Preliminary Investigation of Mobile Banking Attacks in West Africa: Feedback from Orange Money Customers in Burkina Faso

Arthur D. Sawadogo[1(✉)], Zakaria Sawadogo[2], Steve T. M. Ataky[3], Khalid M. Askia[1], Kalmogo Roland[4], and Issa Boussim[5]

[1] Université du Quebec à Montréal, Montreal, Canada
sawadogo.delwende_donald_arthur@courrier.uqam.ca
[2] Université Gaston Berger, Saint-Louis, Senegal
[3] Ecole des Technologies Supérieures, Montreal, Canada
[4] Université Laval, Quebec City, Canada
[5] Université de Ouagadougou, Ouagadougou, Burkina Faso

Abstract. Mobile banking is used to perform balance checks, account transactions, payments, credit applications, and other banking transactions via a mobile device. Until recently, mobile banking was most often done via SMS or the mobile web. In west African countries, these applications are preferred before all others of the same kind due to their proximity and ease of use. However, in recent years, several end-users have fallen victim of attacks aiming at misappropriating their money. In this scenario of attacks, the end-user is the most affected. Unfortunately, there is a crucial lack of information regarding the tricks used by attackers on them, users, not allowing the victims to protect themselves. In this paper, we propose a comprehensive study on Orange Money attacks in the Burkina Faso context. We analyze the different Facebook forums to identify recurring attack methods from the user's point of view. In the end, we propose the bests practices that users should follow.

Keywords: Security · Mobile banking · Mobile money · User experiences · Attacks · Survey

1 Introduction

Mobile banking is the technology that enables customers to access banking and financial services through the mobile smart phones. Owing to the increasing use of smart phones over the past few years, banks and financial institutions have set up mobile banking systems to allow customers to withdraw, transfer and deposit money, making banking transactions more convenient and easier to access.

Mobile money transactions have exploded around the world in 2020, especially in sub-Saharan Africa. According to the GSMA State of the Industry on

Y. H. Sheikh et al. (Eds.): AFRICOMM 2021, LNICST 443, pp. 15–24, 2022.
https://doi.org/10.1007/978-3-031-06374-9_2

Mobile Money 2021 report [1], "Sub-Saharan Africa has been at the forefront of the mobile money industry for over a decade." It continued to account for the bulk of growth in 2020 with 43% of all new accounts. Registered mobile money accounts in Africa grew 12%, that is, to 562 million in 2020, while monthly active accounts were 161 million, an increase of 18%, according to the report. Total transactions reached $ 27.5 billion (up 15%) for a value of $ 495 billion (up 23%). It has 171 active mobile money services. According to the same report [1], West Africa accounts for the year 2020, over 198 million mobile money accounts to create an 18% increase, with 43 million active accounts, or 23% more than in 2019. This part of Africa has a transaction target of 6.4 billion for 495 billion dollars, an increase of 23% compared to 2019.

While mobile banking can offer benefits, it also comes with risks. In fact, the fairly large volume of money passing through mobile money have also contributed to the development of a form of attack with harmful consequences on the population. Indeed, mobile banking services involving several risks include the anarchist, social engineering, attacks, fraud, theft of financial information, etc. Our thesis is supported by Mountain et al. [2] who stated that the massive adoption of mobile banking services makes applications and users particularly attractive targets for cybercriminals. And that 60% of mobile malware specifically targets financial data stored on mobile devices.

Orange Money is by far the most famous mobile banking application in Burkina Faso, nevertheless, in recent years customers have been victims of numerous attacks aimed at misappropriating money. In most cases, these attacks have been successful and are increasingly scaring users. In the literature, there are several works on mobile banking in general, however, less work on attacks linked to mobile banking or mobile money. In this paper, we conduct an in-depth study of Orange Money attacks with a focus on the user's point of view. This paper is structured as follows: In Sect. 2, we discuss the security attacks on Orange Money users and the methods used. We outline security best practices in Sect. 3. We review the literature in Sect. 4. Finally, we discuss validity threats in Sect. 5.

