International Journal of u- and e- Service, Science and Technology
Vol.8, No. 12 (2015), pp.45-54
http://dx.doi.org/10.14257/ijunesst.2015.8.12.05

A Study on Internal User Access Control Method Using Multiple Factors for Safe Financial Information System

Jae-yun Lee[1], Ho-sung Shim[2], Kyeong-Seok Han[3],
Hee-Hoon Cho[4] and Jong-bae Kim[5*]

[1, 2, 3]*Dept. of IT Policy and Mgmt., Graduate School of Soongsil Univ., Seoul 156-743, Korea*
[4,5*]*Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea*
[1]*jae_yun_lee@kftc.or.kr*, [2]*neider@naver.com*, [3]*kshan@ssu.ac.kr*,
[4]*heehoonc@naver.com*, [5*]*kjb123@ssu.ac.kr*

Abstract

Financial information systems operated by financial institutions are based on various customers' information. If leaked for illegal and vicious purposes, financial information can bring a lot of damages, including financial damages. Therefore, continuous demands on IT compliance related to financial information systems have risen as financial policy institutions suggest integrated plans for improvement on clarity of financial information service and reinforcement on safety of information systems operation. In order to meet such demands, financial institutions invested efforts and capital to prevent illegal leaks of financial information outside of barriers, however, it happens that not only do information leaks caused by external factors, but also ones caused by internal information system users occur quite frequently. Therefore, financial information systems must be operated and managed by authorized internal users. For that, this study analyzes various authentication technologies and compliances as advanced research then suggests a new authentication model for financial information system users. Through this model, we expect that the system will be able to secure safety in operation and management of financial information system hence, to deal with illegal leaks of financial information.

Keywords: *Smart Cross Platform, SVM (Smart Virtual Machine), Interpreter, HTML5, Customer information access control*

1. Introduction

Financial information systems operational environment in financial institutions providing payment settlement service has recently varied with the use of media, along with information and communication technology development, and e-Banking transaction continues to be increased. This financial service provides convenience for customers, but information security of non-facing financial transaction due to e-Banking revitalization is also being increased with the constant possibility of e-Banking accidents. The basis of this e-Banking service environment is for the users of the financial service as well as for service providers to check their identity. Therefore, financial institutions invest a lot of money and effort in preventing infringement into the financial information system, removing the weak points of security, preventing leakage of financial information, and checking the legitimacy of financial information system users. Nevertheless, customer information hacking in H Capital in 2011, N company computer network failure, personal

*Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 2005-4246 IJUNESST

information leakage of Samsung Card, financial computer accident in H Bank and S Bank in 2013, personal information leakage of K Card, N and L Card in 2014 occurred through the illegal acquisition of system access and permission of use, all of which emphasize that checking of legitimate user is the most important in system access. With these financial information leakage accidents, checking of overall financial computer security practice and securing of measure were brought for forward. Thus, the Finance Service Commission announced IT security strengthening general measures and best practice of financial company IT security affairs in business process aspect in 2011, and continuously required strengthening of financial information system operations such as having announced a general measure for financial computer security strengthening in July 2013 as well as for prevention of the re-occurrence of personal information leakage in March 2014 [1, 2, 3, 4].

National Industrial Security Center in NIS announced through a material [5] in 2015 that information leakage by insiders reaches 79.9%, such as 52.8% by former staff and 27.1% by current staff in subject of information technology leakage [5]. Despite this financial information system operational environment, checking the legitimacy of internal users in financial information systems is fragmentary, and is operated and controlled with insufficient connection between relevant systems.

Realistically, it is very difficult to detect and prevent every illegal leak and use committed by authorized users from the inside. In order to achieve realizing effective prevention of internal information leaks and inspections for illegal use on information systems, there must be an ability to inspect for tracking illegal uses by re-evaluating information security policies that are currently limited on existing, separate security products, as well as a new inspection system that can visually monitor user actions and track evidences [20, 25].

