International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July -2016 www.irjet.net p-ISSN: 2395-0072

Enhancing the Security of Money Transfer Services: Case of ARB Apexlink Domestic Money Transfer Services

Bayor Lambert[1] ***Joseph Kobina Panford[2]*** ***James Ben Hayfron-Acquah[3]***
[1]MSc. Information Technology Student, Department of Computer Science, CoS, KNUST, Kumasi, Ghana
[2]Lecturer, Department of Computer Science, College of Science, KNUST, Kumasi, Ghana
[3]Senior Lecturer, Department of Computer Science, College of Science, KNUST, Kumasi, Ghana

---

ABSTRACT- *Going digital has a number of benefits likewise a number of challenges. Two main objectives of this study was to find out the various security challenges facing ARB Apexlink Money transfer services used as the case study and also find out the remedies to the security challenges. The nature of the study necessitated the use of technical (Metasploit, Nmap, Nessus) and non-technical (observation and interview) to engage and collect data from the various systems and respondents. Upon completion of the study, it was identified that the transfer service is faced with a number of ports, operating system, Internet explorer and other application software challenges. Most of the vulnerabilities that were identified could be fixed by updating the operating system and upgrading the applications involved. Also it was identified from Metasploit console that there are a number of modules that could be used to exploit the identified vulnerabilities.*

Key Words: **Security, Apexlink Domestic Money Transfer Services, i-tranz, Metasploit**

1.INTRODUCTION

The World Bank (via MIDA), the International Fund for Agricultural Development (IFAD) and the African Development Bank started up and financed a project (Rural Financial Services Project, RFSP) in Ghana. The project sought to promote growth and cut down or completely eradicate poverty in the rural areas. One aim of the project is the provision of Information Technology support to automate the operations of rural and community banks and ensure that the process of handling data is efficient and will result in quality customer satisfaction.

With a successful implementation of the project Rural and Community Banks (RCBs) now offer both domestic and international money transfer services. ARB Apexlink is a domestic money transfer services which enables the transfer of money from one community to another using the network of rural/community banks [1].

1.1 Problem Statement

Advances in information processing and communications technologies, in particular, have fundamentally changed the nature of Apexlink domestic transfer services by influencing the manner in which these services are created, delivered, priced, received, and used. However, according to [1] financial institutions often have questions about the security of the software they use for their transactions especially money transfer services. [2] Also argues that though Computerized Money Transfer service (CMTs) has impact on cash management, the relationship is weak sending an overall negative signal to the stake holders and management that CMTs alone cannot fully manage institutional cash.

The need for financial institutions including RCBs which use CMTs such as the Apexlink domestic money transfer service to fully secure their data and transactions cannot be overemphasized. This study therefore sought to enhance the security of money transfer services, a case of ARB Apexlink domestic money transfer services used by RCBs in Ghana.

1.2. Research Questions

1. What are the security challenges facing ARB Apexlink domestic money transfer services of RCBs in Ghana?
2. What are the remedies to the identified challenges?

1.3. Objectives

1. Identify the security challenges facing ARB Apexlink domestic money transfer services in RCBs of Ghana.
2. Provide remedies to the identified challenges.

1.4. Significance

The study findings will help banks in Ghana, especially Rural and Community Banks to adopt more secure ways of domestic money transfer services since this is about security. The study to a large extent will help unveil certain hidden security challenges affecting Apexlink domestic money transfer services of Rural and Community Banks in Ghana and provide some remedies to help improve services of Apexlink Domestic Money Services.

2. LITERATURE REVIEW

2.1. Definition of Money Transfer Services and Security

Money Transfer Services can be explained as the kind of services where money or funds can move from one place to another with the implementation of several methods, [3]. [3] Claim that this approach is fast, reliable, and very easy to handle; with this approach funds can be transferred all over the world without any stress. According to [4], protecting the reliability of Funds Transfer systems and the information stored in them from unlawful or unapproved access and use is termed as security of a money transfer service. Security issues surrounding Funds Transfer systems are very important to the public and it is usually a major policy issue because of how it is being used, in comparison with other payment systems.

