Vulnerability Analysis in Mobile Banking and Payment Applications on Android in African Countries

Didier Bassolé(✉), Gouayon Koala, Yaya Traoré, and Oumarou Sié

Laboratoire de Mathématiques et d'Informatique (LAMI),
Université Joseph Ki-Zerbo, Ouagadougou, Burkina Faso
dbassole@gmail.com, gouayonkoala1@gmail.com, yaytra@gmail.com,
oumarou.sie@gmail.com
http://www.univ-ouaga.bf

Abstract. In this paper, we analyze vulnerability of some mobile banking and payment applications on Android platforms. This analysis aims at performing vulnerability assessments, facilitating an informed assessment of the information security and privacy risks that mobile banking and payment applications face in African countries, and creating awareness in the research and practice communities. We especially try to assess the risks of attacks related to privacy and data confidentiality by checking access permissions and code vulnerability of these applications. Another purpose of our work is to enable users, businesses and governments to take advantage of the opportunities offered by mobile banking and payment applications while minimising the information security risks to which they are exposed.

Keywords: Vulnerability · Mobile banking · Mobile payment · Security · Android applications

1 Introduction

A study conducted by the international firm Deloitte [11] revealed that 660 million Africans will be equipped with a smartphone in 2020 against 336 million in 2016. This high penetration rate of smartphones in African countries will lead to an increase in the development and use of mobile applications including applications related to financial transactions.

The introduction and development of mobile banking and payment is a real alternative to the very low rate of banking in African countries. Mobile money, electronic wallet attached to an individual via a telephone number, allows to make various financial transactions without a card or a bank account. Mobile banking and payment is thus a formidable opportunity for progress for the entire value chain and its evolution must translate into a new generation of infrastructure services capable of offering customers the same level of security, availability

J. P. R. Thorn et al. (Eds.): InterSol 2020, LNICST 321, pp. 164–175, 2020.
https://doi.org/10.1007/978-3-030-51051-0_12

and performance regardless of the circumstances of the mobile banking and payment transaction.

More concerned about economic than security issues, companies too often pass innovation, ease of use and consumer demands before the basic safety rules. However, when vulnerability in mobile applications are exploited, critical data leaks can be very costly for the enterprise. Many factors, including the multiplicity of hardware platforms and operating systems combined with the personalization possibilities left to devices users and the vulnerabilities of devices and their applications, make mobile a high-risk payment platform.

However, the option of using mobile banking and payment services has become almost natural and it is becoming urgent for users to be made aware of potential security risks. Many users need to be reassured about the reliability and security of their banking transactions mobile. Fundamental issues arise for a secure use of mobile banking: are mobile banking applications safe? Can they be used safely? How can we conciliate innovation and security in the development process of mobile banking and payment applications?

The remainder of this paper is structured as follows: Sect. 2 discusses related works. Section 3 presents our vulnerability analysis process, Sect. 4 discusses results of our analyzes. Section 5 focus on consequences of permissions on privacy and the security of personal data, Sect. 6, provide discussions on mobile banking and payment security services and requirements. We conclude this work in Sect. 7.

2 Related Works

Mobile banking and payments are increasingly being adopted by organisations as a new way of doing business in the 21^{st} century. Thus mobile banking and payments security concerns are becoming more and more pressing as smartphones penetration, and its associated bulk of malicious apps, is increasing in developing countries. Security issues in mobile banking and payments procedure have already had a significant amount of discussion in the literature [4,5,7,10].

In [9], Paul Ruggiero and Jon Foote illustrate Cyber threats to mobile phones. There evoque the fact that the number of new vulnerabilities in mobile operating systems jumped and the number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up. Vishal Goyal et al. develop a framework for analyzing the risks involved in electronic payments in developing countries [1,3]. In [2], K. Linck et al. examine security issues in mobile payment from the customer viewpoint. Their study is considered as a guideline for mobile payment service providers in order to prevent security concerns through appropriate design and communication of payment procedures and to convince customers of the security of their mobile procedures by meeting concerns in informative advertising. In [6], Bradley Reaves et al. perform security analysis of branchless banking applications in the developing World. Their analysis discovers pervasive weaknesses and shows that six of the seven applications broadly fail to preserve the integrity of their transactions. Their analysis

reveals that the majority of these apps fail to provide the protections needed by financial service. Ajit Singh in [8], identify some vulnerabilities in mobile cashless transactions that can be exploited by hackers and result in the denial or theft of services for consumers, as well as the loss of revenue, brand reputation, and customer base for vendors. He also explains how mobile apps developers and end user/customers can prevent their sensitive personal information and transactions from being hacked.

