한국경영정보학회
96년 춘계학술대회

A Study on Risk Analysis and Security Mechanisms for the Internet Security

Bumsuk Jung*
Ingoo Han**

Abstract

In recent years, a number of security problems with the *Internet* have become apparent. New and exiting 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. The importance of security to users of the Internet can no longer be seen as the secondary.

This research address two questions: (1) What are the most serious threats to organizations in the Internet? and (2) What are the appropriate countermeasures against those threats?

The purpose of this paper is to describe a process that can be used to improve the security to the Internet. And, this paper describes threats posed by the Internet security and presents security service and mechanisms available today to enhance the Internet security. Security requirements, security threats, security service, and security mechanisms are addressed dependently. Hence, the requirements of organizations for the Internet security can be considered. Furthermore, based on the result of this study and exiting literature, the gradual process for determining the priorities for Internet security is provided for practical applications.

The exact security needs of systems will vary from organization to organization. By industrial classification, threat assessment that identify and evaluate the threats from the Internet are presented.

Viewing the findings from mail survey, the results of statistical tests indicate strong support for our expectations regarding the differences between industries for both overall level of threats and level of each threats. The threats from the Internet are perceived by banking/financial firms most seriously, comparing with others. Furthermore, our expectation that there is a priority ordering the threats within each organizations is partially supported. The security function, however, is not widely implemented by organizations in Korea.

Key word : Internet, Security , Security Requirements, Security Threats, Security Services, Security Mechanisms, Threat Assessment, Risk Analysis

---

* Dongyang SHL
** Department of Management Information Systems, KAIST, Seoul, Korea

INTRODUCTION

This paper describes threats posed by the Internet security and presents security service and mechanisms available today to enhance the Internet security. Each site has different needs; the security needs of a corporation might well be different than the security needs of an academic institution [Holbrook, et. al 1991]. Any security plan has to conform to the needs and culture of the site. The exact security needs of systems, however, will vary from organization to organization, and each organization is encountered with the different threats from the Internet.

Before designing a secure system, it is advisable to identify the specific threats against which protection is required. This is known as *threat assessment* [Bayle 1988]. By industrial classification, the threat assessment that identify the specific threats against which protection is required preferentially are presented. Based on ranked threats, appropriate security measures are described.

That is, security requirements, security threats, security services, and security mechanisms are addressed dependently and the requirements of organizations for security can be considered.

SECURITY REQUIREMENT

Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements [Carnahan 1992] :

Confidentiality A requirement whose purpose is to keep sensitive information from being disclosed to unauthorized recipients. The secrets might be important for national security, law enforcement, competitive advantage, and personal privacy.

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.

Availability A requirement intended to ensure that systems work promptly and service is not denied to authorized users. From a security standpoint, it represents the ability to protect against and recover from a damaging event.

SECURITY THREATS

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 [Pfleeger 1989; Cooper 1989]. Network security threats generally can be categorized as follows [Stallings 1995; Jung 1995]:

Interruption An asset of the system is destroyed or becomes unavailable.

Interception An unauthorized party gains access to an asset. The unauthorized party could be a person, a program, or a computer.

Modification The content of a data transmission is altered without detection and results in an unauthorized effect [Bayle 1988].

Fabrication An unauthorized party inserts counterfeit objects into the system.

SECURITY SERVICE

Security services are abstract concepts that can be employed to characterize security requirements [Kent 1992]. A paper by Carnahan (1992) stated that a security service is the collection of security mechanisms, procedures, etc. that are implemented to help reduce the risk of associated threats.

The OSI security architecture defines five primary security services as follows [Bayle 1988; Karila 1991; Kent 1992; Jung 1994]:

Data Confidentiality This is defined as "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes".

Access Control This provides "the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner".

Authentication Data origin authentication is defined as "the corroboration that the source of data received is as claimed." Peer-entity authentication is defined as "the corroboration that a peer entity in an association is the one claimed".

Data Integrity This service provides for the integrity of all user data and detects any modification, insertion, deletion or replay.

Nonrepudiation It is defined as preventing "denial by one of the entities involved in a communication of having participated in all or part of the communication."

SECURITY MECHANISMS

ISO 7498-2 includes brief descriptions of a set of security mechanisms, and a table that relates these mechanisms to security services. This list of mechanisms is neither fundamental nor comprehensive [Kent 1992].

