

# MODERN MOBILE APPLICATION SECURITY

**Favour Femi-Oyewole**

G | CISO Access Bank Plc

## A Little About me



*Mrs. Favour Femi-Oyewole is a mother, a woman leader and the Group Chief Information Security Officer, Access Bank Plc. She has over 22 years experience derived from an optimal mix of the academics, enterprise security operations and business leadership*

A graduate of computer science ,(B.Sc.), M.Sc.. Computer Science and M.Sc.. Information Security and currently a doctoral student at the Covenant University, Nigeria. An alumni of both Harvard Kennedy school (HKS, Harvard university and Massachusetts institute of Technology (MIT), USA.

Various certifications from OEMs, security providers & standards bodies including Cisco, Checkpoint, ISACA, EC-Council, BSI (ISO 27001:2013) and PECB

1st woman in the world to win the global certified CISO (C|CISO) of the year (2017) from the EC-Council in USA.

Blockchain Certified Professional (first female in Africa),

Member of the Cybercrime Advisory Council in Nigeria with the mandate of implementing cybersecurity for all sectors in Nigeria and the pioneer chair of Standard and Evaluations Committee

Member of the global Certified Chief Information Security Officer (CCISO) Advisory Board & Scheme Committee of the EC-council in USA.

## THE VERSATILITY AND PERVASIVENESS OF THE MOBILE PHONE

The mobile phone is arguably a companion and holds many sensitive information

- Personal Information
- Organization's Information

Today, banking applications and a host of other applications are brought to our fingertips...

- What adversarial games can hackers and other malicious actors enable through mobile technology?

## THE VERSATILITY AND PERVASIVENESS OF THE MOBILE PHONE

There are about 4.48 billion smart phones users in the world

- ❖ Android has 72.19% share
- ❖ iOS has 27% share
- ❖ Others 0.81%
- Many people spend close to 3hrs per day on their mobile phones? Factor our sleeping time and the proportion of useful time increases!
- Mobile web traffic accounts for over 50% of global web traffic

## COULD IT BE AN ACHILLES HEEL?

What If you were being targeted? Could your phone be a weak point? Remember Al-Jazeera journalists?

## Pegasus:

- not just an ordinary spyware and is just an example from the stables of NSO Group Technologies
- by clicking on a malicious link from an attacker (highly advanced or state actor)
- installs on a number of iOS or Android devices
- secretly jailbreaks the device
- text messages gets read, calls can be tracked, phone location, information from and on installed apps and harvesting of passwords

