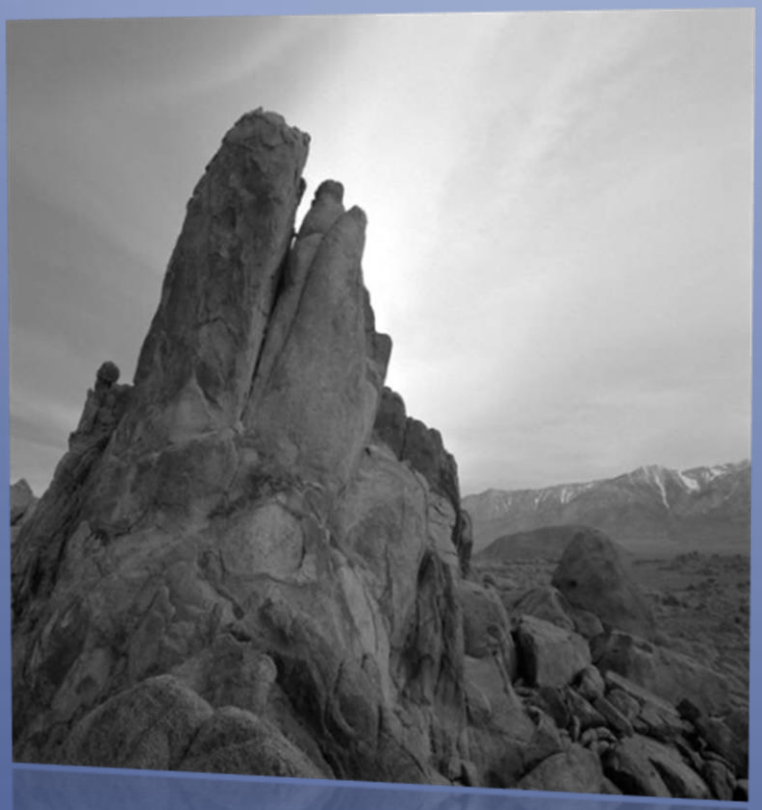


USSD Vulnerability Report on Nigerian Banking System

A way To Prevent Unauthorized Access to Bank Accounts' Funds via Missing or Stolen Mobile Phones.

- By Salim Sulaiman Liman

Table of Contents

EXECUTIVE SUMMARY

Today, many customers of the Banking sector in Nigeria that have registered the usage of Unstructured Supplementary Service Data (USSD) on their mobile phones have been victims of bank accounts "hack" when their mobile phones with the SIM cards associated with their bank accounts are in the hands of attackers. Although all the victims have felt safe at first because they abide by the security precaution of keeping one's secret keys (PIN) away from public and untrusted parties.

In this age where cyber-crimes are gaining popularity in various forms of attacks, unfortunately, keeping one's security keys are not always enough to keep one safe from attackers. There are other ways that security can be breached despite keeping security keys away from public and untrusted parties. Attacks can lead to small or very large loss to their victims. In many ways, one solution does not work for all, but it should be implemented if it will minimize the damage.

INTRODUCTION

This paper focuses on creating awareness and exposing vulnerability in Nigerian Banking System via USSD which has led to monetary loss from bank accounts of victims of missing or stolen mobile phones in Nigeria. The solutions in this paper help to provide means of fixing such vulnerability and reducing the amount of victims if the vulnerability should be exploited.

This paper was written for the reading of technical audiences in the Nigerian banking sector, with the aim of providing better security for their customers.

This paper is aimed at helping with:

- Creating awareness for the vulnerability
- Exploring varieties of ways that such vulnerability can be exploited
- Exploring ways of overcoming the vulnerability

THE VULNERABILITY

Many customers of the Nigerian Banking Sector have been victims of unauthorised transfer of funds from their bank accounts when their phones got stolen or missing, and fall into the hands of cyber-criminals (attackers), even when their PINs are unknown to the attacker.

