Journal of Convergence for Information Technology
Vol. 9. No. 3, pp. 1-7, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.3.001

PC보안 강화를 위한 기술적 취약점 진단항목 개선 연구

조진근
고려대학교 소프트웨어보안학과 석사과정

Study on Improvement of Vulnerability Diagnosis Items for PC Security Enhancement

Jin-Keun Cho
The master's course, Division of Software Security, Korea University

요 약 업무용 PC에 다양한 사이버 공격이 발생하고 있다. PC 보안 위협을 줄이기 위해 사전에 취약점 진단을 통해서 예방하고 있다. 하지만 국내의 취약점 가이드는 진단 항목이 업데이트되지 않아서 이 가이드로만은 대응하기가 어렵다. 본 논문에서는 최근 PC의 사이버 침해사고 사례와 보안 위협에 대응하기 위한 국외의 기술적 취약점 진단 항목에 대해서 살펴본다. 또한, 국외와 국내의 기술적 취약점 진단항목의 차이를 비교하여 개선된 가이드를 제시한다. 제안한 41개의 기술적 취약점 개선 항목을 통하여 다양한 보안 위협으로부터 대응할 수 있다는 것을 알 수 있었다. 현재는 알려진 취약점에만 주로 대응이 가능하지만 이 방법의 가이드 적용을 통해 알려지지 않은 보안 위협을 감소시킬 수 있을 것으로 기대한다.

주제어 : PC보안, 기술적 취약점 가이드, 보안사고, 정보보호, 피싱 공격

Abstract There are various cyber attacks on business PCs. In order to reduce the threat of PC security, we are preventing the vulnerability from being diagnosed beforehand. However, this guideline is difficult to cope with because the domestic vulnerability guide does not update the diagnostic items. In this paper, we examine the cyber infringement cases of PCs and the diagnostic items of foreign technical vulnerabilities in order to cope with security threats. In addition, an improved guide is provided by comparing the differences in the diagnostic items of technical vulnerability from abroad and domestic. Through 41 proposed technical vulnerability improvement items, it was found that various security threats can be coped with. Currently, it is mainly able to respond to only known vulnerabilities, but we hope that applying this guideline will reduce unknown security threats.

Key Words : PC Security, Technology Vulnerability Guide, Security incident, Information Security, Fishing attack

1. 서론

정보통신 기술(ICT)이 발전하고 있는 만큼 사이버침해 사고도 매년 증가하고 있다. 이러한 사고는 개인정보 유출, 시스템 및 데이터 파괴, 서비스 중단 등 금전적인 이득을 취하거나 정치적 혼란을 야기한다. 사이버 범죄자는 각종 보안 장비의 탐지 기술을 회피할 수 있는 공격 수법을 개발하는데 암호화 기술을 악용하여 명령 및 제어 코드를 알아차리지 못하게 하여 탐지가 어려워진 만큼 피해 역시 증가 할 것으로 예측 된다[1].

*Corresponding Author : Jin-Keun Cho(gogg08@korea.ac.kr)
Received January 17, 2019
Revised February 20, 2019
Accepted March 20, 2019
Published March 28, 2019

한국인터넷진흥원에 따르면 공공 및 민간부문의 2017년도에 침해사고 신고접수는 287건이었으며 2018년도에는 500건으로 213건이 증가했다[2]. 침해사고를 경험한 사업체의 2016년도 유형을 보면 악성 코드에 의한 공격(75.5%), 랜섬웨어(25.5%), 애드웨어/스파이웨어 감염(13.0%)으로 악성 코드에 의한 감염이 가장 높게 나타났다.

국내에서는 정보통신기반 보호법을 기준으로 만들어진 주요정보통신기반시설 기술적 취약점 분석 및 평가 방법 상세가이드가 있어 이를 참고하여 점검한다[3]. 2017년 12월에 업데이트가 되었지만, PC 보안 항목은 업데이트되지 않았기 때문에 최신 취약점에 대한 정보가 없다. 이러한 문제는 백신 프로그램 과 운영체제 보안 업데이트에 의존할 수밖에 없다. 그러므로 백신 과 보안 업데이트가 되지 않거나 제로데이 공격에는 대응을 할 수가 없다는 문제가 있다.

