Security Factors for Healthcare Data

Comparing the Security Threats of Online Banking and Healthcare Information Systems

Young-Sil Lee and Hoon-Jae Lee
Division of Computer and Information Engineering
Dongseo University Graduate School
Busan, Rep. of Korea
e-mail: youngsil.lee0113@gmail.com

Esko Alasaarela and Risto Myllylä
Department of Electrical Engineering
University of Oulu
Oulu, Finland
e-mail: esko.alasaarela@ee.oulu.fi

***Abstract*—The number of information security threats in healthcare information systems is increasing tremendously. There are various factors that contribute to these information security threats; most researchers are mainly focused on certain factors such as virus attacks and malware. Thus, certain important factors may have still remained unexplored. In addition, the lack of tools and technologies can also contribute to the limited number of threats recorded in the healthcare system. In this paper, we summarize the security threats in online banking and healthcare information systems (HIS) and analyze the relationship of risk factors through comparison. The findings will serve as recommendations for healthcare service organizations to fill the technology gap between the online banking and HIS security systems.**

Keywords - Online banking security; Healthcare security; Information security; HIS; Security threats.

I. INTRODUCTION AND MOTIVATION

Nowadays, computer and network-based systems are expanding in order to support more healthcare activities, especially in isolated regions (i.e., isolated rural areas in Greece, Scandinavia and Germany), where there is often no availability of central general hospitals. Networked healthcare information systems can fill this gap, by connecting local healthcare service providers with central regional or peripheral hospitals to make tele-consultation, tele-diagnosis and exchange of views possible between remote located doctors in certain patient treatment cases.

Furthermore, medical data maintained in a health information system is directly related to the patients' health and safety. According to the recommendation on the protection of medical data issued by the Council of Europe [1], appropriate technical and organizational measures must be taken to protect personal data against any accidental or illegal destruction, accidental loss, as well as against unauthorized access. These possible threats can severely damage a health information system's reliability and discourage professional use in the future. Therefore, the execution of a risk analysis is a necessity in order to assure a health information system's safety and Quality of Service (QoS) [2].

This study intends to analyze the security threats of health data. First, a review of the information security threats are included and discussed. Beside this, we also compare the existing security threats of online banking with the healthcare information system (HIS). In both cases, the security factors include hacking and blocking as well as accidental and deliberate cases, and also the possibility to change a sensor from one patient to another.

Personal medical information is in various aspects similar to financial data. Accidents caused by incorrect medical information can lead to large-scale litigation, and also translate directly damage to a person's life. According to the estimation of the IOM (Institute of Medicine) under the U.S. Department of Health and Human Services, as many as 98,000 patients per year are estimated to die due to wrong medical information [3]. This occupies eighth place in the United States on the list of the 10 leading causes of death; it is higher than the mortality due to traffic accidents, breast cancers and AIDS.

As for financial institutions, in 2007, one million people in Japan lost their pension paid records. Due to government mismanagement, the data quality may be lost, which may lead to pay back in 25 years according to pension specifications.

Through these incidents, we can see how huge the impact is to the society, both in case of healthcare and financial data, when an incident is about money loss or threat to human life. Currently, there is a clear need for efficient security models in banks or medical institutions, which offer their customers access into their system via Internet.

Online banking started with Security First Network Bank (SFNB) in 1995 [4], and is now rapidly increasing with hundreds of millions of users' across the globe. Many researchers have studied various security threats and its solutions for online banking. On the other hand, the security of personal health information is still not well in order. For this reason, even though it cannot prevent all kinds of security threats, the online banking system has a better security model.

Since healthcare data is at least as important as financial data, the purpose of this paper is to comprehend the factors, which are important in healthcare through this study. We attempt to classify the security threats on each side and analyze the security threats of healthcare information through a comparison with the existing threats of online banking. Also, we describe some online banking security models that can be applied to HIS.

 ISBN: 978-1-61208-243-1

The next section describes the previous studies related to this research. Section III presents the comparison of online banking security and healthcare information system, and Section IV describes some Internet banking security models that can be applied to HIS.

II. RELATED WORKS

In this section, we describe the information security threats as well as summarize the existing security threats in online banking [5] and healthcare information systems [6].