Encipherment This is an essential security mechanism that can provide confidentiality of either data or traffic flow of information and can play a part in or complement a number of other security mechanisms [Bayle 1988].

Digital Signature Using asymmetric cryptography, a signature may be generated by computing a checksum function on the data to be signed, and then enciphering the resulting value with the private component of the originator's asymmetric key pair. A recipient validates a signature by deciphering the signature value, using the public component of the originator's asymmetric key pair, and then comparing the result to the checkvalue computed on the data by the recipient [Kent 1992].

Access Control Mechanisms These mechanisms use the authenticated identity of an entity, its capabilities to determine and enforce the access rights of that entity [Bayle 1988].

Data Integrity Mechanisms Data integrity is closely coupled with confidentiality and can be provided with an Integrity Check Value calculated by using symmetric or asymmetric encryption mechanisms [Karila 1991].

Authentication Exchange The mechanisms may be incorporated into a layer in order to provide peer-to-peer entity authentication. If the mechanisms does not succeed in authenticating the entity, the connection is rejected and terminated [Bayle 1988].

Traffic Padding Traffic padding may involve the generation of spurious traffic, padding of legitimate packets, and transmission of packets to other than the intended destination [Kent 1992].

Routing Control Routing control mechanisms make sure that the routes used by the data across the network are those that have been specified [Bayle 1988].

Notarization This mechanisms provides the assurance that the properties about the data communicated between two or more entities, such as their integrity, origin, time and destination are really what they are claimed to be [Bayle 1988].

RESEARCH MODEL

As reviewed previously, we consider the Internet security at the viewpoint of security requirements, security threats, security services and security mechanisms. Because those security elements map to the security requirements, the mapping provides the framework for developing the protection measures. This mapping to the security requirements bounds the scope of the other elements, and clarifies the effort required to address each element. The research model was developed and depicted in *Figure 1*.

THREAT-SERVICE MAPPING

Figure 2 provides a matrix to show the detail relationships between the threats and security

services.

Data origin authentication is tightly coupled to connectionless data integrity, in that it does not seem very useful to be assured of the source of data if its integrity cannot be established. Peer-entity authentication implies timeliness because of the binding of the identity of the peer entity to a specific association. Thus, the attacks involving the replay of data associated with another association can be thwarted through reliance on this service. Here there is a natural coupling with connection-oriented integrity [Kent 1992].

Access control service provides protection against unauthorized use of a resource. This protection service is applied to various types of a access to a resource [Bayle 1988].

Data confidentiality service helps to protect data on workstations, file servers, etc. from unauthorized disclosure [Carnahan 1991].

The connection-oriented integrity service provides for the detection of any modification, insertion, deletion, or replay of any data within a packet sequence. The use of connection-oriented integrity in conjunction with peer-entity authentication provides a high degree of protection against a wide range of active attacks [Kent 1992].

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver [Stallings 1995].

SERVICE-MECHANISM MAPPING

ISO 7498-2 includes brief descriptions of a set of security mechanisms, and a table that relates these mechanisms to security services. *Table 1* indicates the security mechanisms, alone or in combination with others, used to provide each security service.

Encipherment typically is used to provide confidentiality, but also can support other security

services. This support arises because some techniques for effecting encipherment have the property that any modification of ciphertext results in unpredictable modification of the underlying plaintext. When such techniques are employed, they provide a good basis for integrity and authentication mechanisms at the same or higher layers [Kent 1992].

If the proper form of checkvalue is employed, digital signature can support the nonrepudiation service. It can also support authentication and integrity services where identity of an entity that will validate signed data is not known in advance, or where multiple entities may need to validate the signature [Kent 1992].

If the entity attempts to use an unauthorized resource, or authorized resource with an improper type of access, then the access control function will reject the attempt.

There are a variety of mechanisms used to assure the integrity of a data unit or stream of data [Bayle 1988]. For connection-oriented data transmission, protecting the integrity of a sequence of data units, namely, protecting against misordering, losing, replaying and inserting or modifying data, requires some additional explicit ordering mechanism such as sequence numbering, time stamping or cryptographic chaining.

Authentication exchange may be incorporated into a layer in order to provide peer-to-peer entity authentication. When cryptographic techniques are used, they may be combined with handshaking protocols to protect against replay, i.e. to ensure liveness.

Traffic padding can be used to provide various levels of protection against traffic analysis and offer some traffic flow confidentiality [Kent 1992]. Traffic padding may involve the generation of spurious traffic, padding of legitimate packets, and transmission of packets to other than the intended destination.

