Journal of Convergence for Information Technology
Vol. 10. No. 5, pp. 16-22, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.05.016

Security Education Training Program Characteristics needed to Development Task of Security Software in Security Majors of 5 Universities of Seoul Region

Jin-Keun Hong
Professor, Division of Information Communication Technology, Baekseok University

서울지역 5개 대학 보안 전공들의 보안소프트웨어의 개발 직무에 필요한 보안 교육 훈련 프로그램 특성

홍진근
백석대학교 ICT학부 교수

Abstract In this paper, the technology and capabilities required for the job of developing security software recommended by the Cybersecurity Human Resources Development Framework of the National Initiative for Cybersecurity Education (NICE) were studied. In this paper, we describe what security skills are needed for the task of developing security software and what security capabilities should be held. The focus of this paper is to analyze the consistency between security technologies (core and specialized technologies) required for security software development tasks and the curriculum of information protection-related departments located in Seoul, Korea. The reason for this analysis is to see how the curriculum at five universities in Seoul is suitable for performing security software development tasks. In conclusion, if the five relevant departments studied are to intensively train developers of development tasks for security software, they are commonly required to train security testing and software debugging, how secure software is developed, risk management, privacy and information assurance.

Key Word : Cyber Security, Security Education, Security Workforce, Curriculum, Security Competency

요 약 본 논문에서는 NICE(National Initiative for Cybersecurity Education)의 사이버보안 인력양성 프레임워크에서 권고하는 보안 소프트웨어 개발 직무에 필요한 기술과 역량을 중심으로 연구하였다. 본 논문에서는 보안 소프트웨어의 개발 직무에 어떤 보안기술이 필요하고 어떤 보안 역량을 보유해야 하는지에 대해 살펴보았다. 본 논문의 초점은 보안 소프트웨어의 개발 직무에 필요한 보안기술(핵심기술과 특화기술)과 국내 서울에 위치한 정보보호 관련 학과의 교육과정 사이의 일치성을 분석하는데 있다. 이 분석을 하는 이유는 서울에 위치한 5개 대학의 정보보호 관련 학과에서 실시하는 교육과정이 보안 소프트웨어 개발 직무를 수행하는데 얼마나 적합한 교육체계를 갖추고 있는지를 살펴보기 위함이다. 결론적으로, 만일 연구된 5개의 관련 학과가 보안 소프트웨어의 개발 직무 개발자를 집중적으로 양성하고자 한다면, 공통적으로 보안 테스팅과 소프트웨어 디버깅, 시큐어 소프트웨어 개발 방법, 위험관리, 개인정보식별과 프라이버시, 정보보증에 대한 교육이 필요하다.

주제어 : 사이버보안, 보안교육, 보안 인력, 교육과정, 보안 역량

*This paper is supported by the funding of research program of Baekseok University

*Corresponding Author : Jin-Keun Hong(jkhong@bu.ac.kr)

Received March 25, 2019
Revised April 16, 2020
Accepted May 20, 2020
Published May 28, 2020

1. Introduction

Recently, the government emphasizes software development security. This background is that security weaknesses and vulnerabilities are increasing as the use of software programs increases. This phenomenon is caused by developer mistakes or logical errors. However, these mistakes or logical errors can be used for hacking or cause major security accidents.

In this paper, we became interested in the security technology and security capabilities of the developer required for the development of security software based on the discussion of the importance of software development security. Then security software developers need to discuss what technologies and capabilities they should have. Finding a more comprehensive, detailed, and well-organized security framework or security guide in this regard is not realistically easy.

Thus, in this paper, we sought to approach security software developers presented by NICE around the technology and capabilities of security required. This is because the NICE program is a guideline for National Institute of Standards and Technology (NIST)'s standard cybersecurity training curriculum being presented to foster cybersecurity workforce [1-7]. There are many security training programs going on in the country, but applying the standards of the NICE program to the development of education and training programs is still insufficient.

