A Curriculum Design for E-commerce Security

Hyunwoo Kim
Younggoo Han
Sehun Kim
Department of Industrial Engineering
KAIST, 373-1 Guseong-dong
Yuseong-gu, Daejeon, 305-701, Korea
hwkim@tmlab.kaist.ac.kr yghan@tmlab.kaist.ac.kr shkim@kaist.ac.kr

Myeonggil Choi
National Security Research Institute, 161 Gajeong-dong
Yuseong-gu, Daejeon, 305-350, Korea
mgchoi@etri.re.kr

ABSTRACT

The low cost and wide availability of the Internet have revolutionized electronic commerce (e-commerce) and its applications. Security, then, has become one of the most important issues that must be resolved first to ensure its success. To protect an e-commerce system from existing threats, there must be e-commerce security experts who can help ensure its reliable deployment. This paper presents a curriculum design for e-commerce security in which the Delphi method and the Analytic Hierarchy Process (AHP) method were used. The AHP method determines the priorities of the e-commerce security courses, and the results of the study provide useful guidelines in the design of the e-commerce security curriculum.

Keywords: Electronic commerce, security, curriculum development, e-commerce security expert, AHP method.

1. INTRODUCTION

The low cost and wide availability of the Internet have sparked a revolution in electronic commerce (e-commerce) and its applications. Many organizations have begun exploiting the opportunities offered by Internet-based e-commerce, and many more are expected to follow. Exemplary applications include online shopping, telebanking and Internet banking, teleteaching and distance education, online gambling, and virtual casinos, as well as Pay-TV and video-on-demand services (Oppliger, 1999). While this offers convenience for both consumers and vendors, many consumers are concerned about security and their private information when purchasing products or services over the Internet (Wang, Cao, and Kambayashi, 2002). Recently, there have been attacks on popular websites that resulted in the possible theft of credit card numbers of several thousand customers (He and Wang, 2001). Indeed, security is a major factor in e-commerce services.

Recently, courses in e-commerce have been offered in many schools and departments. These courses can be classified as technical and non-technical courses. Non-technical courses frequently focus on the changes in the business and in the industry due to e-commerce, the development of e-commerce, marketing practices, the processes in marketing research, etc. In technical courses, many academic units provide the contexts to understand the technology, and its applications such as web page design and associated programming languages, linking of databases to the website, customer data collection, catalog development, etc. (Jenkins, 2001).

However, courses in e-commerce security are not enough despite the priority on security to ensure the success of e-commerce. Many schools and academic departments on e-commerce have only one or two courses that deal with e-commerce security. When considering the importance of security in e-commerce, there is a further need to train e-commerce security experts who can help ensure its reliable deployment.

To produce e-commerce security experts, e-commerce security education should be treated more significantly, and sound curricula in e-commerce security are required. In this paper, we suggest a curriculum design for e-commerce security that would be useful in training e-commerce

security experts. An e-commerce security curriculum is designed in consideration of existing e-commerce threats and current information security curricula. To analyze the designed e-commerce security curriculum, the Delphi method and the Analytic Hierarchy Process (AHP) method are applied. The AHP method determines the relative importance of e-commerce security courses (Nam and Kim, 2003; Saaty, 1995). By using the AHP method, we can determine the priorities in e-commerce security courses. To produce e-commerce security experts, these priorities provide useful guidelines in the selection of e-commerce security courses.

The rest of the paper is organized as follows. Section 2 analyzes e-commerce threats and current e-commerce curricula. In Section 3, the e-commerce security curriculum is designed. Section 4 introduces the methodology. Section 5 shows the results of the Delphi and AHP methods. The conclusions are then discussed in Section 6.

2. RELATED WORKS

2.1 E-commerce Security

Without question, security is one of the most important issues that must be resolved to ensure the success of e-commerce. Researchers have studied how to protect e-commerce systems from threats. A number of papers have dealt with threats and related security issues in e-commerce applications (Oosthuizen, 1998; Wright, 2001).

Customer privacy is becoming the most common security issue in e-commerce (Udo, 2001). No customer wants to use a business that distributes sensitive customer data, such as credit card information, without his knowledge or permission. Encryption technologies are widely used to protect customers' privacy. Encryption algorithms and digital signatures support secure applications in E-mail and electronic payment schemes. Public key infrastructure (PKI) also plays an important role in secure e-commerce transactions (Gollmann, 2000).

