JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 6 : 1137~1142 Jun. 2017

사이버보안 전문가 양성을 위한 연구

김슬기 · 박대우*

The Research for Cyber Security Experts

Seul-gi Kim · Dea-woo Park*

Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, Korea

요 약

사이버 해킹공격과 사이버테러는 국민 생활에 피해를 주고, 결국엔 국가 안보가 위협을 당하고 있다. 사이버 해킹 공격으로 원자력 냉각시스템 설계도면이 유출되었으며, 청와대 홈페이지의 해킹, KBS 방송국 해킹 등 사이버사고가 발생하였다. 정보통신기반보호법, 정보통신망이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법이 사이버공격의 책임을 지우고 있으나, 새로운 기술로 무장한 해커의 공격을 막기는 어렵다. 본 논문은 사이버안보를 위한 사이버보안 전문가 양성을 연구한다. 사이버보안 전문가를 위한 지식 데이터베이스를 구축한다. 웹 해킹, 시스템 해킹, 네트워크 해킹의 기술과 평가를 통해 사이버보안 전문가 자격증 제도를 도입한다. 사이버보안 전문가 자격증 운영과 취득방안에 관한 연구를 통해, 국가 사이버안보를 위한 사이버보안 전문가를 육성하는데 도움이 되고자한다.

ABSTRACT

Cyber hacking attacks and cyber terrorism are damaging to the lives of the people, and in the end, national security is threatened. Cyber-hacking attacks leaked nuclear power cooling system design drawings, cyber accidents such as hacking of Cheongwadae's homepage and hacking of KBS stations occurred. The Act on Information and Communication Infrastructure Protection, Promotion of Information and Communication Network Utilization and Information Protection, and the Personal Information Protection Act remove the responsibility for cyber attacks, but it is difficult to prevent attacks by hackers armed with new technologies. This paper studies the development of cyber security experts for cyber security. Build a Knowledge Data Base for cyber security professionals. Web hacking, System hacking, and Network hacking technologies and evaluation. Through researches on the operation and acquisition of cyber security expert certification, we hope to help nurture cyber security experts for national cyber security.

키워드 : 사이버보안, 사이버테러, 전문가, 자격증, 지식

Key word : Cybersecurity, Cyber terror, Expert, Certification, Knowledge

Received 19 December 2016, **Revised** 20 December 2016, **Accepted** 02 January 2017

* **Corresponding Author** Dea-woo Park(E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.6.1137 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/ by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

사이버 세상이 도래하였다. 세계에 연결된 인터넷 정보와 네트워크 인프라(Infrastructure)의 발달로 ICBM (IoT, Cloud, Bigdata, Mobile)은 국민, 산업, 국가 의 데이터에 대한 통합 서비스를 제공한다. 국내의 모르는 곳을 찾아갈 때 스마트폰으로 현재 위치를 파악하고, 목적지를 검색하고, 교통수단을 선택하고 예약하고 결제할 수 있다.

스마트폰 사용자의 자료는, 위치추적은 물론 활동 내역을 알 수 있는 증거 자료가 된다. 사이버 세계의 단점은 이러한 정보를 이용하여, 개인정보와 금융정보를 추적하여, 관련되어 있는 사회와 국가의 인프라에 대한 사이버공격과 사이버테러를 일으킬 수 있다는 점이다.

예를 들어 3월 4일 발생한 DDoS(Distributed Denial of Service) 공격, 7월 7일 발생한 DDoS 공격, 카드3사(KB국민카드, 롯데카드, NH농협카드)의 개인정보유출 사건, 피싱(Phishing), 파밍(Pharming), 스미싱(Smishing), 카드사기, 전자금융사기로 인해 소액결제 피해 발생 또는 개인의 금융정보를 탈취[1] 등의 사이버공격은 국민의 실생활에서 경제적 피해를 가져다주고 있다. 2013년 3월에 발생한 MBC, KBS, YTN 등 주요 방송국에 대한 해킹공격은 방송시스템 마비라는 심각한 결과를 초래하였다[2].

따라서 국가사이버안보와 사이버 보안을 위한 전문가가 필요하고, 전문가를 양성하고, 전문가를 측정하기 위한 전문기술과 소양을 갖춘 사이버보안전문가 양성에 관한 연구가 필요하다.

본 논문은 사이버안보를 위한 사이버보안 전문가 양성을 연구한다. 사이버보안 전문가 양성을 위한 Web hacking, System hacking, Network hacking 등에 대한 보안 Knowledge(지식)을 Data Base(DB)에 축적하고, 사이버보안 전문가를 위한 Knowledge DB를 구축한다. Web hacking, System hacking, Network hacking의 기술과 평가를 통해 사이버보안 전문가 자격증 제도를 도입한다. 본 논문은 사이버보안 전문가 자격증 운영과 취득방안을 연구하여, 국가의 사이버안보를 강화하는 방안을 제시하고자 한다.