However, as security measures so far have been mainly focused on protecting internal resources from attacks from outside, now is the time to protect such assets from internal users as paradigms shift, and the latter idea takes a big portion of future security measures. Therefore, it must occur that not only do we need technologies to deal with internal threats effectively, but also approaches to management and operation perspectives [20, 26].

Therefore, this study is going to suggest a certification model that checks the legitimacy of internal users in financial information systems for internal user certification model suggestion with multiple factors, as an advanced study, by analyzing all compliances [1, 2, 3, 4, 6, 7, 14] related to internal user certification by financial information systems operational agency, such as payment settlement systems and components, financial information system operational management stages and access components, user certification strengthening factors, the principle of financial market infra by payment settlement system commission and technical committee of international securities supervisory agency (PFMIs), and ISO/IEC 27001, a standard for international information protection management system, and e-Banking supervisory regulation.

2. Related Works

2.1. Concept of Payment Settlement System

Payment settlement is defined as economic subjects, such as individuals or companies, solving of claim · obligation relationship between transaction parties by economic activity, using payment means like cash. Payment settlement system is defined as an institutional strategy, enabling transfer of funds and payment of financial investment products, and it specifies payment means, participant institutions, operational organization, business process regulation and procedure, and computer systems as its components [7].

Domestic payment system is classified into wholesale payment system, which handles large amounts of funds, and the retail payment system, which handles small amounts of money in large quantities, depending on object of payment. As a money settlement system which mainly handles micro payment of companies or individuals, the retail payment system is widely in transaction object with man payment cases.

Payments, such as transfer account, credit card, check, and Giro are mainly handled by the retail payment system. Retail payment system can be divided into note exchange system, Giro system, finance joint network, and e-commerce payment settlement system [7].

2.2. Components of Payment Settlement Service

Payment settlement service is composed of finance transaction customer, financial information system operational institution, financial institution, and outside participant institution. Financial information systems operational institution plays a role of connecting financial transaction customers and the financial institution or outside participant institution.

The operational area of financial information systems can be divided into areas of management, technology, and physical. Management area is overall activity making people who are concerned comply with advance definition such as policy, instruction, standard, and procedure related with security activity. Technical area is overall activity for devising control measures and plan to grasp and remove and relieve security related threats in information systems, and building and operating of the systems. Physical area is an activity for blocking, monitoring unauthorized access or illegal use of building, facility, and equipment in which information system is installed. Technical field security area can be divided into network, information system, data, DB security, and terminal (PC).

2.3. Financial Information System Operational Management Stage

The stage for the operational management of financial information systems can be divided into the stage for advance registry of information required for internal users to access the system, and the stage for operation and management after such registry and access. In the course of access to the system for advance registry and operational management of internal user information, various certification methods and security elements are used.

2.4. Financial Information System Access Components

Overall elements required for the operational management of financial information systems are composed of accessor, use medium in financial information systems aspect, terminal (PC) used by internal users, technology used for user certification, and communication channel used upon transmission of relevant information.

2.4.1. Financial Information System Accessor and using Medium

Accessor to financial information systems can be divided into application program developer, system operational management related user, and business operational manager. The user certification model suggested by this study targets only internal users who operate and manage financial information systems. As a technical field, using the medium of certification model in systems aspect is divided into access purpose of internal user and using medium according to its role and function. Generally, as terminal access using emulator software and security measures, we have root administrator account access by top-notch privilege of the system using SSH and https, DB administrator account access for management on DBSM and other data, administrator account access for work operations, systems access through system management tools as client and server software, system access via consoles, access through programs, access among systems and more [20].

2.4.2 User's Terminal

The terminals used by internal users for operational management of financial information system could be various, but generally PC and notebook are used most.

