International Journal of Engineering and Mathematical Sciences
January – June 2018, Volume 13, Issue – 1, pp.47 – 53.
ISSN (Print) – 2319 - 4537, (Online) – 2319 - 4545.

IJEMS

Evaluation of Guidelines for Security threats in Mobile-Phone Banking

[1]Ngomeh Augustine Wafula Prince, [2]Kelvin KabetiOmieno, [3]Samuel Mbuguah
[1,2,3]Department of Information Technology
[1,3]Kibabii University, P.O. Box 1699-50200, Bungoma, Kenya
[2]Masinde Muliro University of Science and Technology, P.O. Box 190-50100, Kakamega
[1]pawngomeh@kibu.ac.ke, [2]komieno@mmust.ac.ke, [3]smbugua@kibu.ac.ke

Abstract

Globally, banking institutions are using mobile phones to provide financial services to reach those with or without bank accounts. However mobile phones do suffer from security threats when used for banking purposes these threats become more critical. The purpose of the research was to investigate the use of user guideline as a tool to mitigate against security threats in mobile phone banking. The objectives of the research were to determine the security threats in the mobile banking, to identify the existing guidelines in mitigating threats in mobile phone banking and to design improved user guideline to minimize the security threats in mobile phone banking. This research adopted a descriptive survey design; Qualitative approach was used in objective two which was concerned with subjective assessment of attitudes, opinions and behavior. Generally, the technique of focus group interviews and depth interviews was used in identifying the use of existing guidelines in mitigating mobile phone security threats. In objective three Simulation approach was used, which involved the construction of an artificial environment within which relevant information and data can be generated. This permitted an observation of the dynamic behavior of a system (or its sub-system) under controlled conditions. Data collection tools included use of interviews and questionnaires. Descriptive statistics was used in data analysis that included frequency percentage mean and mode. This research was expected to provide improved user guidelines that will help in the reduction of the security threats posed in mobile phone banking. The research was expected to further suggest the challenges of the existing guidelines in use to those of adoption of the designed use guidelines.

Keywords: Mobile Phone, Banking, Security, Threats, Guidelines.

Introduction

Mobile phone banking is a term used for performing balance checks, account transactions, payment credit applications and other banking transactions through a mobile device such as a mobile phone (Herzberg A. , 2003). mobile phone banking has the potential to extend financial services through virtual accounts to millions of poor people globally, utilizing mobile phone technology for micro finance significantly lowers transaction costs while expanding outreach to rural areas it enhances mobility, portability efficiency and availability (Cracknell, 2004) as a result a lot of security threats have come up like the services may from time to time be un available due to system maintenance or circumstances beyond control such as mobile carrier outages, loss of phone, errors or damage caused to the mobile phone as a result of using ATM cards, virus , a client suffers as a result of relying on information obtained via mobile phone banking service (Mallat, 2004) But as consumers use their

phones for banking, shopping and more, there are even more malicious forces interested in that data and other information on your handset.

Problem Statement

Mobile phone account holders transact details like funds transfer, bill payment, share trade, check order and also inquiries like account balance, account statement, check status, transaction history and so forth. It means that the account holder is interacting with the files, databases of the bank. Database at the server end is sensitive in terms of security. Customers distrust mobile devices to transfer money or for making any transactions. The problem is that security is a major concern for the customer's fulfillment as customers continue losing money despite having the existing guidelines in place, there is need to evaluate the existing guidelines in place and design a use guideline incorporated with the existing guidelines to help in reducing mobile phone security threats in mobile phone banking.

General Objectives

The purpose of the research is to investigate the use of user guidelines as a tool to mitigate against security threats in mobile phone banking

Specific Objectives

i. To determine security threats in the mobile phone banking industry.

ii. To identify the existing guidelines in mitigating threats in mobile phone banking system

iii. To design improved user guideline for minimizing the security threats in mobile phone banking system

Security Threats Brought By Mobile Phone Banking System

Handset operability: There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. Lack of common technology standards for mobile banking.

Malware: Software that's designed to be harmful. It can be configured to steal information from your phone, or give an attacker some control over the handset to, say, send spam text messages to everyone on your contact list. It's often hidden in games and other apps, so download only from well-reviewed, trusted developers.

Spyware: Software that collects phone data such as call history, text messages, location, contact lists, emails and camera pictures. The phone's owner is usually unaware. Read the fine print before downloading to see what data the app wants access to.