2.2. Software Security in Money Transfer Services

According to [5] Software security is explained to mean the implementation of mechanism to safeguard the software against harmful attacks and other hacker threats in that the software will continue to work properly during such attacks/threats. Security is needed to ensure authentication, integrity and availability. Any compromise to these three factors makes the software unsecure.

System flaw is a weakness that permits an attacker to decrease the assurance of a system's information. Vulnerability involves the combination of three things: a system flaw, availability of the flaw to an attacker, and the attacker's ability to abuse the flaw. To successfully exploit the vulnerability by an attacker, there must be at least one tool that is designed to break the system through the flaw.

A report by [6] stipulates that the design of a secured system must provide protection against the various types of vulnerabilities and these vulnerabilities fall into two major categories:

Accidental Disclosure: This is a failure of software, equipment, components, or subsystems that result in the revelation of some data or the abuse of the elements of the system.

Deliberate Penetration**:** this is a thoughtful and underground attempt to (i) access data enclosed in the target system, (ii) manipulate the system to function in such a way that will be to the benefit of the menacing attacker, or (iii) operate the system with the aim of rendering it inaccessible to he authentic user.

2.3. Security of Data in Money Transfer Services

According to the 2014 Data Breach Report of Verizon, databases are one of the mostly compromised assets. They are targeted so often because at the heart of any organization is their database which is for storing records of customers and other confidential business data. Very important information that moves over a network can be secured by encryption. Encryption is a powerful security mechanism because it can make decryption mathematically infeasible if you do not possess the decryption key". According to [4], encryption by itself can protect the confidentiality of information, but other techniques are still needed to protect the integrity and authenticity of information.

2.4. Authentication in Money Transfer Services

According to [8] Authentication is the process of identifying and proving the identity of a user who tries to send a message or gain access to data. Authentication requires users to answer the question, "Who or what are you?" It is on record that authentication can protect resources.

According to [8] there are approaches to using an automated authentication system. The security scheme usually require of the user to supply some form of information that is secret to only the user. Some combination of other methodologies can be merged as well. The first approach as in password is the classical approach. The second approach, asking for some personal belonging such as a voter identification card has a key problem, since what is recognized by the security system is not the user in person but the properties. The third approach, recognizing some attributes that are exclusive for the user, is known as biometric security and it tries to get around the earlier problems mentioned.

2.5. Hardware Leakage Points

[6] Reports states that hardware parts of systems are prone to failures that can lead directly to a leak or result in a failure of the mechanisms that are used to protect other parts of the system, which include software failure. Also, operating equipment is prone to tapping devices or being exploited. There are forms of malfunction that affect the security mechanisms directly. The failure of any hardware portion can possibly disturb security controls.

2.6. Organizational Leakage Points

According to [6] there are two principal organizational leak points, institutional operating procedures and at the workplace so that confidential personnel security clearances. Personnel security clearances concern the administration, structure and mechanism

of the organizational apparatus that are used to grant personnel security permissions. It is however acceptable to have satisfactory standards and techniques that could be used by the authority to guarantee the trustworthiness of those who are cleared. This does not however discharge the system designer of the massive responsibility to include methods that reduce the effect of harm that can happen by a malicious individuals who are working from the inside of the secured working environment. On the contrary, any terminal may be used to perform any duties. These duties must be subject to the clearance, needs and restrictions of that person at that moment of installations.

2.7. Meatware or "Human Factor" Security in Money Transfer Services

Techopedia Dictionary defines Meatware as the human entities that operate or use a computer for any computing process. The term is conceptually used to define the human side of a computer and reflects the computer's dependence on something much more, organic-humans. According to [9] sophisticated techniques make it difficult for antimalware tools and researchers to find, analyze and detect malicious code. Humans are the weakest link through extensive use of social engineering, trying to trick people into doing something that undermine their security. In many cases the wrong behaviours of users; the failure to comply with security policies and lack of awareness targets the system, expose the confidentiality, integrity, availability. The most effective methods are phishing scams that designed to disclose information such as usernames, passwords, personal identification numbers, and other information. People are not only weak because of unawareness.

