Industry Contingent Security Threats to Internet-based Business

Bumsuk Jung[a], Ingoo Han[b], and Sangjae Lee[c]

[a]*Enterprise Solution Division, Tong Yang Systemhouse Corp.*
24, Ogum-Dong, Songpa-gu, Seoul, 138-130, Korea
Tel: +82-2-405-7560 Fax: 82-2-402-6183, e-mail: bsjung@tysystemhouse.com

[b]*Korea Advanced Institute of Science and Technology*
207-43 Cheongryangri-Dong Dongdaemun-Gu, Seoul 130-012 Korea
Tel: +82-2-958-3613, Fax: 82-2-958-3604, e-mail: ighan@kgsm.kaist.ac.kr

[c]*Korea Advanced Institute of Science and Technology,*
207-43 Cheongryangri-Dong Dongdaemun-Gu , Seoul 130-012 Korea
Tel: +82-2-958-3673, Fax: 82-2-958-3604, e-mail: sangjae@kgsm.kaist.ac.kr

Absrtact

In recent years, a number of security problems with *the Internet* have become apparent. New and existing Internet users need to be aware of the high potential for security incidents from the Internet and the steps they should take to secure their sites. Before designing a secure system, it is advisable to identify the specific threats against which protection is required. The threats for Internet are classified into *interruption*, *interception*, *modification*, and *fabrication*. The extents of these threats are examined across four industries - manufacturing, banking/financial, research institution/university, and distribution/service. Banking/financial firms generally perceive the four categories of threats to the Internet more seriously than other industries. The companies in manufacturing industry consider *interruption* more seriously than other threats. Research institutions/universities and distribution/service companies regard *modification* and *interruption* as more critical threats than other threats.

Introduction

New and existing Internet users need to be aware of the high potential for computer security incidents from the Internet and the steps they should take to secure their sites. Before designing a secure system, it is advisable to identify the specific threats against which protection is required. This is known as *threat assessment* [1]. Many measures and mechanisms now exist to provide sites with a higher level of assurance and protection. The importance of security to users of the Internet can no longer be seen as the secondary.

The purpose of this paper is to present the threats posed by the Internet security and to examine the difference in each of threats across four industries. The threats for Internet are classified into *interception*, *fabrication*, *modification* and *interruption*. The extents of these threats are suggested across four industries - manufacturing, banking/financial, research institution/university, distribution/service. Each site has different needs; for instance, the security needs of a corporation might well be different than the security needs of an academic institution [4]. Any security plan has to conform to the needs of the site. The exact security needs of systems, however, will vary across industries, and each industry is encountered with the different threats from the Internet. Appropriate security services to enhance the Internet security are also described.

Security Threats to Internet

Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements [2, 7, 8, 10], confidentiality, integrity, and availability. Network security becomes important to provide the network entities with completely reliable network services, in terms of the *confidentiality, integrity* and *availability* [6].

(1) Confidentiality: a requirement whose purpose is to keep sensitive information from being disclosed to unauthorized recipients. Confidentiality indicates that assets of IS are accessible only by authorized users. The types of access include "read" -type access: reading, printing, or viewing. Confidentiality might be important for national security, law enforcement, competitive advantage, and personal privacy.

(2) Integrity: a requirement meant to ensure that information and programs are changed only in a specified and authorized manner. It may be important to keep data consistent or to allow data to be changed only in an approved manner. Integrity is a measure of the information's accuracy and reliability (Smith 1989).

(3) Availability: a requirement intended to ensure that

systems work promptly and service is not denied to authorized users. Those objects to which an authorized user has legitimate access should be available when he or she demands proper access. From a security standpoint, it represents the ability to protect against and recover from a damaging event. The availability of properly functioning computer systems is essential to the operation of many large enterprises and sometimes for preserving lives.