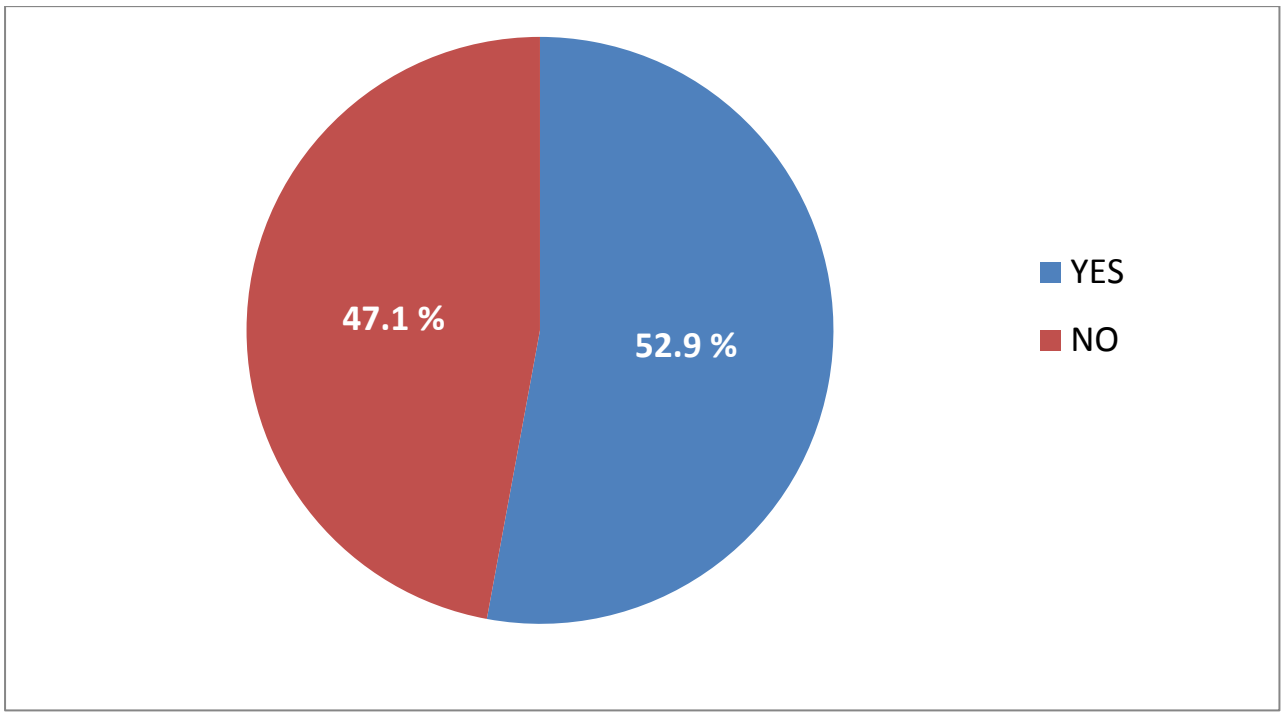
The USSD system for all banks in Nigeria demands the customers to input their PIN when trying to transfer funds from their customers account. But the flaw in "some" banks' USSD system has allowed attackers to bypass such security to follow another route and steal customers' funds.

Buying airtime from one's mobile phone has been easier with the use of USSD system programmed for banks in Nigeria. All banks' USSD systems also require customers' PIN when buying airtime for a third party. **However, the vulnerability lies in when customers are buying airtime for themselves because not all the banks prompt their customers to input their PIN in this situation.**

SURVEY ON BANKS WITH THE VULNERABILITY

A survey was carried out on One Hundred and Two (102) Nigerians on their banking experience. They submitted the name of the banks they are operating on, and a yes/no response to whether their banks request for their PIN when buying airtime for themselves via USSD.

DATA



Out of 102 responses from the survey, 48 customers belong to the banks with such vulnerability while 54 customers belong to banks without such vulnerability in their USSD system.

Based on Statistics, using this data as sample data and extending it to, for example, three million customers of the banking sector, we can see that **47.1% (1,413,000)** of the customers are open to such vulnerability.