본 논문에서는 제2장에서 사이버보안 위협 요소에 대해 살펴보고 제3장에서 위협 현황과 사고 사례를 살펴본다. 제4장에서는 국내와 국외의 기술적 취약점 점검 항목을 비교 분석을 한 후 개선된 항목을 제시한다. 제5장에서는 연구를 마무리 짓는다.

2. 관련 연구

2.1 선행 연구

한경희[4]는 금융권의 사이버 보안과 관련된 법적 대응 체계 및 PC 보안 위협에 대한 현황과 개선된 대응 방안을 제시한다. 주요 대응 방안으로는 보안 USB 사용, 문서보안, 개인정보 통제 솔루션 활용과 물리적인 디스크 미사용 시 데이터 영구삭제, 네트워크 보안 솔루션을 통해 인가되지 않은 접근을 차단하도록 한다. 개선방안으로는 자동점검시스템을 적용하여 업무 종료 시 바이러스 업데이트 및 정밀검사를 수행하여 악성 코드 감지 시 자동 치료, 운영체제 보안 업데이트, 문서암호화 정책을 수행하도록 한다. 이처럼 운영했을 때 기존보다 바이러스 점검 및 암호화 수행 확률 15% 향상된 결과를 얻는다고 말한다. 또한, 사전 예방을 위한 점검과 이벤트 기록, 보안 교육과 감사 제도를 통한 직원들의 보안 인식이 향상된다고 설명한다.

김상현[5]은 주요정보통신기반시설 기술적 취약점 점검 가이드를 통해 점검에 대한 의견을 100명을 대상으로 평가하였다.

공공기관 종사자 41%, 정보보안 회사 종사자 23%가 응답한 결과 현재 가이드로는 보안 수준을 정확히 파악이 안 되며 취약점 조치를 하여도 사이버 침해 대응에는 많은 부분 도움이 되지 않는다고 하였다. 해킹 메일이나 특정 OS 취약점, 프로그램의 취약점, 피싱·파밍과 같은 사회공학 기법에 대한 점검 항목이 없어 대응할 수 없기 때문이다. 그러므로 점검 방식에 관한 연구가 지속적으로 필요하다고 설명한다.

2.2 사이버보안 위협 분류

미국의 비영리 단체 중 하나인 Center for Internet Security(CIS)에서는 전 세계적으로 IT 전문 지식을 활용한 CIS Controls V7을 만들어서 사이버보안 위협과 완화하는 방안에 대해 설명한다. 크게 기본 보안 통제, 기초적인 보안 통제, 조직적인 보안통제로 3가지로 구분하고 총 20개의 항목을 정의 한다[6]. 첫 번째 기본 보안 통제 항목에서는 하드웨어/소프트웨어 자산관리, 지속적인 취약점 관리, 접근 권한 통제, 모바일, 노트북, 서버와 같은 전산장비의 하드웨어 및 소프트웨어 구성을 안전하게 보호, 감사 로그와 모니터링을 통한 분석을 요구한다. 두 번째로 기초적인 보안 통제에서는 이메일 및 웹 브라우저 보호, 악성 코드 방어, 네트워크 포트, 프로토콜, 서비스 통제, 데이터 백업 및 복구, 방화벽, 라우터, 스위치와 같은 네트워크 장비의 보안 구성, 인가된 네트워크 영역만 허용, 데이터 보호, 무선 네트워크 통제, 계정 관리 등을 요구한다. 마지막 세 번째로 조직적인 보안 통제 항목에서는 직원들의 보안 인식을 위한 교육 프로그램 구현, 소프트웨어 개발 시 필요로 하는 보안 요구 사항(secure cording, 동적 및 정적 분석을 통한 검증 등) 소프트웨어의 사고 대응 절차 및 보안 이슈, 위협 시나리오 관리, 침투 테스트 및 대응 훈련을 요구한다.