Hacking and distribution of viruses are also serious threats to e-commerce. They mostly attack networks or e-commerce sites to render e-services unavailable. Businesses mainly use firewalls to protect their internal networks. Firewalls have now become the main points of defense in the business security architecture. Various complementary systems, such as Intrusion Detection System (IDS), Virtual Private Network (VPN), Information Retrieval System, etc., have also been applied (Marchany and Tront, 2002).

Even if the security technologies are applied well, non-technology factors, such as human errors, can make e-commerce system unstable. The individuals operating systems have become the most obvious vulnerable avenues of attack for internal and external threat (Arce, 2003). To minimize the damage caused by human errors, social engineering technology must be applied adequately.

To protect e-commerce systems from existing threats, all the security factors mentioned above should be considered. Additionally, e-commerce managers and engineers who have expert knowledge on security are required to manage these factors adequately. However, there are still very few researches on e-commerce education that focus on e-commerce security.

2.2 E-commerce Curriculum

Nowadays, e-commerce education is one of the most common courses in many educational institutions. Many colleges, graduate schools, and MBA programs include e-commerce education in their curricula. To investigate the current state of e-commerce education, we surveyed the curricula of e-commerce programs in 14 undergraduate schools, seven graduate schools, and five MBA courses. Those curricula differed in the number and depth of subjects, but there have been many structural similarities.

From a brief survey of those e-commerce curricula, e-commerce programs are classified into technical and non-technical courses. Technical courses are mainly related to the development and management of e-commerce systems. These courses focus on educational issues, like web and database technologies, telecommunication and networking, programming methods, and other technical concerns. Non-technical courses include the basic concepts of e-commerce, finance, accounting, marketing, public policy, leadership, and social engineering. Technical courses mainly focus on e-commerce system development, while non-technical courses are more related to the training of e-commerce managers.

The current e-commerce system requires an e-commerce professional to have a thorough knowledge of both technical and non-technical courses. In particular, the e-commerce professional must obtain an expert knowledge in e-commerce security. However, security-related courses have not been sufficiently organized to meet such demands. Among the examined 26 e-commerce programs, only 14 programs include related courses to e-commerce security in their curricula. In addition, those programs have, at most, one or two security courses, whose contents are inconsistently constructed. This shows that there are not enough courses that deal with e-commerce security, and e-commerce security guidelines or standards barely exist. Therefore, sound curricula must be required to ensure e-commerce security, based on well-organized guidelines to produce e-commerce security experts.

3. E-COMMERCE SECURITY CURRICULUM DESIGN

In this paper, we suggest an e-commerce security curriculum, which is designed to train e-commerce security experts. A number of factors have contributed to the design of a new curriculum in e-commerce security education. In the previous section, many threats to the success of e-commerce have been detected, and the current e-commerce curricula have been found insufficient in training e-commerce professionals. Therefore, the information

security curricula must be used to develop an e-commerce security curriculum. Materials that were related to e-commerce threats from information security curricula were chosen, and were utilized in the construction of e-commerce security education courses (Armstrong and Jayaratna, 2002; Kim and Surendran, 2002; Kim and Choi, 2002).

An e-commerce security curriculum should include fundamental security knowledge, security management, and system development. Encryption technologies and knowledge about hacking and viruses are classified as fundamental security knowledge because they are basic knowledge about e-commerce threats that are mentioned in section 2.1, and should be considered in the development of every e-commerce system. The contents about security management consist of e-commerce standards, laws, ethics, and security management and evaluation. These are partly related to human factors. The knowledge about system development concerned system technology, including web and database design, firewall, IDS, etc.

A total of 27 courses are developed conclusively for e-commerce security education. They are classified into three types: eight security managerial courses, five fundamental security courses, and 14 technology-based courses. The courses on e-commerce security education are as follows.