Routing Control is another mechanism in support of confidentiality. It is employed to constrain the paths that data traverse from source to destination. This mechanism make sure that the routes used by the data across the network are those that have been specified [Kent

1992].

The most commonly cited use for notarization is in conjunction with nonrepudiation services [Kent 1992]. This mechanism provides the assurance that the properties about the data communicated between two or more entities, such as their integrity, origin, time and destination are really what they are claimed to be.

HYPOTHESES

The weight given to each of the three major requirements depends strongly on circumstances [System 1991]. For illustration, and to make the problem tractable, organizations are arbitrarily categorized into four types, each of which has different requirement with regard to network security. The four categories selected are [System 1991]:

Banking Financial These organizations must protect the integrity of account records and of individual transaction. Protection of personal privacy (credit histories) is important, but not critically so.

Manufacturing The secrets might be important for reasons of competitive advantage (manufacturing costs or bidding plans). The risk of loss of confidentiality with respect to a major product announcement will change with time.

Research Institution/University Since the product of these organizations is accumulated research records and security is important for private information, interception is the most important threat. Alteration of data would be of almost equal concern.

Distribution/Service The availability of properly functioning computer systems (e.g., for handling airline reservations) is essential to the operation of many service firms.

Based on above description, the hypotheses are developed as follows :

H 1 *For the overall level of threats to the security requirement in the Internet, there are differences among the industries.*

H 1.1 For the level of Interception, there are differences among the industries.

H 1.1 For the level of Fabrication, there are differences among the industries.

H 1.2 For the level of Modification, there are differences among the industries.

H 1.4 For the level of Interruption, there are differences among the industries.

H 2 In each of the industries, there exist a priority order for the threats to the security requirement in the Internet.

H 2.1 To the manufacturing firms, the threat of interception (threats to confidentiality) is prior to others.

H 2.2 To the banking/financial firms, the threat of fabrication and modification (threats to integrity) are prior to others.

H 2.3 To the research institution/university, the threat of interception (threats to confidentiality) is prior to others.

H 2.4 To the distribution/service firms, the threats of interruption (threats to availability) is prior to others.

DATA COLLECTION

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 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.

SURVEY SAMPLE

The sample consists of manufacturing (28.7%), banking/financial service (25.3%), research institution/university (27.3%), and distribution/service (16.7%). *Table 2* presents information on the types of connection to the Internet, the purpose of using the Internet, the organized level of

department in charge of security, the level of documentation that state the Internet security policy, procedure, and standard, the Internet security countermeasures implemented.

As shown in *Table 2*, the percentage of dial-in connection is relatively high in manufacturing and banking/financial firm. It suggests that they perceive the threats from the Internet more seriously than others. Besides, most organizations use the Internet for the purpose of collecting the information for their operation or business. The low percentage of the electronic commerce presents that it has not been activated yet in Korea, due to several reasons such as security. It also suggests that the security function is less widely implemented in industries like manufacturing and banking/financial firms than in all other organizations. Among responding organizations, the number of organizations that have department of security or security policy are low.

THE DIFFERENCES OF THE THREATS AMONG INDUSTRIES

Analysis of variance (ANOVA) was 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 3(a)*. The value of overall level of threats are the mean values for the threats for which each industry evaluated. Viewing this result from the perspective, the F probability indicates strong support for our expectations regarding the differences between industries for overall level of threats.

To explore this further, t-tests of group differences were conducted between industries for the overall level of threats. Results presented in *Table 3(b)* show that while there were statistically significant differences between banking/financial firms and others at the high significance level, there were no significant differences between other industries. Those empirical results indicate that banking/financial firms perceive the overall level of threats most seriously, compared with others.

THE DIFFERENCES OF THE EACH THREATS AMONG INDUSTRIES

Hypothesis 1.1, 1.2, 1.3, and 1.4 can be tested for each category of the threats from the Internet. With respect to each threats, ANOVA was used to test whether there were significant differences among industries. The *F*-probabilities shown in *Table 4* provide strong support for the *hypothesis 1.1, 1.2, 1.3, and 1.4* that the perceived seriousness of each threats will differ among industries.

T-tests of the difference between the mean values for the industries were conducted to test further. The results of the *t*-tests are presented in *Table 5(a), 5(b), 5(c), and 5(d)*, respectively and show that while there exit statistically significant differences between banking/financial firms and others at the high 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 threats 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.

