IDENTIFYING THE SECURITY ISSUES OF UNSTRUCTURED SUPPLEMENTARY SERVICE DATA BANKING IN NIGERIA

Amaka Patience Binitie
Computer Science Department
Federal College of Education (T)
Asaba.

Abstract

Unstructured Supplementary service Data (USSD) is a mobile phone based technology that provides ease of service to users. Many organizations like bank, mobile network operators, commercial organizations and others have adopted USSD as a means of reaching their customers, including those in rural areas and those with low end mobile phones. The fact that USSD does not require internet access boosted its penetration in developing countries like Nigeria. Some customers have experienced fraudulent transactions on their account, carried out through USSD service. The central bank of Nigeria has mandated all banks to provide security to customer's details on USSD channel. Identifying the possible attacks will help in providing solutions to these attacks. Various attacks such as impersonation, eavesdropping, shoulder surfing among others were identified through the course of the research. These attacks were made possible as a result of many factors which include, improper session management, conveying user's PIN in plaintext, weak encryption and others. Having identified these attacks and their vulnerabilities, the focus point of future work will be identifying the actual point on USSD channel where each attack can be launched.

Keywords- unstructured supplementary service data, vulnerability, mobile banking, customers, attacks

GSM network is used widely in networking mobile connections. Its initial design was for use in voice communications but as the stage of mobile phone increases, more features were added, the most popular of which is Short Message Service (SMS) and later, USSD. The encryption algorithm on GSM network has been reverse engineered (Briceno, Goldberg &Wagner, 1999), thereby putting sensitive data moving through the network at risk of interception. The initial design of GSM was not for

carrying sensitive data but non sensitive messages. During the design, security measures for non repudiation, mutual authentication, data confidentiality, and end to end security were not included with respect to message services (Emmanuel, 2007). Most of the mobile financial institutions in third world countries uses Unstructured supplementary service data (USSD) technologies including Nigeria, which is a capability built into the Global system for mobile communication (GSM) standard, that allows high speed, bidirectional communications between mobile handsets and applications (Globitel, 2018). This service faces various attacks which the customer and banks need to tackle. But before tackling these attacks, there is need to identify these attacks.

Mobile phone also known as handset is mobile equipment used in communication between users or between a user and the mobile network. Mobile phone is among the commonest device possessed by the rich and poor, educated and uneducated. Many of the users have more than one. The world mobile industry has over 5 billion subscribers, according to real time data from GSMA intelligence, the research arm of GSMA (GSMA, 2017). This means that more than two-third of the global population is now connected to mobile services. Nigeria is not left out. There are over 162 million mobile subscribers and smart-phone penetration rate of 84% in Nigeria (Adeputun, 2018). The chief executive officer of Jumia Nigeria, Anammah made the assessment at the 2018 Mobile Report Launch that "the availability of lower price point phones has paved way for more Nigerians to own mobile phones (Adeputun, 2018).

During the last two decades, mobile technology has achieved great progress and has became one of the most important accessories in people's everyday lives all over the World. As posited by Gurung (2016), there are almost 3.6 billion mobile phone users all around the world which is almost half of the world's population. According to Suhas (2018), 2014 witness over 3 billion mobile users worldwide. Mobiles phones will become the preferred and most commonly used web device globally by 2013. Taking into account the success of mobile content services such as ringtones, games, telephone calls, short messaging and other applications, the functional capabilities of mobile telephony have been rapidly expanding and have extended their usage well beyond the classical communication applications (Zhang, 2012). It is apparent that consumers are more than willing to utilize mobile phones for several purposes. As a result, a large number of mobile applications are being built for multiple platforms (Android, J2ME, Symbian, etc.) and domains (mobile payments, mobile VAS, mobile commerce, etc.). According to Zhang (2012), although the IT infrastructure is usually undeveloped in rural areas, remarkably in most of the developing countries mobile telecommunication sector achieved rapid expansion in recent years which is partly as a result of the significant decrease of the cost of mobile phones and mobile services. The fast

increasing number of subscribers open up new business ventures and gives financial institutions some additional channels for them to deliver their services (Suhas, 2018). Several factors have led to the attraction for mobile services. According to Zhang (2012), mobile devices, and in particular, mobile phones have become the attraction for consumers, service providers and merchants in the business world, everyday life, and in fields of communication. Mobile phones are also providing an unprecedented opportunity for expansion of financial transactions of all types like: enquiry (balance enquiry/ mini statement/ currencies rates), money transfer, bill payment, cheque book request and many other banking services in developing countries where the number of phone users can exceed the number of those having bank accounts (El-safi, 2013).