Security Managerial Courses
Introduction to E-commerce Security, Privacy and Ethics, Laws and Regulations, E-commerce Security Policy, E-commerce Standards, Security Projects for E-commerce, E-commerce Security Evaluation, and Risk Analysis Management

Fundamental Security Courses
Mathematical Cryptography, Encryption Technology, Public Key Infrastructure (PKI), Analysis of Hacking Techniques, and Handling Computer Viruses

Technology-Based Courses
Database Concept and Design, Database Management and Security, Website Design and Management, Web Server Implementation and Management, Web Programming Language, Server Authentication System, Firewall Technology, Network Security, Mobile Computing Security, Virtual Private Network, Information Retrieval System Design, Electronic Payment and Security, Intrusion Detection System, and Distributed Computing Security

The detailed explanation of these courses is provided in Appendix A. Although these courses consist of the essential components related to e-commerce security, it is difficult to cover all of them in e-commerce education because e-commerce education should also cover general subjects about e-commerce, including finance, marketing, etc. Therefore, it is recommended that more important courses for e-commerce security must be selected and taken with general e-commerce subjects. We evaluate the relative importance of e-commerce security courses to provide guidelines in creating an e-commerce curriculum that would be useful in producing e-commerce security experts.

4. METHODOLOGY

In this paper, we use a phase of the Delphi method and the Analytic Hierarchy Process (AHP) method to determine the relative importance of e-commerce security courses. The outcome from using the Delphi method is used as input for the hierarchical processing procedure in AHP. The AHP method is a flexible multiple-criteria decision-making (MCDM) technique (Saaty, 1995). It helps set priorities and make the best decision qualitatively and quantitatively. It serves as a framework in structuring complex decision-making problems and in providing judgments based on knowledge, experience, or feeling. The AHP method has been successfully applied in software and computer selection (Maiden and Ncube, 1998; Zviran, 1993), and some applications of AHP have been introduced in books (Golden, Wasil, and Harker, 1989; Saaty and Vargas, 2000).

The research process of this paper consists of three steps.

Step 1: Creating a full list of e-commerce security cou-rses and developing the hierarchical model of the list to apply AHP.
Step 2: Gathering relational data to compare alternatives by using the Delphi method.
Step 3: Estimating the priorities of e-commerce security courses.

The detailed research procedure performed in each step is as follows.

In step 1, we create a full list of 27 e-commerce security courses. (The full list was already mentioned in the previous section.) To apply AHP, the components of the list are further divided into a three-level hierarchy. Figure 1 shows the hierarchy of the e-commerce security courses.
In step 2, we use the Delphi method in gathering relational data to determine the order of importance of each of the e-commerce security courses. The outcome of the Delphi approach is used as input for the hierarchical processing procedure in AHP.

In this step, we prepare a questionnaire based on the hierarchy of e-commerce security courses. In the questionnaire, pairwise comparisons are made among all the factors at each level in the hierarchy. The pairwise comparison process elicits qualitative judgmental statements that indicate the strength of the decision maker's preference in a particular comparison. Saaty suggests the use of a 1-9 scale to quantify the strength of the decision maker's feelings between any two alternatives with respect to a given attribute (Saaty, 1995). An explanation of this scale is presented in Table 1.

In step 3, the relative weights of the e-commerce security courses are estimated, and the survey results are analyzed. To use the AHP, a judgment matrix should be obtained from the input data collected through the Delphi method.