PRIORITY ORDER FOR THE THREATS IN EACH INDUSTRY

In order to test the hypothesis 2, we need to conduct both of following tests. The first one is a mean value test, which compares the absolute mean value for a threat to those for others. The second one is a pairwise t-test, which tests the differences in mean value between threats in a pairwised manner. The results shown below partially correspond to our expectation that there is a priority order in the threats within each industries.

Priority Order in Manufacturing Firms The results of mean value test (presented in *Table 6*) indicate that the mean value for interruption is higher than for others. The results of pairwise *t*-test showed that while there were significant differences between interruption and interception as well as interruption and fabrication, the differences between other threats were not

statistically significant. Hence, the results of both tests do not support the *hypothesis 2.1*.

Priority Order in Banking Financial Firms As presented in *Table 7*, the mean value for fabrication is higher than for others. The mean values for fabrication, modification, and interruption were so close that it appeared that there might not be a significant difference between these threats. The results of pairwise *t*-test, even though there were significant differences between fabrication and interception, indicate partial support for the *hypothesis 2.2*.

Priority Order in Research Institution/University *Table 8* indicate that the mean value for modification is higher than for others. The *hypothesis 2.3*, hence, cannot be accepted due to only the result of mean value test showing that the mean value for interruption is not higher than for others but for interception.

Priority Order in Distribution/Service Firms *Table 9* shows that the mean value for interruption is higher than for others. This corresponds to our expectation that distribution/service firms perceive the threat of interruption as the most serious one. The results of pairwise *t*-test, however, showed that there were not statistically significant differences between those threats.

CONCLUSION

This study address the Internet security at the viewpoint of security requirements, security threats, security services, and security mechanisms. Based on the existing literature, the relationship between security threats and security services was provided. In creating the list of threats, we believed that their importance would vary by industries : banking/financial, manufacturing, distribution/service, research institution/university.

Its major contribution is to find that the threats from the Internet vary among industries. Through threat assessment, this study presents an initial attempt to collect the empirical data concerning the seriousness of perceived threats as well as the Internet security. Viewed from an organization's perspective, the findings point to some implications for the organization.

Furthermore, against those threats, appropriate and available security measures are described, according to the mapping threats to security service. The work of ISO, aimed at achieving an architecture for secure OSI communications and secure communication protocols, has been presented.

LIMITATIONS AND FURTHER RESEARCH ISSUES

The security countermeasure is divided into technical measures, managerial measures, physical measures, and legal measures [Park, et.al 1994]. In this study, technical measures were emphasized for the Internet security. However, in order to implement effective security, these measures should be kept pace with others. One direction for future research is to consider those measures in parallel.

Another direction would be the development of the more precise and detailed hypothesis. Even though in the same industry, there may exist some differences in security requirements according to whether it is a manufacturing firm with new technology or not.

REFFERENCE

1. Bayle, A. J. "Security in Open System Networks : A Tutorial Survey," *Information Age*, Vol.10, No.3, Jul 1988, pp. 131-145.
2. Carnahan, L. J. "A Local Area Network Security Architecture," In *Proceedings of The 15th National Computer Security Conference* 1992, pp. 340-349.
3. Cooper, J. A. *Computer and Communication Security*, McGraw-Hill 1989.
4. Cox, R. and M. O'Neill, "Risk Management of Complex Networks," In *Proceedings of The 15th National Computer Security Conference* 1992, pp.544-553.
5. Dennison, M. W. L. and K. C. Toth, "Practical Models for Threat/Risk Analysis," In *Proceedings of The 14th National Computer Security Conference* 1991, pp. 427-435.

6. Holbrook, P. and J. Reynolds, *Site Security Handbook*, RFC 1244, Internet Engineering Task Force, July 1991.

7. Jung, J. W. "Introdution to Network Security," In *Proceedings of The 1st Korea Computer Network Security Workshop* 1995, pp. 5-50.

8. Karila, A. T. "Open System Security : An Architectural Framework," 1991, available for anonymous *ftp* from `coast.cs.purdue.edu` as `/pub/doc/network/Arto_Karila_OpenSystemsSecurity.tar.Z`

9. Kent, S. "Architectural Security," In Lynch, D. C. and Rose, M. T. (Ed.), *Internet System Handbook*, Addison-Wesley 1992, pp. 369-419.

