ISSN:2321-1156
International Journal of Innovative Research in Technology & Science(IJIRTS)

A STUDY ON IMPROVED FRAUD DETECTION METHODS IN THE MOBILE MICRO PAYMENT SERVICE

Eunyoung Choi, KISA; Youngsang Shin, KISA; Taejin Lee, KISA

Abstract

The increase in the number of smart-phone users due to the mobilization of the internet has led to an environment in which a great variety of services based around the mobile phone is being developed and distributed. Micro payment services are being actively used because of their convenience, but unfortunately there are many shortfalls in terms of security. Together with the popularization of the micro payment method, text messages containing advertisements and other contents have been used for the Smishing of users' personal information in financial scams. As such, some methods have been proposed to resolve the issue, but they have been inappropriate solutions for the rapidly changing IT environment. The purpose of this paper is to propose an approach for enhancing methods of fraud detection in the mobile micro payment services.

I. Introduction

Smartphones are commonly being used as a medium of financial payment, such as mobile banking and on/offline payment, due to their ongoing popularization [12] and the rapid development of mobile communication services. Smartphones can be utilized for numerous financial purposes such as mobile banking through bank/card mobile applications and smart phone micro payment services. Mobile micro payment services that enable the users to take care of payments by inputting their birthdate and mobile phone number instead of any other financial information are being actively used among many other mobile services because it is their convenience. However, a character that smartphones can be installed many applications without scanning malware have generated security vulnerabilities. Especially, a Smishing attack mainly occurs in this services. Smishing (SMS+phishing), which was named by McAfee[13], occurs when a smartphone user click a web site link in text messaging[8]. But Smishing methods have evolved together with the advance in IT technology. It can be prevented by telecommunication companies offer text filtering services that warn the users of potentially harmful content if the text contains suspicious URLs or if the sender's number is included on a blacklist. However, these methods might not be very effective in preventing Smishing, considering IT technology environments.

Credit card companies and banks have developed and are now utilizing fraud detection technology to block or prevent irregular transactions, and fraud detection technology has become an area of particular interest for credit card companies. More recently, research has begun based on data mining and machine learning[1,10]. However, the mobile micro payment services lack similar research and development for the area of fraud detection.

This paper is consisted as follows. In Section 2, we introduce the micro payment service environment together with its security weaknesses and the attack patterns observed in the service. In Section 3, we present general fraud detection methods in the banking industry, and then we propose a developmental strategy for a method of fraud detection in the mobile micro payment service in Section 4. Finally, we conclude in Section 5.

II. Explanation of the mobile micro payment service and analysis of security threats

In this section, the definition and mechanism of the mobile micro payment service as well as the details of potential attack patterns will be presented.

A. Mobile Micro Payment Service

The main elements of the mobile micro payment service are the user, the telecommunications company, and the payment agency. The system operates as shown in Figure 1.

Users who wish to buy a product use their mobile phone number as the payment method by obtaining certification from the telecommunication company for the payment agency (PG).

The service is used according to the following procedure:

1) A user begins the payment process at the site in which he/she chooses to buy a product.
2) The site's payment method provides the user with the payment screen of the payment agency.
3) The user inputs his/her birthdate and mobile phone number.
4) The payment agency uses the information provided by the telecommunication company to identify the user. If the user is successfully identified, the telecommunication company sends the payment agency a success message. If the identification process fails, a failure message is sent.

5) The payment agency forwards a verification code or requires an additional identification process or finishes the process.

① If the telecommunication company successfully identi fies the user and the process is cleared through the fraud detection system within the payment agency, a verification code is forwarded to the user.

② If the payment agency's fraud detection system finds the transaction abnormal, the service is terminated even if the telecommunications company approves the transaction.

③ Even if the telecommunication company successfully identifies the user and the fraud detection system clears the process, an additional ARS voice verification process is requested if it is suspected to be abnormal.

6) The user inputs the verification number he/she has received into the payment screen.

7-9) The payment agency verifies the verification number.

- If the verification number is correct, the payment agency will request payment to the telecommunication company. The telecommunication company then adds the payment to the mobile bill.
- If the verification number is incorrect, the payment process stops.

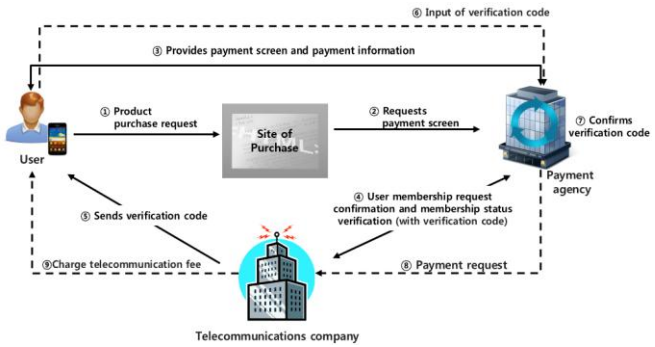

Figure 1. A process of mobile micro payment service

The fraud detection method is applied in step 5 of the process. In this process, the IP black lists, and phone numbers that users previously identified as having made illegal micro payments are used to prevent abnormal transactions or to request additional verification processes.