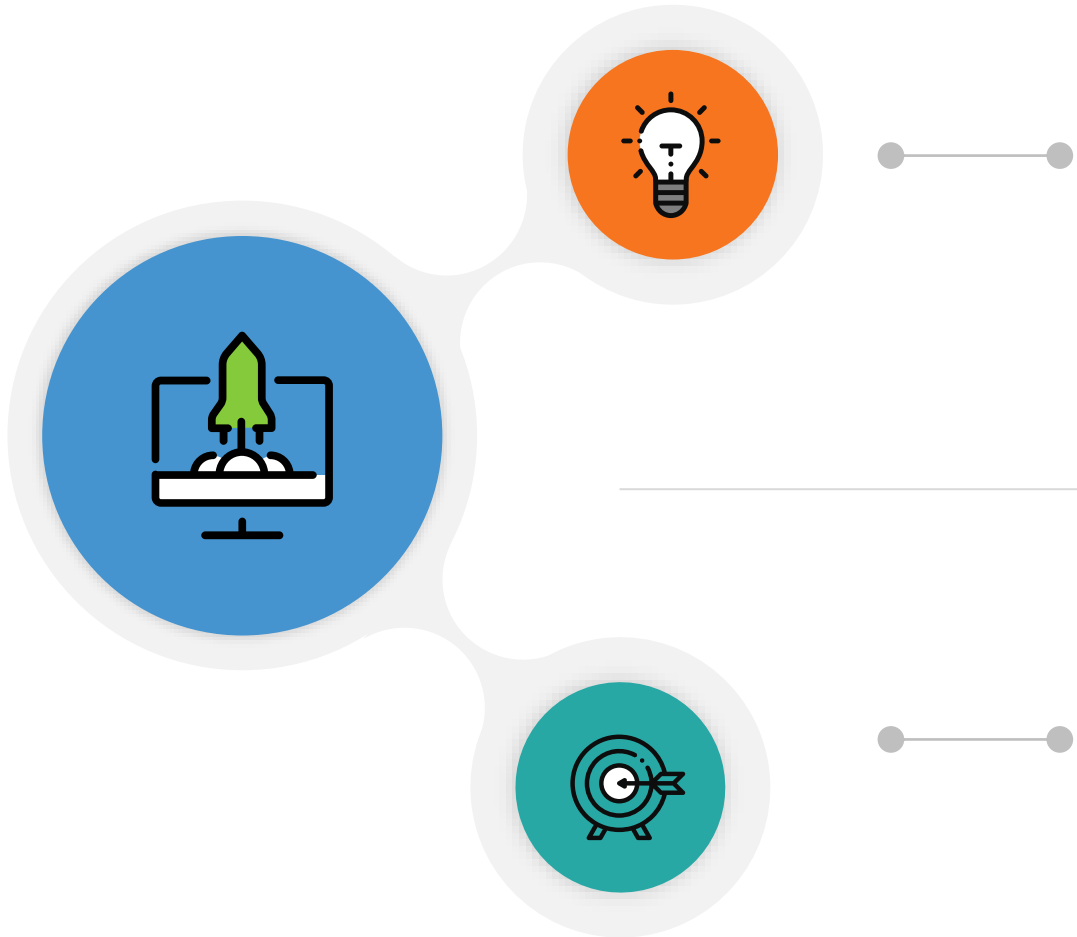
## SIMPLE CASES

Do you like installing Apps on your phone ?

Google Play have a lot of Apps and some are just masquerades with malicious intentions

## What they can do?

- collect and send GPS coordinates, contact lists, e-mail addresses etc. to third parties
- send SMSs to premium-rate numbers and subscribe infected phones to premium services
- record phone conversations and send them to attackers
- take control over the infected phone
- download other malware onto infected phones