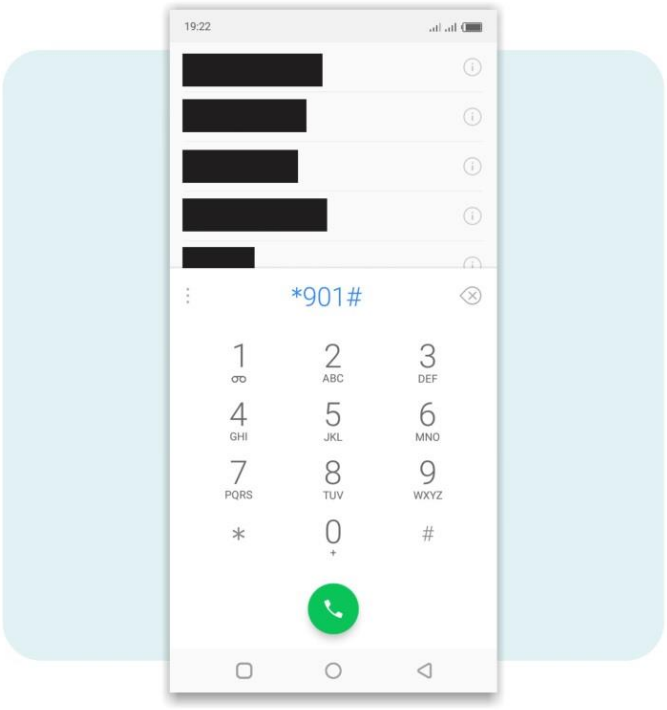
BANKS WITH THE VULNERABUILITY ACCORDING TO SURVEY

1. Access Bank PLC / Diamond Bank
2. Guarantee Trust Bank
3. First Bank of Nigeria
4. Jaiz Bank
5. Providus Bank
6. United Bank of Africa
7. Fidelity Bank
8. Zenith Bank
9. First City Monument Bank
10. Heritage Bank
11. Union Bank

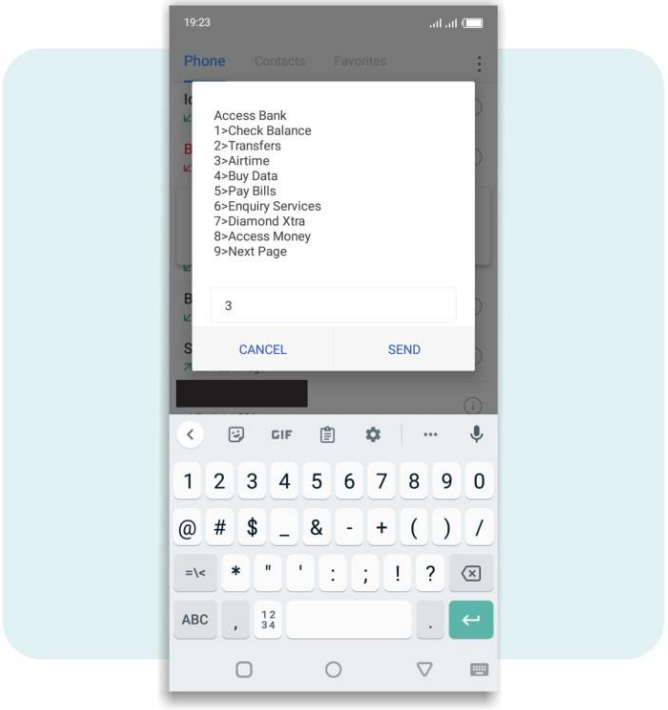
PLEASE NOTE: Data accuracy may not be 100% due to Human error with the survey.