In a study on vulnerabilities in mobile financial applications published in 2018, *Positive Technologies* [12] found that most of the applications analyzed in 2016 had vulnerabilities whose main threat was access to sensitive customer data. This study shows that in 2017, attacks on mobile banking applications concerned identity theft, access to customer banking data and fraudulent transactions (Fig. 1). In order to avoid these risks, the study recommends that banks pay more attention to an appropriate architecture, careful formulation of technical requirements and secure development. It is necessary to rigorously test applications and security mechanisms.

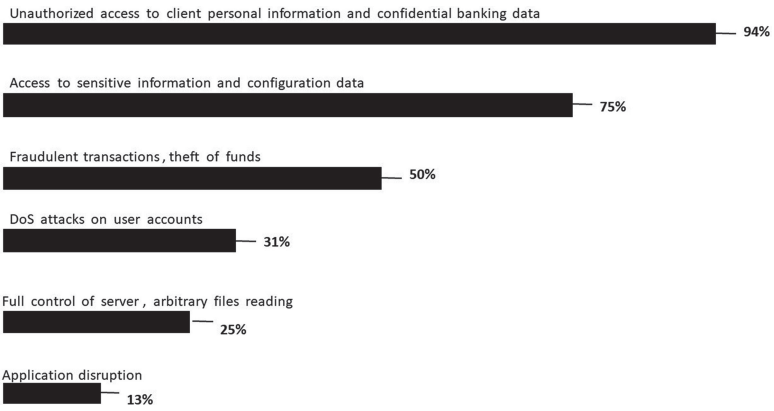


Fig. 1. Potential impact of attacks on mobile banks (vulnerable applications)

According to a new study published in 2019 by *Positive Technologies* [13], it appears that unsecured data storage (Fig. 3) and authentication data (Fig. 2) are gaps that offer opportunities for cyber attackers. This study also reveals that malware also comes from official app stores. Following the example of Anubis, a bank trojan horse that managed to avoid the security checks performed by Google Play and the Android security system.

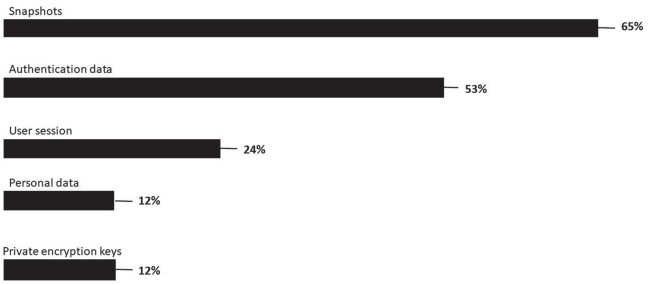


Fig. 2. Main leaks in client-side components (percentage of vulnerable applications)

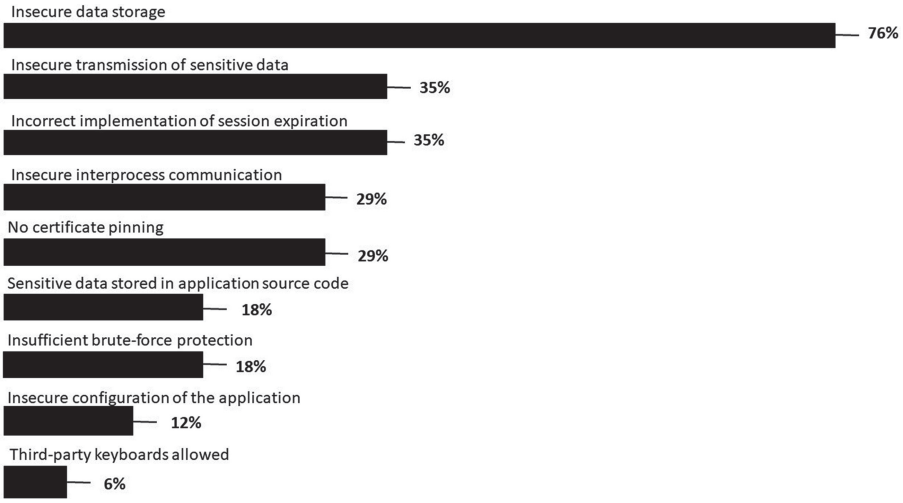


Fig. 3. Vulnerabilities of mobile applications (percentage of client-side components)