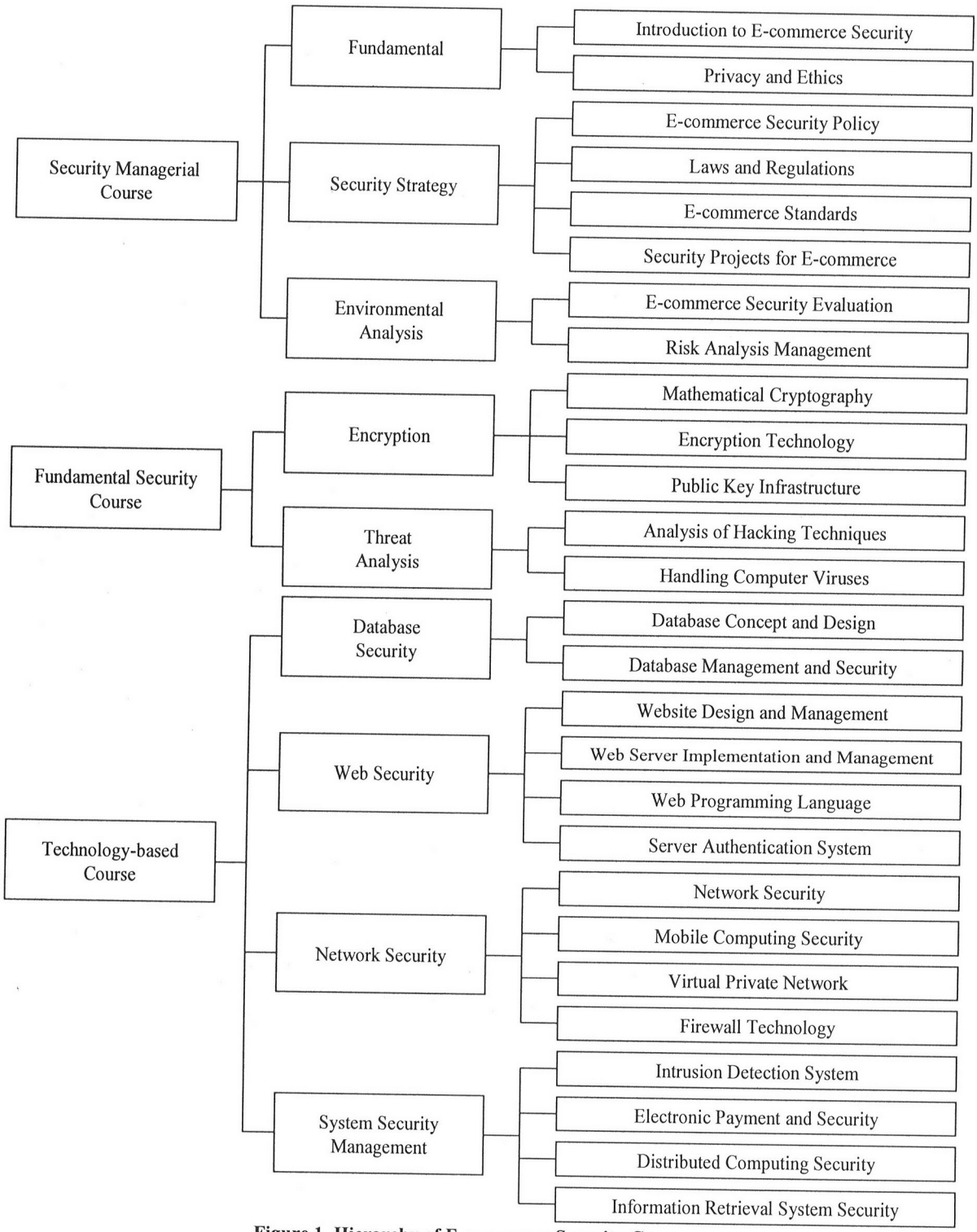


Figure 1. Hierarchy of E-commerce Security Courses

Intensity of importance	Definition	Explanation
1	Equal importance	Both factors contribute equally to the objective or criterion
3	Weak importance of one over another	Experience and judgment slightly favor one factor over another
5	Essential or strong importance	Experience and judgment strongly favor one factor over another
7	Very strong or demonstrated importance	A factor is favored very strongly over another, its dominance demonstrated in practice
9	Absolutely importance	The evidence favoring one factor over another is unquestionable

Table1. Scale used in Pairwise Comparisons

Saaty's eigenvalue method is the most preferred approach in this estimation (Saaty, 1995). In this section, no attempt is made to prove the mathematical founda-tions for AHP.

5. ANALYSIS OF THE E-COMMERCE SECURITY CURRICULUM

To determine the relative importance of e-commerce security courses, a questionnaire was sent to research groups, e-business managers, system engineers, etc. Participants were asked to check relative importance in pairwise comparisons, which are shown in Appendix A. The questionnaire was sent via E-mail to 500 professionals in universities, research institutes, e-businesses, and IT companies. A total of 67 professionals returned the questionnaires for a response rate of 13.4%, which is normal for a mail survey. Some participants might have refused to respond to the questionnaire due to unfamiliarity with the subject. The respondents' classification by job is shown in Table 2.

Position	Total Number	Percentage (%)
Faculty in University	6	9.0
Researcher in Security Institute	15	22.4
E-business Consultant	7	10.4
E-business Manager	15	22.4
E-commerce System Developer	12	17.9
Security Manager in IT Company	12	17.9
Total	67	100.0%

Table 2. Classification of Respondents by Job

By multiplying the weights of the first, second, and third levels in the hierarchy, the overall rankings of the e-commerce security courses could be determined. Table 4 shows the priority rankings of e-commerce security courses based on the results of Table 3.