2.8. Location and Personnel-Based Security

Data could be kept on offsite servers if accounting is offered as a service. This requires that there should be security measures information is safeguarded in the clients' workplace and offices of the service provider. According to [9] another significant factor to be considered is the social characteristics of staff who get involved with the process of inputting, storing, and accessing information. He included that staff of the software provider must partake in information security training so as to know about protocols that are required to deal with private financial information. He also added that, staff of the financial institution must also receive training so as to be able to handle delicate accounting information. This can involve learning the signs and symptoms of possible online security threats, how to create strong passwords and how to store them, and how to safely logout of systems.

2.9. Privacy in Money Transfer Services

Privacy may be interpreted as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [10]. According to [8] there exist four types of privacy: territorial privacy, information privacy, communications privacy, and bodily privacy. Information privacy is the kind of privacy that involves the capacity of an individual to regulate information about one's self. Privacy intrusion occurs when individuals are not able to conserve a significant level of control over their personal information and how they are used. According to [11], many threats exist in fund transfer, like data transaction attacks and abuse of personal and financial information, breed security threats.

3. METHODOLOGY

3.1. Study Population

ARB Apex bank and the RCBs can boast of having over 600 employees. The study population is made up of all RCBs in Ghana.

3.2. Type of Study

The study was a case study of enhancing the security of ARB Apexlink domestic money transfer services. This approach involves procedures and techniques of investigating into and understanding the dynamics of a particular system. It has been adopted because it is the best approach for the study of contemporary issues and in situation where the boundaries between the phenomena and context are not clearly evident as it is with the case of the Apexlink Transfer Services in Rural Banks and the security of money transfer services. In order to describe the research area and the components used in this study, the descriptive research was adopted. The purpose of using this descriptive research is to give oral appearance of the materials and techniques used.

3.3. Sampling Technique and Sample Size

The study used various sampling techniques to aid in the collection of data. These included the convenience sampling and purposive sampling techniques. With convenience sampling, the RCBs were selected because they were accessible for the study. Respondents were purposively chosen simply because they were the right people that can provide the required responses for the

study. All the necessary materials, systems, devices, respondents involved and the reports generated by this study are with respect to the sampled RCBs.

3.4. Data Collection Methods

With the nature of this study, numerous data collection methods (technical and non-technical) combined were used in order to produce a comprehensive report. The technical data collection method enabled collection of data from the systems being used. The non-technical methods allowed the researcher to gather information from experts and professionals (staff) in the case. These methods were observation, interview and document analysis which allowed the researcher to interact with the meatware, hardware and some software considered to be relevant to the study.

3.5. Data collection tools

The tools used in collecting data for this study included:

1) **Metasploit:** It was used extensively to detect the security flaws in the systems of the transfer service. In this study, msf console was the chosen style for accessing the Metasploit framework.
2) **NMap ("Network Mapper"):** is a free utility that is used for network discovery and security assessment. In this study Nmap was ran from the Metasploit console. It comes with massive flexibility, power and portability [12].

Nessus: It tests the target for a variety of vulnerabilities and gives a comprehensive report on it. This code was executed

msf>db_connect
msf3:8b826ac0@127.0.0.1:7175/msf3
msf> load nessus

Aside the above stated tools observation checklist and interview guide were also used for the purpose of this study.

3.6. Data Processing and Analysis

There was the need to process and analyze the data collected during the administration of the interview guide and observation checklist. Quantitatively, items on the interview checklist were entered and coded in Microsoft office excel statistical software. Using Excel, the data was then set out according to the responses. This led to the generation of frequencies for each variable. Responses which do not have any bearing on the variables were discarded. Based on the data collected, multiple correlation analysis was performed using SPSS to detect the relationship between the individual variables and the number of vulnerabilities (security issues) identified on the systems of the RCBs.Qualitative techniques were also used to assess people's perceptions regarding the security challenges of Apexlink Domestic Money Transfer Services. This involved a description of the responses gathered from the observation checklist and the drawing of the implication and conclusion. This is in conformity with the aim of qualitative analysis as in the opinion of Punch.