3 Vulnerability Analysis Process

3.1 Applications to Analyze the Degree of Data Exposure

Mobile banking and payment applications are used to provide services to the customers. The banking, financial and other payment applications are relatively more sensitive to security compared to other category of non-financial applications. Studies conducted on certain categories of applications have identified security breaches of data stored via mobile applications. Thus, through this study, we wish to place particular emphasis on the degree of data exposure with the use of financial applications in Africa. Our sample includes a total of fifty-three (53) applications from African banks or banks with subsidiaries in Africa. Our choice is motivated on the one hand by the high number of users of the Android platform making them targets for malware authors [14,15].

On the other hand, several studies report a high risk of attack risks for Android applications compared to iOS applications [12,13].

All these applications have been downloaded on Google Play. This approach allows us to have applications that have undergone Google's verification tests before being published. The objective is to assess the risk associated with financial applications, including the risk of data privacy attacks. This consists of verifying access authorizations, code vulnerability, and intellectual property protection (piggybacking) of these financial applications.

3.2 Analysis Process

Our study concerns mobile banking applications in Africa. This analysis concerns fifty-three (53) mobile applications of the main banking players emerging from the African market such as Ecobank, Coris Bank International, UBA (United Bank of Africa), BOA (Bank Of Africa), Diamond bank, etc. and subsidiaries of banks such as Société Générale, Standard Chartered, etc. present in Africa. For the analysis of these applications, we used the static and dynamic approach. This analysis concerns the characteristics, interactions, permissions granted and security of personal data in each application. For the static analysis, we proceeded by reverse engineering with Apktool (Fig. 4). It allowed us to obtain the source code for each application we inspected. The inspection concerned the manifest files in order to analyse the characteristics of each of the applications. It verifies the interactions of an application or its components with the system and reveals potential security threats and privacy breaches. Apktool is used to disassemble (or reassemble) the file *class.dex* in the apk and get the bytecode of the file *.dex*. It is used with the tools smali and baksmali. smali allows you to have the files in a more human-readable format and also to compile the file if you have made changes. baksmali is used to decompile the files *class.dex*. For dynamic analysis, we used the virustotal platform (with more than sixty antiviruses) for malware detection.

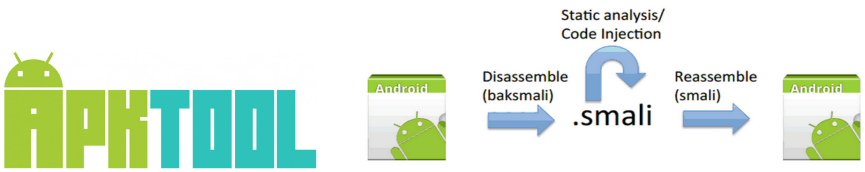


Fig. 4. Tools and procedure for decompiling/recompiling an apk.

4 Results of the Analysis

One of the disadvantages of the Android security model is the permissions management. Android has approximately one hundred and thirty (130) permissions, including permissions that are at risk with respect to their access to sensitive and personal information. Some permissions are new and more exploited by malware authors and are dangerous with regard to their access to sensitive personal data. As a result, they are more exploited by malware authors.

Malware developers exploit weaknesses in permissions management at several levels. For each application analyzed, we have the most dangerous access required and all permissions granted.

In the Fig. 5, we associate each permission with the number of analyzed applications with this authorization.

In the Fig. 6, we have associated the number of permissions it contains with each application analyzed.