First, we would like to describe at the overall understanding of cybersecurityand prior research on education and training. Duan studied the design and development of cybersecurity curricula and experiments [8]. Akhtar Lodger and others studied innovative modular approaches for cybersecurity education [9] and presented that this module, proposed in an independent and loosely coupled, be applied as a target for cybersecurity training in all computer education [10]. Sayed Naqvi et al proposed a working-level digital forensics curriculum for next-generation training [11]. Shiva Azadgan et al studied the cyber-operating curriculum of the undergraduate course, which meets the stringent requirements of the National Security Agency (NSA) cyber-operating program [12]. Kim and others studied the analysis in a cybersecurity ecosystem using the NICE framework. The paper emphasized the lack of a comprehensive view of each domain of cybersecurity [13].

Miloslavskaya and others conducted studied tailored to the mapping of information security manual roles and the cybersecuritycapabilities framework [14]. Conklin et al. focused on the results of the NICE study [15]. In Alsmadi's paper, the NICE framework is analyzed around cybersecurity programs in Arab and Saudi Arabia countries, and recommendations are proposed [16]. Caulkins Bruce D. and others are focused on the National Cybersecurity Workforce Framework, the Department of Homeland Security, and the National Initiative for Cybersecurity Care and Studies Education Framework [17].

The prior studies so far have adequately studied realistic needs, along with the individual importance of cybersecurity education and training programs. However, research on whether the standard guidelines of education and training programs are properly applied at university sites is found to be insufficient in terms of fostering the development workforce of security software among tasks of cybersecurity. Therefore, in this paper, attention was paid to whether the measures presented in the standard guidelines are adequately presented and operated in the education and training programs at university sites.

This paper describes on the appropriateness of education training in cybersecurity from the

framework criteria of human resources cultivation in NICE cybersecurity area.

The paper determined that it was necessary to examine whether the education and training programs of security personnel operated by majors from five universities located in Seoul (one representative university located in Seoul, two cyber universities, and two women's universities) were appropriate based on the job skills and capabilities provided by the standards of the NICE framework. In this paper, among the criteria presented by NICE, we studied what technologies are required for the job of developing security software and what capabilities are required. From this, we studied the relevance of skills and skills to the security education and training courses currently run by universities and the tasks presented by NICE.

However, the current study lacked discussion about whether the capabilities required for the development of secure software were adequately developed in the university's security major's education program. However, university sites require objective judgement as to what criteria they were created by and whether the technology directly overrides this security software development task when they open a cybersecurity curriculum. It is also necessary to review from this standard whether the curriculum is properly organized and operated.

Therefore, this paper first identified the security capabilities and technologies required by the development tasks of security software presented by NICE. And we judged that the criteria that NICE presents could be objective criteria that can be applied to security practice sites. This is because they do not find other criteria that are better than the criteria that NICE presents. Thus, in this paper, the skills and capabilities of security required for the job of developing security software among classification of NICE security tasks were analyzed. From this point on, the appropriateness of education and training programs for related tasks conducted by university majors was studied.

The composition of this paper is as follows. First, Chapter 2 describes the security task classifications that NICE presents. Among these categories, the technology required for the task of developing security software was first described as a need technology and the skills required for the task. In addition, IT technology and security technology were divided into required competences. Chapter 3 analyzed security training courses (security technology areas) of universities located in Seoul. Security technologies and capabilities required by security software development task were compared to education and training programs run by universities. And we come to a conclusion in Chapter 4.

2. Technology Characteristics of Task in Security Software Development

2.1 Need Technology for task of security software development

The task of developing security software can be presented with information assurance engineers, information assurance software developers, information assurance software engineers, secure security software engineers and security engineers. The preferred technologies for security are information assurance, legal code ethics, personal safety and security, information system and network security, vulnerability assessment, computer network defense, security principle, cryptography, criminal law, computer forensics, public safety and security, and information system security certification, communication

security management technology. As shown in Table 1, the capabilities required for the design of secure software require such capabilities as vulnerability assessment, information assurance, cryptography, and risk management.

