Form 2

Dissertation Abstract

Report no.	(Course-based) No. 1244	Name	Tej Narayan Thakur
Dissertation title	Modeling of Secure Mobile Banking System in E-Banking (オンラインバンキングにおける安全なモバイルバンキングシステムのモデル化)		

Abstract

※The abstract should be in keeping with the structure of the dissertation (objective, statement of problem, investigation, conclusion) and should convey the substance of the dissertation.

Mobile banking system is an electronic channel for E-Banking (Electronic banking) that provides banking services and products to banking users on their mobile devices. In the modern digital world, mobile users are increasing day by day and wish to have all the enhanced banking services on their mobile devices because of the ease of use of mobile technologies. At the same time, they are afraid of using the mobile banking system because of the growing phishing attacks. In addition, secure mobile banking systems providing enhanced banking services are solutions to fulfill the requirements of mobile banking users. The main objective of this research is to develop secure and enhanced models for mobile banking system to increase the use of mobile banking in E-Banking.

In this thesis, to increase the use of mobile banking systems, we have the following five problems: (i) phishing attacks in the mobile banking system at application installation level, (ii) phishing attacks in the mobile banking system at authentication level, (iii) phishing attacks in the mobile banking system at transaction level, (iv) unavailability of enhanced banking services in the mobile banking system and (v) unavailability of enhanced banking services in the branchless banking system. Moreover, we propose practical solutions to the mentioned problems to increase the use of the mobile banking system.

In the first problem, we study the phishing attacks during the installation of the mobile banking applications to start mobile banking. Mobile banking users receive phishing emails/SMS from phishers, follow the links, download phishing apps, and install phishing apps. To solve the first problem, we propose an anti-phishing model to mitigate phishing attacks at the application installation level.

In the second problem, we look at the phishing attacks during the input of login credentials to authenticate in the mobile banking system. Mobile banking users install phishing apps and input the login credentials in phishing apps for authentication. To solve the second problem, we propose an anti-phishing model to mitigate phishing attacks at the authentication level.

In the third problem, we notice the execution of fraudulent transactions in the

mobile banking system. Mobile banking users provide the login credentials in the phishing apps or phishing login interfaces unknowingly. In this way, phishers steal the login credentials from mobile banking users using phishing apps or phishing login interfaces. They employ the stolen login credentials to execute fraudulent transactions. To solve the third problem, we propose an anti-phishing model to mitigate phishing attacks at the transaction level.

In the fourth problem, we consider the unavailability of enhanced banking services in mobile banking. Mobile banking users do not have enhanced banking services such as cheque clearing, lending, etc. in the mobile banking system. To solve the fourth problem, we propose a contactless mobile banking system to deliver enhanced banking services to the mobile banking users.

In the fifth problem, we consider the unavailability of enhanced banking services in the branchless banking system. To solve the fifth problem, we propose a hybrid model of mobile banking based branchless banking system to deliver branchless banking services as well as enhanced banking services to the unbanked people of rural areas. Moreover, we used SPIN to verify our proposed models and our experiments verified the proposed models to use them in the real banking world.