2.4.3. User Certification Technology

User certification technology is to acknowledge that the person who claims himself as a legitimate user to the information system concerned. This is done with stages of identification wherein the user reveals himself to the certification system, certification that the information system certifies user, and granting of access right for use of system resources by access approver‘ s access control mechanism. In particular, certification process has mandatory requirements for service requester to perform for the service from service provider [10, 16, 17, 18]. Certification technology as an identification technology can be divided into information known by user, information of user‘ s belongings, and certification using user’ s physical or behavioral characteristics [9,11, 13, 15, 20, 21, 22, 23, 24]. The terminal most used in the certification of internal users is PCs, because the PC is a terminal that has a wide range of uses.

Table 1. Type of User Authentication Technology

Category	Content	Characteristic	Type
Knowledge base (What you know)	Knowledge or information known to the user can be used as method to make the user authenticated	- Simple mechanism - No additional devices required, but easily exposed - Easy to be used and modified as it is user friendly and possible loss due to heavy dependence to user's memory	ID/PWD, virtual keyboard, Q & A, patterns and images
Possession base (What you have)	Token information possessed by user can be used as method to make the user authenticated	- Highly secured with high risk on theft or lost - Complex mechanism, uncomfortable to carry and excessive cost for installation	IC card, accredited certificate OTP (one time password)
Living body base (What you are)	Biological characteristics of the user can be used as method to make the user authenticated	- Highly secured with difficulties of forgery but devastating damage when leaked - Suitable for physical security - Lowered credibility due to relatively high error rate - Massive cost for installation and management	Biological – face, finger print, vein and iris Behavioral – voice and signature

2.5. User Certification Strengthening Elements

Financial information systems certification of internal user can be found in various ways. The technology used for financial information system user certification varies a lot, but ID and password are used the most. Two factors and two channels that use more than 2 certification technologies are available for providing enhanced security and removing weak points compared with single certification of one factor and on channel technology [9, 10, 11, 13, 14, 19]. Also, the efficiency of multi factor and multi-channel certification can be different depending on the point of using them, and it is desirable in minimizing information leakage of certification to apply certification technology when specific service is used. Also, when using certification technology, we can enhance safety and confidentiality by selecting and applying encryption algorithms appropriate for the characteristics of transmission information. We can enhance safety by sharing information between relevant systems used for user certification and record of performance in the course of operational management for financial information systems of the internal user, and using them for system access and performing of the important work of users based on information shared [13, 15, 19].

3. Model of Certification for Internal using Multi-factor

Financial information system user certification strengthening factor in advanced studies and internal user certification model of financial information systems based on various compliance factors [1, 2, 3, 4, 6, 7, 14] should satisfy the factors in Table 1, and we suggest internal user certification model.

Table 2. An Internal User Authentication Model Requirements

Division	Conditions like user certification strengthening elements	Compliance factor	Model components
Financial information system	System used to provide financial information	-	Information system
Service user	Financial transaction customers for financial service	-	Financial service user
User account	- Operational management manager of information system - Grant to individuals according to information system access purpose	e-Banking supervisory regulation, administration Information system access rights management rules	Account management, tracking monitoring Password management, information system, internal user
Using terminal (PC)	- Designation, operation as an important using terminal	e-Banking supervisory regulation, administration	PC

	- Prior approval and use of terminal user	information system access rights management rules	
User certification	Password, security token, Smart Card, HSM, OTP, biometrics Recognition, IC Card	General measures in e-Banking field, administration information system access rights management rules	ID/password, OTP Server security system
Access rights control	- Devise access control means (physical, technical, managerial) - Devise identification and access rights means	PFMIs, ISO/IEC 27001, K-ISMS, e-Banking supervisory regulation, general measure for e-Banking field, administration information system access rights management rules	-
Approval of important work performance	Manager when operating important works which weigh impact on information system Authorization	e-Banking supervisory regulation	Tracking audit, OTP Server security system
System access and activity record	- Record of information system user access and performing activity Maintenance - Use for post tracking audit	e-Banking supervisory regulation, general measures in e-Banking field, administration information system access rights management rules	Tracking audit, information, server security system