We identified thirty-nine different permissions in all the applications analyzed. Most applications have access to networks, location data, camera, user tasks, device status, messaging, contacts, accounts, calls, voicemail, etc. We therefore checked the seriousness of these different permissions. Of the thirty-nine permissions identified, twenty-five are considered more risky. Thus, according to our analysis:

- 71.7% of the analyzed applications access precise location and write information to the memory card while 43.4% provide SD card read access;
- 45.28% of the applications analyzed provide access to the camera and 13.21% of the applications allow voice (audio) recording;
- 60.38% of the applications analyzed allow contacts to be read, 16.98% to be written and 18.87% to be used to make telephone calls;
- 35.85% of applications provide access to accounts and 3.77% of applications provide access to user activities;
- Only one application grants access to SMS (send, receive and read) and 7.55% of applications grant access to Bluetooth;
- In addition, all analyzed applications require Internet access;
- In 30.18% of Android applications that we have analyzed the android attribute: allowBackup is set to “true”. This allows you to create a backup copy of the application data when the device is connected to a computer. An attacker can use this vulnerability to obtain the application data.

The results of the dynamic analysis revealed five (5) malware, including trojans in three (3) applications. Static analysis has identified applications that can be used to display account balances, transfer money, make mobile payments, etc. This analysis identified authorization abuses that could compromise the confidentiality of sensitive data.