B. Security Threats

The payment of the mobile micro payment service process is completed upon completion of the payment agency after the user has inputted the verification code. Due to the operational structure of the service, it is exposed to two types of attacks on the system.

(i) Smishing method

Smishing is a compound word consisting of SMS and phishing. This term refers to attacks made based on the SMS service.

First, the attacker creates a malicious application that can leak personal information such as phone number, financial data, and so on. The attacker then sends text messages to smartphones that contain the URL to install the application. The user clicks on the URL and downloads the malware code.

The malicious software sends the mobile phone user's personal information to the attacker's server. The attacker then utilizes the information received through the application to purchase products. The verification code sent to the user of the phone is transmitted to the attacker through the application without the user noticing. The attack method is as illustrated in Figure 2 below.

In this way the attacker can purchase items on the internet without the mobile phone user noticing. While the user remains completely unaware of that is happening, the user can extract personal information and use the information to inflict financial losses.

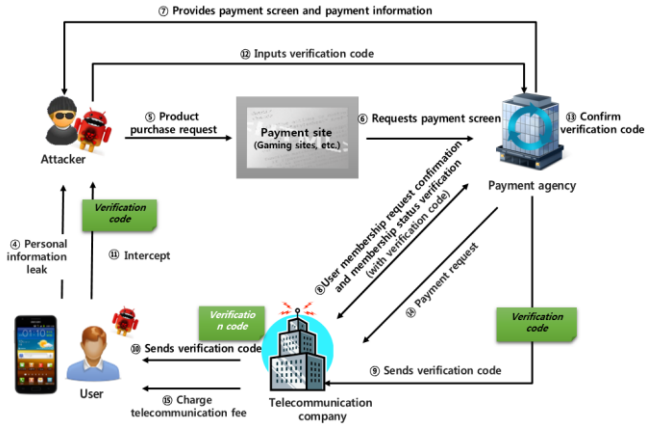

Figure 2. A Smishing attack process in the mobile macro payment service

(ii) Voice communication method

The attacker sends an SMS stating that 'purchase will be authorized' and leads the owner of the mobile phone to call the attacker. The attacker simultaneously inputs the user's personal information into the internet site in which the purchase will take place. The attacker asks the user to repeat the verification code sent by the site in order to 'cancel the purchase' while actually using the information to make the purchase.

The voice communication method is a relatively new method, while the Smishing method is the more common attack method. Although the mobile micro payment service uses various methods of fraud detection, it has difficulties identifying threats because the correlation between the malicious application and the payment information is hard to identify.

III. Fraud Detection System (FDS)

In this section, the function of the fraud detection system used by credit card and banking services in order to detect financial fraud will be explained.

The Fraud Detection System (FDS) is a system that uses a comprehensive list of information such as mobile device information, IP address, transaction record, etc. to detect abnormal transactions and to prevent financial fraud. The fraud detection system consists of the following four functions: information gathering, analysis and detection, response, and monitoring/surveillance[11]. A structure of Fraud Detection System is shown in Figure 3 below.

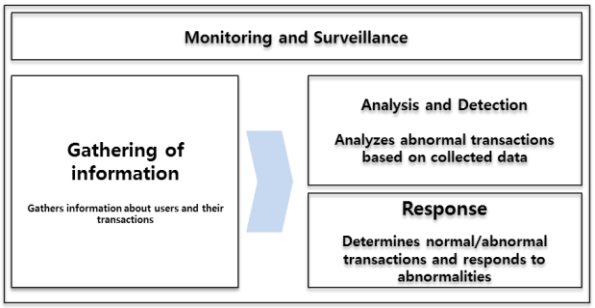

Figure 3. Structure of Fraud Detection System

The details of each of the functions are as follows:

- Information gathering function: This function gathers information on the user media environment and types of fraud to improve the accuracy of the fraud detection system.
- Analysis and detection function: This function analyzes the information gathered by user type and transaction type, examines the relationships and patterns between the collected data, and uses the information to detect any abnormal transactions.
- Response function: This function takes such actions as terminating a transaction according to the result of the analysis.
- Monitoring/surveillance function: This one overlooks the entire process of the fraud detection system and keeps on eye out for potential threats to the system.

The information gathering and analysis/detection functions are crucial to the accurate detection of fraud.

(i) Information gathering function

Through this function, the FDS gathers information on the user media environment and the various types of fraud.