The Intrusion Detection System course is considered the most important course among e-commerce security courses. Many technology-based courses show high priorities – 1st, 2nd, 5th, 7th, and 10th. The E-commerce Security Policy course is ranked 3rd, the highest rank among security managerial courses. The security policy influences security management infrastructure, training of employees, security documentations, etc., which are closely related to the human factors in a company. The fact that security policy is ranked relatively high means people think that the human factor is important in the success of e-commerce security. Among fundamental security courses, the Analysis of Hacking Techniques course is ranked highest. On the contrary, all encryption courses received low priorities compared to other e-commerce security courses. The Mathematical Crypto-graphy course is ranked lowest, and the Encryption Technology and PKI courses are ranked 24th and 18th, respectively. This shows that people view that theoretical studies on encryption technology are not significant in e-commerce security education.

The priorities of e-commerce security courses can be used to develop an e-commerce security curriculum in e-commerce education institutes. When designing a practical and efficient e-commerce curriculum in training e-commerce security experts, the priorities given in Table 4 provide useful guidelines in the selection of e-commerce security courses.

6. CONCLUSIONS

In e-commerce environments, security should be considered as an essential factor in their success. In this paper, a curriculum design on e-commerce security was provided to train e-commerce security experts. The 27 e-commerce security courses were constructed by considering existing e-commerce threats, current e-commerce courses, and information security curricula. The Delphi method and the AHP method were used to determine the relative importance and the overall rankings of the designed e-commerce security courses.

The current e-commerce system requires an e-commerce professional to have a thorough knowledge of security issues in e-commerce. However, it is difficult to cover all of them in e-commerce education because e-commerce education should also cover general subjects about e-commerce. Therefore, more important courses for e-commerce security should be selected. The research results can serve as useful guidelines in the development of secure e-commerce curricula.

To improve the validity of our achievements, the proposed work needs to be verified by further studies. There are very few researches on e-commerce security requirements. A further study on e-commerce security requirements may contribute to designing a more suitable curriculum in e-commerce security. Additionally, our work can provide

Course Classification		Courses	Weight
Security Managerial Course (0.281)	Fundamental (0.105)	Introduction to E-commerce Security	0.75
		Privacy and Ethics	0.25
	Security Strategy (0.637)	Laws and Regulations	0.275
		E-commerce Security Policy	0.475
		E-commerce Standards	0.158
		Security Projects for E-commerce	0.092
	Environment Analysis (0.258)	E-commerce Security Evaluation	0.25
		Risk Analysis Management	0.75
Fundamental Security Course (0.135)	Encryption (0.25)	Mathematical Cryptography	0.086
		Encryption Technology	0.297
		Public Key Infrastructure (PKI)	0.618
	Threat Analysis (0.75)	Handling Computer Viruses	0.25
		Analysis of Hacking Techniques	0.75
Technology-Based Course (0.584)	Database Security (0.086)	Database Concept and Design	0.167
		Database Management and Security	0.833
	Web Security (0.292)	Website Design and Management	0.185
		Web Server Implementation and Management	0.283
		Web Programming Language	0.211
		Server Authentication System	0.321
	Network Security (0.292)	Firewall Technology	0.305
		Network Security	0.528
		Mobile Computing Security	0.061
		Virtual Private Network	0.106
	System Security Management (0.331)	Information Retrieval System Design	0.275
		Electronic Payment and Security	0.158
		Intrusion Detection System	0.475
		Distributed Computing Security	0.092

Table 3. Weights of E-commerce Security Courses

Rank	Course
1	Intrusion Detection System
2	Network Security
3	E-commerce Security Policy
4	Analysis of Hacking Techniques
5	Server Authentication System
6	Risk Analysis Management
7	Information Retrieval System Design
8	Firewall Technology
9	Laws and Regulations
10	Web Server Implementation and Management
11	Database Management and Security
12	Web Programming Language
13	Website Design and Management
14	Electronic Payment and Security
15	E-commerce Standards
16	Handling Computer Viruses
17	Introduction to E-commerce Security
18	Public Key Infrastructure (PKI)
19	E-commerce Security Evaluation
20	Virtual Private Network
21	Distributed Computing Security
22	Security Projects for E-commerce
23	Mobile Computing Security
24	Encryption Technology
25	Database Concept and Design
26	Privacy and Ethics
27	Mathematical Cryptography

Table 4. Priority Rankings of E-commerce Security Courses

more reliable results if we apply our method to larger and more various respondents.