Technologies like Wireless Application Protocol (WAP) which is best described as the mobile internet, short message service (SMS), Unstructured supplementary service data (USSD), and Interactive Voice Response (IVR) allows customer to access mobile financial services, which is the focus of this research, (Suhas, 2018).

USSD technology is built into the GSM standard for support of transmitting information over the signaling ch**a**nnels of the GSM network. It gives a customer the opportunity to request for information regarding his account and carryout other financial transactions (Chandran, 2014). The stakeholder involves the customer at one end, the mobile network operator at the middle and the institution at the other end. USSD has a number dialing interface which makes it easier for majority of Nigerians in the rural area who are considered numerically literate to adopt. USSD does not require internet access. It is easier to be adopted and implemented on all types of GSM handset. USSD can be Menu based or non Menu- based. In menu-based USSD which is interactive, the user dials a code that starts with asterisks (*) and ends with a hash (#). As the request from the user gets to the server it responds with a menu presented on the users mobile device. The user then types the serial number of the item of his choice and clicks the send button. The iteration continues until all the required input fields for the transaction have been captured. Then the transaction server is invoked and a transaction response similar to non-menu based section is sent back. For non menu based USSD transaction, the user types in the string of numbers starting with Asterisk (*), but this time followed with more asterisks to accommodate the requirements and finally hash (#). After which the user presses the send button. For financial transactions, which is the focus of this research, among the items required to be keyed in are; PIN, destination account, amount to be transferred and so on.

USSD technology is used for the development of mobile chatting, m-commerce, call back services, prepaid balance, software upgrades and mobile banking (Sanganagouda, 2012). The USSD software solutions widely developed for many

services like, mobile money services, location-based services, mapping services, recharge/booking services, and mobile payment and banking services (Zhou, Herselman & Coleman, 2015). When compared with SMS communication channel, USSD is better. USSD enables direct communication to be established between sender and receiver, which promote faster data transmission. USSD communication is session-oriented and it is easily implementable while being more user-friendly. The USSD application is connected as interface between the customer's telecom provider and his financial service provider. The customer can transact through handheld devices as well as in Internet Protocol mode. USSD technology offers mobile based services that do not require internet access.

Despite the fact that USSD technology does not store data like SMS, it lacks security in major areas. This paper is aimed at identifying various types of attacks that USSD is susceptible to. In USSD communications, the mobile device is only needed for message/item presentation to the user. Since responses which include users sensitive details are sent unencrypted to the server, security of users responses to the items presented at the mobile interface is completely dependent on the mobile phone encryption. It is obvious that the users PIN which appears in plain text and other sensitive data entered by the user can be obtained.

USSD Mobile Banking

USSD mobile banking in Nigeria

The introduction of Unstructured Supplementary Service Data (USSD) mobile banking services across banks in Nigeria has repositioned banking system. Banking transactions are now made easy for bank customer no matter the location and type of phone used in the transaction. It is menu based and can provide many services including , buying airtime, opening bank account, checking account balance, transferring money to same bank (intra- bank transfer) and other banks (inter- bank transfer), payment of utility bills and others (Suhas, 2018). Apart from the basic banking operation performed, each bank determines other services that can be carried out using their banks USSD code. It contains up to 182 bytes. Message received via USSD are not stored, unlike SMS messages that are stored.

How USSD Banking Works in Nigeria

A customer is required to have a bank account linked to a particular mobile phone number to perform a USSD transaction. USSD is phone independent and no special type of SIM is required; just the SIM that carries the registered Mobile number is needed. Some banks do not require their Customer's to be physically present to register

for USSD banking transaction, while some do require. All bank accounts are considered legible for USSD transaction. Customers are not provided with option of opting out of the use of USSD at the point of opening account. Registration is done with mobile phone containing the mobile phone number linked to the account. During registration, the user is required to supply details from the debit card or Bank Verification Number (BVN) linked to the account, depending on the bank. During registration, if a session times out after 20 seconds of staying idle, the user will be asked to start from the session timed out, instead of starting all over. Each bank determines the daily limit of transfer using the USSD code, but since October 2017, Central Bank of Nigeria (CBN) has fixed the general daily limit at one hundred thousand naira (₦100, 000) (CBN, 2017). Each bank has a unique USSD code for transaction. These codes are made available at the banks website. Different banks have different ways of authenticating the user. Some banks may request for the last 4 digits of users BVN, or last 4 digits of the users debit card and personal identification number (PIN). The user is always directed to visit the nearest branch of the bank or call a customer care line provided when password is forgotten. When a user repeats a transaction that has been delayed or interrupted by the network, this could amount to double processing of the transaction (Ayeni, 2017).

