A literature survey on ELECTRONIC BANKING security issues

Maureen Grace W, David Kiragu N, and Patrick Ngumi
Internet resources have made business life quite interesting to businesses and their customers. Banks have also enjoyed the fruits of computing revolution for the past couple of years. Every success comes with a set of challenges and electronic banking for banks has posed several security threats to system developers, banks and customers or users. There are many security threats which have presented themselves over time while at the same time solutions to counter the threats have been sought through investments in research and development. This research paper reviews empirical and general literature on the various threats and their proposed solutions. After the literature review the paper concludes that despite the challenges facing e-banking, there are enough good reasons to continue improving online banking along other electronic delivery channels. Online banking continues to present operational and financial advantages to banks and hence banks should be in the forefront in support and funding more research and development on security measures for improving the authenticity of e-banking.

**Key Words:** e-banking, internet security, online banking, vishing, phishing

**INTRODUCTION**

Internet has continued to provide a versatile platform for business entities to offer their services to customers in a convenient manner. The revolutionary and transformative approach to business activities have been enabled through internet based solutions. In the world of business, banks have not been left behind in the adoption of computing related solutions to their businesses. Electronic banking is one of such ICT adoption that has empowered banks towards taking their services and profitability to a higher notch. However, this good success has not come without challenges and one of the biggest headaches to system developers, banks and customers are the system security threats that can easily eroded banks’ reputation and customer confidence (Ganesan and Vivekanandan, 2009).

The rise of many technological capabilities has led to the development of many product offerings which and have improved operational efficiency of banks. These successes have led to possibilities of technology misuse. Electronic banking is neutral and can be used in the ways that most of us would consider beneficial, as well as in ways that are harmful. Many users of electronic banking are hesitant to use the system due to the fear of system security. Electronic banking security issues have brought many concerns from government, businesses, banks, individuals and technology experts (Hertzum, Jorgense and Norgaar, 2004).

According to Leyden (2004) security issues come in different forms and types of online attacks. Online attackers exploit known weaknesses of some operating systems. They also make unauthorized entry into websites during a short time frame thus denying service to other customers. Breach of security could result in direct financial loss to the bank. This could arise when hackers access bank servers, retrieve and use confidential customer information. The security threat may arise from internal sources like employees or externally from ‘professional’ hackers.

**Types of E-banking Security Threats**

Electronic banking security issues present themselves in form of threats. The following section discusses various
e-banking threats and how they occur.

Botnets
A botnet is a large network of fictitious personal computers that are centrally controlled from a server. The hijacked computers are added into the network and controlled using internet relay channels. According to Mirkovic (2005), crackers can assemble very many botnets. For example, in Norway it was found to have at least 10,000 zombie computers which were being controlled by use of a remote server. Leyden (2004) asserts that globally, the Internet has many botnets. Markoff (2004) reported on 20 September 2004 in the New York Times, that the number of botnets increased from less than 2,000 to more than 30,000 during first six months of year 2004 and they were monitored by Symantec. Markoff (2004) argues that Symantec also saw a dramatic increase in e-commerce attacks during the same period.

Phishing
This is also sometimes called credential harvesting. This is an attack meant to approach a victim and convince him to provide their online banking personal details to an unknown person. This mostly happens where the hacker impersonates details which appear like the original set of details. The hacker normally gathers the details from a genuine login making it hard to differentiate a hacker from a genuine login. The user is cheated by use of a fake email message and he ends up providing personal and private login credentials. The emails contain a convincing message that should trick the recipient into visiting the spoofed web site and revealing his log on credentials. The use of the e-banking link is cheated into a fake internet link which harvests all his login details and the hacker then afterwards takes control of the customer account (Laerte, Marcelo, Bernardo, Flavio and Rafael, 2011).