Ⅱ. 사이버보안 전문가 Knowledge DB

2.1. Web hacking

웹(Web)은 문자뿐만이 아닌 영상, 음성 등이 혼합된 멀티미디어 정보를 통신망으로 세계 각지에 연결시켜 주는 서비스다.

웹 사이트의 취약점을 공격하는 기술적 위협으로, 웹 페이지를 통하여 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위를 뜻한다.

2013년 OWASP(The Open Web Application Security Project) Top 10[3]에서 뽑은 취약점으로는 인젝션(Injection), 인증 및 세션 관리 취약점, XSS(Cross Site Scripting), 취약점 직접 객체 참조, 보안 설정오류, 민감 데이터 노출, CSRF(Cross Site Request Forgery), 알려진 취약점이 있는 컴포넌트 사용 등 다양한 취약점이 선정되었다.

OWASP Top 10은 2004년 이후로 매 3년마다 웹 애플리케이션에서 가장 위험한 취약점 10가지를 선정하며, 각 취약점의 항목은 순위가 높을수록 위험성이 더 높은 것으로 알려져 있다[4].

Table. 1 4 Techniques of typical web hacking

Type	Content
SQL Injection	It occurs when untrusted data is sent to the interpreter as part of the command or query, and malicious data from the attacker can be fooled into the interpreter to access unexpected command execution or unauthorized data.
Zero Board	Some Zeroboard php programs have flaws that can run php files remotely, and you can run computer commands to manipulate the screen or manipulate the computer.
Cross Site Script	This occurs when an application sends data to a web browser with untrusted data without proper confirmation or restriction, allowing an attacker to execute a script within the victim's browser, thereby stealing the user's session, tampering with the website, Can be redirected.

표 1은 국가정보원의 3대 취약점으로 선정된 대표 취약점이다. 국가정보원 국가사이버안전센터(NCSC)에서 국내 각 기관에서 홈페이지 해킹에 많이 악용되었던 보안취약점을 선정하고 발표하였다.

2.2. System hacking

운영체제 기반의 해킹 유형은 일반적으로 공격하고자 하는 System(시스템)이 결정되면 먼저 운영체제 종류를 파악한 다음 그에 따른 취약점을 발견하고 다양한 공격방법을 시도한다.

시스템의 프로그램 취약점을 이용한 해킹으로 버퍼 오버 플로우(Buffer overflow), 포맷 스트링(Format string)과 같은 기법을 이용하여 취약한 시스템을 공격하여 해당 시스템에 접속하여 관리자 권한을 획득하는 행위를 뜻한다.

그림 1은 국가정보통신망 해킹 시도 건수로 정부부처, 지자체 등 국가정보통신망 이용기관을 대상으로 시도되었다. 이때 해킹시도 차단건수는 신・변종 공격을 탐지 후 정밀분석하여 공격자 IP를 차단한 건수를 의미한다. 해킹 시도 중 유형별로는 비인가 접근시도가 가장 많았으며, 정보유출, 시스템권한획득 순으로 다양한 해킹시도가 발생했다.

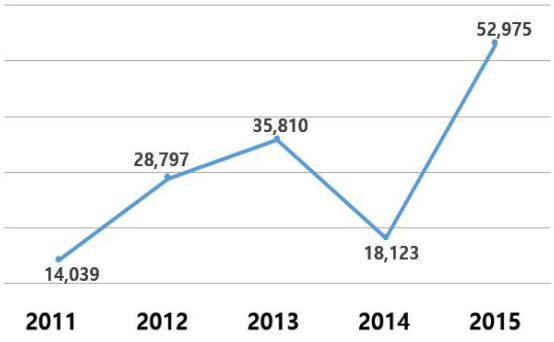

Fig. 1 Number of national information network hacking attempts (source : Ministry of the Interior)

시스템해킹에서 자주 사용되는 해킹방식은 비인가 접근시도가 가장 많다. 비인가 접근시도라는 것은 백도어(Back door)를 뜻한다. 백도어의 종류로는 로컬 백도어, 원격 백도어, 트로이 목마형, 등 다양한 종류가 있다.