2 Security Attacks

As motivation of this work, we did a survey on the social network Facebook. Facebook is the most used social network in Burkina Faso. It holds about 100% of mobile connections in Burkina (every single person who has a mobile connection has a Facebook account whether it is active or not), in other words, 7.8% of the Burkina Faso population has a Facebook account [3]. We start by parsing forums to extract relevant information and attacks victims. Then, we built an anonymous survey share in these forums firstly and identified victims.

2.1 Preliminary Study

We needed to have a template that can yield to capture the most relevant information about attacks performed (Fig. 2). We consider features such as the outcome (finality) of the attack, the mobile-type of the victim (terminal). This

```
Anonymous author
June 10, 10:19 AM -
Victim of a theft!
I went to make a withdrawal of 35,000f tonight, when I got there I wrote my number on the piece of paper
on the piece of paper as usual to give to the
to give to the manager for the withdrawal or was
6:33 pm at the same time, that is to say 6:35 pm, I received a
receive a code message where I should
validated by #120* secret code# to make the withdrawal
the withdrawal that is what is normal I did I wait for the money! The lady tells me that she
to validate I show her the message
she tells me that it is not on her number that
I validated! She shows me these transaction numbers it's not the same number!!!
Strange thing!
I look in the phone my messages
I see that at 18:36 the message from the lady
had come telling me to validate for the withdrawal!
But I had already validated!
There was a young man who wanted to do an operator
but finally he left without doing anything! So they stole 30.000f from me!
My question is the customer who came in
behind me who saw my number written on the piece of paper
on the piece of paper and at the same time launched
the manager to make the withdrawal?
Or was it the manager who told me off?
So just tell you to be very careful
when you write your number on the paper
for your withdrawals.
```

Fig. 1. Example of post in the Facebook forum "Ils m'ont arnaqué" ("They ripped me off") Translated by us.

parameter allows to reduce the scope of analysis in order to find flaws in the applications. Indeed, if the victim's application is a smart phone, then the idea of piggybacked apk, backdoor or spy application on the phone could be interesting to investigate. On the other hand, if the victim's cell phones are simple phones, then the security of GSM applications could also be considered for example. Whatever the type of phone used, social engineering attacks can also be performed. In addition, we check whether the attack was carried out remotely or in the presence of the victim (proximity) and how much money was targeted by the attack. We parsed 100 posts on 3 different forums and got the information about attacks. We analyze these information and extract relevant and recurrent information about attacks methods. We explore also Deogirikar et al. [4] work that offer a study on security attacks. They identified different methods used to perform a security attack on mobile device. Based on this previous work and considering the information extracted in this preliminary study, we can propose a summary (Fig. 2) of the different possible attacks on Orange Money applications. We assume that this list is not exhaustive, but we have retained the most relevant ones from the user's experiences. To more assess our process, we build a template (Fig. 3) in order to catch relevant information on each post manually parsed. The main information that we consider are:

- Finality: It is a boolean that takes true if the attack is successful and false if it is not.
- Method: We identify these techniques by analyzing the messages, and by reading the public reports issued by the police.