2.3 악성코드

악성 코드는 맬웨어(malware, malicious software), 악성 프로그램(malicious Program)이라고도 한다. 마이크로소프트에서는 악성 코드를 하나의 컴퓨터, 서버 또는 컴퓨터 네트워크에 피해를 주도록 설계된 모든 프로그램 이라고 통칭 한다. 악성 코드의 주요 감염경로는 웹 사이트, P2P 서비스 이용, 셰어웨어, 불법복제 프로그램을 사용, 내부자(해커)가 직접 설치, 이메일, 메신저의

첨부파일을 열 때 침투 한다[7,8].

Trojan Horse	Trojan Horse is a malicious code that can not self-replicate, causing malicious code to be injected into another program causing the user to run the program.
Worm	Worm is capable ofcopying itself, moving the computer and computer by itself, spreading it, and moving and spreading between programs and programs.
Spy-ware	Spy-ware is included in software programs that are mainly distributed free of charge. It is a program that is designed to send infromation to an attacker without any consent in an infected network or computer.
Bot	Bot is a program that allows an attacker to take controlof a user's computer. Bot Master can freely manipulate computers infected with Bot and retrieve information stored on Computer, soit can easily leak information and is used for attacking other systems.
Backdoor	Backdoor is a tool that allows a system or application to access the system without going through normal authentication procedures.
Ransomware	Ransomware is a kind of malicious software that infects Windows PC or server systems to restrict all access and requires some sort of expense to clear the infection.
Virus	irus infiltrates a computer system and infects a virus-infected file or a parasitic program by infecting itself or a perverted person and then infecting another.
Ad-ware	Ad-ware is a program that allows the user to fix an initial screen of a user's computer to a specific site or execute a code that can execute an unintended behavior and information of a user who displays an advertisement pop-up window.

Fig. 1. Malicious code classification Description

대표적인 악성 코드는 Fig. 1. 와 같이 Trojan Horse, Worm, Spy-ware, Bot, Backdoor, Ransomware, Virus, AD-ware 가 있다[9,10].

2.3 APT(Advanced Persistent Threats)

지능형 지속 공격은 공격 대상이 눈치를 채지 못하도록 은밀하게 침투하여 오랜 시간 동안 잠복하면서 정보를 천천히 살펴본 후 공격을 한다. 침투가 성공하면 사내 보안서비스를 무력화시키고 은밀하게 정보를 유출하는 것과 동시에 공격 흔적을 지우면서 정보를 탈취하기 때문에 정보가 유출여부를 바로 확인하기 어렵다. 침투 방법에는 웹을 통한 Watering-Hole과 Spear Phishing 등이 있다. 공격대상이 웹 페이지 접속이나 이메일을 통해 악성 파일을 다운로드 받아 실행하게 되는 데, 이 과정을 드랍퍼 단계라 한다. 악성 코드가 실행이 되면 C&C 서버와 통신이 이루어진다. 즉, 이때부터 악성 파일을 받은 PC를 제어할 수 있는 권한을 해커가 획득함으로써 정보유출이 가능해진다[11].

3. 위협 분석

3.1 사이버침해 사고 현황

한국인터넷진흥원 2018년 하반이 악성 코드 은닉사이트 탐지 동향 보고서에 따르면, Fig. 2. 와 같이 정보유출(기기정보)이 25.1% 비율로 가장 많이 탐지되었으며 랜섬웨어 20.1%, 정보유출(계정정보) 19.1%, 다운로더 13.1%, 가상통화 채굴 7.5% 순으로 다양하게 탐지가 되었다[12].