Security Issues with USSD banking in Nigeria

USSD banking is more secure than SMS banking due to its feature of not storing details on the user phone. Despite this security advantage, it has lots of challenges raging from GSM lack of end to end encryption to server security policies (Nyamtiga, Sam & Laizer, 2013). There are inherent flaws in the authentication requirements for USSD transactions. From the report published by guardian newspaper (Odita, 2018), some arrested robbers confessed that all that they needed to withdraw money from victims account was the customer's phone number which is on the SIM card. All bank customers have their Bank Verification Number (BVN) linked to their phone numbers. The USSD Dirty code for obtaining BVN number is readily available (Borgaonkar, 2013), which a fraudster will dial using the SIM card to obtain the last 6 digits of BVN number, which is needed to access victims account. In order to reduce the risk mentioned above, CBN has directed that daily limit of transfer using USSD cannot exceed one hundred thousand Naira (₦100, 000) a day. Also any transaction that is above twenty thousand Naira (₦20,000) will require a PIN and a soft token (CBN, 2017). This cannot be said to solve the problem as long as BVN will be used for authentication of amounts below ₦20, 000. In other to implement provision of soft token for transactions above ₦20, 000, some banks in Nigeria, has added keying in the last 6-digits of the debit card after keying in the PIN. This is still a problem to customers who

do not use Debit cards and accounts that do not use Debit card based on the banks policy, such as Diamond Banks', High interest deposit account (HIDA).

The Framework also places emphasis on the need to protect the financial information through end to end encryption, masked PIN entry and strong encryption mechanism to protect the USSD channel. The implementation of these will provide much security for the channel.

Some Bank customers have lost much money through USSD channel once their phone is stolen. This has guided the direction of this research in identifying possible attacks that USSD technology is prone to. Identifying these attacks is a step in the direction of providing solution to USSD issues. This work is aimed at identifying various types of USSD attacks and vulnerabilities.

Various USSD Attacks

Discussed below are various types of USSD technology attacks;

Eavesdropping

This is the capability that an unauthorized person intercepts private communication between authorized users with the aim of stealing data. It is also known as sniffing or snooping attack. Eavesdropping attack carried out at the mobile interface is done through shoulder surfing attack (Van der merwe & Abad, 2003).

Shoulder- surfing

This is an act of eavesdropping users' information through observation or use of camera. The information gotten by the intruder is used to impersonate the target user and/or the network and carry out replay attack (Sector, 2018).

Replay attack

As a primer, a replay attack is an attack where an attacker sniffs data sent by the application and then resends them at a different time with a malicious intent. By misusing the previously exchanged messages between the subscriber and network, an adversary can perform replay attack (Borgaonkar, 2013). This attack is easily carried out in USSD transaction when a mobile device with installed USSD application is in the hands of an adversary and the USSD Application server is unable to authenticate USSD request originator during the fraudulent transaction. The authentication of USSD request originator requires the combination of, Mobile station International Subscriber Directory number (MSISDN), Personal Identification Number (PIN), International Mobile Equipment Identity (IMEI), unique message tracking ID, among others. An adversary can carry out transactions, while the USSD application server believes it is coming from the legitimate user.

Man in the Middle attack

This is an attack whereby the intruder has the ability to eavesdrop, spoof, delete, re-order, replay, and modify signaling and user data exchanged between the users involved by staying in-between the target user and an authentic network (Ramesh, Kifle & Abadi, 2016).

Repudiation

This is an attack where the authoring information of an action has been changed by a malicious user. This becomes possible since there is no mutual authentication between mobile device and Base Station Controller (Borgaonkar, 2013). The legitimate user will deny having authorized such transaction since it did not emanate from the user.

Impersonation

This is a situation where an unauthorized individual gains access to a network and sends signal to the network, in an attempt to make the network believe they originate from the target user (Van der merwe & Abad, 2003).

Denial of Service Attack

This attack occurs at communication and application server backend. The attacker injects numerous service request packets in order to overwhelm the service capability of the server (Bocan & Cretu, 2006). The legitimate user will continue to experience "connection problem" and will not be able to get access to service requested.

Encryption suppression/USSD Redirection

Messages received over the radio interface cannot be authenticated by the Mobile Station (MS). Since encryption is not enabled by the network when USSD transaction is initiated by spoofing the cipher mood command, the intruder uses this weak point to eavesdrop on the target user. The attacker sets up a false BTS and tricks the target user into camping to it (Phipps,Mare, Ney, Webster & Heimerl, 2018). The attacker then connects to the genuine network using personal subscription and subsequently eavesdrops on the target user's transmitted data (Toorani & Beheshti, 2009).