A. Threats to information security

Information security threats can be classified into three categories, as found below [7][8].

First, there are environmental threats, which include natural disasters and other environmental conditions. Earthquakes, fire, floods and storms are examples of natural disasters. The likelihood of a natural disaster affecting an organization is greatly dependent on its location, information processing facilities and stored data. For example, a computer facility near bush land will be more likely to be affected by bushfire than one that is located in the city area. The failure of a power supply is an example of an environmental conditions threat, when uninterruptible power supply equipment and back-up file systems are not available.

Secondly, deliberate threats are those threats that involve the destruction or manipulation of data, software or hardware. These threats include denial of service, malicious code such as viruses and worms, theft and fraud. Various vulnerabilities are identified to be the cause of these threats such as inadequate network management (resilience of routing), lack of firewall, not using the latest version of the operating system and lack of physical security.

Lastly, accidental threats are threats that are related to errors and omissions. Errors and omissions by employees or insiders are the main causes of information security problems [9].

A communication failure could be caused by accidental damage to network cabling, loss of network equipment such as routers or servers and software failure. Examples of vulnerability, which could lead to an incident, include lack of redundancy and back-ups, inadequate network management, lack of planning and implementation of communications cabling or inadequate incident handling. Due to the existence of so many variables that can possibly occur as threats to a computer system, it is useful to have an appropriate tool for threat analysis [10].

Since there are many variables that have no possibility to become threats to a computer system, it is very important to come out with an appropriate tool to perform threat analysis. Using an appropriate tool will enable the system to analyze threats accurately and come up with the best solution on how to overcome these security threats.

B. Online banking security threats

Due to its benefits, which allows internet users to access and manage their bank accounts from anywhere on the world at any time, online banking has now grown rapidly from a niche service to a major new way of banking. However, since the Internet is not originally designed for online banking, online banking is now facing a wide range of security risks for both the banks and the online banking users such as brute-force attacks, distributed attacks and social phishing. Therefore, the banks have to improve their online banking security systems constantly, which means the banks have to keep investing in security systems all the time.

Online banking is a series of processes in which a bank client logs onto the website of the bank through a web-browser installed on the PC and carries out various transactions such as account transfers. Online banking is carried out in four major stages, illustrated below in Figure 1.

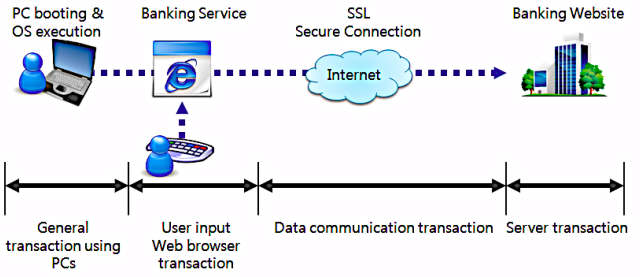

Figure 1. Online Banking Transaction [5].

a. The user turns on the PC and boots the OS.
b. After the web-browser is open, the end user accesses the online banking website of the bank and enters the ID or Personal Identifying Number (PIN) and the password by using the keyboard.
c. The data input is encrypted by SSL (Secure Socket Layer) and transmitted to the bank's server.
d. The bank's server decrypts the transmitted information and processes the user's authentication, account inquiry, account transfer, etc.

The ordinary PC environment is exposed to many types of threats because of insecure web surfing and use of a variety of unverified programs. If a user carries out an online banking transaction in an environment that is exposed to such kinds of threats, there is no way to guarantee the safety of that online banking transaction.

Most of the recent hacking tools are circulated throughout the web and they can be inadvertently downloaded and executed in the user's PC while the user is enjoying of web surfing or checking e-mail.

Once these hacking tools are planted into a user's computer, they will then capture the password, account number and personal data, which the user is typing. Furthermore, they are even capable of replacing the input screen that the user is watching with a counterfeit website of the bank, which the hacker had installed in advance. The user's input data are not transmitted to the bank because these hacking tools redirect the user's input data to the hacker's server instead for illegal account transfers. Thus hackers and hacking tools can attack the system using many tricks in a number of different ways during the online banking process, as shown in Figure 2.