DEMOSTRATING THE VULNERABILITY

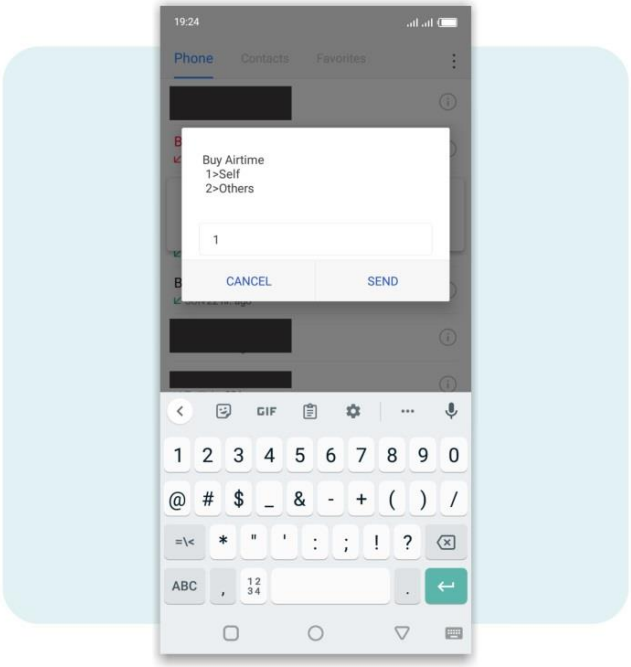
For educational reasons, the targeted bank in this example is ***Access Bank PLC***.



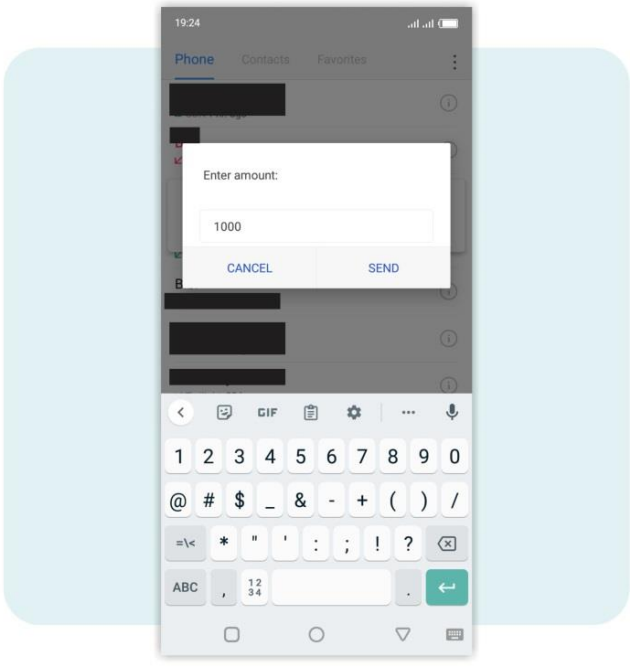
STEP 1: Dial USSD code



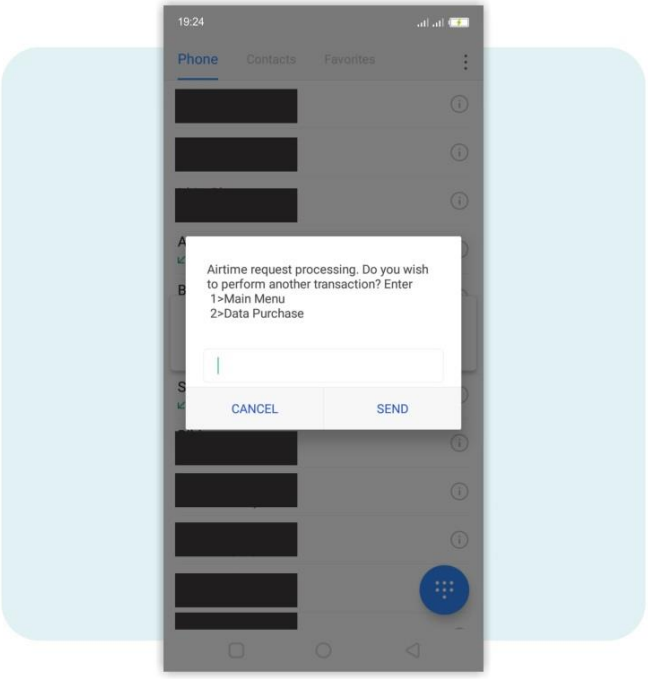
STEP 2: Select option '3' to buy airtime



STEP 3: Select option '1' to buy airtime for self



STEP 4: Enter airtime amount



STEP 5: Airtime purchase successful

No prompt for customer's PIN throughout the airtime purchase process.