10. Knowles, T. "Security, OSI and Distributed Systems," *Information Age*, Vol. 11, No. 2, April 1988, pp. 79-84.

11. Lee, P. J. "Computer Information Security," In *Proceedings of The 6th workshop on Information security and cryptography* 1994, pp. 31-83.

12. Loch, K. D., H. H. Carr and M. E. Warkentin, "Threats to Information Systems : Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16, Jun 1992, pp. 174-186.

13. Muftic, S. *Security Mechanisms for Computer Networks*, John Wiley & Sons 1989.

14. NIST, "Connecting to the Internet: Security Considerations," *CSL Bulletin*, National Institute of Standards and Technology 1993.

15. Park, Y. H., S. J. Moon, S. H. Kim, S. K. Kang and J. H. Leem, "A Study on Prevention Scheme for Communication Network from Computer Crime," *Journal of Data Communication Security Institute*, Vol.4, No.2, Jun 1994, pp. 47-55.

16. Pfleeger, C. P. *Security in Computing*, Prentice Hall 1989.

17. Pierson, L. G. and E. L. Witzke, "A Security Methodology for Computer Networks," *AT&T Technical Journal*, May/June 1988.

18. Piscitello, D. M. and A. L. Chapin, *Open Systems Networking*, Addison-Wesley 1993.

19. Rainer, R. K., C. A. Snyder, and H. H. Carr, "Risk Analysis for Information Technology," *Journal of Mnagement Information Systems*, Vol.5, No.1, Summer 1991, pp. 129-147.

20. Seo, B. H. and S. C. Han, "A Study on The Security Countermeasure of KREONet and STIS," In *Proceedings of The 3th workshop on Information security and cryptography* 1991, pp. 20-61.

21. Shin, J. T., K. Y. Hong, and C. R. Kim, "On Security Technology in Secure Computer & Network System," In *Proceedings of The 3th workshop on Information security and cryptography* 1991, pp.201-213.

22. Smith, M. R. "Computer Security - Threats, Vulnerabilities and Countermeasures," *Information Age*, Vol.11, No.4, Oct 1989, pp. 205-210.

23. Stallings, W. *Network and Internetwork Security Principles and Prictice*, Prentice Hall 1995.

24. Straub, D. W. Jr. "Effective IS Security: An Empirical Study," *Information Systems Research*, Vol. 1, No. 3, 1990, pp. 255-276.

25. System Security Study Committee, *Computers at Risk*, National Academy press 1991.

MECHANISMS / SERVICES	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Authentication								
Peer Entity Authentication	Y	Y	.	.	Y	.	.	.
Data Origin Authentication	Y	Y	.	.	.	.	.	.
Access Control	.	.	Y	.	.	.	.	.
Confidentiality								
Connection Confidentiality	Y	.	.	.	.	.	Y	.
Connectionless Confidentiality	Y	.	.	.	.	.	Y	.
Selected field Confidentiality	Y	.	.	.	.	.	.	.
Traffic Flow Confidentiality	Y	.	.	.	.	Y	Y	.
Integrity								
Connection Integrity with recovery	Y	.	.	Y	.	.	.	.
Connection Integrity without recovery	Y	.	.	Y	.	.	.	.
Selected Field Connection Integrity	Y	.	.	Y	.	.	.	.
Connectionless Integrity	Y	Y	.	Y	.	.	.	.
Selected Field Connectionless Integrity	Y	Y	.	Y	.	.	.	.
Nonrepudiation								
Nonrepudiation, Origin	.	Y	.	Y	.	.	.	Y
Nonrepudiation, Delivery	.	Y	.	Y	.	.	.	Y

Y = The mechanism is considered to be appropriate, either on its own or in combination with other mechanisms.
. = The mechanism is considered not to be appropriate.

Table 1 Relationship of Security Services and Mechanisms

Questions	*Ind. 1*	*Ind. 2*	*Ind. 3*	*Ind. 4*	*All*
Types of Connection					
Dedicated Connection	11.6	2.6	52.0	58.5	28.7
Dial-In Connection	65.1	63.2	44.0	14.6	46.7
Both of Above	0.0	0.0	4.0	14.6	5.3
No Connection	7.0	18.4	0.0	4.9	8.7
Under Consideration	16.3	15.8	0.0	7.3	10.7