Security threats that can arise in the Internet will compromise the controls to ensure security requirements. The threats in the Internet are similar to those that may occur in any existing international or national computer networks. The "threats" to assets are circumstances that have the potential to cause loss or harm; human attacks are examples of threats, as are natural disasters, inadvertent human errors, and internal hardware and software flaws [3, 8]. In this study network security threats are categorized as *interruption*, *interception*, *modification*, *fabrication* [5, 11]. The four categories of threats can be described as follows:

(1) *Interruption*: An asset of the system is destroyed or becomes unavailable. Examples include destruction of a piece of hardware, such as a hard disk, the disabling of the file management system, erasure of a program or data file, or failure of an operating system manager.
(2) *Interception*: An unauthorized party gains access to an asset. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, the illicit copying of files or programs and traffic analysis.
(3) *Modification*: The content of a data transmission is altered without detection and results in an unauthorized effect. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.
(4) *Fabrication*: An unauthorized party inserts counterfeit objects into the system. Examples include the insertion of spurious messages in a network or the addition of records to a file.

The types of threats on the security of a network can be characterized by viewing the function of the computer system as providing information. In general, there is a flow of information from a source to a destination [8]. This normal flow and four general categories are depicted in Figure 1.

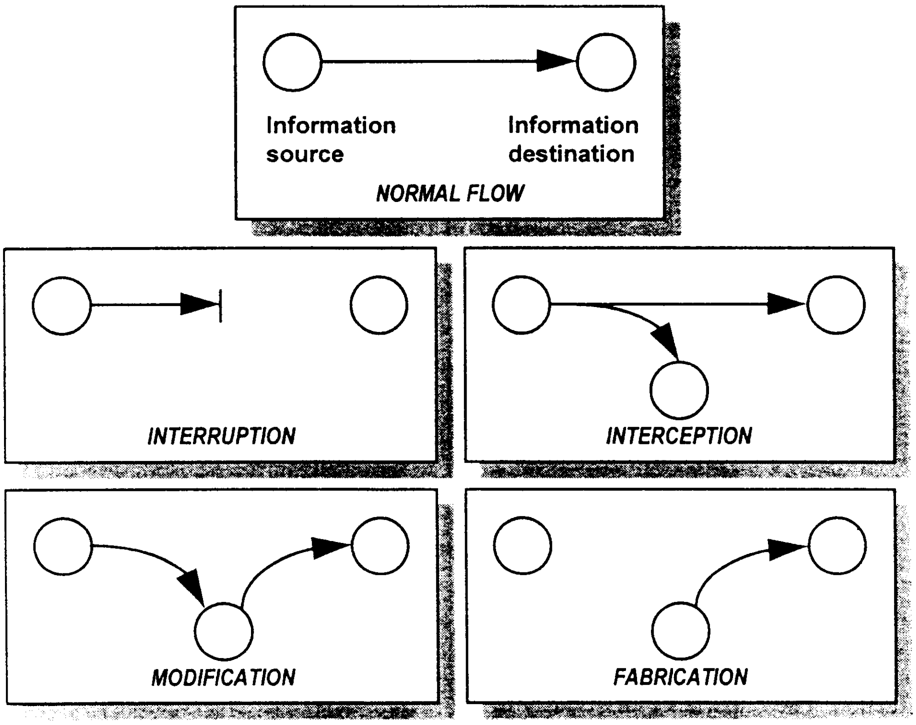

Figure 1: Categories of Security Threats

Three major requirements are related to the four threats. Interruption is a threat to availability as assets become lost or unusable from its occurrence. Interception badly affects confidentiality of an asset as some authorized party has gained access to an asset and read the data or program files. Modification of assets becomes a threat to integrity as an unauthorized party not only access but tampers with an asset. Fabrication also lowers integrity of assets as spurious transactions may be added to a network communication system or an existing database.

There are differences among the industries in the overall level of threats to the security requirement in the Internet. The weight given to each of the three major requirements describing needs for information security - confidentiality, integrity, and availability - depends strongly on circumstances [7]. For example, a system that must be restored within an hour after disruption represents, and requires, a more demanding set of policies and controls than does a similar system that need not be restored for two to three days. There are differences among the industries in the overall level of threats to the security requirement in the Internet. Organizations are arbitrarily categorized into four industries, each of which has different requirement with regard to network security. The four categories selected are manufacturing, banking / financial, research institution / university, distribution / service.