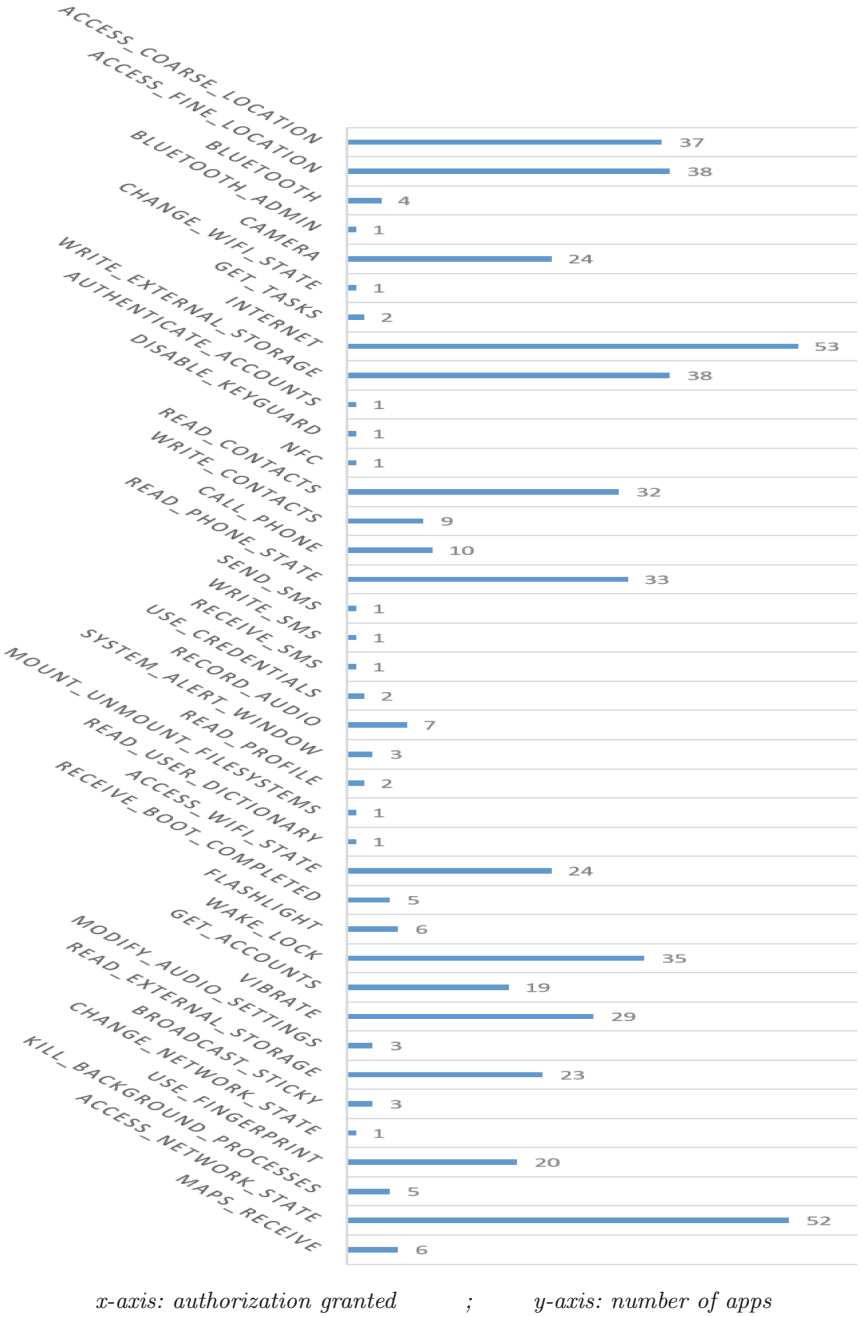
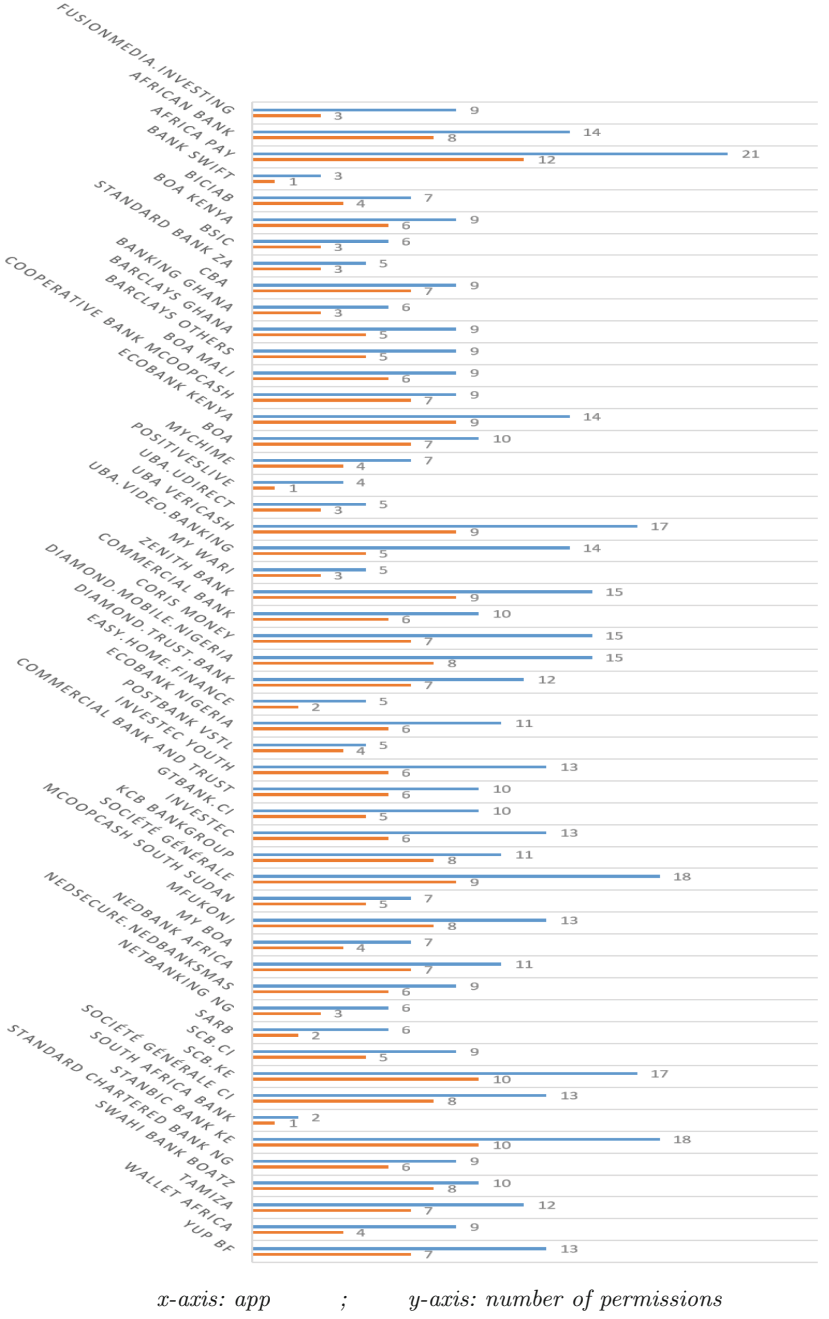


Fig. 5. Number of apps per permission



x-axis: app ; y-axis: number of permissions

Fig. 6. Number of permissions per app

5 Consequences of Permissions on Privacy and the Security of Personal Data

In our analysis, the granting of permissions is important in data protection. Although some permissions are required for the application's features, their management remains a concern for the security of the data stored on the devices. In addition to the ignorance of some users, authorizations giving access to sensitive resources expose these resources to malware threats. The need to find alternatives is essential for the protection of sensitive resources.