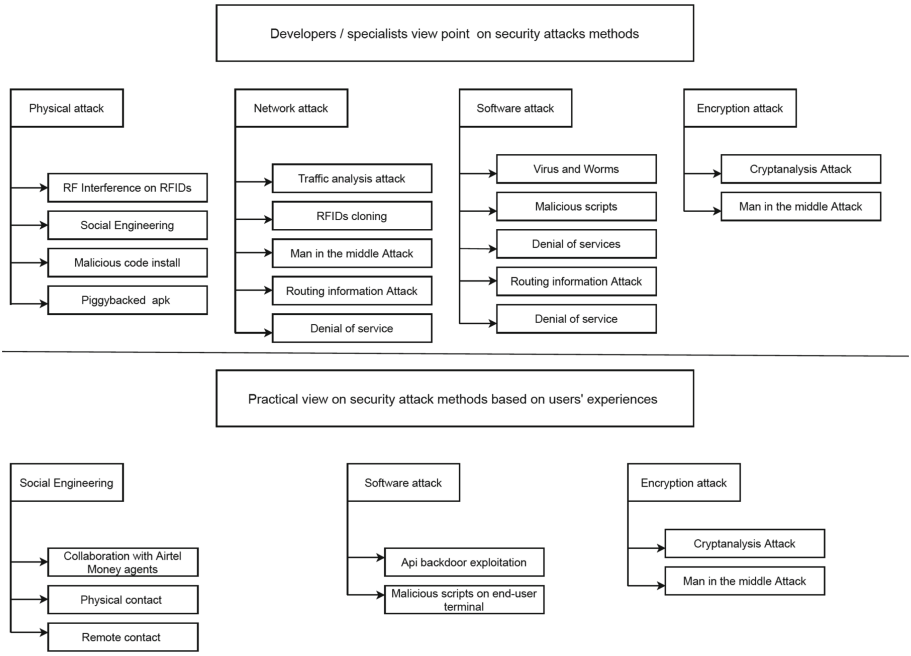

Fig. 2. Security attacks methods

– Proximity is the characteristic that checks in the item whether the attack was performed with a physical contact of the victim or not. We consider two proximity values. True if the criminal was around the victim during the attack and false if it was an online or remote attack.
– Terminal: we check the type of the victim terminal, We consider two main types of terminal: smartphone/IPhone and simple phone.
– Amount: captures the amount stolen and allows the financial impact of these attacks to be noted (Table 1).

Table 1. Template for information extraction in posts

Features	Possible values
Finality	True or false
Method	Social enginering, apk flagged back door, agents collaboration, etc.
Proximity	True or false
Terminal	Smartphone/Iphone or Simple phone
Amount	Value in fcfa of the amount stole

2.2 Online Survey

The purpose of the interview in this paper was to get feedback from possible victims and from all those who has had an experience. We therefore used the template to create the questions anonymously. 13 people responded to the form and the results can be found in the Table 2. The results obtained shows us the importance of making users aware of the risks linked to the use of mobile banking applications and to protect themselves (Table 3).

Table 2. Statistics on the collected datasets

Question tags	Question content
Q1	Have you ever suffered an Orange Money attack in order to steal your money?(Avez vous déjà subi une attaque Orange Money dans le but de voler votre argent?)
Q2	Was the attack successful? (L'attaque à t'elle aboutie?)
Q3	Were you using a smart phone at the time of the attack? (Utilisiez-vous un téléphone intelligent au moment de l'attaque ?)
Q4	Were you in the presence of a stranger during the attack? (Etiez vous en presence d'un inconnu lors de l'attaque ?)
Q5	Did you receive a call or text message before the scam? (Avez vous reçu un appel ou un message text avant l'arnaque)
Q6	What was the amount involved? (Quel était le montant concerné?)

Table 3. Survey results

Questions	1	2	3	4	5	6	7	8	9	10	11	12	13	Total
Q1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	- 13 Yes/O No
Q2	Yes	No	Yes	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	8 Yes/5 No
Q3	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	11 Yes/2No
Q4	No	No	No	No	No	No	No	No	No	No	No	No	No	0 Yes/13 No
Q5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	13 Yes/0 No
Q6	30k	100k	200k	130k	25k	50k	100k	15k	50k	35k	150k	225k	90k	1,2 M

2.3 Discussions

In this section we discuss our preliminary study and investigation. Firstly, we summarize the different methods used by the attackers from the users' point of view and then we discuss the users' feedback on the use of the Orange Money application.

Security Attacks Methods. As Fig. 2 shows, we have three main categories of security attacks on Orange money application based on user return of experience.

Social Engineering. The first category is the most famous and the most critical of all. It concerns social engineering attacks. Social engineering refers to a variety of malicious activities achieved through human interaction. Psychological manipulation is employed to trick users into making security mistakes or giving away sensitive information. In this particular case the social engineering attack can be carried out in several ways:

- With the complicity of the Orange Money legal agent, in this case the agent could transfer to the attackers the numbers of people who have a large amount of money in their accounts or people who have just made transactions so that the scammer can use this to carry out its attack.
- Physical contact refers to the case where the attacker is in the same physical environment as the victim. In this case, the attacker can secretly record the attacker's number if the attacker spells it out loud, or quickly offer a malicious copy of a transaction that the user performs in the environment (e.g. Fig. 1).
- Remote contact is the case where the attacker tries to convince the user through a message or a call to perform a non-legitimate transaction in order to steal his money.