4. ANALYSIS AND INTERPRETATION OF RESULTS

4.1. Findings from Technical Tools

The scope of the study was defined to include three IP addresses and the vulnerability testing was specified not to be in-depth. The various identified vulnerabilities were explained and document analysis was used to state, explain and validate the severity and possible exploits. The source of the documents to be analyzed was National Vulnerability Database (NVD) of United States and the exploits available in the form of modules in Metasploit were shown and explained.

4.1.1. Information gathering using Nmap tools

By typing **msfconsole** at the terminal, the Metasploit framework was activated and ready to be used. Nmap is incorporated into the Metasploit framework and can be used together with a number of parameters (-sT, -sS, -sU, -sA).

TCP Connect

```
msf > nmap -sT -p1-10000 xxx.xxx.xxx.001

[*] exec: nmap -sT -p1-10000 xxx.xxx.xxx.001

Starting Nmap 5.51SVN (http://nmap.org ) at 2016-02-19 17:03 IST

Nmap scan report for xxx.xxx.xxx.001

Host is up (0.0058s latency).

Not shown: 9997 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

MAC Address: 08:00:27:34:A8:87

Service Info: OS: Windows
```

Figure -1: TCP Connect (-sT) scan report

Figure 1 is the report of the TCP connect scan with the –sT parameter. The –p parameter is the range of ports intended to be tested by the scan. This scan revealed a number of opened ports and their associated running services. It also revealed the MAC address as well as the operating system type. The ports were scanned from 1 to 10000 and it revealed that ports 135, 139 and 445 were opened.

Table -1: Opened ports and services running on the target machines.

IP Address	Port	State	System	Service
xxx-xxx-001	21, 22, 80, 135	Open	Windows	ftp, Ssh, http, msrpc
xxx-xxx-002	22, 80, 139	Open	Windows	Ssh, http, netbios – ssn
xxx-xxx-003	20, 22, 80, 445	Open	Windows	ftp, Ssh, http, Microsoft-ds

From table 4.1, the IP addresses of target machines were obtained and scanned to identify opened ports and running services. The first target had four ports opened and four services (ftp, Ssh, http, msrpc) running on each port. The second machine had three opened ports and three running services running of those ports. The third target machine had four opened ports and four running services. All the three target machines were using Windows operating system.

4.1.2. Discovery and assessment of Vulnerability phase

Table -2: The number of vulnerabilities found on the target machines.

IP Address	High	Medium	Low	Total
xxx-xxx-001	4	2	0	6
xxx-xxx-002	1	0	0	1
xxx-xxx-003	3	1	0	4
Total	8	3	0	11

Table 2 indicates the identified vulnerabilities and their severity (High, Medium, and Low). Eleven total vulnerabilities were identified as a result of the penetration testing. Eight of the identified vulnerabilities are flagged as high, three were medium. Table 3 stipulates the identified vulnerabilities, target systems, severity level and the number of IP addresses the vulnerability was found on. It also shows whether there is a patch for it or not and whether is a known publicly available exploit that could be used to capitalize on the vulnerability. Typically it is in table 3 that the vulnerability found the Window operating system which became public in 2014 titled CVE-2014-0262 ranked as high in terms of severity and existed on two out of the three target systems. There was a patch for this vulnerability and also there was a publicly known exploit which is available in Metasploit framework.

Table -3: Identified vulnerabilities in OS, IE, Firefox and Flash

S/N	Vulnerability	System	Severity	IP Address	Updates	Exploit
1	CVE-2014-0262	OS	High	2/3	Yes	Yes
2	CVE-2015-1701	OS	Medium	1/3	Yes	Yes
3	CVE-2015-1756	OS	High	3/3	Yes	No
4	CVE-2015-1716	OS	Medium	3/3	Yes	No
5	CVE-2015-1645	OS	High	2/3	Yes	No
6	CVE-2009-3270	Explorer 7	Medium	3/3	No	No
7	CVE-2007-1114	Explorer 7	High	3/3	No	No
8	CVE-2015-5119	Adobe flash	High	3/3	Yes	Yes
9	CVE-2014-4114	OS	High	3/3	Yes	Yes
10	CVE-2012-1889	Explorer 9	High	2/3	Yes	Yes
11	CVE-2011-5164	OS	High	3/3	No	Yes

CVE-2014-0262

This vulnerability is found in the operating system kernel drivers in Microsoft Windows 7 – wind32K.sys. It gives normal users more privileges through an application that is crafted. This crafted application is referred to as "Win32k Window Handle Vulnerability". The vulnerability allows information to be disclosed, modified in an unauthorized manner. It also allows services to be disrupted. Using the CVSS version 2.0, this vulnerability is considered as high with a score of 7.2.