Main composition factors of user authentication models suggested above perform following functions when a user is authenticated during processes. The account management system performs managerial functions as requests, approvals, modifications and deletions by making user accounts with system perspective that are given to the information system user in interacting with access target information system, before the system is used. The server security system performs control functions by making service privileges such as access of user's information system, execution of programs and commands, and material access interact with OTP system and tracking system. The tracking inspection system performs monitoring on user works and performance activities, surveillance and work activity recording in interacting with OTP, server security system and access target information system. OTP system is a system as an additional authentication method that performs additional verifications on authenticity of user privilege at the moment of major command execution that affects the information system when accessing the information system and after accessing the information system in interacting with the tracking inspection system, server security system and access target information system. Password management system performs functions that approve specific time usage and generate passwords in either real-time or allocated time in interacting and syncing with tracking inspection system, access target information system in real-time basis.

This study designed and realized the suggested model in order to strengthen safety and confidentiality when checking internal user legitimacy in systems operational management, by reflecting 5 factors as follows. This study, as for user certification technology, realized overall information of certification in advance first, by using channels like ID/password and OTP and multi-factor certification technology, second, periodical auto creation and management of password by password management system, third, mutually connecting of account management, server security, firewall, tracking audit, OTP, and password management system, as well as strengthened confidentiality by using the information shared in advance, when needed. Fourth, this study designed and realized an application stage of certification technology according to the importance of work performance in order to strengthen legitimate user certification upon the information system internal user‘ s access. This study designed and realized for user certification to be performed upon performing of important functions.

Table 3. Securing of Safety upon Certification Technology

Safety securing degree	ID/password + server security	Account/tracking audit	OTP	password management
General (Low)	○			
Initial period	○	○		
Middle	○	○	○	
Suggested model (High)	○	○	○	○

Financial information system internal user is available for system access only when they register relevant information in advance before system accesses through 9 stages of user-terminal (PC)-account management system-tracking monitoring system-password management system-OTP system-firewall-access information system and server security system.

When financial information system internal users perform a simple function after access to the system with prior information registry, it is designed and realized for work performance to be available so that the safety of system operation will be secured through 7 stages of user-terminal (PC)-tracking monitoring system-OTP system-firewall-access information system and server security system.

Also, when user performs an important function which weighs influence on systems such as system shutdown after access to financial information system, it is designed and realized for the safety of system operation, through 17 stages of user-terminal (PC)-tracking monitoring system-OTP system-firewall-access information system and server security system-password management system-access target system-server security system-important work commands input-tracking monitoring system-OTP system-tracking monitoring system-access target information system-server security system-important work command execution.

4. Conclusions

Despite the fact that various compliances exist such as financial policy-making body continuously demanding the strengthening of safety in financial information system operation, there is no research or study about standard levels of the internal user certification model. Therefore, this study suggested a model that satisfies the condition of financial information systems internal user certification model, based on user certification strengthening factors and the content for demand of various compliances.

The internal user certification model suggested by this study is one that uses dual channel and multi-factor in the absence of applicable standard certification model to finance operational environment and internal user in which financial information security threats are increased. The suggested model was made available not only for the securing of safety in systems operational management but also for the response of illegal leakage of important information, by using it as means for legitimacy certification of user and strengthening of access control upon internal user‘ s access to financial information system, by applying it to actual work of institutions in which it is actually built. And it is expected that the same model will be used as an improvement model for individual financial institutions.

Nevertheless, access control for each access path should be considered, as access path for internal/external user access in view of financial information system vary a lot. Also, an additional study for user‘ s convenience, carrying handiness, costs for building, and efficiency for using information system resource are required due to the insufficiency of such studies, as only the safety of information system operation is being emphasized in this paper.