- User media environment information: Using a collection program and/or a plug-in technique, information of the environment (hardware, OS and application information, network information) of the media being used to access financial services (PC, smartphone, etc.) is collected and used to detect abnormal patterns.
- Information on various types of frauds: This collects information provided by related agencies as well as information on abnormal financial behavior, and uses such information to detect abnormalities during financial transactions.

(ii) Analysis and detection function

This function utilizes the information collected to identify fraud. The detection method is divided into two models, namely the misuse detection model and the abnormality detection model.

- Misuse detection model: This model uses previous patterns of misuse to detect fraud.
- Abnormality detection model: This model identifies what action is not likely to take place in a financial transaction in order to detect fraud. Data mining can be used as a method of this function.

IV. A Proposal of an approach to advancing the fraud detection function in the mobile micro payment service

This section is aimed at advancing the fraud detection function that takes into account the environmental characteristics of the mobile micro payment service.

The existing methods of fraud detection rely on previous accidents and the information obtained from such events (such as IP addresses, mobile phone numbers, etc.), and are therefore not fully capable of detecting new types of abnormal transactions. Additionally, mobile micro payment services are usually made with the use of a smartphone infected with malicious applications, a fact that will need to be taken into consideration in further studies.

A. Development of information gathering technology

Currently, banks and credit card companies are collecting information from mobile devices, OS versions of the payment device, manufacturers' information, and network information. The current mobile micro payment service requires the payment site to state the payment price and time

of usage, while requiring the user to input his/her mobile phone number, date of birth, and IP information. However, the current information required to utilize the micro payment service is insufficient to collect information for fraud detection. Therefore, it is necessary to develop a technology capable of gathering and exploiting more varied types of information.

The types of technology that could be developed are as follows:

- **Plug-in type**: A standard payment software (which is used for the macro payment services) can be utilized to gather information.
- **Distribution of programs**: The user installs a program in the process of using the mobile micro payment service which gathers information.

Based on this technology, it is possible to identify the payment pattern of the users in order to use the information for fraud detection. For example, the additional items of information required are as follows:

- **[Location Information]** : Information on the location where a payment is being processed needs to be collected. By gathering information on where a user's payments usually take place, it is possible to detect deviations from the usual location.

- **[Device Information]** : Information on whether a user is accessing a micro payment service through a PC or mobile phone in person needs to be collected. With this information, it is possible to identify the payment pattern of the user so as to detect deviations from the norm.

Additionally, information on malicious applications relating to mobile micro payment fraud needs to be collected.

To that end, a technology for collecting and analyzing information on Smishing SMS and malicious applications needs to be developed.

- **Gathering of Smishing SMSs**: By collecting Smishing SMSs, it is possible to comprehend the trend of Smishing SMSs used to distribute malicious applications. By sharing information on such a trend, it is possible to reduce the installation rates of malicious applications.

- **Gathering/analyzing malicious applications**: It is possible to gather information on the attacker by gathering information on the distribution routes of the malicious application, the IP used to extract users' information, and the e-mail and location of the attacker used in the production of the malicious application.

- **Correlation analysis:** Information (mobile phone number) on users who inadvertently install a malicious application after receiving a Smishing SMS can be used as additional information to detect cases of financial fraud. For instance, if a telecommunication company registers the number of a user who has received a Smishing SMS and installed a malicious application to pass on to the payment agency, the agency can use this information to create a blacklist for future reference.

Based on the collection and analysis of additional information related to payment information and malicious applications, it is possible to detect patterns of fraud.

B. Utilization of the machine learning method

To increase the capacity of the fraud detection system in the mobile micro payment environment, it is essential not only to develop misuse detection models such as the Fraud Detection System, but also to develop technology which enables application of the abnormality detection model. In the financial sector, the Decision Tree method had been applied to detect abnormalities in the initial stages. This is because the detection process is graphic in the sense that it illustrates it through a tree structure, and is also easier to explain to users in the financial sector. Other machine learning methods used to detect fraud[6,9] include the Decision Tree [5], SVM (Support Vector Machine) [3], Neutral Networks [2], Bayesian Networks [7], and Random Forest [4] methods, which have the following characteristics. Each method is described in table 1.

Table 1. Explanation of machine learning methods used in financial fields.

Types	Description
Decision Tree	This is a tree type of detection model that connects the observation value with the desired value of a certain item.
Support Vector Machine	This is a detection model that determines to which range a new date will belong based on given data groups.
Neutral Networks	This operates like a parallel functioning nerve network to identify patterns in data and uncover hidden information.
Bayesian Networks	This is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG).
Random	This model classifies data and average

Forest	estimates through numerous Decision Trees.

With all of these methods, it is possible to use Machine Learning, which has input from previous transaction information to identify new entering data and identify abnormal transactions. The following process is required to develop such technology.