Purpose ✣					
Collecting Information	81.4	76.3	100.0	90.2	85.3
E-Mail	16.3	10.5	40.0	70.7	33.3
Electronic Commerce	0.0	0.0	16.0	0.0	2.7
Publicity	9.3	18.4	24.0	36.6	22.0
Others	2.3	2.6	0.0	12.2	4.7
Security Department					
Exists	0.0	15.8	8.0	9.8	8.0
Security Staff Exists	27.9	21.2	40.0	36.6	30.7
None	72.1	63.2	52.0	53.7	61.3
Levels of Documentation					
Documented	2.3	2.6	16.0	7.3	6.0
Under Consideration	51.2	50.0	36.0	68.3	52.7
Not Under Consideration	46.5	47.4	48.0	24.4	41.3

✣ Since multiple answers were allowed for this question, the total % might exceed 100 %.
Ind. 1 : Manufacturing Ind. 2 : Banking/Financial
Ind. 3 : Distribution/Service Ind. 4 : Research Institution/University

Table 2 Internet and Extent of Security

Industry	*Mean*	*Std. Dev.*	*F-Value*	*F-Prob.*
Manufacturing	16.14	3.59		
Banking/Financial	18.84	2.27		
Research/University	15.80	3.64		
Distribution/Service	16.08	3.56	7.01	.0002

Table 3(a) Result of ANOVA - Differences of the Threats among Industries

Industry		*t-Value*	*2-Tail Sig.*
Banking/Financial	vs.		
	Manufacturing	4.09	.000
	Distribution/Service	3.45	.001
	Research/University	4.49	.000
Manufacturing	vs.		
	Distribution/Service	.07	.943
	Research/University	.43	.668
Distribution/Service	vs.		
	Research/University	.30	.765

Table 3(b) Results of t-Test of the Threats between Industries

Industry	*Mean*	*Std. Dev.*	*F-Value*	*F-Prob.*
Interception				
Banking/Financial	4.53	.79		
Manufacturing	4.00	1.18		
Distribution/Service	3.94	.91		
Research/University	3.65	1.06	5.11	.0022
Fabrication				
Banking/Financial	4.79	.57		
Distribution/Service	4.06	1.15		
Research/University	4.01	1.11		
Manufacturing	3.83	1.08	6.31	.0005
Modification				
Banking/Financial	4.76	.62		
Research/University	4.14	1.07		
Manufacturing	4.08	1.11		
Distribution/Service	3.98	1.08	4.52	.0040
Interruption				
Banking/Financial	4.76	.58		
Manufacturing	4.23	1.02		
Distribution/Service	4.10	1.05		
Research/University	4.01	.96	5.11	.0022

Table 4 Result of ANOVA - Differences of Each Threats among Industries

Industry		*t-Value*	*t-Prob.*
Banking/Financial	vs.		
	Manufacturing	2.39	.019
	Distribution/Service	2.72	.008
	Research/University	4.20	.000
Manufacturing	vs.		
	Distribution/Service	.22	.827
	Research/University	1.44	.152
Distribution/Service	vs.		
	Research/University	1.15	.254

Table 5(a) Results of t-Test of Interception between Industries

Industry		*t-Value*	*t-Prob.*
Banking/Financial	vs.		
	Research/University	3.96	.000
	Manufacturing	4.56	.000
	Distribution/Service	2.95	.006
Research/University	vs.		
	Manufacturing	.70	.487
	Distribution/Service	.17	.867
Manufacturing	vs.		
	Distribution/Service	.75	.456

Table 5(b) Results of t-Test of Fabrication between Industries

Industry		*t-Value*	*t-Prob.*
Banking/Financial	vs.		
	Research/University	3.22	.002
	Manufacturing	3.45	.001
	Distribution/Service	3.30	.002
Research/University	vs.		
	Manufacturing	.23	.817
	Distribution/Service	.58	.566
Manufacturing	vs.		
	Distribution/Service	.37	.715

Table 5(c) Results of t-Test of Modification between Industries

Industry		*t-Value*	*t-Prob.*
Banking/Financial	vs.		
	Manufacturing	2.94	.004
	Distribution/Service	2.88	.007
	Research/University	4.25	.000
Manufacturing	vs.		
	Distribution/Service	.50	.616
	Research/University	1.02	.311
Distribution/Service	vs.		
	Research/University	.36	.722