The particularity of these applications is Internet access. Since all these applications provide access to the Internet, any other access to a sensitive resource increases the risk of data leakage. With Internet and SMS access, a malicious application can read SMS and send overpriced SMS to third parties. Also access to the location (38 apps involved in our analysis) allows a malicious application to send the user's position to a third party. Access to the camera allows a malicious application to take image or video files and transmit them to third parties over the Internet. In addition, there is access to audio recording and memory card access, all of which compromise the confidentiality of personal data in the presence of a malicious application.

We have permissions giving access to user information, to the user's location, to produce and send personal data and having control over the device's hardware and access to the Internet. As a result, these accesses to user information make the application more vulnerable to the risks of malicious attacks. Permissions may each be harmless but granted together, the risk of exposing confidentiality can increase considerably.

6 Mobile Banking and Payment Security Services and Requirements

The increasing complexity of the technologies used to develop mobile applications and the lack of security expertise of multiple developers of such applications in developing countries, can largely explain the recurring vulnerabilities they present. In order to limit the risks in mobile banking and mobile payment apps, some good practices can be applied. Securing user data requires a responsible attitude from application developers and users themselves.

6.1 Requirements and Recommendations for Developers and Decision-Makers

In addition to the proposals made in [16,17] against the threats mentioned, we propose various preventive measures to prevent the violation of the privacy of users of mobile banking applications.

1. Do not store data on the handset to avoid exposing the device to theft or malicious application. The storage of sensitive information is a key point

of security for a mobile application. If the storage of sensitive information is absolutely necessary, the data must be encrypted. In this case, the type of encryption to be used depends on the type of sensitive information to be stored on the equipment (secure container of the equipment, third-party encryption container, etc.). No sensitive information should be stored in application logs, caches (http queries), local databases (SQLite), or, of course, in application code.

2. Restrict application permissions to what is strictly necessary to limit impacts in the event of an attack. Sensitive permissions (sending SMS, GPS positioning, etc.) must be examined carefully.
3. Secure transactions on the network, including exchanges between the application and its server. The data that passes between the server and the mobile are often sensitive (business data, personal data). We must ensure that strict management of access and user rights is carried out on the server side. All communications must be encrypted because it is not uncommon to connect to unsafe networks (public wifi).
4. Use existing cryptographic means, safe and robust, and in no way its own cryptographic algorithms. When encrypting streams by means of a certificate (for example, for HTTPS), it is essential to verify the validity of the server certificate (validity end date, no self-signed certificate, recognized certification authority, etc.).
5. Encrypt the application before distributing it via the blinds and use separate channels of communication for sensitive data.
6. Use adequate means for testing applications in order to address programming risks. The major questions for testing applications: what are apps writing to the file system? How is data stored? How are apps communicating via HTTP and Web Services? SSL? How are apps communicating over the network? TCP and Third-party APIs. Use HTTPS instead of HTTP and accept only valid SSL Certificates.
7. Injection flaws tend to be easier to discover when examining source code than via testing. Scanners and fuzzers can help attackers find injection flaws. Follow secure coding practices from respective platforms.
8. Developers need to learn more about the importance of secure storage of private and sensitive data.
9. They must disable the backup of the application by setting the android attribute: allowBackup to “false”.
10. Also, more vigilance is needed during the design phase to avoid a high number of vulnerabilities created during this stage.

6.2 Proposals for Solutions for Users

As the main victim, users must be careful in the use of smartphones and associated mobile applications so as not to compromise their devices by extending their functionality, granting dangerous access, disabling protection, etc. To regularly integrate patches, users must update their operating system. Therefore, for application updates, they must take care to check for new authorizations

added. They must limit application permissions to what is strictly necessary to limit impacts in the event of an attack. Sensitive permissions (sending SMS, GPS positioning, etc.) must be carefully examined. When applications require too wide access to features or data, users should not grant them if the authorizations requested are unreasonable in relation to the purpose of the application. They should carefully check the links received by email or SMS before opening them from any source. And if the linked address contains spelling mistakes, the email is not authentic.