- First, it is necessary to analyze the detection methods of the fraud detection system of the mobile micro payment service.
- Next, identify features of abnormal transactions through the previously mentioned method of analysis.
- Based on these features, the machine learning algorithm with the highest accuracy needs to be chosen and optimized for the current system.

Further research is required to keep the advantages(real time payment) of the mobile micro payment method while providing such functions.

V. Conclusion

Due to the widespread use of smartphones and the rapid increase in the number of users, various financial tools for smartphones have been developed and distributed. However, although the mobile environment does provide a sense of handiness, it is more open to security threats. This is especially true for mobile micro payment services, which are open to fraud through Smishing and other types of threats. This increase in the number of threats calls for greater interest in the development of fraud detection technology, but, in order to advance the accuracy of fraud detection technology, it will be necessary to increase the amount of information gathered and to further develop machine learning methods.

Although this approach has been adopted on the grounds of the mobile micro payment service, it has the potential to be applied in the financial sector to further its security as well.

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0132-15-1004, Development of Profiling-based Techniques for Detecting and Preventing Mobile Billing Fraud Attacks)

References

[1] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland, “Data mining for credit card fraud: A comparative study”, Decision Support Systems, pp. 602-613, 2011.

[2] S. Benson Edwin Raj and A. Annie Portia, “Analysis on Credit Card Fraud Detection Methods” IEEE-International Conference on Computer, Communication and Electrical Technology, pp.152-156, 2011.

[3] Silvia Cateni, Valentina Colla and Marco Vannucci, “Outlier Detection Methods for Industrial Applications”. Advances in Robotics, Automation and Control, 2008.

[4] Liu, Chengwei, Chan, Yixiang, Alam Kazmi, Syed Hasnain, and Fu, Hao, “Financial Fraud Detection Model: Based on Random Forest”, International Journal of Economics and Finance, 2015.

[5] Efstathios Kirkos, Charalambos Spathis and Yannis Manolopoulos, “Data mining techniques for the detection of fraudulent financial statements”, Expert Systems with Applications 32 (4), 2007.

[6] Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana and Yo-Ping Huang, “Survey of fraud detection techniques”, Networking, Sensing and Control, IEEE International Conference on (Volume 2), 2004.

[7] Sherly K.K, “A comparative assessment of supervised data mining techniques for fraud prevention” ,TIST.Int.J.Sci.Tech.Res,Vol.1, 2012.

[8] Anna Kang, Jae Dong Lee, Won Min Kang, Leonard Barolli and Jong Hyuk Park, “Security Considerations for Smart Phone Smishing Attacks”, Advances in Computer Science and its Applications, 2014.

[9] Abuj Sharma, Prabin Kumar Panigrahi, “A Review of Financial Accounting Fraud Detection based on data mining techniques”, International Journal of Computer Application, Vol 39-No.1, 2012.

[10] C. Whitrow · D. J. Hand · P. Juszczak, D. Weston and N. M. Adams, “Transaction aggregation as a strategy for credit card fraud detection”, Data Mining and Knowledge Discovery, February, 2009.

[11] ITU-T X.asp-7, Technical Capabilities of fraud detection and response for services with high assurance level requirements.

[12] Estunation of Smartphone Penetration, Gartner historical jefferies & Company.Inc(2014), http://zeendo.com/info/smartphone-users-by-country/.

[13] Protect yourself from 'Smishing', Macfee Blog Central. 2012.

Biographies

EUNYOUNG CHOI received the B.S. degree in Mathematics from Korea University, Korea in 2001, the M.S degree in Information Security from Korea University, Korea, in 2003, and the Ph.D. degree in Information Security from Korea University, Korea, 2009, respectively. Currently, She is a general researcher at Korea Internet & Security Agency in Korea. Her research areas include mobile security, cyber financial security, cryptography and information security. Dr. Eunyoung Choi may be reached at bluecey@kisa.or.kr

YOUNGSANG SHIN received the B.E. degree in Computer Engineering from Pusan National University, Busan, Korea, in 1998, the M.S. degree in Computer Science from the University of Wisconsin, Madison, WI, U.S.A. in 2004, and the Ph.D. degree in Computer Science from Indiana University, Bloomington, IN, U.S.A. 2011, respectively. Currently, he is a general researcher at Korea Internet & Security Agency in Korea. His research areas include network/system intrusion prevention, cyber threat intelligence, cloud security, mobile security, web security, and cyber financial security. Dr. Youngsang Shin may be reached at ysshin@kisa.or.kr

TAEJIN LEE received the B.E. degree in Computer Engineering from Pohang University of Science and Technology, Korea, in 2003, the M.S. degree in Computer Science from the University of YONSEI University, Korea, in 2008. Currently, he is a team manager at Korea Internet & Security Agency in South Korea. His research areas include network/system intrusion prevention, cyber threat intelligence, malware security, mobile security, web security, and cyber financial security. Taejin Lee may be reached at tjlee@kisa.or.kr