



بسم الله الرحمن الرحيم



**Sudan University Of Science and Technology**

كلية الدراسات العليا

**College Of Graduate Studies**

# **Security Evaluation of Mobile Banking Applications In Sudan**

**تقويم أمني لتطبيقات الموبايل المصرفي في السودان**

**A Thesis submitted in partial fulfillment of the requirements of Master degree in Information Technology**

**by :**

Khalid Abdelhadi Khalid

**Supervised by :**

Dr : Yahia Abdalla Mohamed Hamed

2020

# **Dedication**

To My Father, And Mother

To My Sisters And Brothers

To My Friends,

To Those Who Gave Me All Kind Of Support, To All ,I  
Dedicate This Work .

# Acknowledgements

Praise is to **Allah** , the almighty for having guided me at every stage of my life.

I would like to thank my research supervisor **Dr. Yahia Abdalla Mohamed Hamed** for giving me the opportunity to work with him and guiding and helping me throughout this research and other courses.

Also I would like to thank **Dr. Feisal** for his encouragement and insightful comments.

## Table of contents:

Dedication .....	ii
Acknowledgement.....	iii
Table of contents .....	iv
List of abbreviation .....	vii
List tables.....	viii
List of figures .....	ix
Abstract .....	x
المستخلص.....	xi
<b>Chapter 1.....</b>	<b>1-4</b>
1-1 Introduction.....	2
1.1.2 Mobile apps Security Testing.....	3
1.2 Research Problem.....	3
1.3 Research Objectives.....	3
1.4 scope and limitations.....	4
1.5 thesis organization.....	4
<b>Chapter 2.....</b>	<b>5-9</b>
2.1 Introduction.....	6
2.2 Mobile banking.....	6

2.3 Benefits of mobile banking.....	6
2.4 vulnerabilities of mobile banking .....	7
2.5 literature review and previous studies.....	7
2.6 Summary of previous studies .....	9
<b>Chapter 3.....</b>	<b>10-21</b>
3.1 introduction .....	11
3.2 privacy .....	11
3.2.1 Important of privacy.....	11
3.2.2 Privacy In android.....	12
3.2.3 Privacy In iOS.....	14
3.3 securing app code (Reverse Engineering).....	14
3.3.1 APK format .....	16
3.4 multi factor authentication.....	17
3.5 security communication.....	18
3.6 securing data storage.....	19
3.7 session time out.....	21
<b>Chapter 4.....</b>	<b>22- 46</b>
4.1 Introduction.....	23
4.2 privacy .....	23
4.2.1 Step one testing .....	23
4.2.2 Step two evaluation .....	27
4.3 Securing App Code & Reverses Engineering.....	27

4.3.1 Step one testing .....	28
4.3.2 Step two evaluation .....	30
4.4 Multi – Factor Authentication.....	32
4.4.1 Step one testing .....	32
4.4.2 Step two evaluation .....	35
4.5 Secure Communication .....	35
4.5.1 Step one testing .....	35
4.5.2 Step two evaluation .....	38
4.6 data storage Encryption .....	38
4.6.1 Step one testing .....	39
4.6.2 Step two evaluation .....	43
4.7 Session Time Out .....	43
4.7.1 Step one testing .....	43
4.7.2 Step two evaluation .....	45
<b>Chapter 5.....</b>	<b>47-51</b>
5-1 Conclusion.....	48
5.2 future work.....	48
5.3 References.....	49

## **List of abbreviations:**

- 1- **EFTPOS** Electronic Funds Transfer At Point Of Sale .
- 2- **DDoS** Distributed Denial Of Service.
- 3- **MITM** Man-In-The-Middle Attacks.
- 4- **APK** *Android Application Package*
- 5- **CIA** Confidentiality, Integrity, Availability.
- 6- **SNIA** Storage Networking Industry Association.
- 7- **GPS** Global Positioning System
- 8- **QR Code** Quick Response Code
- 9- **IMEI** International Mobile Equipment Identity
- 10- **Sqlite** Android Database
- 11- **IPIN** Is A 4digit Code Used When Making Purchase Through The Internet And Mobile Application .
- 12- **HTTP** Hypertext Transfer Protocol.
- 13- **HTTPS** Hyper Text Transfer Protocol Secure.
- 14- **TLS** Transport Layer Security .