Vishing
This is a method used by hackers by calling the e-banking account holder. The hacker makes a call to the customer and looks genuine and the customer is tricked into disclosing his account login details. The hacker then quickly gets to the customer account to conduct his malicious account manipulation. Some hackers have even converted into using VOIP calls and international lines to make the call look more genuine. Automated calling systems used by some banks can be used by hackers to trick customers to disclose personal identifications and they are eventually used by the hackers (Markoff, 2004).

Hardware Key Loggers
According to Anderson (2001), this method uses a data capturing device which is set at the back of the computer and between the keyboards. This is mainly used to monitor the character inputs on the keyboard. This method is mainly used at public outlets like cyber cafes. The keyboard input is monitored and then used to hack online customers systems. This method can also be used by hackers who have access to computers of senior officers of a bank who may have approval powers or have access to premium customer accounts.

Domain Name System (DNS) Cache Poisoning
According to Ollmann (2005), this refers to diversion internet traffic or search to a fictitious website. Ollmann (2005) cautions that even typing the URL address by hand in the browser might lead to a malicious site. This method of attack is sometimes referred to as pharming or DNS hijacking. In pharming, the attacker changes the URL when a customer is online and then capturing then the IP address is copied making it possible for the attacker to take control of the user computer.

Secure Sockets Layer (SSL) Encryption
A Trojan (......) is used to capture information entered into web forms before it is encrypted by SSL and sent to the financial institution. The Trojan drops a DLL and registers it as a browser helper object (BHO) within Microsoft’s Internet Explorer. When a customer visits particular websites, the Trojan creates a pop-up window which encourages the user to fill in the logon details. Once the data is input in the Trojan generated window then it is not encrypted (Deepshikha and Devanand, 2009).

Shoulder Surfing
Shoulder surfing involves a hacker observing and noting what a computer user is inputting from the keyboard. The hacker notes that PIN of a card before steal it the physical card for conducting the intended card fraud. A more sophisticated variant uses closed-circuit television to observe the PIN. This is mainly for targeted victims whom the hackers are well known to (Herzogl and Shahmehri, 2007).

Hybrid attacks
Nothing limits an attacker to only one type of attack. For the attacker the most successful methods are hybrid attacks that combine strategies from both local and remote attacks. The attacker can use sniffing which involves monitoring the network monitors. This method uses software to capture keystrokes from a particular PC. There is also guessing of passwords by using software to test all possible combinations to gain entry into a network. Random dialling technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack. Social
engineering involves the attacker calling the bank’s help
desk impersonating an authorized user to gain
information about the system including changing
passwords Hämija and Tygar, 2005).

Suggested Solutions to Security Concerns
To ensure that the benefits of e-banking are not eroded
by the work of hackers, several methods and
mechanisms have been proposed to ensure secure e-
banking systems.

Enhanced System Architecture and Design
Williamson and Money (2006) assert that appropriate
system architecture and control is an important factor in
managing various kinds of internet operational and
security risks. A bank continuously faces the risk of
having chosen systems that are not well designed or
implemented. A case in point, a bank is faced with the
risk of an interruption or reduced speed of its existing
systems if the electronic banking or electronic money
system it chooses is not compatible with user
requirements. Several banks normally outsource to
external experts when implementing or servicing their e-
banking activities. Outsourcing such services may look
desirable due to the economic sense it brings on boards
but reliance on outsourcing exposes a bank to
operational risks. Service providers may not have the
required expertise to deliver services expected by the
bank, or may fail to update their technology in a timely
manner.

Operations of service providers could be interrupted
due to system breakdowns or financial strains leading to
the danger of bank’s ability to deliver products or
services. The speed and rate at which information
technologies are changing poses a major problem to
banks and can even lead to system obsolescence and
eventually can ground the bank’s e-banking services.
This therefore calls for banks and bank providers to
continually upgrade softwares in order to avoid system
security challenges that present themselves with aged
technology. The softwares should also be upgraded from
authentic sources because it can pose the risk of hacking
from links that present fictitious software upgrade links
which end up corrupting the systems and stealing crucial
information (Ganesan and Vivekanandan, 2009).