USSD Vulnerabilities

The following vulnerabilities of USSD make it possible for the attacks discussed above.

i. **Weak Encryption**

When customer's sensitive data like, customer account number, credit/debit card numbers, PIN, passwords and beneficiary details (account numbers, balance summary) are not well encrypted, this can open a way for fraudulent transactions (Borgaonkar, 2013).

ii. **Poor handling of USSD Content Error Tests**
Sensitive information about user, service provider and USSD application may be revealed when carrying out Error test on the USSD contents. An attacker quickly captures these details for launching attack.

iii. **Delayed USSD Response Time**
Delivery notifications, transaction success messages and alerts may be delayed or tampered with if the USSD response time is not properly implemented. Valid requests from authentic users should be given a quick response.

iv. **Improper Session Management**
An adversary can carry out fraudulent financial transaction from a victim's mobile phone if the session time out is not properly implemented (Suhas, 2018).

v. **Improper Data Validation in USSD IP Mode Applications**
When USSD IP mode is not properly validated, a fraudster can purposely inject Query into the database and other scripts in user input. The attacker does this so as to use the platform to carryout malicious acts at the database and during user's active sessions.

vi. **User PIN appears in plain text**
When user's PIN is not sufficiently protected, an adversary can capture this information through shoulder surfing, and use it authenticate as customer (Sector, 2017).

vii. **Over the air (OTA) transmission between mobile device and application server**
Unencrypted message sent over the air can be captured by an adversary at any point of attack on the channel (Sector, 2017).

viii. **Lack of two-factor authentication**
Using one factor or no authentication mechanism makes the channel vulnerable to attack. An attacker finds it very easy to capture the sensitive data (Swivel, 2012).

Summary of USSD Vulnerabilities, Threats and Risk

a. **Vulnerability**
This is the weakness in a security program that threat exploits in order to gain unauthorized access.

b. **Threat**
This is anything that has the capability of gaining unauthorized access to a confidential data.

c. **Risk**
This is the negative effect of threat exploiting vulnerabilities.

Table 1 shows the summary of USSD Vulnerabilities, threats and risks.

TABLE I. Summary of USSD Vulnerabilities, Threats and Risk/Attack

Vulnerability	Threat	Risk/Attack
Users PIN appears in plain text	Shoulder surfing (eavesdropping)	Identity theft, Disclosure of Information, replay attacks
Over the air transmission between Mobile Station (MS) and Bank Server	Traffic Interception (eavesdropping)	Identity theft, information disclosure, replay attacks, man in the middle attack
Lack of two-Factor authentication	User Masquerading	Fraudulent transactions, provider liabilities
Poor handling of USSD Content Error Tests	Revealing of customers, USSD application and service providers sensitive data	Sensitive Data theft.
Delayed USSD Response Time	Message modification	Replay attack, fraudulent transactions
Improper Session Management	Replay of transactions	Replay attack, fraudulent transaction
Improper Data Validation (USSD IP Mode Applications)	Flooding the USSD database with meaningless request	Denial of Service attack
Weak Encryption	Message modification, replay of transaction.	Local or server data content theft, theft of service, fraudulent transfer of funds

Conclusion and Future Work

This paper presented various advantages of USSD technology in mobile bank transaction. Ease of use and availability of service anywhere, anytime were among the enumerated advantages. The fact that USSD does not store messages like Short message service (SMS) makes it more secure than SMS. It was also stated that there has been cases of users experiencing fraudulent transaction being carried out on their accounts through USSD channel. The paper showed that various attacks can be launched on USSD channel, which include, shoulder surfing, man in the middle attack, eavesdropping and others. These attacks were made possible by weak encryption of user's sensitive details, improper session management among others. Therefore, identifying these attacks and their causes, will guide researchers in providing solution to these attacks. Hence this paper recommends, combined effort by the stake holders in USSD mobile banking in mitigating various USSD attacks. Future work will show various attack points on USSD channel and their associated attack.

References

Briceno, M., Goldberg, I. & Wagner, D. (1999). "A pedagogical implementation of A5/1". [online].
Available: *http://www.scard.org/gsm/a51.html*.

Emmanuel, A. (2007). "Mobile banking in developing countries: secure framework for delivery of SMS
Banking services" [online]. Master thesis in Radboud University Nijmegen. *Available: https://masalai.files.wordpress.com/2009/03/sms-bank-in-developing-countries.pdf*.