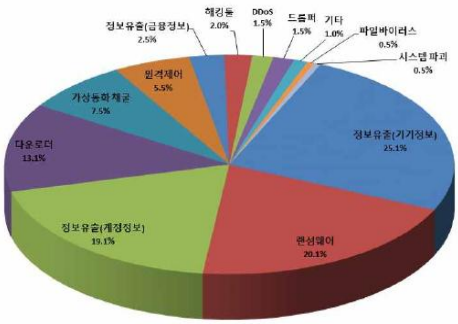

Fig. 2. Rate of types of malware

3.1.1 A사 금융정보 탈취

2018년 3월 구체적인 피해규모에 대해서는 밝혀지지 않았지만, 공격자는 거래처 발신자로 위장하여 악성 링크가 포함된 메일을 A사 직원에게 보냈다. 이 메일에는 악성 링크가 포함되어 있었고 업무 담당자가 이 악성 링크를 열람한 후 MS 워드파일을 다운로드 및 열람을 하였다. 이 문서를 열람 시 매크로 기능(콘텐츠 사용)을 사용하도록 유도 한다. 매크로 기능을 활성화하면 악성 코드가 실행이 된다. 코드가 실행되면 PC의 시스템 정보를 탈취한 후 두 번째 해킹 공격을 준비 한다. 악성 코드 유포지에 접속하여 추가로 파일을 다운로드 받게 하고 공유 폴더를 이용해서 네트워크의 다른 PC 20여 대에도 악성 코드에 감염시켰다. 추가로 다운로드 하는 모듈에는 네트워크 전파, 금융정보탈취모듈이 존재하였다.

최근에는 APT(Advanced Persistent Threats, 지능적 지속 위협) 공격 특징을 가진다. 특정 기업으로 대상이 확대되고 발신자 정보를 위조한 해킹 메일을 전송하는 방식으로 바뀌었기 때문이다. 이러한 공격은 이메일 보안솔루션, 스팸 메일 차단 솔루션을 통해서 악성 메일로 분류하기가 어려운 문제가 있다[13].

3.1.2 B사 개인정보 유출 사고

암호 화폐 거래소인 B사는 2017년 4월에 최초에 직원 PC가 감염되어 개인정보가 탈취되었다. 탈취된 개인정보는 이용자 정보 31,506건과 계정정보 4,981건 등 총 36,487건으로 밝혀져 과징금 4,350만 원, 과태료 1,500만 원 부과했다. 감염 경로는 공격자는 B사 직원 채용 기간

중 17년 4월 29일에 회사와 자문계약 관계에 있는 A 씨에게 원격제어 악성 코드가 포함된 이력서 파일을 첨부한 Spear Phishing 메일을 발송하였으며 이를 실행한 A 씨의 개인용 컴퓨터가 감염되었다. 감염에 성공한 공격자는 개인정보 파일을 포함한 다수의 파일을 획득하였으며 이 데이터를 가지고 사전대입공격을 하여 266개의 이용자의 계정이 탈취되어 이용자가 보유하고 있던 가상화폐가 탈취되었다[14].

4. 기술적 취약점 가이드 개선 방안

4.1 국내 현황

국내는 현재 한국인터넷진흥원에서 주요 정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드를 제공한다. 이는 국가·사회적으로 중요한 제어시설에 대한 해킹에 대해 보호하기 위해 국가에서 정보통신기반 보호법 제정하였고 이를 기반으로 만들어졌다[15]. 하지만 2014년에 나온 이후 2017년 12월에 개정되었지만, PC 보안 항목에 대해서는 업데이트가 되지 않아 최신 취약점에 대한 항목을 다루고 있지 않다. 현재는 기술적 취약점 중요도를 상 14개, 중 5개, 하 1개로 구분하여 총 20개 점검 항목으로 구성되어 있다[16].

4.2 미국 국방성 현황

미국 국방성(United States Department of Defense, DoD)에서는 국방정보시스템국(Defense Information Systems Agency, DISA)에서 제공하는 보안 기술 실행 지침인 STIG(Security Technical Implementation Guides)를 통해 보안체계를 강화하고 있다. PC 보안을 위해 Windows Client OS 별로 가이드를 만들어서 제공하고 있으며 본 논문에서는 Windows 10을 참고로 한다. Windows 10 가이드를 다루는 이유는 해당 버전부터 새로운 보안 기능을 제공하고 있으며 Windows 7 의 공식 지원 기간이 2020년 1월 14일에 끝나기 때문이다. 이 가이드에서는 중요도 상 26개, 중 232개, 하 22개로 총 280개로 구성되어 있으며 국내와는 다르게 분류 없이 상세 점검 항목으로만 구성되어 있다[17].