7 Conclusion

Mobile banking and payments are an important technological innovation that increasingly impacting the financial ecosystem in African countries. Therefore, for widespread use and customer acceptance of mobile banking and payments services, both perceived and technical levels of security should be high. For customers, privacy should not be compromised and there should be no possibility of financial losses. Then, we invite engineers, designers and developers of mobile banking services and applications from African countries to integrate safety and security aspects into their development process and to strike a balance between user-friendliness and security. It is very necessary and fundamental to take account all the subtleties of implementation of security mechanisms, apply SSDLC practices, and rigorously test applications and security mechanisms.

Taking into account the future, particularly the economic challenges of information security, it is essential that the various players (users, decision-makers and practitioners) in mobile banking and mobile payment pool their efforts and experiences in order to reduce the impact of vulnerabilities in mobile applications.

References

1. Goyal, V., Pandey, U. S., Batra, S.: Mobile banking in India: practices, challenges and security issues. Int. J. Adv. Trends Comput. Sci. Eng. **1**(2), 56–66 (2012). ISSN No. 2278–3091
2. Linck, K., Pousttchi, K., Wiedemann, D.G.: Security issues in mobile payment from the customer viewpoint. In: Ljungberg, J. (Hrsg.) Proceedings of the 14th European Conference on Information Systems (ECIS 2006), Göteborg, Schweden, pp. 1–11 (2006)
3. Pousttchi, K., Giaglis, G.M., Werthner, H., Tschammer, V., Froeschl, K.A.: Conditions for acceptance and usage of mobile payment procedures. In: Proceedings of the 2nd International Conference on Mobile Business, Austria, Vienna, pp. 201–210 (2003)
4. Harris, M.A., Patten, K.P.: Mobile device security considerations for small-and medium-sized enterprise business mobility. Inf. Manag. Comput. Secur. **22**(1), 97–114 (2014). https://doi.org/10.1108/IMCS-03-2013-0019
5. Wang, Y., Hahn, C., Sutrave, K.: Mobile payment security, threats, and challenges. In: 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), pp. 1–5 (2016)

6. Reaves, B., Scaife, N., Bates, A., Traynor, P., Butler, K.R.B.: Mo(bile) money, mo(bile) problems: analysis of branchless banking applications in the developing world. In: The Proceedings of the 24th USENIX Security Symposium, Washington, D.C., 12–14 August 2015 (2015). ISBN 978-1-931971-232. https://www.usenix.org/node/190885
7. Krueger, M.: The future of m-payments—business options and policy issues. Electronic Payment Systems Observatory (ePSO), Institute for Prospective Technological Studies, August 2001. http://epso.jrc.es/Docs/Backgrnd-2.pdf
8. Singh, A.: Cashless India: leveraging possibilities and facing security challenges in the mobile Space. https://www.globallogic.com/gl_news/cashless-india-leveraging-possibilities-and-facing-security-challengesin-the-mobile-space/
9. Ruggiero, P., Foote, J.: Cyber threats to mobile phones. US-CERT http://www.us-cert.gov/
10. Karnouskos, S. et al.: Secure mobile payment–architecture and business model of SEMOPS. In: Evolution of Broadband Service, Satisfying User and Market Needs, EURESCOM Summit 2003, Heidelberg, Germany, 29 September–1 October 2003 (2003)
11. Les tendances 2018 du secteur des technologies, médias et télécommunications (TMT) en Afrique. https://www2.deloitte.com/fr/fr/pages/presse/2018/des-foyers-africains-connectes-a-internet-via-les-technologies-mobiles.html
12. Financial application vulnerabilities. https://www.ptsecurity.com/ww-en/analytics/financial-application-vulnerabilities/. Accessed 23 Apr 2018
13. Vulnerabilities and threats in mobile applications. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/. Accessed 19 June 2019
14. Mobile Threats Report, Juniper Networks Third Annual, March 2012 through March 2013
15. Symantec, 19 August 2013. https://www.symantec.com/security-center/writeup/2013-081914-5637-99
16. National Institute of Standards and Technology. Guidelines on Cell Phone and PDA Security (SP 800-124). http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
17. Stallings, W.: Cryptography and Network Security: Principles and Practice, 6th edn. Pearson, London (2013)