Table 1. Security Competence for task of security S/W development

Competence	Contents
Security technology	Cryptology, risk management, legal ethics, information system security, network security, vulnerability assessment, information assurance, security

2.2 Needs Technologies for Task of Security Software Development

The workforce developing secure software should have capabilities in such technologies as computing network and protocol technology, network security technology, security development methodology, risk management, legal policy ethics, cybersecurity principles, cybersecuritythreat technology, and vulnerability technologies. Security software developers should have an understanding of enterprise information security structures and information assurance, security evaluation and verification. In software development, an understanding of information assurance is needed. Understanding the principles of information assurance should be understood in confidentiality, integrity, availability, reliability and denial-of-service. Understanding of personal information identification, data security standards, and privacy impact assessment is necessary. Understanding of penetration testing principles and tool techniques is necessary and understanding of security environment settings, security threats and vulnerabilities, ID management technology, and protection requirements. When designing secure software, it also requires understanding and analysis of secure coding technologies, code analysis tools, black box security testing capabilities, secure test planning and design capabilities, software debugging, and safe software development methodology. Understanding of the requirements and procedures of supply chain security and risk management policies, in-depth defense applications and network security structures is necessary.

3. Security Education Program for Information Security majors

The security curriculum at Seoul-based 5 universities was compared and analyzed with the required technology based on the NICE workforce classification (Security Software Development Task). Security core technologies common to the security software development tasks presented by NICE are network security technologies, security development methods, risk management, legal policy ethics, cybersecurity principles, cybersecurity threats, and vulnerability technologies. Security software developers must have these security technologies. Table 2 compares the core common skills that security software developer should have and the subjects that university security-related majors are offering. For Korea University's Information Protection Convergence major, if you compare programs run by Korea University against the capacity required for the job of developing security software based on NICE, you can present them as shown in Table 2 (*). However, among the core technologies, additional subjects such as security development methods and law, policy and ethics are needed. For the "Big Data Information Protection" major at Cyber University in Seoul, additional courses such as security development methods, risk management and vulnerability subjects are needed among core technologies. For Sungshin Women's University's Convergence Information Technology (***), additional subjects such as security development methods and risk

management courses are required among key technologies. For the information protection engineering department at Sejong Cyber University (****), additional opening of subjects such as security development methods, risk management and vulnerability is necessary. Ewha Womans University's cybersecurity major (*****) requires additional opening of subjects such as security development methods and law policy ethics among core technologies. However, it is believed that education on cybersecuritythreats and vulnerabilities is being replaced by cybersecurity and practice, cybersecurity projects, internships, and cybersecurity field training.

Table 2. Core technologies for Security S/W Capabilitie

Core Technology	Opened subjects in related major of Universities				
	*	**	***	****	*****
Network security	NS	NS iS	NSP	iS Wns IotS	NS
SDM					
RM	RM				RM
Law Policy Ethics		SM&L	ISL&S P&E	IsL&cL	
cybersecurityPrinciple	IS	IS CS	IS	CS	CS CSp Cspd Csi Csft
cybersecurityThreat	HP	H&S	Hp	S&h Ct&r	
Vulnerability	MC		Mca		

※ Software Development Method(SDM), Risk management(RM)
*Korea University: Network Security(NS), Risk Management(RM), Information Security(IS), Hacking Practices(HP– basic/ advanced), Malicious Code(MC)
**Seoul Cyber University: Network Security(NS), Internet Security(iS), Security management & Law(SM&L), Information Security(IS), Cyber Security(CS), Hacking & Security(H&S)
***Sungshin Womans University: Network Security Practices(NSP), Information Security Law & Standard(ISL&S), Privacy&Ethics(P&E), Information Security(IS), Hacking program(Hp), Malicious code analysis(Mca)
****Sejong Cyber University: internet Security(iS), Wireless network security(Wns), IoT security(IotS), Information security Law & cyber Law(IsL&cL), Cyber Security(CS), Security & hacking(S&h), Cyber terror & response(Ct&r)
*****Ewha Womans University: Network Security(NS), Risk Management(RM), Cyber Security(CS), cybersecurityproject(CSp), cybersecurityproject design(Cspd), cybersecurityintership(Csi), cybersecurityfield training(Csft)