4.3 호주 현황

호주 정부는 사이버보안센터(Australian Cyber Security Center)를 설립하여 사이버보안을 주도 하고 있다. 호주도 미국 국방성과 마찬가지로 PC 보안을 위해 Windows Client OS 별로 가이드를 만들어서 제공한다. 동일하게 Windows 10 가이드를 참고하였으며 중요도 상 20개, 중 52개, 하 6개로 총 78개로 구성되어 있으며 세부항목은 총 300개를 가이드 하고 있어 국내와 미국 국방성과 비교하였을 때 가장 많은 항목을 가이드 하고 있다[18].

4.4 기술적 취약점 개선 항목 도출

국내, 미국 국방성, 호주에서 각각 가이드 하고 있는 항목을 분석하여 Fig. 3과 같이 분류하고 기존에 점검 항목 20개에서 개선 후 총 58개로 39개의 새로운 항목을 생성했다. 이 중에서는 기존 항목에서 불필요하여 제거하거나, 항목을 합쳐서 만들었기 때문에 실제로는 41개를 생성했다.

Category	Severity(AS-IS)			Severity(To Be)		
	High	Medium	Low	High	Medium	Low
Account Management	2	1		3	3	
Service Management	3	2	1	2	4	1
Patch Management	3			3		
Security Management	6	2		7	10	2
Application Management				3	3	
Credentials Management				2		
Rights Management				1	3	
Network Management					6	
Boot Management					4	
Audit Log Management					1	
Sub Total	14	5	1	21	34	3
Total	20			58		

Fig. 3. Summary of vulnerability improvements lists.

또한, Table. 1과 같이 기술적 취약점항목을 개선하였다.

Table 1. vulnerability improvements lists.

Title	Severity	Etc
Admin rights management	High	new
Multi-factor authentication	High	new
Password Management	High	
Eliminate unnecessary services	High	
Do not use commercial messenger(Windows Messenger, MSN, NET Messenger)	High	
Install the latest operating system security patch	High	
Install the latest service pack	High	
Install the latest security patches and vendor recommendations for applications	High	
Remove unused ActiveX	High	
Controlled Folder Access	High	new
Memory protection	High	new

Install antivirus programs and update periodically	High	
Enable real-time protection provided by antivirus programs	High	
Establish security measures against removable media such as CD, DVD, USB memory, etc.	High	
Setting the screen saver wait time and setting password protection on restart	High	
Enabling the OS-provided Intrusion Prevention	High	
Application hardening	High	new
Application white listing	High	new
Credentials setting for credentials	High	new
Manage credential items	High	new
Rights Management	High	new
Prevent automatic logon from the Recovery Console	Medium	
Account lockout	Medium	new
Disable guest Account	Medium	new
Set the file system to NTFS format	Medium	
Do not allow multibooting with other operating systems	Medium	
Disable Microsoft Account	Medium	new
Microsoft Windows system information communication settings	Medium	new
Prohibit Remote Assistance	Medium	
Use BIOS and UEFI password	Medium	new
Controlling the use of removable storage devices	Medium	new
Prevent file and print sharing	Medium	new
Local Disk Encryption	Medium	new
Power Shell Security Settings	Medium	new
Remote Desktop Services security settings	Medium	new
Windows Remote Management settings	Medium	new
Safe mode access prohibited	Medium	new
System encryption settings	Medium	new
Attack Surface Reduction	Medium	new
Microsoft Edge Security Settings	Medium	new
Installation Application Management	Medium	new
Set anonymous connection limits	Medium	new
Set backup and recovery permissions	Medium	new
Set user permissions	Medium	new
Bridging networks settings	Medium	new
Secure channel communication settings	Medium	new
Disable Wi-Fi Sense	Medium	new
SMB Security Settings	Midium	new
Session locking	Midium	new
Disable Bluetooth	Midium	new
Checking for misidentified drivers at boot time	Midium	new
Using Measured Boot	Midium	new
Using Secure Boot	Midium	new
Non-primary hard disk non-boot settings	Midium	new
Audit log settings	Midium	new
Delete the contents of the Temporary Internet Files folder at browser shutdown	Low	
Disable the Hide file extensions setting	Low	new
Hide file and folder security attributes	Low	new