 ISBN: 978-1-61208-243-1

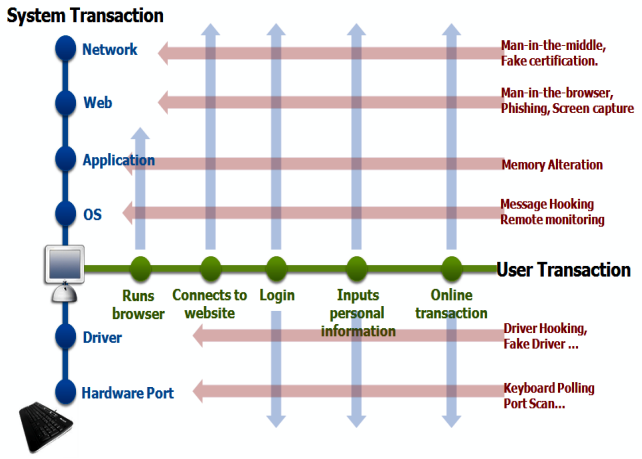

Figure 2. Threat can pervade every stage of the transaction [5].

C. *Healthcare information system security threats*

Today, the usage of information systems in the healthcare environment provides many potential benefits such as improving the quality of care, reducing medical errors and enhancing the readability, availability and accessibility of information. However, HIS security threats have increased significantly in recent years as well. Therefore, storing health information in electronic form has raised concerns about a patient's health, privacy and safety. Basically, HIS is threatened by both accidental events and deliberate actions, which can severely damage the reliability of HIS and consequently discourage professionals to use it.

Furthermore, the lack of adequate protection for sustaining confidentiality, integrity and availability aspects leads to the need to investigate potential threats, particularly in the HIS domain. In addition, weakly organized security management and unawareness of risk analysis practices, especially in the healthcare organizations, need particular attention.

The International Standard for Health Informatics for Information Security Management in Health, using ISO/IEC 27002 (ISO27799: 2008) [11], has defined HIS as a repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely and accessible by multiple authorized users. There are various types of threat categories introduced in this standard. It classifies HIS threats into 25 types.

Basically, the HIS threats have been classified into two main categories, namely, internal threats and external threats [12]. The internal threats include various types of employees' behavior such as an employee's ignorance, curiosity, recklessness, inadequate behavior, taking someone else's password and giving a password to another employee. The external threats include viruses and spyware attacks, hackers and intruders on the premises.

In addition, HIS threats can be categorized into 19 types based on case studies conducted using the selected risk analysis method [2]. One finding shows that the most critical threat to the HIS is a server power failure. Furthermore, a power failure in a workstation, a network software failure and a tele-monitoring software failure also present high-risk threats. Besides this, there are also a number of high-risk threats related to human factors, such as user errors in using the HIS and the masquerading of the user's identity during system operation.

Furthermore, another study has identified 25 types of patient monitoring system threats [13]. The most critical threat is a power failure of the server, while the power failure of a personal home computer is the second most critical failure for the system. Also, air-conditioning failures, system and network software failures, monitor support software failures and medical record software failures are also treated as the high-risk threats. However, this study also identified a number of high-risk threats related to human factors, such as user errors in using masquerading software.

III. COMPARISON OF INTERNET BANKING AND HEALTHCARE INFORMATION SYSTEM

In this section, we provide a classification of security threats based on existing research results and comparison between online banking and healthcare information systems based on important security comparison factors.

A. *Classification of threats*

Figure 3 presents the known threats, which affect each security method discussed in this paper.

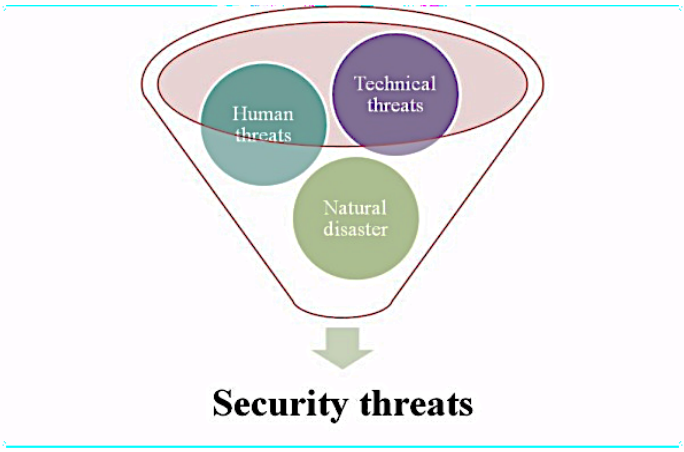

Figure 3. Classification of threats.