References

[1] “Financial company information technology (IT) sector protection business best practices”, FSS, **(2011)**.
[2] “Electronic banking supervisory regulations”, FSC, **(2013)**.
[3] “Computerized comprehensive financing security measures”, FSC, **(2013)**.
[4] “Relapse prevention comprehensive measures of leakage of personal information of the financial sector”, FSC, **(2014)**.
[5] Industrial confidentiality Center, NIS.
[6] Prime minister’s Directive, “Information system access rights management provisions of the Administrative agency”, **(2013)**.
[7] “The payment system in Korea”, Bank of Korea, **(2014)**.
[8] S. G. Yun, “Enhanced techniques of internet banking security system using OTP”, **(2010)**.
[9] Y. J. Lee, “Study on user authentication and e-banking system using a dual channel”, **(2011)**.
[10] C. W. Jeong, “Empirical studies on the user terminal authentication system for fraud prevention certificate”, **(2012)**.
[11] J. S. Lee, “Secure Internet Banking service model design and certification scheme”, **(2013)**.
[12] “Payment and information technology, electronic banking security measures and OTP Usage”, KFTC, **(2006)**.
[13] “Payment and information technology, safety analysis of Internet banking authentication means”, KFTC, **(2007)**, pp. 119-139.
[14] “Payment and Information Technology”, KFTC, **(2012)**.

[15] "Certification means your major sectoral studies of electronic financial transactions", KFTC, **(2012)**.

[16] E. J. Choi, C. O. Kim and J. S. Song, "Password-Based Authentication Protocol for Remote Access using Public Key Cryptography", Kiise, vol. 30, no. 1, **(2003)**, pp. 75-80.

[17] S. W. Lee, H. S. Kim and K. Y. Yoo, "A Password - based Efficient Key Exchange Protocol", Kiise, vol. 31, no. 4, **(2004)**, pp. 347-352.

[18] "Computer Data Authentication", FIPS 113, **(1985)**.

[19] "Payment and information technology, current status and future prospects of authentication methods", KFTC, **(2011)**, pp. 31-69.

[20] Y. C. Oh, "An Information System Audit Model for the Prevention of Unlawful Usage by Insider", Graduate School of Information Science Soongsil University, **(2009)**.

[21] T. S. Kim, "Study on identity and access management system based on public key infrastructure", Graduate School of Sungkyunkwan University, vol. 12, **(2010)**.

[22] S. B. Hong, "An enhanced user authentication using QR code and PIN", Graduate School of Information Science Soongsil University, **(2011)**.

[23] K. H. Jung, "A Design of User Authentication System Using OTP In The Environment Of Web Session", Graduate School of Information Science Soongsil University, **(2010)**.

[24] "A Study on Single-Sign-On for Information Systems in Public Sectors", NIA, **(2004)**.

[25] "National ICT Master Plan", CIS, **(2008)**.

[26] "National Informatization Guide", NIA, **(2008)**.

Authors

Jae-yun Lee, he received his bachelor`s degree(1985) in Computer Science from Hannam University in Korea and master's degree of Computer System in Konkuk University, Korea (1994). He worked in the IT field as a System engineer over 29 years. His current research interests include Risk Management and Security.

Ho-sung Shim, he received his bachelor`s degree in Urban Engineering from Busan National University in Korea, (1995). He worked in the IT field as a Opensource Software Planer and Educationalist over 15 years. Now He is CEO of Korea Opensource Software Association., LTD. since 2011

Kyeong-Seok Han, he received his bachelor's degree of Education (1979) and master's degree of Management (1984) in Seoul National University, and doctor's degree of MIS in Purdue University, USA (1989). Now he is a professor in the Dept. of Management, Soongsil University, Seoul, Korea. His research interests focus on Technical MIS, Digital Economy, Agent-Eased Simulation, Web Programming, ERP.

Hee-Hoon Cho received his bachelor's degree of Computer Science in Korea Polytechnic University (2015). He is studying his master's degree of software engineering in the Graduate School of Software, Soongsil University, Seoul. His current research interests include Open source software and Security.

Jong-Bae Kim, he received his bachelor's degree of Business Administration in University of Seoul, Seoul (1995) and master's degree (2002), and his doctor’s degree of Computer Science in Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.