Privacy threats**:** Applications that you know collect or use sensitive data from your phone, like your location or personally identifying information. Some apps are open about using such data for marketing purposes, which is something to consider before you download.

Vulnerable applications: Apps that contain software vulnerabilities attackers might exploit to access information that app has collected from your phone, or remotely take control of the phone. Developers typically offer updates or patches to negate security threats, so make sure your phone's software and apps are up to date.

Phishing scams: These are attacks designed to trick you into providing log-in information or other personal information. Attackers send links in emails and text messages that redirect users to web pages designed to mimic legitimate businesses, often banks. Avoid clicking on links in emails, and look for telltale signs like misspellings.

Drive-by downloads: Downloads that begin automatically when a user visits a web page. You're usually lured there by spam or advertising, so be careful where you click.

Browser exploits: These are attacks that take advantages of vulnerabilities in a web browser or supporting software. Make sure your phone's software is up to date.

***Network exploits*:** These take advantage of flaws in your phone's mobile operating system. There's nothing you do that triggers it. Just hope your provider has a good security system in place.

Wi-Fi sniffing: Attackers intercept data from apps and web pages that is sent unencrypted. Be cautious about what you do on your phone, and check that apps or sites for mobile banking are both encrypted and secure.

Lost or stolen devices: Both the phone and the data are valuable these days. Protect your phone with a password and other security measures. The iPhone, for example, has a setting to automatically erase all data on it after ten failed password attempts.

SQL injection (SQLi) is an application security weakness that allows attackers to control an application's database – letting them access or delete data, change an application's data-driven behavior, and do other undesirable things – by tricking the application into sending unexpected SQL commands.

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application

Existing Guideline to Mobile Phone Banking Security Threats

Fraud monitoring

It monitors how and where your card is being used. More importantly, Total Security Protection blocks potential fraud if unusual patterns are detected.

Secure technology

Fraud prevention and security systems protect you with latest encryption technology and secured email communication.

Select intricate passwords

Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, a series of consecutive numbers, or a single word that would appear in a dictionary. Combinations of letters, numbers, and special characters make the strongest passwords. When opening new accounts, you may find that many businesses still ask for your mother's maiden name. Find out if you can use a password instead.

Verify a source before sharing information

Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact and are sure you know who you're dealing with. Identity thieves are clever, and may pose as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

Research Methodology

Research Design

This study adopted a descriptive survey design. It was concerned with determining the security threats in the mobile banking; Information is collected by interviewing and administering a questionnaire to a sample of individuals. Qualitative approach to research was used in objective two which was concerned with subjective assessment of attitudes, opinions and behavior. Generally, the techniques of focus group interviews, projective techniques and depth interviews were used in identifying the use of existing guidelines in mitigating mobile phone security threats and the security threats that came about after employing mobile phone banking, In objective three Simulation approach was used.

Research Results and Discussions

This chapter discusses the research results and main findings. The study shows that 80% of the respondents used mobile banking service and 70% experienced mobile banking security threats , the type of security threats experienced included ,poor network, transaction delays , malware ,spyware virus , phishing scams , driven by downloads , lost or stolen devices , browser exploits , wifi sniffing , network exploits , vulnerable applications and privacy threats

The study showed that 65% of the respondent do not understand the security settings their mobile phones.

The findings reveal that 85% of the respondents were not provided with the user guidelines and privacy statement and for those provided with the user guidelines and privacy statement rated satisfactory rate of the existing guidelines and privacy statement as follows very high 5%, high 10%, medium 20%, low 25% and very low 40%. The findings reveal that 70% of the respondents stated that the existing guidelines and privacy statement does not address the technical, non-technical, theory related and practice related security threats

A descriptive statistics was employed to analyze the data provided by the respondents on the security threats on mobile phone banking. It was found out that majority of users do not understand how to configure mobile phone banking security. In addition users will always leave mobile banking on after transacting thus posing their information and data at risk. In addition, the mobile banking security architecture has weakness on the authentication authorization and encryption technique. Basing on this outcome improved user guidelines was developed by suggesting on how the security threat in

the authentication, authorization and encryption can be improved. User's lack of knowledge was a key weakness and it was also addressed. The section below provides a procedure on how the proposed user guideline was developed.

Authentication and authorization

In this regard it was established that the weakness found in mobile phone banking security architecture need to be improved. The main weaknesses were weak authentication, encryption and authorization. In authentication and authorization, only the device is authenticated and not the user. To improve authentication and authorization, application layer security should be employed to provide additional security measures. Employing application layer security limits the mobile phone devices to connect automatically whenever it is on a network.