HOW ATTACKERS CAN DETECT VICTIM'S BANK

Although, at first, attackers may not know the banks their victims are operating on, but there are ways to obtain this information once the victims' mobile phones or SIM cards are in their hands.

METHOD 1

- SMS CHECKING: Bank Customers leave bank messages in their phones, like bank alert SMS for credit or debit, in other to easily check their transactions and keep close records of their accounts' balances. With this, attackers can easily detect which bank their victims are operating on, and then carry out their attacks if the victims' bank falls under the ones with this USSD vulnerability.

METHOD 2

- USSD BRUTEFORCING: This will come in handy for the attackers when there are no banks SMS saved in their victims' phones or SIM cards. By trying out multiple USSD codes for banks in Nigeria, the attackers can finally arrive at the one their victims are operating on. The attackers will know their victims' bank after seeing the welcome/menu message of the corresponding banks after dialling a USSD code.

EXPLOITING VULNERABILITY TO GAIN PROFIT

METHOD 1

- **SIM TRANSFER:** Through transferring the airtime into their SIM cards after withdrawing all the funds in their victims' account. There are numerous platforms in Nigeria that buy airtime for less and pay the seller in cash. For example, ₦10,000 naira airtime from victim's SIM card can earn the attacker a sum of ₦7,000 when sold on these platforms that gain 30% off their sellers.

LIMITATION OF METHOD 1

- When victims' are already registered on their Internet Service Providers' (ISP) airtime transfer system with a PIN that is unknown to the attacker. Then they cannot sell the airtime out of their victims' SIM cards. If victims' haven't registered, the attackers will do so and be the owners of the transfer PIN.

METHOD 2

- **DATA BUNDLE TRANSFER:** Through buying and transferring data from the victims' SIM cards, attackers can use this method to gain their profits after exploiting the vulnerability since data transfer system from ISPs does not require PIN, and sell out the purchased data bundle.

OVERCOMING THE VULNERABILITY

This paper explains ways to overcome the discussed vulnerability. Some of which can be done by customers (potential victims) with little technical knowledge, banks, and ISPs.

BY USERS

- **SIM LOCK:** Customers should enable SIM cards PIN lock so as to prevent attackers from gaining access to their banks through the SIM cards associated with their bank accounts even when their SIMS are inserted in another phone. Banks can create such awareness to all their customers.