It does not present all the threats, which may exist in such a method, but it shows that those methods are currently vulnerable to several attacks. Basically, the threats were categorized based on relevant standards [11][14] and also based on a comparative study of previous works and publications in this research.

We have classified the threats into three categories, which include technical threats, human threats and natural disasters. First, technical threats are caused by a technical problem, such as the technical failure of a network or system, a variety of malicious attacks through malicious code, etc. Human threats belong to information leakage by insiders or staff, and unauthorized user access, user's negligence, etc. Finally, there are threats of natural disasters, caused by a

 ISBN: 978-1-61208-243-1

variety of adverse circumstances, such as water damage, fire and earthquake, etc.

In Figure 4, the technical and human threats are classified in more details.

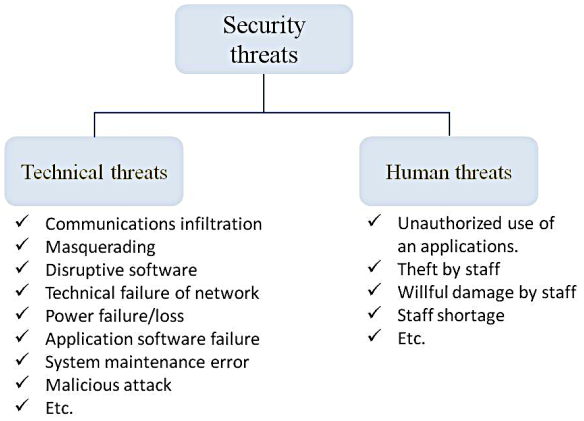

Figure 4. Classification of technical and human threats.

B. Comparison factors

Table I depicts 13 types of factors according to the major threat categories. We consider four categories for comparison, such as authenticity, confidentiality, integrity and availability, which are general factors in cryptography.

TABLE I. COMPARISON FACTORS

	Factors	Description
Authenticity	Password	How many digits and what kind of combinations are used?
	Authentication	How to provide authentication?
	Transfer protocol	What kind of protocol to be used for data transfer?
	Unauthorized access	How can the access of an unauthorized user be prevented?
Confidentiality	Communication interception	How can interception by a malicious third party be prevented?
	Data encryption	What kind of algorithm is used for data encryption?
	Non-repudiation	How to achieve non-repudiation?
Integrity	Social engineering attacks	Impersonation, persuasion, bribery, shoulder surfing and dumpster diving, etc.
	Malware attacks	Malicious virus, worm, Trojan horses, spyware and adware, etc.
	Acts of human error or failure	Entry of erroneous data by staff, accidental deletion or modification of data by staff
Availability	Power failure	Server down due to power failure, Air-conditioning failure of the server, Interruption by service provider
	Hardware/software failures or errors	Insufficient storage software, Hardware/Software maintenance error, Application software failure
	Natural disaster	How can the failures from fire, water-damage etc. be prevented?

At first glance, it might seem that authenticity is included in the concept of integrity. Integrity is more specifically about the content of the data itself. Authenticity involves the assurance that the data was created or sent by the source it appears to be from.

Integrity, as a concept, means that there is resistance to alteration or substitution of data, and/or that such changes are detected and traceable. When data might be changed by accident or malice, preventing the change is of the first concern, and detecting it is the second. Integrity can be maintained on many levels, from hardware to application logic.

Confidentiality means, at the core of the concept, that the data is hidden from those are not supposed to see it. We can accomplish confidentiality in a number of ways such as ensuring encryption of the data so that it cannot be intercepted or accessed during transmission or transport etc. While encrypting is a sure way of keeping the data confidential, it is not the only way.