Encryption

To achieve proper encryption AES and DES encryption techniques should be used to provide proper encryption and decryption. In the guideline, instead of the E0 encryption currently being used, AES algorithm, known for of its higher efficiency in block encryption should be used for data transmission and DES algorithm should be used for the encryption of the AES key due to its key management advantages. Thus the dual protection using AES and DES algorithm will make the data transmission using Bluetooth more secure. Use of such strong encryption will enhance security in mobile banking.

Policy

From data analysis from the respondents, it was evident that users of mobile banking lack knowledge on how to configure these devices. Majority will leave them on after use not a aware of the risks they posing the information they have stored in these devices. At some extend developers of these devices do not include user guideline and the risks of using such devices. Thus in order to improve on user awareness, a policy should be provided to users. The policy should include device configuration guidelines, security policies, and enforcement mechanisms for the use of mobile banking. They should provide an adequate level of knowledge and understanding for the users. Users should understand the security policies that address the use of mobile banking devices and their own responsibilities. The developers should include awareness based education to support user's understanding and knowledge of mobile banking security. Policy documents should include a list of approved uses for mobile banking, and the type of information that may be transferred over networks. The security policy should also specify a proper password usage scheme. Most users do not pay attention while assigning strong pass codes because most of them are not aware of the proper techniques.

Proposed user guidelines for security in mobile Banking

The above detailed results was combined together to a achieve a secured mobile banking user guidelines shown in the figure below.