## List of tables:

Table 1:1( version of application ).....	4
Table 2:1 (content android application).....	17
Table 4:1 (result of evaluation privacy).....	27
Table 4:2 (result of evaluation revere engineering).....	31
Table 4:3 (result of factor authentication).....	35
Table 4:4 (Result of the connection check).....	38
Table 4:5 (Result of data storage check).....	43
Table 4:6 (Result of session time out).....	45
Table 5:1 (security Evaluation).....	48



## **List of figures:**

Figure 3:1 (evaluation factor).....	11
Figure 3:2(android permission).....	12
Figure 3:3(IOS permission).....	14
Figure 3:4(reverse engineering tools).....	16
Figure 3:5(multi factor authentication).....	18

## Abstract

Mobile banking is an electronic banking service that allows customers to conduct financial transactions remotely through a bank application, as the number of subscribers to mobile banking applications in Sudan until the end of 2018 reached about 5.6 million subscribers, an increase of (96.9%) from the end of 2017.

The research selected most important and popular 13 banking applications and discussed the security assessment of these applications based on six factors represented in: **first privacy**, which are the powers that the application needs, **secondly reverse engineering** and reading the source code, can the application be modified and rebuilt, **third verification factors** and what are the requirements that the banking application needs to connect To the bank account, **fourthly securing the connection** between the application and the server, and is the sent data encrypted? **Fifthly, securing the data stored** on the phone, and how is the data stored on the phone, is it encrypted and what is the risk of this data? **Sixth, the session duration**, which is the time during which the banking application remains connected with The server can perform all operations at this time.

The research reached a noticeable difference in the applications in terms of privacy and the powers that some applications need that may affect the privacy of the user, and in terms of security, there are some security threats.

The research recommends limit access privileges, encrypting the application code, encrypting the connection, using two-line verification, saving sensitive data on the service provider, and some methods that can be used to reduce the risk of these security threats.

## المستخلص

الموبايل المصرفي هو خدمة إلكترونية مصرفية تسمح للعملاء بإجراء المعاملات المالية عن بعد بواسطة تطبيق خاص بالبنك حيث بلغ عدد المشتركين في تطبيقات الموبايل المصرفي في السودان حتي نهاية عام 2018م حوالي 5.6 مليون مشترك وذلك بنسبة زيادة (96.9%) عن نهاية عام 2017م .

قام البحث بإختيار اهم واشهر 13 تطبيق مصرفي وناقش التقييم الامني لهذه التطبيقات بناءا علي ستة عوامل متمثلة في: **اولا الخصوصية** وهي الصلاحيات التي يحتاجها التطبيق ، **ثانيا الهندسة العكسة** وقراءة الكود المصدري وهل يمكن التعديل علي التطبيق واعاده بناه ، **ثالثا عوامل التحقق** وماهي المتطلبات التي يحتاجها التطبيق المصرفي للوصول الي الحساب المصرفي ، **رابعا تأمين الإتصال** بين التطبيق والمخدم وهل يتم تشفير البيانات المرسله ، **خامسا تأمين البيانات المخزنة** علي الجوال وكيف يتم تخزين البيانات علي الجوال هل يتم تشفيرها وماهي خطورة هذه البيانات ، **سادسا مدة الجلسة** وهي عبارة عن الزمن الذي يظل فيه التطبيق المصرفي متصل مع المخدم وفي هذه المده يمكن اجراء جميع العمليات .

وتوصل البحث للتباين الملحوظ في التطبيقات من ناحية الخصوصية والصلاحيات التي تحتاجها بعض التطبيقات التي قد تمس خصوصية المستخدم ، ومن الناحية الامنية وجود بعض المهددات الامنية .

ويوصي البحث بالحد من صلاحيات الوصول ، تشفير الكود الخاص بالتطبيق، تشفير الاتصال ، استخدام التحقق بخطوتين ، وحفظ البيانات الحساسة على مزود الخدمة ، و ببعض الطرق التي يمكن استخدامها للتقليل من خطر هذه المهددات الامنية .