Methods

Research Design

The research addressed two question: (1) What is the general state of Internet security? and (2) What is the difference in four kids of threats (*interception*, *fabrication*, *modification* and *interruption*) across industries (Manufacturing, Banking/Financial, Research Institution/University, Distribution/Service)? To check for external validity and relevancy, the questionnaire was pilot-tested by several graduate students and IS professors at Korea Advanced Institute of Science and Technology. The participants were asked, "Evaluate the importance of each security requirement of your organizations considering the threats from the Internet." and "Evaluate the extent of damage to your system and operation, assuming each threat is manifest." A five-point Likert-type scale represented each item.

The data used in this research were obtained by using the mail survey technique. The questionnaire instruments were sent to a random sample of 1006 senior MIS managers and data processing center managers in Korea. The respondents are the persons in charge of MIS department or data processing center. The organizations were randomly drawn from the Internet Web that introduces Korean organizations. 150 organizations returned the instruments, for a response rate of 14.9 percent, which is usual for a mail survey. Some participants may have elected not to respond and others refused to respond to selected questions due to unfamiliarity of the subject.

Table 1 shows a classification of the sample by the industry of the sampled organizations. The sample consists of manufacturing (28.7%), banking/financial service (25.3%), research institution/university (27.3%), and distribution/service (16.7%).

Table 1: Distribution of Four Industries

Industry	Total Number	% of Organizations
Manufacturing	43	28.7
Banking/Financial	38	25.3
Research/University	41	27.3
Distribution/Service	25	16.7
Others	3	2.0
Total	150	100

Data Analysis and Results

Analysis of variance (ANOVA) is used to test whether there exist significant group differences with respect to the overall level of threats from the Internet; the result is presented in Table 2. The overall level of threats is represented by the mean values of the threats. The *F* probability indicates a strong support for our expectations regarding the differences between industries for overall level of threats.

Table 2: Result of ANOVA - Differences in Threats

Industry	Mean	Std. Dev.	F-value	p-value
Manufacturing	16.14	3.59	7.01	0.0002
Banking/Financial	18.84	2.27		
Research/University	15.80	3.64		
Distribution/Service	16.08	3.56		

T-tests of group differences are conducted between industries to see the difference in the overall level of threats. Table 3 shows that banking / financial firms perceive the overall level of threats most seriously, compared with others. While there are statistically significant differences between banking/financial firms and others, there are no significant differences between other pairs; manufacturing firms and distribution/service, manufacturing firms and research / university, distribution / service and research / university.

Table 3: Results of t-Test of Differences in Threats

(T-value is provided for the difference between industries in column and row.

Number in parenthesis indicates two-tailed significance.)

	Manufacuring	Banking/ Financial	Research/ University	Distribution/ Service
Manufacturing	—	—	—	—
Banking/ Financial	-4.09 (0.000)	—	—	—
Research/ University	0.43 (0.668)	4.49 (0.000)	—	—
Distribution/ Service	0.07 (0.943)	3.45 (0.001)	-0.30 (0.765)	—

With respect to for each category of the threats from the Internet, ANOVA was used to test whether there were significant differences among industries. The *F*-probabilities shown in Table 4 provide strong support for the difference of the perceived seriousness of each threat among industries.

Table 4: Results of ANOVA - Differences in Threats

	Industry	Mean	Std. Dev.	F-Value	F-Prob.
Interruption	Banking/Financial	4.76	0.58	5.11	0.0022
	Manufacturing	4.23	1.02		
	Distribution/Service	4.10	1.05		
	Research/University	4.01	0.96		
Interception	Banking/Financial	4.53	0.79	5.11	0.0022
	Manufacturing	4.00	1.18		
	Distribution/Service	3.94	0.91		
	Research/University	3.65	1.06		
Modification	Banking/Financial	4.76	0.62	4.52	0.0040
	Research/University	4.14	1.07		
	Manufacturing	4.08	1.11		
	Distribution/Service	3.98	1.08		
Fabrication	Banking/Financial	4.79	0.57	6.31	0.0005
	Distribution/Service	4.06	1.15		
	Research/University	4.01	1.11		
	Manufacturing	3.83	1.08		