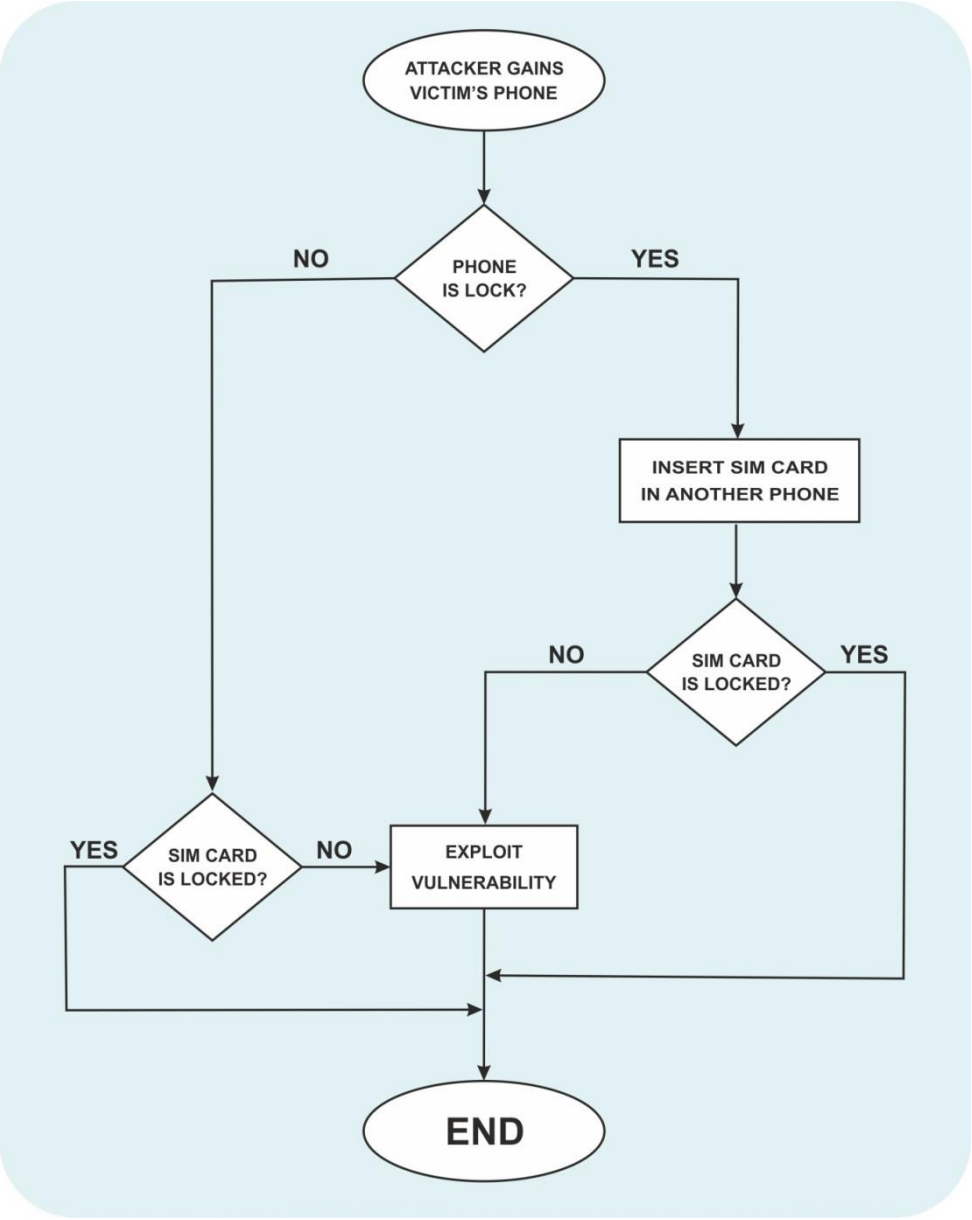


Figure 6 above shows how the attack can proceed, and also shows that SIM card lock is effective.

- **ENABLE AIRTIME TRANSFER PIN:** Customers of ISP should enable airtime transfer PIN to prevent attackers from selling out airtime from their SIM cards.

BY BANKS

- Banks (those with such vulnerability) should enable PIN request from their customers even when airtime purchase is for the SIM card associated with the bank account.

BY ISP

- ISPs should require users to use PIN in all transactions even for data bundle transfer.

CONCLUSION

This paper was written to create awareness concerning the USSD vulnerability that can be exploited by attackers to steal funds from victims' bank accounts. The solution in this paper will reduce the risk on banks' customers' accounts when their phones fall in the wrong hands.

Central Bank of Nigeria (CBN), Chattered Institute of Bankers Nigeria (CIBN), Nigerian Deposit Insurance Cooperation (NDIC), and other bodies that check commercial banks within country should create awareness to all commercial banks in the country so that those with such vulnerability in their USSD system will fix it.

ABOUT AUTHOR

- This Paper was written by **Salim Sulaiman Liman**, a student from the Department of Computer Science, Ahmadu Bello University, Zaria.
- **Author's Email:** salimsulaiman360@gmail.com
- **Author's Phone:** 08164626581, 09073139060.