In any information system, the information must be available when it is needed. This means that, the security controls and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times. It attempts to prevent service disruptions due to power outages, hardware failure, and system upgrades. Ensuring availability also prevents denial-of-service attacks.

C. Results and analysis

From Table II, we can see that the result of comparison between online banking and healthcare information systems applies various factors. We have analyzed the requirement per each item for providing sufficient security and also provided information on the currently used technologies. For the analysis we have investigated the most common technologies both in online banking and healthcare information systems.

First, in online banking, a password is employed combining characters and numbers within 30 digits using a virtual keyboard to prevent a key logger. In addition, to authenticate the use of OTP (One-time password) and certificate, it uses the HTTPs, SSL/TLS protocols for secure communications. Some technologies are dependent on a system, such as a firewall, browser protection, backup system, etc. Also, to prevent communication interception, a pass-phrase, firewall, SMS and transaction monitoring are commonly used. The pass-phrase is a security model based on information held by the user. It is usually used as a second authentication method in a transaction that involves money transfers.

Some cases of healthcare information Systems (HIS) are using a six-digit character password, depending on the system. The transport protocols are TCP/IP (Transmission Control Protocol/Internet Protocol) and FTP (File Transfer Protocol) for file transfers and data encryption formed using WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access), if using wireless communication; it also performs data encryption using PKI (Public Key Infrastructure).

 ISBN: 978-1-61208-243-1

TABLE II. COMPARISON RESULTS

	Factors	Requirement	Online Banking	HIS
Authenticity	Password	Combination of numbers and characters of more than 8-digits or Bio-metrics	Mixed numbers and characters within 6 to 30-digits, virtual keyboard	6-characters (depending on the system)
	Authentication method	Using high-grade security media	Digital certificates, OTP, security card, etc.	No fixed rules
	Transfer protocol	Mutual and secure authentication protocol	HTTPS, SSL/TLS	TCP/IP, FTP
	Unauthorized access	Strong password techniques One-way hash functions Use of personal characteristics	Firewall, Access control technologies	Firewall, Access control technologies (depending on the system)
Confidentiality	Communication interception	Transaction monitoring secure	Pass-phrase, Firewall, SMS, Transaction monitoring	WEP/WAP
	Data encryption	Cryptographic algorithm (i.e., AES-128, SEED)	128-bit SSL encryption 256-bit SSL encryption (EV SSL)	PKI (Public key infrastructure)
	Non-repudiation	Digital signature	Digital signature through certificates	Digital signature
Integrity	Social engineering attacks	defined consequences for violating the policies, education and training	Positive identification	Positive identification
	Malware attacks	Firewall, anti-virus software, real-time monitoring	Browser protection	Browser protection
	Acts of human error or failure	Regular security audits Limited access to system	Regular security audits Limited access to system	Depending on the company policy
Availability	Power failure	Auxiliary power, Backup system, alarm, etc.	Backup system (depending on the system)	Backup system (depending on the system)
	Hardware/software failure or errors	Regular system maintenance	Regular system update and maintenance	Regular system update and maintenance
	Natural disaster	environment monitoring (i.e., Fire detection sensor)	Real-time environment monitoring in server room	Real-time environment monitoring in server room

On the other hand, to prevent availability breakdowns, through such incidents as power failure, system errors, system failure or natural disaster, both systems provides a backup system, regular system updates and maintenance, etc., but it depends on the system. In the case of integrity maintenance, the use of positive identification, browser protection software or the introduction of some policy such as regular security audits and limited access to system, were implemented. However, those also depend on the system. For reference, positive identification is a model where the user is required to input some secret information only known to him in order to identify himself.

IV. DISCUSSION

In this section, we describe some online banking security models that can be applied to HIS. Many different advanced fraud detection technologies are being applied for fraudulent detection and prevention of online banking transactions. Hence, if a system has better security control, the threats can be reduced.

A basic knowledge of authentication is an important step towards security control. Authentication is any process by which you verify that you are who you claim to be and have been permitted to access to a system. In the online banking case, there are a variety of technologies and methodologies financial institutions can use to authenticate a customer. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, among others. The level of risk protection afforded by each of these techniques varies. Thus, online banking systems are used according to their combinations. The selection and use of authentication technologies and methods should depend upon the results of the financial institutions' risk assessment process. If we can apply these various techniques to HIS, this can be a safeguard against unauthorized access and use.