CVE-2015-1756

This vulnerability is termed as "Microsoft Common Control Use After Free Vulnerability" which is found in Microsoft Common Controls in Windows 7 SP1, Server 2012 and more. It lets remote attackers who get assistance to execute a random code through web site or web links that are specifically crafted and calls the F12 Developer Tools feature of Internet Explorer. Although the victim must interact with the website, web link or the linked contents before the attacker can be successful. It is kind of hard on the part of the attacker if the victim does not access the crafted file.

CVE-2015-1645

This vulnerability allows random codes to be executed through specially crafted random code called Enhanced Metafile (EMF). It is also known as EMF Remote Code Execution Vulnerability".

CVE-2007-1114

In Microsoft Internet Explorer 7, the child frames receive the default charset from the parent window. This happens when a value for the charset is unspecified in an HTTP Content-Type header or META tag. As a result of this, remote attackers get the permission to perform what is called cross-site scripting (XSS) attacks, which is confirmed by the UTF-7 character set.

CVE-2015-5119

This vulnerability exists in the Byte Array class that can be found in the Action Script 3 (AS3) that is executed in Adobe Flash Player versions of 13.xxx to 13.0.0.296 and also 14.xx to 18.0.0.194. It allows remote users to run a random code and as a result can cause denial of service attack through flash materials. The security strength of this vulnerability is critical and as such all the versions on the target machines must be updated to the latest version of at least the version that can solve the problem.

CVE-2014-4114

This vulnerability allows remote users or hackers to run a random code through specially designed OLE object in a document. It allows publicly know malicious program called "Sandworm" to penetrate the operating system. It is also known as Windows OLE Remote Code Execution Vulnerability".

CVE-2011-5164

This vulnerability is found in VanDyke Software AbsoluteFTP 1.9.6 through 2.2.10 as a result in overflow in stack-based overflow. This vulnerability allows the execution of random code on FTP server through a specially created file name in LIST command response.

4.1.3. Possible Exploitation on CVEs

CVE-2014-0262 was one of the vulnerabilities identified in the Windows operating system. The severity of the vulnerability was high and the problem affected two out of the three target machines. The update intended to fix this flaw is found in update version 2839984 in MS13-101 and so attempt was made to check if the update existed on such machines. It could be identified in figure 2 that the update developed to fix this flaw was not found in the list of updates. If it existed, it would be directly under the selected update in figure 1. Once the update is not downloaded and installed, the CVE-2014-0262 security flaw still exist and the Mestaploit module in the exploitation phase could be used to exploit the target machine. The consequences could be very fatal depending on the attacker's intention.

CVE-2015-1701 was also found to be a flaw in the operating system. This flaw only existed in one target machine. The severity level is medium. It was also identified that the flaw could be fixed by applying the 3034344 in MS15-023 update. The vulnerability affected only one out of the three target machines. As a result the available update was traced to find out if it existed on the secured machines. The update exists and for that reason the two machines were considered to be safe when it comes to the CVE-2015-1701 vulnerability. But the one without the update is vulnerable and the Metasploit module could be used to exploit that target.

CVE-2015-1756 security flaw affected all the three target machines and the severity level is high. The update to fix this flaw was found in 3051768 in MS15-054. The update needed to patch the CVE-2015-1756 security flaw found in the Windows operating system has not been downloaded and installed. There was no publicly known exploit (module) that could be used to manipulate the systems on which this flaw was found.