표 2는 시스템 해킹에 사용된 대표적인 3가지 방법으로 시스템의 취약점을 공격할 때 쓰이는 방식이다.표 안에 설명된것처럼 이때 사용되는 백도어라는 것은 시스템 접근 시 사용자 인증 등 정상적인 절차를 거치지 않고 응용프로그램이나 시스템에 접근하도록 도와주는 도구이며, 공격자가 시스템에 최초 침입을 한 후, 자신이 원할 때 재침입하거나 권한을 쉽게 획득하기 위해 설치하는 통로라고 할 수 있다[2].

Table. 2 4 Techniques of typical system hacking

Type	Content
Back door	It is possible to access the application program or system without relying on normal procedures such as user authentication for accessing the system.
Buffer overflow	The C / C ++ compiler does not perform an array bounds check to write data larger than the declared size, and allows arbitrary data to be written and executed in the stack or heap area.
Password Cracking	In the case of short words or passwords in dictionary entries, a list of keyboard layouts, inferred words in user account information, or a case in which the length of passwords is not set, the passwords are divided into weak passwords.

2.3. Network hacking

Network(네트워크)는 정보기기 사이에서 전송매체를 이용하여 데이터 통신을 제공하며, 현재의 단말기와 시스템들은 대부분 네트워크에 연결되어 사이버 세계는 네트워크로 연결된 통신이 되고 있는 상황이다.

네트워크 보안은 개방형 네트워크 환경에서 전달되는 정보의 변조, 조작, 위조, 유출, 무단침입 등의 불법 행위로부터 정보를 보호하는 것을 의미한다[3].

그림 2는 2015년도 상반기 DDoS 월간 공격 동향이다. 총 123회가 발생되었으며, 1분기에만 70.70%가 발생되었고, 6월 말부터 다시 공격횟수가 상승하고 있다.

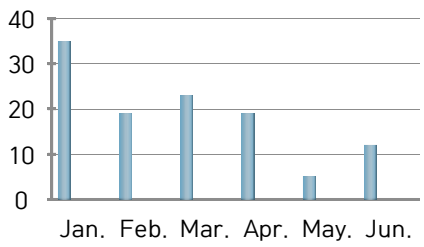

Fig. 2 Monthly Attack Trend of DDoS in the first half of 2015 (source : DDoS trend analysis report for the first half of 2015)

2.4. 전문가 자격증

개인정보보호법은 개인정보 처리단계별 규정을 두고 있으며, 개인정보보호 책임자를 임명해야 하나, 현실상황은 제대로 반영되지 않고 있다.

또한 2015년 하반기동안 38%가 북한의 지능형 사이버공격의 타깃이 되었다. 북한의 사이버공격 위협이 커지고 있는 시점에서, 조직력과 기술력을 갖춘 해커의 기습적인 사이버공격을 막기 위해 사이버보안 기술에 대한 DB 형성 및 사이버보안 전문가 인력 양성체계를 마련해야 한다.

개인정보유출과 사이버안보를 위협하는 해킹 공격은 일반인들이 접근하기 어려운 전문가 영역이기 때문에 사이버해킹을 직접 해본사람일수록 사이버보안에 대해서 파악하기도 쉽다. 공격방법을 잘 알면 보안대응 방법도 잘 알기 때문이다.

따라서 사이버보안전문가, 개인정보보호 책임자 자격증가 과정을 만들어 자격증을 발급해야 한다.

또한 개인정보보호책임자와 사이버보안전문가는 보안지식과 실습을 통해서 능력을 갖춰야한다[4]. 이때 교육기관에서는 주로 정보보호 개념과 이론위주의 교육이 진행되기 때문에 전문가 자격증 교육을 이수한사람도 실질적으로는 업무를 수행하는데 어려움이 있다[5].

사이버보안전문가, 개인정보보호책임자 자격증은 사이버안보를 위해서 필요하며, 개인정보보호책임자는 법률과 정보보호 시스템을 완전히 이해하고 실습할 수 있도록 PC와 스마트폰에서 학습 실습을 위한 Knowldge DB 구축 및 온라인 프로그램 개발에 대한 내용을 바탕으로 자격증학습[6]을 진행한다.

Ⅲ. 사이버보안 전문가 양성을 위한 평가

3.1. Web hacking 평가

웹의 구성요소 파악, 웹 공격기법 및 웹 관리에 대한 지식을 평가한다.

웹 해킹의 기본인 본인의 IP확인부터 웹 브라우저와 웹서버, 웹 애플리케이션, 데이터베이스 서버를 통해 인젝션, XSS, CSRF 등 웹 기반의 공격 기법해킹지식을 이해해야한다. 웹 해킹 지식평가로는 취약한 인증 및 세션관리, 불안전한 직접 객체 참조, 잘못된 보안설정, URL 접속제한 실패, 불충분한 전송 계층 보호, 확인되지 않은 리다이렉션 및 전달상태가 발생하지 않도록 웹 보안 평가를 진행할 것이다.