SMS challenge code
This is a two level authentication method. The customers
logs on to his account using his name and then the
system sends a verification code to his mobile phone.
The code is sent via SMS and it is entered as a second
level login verification. This code is a temporary
password. This two-factor authentication works fine and
is quite convenient for most users. One major advantage
is that most users already have a mobile phone and
therefore no extra hardware may be used or may be
necessary during the process. This method calls the
users to ensure security of their mobile phones,
otherwise, hackers can get access to the phones and
pretend to be the real account users and they could end
up using the verification code to access the account for
malicious transactions (Solanki, 2012).

Image verification
The PassMark system, a software for image verification
was introduced by the Bank of America in 2005 (Riess,
2005). The system is based on a shared secret between
the bank and the user, consisting of an image and a
verification phrase. When the customer logs to the
system he supplies a system ID and an image appears
on the screen. The image is known to him as his
verification identity. The customers are required to login
only when they see their known picture and when they
have verified the login credentials. This method should be
used carefully because the hackers can also capture the
screen details of the user and divert the login to the
wrong IP address and then to the wrong website mainly
using phishing (Hiltgen, Kramp and Weigold, 2005).

Dynamic Security Skins (DSS)
DSS is an extension of image verification approach and
was introduced by Dhamija and Tygar (2005). A
photographic image chosen by the user is transparently
overlaid on web forms that include sensitive information
prompts. In addition a “visual hash” which can be seen as
a unique graphical pattern, is overlaid as well. The visual
hash is tied to the secure session and changes with each
session. This makes it impossible for an attacker to feed
a cheating pop-up that is identical to the password
prompt. In dynamic security skins the whole spoofed web
site is contained in one legitimate SSL session and the
attack would be the same as for image verification
protection. The limitation of this method comes when
hacker manages to penetrate the authentication process.

Public Key Infrastructure (PKI) based hardware token
A Trojan can steal the private key and PIN for a PKI
based software token. Therefore tamper resistant key
storage must be used to ensure high security. According
to Hiltgen et al.(2005) smartcards with external smartcard
reader devices are the most recommended solution for
this kind of weakness. Hiltgen et al.(2005) proposed a
two- stage; smartcard PKI based implementation of such
a solution. There is storage of pre-generated key pairs
and certificates on a tamper proof smartcard. The PIN
code is used on the external device keypad to unlock the
key vault in the smartcard. This means that a key logger
is not able to intercept the PIN code. A signed Java
applet which is downloaded from the bank’s web site
communicates with the card reader on one side and with
the bank on the other. This enables the applet to authenticate itself against the card reader. The card reader also generates a common authenticated SSL channel from the bank server when signing login into a session occurs. This assists to eradicate human interventions in the process and prevents most forms of impersonation.

4: Conclusion
As discussed in the prior sections, e-banking has become an integral component for offering services to customers. Due to this continued importance the numbers that use e-banking in the world are soaring. E-banking has even been taken to the smart phones and ipads. The phone is more personalised than the use of public cyber cafes for accessing online banking and therefore bank customers should be encourage to use such more secure channels and hardware. One obvious advantage of e-banking is its twenty four hour capability. It is also able to reduce queues in the banking halls, conduct high volume of transactions and can be used even in remote locations. All these advantages have made hackers to gain interest on how to access financial information of the users. Banks and systems developers will need to continue improving the versatility of online banking resources to enable banks secure the confidence required from their customers.

The major challenges arising from Internet banking is mainly security and safeguarding of information exchanged between customer and bank. System developers have an ongoing challenge to make online banking reliable by ensuring systems that have timely detection and prevention of intrusions. There should also be continued investment in research and development to ensure that hackers are not ahead of the game of developers. It is also wise for all users of internet banking to appreciate that like any other system whether manual or electronic, online banking has its own weaknesses and risks and hence the need to be cautious and diligent when using such delivery platforms. Developers eventually need to venture into security authentication systems that use biometric methods which help to narrow the incidences of impersonation.

REFERENCES