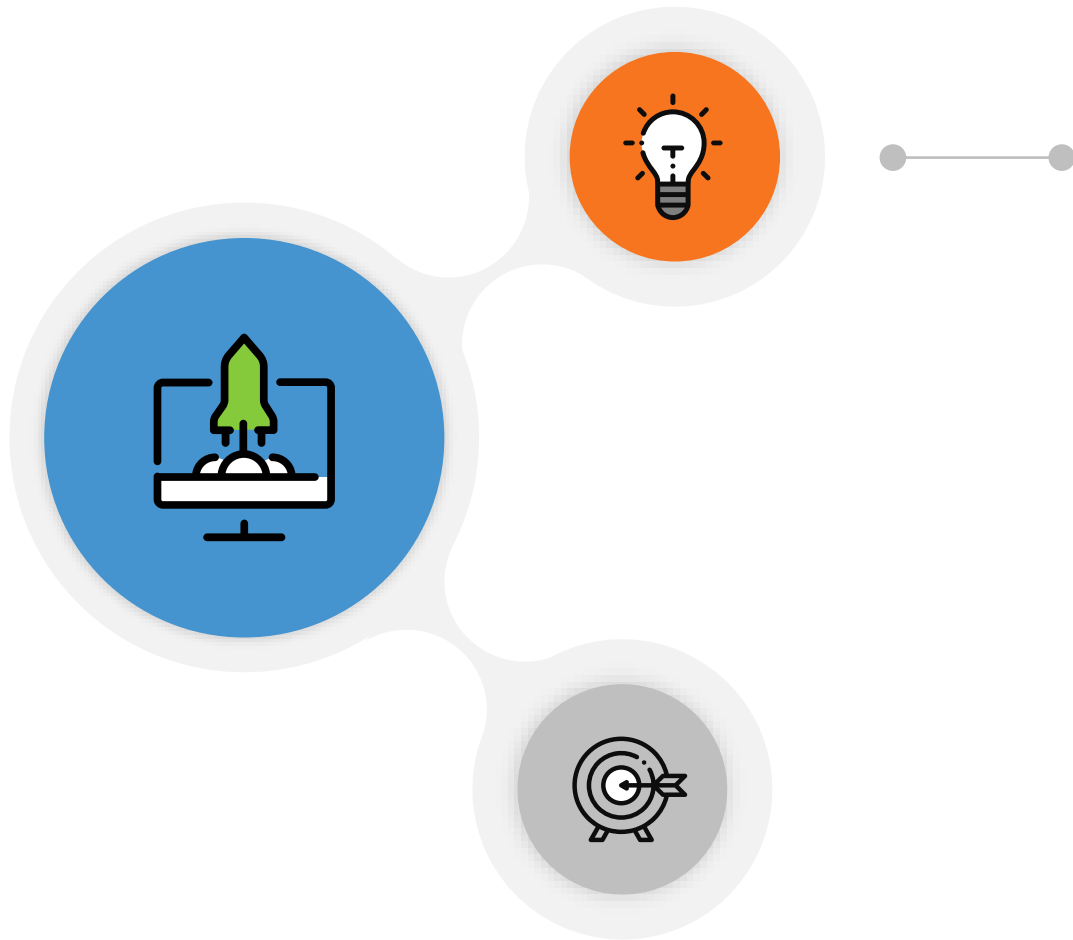


## Forensics

the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

## Security Assurance

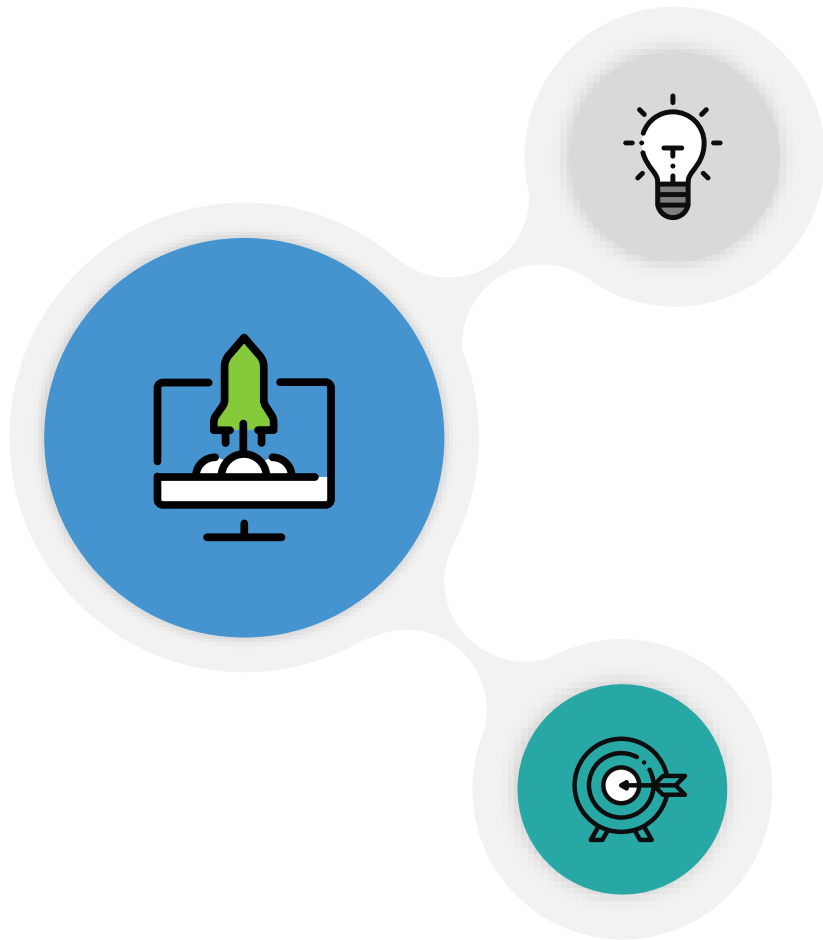
Entails testing for consistent behavior, identifying, quantifying, and prioritizing the vulnerabilities and can be extended to actively evaluating the security of the system by simulating malicious attacks



## Forensics

- The acquisition and analysis of data from devices
- Can involve internal corporate investigations, civil litigation, criminal investigations
- Can span intelligence gathering and matters involving national security.
- A fast growing and evolving field in digital forensic discipline
- Important items to consider includes:
  - ❖ Chain of custody
  - ❖ Detailed notes and complete report
  - ❖ How investigation result was validated





- Supports the organization's quality assurance objectives
- ensures the product delivered to the user is secure and delivers consistent behavior in use
- Helps anticipate and protect against future attacks

● — ●  
**Security Assurance**

# **PART B**

## FRAMEWORK FOR MODERN MOBILE SECURITY TESTING

### The Open Web Application Security Project (OWASP)

- A nonprofit foundation that works to improve the security of software.
- Uses community-led open-source software projects with a large contributor base of experts and members numbering over tens of thousands of member
- The OWASP Foundation is the source for developers and technologists to secure the web
- Identified resources are the MSTG and the MASVS

## **OWASP Mobile Security Testing Guide (MSTG)**

MSTG is a comprehensive manual for testing the security of mobile apps. It describes processes and techniques for verifying the requirements listed in the MASVS, and provides a baseline for complete and consistent security tests.