The following Table 3 lists the special technologies that security software developers should have first. It also indicates whether the university's security majors are offering a subject related to the technology. If the following majors want to focus on fostering developers of secure software, complementary training on the following technologies is required on the basis of NICE criteria. For Korea University's Information Security Convergence major, supplementary education is required for technologies such as personal information identification and privacy, security management, security testing and software debugging, secure security development methods, and information assurance (enterprise information security structure, Confidentiality Integrity Availability(CIA)). For Big data Information Security majors (**) at Seoul Cyber University, supplementary education is needed on technologies such as intrusion detection, secure coding, security testing and software debugging, secure security development methods, supply chain security and risk management, DiD application security, and information assurance (assessment and verification of software). For the Convergence Information Engineering Department (***) of Sungshin Women's University, supplementary training is required for technologies such as personal information identification and privacy, intrusion detection, secure coding, security testing and software debugging, security software development methods, supply chain security and risk management, and information assurance. For Sejong Cyber University's Information Security Engineering Department (****), complementary training is required for technologies such as privacy, security management, secure coding, security testing and software debugging, security software development methods, supply chain security and risk management, and information assurance (including assessment and verification of software). In the case of Ewha Womans University's Cybersecurity major (*****),

complementary training is required on technologies such as personal information identification and privacy, security testing and software debugging, how to develop secure software, supply chain security and risk management, and information assurance (including evaluation and verification of software).

Table 3. Special technologies to develop Security S/W Competence

Special Technology		Opened subjects in related major of Universities				
		*	**	***	****	*****
PII & privacy impact evaluation, data security standard			Da&s			
Intrusion test&tool		Ia&r			Id	Ids
Sec management			Scs	ISMS		Bas
Secure coding, code analysis and tool		SS SC				Sc&p
Security testing S/W debugging						
Secure software development method						
Supply chain security and risk management		RM				
DiD application program and NW security architecture		NS Hp Ia&r		Ca&p		Sc
Application firewall			As			
Encryption and DS based on PKI		IS				
Information Assurance	Enterprise Information Sec. Arch.			CIS ISa	Is	Cpss
	Security E&V	ISSEM		PSECD PSEM		
	Software development					
	Conf Integrity Availability Reliability Nonrep					

※ Security(Sec), Architecture(Arch), Evaluation& Verification (E&V), Confidentiality(Conf), Nonrepudiation(Nonrep), Security management(Secure configuration management, security threat and vulnerability, ID management, protection requirement)
*Korea University: Intrusion accident & rePsponse(Ia&r), Network Security(NS), Hacking practices(Hp, advanced), Information Security System Evaluation Method(ISSEM), Software security(SS), Secure Coding(SC), Risk Management(RM), Information Security(IS)
**Seoul Cyber University: Data application & security(Da&s), Security control service(Scs), Application security(As)
***Sungshin Womans University: Convergency Industrial Security(CIS), Information Security architecture(ISa), Information Security Product Security Evaluation Criteria Design(PSECD), Information Security Product Security Evaluation Method(PSEM), Crypto application & practices(Ca&p), Information security management system practices(Business/Individual; ISMSp(B/I))
****Sejong Cyber University: Industrial security(Is), Intrusion detection(Id)
*****Ewha Womans University: Cyber Physical system security(CPss), Intrusion detection system(Ids), Bio authentication security(Bas), Secure coding & practices(Sc&p), Security control(Sc)

4. Conclusion

In this paper, the technology and capabilities required for the job of developing security software recommended by the Cybersecurity Human Resources Development Framework of the National Initiative for Cybersecurity Education (NICE) were studied. The focus of this paper is to analyze the consistency between security technologies (core and specialized technologies) required for security software development tasks and the curriculum of information protection-related departments located in Seoul, Korea. It is to analyze the relevance between the curriculum. In conclusion, if the majors discussed in this paper want to cultivate talent in developing competent security software, education on technologies such as information assurance, risk management and vulnerability assessment should be strengthened. In future research, we would like to analyze the educational curriculum and its characteristics of information security majors at domestic women's universities.