Source: Author, 2018

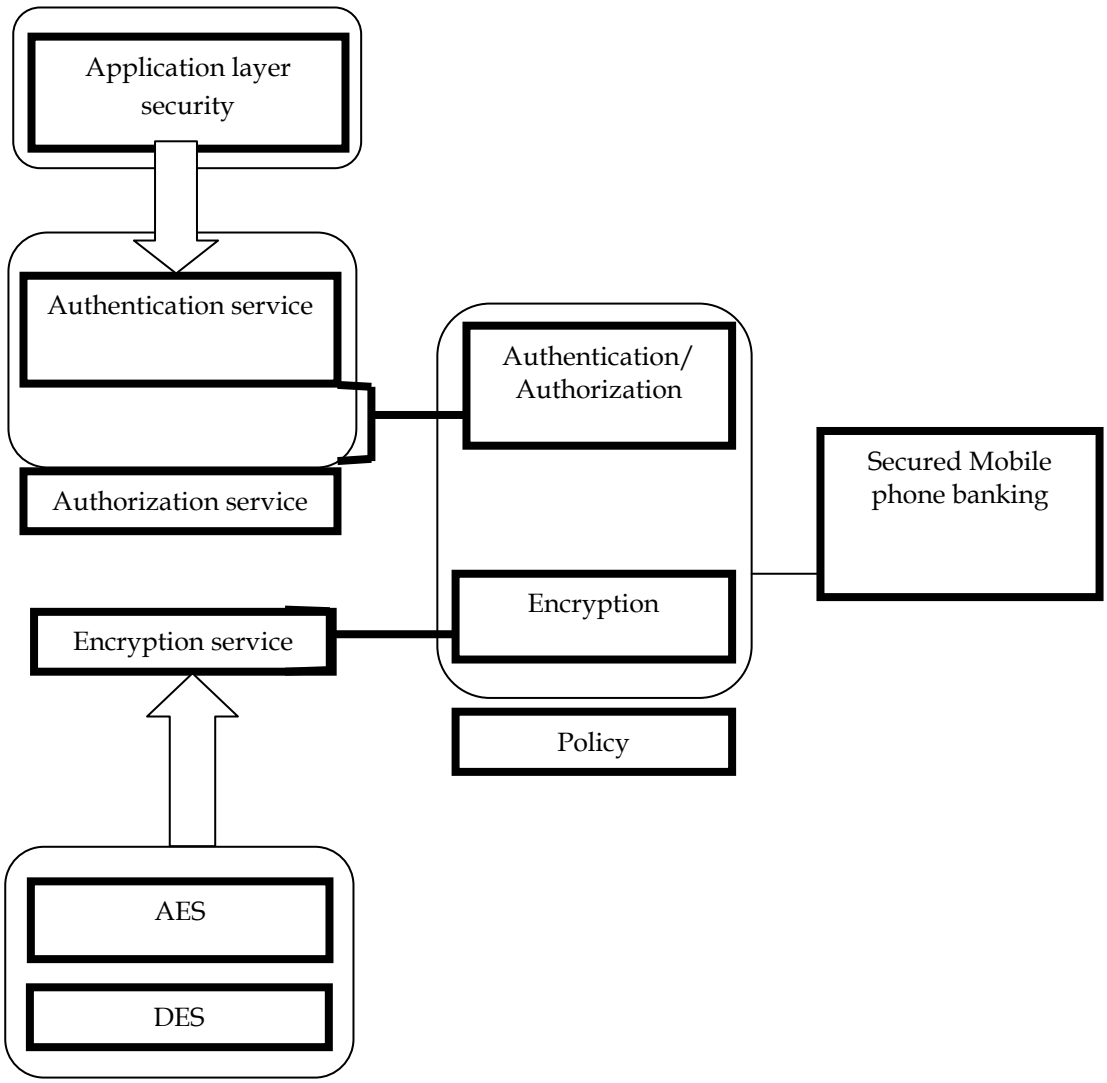

Figure 1.0 Proposeduser guidelines

Conclusion

The results of this paper indicate that mobile phone banking users face a number of challenges in relation to securing information and data held in their mobile phones. This study presented an overview of some of the weakness of mobile phone banking security architecture and how this weakness has led to major attacks thus posing security threats to user information while having the existing guidelines in place. The first research question sought to determine the security threats brought by mobile banking. This was answered through results from descriptive statistics questionnaires and the interview questions. The second research question sought to identify the existing guidelines and how they help in mitigating the mobile phone banking security threats. This was answered through descriptive statistics and the interview questions. The last research question

sought to design an improved user guideline in cooperated with the existing guidelines to help in mobile phone banking security threats reduction basing on the answers for the first and second research questions. This was answered through analysis of the findings of the first and second research question that lead to the design of an improved user guideline

Recommendations

Mobile phone banking security threats can be mitigated by an understanding of the technology, strong security policies, enforcement of the security policies, strong system/node configuration guidelines, and strict adherence to those user guidelines. Thus Mobile banking security guidelines should be included in the phone manual to help the user understand the settings.

References

1. Bartlett. (2001). Determining Appropriate Sample Size in Survey Research. Organizational Research, 43-48.
2. Cawley. (2013). Regulation and the development of mobile and broadband services. Research and innovation, 2-4.
3. Chandrasekar. (2016). Internet Security Threat Report. Mountain View, CA 94043 USA: Symantec.
4. Dr.Debashis Chakraborty. (2012). Validity of the instruments. Validity of the instruments, 4-8.
5. Fidgen. (2016). Risks of mobile banking. Android is fraudster's heaven, 1-10.
6. GauravGarg CR Kothari. (2014). Research Methodology. JALPUR: NEW AGE INTERNATIONAL (P) LIMITED PUBLISHERS.
7. Grant. (2011). THE GROWTH OF MOBILE MALWARE. Mobile Threats, 3-10.
8. Herzberg. (2003). Mobile Banking Systems and Technologies. Mobile banking services, 1246-1247.
9. Lasser. (2012). Understanding customer-specific factors underpinning internet banking adoption. International Journal of Bank Marketing, 1-10.
10. Lee. (2003). Trust and Technology Acceptance on mobile banking. Mobile Banking, 1-2.
11. Lin, L. a. (2005). An Empirical Investigation on Consumer Acceptance of Mobile Banking. Business and Management Research, 32-33.
12. Litan, G. (2011, July 1). Mobile banking and payments. Online Banking Security, p. 1.
13. Mallat, R. &. (2004). Mobile Banking Services. Communications of the ACM, 1-6.
14. Mugenda&Mugenda. (2003). Research Methods. Nairobi: Focus publisher ltd.
15. Mugenda&Mugenda. (2013). RESEARCH METHODS. Nairobi: Focus Publishers Ltd.
16. Muhammad Bilal, G. S. (2011). Bio-metric Trust and Security in mobile banking. International Journal of Advanced Research in Computer Science and Electronics Engineering, 81-85.
17. O' Leary. (2006). Analysing Research Methodologies. Science & Education , 607.
18. O'Reilly. (2012). Push technology. server push, 1-2.
19. Patton. (2002). Qualitative evaluation and research methods. Designing Qualitative Studies, 169-181.
20. Sia, K. C. (2012). pull technology. client pull, 2-4.