The following proposals are examples of security models that can be help to provide authentication. Hiltgen et al. [15] presents two challenge-response online banking authentication solutions – one based on short-time passwords and the other on certificates – and then describes how easily these solutions can be extended if sophisticated content-manipulation attacks arose. The short-time password solution

 ISBN: 978-1-61208-243-1

use symmetric cryptography in combination with a hardware security module (smart card) and an offline (stand-alone) smart-card reader. This solution provides convenient mobility for people who want to bank online anytime anywhere, not just from their homes.

In the certificate-based solution, a two-stage, PKI-based online banking authentication solution is used. It is characterized by open standards and a programmable, certified, secure, smart-card reader connected to a potentially exposed PC. This solution uses a dedicated FCR (FINREAD card reader) along with an appropriate financial transactional IC card reader (FINREAD) and financial card reader identification application (FCRIA), both of which are loaded onto the user's FCR to secure the authentication process.

Tiwari et al. [16] proposes an authentication system that is both secure and highly usable, based on a multi-factor authentication approach. It uses a novel approach to create an authentication system based on TICs (Transaction Identification Code) and SMS to enforce an extra security level for the traditional login in a username/password context. TICs are user specific unique transaction identification codes, which are issued by banks or financial institutions for their users. This code is similar to the One-time Password (OTP) and the code is used only once. This paper also suggests an encryption/decryption technique that would be used to keep TICs as secret codes on cell phones/PDA. The user can easily pick up a TIC (from the stored list of TICs) to initiate a secure web transaction using her/his cell phone/PDA, instead of typing a complicated TIC code in each transaction.

Dandash et al. [17] presents a security analysis of a proposed online banking model compared with current existing models used in detection and prevention of fraudulent Internet payments. Their proposed model facilitates online banking Fraud Detection and Prevention (FDP) by applying two new secure mechanisms, a Dynamic Key Generation (DKG) and a Group Key (GK). Such mechanisms satisfy all transaction security properties of payment systems as they enforce strong authentication and authorization methods.

Hu et al. [18] proposes a secret key based security scheme for achieving secure online banking. Encryption equipment is adopted at certification servers and client terminals and a secure certification protocol is established by using secret key encryption, combined secret key and smart card techniques. In this paper, the encryption hardware and secret key encryption algorithm passed the security tests performed by an authorized department. Along with this, the use of authentication and digital signature certification guarantee double security. Also, a one-time secret key is generated automatically according to a generation algorithm and is unrepeatable.

In addition to this, a mutual authentication, also called two-way authentication, is a process or technology in which both entries of a communications link authenticate each other. In a network environment, the client authenticates the server and vice-versa. In this way, network users can be assured that they are doing business exclusively with legitimate entities and servers can be certain that the users are attempting to gain access for legitimate purposes. Currently, mutual authentication is gaining acceptance as a tool that can minimize the risk of online fraud in e-commerce. If we can apply this to HIS, it can reduces the risk that an unsuspecting network user will inadvertently reveal security information to a malicious or insecure web site.

Institutions should establish a firm policy to provide availability in case of power failure, hardware/software failure or error and human failure or error. The policy, such as regular security audits, system updates or limited access, could help to reduce security accidents.

V. CONCLUSION

This paper aims to investigate the current debate regarding the threats and vulnerability of healthcare data. It reviews some possible remedial actions to defend against these threats. The aim of this research was to critically analyze existing research and findings dedicated to healthcare security issues and its information security problems.

We found that although the findings of the reviewed research are somewhat contradictory, the Internet is mostly seen as a security threat. Some technologies, such as anti-virus software; spam guard; email filtering and encryption; firewalls and so on, are used successfully by the service provider organizations to protect the information. However, some areas are still vulnerable to security threats.