3.2. System hacking평가

시스템 구성, 시스템을 기반으로 하는 공격방식에 대한 지식을 평가한다.

시스템 해킹 지식평가로는 시스템 보안 패치, 방화벽 관리, IPS(Intrusion Prevention System) 관리, 계정관리, 패스워드 관리, 파일 및 폴더 관리, 보안 관련 정책, 로그 분석, 침입 추적에 관한 지식을 이해하고, 이러한 공격에 대응하기 위한 관리 및 보안설정방법을 학습하며 시스템 보안 평가를 진행할 것이다.

3.3. Network hacking 평가

네트워크의 구성 및 종류에 대한 개념, 네트워크 기반의 공격방식에 대한 지식을 평가한다.

네트워크 해킹 지식평가로는 방화벽, 침입탐지시스템, 가상사설망, 허니팟, 기타 보안 솔루션에 대한 지식을 이해하고 네트워크 기반의 공격기법인 Sniffing, Spoofing, DoS, DDoS 공격에 대응하고 안전한 네트워크 관리를 위한 보안기술을 학습하며 네트워크 보안 평가를 진행 할 것이다.

3.4. 사이버보안전문가 평가 측정

사이버보안전문가(2급,3급) 과정에서는 Web 해킹과 보안, 시스템 해킹과 보안, 네트워크 해킹과 보안 과정의 knowledge Data Base 구축과 특허 출원을 하며, 자격증 시험 평가 문제 1,000문제 이상을 개발한다.

개인정보보호책임자(2급, 3급) 과정에서는 수집처리유지파기, 보안관리 암호화, 법제도 처벌 과정의 knowledge Data Base 구축과 특허 출원을 하며, 자격증 시험 평가 문제 1,000문제 이상을 개발한다.

위 내용을 자격증 과정의 knowledge DB에 구축하고, 온라인 Contents로 만들어 개인정보와 사이버보안을 위한 전문가 양성한다.

3.5. Hacking 평가 방법 기준

Hacking 평가 방법으로는 사이버보안전문가와 개인정보보호책임자 두 항목으로 나뉜다.

사이버보안전문가에서는 평가항목을 3급, 2급으로 나눈 후 Web, System, Network 각 평가비중을 15%,

15%, 20%로 구성한다. 평가내용으로는 네트워크보안 등 보안에 관련된 해킹방식, 원리 문제로 평가한다.

개인정보보호책임자에서는 평가항목을 3급, 2급으로 나눈 후 수집/처리/유지/파기, 보안관리 암호화, 법제도 처벌, 각 평가비중을 15%, 20%, 15%로 구성한다. 평가내용으로는 정보주체의 동의와 정보주체 동의 없이 수집 등 법률의 특별한 규정으로 평가한다.

Ⅳ. 사이버보안 전문가 자격증 도입

4.1. 사이버보안전문가 자격증 도입

사이버보안전문가는 웹, 시스템, 네트워크 등 해킹과 보안 지식을 가지고 체계적으로 보안업무 수행할 수 있는 능력을 가진다. 자격기준으로는 관련학과의 대학졸업자 등 또는 그 졸업예정자로서 IT업계 및 유사 직무분야에서 4년 이상 실무에 종사한 사람 등 자격기준을 세운다.

정보보호책임자, 사이버보안전문가 민간자격증 취득 후 취업 알선 네트워크를 확보한다.

공공기관이나 기업들은 전문가 인력을 확보하게 되면 보안사고가 발생하였을 경우 침해사고에 대응 할 수 있다.

기존 자격증과 사이버보안 자격증을 비교했을 때, 기존자격증은 정보보안기사로 예로 든다. 정보보안기사는 국가기술자격증으로 분류된다.

사이버보안전문가와 개인정보보호책임자 자격증은 처음 도입되는 것으로 민간자격증으로 도입되어, 일정 요건을 갖추면 국가자격증으로 전환되어야 한다.

또한 기존자격증은 강의형식으로 교육이 진행되지만 사이버보안전문가는 인터넷으로 강의 및 실습할 수 있도록 PC와 스마트폰에서 학습 실습을 통해 더욱 활성화가 될 것이다.

커리큘럼은 2급을 기준으로 처음 시작단계에서는 운영체제에 대한 학습과 컴퓨터구조론 등을 학습한다. 온라인 학습과 실습을 통해 기준(60점) 이상이 통과 될 경우 중급단계를 학습하게 되는데, 중급에서는 정보보안 실무 및 네트워크공격기법, 정보보안 감사, 시스템해킹 실무 등을 학습한다. 약 6과목을 수강한 후 자격시험을 치러 자격증을 취득한다.