REFERENCES

[1] C. Curricula. (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. New York : IEEE Computer Society. https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf

[2] W. Park & S. Ahn. (2017). Enhancing Education Curriculum of cybersecurityBased on NICE. *KIPS Trans. on Comp. and Comm. Sys., 6(1),* 321-328. DOI : 10.3745/KTCCS.2017.6.7.321

[3] S. Hong. (2018). A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S. *Journal of the Korea Institute of Information Security and Cryptology, 28(1),*

249-267.
DOI : 10.13089/JKIISC.2018. 28.1.249

[4] Competency Model Clearinghouse. (n.d.). *Cybersecurity Competency Model* (Online). https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity

[5] https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx

[6] William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte. NICE Cybersecurity Workforce Framework. NIST SP 800-181.

[7] NICE Webinar Series. (n.d.). *How You can influence an updates to the NICE framework*(Oline). https://www.nist.gov/system/files/documents/2019/12/04/NICEFramework_Webinar_FINAL.pdf

[8] D. Yuan. (2017). Design and develop hands on cyber-security curriculum and laboratory. *Computing Conference 2017* (pp. 1176-1179). IEEE.
DOI : 10.1109/SAI.2017.8252239

[9] A. Lodgher, J. Yang & U. Bulut. (2018). An Innovative Modular Approach of Teaching cybersecurityacross Computing Curricula. *In 2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE.
DOI : 10.1109/FIE.2018.8659040

[10] S. Naqvi, P. Sommer & M. Josephs. (2019). A Research-Led Practice-Driven Digital Forensic Curriculum to Train Next Generation of Cyber Firefighters. *In 2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1204-1211). IEEE.
DOI: 10.1109/EDUCON.2019.8725129

[11] S. Azadegan & M. O'Leary. (2016) An undergraduate Cyber Operations curriculum in the making: A 10+ year report. *In 2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 251-254). IEEE.
DOI : 10.1109/ISI.2016.7745484

[13] K. Kim, J. Smith, T. A. Yang & D. J. Kim, (2018). An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the NICE Framework. *In 2018 National Cyber Summit (NCS)* (pp. 1-7). IEEE.

[14] N. Miloslavskaya & A. Tolstoy. (2016). State level views on professional competencies in the field of IoT and cloud information security. *In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 83-90). IEEE.

[15] Conklin Wm Arthur, Cline Raymond E, Roosa Tiffany. (2014). Re engineering cyberseucirty educationin the US : An analysis of the critical factors. *System Sciences (HICCS) 47th Hawaii International Conference 2014* (pp. 2006-2014). IEEE

[16] I. Alsmadi & M. Zarour. (2018). Cybersecurity programs in Saudi Arabia: Issues and Recommendations. *In 2018 1st International Conference on Computer Applications & Information Security* (ICCAIS) (pp. 1-5). IEEE.

[17] B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman & R. Leis. (2016). Cyber workforce development using a behavioral cybersecurity paradigm. *In 2016 International Conference on Cyber Conflict (CyCon US)* (pp. 1-6). IEEE.

홍 진 근(Jin-Keun Hong) [정회원]

- 1991년 경북대학교 전자공학과(공학사)
- 1994년 경북대학교 정보통신공학전공(공학석사)
- 2000년 경북대학교 정보통신공학전공(공학박사)
- 2004년 ~ 현재 백석대학교 ICT학부 교수

- 관심분야 : 융합 신기술 및 보안
- E-Mail jkhong@bu.ac.kr