The comparison of mean threat value indicate that the mean value for *interruption*, *fabrication*, *modification*, and *interruption* is higher than for other threats in manufacturing, banking/financial, research institution/university, and distribution/service industries, respectively. For instance, manufacturing and distribution/service companies perceive *interruption* as more critical threats than others. This indicates the availability of information is important for these industries. The key to effective use of Internet in these industries is to integrate information collected through Internet with internal IS applications so that effectiveness and efficiency of the operation can be improved. Better customer service and improved inter-firm relationships are possible from system integration because customers' needs can be promptly met. This is especially critical in systems such as JIT (Just In Time) production systems and quick-response retailing systems. The threats of *interruption* to these systems should be greater because the response and turnaround times are critical for the success of the system.

The threats of *fabrication* are slightly more important than other threats for banking/financial companies. Integrity can be critical in payment systems than other requirements when a large number of transactions occur repetitively and minor errors in value or quantity of transactions cannot be allowed. The threats of interception is less critical than others, reflecting that the occurrence of computer abuse using others' identification is less concern among IS managers. The threat of *modification* is greater than others in research/universities, especially than the threat of *interception*. This states that the respondents in the research institution and universities believe themselves to be at low risk from external intruders to reveal and utilize the research data and results stored in their systems. However, they are anxious about that the data and research results might be altered or modified, as it takes much times and efforts to produce these research results.

T-tests of the difference between the mean threat values for the industries are conducted. The results of the t-tests are presented in Table 5 and show that while there exit statistically significant differences between banking/financial firms and others at 0.05 significance level in the case of each threat, there were no significant differences between others. That is, the expectation that there are differences among industries for the level of each threat is supported. Further, it indicates that, compared with other industries, banking/financial firms perceive the magnitude of the damage from each category of the threats most seriously.

Implications and Conclusions

The results suggest several implications for practitioners to cope with Internet threats. First, banking/financial firms generally perceive the four categories of threats to the Internet more than other industries. Poorly controlled vulnerabilities in financial applications connected to Internet expose organizations to fraud that can result in major financial losses and embarrassment. The opportunity to commit a major EFT fraud is much greater then what some financial managers predict. Computer crimes or "opportunistic behaviors" are more likely to occur because of greater motive and opportunity to obtain illicit benefits. This validates the fact that Internet security market in financial application is rapidly responding to the threats by providing authentication and encryption technologies to the customers and by implementing new products.

Second, the results indicate strong support for our expectations regarding the differences between industries for both overall level of threats and level of each threat. Companies in manufacturing industry consider interruption more seriously than other threats. Research institutions/universities and distribution/service companies regard modification and interruption as more critical threats than other threats, respectively. Internet connections will never be 100 percent secure; an organization should assess the threats it is trying to prevent and weigh the benefits against costs of various security measures [9]. The threats for Internet that are classified into interception, fabrication, modification and interruption are different across industries due to various demands for security requirements; confidentiality, integrity, and availability. Companies should understand the security requirements of their industry and prepare for appropriate security services suggested in this study. Since available resources are limited, it is not possible for IS managers to develop all of the necessary controls. The guidance of control designs needs to be given such that the extent of critical threats can be reduced appropriately The appropriate levels of various controls should be determined in view of industrial contingencies. Different industrial environments can be considered to affect the sensitivity and vulnerability of the system and the desirable levels of various controls.

Table 5: Differences in each Threat between Industries
(T-value is provided for the difference between industries in column and row. Number in parenthesis indicates two-tailed significance.)

