle already stated	3
DAP	- Store the PIN code. - Display two arrays and the user slides the second array to correspond a digit of the PIN code existing in the second array with the reference digit existing in the first array	2

Table 7. DAP vs SCCP.

SCCP	DAP
Uses only credit card	Uses Smartphone. User can select a credit card from a list
Vulnerable to the theft of the credit card	Resistant to the theft of the Smartphone
No PIN code	Use of PIN code
No confirmation message after payment	Confirmation message after payment indicates transaction details and can be used as an intrusion test
No Secure Element	Use of Secure Element

Table 8. DAP vs Nana et al's solution.

Attack/Solution	Nana et al.'s solution	DAP
Default fingerprint reader	V	R
Camera recording (if password or PIN code is used)	V	R
Shoulder-Surfing (if password or PIN code is used)	V	R

- The type of the used Secure Element is conforming with EMV, Globalplatfrom and Javacard. It has an important capacity of memory and it is movable. So, it could be placed with its NFC applications and its PIN code in a new Smartphone.
- The proposal is economic in terms of hardware resources as it requires only the addition of commodity component which is small touch pad with its cover shell.

As future works, we would consider securing the information flows between the components of Smartphone namely he host controller, the NFC controller and the Secure Element by creating security tunnels

References

Alcime, M., Ghartouchent, M., & Rached, N. (2013). NFC technology: Study report. U N I V E R S I T E P A R I S - E S T M A R N E - L A - V A L L E E

Badra, M., & Badra, R. B. (2016). A lightweight security protocol for NFC-based mobile payments. *Procedia Computer Science*, *83*, 705–711. https://doi.org/10.1016/j.procs.2016.04.156

Dennis, G., Kevin, L., Michael, S., Tahin, S., & Linda, Z. (2018). Security analysis of near-field communication (NFC) payments. *Courses.csail.mit.edu*.

El Madhoun, N., & Pujolle, G. (2016, August). Security enhancements in EMV protocol for NFC mobile payment. *2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin,* (pp. 1889–1895). doi: 10.1109/TrustCom.2016.0289.

Gaddam, A., Aissi, S., & Nagasundaram, S. (2018). U.S. Patent No. 9,978,094. Washington, DC: U.S. Patent and Trademark Office.

GSMA. (2018, May). NFC Functions and Security Certification overview.

Guerar, M. (2017). *Security problems in embedded systems* (Doctoral dissertation). University of Oran.

Guerar, M., Migliardi, M., Merlo, A., Benmohammed, M., & Messabih, B. (2015, July). A completely automatic public physical test to tell computers and humans apart: A way to enhance authentication schemes in mobile devices. In *2015 International Conference on High Performance Computing & Simulation (HPCS)* , Amsterdam, Netherlands, (pp. 203–210). IEEE.

Guerar, M., Migliardi, M., Merlo, A., Benmohammed, M., Palmieri, F., & Castiglione, A. (2016). Using screen brightness to improve security in mobile social network access. *IEEE Transactions on Dependable and Secure Computing*, *15*(4), 621–632. doi: 10.1109/TDSC.2016.2601603

Gyamfi, N. K., Mohammed, M. A., Nuamah-Gyambra, K., Katsriku, F., & Abdulah, J. D. (2016). Enhancing the security features of automated teller machines (ATMs): A Ghanaian perspective. *International Journal of Applied Science and Technology*, *6* (1).

Jensen, O., Gouda, M., & Qiu, L. (2016, January). A secure credit card protocol over NFC. In *Proceedings of the 17th International Conference on Distributed Computing and Networking* , Singapore Singapore, (p. 32). ACM.

Khan, H., Hengartner, U., & Vogel, D. (2018, April). Evaluating attack and defense strategies for Smartphone pin shoulder surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montréal, QC, Canada, (p. 164). ACM.

Kim, S., Yi, H., & Yi, J. H. (2014). FakePIN: Dummy key based mobile user authentication scheme. In *Ubiquitous information technologies and applications* (pp. 157–164). Springer.

Luo, X., Woznowski, P., Burrows, A., Haghighi, M., & Craddock, I. (2016, May). Splash: Smart- phone logging app for sustaining hydration enabled by NFC. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA,* (pp. 1526–1532). ACM.

Merkus, J. (2018). *Security evaluation of the NFC contactless payment protocol using model based testing.* (Master's thesis, Open University of Nederland).

Positive technologies. (2018). Attacks against ATMs using Greendispenser: Organization and techniques.

Promontory an IBM Company. (2017 November). Biometric authentication in payments: Considerations for policymakers.

Romo, J. T. (2014). *Towards seamless and secure mobile authentication*. Arizona State University.

Shubhra, J. (2017, October). ATM frauds: Detection & prevention. *International Journal of Advances in Electronics and Computer Science*, *4*(10).

Smart payment association. (2018 May). Biometrics in payment: Breaking down barriers with high value payments.

Solat, S. (2017). Security of electronic payment systems: A comprehensive survey. *arXiv preprint arXiv:1701.04556*.

U.S. Payments Forum. (2018, January). Mobile and digital wallets: U.S. Landscape and strategic considerations for merchants and financial institutions.

UK Finance. (2018 March). Annual fraud update: Payment cards, remote banking, check and authorized push payment scams.

Varalakshmi, V. (2015). A Survey on secure PIN authentication for ATM transactions. *International Journal of Advanced Research in Science, Engineering and Technology*, *II*(10), 951–954.

Wadii, E. L., Boutahar, J., & Ghazi, S. E. (2017). NFC technology for contactless payment echosystems. *International Journal Of Advanced Computer Science And Applications*, *8* (5), 391–397. doi: 10.14569/IJACSA.2017.080548

Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. (2018). A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish for guessing attacks prevention. *Journal Computer Science Applications and Information Technology*, *3* (2), 1–7. doi: 10.15226/2474-9257/3/2/00132

Yi, H., Piao, Y., & Yi, J. H. (2014). Touch logger resistant mobile authentication scheme using multimodal sensors. In *Advances in computer science and its applications* (pp. 19–26). Springer.

Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone device. *IJACSA) International Journal of Advanced Computer Science and Applications*, *7* (4), 206–219. doi: 10.14569/IJACSA.2016.070426