7. ACKNOWLEDGEMENTS

This work was sponsored in part by the Korean Ministry of Information and Communication under the University IT Research Center Project.

8. REFERENCES

Arce, I. (2003), "The Weakest Link Revisited." IEEE Security & Privacy Magazine, Vol. 1, Issue 2, March-April 2003, pp. 72-76.

Armstrong, H., N. Jayaratna (2002), "Internet Security Management: A Joint Postgraduate Curriculum Design." Journal of Information Systems Education, Vol. 13, No. 3, 2002, pp. 249-258.

Golden, L. B., E. A. Wasil, and P. T. Harker (1989), The Analytic Hierarchy Process: Applications and Studies. Springer-Verlag, Berlin.

Gollmann, D. (2000), "E-commerce Security." Computing & Control Engineering Journal, Special Feature on E-commerce, Vol. 11, No. 3, June 2000, pp. 115–118.

He, J. and M. Wang (2001), "Cryptography and Relational Database Management Systems." 2001 International Symposium on Database Engineering & Applications, July 16-18, pp. 273-284.

Jenkins, A. M. (2001), "Meeting the Need for E-commerce and E-business Education: Creating A Global Electronic Commerce Concentration in the Master of Business Administration (MBA) Program." 9th European Conference on Information Systems, June 27-29, pp. 1081-1086.

Kim, K., K. Surendran (2002), "Information Security Management Curriculum Design: A Joint Industry and Academic Effort." Journal of Information Systems Education, Vol. 13, No. 3, 2002, pp. 227-236.

Kim S., M. Choi (2002), "Educational Requirement Analysis for Information Security Professionals in Korea." Journal of Information Systems Education, Vol. 13, No. 3, 2002, pp. 237-246.

Maiden, N. A., C. Ncube (1998), "Acquiring COTS Software Selection Requirements." IEEE Software, Vol. 15, No. 2, March 1998, pp. 46-56.

Marchany, R. C., J. G. Tront (2002), "E-commerce Security Issues." Proceedings of the 35th Hawaii International Conference on System Science, January 7-10, pp. 2500-2508.

Nam, C., B. Kim (2003), "A Study on E-commerce Firms' Selecting Criteria for Small Package Express Service Provider by Using the Analytic Hierarchy Process." The Journal of Internet Electronic Commerce Research, Vol. 3, No. 1, February 2003.

Oosthuizen, G. (1998), "Security Issues Related to E-commerce." Network Security, No.5, 1998, pp.10-11.

Oppliger, R. (1999), "Shaping the Research Agenda for Security in E-commerce." Proceedings of the 10th International Workshop on Database & Expert Systems Applications, 1999, pp. 810-814.

Saaty, T. L. (1995), Decision-Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World. RWS Publications.

Saaty, T. L., and L. Vargas (2000), Models, Methods, Concepts, and Applications of the Analytic Hierarchy Process. Kluwer Academic Publishers, Boston.

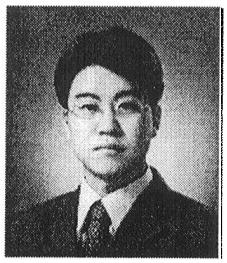
Udo, G. J. (2001), "Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study." Information Management & Computer Security, Vol.9, No.4, 2001, pp. 165-174.

Wang, H., J. Cao, and Y. Kambayashi (2002), "Building a Consumer Scalable Anonymity Payment Protocol for Internet Purchases." Proceedings of RIDE-2EC, February 24-25, pp. 159-168.

Wright, A. (2001), "Controlling Risks of E-commerce Content." Computers & Security, Vol.20, No.2, 2001, pp. 147-154.

Zviran, M. (1993), "A Comprehensive Methodology for Computer Family Selection." Journal of System Software, Vol. 22, No. 1, July 1993, pp. 17-26.

AUTHOR BIOGRAPHIES



Hyunwoo Kim received the B.S. degree in industrial management and M.S. degree in industrial engineering from Korea Advanced Institute of Science and Technology (KAIST) in 1999 and 2001, respectively, where he is pursuing the doctoral degree in industrial engineering. His research interests are in the areas of information system security evaluation, e-commerce security, and optimal design and analysis of intrusion detection systems in ad hoc networks.

Younggoo Han received the B.S. degree and M.S. degree in industrial engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, in 2002 and 2004, respectively, where he is pursuing the doctoral degree in industrial engineering. His research interests are topics in e-commerce security, secure communication in wide-band networks, and intrusion detection system.