The awareness of information security is now growing rapidly. In the long run, information security will be one of the most important issues for modern organizations. The inclusion of biometrics, encryption, digital signatures, intrusion detection systems, security education and training, virus control and compliance with data protection legislation and policy will be of primary importance. The findings of this study will serve as recommendations for healthcare service organizations when defining requirements for the security issues. Simply speaking, it is a question of filling the technology gap between the security solutions in the online banking and healthcare information systems.

ACKNOWLEDGEMENT

The authors would like to thank the SIMSALA project, in the Optoelectronics and Measurement Techniques Laboratory of the University of Oulu, and its funders for the resources and environment to do this study.

REFERENCES

[1] Council of Europe, "Recommendation No. R (97) 5 on the Protection of Medical Data," adopted by the Committee of Ministers on 13 of February 1997 at the 584th meeting of the Ministers' Deputies.

[2] I. Maglogiannis and E. Zafiropulos, "Modelling Risk in Distributed Healthcare Information Systems," The 28th Annual International Conference of the IEEE on Engineering in Medical and Biology Society (EMBS), 2006, pp 5447-5450.

[3] L. T. Kohn, J. M. Corrigan, and M. S. Donaldson (editors), "To Err Is Human: Building a Safer System," The National Academies Press, 2000.

[4] B. B. Christopher, "Recent Developments Affecting Depository Institutions," FDIC Banking Review, Vol. 8, No. 3, 1996.

 ISBN: 978-1-61208-243-1

[5] AhnLab, "Online Banking: Threats and Countermeasures", White paper, 2010. URL http://www.techrepublic.com/whitepapers/online-banking-threats-and-countermeasures/2557803, last accessed 13.10.2012.

[6] G. N. Samy, R. Ahmad, and Z. Ismail, "Threats to Health Information Security," Proceedings of the Fifth International Conference on Information Assurance and Security (IAS), Xi'an, China, 2009.

[7] T. R. Peltier, "Information Security risk Analysis," Auerbach Publications: Boca Raton, FL, 2005.

[8] B. Jung, I. Han, and S. Lee, "Security threats to internet: a Korean multi-industry investigation," Information & Management, Vol. 38, No. 8, 2001, pp. 487-498.

[9] R. Power, "CS/FBI Computer Crime and Security Survey," Computer Security Issues & Trends, Vol. 8, No. 1, Spring 2002.

[10] R. Ahmad, G. N. Samy, N. Khilwani, P. A. Bath, and Z. Ismail, "Threats Identification in Healthcare Information Systems using Genetic Algorithm and Cox Regression," In Fifth International Conference on Information Assurance and Security (IAS), Xi'an, China, 2009.

[11] British Standards Institution, "Health Informatics - Information Security Management in Health using ISO/IEC 27002," (ISO27799:2008), London, 2008.

[12] E. Vaast, "Danger is in the eye of the beholders: social representations of information systems security in healthcare," Journal of Strategic Information Systems, Vol. 16, Issue 2, June, 2007, pp. 130-152.

[13] I. Maglogiannis, E. Zafiropoulos, A. Platis, and C. Lambrinoudakis, "Risk analysis of a patient monitoring system using Bayesian Network modelling," Journal of Biomedical Informatics, Vol. 39, Issue 6, 2006, pp. 637-647.

[14] British Standards Institution, "Information Technology - Security Techniques: Code of Practice for Information Security Management," BS ISO/IEC 27002:2005 BS 7799-1:2005, London, 2005.

[15] A. Hiltgen, T. Kramp, and T. Weigold, "Secure Internet Banking Authentication," IEEE Security & Privacy, Vol. 4, Issue 2, 2006, pp. 21-29.

[16] A. Tiwari and S. Sanyal, A. Abraham, S. J. Knapskog, and S. Saynal, "A Multi-factor Security Protocol for Wireless Payment-Secure Web Authentication using Mobile Devices," IADIS International Conference Applied Computing, pp. 160-167, 2007

[17] O. Dandash, P. D. Le, and B. Srinivasan, "Security Analysis for Internet Banking Models," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp.1141-1146, 2007.

[18] X. Hu, G. Zhao, and G. Xu, "Security Scheme for Online Banking Based on Secret Key Encryption," Second International Workshop on Knowledge Discovery and Data Mining, pp.636-639, 2009.

 ISBN: 978-1-61208-243-1