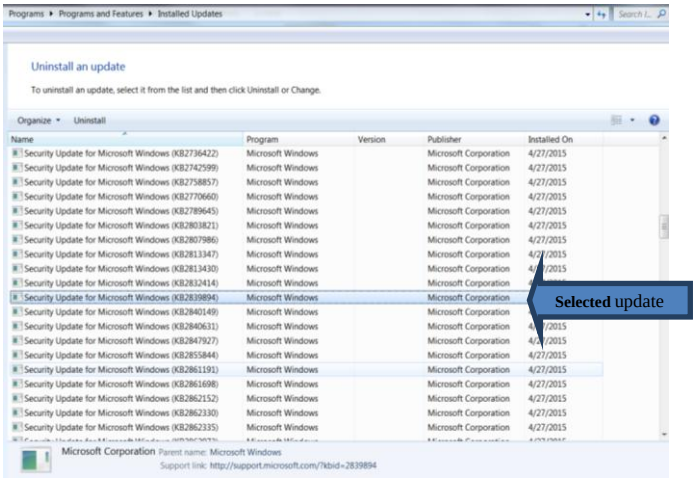

Figure -2: Checking for installed patch for CVE-2014-0262

4.2. Findings from Non-Technical Tools

4.2.1. Findings from Observation

- Verification / Authentication of Staff

It was observed that the authentication method used by all staff especially those in charge of ARB Apexlink transfer services was password. These are generated by the Information and Communication Technology (ICT) unit of ARB Apex Bank National. This password is a combination of alphabets and figures which can be used for at most three (3) months. Within the 3 months a staff who forgot the password, have been reassigned or replaced by other staff will have to call the ICT unit for the password to be changed or replaced. Calling the national ICT center is fraught with consequences which include delays in resetting the password. As a result of the hassle associated with password issues, staff who have the tendency of forgetting their passwords are forced to write their passwords down (diaries, other documents). Password theft is a serious concern worldwide among system users who write their passwords and usernames down.

- Firewall and Antivirus use and Update

All machines of the RCBs observed have firewall protection and antivirus installed on them however some machines antivirus software had not been updated for at least forty days. Antivirus and firewall updates are recommended to happen at most seven days. Potential attacker can take advantage of the flaws found in the operating system and other software and exploit the vulnerability by by-passing the outdated rules of the antivirus and firewall. It was also realized that when installing new machines there was no checks for malware and viruses or possible backdoors created with the believe that all devices begin their lives completely safe, but become less secure as time goes on. This actually is not true. There are reported cases when so many devices come with vulnerable adware like Superfish pre-installed on them.

- Continuity of Physical Protection

It was also realized that the RCBs do not have their equipment and associated materials (e.g., media containing copies of programs) used for handling classified information continuously protected against unauthorized change to commensurate with the security level at which they most recently have been certified.

- Database Audit Trail

The RCBs turn to native audit tools provided by their database vendors or rely on adhoc and manual solutions. These approaches do not record details necessary to support auditing, attack detection, and forensics. It was realized that the Critical Patch Updates (CPU) release on 12th February, 2016 and 19th April, 2016 have not been applied.

- System ability to Adapt to Security Controls

It was observed that the system is adaptable so that security controls can be adjusted to reflect changes in the classification and sensitivity of the files, operations, and the needs of the local installation. There is a convenient mechanism whereby special security controls needed by a particular user can be embedded easily in the system. Because it would be too costly to treat each installation as an individual instance and to conceive an appropriate set of unique safeguards, the security control problem ideally is solved with generality as stated by one of the staff.

4.2.2. Findings from Interview

Out of the thirty respondents, five were I.T. persons. Table 4 summarizes the number of respondents and their fields.

Table -4: Respondents and their fields

Field	Number
I.T.	5
Accountant	5
Manager	4
Accounts reconciliation officer	3
Cashier	10
Project officer	3
Total	**30**

- Number of I.T Persons in each RCB

The first RCB had one I.T. person, the second RCB had three I.T. persons and the third RCB had only one I.T. person as shown in table 5. In table 8 the correlation

analysis suggest that there is a strong inverse relationship between the number of vulnerability and the number of IT persons in the RCBs, however the coefficient of -0.918 is not significant.