Table 5(d) Results of t-Test of Interruption between Industries

Mean Value Test			
		Mean	*Std. Dev.*
Interruption		4.23	1.02
Modification		4.08	1.11
Interception		4.00	1.18
Fabrication		3.83	1.24
Pairwise t-Test			
Interruption	vs.		*t-Value*	*2-Tail Sig.*
	Modification	.78	.440
	Interception	2.13	.039
	Fabrication	2.12	.040
Modification	vs.		
	Interception	.39	.698
	Fabrication	1.93	.060

Table 6 Priority Tests for Manufacturing Firms

Mean Value Test			
		Mean	*Std. Dev.*
Fabrication		4.79	.57
Modification		4.76	.62
Interruption		4.76	.58
Interception		4.53	.79
Pairwise t-Test			
Fabrication	vs.		*t-Value*	*2-Tail Sig.*
	Modification	1.00	.324
	Interruption	.57	.571
	Interception	2.70	.010

Table 7 Priority Tests for Banking/Financial Firms

Mean Value Test			
		Mean	*Std. Dev.*
Modification		4.14	1.07
Fabrication		4.01	1.11
Interruption		4.01	.96
Interception		3.65	1.06
Pairwise t-Test			
Modification	vs.		*t-Value*	*2-Tail Sig.*
	Fabrication	1.73	.092
	Interruption	.90	.372
	Interception	2.91	.006
Interruption	vs.		
	Fabrication	.02	.986
	Interception	2.92	.006

Table 8 Priority Tests for Research Institution/University

Mean Value Test			
		Mean	*Std. Dev*
Interruption		4.10	1.05
Fabrication		4.06	1.15
Modification		3.98	1.08
Interception		3.94	.91
Pairwise t-Test			
Interruption	vs.	*t-Value*	*2-Tail Sig.*
	Fabrication	.24	.814
	Modification	.68	.503
	Interception	.72	.476

Table 9 Priority Tests for Distribution/Service Firms

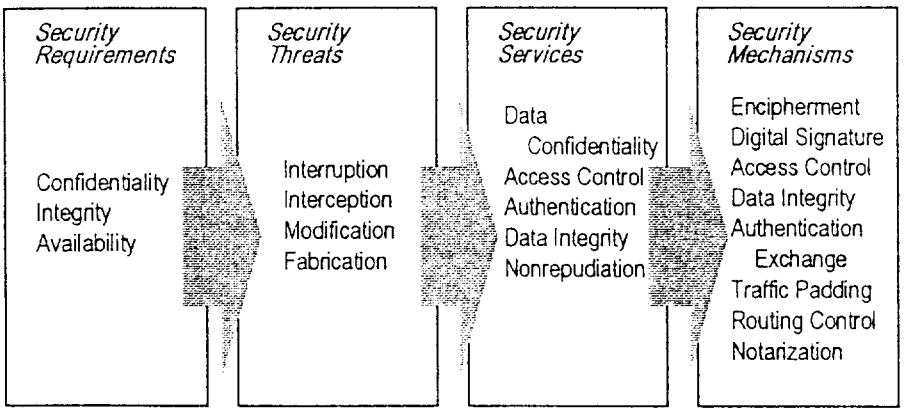

Figure 1 Research Model

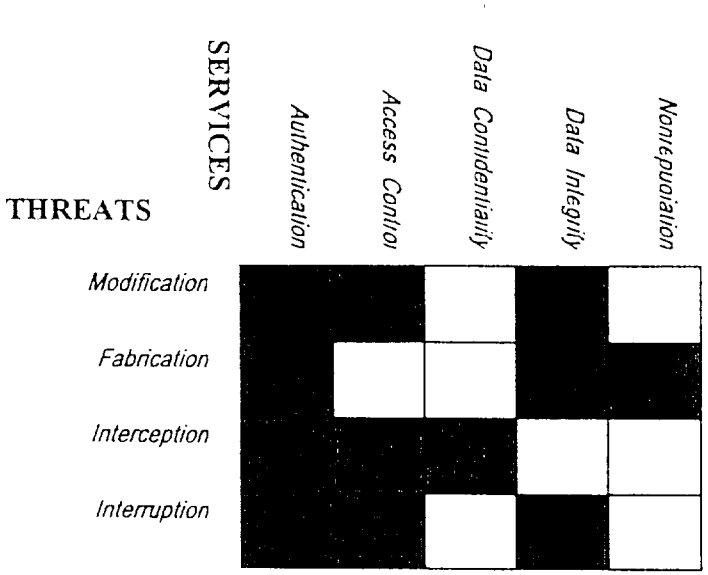

Figure 2 Mapping Threats to Security Services