4.2. 사이버보안 자격증 교육현황

현재 사이버보안에 관련된 교육으로는 많은 기관에서 진행되고 있다. KISA, KG ITBANK, 코리아정보보안아카데미, KH정보교육원등 온라인과 오프라인 강의 등으로 수업을 진행하고 있다[7].

교육내용으로는 개인정보안정성 확보조치, 개인정보보호법 이해하기 등 수업을 수강 할 수 있도록 마련되어있다.

해킹, 사이버보안은 경험적이고 비공개적인 기술로 학술적인 선행연구가 부족하여 중요정보, 개인정보, 금융정보에 대한 악성코드의 제작과 배포, 방어 시스템의 교육준비가 어렵고, 실제 knowledge DB가 거의 없는 형편이다. 또한 정보보호, 사이버보안 교육 실습할 수 있는 사이트가 찾기 힘들어, 교육 및 실습할 수 있는 환경이 부족하다.

4.3. 사이버보안 자격증 취득 향후 방안

정부, 공공기관 등에서는 사이버보안 전문가, 정보보호책임자, 사이버전사, 해킹보안 전문요원, 해킹 포렌식 수사요원이 매우 부족한 상태라 많은 인력을 필요로 하고 있다.

사이버안보와 사회의 정보보호를 위해 사이버보안 전문가 및 사이버전사를 양성하고, 개인정보 관리를 위하여 매년 예산을 증액시키고 인력양성제도를 시행하고 있지만 해킹, 보안, 개인정보보호 실습교육이 거의 없기 때문에 인력양성이 필요하고 사이버보안전문가가 부족한 상황이다.

Ⅴ. 결 론

본 논문에서는 사이버보안 전문가 양성과 사이버보안 전문가 자격증을 도입하기 위한 연구를 하였다.

계속되는 사이버공격에 대한 해킹개념과 자격증에 관련된 지식 및 교육과정, 개인정보보호법을 지켜야 하는 사이버보안 전문가 양성을 제안하였다.

사이버보안전문가 평가 측정에서 다양한 해킹방식 이론에 대한 교육을 학습한 후 실습을 통해 교육이 이루어지면 자격증 과정을 개설하여, 자격증 학습-평가-인증 과정을 위한 전문가들의 Knowledge DB를 구축하고 인터넷과 스마트폰을 통한 교육과 실제 실습을 포한

한 평가를 제안한다.

향후 논문에서는 보안전문가 양성이 실제 공공기관과 기업에 사이버보안과 개인정보보호에 미치는 효과에 관한 연구가 필요하다.

REFERENCES

[1] D. W. Park, "Analysis of Mobile Smishing Hacking Trends and Security Measures," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 11, pp.2615-2622, Nov. 2015.

[2] S. O. Yun, "A Study on the Classification of Risks Caused by Big Data," *Journal of Korean Association for Regional Information Society*, vol. 16, no.2, pp.93-122, Jun. 2013.

[3] The Open Web Application Security Project. The Ten Most Critical Web Application Security Risks [Internet]. Available: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf.

[4] J. C. Moon, S. J. Cho, "Vulnerability Analysis and Threat Mitigation for Secure Web Application Development," *korean society of computer information*, vol. 17, no. 2, pp. 127-137, Feb. 2012.

[5] B. J. Kang, K. S. Han, E. G. Im, "Malicious code status and Detection technologies," *Korean Institute of Information Scientists and Engineers*, vol. 30, no. 1, pp. 44-53, Jan. 2012.

[6] B. H. Kim, D. W. Cho, "Network security technology trends and prospects," *Korean Institute of Communications and Information Sciences*, vol. 31, no. 4, pp. 99-106, Mar. 2014.

[7] S. G. Kim, D. W. Park, "The Research for Cyber Security Experts," *in Proceeding of Conference on Korea Institute of Information and Communication Engineering*, KOREA, vol. 20, no. 1, pp. 182, May 2016.

김슬기(Seul-gi Kim)

2016 2월 : 호서대학교 디지털디스플레이공학과 (학사)
2016년 ~ 현재 : 호서대학교 벤처대학원 융합공학과 (석사)
※관심분야 : 사이버보안, Forensic

박대우(Dea-woo Park)

1998년 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현 재 : 호서대학교 벤처대학원 교수
※관심분야 : Hacking, Forensic, CERT/CC, 침해사고 대응, e-Discoverty, 사이버안보, 네트워크 보안, 스마트폰 보안