Table -5: Number of I.T Persons in each RCB and the number of vulnerabilities

RCBs	I.T Persons	No. of vulnerabilities
1	1	6
2	3	1
3	1	4
Total	**5**	**11**

Source: researchers field survey, 2016

- Number of Security workshops organized in each RCB

It was identified that the first RCB had not organized any security related workshop for its staff for the past years of active operation. The second RCB had organized three (3) security related workshops and the third RCB had organized one (1) workshop as shown in table 6. The correlation analysis in table 8 shows that there is a strong inverse relationship between the number of vulnerabilities and the number of security workshops organized, however the coefficient of -0.918 is not significant.

Table -6: Number of Security Workshops in each RCB and the number of vulnerabilities

RCBs	Number of Security Workshops	No. of vulnerabilities
1	1	6
2	3	1
3	1	4
Total	**5**	**11**

Source: researchers field survey, 2016

- Required Knowledge level of Staff in I.C.T.

Table 7 shows the responses of respondents on their level of knowledge in I.C.T. In the first RCB 8 respondents said they do not have basic knowledge in I.C.T, 3 respondents in the second RCB and 3 in the third RCB. The coefficient of 0.803 from the correlation table in table 8 suggests that if an RCB has more of the staff without basic I.C.T knowledge, there will tend to be more security vulnerabilities; however the coefficient is not significant.

Table -7: Respondents' response on their level of I.C.T. knowledge

Bank	Yes	No	No. of Vulnerability
1	2	8	6
2	7	3	1
3	1	3	4

Table -8: Correlation Analysis

		NO OF VULNERABILITY	NO OF I.T PERSONS	NO OF SECURITY WORKSHOPS	NO OF STAFF WITHOUT KNOWLEDGE IN I.T
NO OF VULNERABILITY	Pearson Correlation	1	-.918	-.918	.803
	Sig. (2-tailed)		.260	.260	.407
	N	3	3	3	3
NO OF I.T PERSONS	Pearson Correlation	-.918	1	1.000**	-.500
	Sig. (2-tailed)	.260		.000	.667
	N	3	3	3	3
NO OF SECURITY WORKSHOPS	Pearson Correlation	-.918	1.000**	1	-.500
	Sig. (2-tailed)	.260	.000		.667
	N	3	3	3	3
NO OF STAFF WITHOUT I.T KNOWLEDGE	Pearson Correlation	.803	-.500	-.500	1
	Sig. (2-tailed)	.407	.667	.667	
	N	3	3	3	3

**. Correlation is significant at the 0.01 level (2-tailed).

4.3. Summary of Main Findings

4.3.1. Research question one

What are the security challenges facing ARB Apexlink domestic money transfer services of RCBs in Ghana?

- The CVE-2014-0262 security flaw found in the Windows operating system which allows local users to leverage administrative privileges pertains to two out of the three target

machines. The severity is high. Update and exploit exist for this vulnerability.

- Also the CVE-2015-1701 vulnerability that existed in Win32k.sys in the kernel-mode drivers in Windows 7 which allows users to get access to the system was found on only one of the three target machines.
- Again CVE-2015-1756 also existed on all the three target machines. This vulnerability has patch but there is no publicly known exploit.
- CVE-2009-3270 and CVE-2007-1114 has no updates to fix them. Also they do not have updates to patch them.
- RCBs do not have enough qualified experts to handle I.T related matters and for that matter security issues take longer time to be addressed.
- The staff are verified by the system through the use of password which has some handling problems that could lead to inappropriate safe keeping.
- Installed antivirus software on devices are not updated regularly
- New devices are not checked thoroughly to be sure they are safe from virus infections, superfish or existence of backdoors.
- Equipment and associated materials used for handling classified information are not continuously protected.
- The RCB relies on native audit tools to perform database audit which come with a number of challenges.
- Flash drives are used by staff to share files within the outside the bank.
- The system does not automatically provide records to the system administrator to effectively monitor user activities.

4.3.2. Research question two

What are the remedies to the identified challenges?