Globitel, (2018). "USSD gateway", [online]. Available: *www.globitel.com/ussd-gateway/*.

GSMA, (2017). " Number of mobile subscribers worldwide hits 5 billion" [online]. Available:*https://www.gsma.com/.../press.../number-mobile-subscribers-worldwide-hits-5-billion*.

Adeputun, A. (2018). "Nigeria becoming mobile first country with 162m subscribers-Jumia" [online]. Available: *https://www.vanguardngr.com/2018/03/nigeria-becoming-mobile-first-country-162m-subscribers-84-penetration-rate-jumia/*.

Gurung, S. (2016). " Data authentication principles for online transactions", Master Theses Submitted to the Department of Informatics, University of Oslo, [online]. Available: https://www.duo.uio.no/handle/10852/50244.

Suhas, D.(2017). "Mitigating security risks in USSD based mobile payment applications", [online]. Available: *www.aujas.com*.

Zhang, F. (2012). "Secure mobile service-oriented architecture". PhD thesis in Communication Systems in KTH Royal Institute of Technology, School of Information and Communication Technology Communications Systems [online]. Available: *http://www.diva-portal.org/smash/get/diva2:527836/FULLTEXT01*.

El-Safi, A.A. (2013)"Mobile banking project", Sudan-faculty of mathematical Sciences, University of Kharthoum, "unpublished". *Masters Thesis.*

Chandran, R. (2014) "Pros and cons of mobile banking" *International Journal of Scientific and Research Publications, 4(10),* Pp. 1-5.

Sanganagouda, J. (2012) "USSD- a potential communication technology that can ouster SMS dependency", *International Journal of Research and Review in Computer Science, 2 (2),* Pp. 295.

Zhou, M., Herselman, M. & Coleman, A. (2015). "USSD technology a low cost asset in complementing public health workers work process" *IWBBIO partII*, LNCS 9044, Pp.57-64, Spring International Publishing Switzerland.

Central Bank of Nigeria (CBN), (2017). "Exposure draft of regulatory framework for unstructured supplementary service data (USSD) for the Nigerian financial system", [online].Available: *https://www.cbn.gov.ng/out/2017/ccd/ussd%20f, ramework.pdf.*

Ayeni, T. (September 4th, 2017). " How to safely use USSD mobile banking service in Nigeria, [online]. Available: *https://kikiotolu.com*.

Nyamtiga, B. W., Sam, A. & Laizer, L.S. (2013). "Security perspectives for USSD versus SMS in conducting mobile transaction: A case study of Tanzania", *International Journal of Technology Enhancements and Emerging Engineering Researches, 1(3),* Pp. 38-43.

Odita, S. (January 25th, 2018). "How bank worker, syndicate use stolen SIM cards to steal millions from Customer account", [online]. Available: *https://guardian.ng/news/how-bank-worker-syndicate-use-stolen-sim-cards-to-steal-millions-from-customers-account/.*

Borgaonkar, R. (2013). " Dirty use of USSD codes in Cellular Networks" Security in Telecommunications, Technische Universitat Berlin, 2013. Available: *https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-Dirty_use_of_USSD_codes_in_cellular-Ravi_Borgaonkor.pdf.*

Van der merwe, P.B. & Penzhorn, W.T. (2003). "Mobile commerce over GSM: a banking perspective security". *Masters thesis*, University of Pretoria.

Ramesh, G., Kifle, B. N. & Abadi, F. A. (2016). "A security protocol for mobile banking and payment using SMS and USSD in Ethiopia", *International Journal of Research and Applications, 3(10),* Pp. 427-433.

Bocan, V. & Cretu, V. (2006). "Mitigating Denial of Service Threats in GSM Networks," Proceedings of 1st IEEE , *International Conference on Availability, Reliability and Security (ARES'06).*

Phipps, R., Mare, S., Ney, P. Webster, J. & Heimerl, K. (2018). "ThinSIM based attacks on mobile money systems. *COMPASS* '2018.

Toorani, A. & Beheshti, A.A. (2009). "Solutions to GSM security weaknesses", *Proceedings of the 2nd International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST08)* (2009), University of Glamorgan, Cadiff, UK, Pp. 576-581.

Sector, S. (2017). "ITUT Focus Group Digital Financial Services: Security Aspect of Digital Financial Services" (2017) [online]. Available: *www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS-SecurityReport.pdf*.

Swivel, (2012)." Two factor authentication and Swivel" Infosecurity Europe, [online]. Available: *www.infosecurityeurope.com/__novadocuments/21950*.