(a) Interruption

	Manufacturing	Banking/ Financial	Research/ University	Distribution/ Service
Manufacturing	—	—	—	—
Banking/ Financial	-2.94 (0.004)	—	—	—
Research/ University	1.02 (0.311)	4.25 (0.000)	—	—
Distribution/ Service	0.50 (0.616)	2.88 (0.007)	-0.36 (0.722)	—

(b) Interception

	Manufacturing	Banking/ Financial	Research/ University	Distribution/ Service
Manufacturing	—	—	—	—
Banking/ Financial	-2.39 (0.019)	—	—	—
Research/ University	1.44 (0.152)	4.20 (0.000)	—	—
Distribution/ Service	0.22 (0.827)	2.72 (0.008)	-1.15 (0.254)	—

(c) Modification

	Manufacturing	Banking/ Financial	Research/ University	Distribution/ Service
Manufacturing	—	—	—	—
Banking/ Financial	-3.45 (0.001)	—	—	—
Research/ University	-0.23 (0.817)	3.22 (0.002)	—	—
Distribution/ Service	0.37 (0.715)	3.22 (0.002)	0.58 (0.566)	—

(d) Fabrication

	Manufacturing	Banking/ Financial	Research/ University	Distribution/ Service
Manufacturing	—	—	—	—
Banking/ Financial	-4.56 (0.000)	—	—	—
Research/ University	-.70 (0.487)	3.96 (0.000)	—	—
Distribution/ Service	-.75 (0.456)	2.95 (0.006)	-0.17 (0.867)	—

Third, the security function is not widely implemented by organizations in Korea, even though they perceive the threats from the Internet seriously. The responding organizations might not be familiar with the Internet, and much less with the threats from the Internet. There are few organizations that experienced the attacks from intruders. There is generally little computer abuse in the system connected with Internet so it is difficult to justify the investment of controls in order to reduce computer abuse. The use of Internet in Korea is rapidly growing and the results of this study may reflect unique characteristics of Korean companies. The significance of some threats may change as the diffusion of Internet based system proceeds. For instance, as the strategic impact of Internet-based system in manufacturing becomes greater and the system takes an integral part of IS in the future, the influence of the threats to integrity of system (i.e., modification, fabrication) on system security may become greater and appropriate integrity controls will be more needed.

This study addresses the threats to Internet security. The first step IS managers can take to secure a corporate network environment connected to Internet is to understand the range of threats associated with Internet access. The desired security measures must then be implemented against each of these threats. The level of threats would vary by industries: manufacturing, banking/financial, distribution/service, research institution/university. This study presents an initial attempt to collect the empirical data concerning the seriousness of perceived threats as well as the Internet overall security.

Furthermore, against those threats, appropriate and available security services are described, according to the mapping threats to security service. Currently, the OSI security architecture and security services have been defined and are in the process of being internationally voted on. The work of ISO, aimed at achieving an architecture for secure OSI communications and secure communication protocols, has been presented.

References

[1] Bayle, A.J. 1988. Security in Open System Networks: A Tutorial Survey. *Information Age* 10(3):131-145.

[2] Carnahan, L.J. 1992. A Local Area Network Security Architecture. In *Proceedings of The 15th National Computer Security Conference*:340-349.

[3] Cooper, J.A. 1989. *Computer and Communication Security*. McGraw-Hill.

[4] Holbrook, P. and Reynolds, J. 1991. *Site Security Handbook*, RFC 1244, Internet Engineering Task Force.

[5] Jung, J.W. 1995. Introdution to Network Security. In *Proceedings of The 1st Korea Computer Network Security Workshop*: 5-50.

[6] Muftic, S. 1989. *Security Mechanisms for Computer Networks*. John Wiley & Sons.

[7] National Research Council (NRC), 1991. *Computers at Risk: Safe Guarding in the Information Age*. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Academy press.

[8] Pfleeger, C.P. 1989. *Security in Computing*. Prentice Hall.

[9] Santos, R.A.. 1999. Internet Security. *IS Audit & Control Journal* (1):33-38.

[10] Smith, M.R. 1989. Computer Security - Threats, Vulnerabilities and Countermeasures. *Information Age* 11(4):205-210.

[11] Stallings, W. 1995. *Network and Internetwork Security Principles and Practice*. Prentice Hall.