- It has been identified that most of the security loop holes found while using the technical tools (Metasploit, Nmap and Nessus) can be fixed by updating with the right update. Apart from CVE-2009-3270 and CVE-2011-5164 the rest could be fixed by downloading and installing the right patch.
- The RCBs should employ more (at least two) highly qualified I.T. persons to handle the affairs of I.T related issues in the bank. If the RCBs cannot afford to pay monthly salaries, then they can outsource most I.T. related works to trusted companies. This would help if the security levels of the bank would be abreast with the standards.
- There should be a delegation of system privileges that would allow the I.T. person in the case bank to work on password related issues. This would help reduce the number of hours it takes to solve a password problem.
- Since attackers are always working on the clock to find new security flaws in systems, antivirus and firewall companies are also constantly developing access and security rules to counteract the effects of malicious activities. As a result of this the antivirus and firewall updates on the target and other machines should be done regularly.
- The ARB national should employ more staff to work on i-Tranz 2.0 problems especially update problems. This will ensure that reported problems are solved within time.
- Since most attacks are triggered with the download of malicious files, staff must be prohibited with serious sanctions from accessing other websites with corporate network and PCs especially downloading files from untrusted websites.
- Flash drive usage must be limited. Even if at all, such drives should be scanned or reformatted to ensure that only malicious free drives are used in the bank.
- It was realized that most of the staff do not have basic I.C.T skills and as such the bank could organize in-service training in the form of workshops for staffs. This will ensure that they know their way out of the system to download and apply updates for their computers, antivirus and firewalls.

3. CONCLUSIONS

The banking field is a service field. They provide a lot of services to their clients and customers. The computerization of this sector has helped in a lot of ways including the ability to transact funds transfers. However, there are a number of security challenges that pertain to the transfer service. The servers, operating systems, application software, human factors and others seem to have a challenge. This study has uncovered some of the challenges of the systems used at the bank and the problems with staff with the aim of helping to improve on the security of the domestic money transfer service. The study has also concluded

that there is direct relationship between the number of vulnerabilities (security issues) and factors such as the number of I.T personnel in an RCB, the number of workshops on security held and staff knowledge level on I.C.T. The tremendous growth in the Internet and electronic money transfer services has therefore brought about a lot of serious security challenges to the network. Many of other practical attacks on such money transfer systems have been identified with procedural vulnerabilities listed as one of the main challenges.

REFERENCES

[1] Ajai and Azeb (2010), Rural Banking: the Case of Rural Banks in Ghana. Retrieved from: www.documents. Worldbank.org

[2] Bitwababo A. (2011), Computerized Funds Transfer and Cash Management. Retrieved from: eropository.uonbi.ac.ek>handle>Agen

[3] Imperva (2013) Application Defense Center Retrieved 2016-3-26 from: www.imperva.com/DefenseCenter

[4] Bellare M. (2000) *Entity Authentication and Key Distribution* - Computer Science Retrieved 2016-3-11 from: https://cseweb.ucsd.edu/~mihir/papers/eakd.pdfR. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] RAND, (2015). System Vulnerabilities, Retrieved 2015-12-15 from: www.rand.com

[6] Open Data Alliance (2013). Data Security, Retrieved 2016-04-15 from: https://opendatacenteralliance.org/docs/Data_Security_Framework_Rev1.0.pdf

[7] Convery S. (2004), Authentication and Authorization Controls. Retrieved 2015-12-6 from: www.cisco.com>press>101-aaa-part1

[8] Davies C. (2006), Information Privacy, Retrieved 2016-5-3 fromwww.researchgate.net/ profile/Heng_Xu6/publication/220260183_Information_Privacy_Researh_ An_Interdisciplinary_Review/links/543157530cf29bbc12789742

[9] Robert R. (2008), Computer and Information Security. Retrieved from: https://books.google.com.gh>books

[10] Alan Westin (2007). Social and Political Dimensions of Privacy. Retrieved From: onlinelibrary.wiley.com › ... › Journal of Social Issues › Vol 59 Issue 2

[11] Chan J. (2004). Essentials of patch management policy and practice. Retrieved 2016-5-10 from: http://www.patchmanagement.org/pmessentials.asp

[12] Wolfgang M. (2002), Host Discovery with Nmap, (available online http://www.dtic.mil/bin/GetTRDoc?AD=ADA406645, accessed on 29/06/2016.)

[13] Nair and Fissha (2010) Ghana's Rural Finance System and Climate Regime Retrieved 2016-2-26 from: www.bu.edu/.../Capstone-2010-A-Ghanas-rural-finance-system-and-climateregime