Sehun Kim received the B.S. degree in physics from Seoul National University, Seoul, Korea, in 1972, and the M.S. and Ph.D degrees in operations research from Stanford University in 1978 and 1981, respectively. In 1982, he joined the faculty of the Korea Advanced Institute of Science and Technology (KAIST). He has published a number of papers in IEEE Trans. on Vehicular Technology, Computer Networks, Telecommunication Systems, IEICE Transactions on Communications, International Journal of Satellite Communications, and Journal of KIISC (Korea Institute of Information Security and Cryptology). He served as the chief editor of the Journal of KIISC from 1990 to 1993.

Myeonggil Choi is a senior engineer at National Security Research Institute, Electronics and Telecommuni-cations Research Institute (ETRI) in Korea. He received the M.S. degree from Pusan National University and Ph.D. degree in Management Information Systems from Korea Advanced Institute of Science and Technology (KAIST) in 2004. He worked at Agency for Defense Department (ADD) as researcher and has worked for National Security Research Institute, Electronics and Telecommunications Research Institute (ETRI) in Korea. His recent research issues include Network Security, Information System Security Evaluation, E-Commerce Security and Information Security Management.

Appendix A
Pairwise Comparison Form of the Top Levels in the Curriculum Hierarchy

Component	← Left side is more important				Equal	Right side is more important →				Component
	Absolute	Very Strong	Strong	Weak		Weak	Strong	Very Strong	Absolute	
Security Managerial Course										Security Fundamental Course
Security Managerial Course										Technology-Based Course
Security Fundamental Course										Technology-Based Course

Appendix B
Topics covered in the E-commerce Security Curriculum

Course Name	Course Focus
Introduction to E-commerce Security	General information on e-commerce security
Privacy and Ethics	Issues and examples of privacy and ethics in e-commerce
Laws and Regulations	E-commerce and security laws and regulations, laws on privacy, electronic payment, and criminology
E-commerce Security Policy	Strategy, documentation, adoption, analysis and management, and education of e-commerce security policies
E-commerce Standards	Standardization in e-commerce, security issues in e-commerce standards
Security Projects for E-commerce	Practical project in the e-commerce security design, building, and testing
E-commerce Security Evaluation	Evaluation method of e-commerce security, design, and management of the e-commerce security evaluation system
Risk Analysis Management	Risk assessment, risk analysis methods, and risk management
Mathematical Cryptography	History, concept, and mathematics of cryptography
Encryption Technology	Symmetric and asymmetric key distribution, protocols and key management, and digital signatures and certificates
Public Key Infrastructure (PKI)	Architecture of PKI, function of PKI components, authentication, and procedure in PKI
Handling Computer Viruses	Types and evolutions of worms and viruses, and protection and response methods
Analysis of Hacking Techniques	Types and examples of hacking, protection, and response and tracking methods
Database Concept and Design	Database theory, models, normalization, physical storage, record access paths, design, performance evaluation, and database integrity and inference
Database Management and Security	Security controls, transaction schedules and protocols, recovery techniques, and encryption in databases
Website Design and Management	Webmaster functions, Internet strategy, information architecture formulation, and security
Web Server Implementation and Management	Architecture, function of the client-server system, web server design, strategy, security, and application
Web Programming Language	XML programming, Java programming, HTML, SQL, TCL programming, and Oracle applications
Server Authentication System	Encryption methods, electronic keys, encryption protocols, and secure payments in client-server systems
Firewall Technology	Concept, architecture of a firewall, design and implementation, network and PC firewall, and applications
Network Security	TCP/IP, Net BIOS, RTS, network management protocols, network statistical analysis, debugging, routing, and managing network security
Mobile Computing Security	Wireless Internet theory, wireless communication security, security design, and applications in mobile computing environments
Virtual Private Network	Concept, architecture, components of VPN, VPN design, encryption of VPN, and implementation
Information Retrieval System Design	Data recovery, network reconstruction, website, and server retrieval
Electronic Payment and Security	Type of electronic payment systems (digital cash, e-check, smart card, etc.), and security of electronic payment tools
Intrusion Detection System	Host-based and network-based intrusion detection, anomaly and misuse detection, detection and response methodologies, tracking, and implementation of IDS
Distributed Computing Security	Design of distributed computing, distributed computing model, and the security design of distributed environments

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096