## **Mobile Application Security Verification Standard (MASVS):**

MASVS serves as framework to offer a baseline for mobile application security (MASVS- L1), while also allowing for the inclusion of defense-in-depth measures (MASVS-L2) and protections against client-side threats (MASVS-R)

## TOOLS FOR TESTING

Different tools are available in order to be able to manipulate requests and responses, decompile apps, investigate the behavior of running apps and other test cases and automate them. A few of numerous interesting one's asides tools included in your Kali Linux or Parrot Security OS are:

- Frida
- Radare2
- Ghidra
- MobSF
- BurpSuite
- Cycrypt

## Example Installation of MobSF (Mobile Security Framework)

MobSF (Mobile Security Framework) is an automated, all-in-one mobile application pentesting framework capable of performing static and dynamic analysis. The easiest way of getting MobSF started is via Docker.

1. `$ docker pull opensecurity/mobile-security-framework-mobsf`
2. `$ docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest`

It can also be installed and started locally on your host computer by running

1. # Setup
2. `git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git`
3. `cd Mobile-Security-Framework-MobSF`
4. `./setup.sh` # For Linux and Mac
5. `setup.bat` # For Windows
6. # Installation process
7. `./run.sh` # For Linux and Mac
8. `run.bat` # For Windows

## AFTER INSTALLATION

Once you have MobSF up and running you can open it in your browser by navigating to `http://127.0.0.1:8000`.

Simply drag the APK you want to analyze into the upload area and MobSF will start its job.

After MobSF is done with its analysis, you will receive a one-page overview of all the tests that were executed. The page is split up into multiple sections giving some first hints on the attack surface of the application.




A one-page overview of all the tests that were executed by MobSF and the multiple sections are evident below

The screenshot displays the MobSF web interface with a dark sidebar on the left and a main content area. The sidebar contains navigation options: Information, Scan Options, Signer Certificate, Permissions, Binary Analysis, Android API, Browsable Activities, Security Analysis, Malware Analysis, Reconnaissance, Components, Download Report, and Start Dynamic Analysis. The main content area features a top navigation bar with 'Recent Scans', 'API Docs', 'About', and a 'Search MD5' input field. Below this, there are three primary sections: 'App Icon' showing a shield icon with a 'U', 'App Score' with metrics (Average CVSS: 7.5, Security Score: 25/100, Trackers Detection: 0/205), and 'File Information' listing details like Name (UnCrackable-Level1.apk), Size (0.06MB), MD5, SHA1, and SHA256 hashes. To the right, 'App Information' lists Name (UnCrackable1), Package Name (owasp.mstg.uncrackable1), Main Activity (sg.vantagepoint.uncrackable1.MainActivity), Target SDK (28), Min SDK (19), Max SDK, Android Version Name (1.0), and Android Version Code (1). Below these is a 'Play Store Information' section. At the bottom, a dashboard shows four categories: ACTIVITIES (1), SERVICES (0), RECEIVERS (0), and PROVIDERS (0), each with a 'View' link and a corresponding 'EXPORTED' summary card below it.

**MobSF**    Recent Scans    API Docs    About    Search MD5

### App Icon



### App Score

Average CVSS **7.5**  
Security Score **25/100**  
Trackers Detection **0/205**





### File Information

Name UnCrackable-Level1.apk  
Size 0.06MB  
MD5 6aa29e071a3e12f5122a3cfe2354a53c  
SHA1 85a5cf85a6b31cd020ee9d4a55b805a8dc6770cc  
SHA256 1da8bf57d266109f9a07c01bf7111a1975ce01f190b9d914bcd3ae3dbef96f21

### App Information

Name UnCrackable1  
Package Name owasp.mstg.uncrackable1  
Main Activity sg.vantagepoint.uncrackable1.MainActivity  
Target SDK 28    Min SDK 19    Max SDK  
Android Version Name 1.0  
Android Version Code 1

### Play Store Information

<b>1</b> ACTIVITIES View	<b>0</b> SERVICES View	<b>0</b> RECEIVERS View	<b>0</b> PROVIDERS View
 EXPORTED ACTIVITIES <b>0</b>	 EXPORTED SERVICES <b>0</b>	 EXPORTED RECEIVERS <b>0</b>	 EXPORTED PROVIDERS <b>0</b>

## Basic Information displayed in the MobSF sections:

- Basic information about the app and its binary file.
- Some options to:
  - ❖ View the AndroidManifest.xml file.
  - ❖ View the IPC components of the app.
- Signer certificate.
- App permissions.
- A security analysis showing known defects e.g. if the app backups are enabled.
- List of libraries used by the app binary and list of all files inside the unzipped APK.
- Malware analysis that checks for malicious URLs.

# **PART C**

# THANK YOU

Favour Femi-Oyewole



Access Bank Plc



+234 9070 6364 81



[www.accessbankplc.com](http://www.accessbankplc.com)  
[asfavour@hotmail.com](mailto:asfavour@hotmail.com)