Software Attacks. In this scenario the attacker exploits the fact that the victim uses a smart phone. This could be done for example by installing malicious code on the remote user's phone in order to gather personal information to carry out the attack. A second illustration is to use a backdoor in the orange money apk or to invite the user to download a piggybacked application.

Encryption Attacks. The third category refers to encryption attacks. An encryption algorithm is the method used to transform data into cipher text. An algorithm uses the encryption key to modify the data in a predictable way, so that even if the encrypted data appears random, it can be transformed back into plain text using the decryption key.
In the encryption attack scenario the attacker uses means to obtain encrypted information in a chat between the user's terminal and the network. This type of attack is increasingly difficult due to the evolution of encryption, hashing and trusted third party methods.

Users Return of Experience. In this section we discuss user feedback on the use of Orange Money applications. From our preliminary study, we have noted the following points.

Most users are enthusiastic about the application and do not intend to unsubscribe. They feel that despite the small incidents and attacks that occur, the application remains the preferred one and covers more territory than other applications. In addition, each user will just have to be more vigilant to avoid attacks that are mostly based on social engineering.

The regret of some users concerns the silence of the legal managers of this application in front of the multiple attacks perpetrated. Moreover, according to the posts collected in the forums, no refund is offered to the victims of these attacks. The solution would therefore be to increase communication and support for victims by the legal authorities.

3 Best Practices in Security

Handsets, mobile operating systems, numerous SMS or MMS applications, and network transport data transfer all pose threats to the mobile banking payment system. Email and phone calls might pose hazards to our mobile phones, resulting in data loss. Users who avoid receiving unexpected SMS messages can keep their phones safe.

Although user mobile applications are one of the most secure means for executing crucial payment systems or transactions, they may still be vulnerable to mobile attacks. To use encryption, an organisation or application could have control over network and transport protocols. Clients or users can delete temporary data and encrypt sensitive data stored locally.

To enhance the security of mobile banking applications, several security measures can be adopted, including second factor authentication, data encryption, site keys with security questions and images, registered mobile device authentication, and antivirus apps [5–8]. Listed below are some protection strategies and best practices for users of mobile banking apps.

3.1 Social Engineering

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email, calls, messages or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, do some risky actions, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky. However, adopting certain habits could help to avoid social engineering attacks.

- Remove any requests for financial information or passwords. If you are asked to respond to a message with personal information, it is a scam.
- Remove any requests for financial information or passwords. If you are asked to respond to a message with personal information, it is a scam.
- Double check the sender's number of the Orange Money message.
- Don't be very reactive on the tempting offers or the alleged transfer errors we receive. Taking the time to analyze calmly would be the ideal solution to avoid making unforgivable mistakes.
- In withdrawal agencies, avoid unintentionally disclosing our account information by speaking out loud. Writing on a piece of paper and handing it to the agent would be recommended to avoid this.

3.2 Software and Encryption Attacks

Software developers do their best for the security of their applications by using several approaches to ensure user safety. However, these methods are of no use if the problem comes from malicious applications designed specifically as an alternative by attackers and capturing the interest of users due to their easy access. In this section we do not make any assumptions about possible security holes in orange money apks, we highlight possible reasons for attacks on the integrity of apks and propose a set of best practices for users to avoid them.

- Jailbroken phones should not be used for mobile banking. There are many people who jailbreak their smartphones in order to gain additional benefits. However, jailbreaking smart phones exposes the operating system to vulnerabilities. Users should avoid jailbreaking or rerouting their smartphones to protect themselves from various security threats.
- Ensure that you do not install apps from third parties. It is common for people to download free applications from third parties. However, many free apps from third parties contain viruses Only download mobile banking apps from the legal official website.
- Install anti-virus apps on your mobile device. As a part of the mitigation of risks, mobile anti-virus apps will offer partial protection from malware. Install antivirus software recommended by leading companies these antivirus products have been tested by organizations such as PC Magazine [9] every year.
- When using mobile banking apps, use a secured Wi-Fi network unsecured or unencrypted Wi-Fi networks can expose sensitive information to hackers. Connecting to public Wi-Fi networks while using a mobile banking app is not recommended.

4 Related Work

In this section we will review the literature on mobile banking attacks. Wazid et al. [10] presented the evolution of mobile banking and discuss the various threats associated with it as well as some of the malware attacks.

Masrek et al. [11] developed a conceptual trust model that covers the three mobile banking trustees that are retail banks that provide mobile banking services; the mobile telecommunications provider that provides mobile Internet services; and the mobile gadget used as a medium for performing mobile banking transactions. The model should be of interest to both the researcher and the practitioner as it will help identify factors influencing consumer confidence building in mobile banking, thus leading to increased adoption and use.

Agu et al. [12] did a study to assess the attitude of bank customers towards the adoption of mobile banking services and the challenges of the mobile phone in conducting banking transactions in Nigeria with a focus on attacks. They have a survey research approach and data was collected from 200 respondents, including bank staff and bank customers. Recommendations have been proposed

to increase the level of adoption of mobile banking services in Nigeria and will help reduce attacks.

Krishanan et al. [13] have researched a money mobile technology acceptance model with aspects of perceived risk, perceived cost and perceived interactivity. This study allowed an empirical analysis of the intention of Malaysian consumers to use mobile banking services.

Krassie et al. [14] review some relevant standards and protocols for mobile banking and discuss mobile banking and their adoption within a conceptual framework. To help implement secure, reliable and easy-to-customize user interfaces for mobile banking.

5 Threat to Validity

Non-representative Sample: The number of users of the Orange Money application in Burkina is very high. The data we used for this study may therefore not be representative. This could constitute a threat to validity of this study.

Threat to Survey Data: It is common for scam victims to avoid revealing their exact scam story for fear of being judged. It could be that some people did not answer the form honestly and this could also be a threat to validity.

6 Conclusion

In this work we present a preliminary study of attacks on the Orange Money application in Burkina Faso. We based our work on feedback from victims by exploring facebook forums. The attacks perpetrated are most often based on the ignorance or negligence of the victims, hence the need to sensitise users on the different methods used by the attackers as well as the different solutions. We therefore carry out a detailed analysis of the various attacks and propose a set of best practices to avoid these attacks. In future work it would be interesting to propose a study on the detection of flaws in the application software and also on the possibilities of attacks on the encryption.

References

1. GSMA: State of the Industry Report on Mobile Money, pp. 1–75. GSMA (2021)
2. Mountain View: Sécurité des services bancaires mobiles 1 adulte sur 3 à l ' échelle mondiale accédera à ses services bancaires sur son appareil mobile, pp. 1–6 (1877)
3. lekiosquedigital: The digital kiosk (2018). https://lekiosquedigitalduburkina.com. Accessed 20 June 2021
4. Deogirikar, J., Vidhate, A.: Security attacks in IoT: a survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37. IEEE (2017)
5. He, W., Tian, X., Shen, J.: Examining security risks of mobile banking applications through blog mining. In: MAICS, pp. 103–108 (2015)

6. Cognizant. Cognizant (2018). https://www.cognizant.com/us/en/industries/banking-technology-solutions. Accessed 20 June 2021
7. Chandramohan, M., Tan, H.B.K.: Detection of mobile malware in the wild. IEEE Comput. Archit. Lett. **45**(09), 65–71 (2012)
8. La Polla, M., Martinelli, F., Sgandurra, D.: A survey on security for mobile devices. IEEE Commun. Surv. Tutor. **15**(1), 446–471 (2012)
9. PCmag. PC Magazine. https://www.pcmag.com. Accessed 21 June 2021
10. Wazid, M., Zeadally, S., Das, A.: Mobile banking: évolution et menaces: menaces de logiciels malveillants et solutions de sécurité. IEEE Consum. Electron. Mag. **8**, 56–60
11. Masrek, M., Uzir, N., Khairuddin, I.: Examining trust in mobile banking: a conceptual framework (2012)
12. Agu, O., Simon, N., Onwuka, I.: Mobile banking - adoption and challenges in Nigeria. Int. J. Innov. Soc. Sci. Hum. Res. **4**(1), 17–27 (2016)
13. Krishanan, D., Khin, A.A., Lock Teng, K.L., Chinna, K.: Consumers' perceived interactivity and intention to use mobile banking in structural equation modeling. Int. Rev. Manag. Mark. **6**(4), 883–890 (2016)
14. Petrova, K.: Mobile Banking: Background, Services and Adoption. Auckland University of Technology (4) (2003)