5. 결론

5.1 결과

국외에서 PC 보안 가이드와 국내를 비교하여 41개의 개선된 점검항목을 제시했다. 개선된 가이드에서 PC 보안 위협에 대한 취약점에 대응하기 위한 중요사항 첫 번째는 PC의 관리자 권한을 가진 계정을 사용하지 않는 것이다. 사용자권한 계정으로 사용할 경우 글로벌 보안 회사인 Avecto는 2016년에 530건의 Microsoft 취약점 중에서 94%를 완화할 수 있다고 하였다.

두 번째는 2017년에 가장 많이 발생하였던 SMB 취약점을 통한 취약점 공격에 대응할 수 있다.

세 번째는 Application을 White List로 통제하면 최근 가장 많이 발생하는 전자메일이나 메신저, 인터넷 등을 통한 피싱 공격 대응에 효과적이다. 이러한 공격 행위의 공통점은 악성파일을 다운로드 후 실행 하였을 때 대부분 유저 영역에서 다운로드 되고나서 실행이 되기 때문에 다운로드는 가능하더라도 실제로 실행파일, 스크립트 등을 통해 감염을 시작하려고 했을 때 공격이 차단되기 때문에 사용자의 실수나 백신 프로그램이 탐지를 못하더라도 위협을 감소시킬 수 있다.

네 번째는 Windows 10의 메모리 보호 기능을 활용하여 Buffer Overflow와 같은 메모리의 취약점을 이용한 공격과 폴더 접근 통제를 통해 Ransomware 공격에 대응할 수 있다.

마지막으로 Windows에서 제공하는 다양한 보안 감사 설정을 통해 침해사고 발생 시 이벤트를 통해 조사 및

분석하는데 유용할 것이다. 이처럼 Windows PC의 보안 설정을 강화하게 되면 다양한 보안 위협으로부터 완화시킬 수 있다.

5.2 보완 사항

아직 알려지지 않은 공격방식에 대해서 대응할 수 있는지는 취약점이 공개 된 후에 검증할 수 있다. 향후 지속적인 사례 수집과 취약점 스캐너를 활용하여 이러한 보안 설정이 얼마나 효과가 있는지 연구가 계속 수행될 것이다. 또한, 공격이 다양해지는 만큼 취약점을 보완하기 위한 가이드의 지속적인 업데이트가 필요하다.

REFERENCES

[1] CISCO. (2018). *Annual Cyber Security Report in 2018.* USA : CISCO Publishing.

[2] Ministry of Science and ICT. (2019). *Number of hacking accident* http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1363

[3] Y. R. Jae & J. W. Cho. (2007). *A Study on the Evaluation Consulting Methodology of Important Information Communication Base Facility 5(1),* 55-68.

[4] K. H. Han. (2015). *A Study on Threat Analysis of PC Security and Countermeasures in Financial Sector*. master dissertation. Korea University, Korea,

[5] S. H. Kim. (2016). *The Critical Information and Communication Infrastructure Technical Field Vulnerability Assessment Improvements Research.* master dissertation. Konku University, Korea,

[6] CIS. (2019). *CIS Controls V7 in 2019. Center for Internet Security.* https://www.cisecurity.org/controls/

[7] B. B. Jeon. (2018). *A Study on the Countermeasures for Detecting Malicious Codes by Cyber Threats.* master dissertation. Kongju National University, Korea,

[8] L. D. Yu. (2015). Title. *Threats and countermeasures of malware 5(1),* 13-18.

[9] S. Y. Hong. (2014). Title. *Analysis and Countermeasure of Malicious Code, 4(2),* 13-18.

[10] S. H. Hong & J. A. Yu. (2018). Title. *Ransomware attack analysis and countermeasures of defensive aspects 8(1),* 139-145.

[11] M. S. Gu & Y. Z. Li. (2015). Title. *A Study of Countermeasur es for Advanced Per sistent Threats attacks by malicious code, 5(4),* 37-42.

[12] KISA. (2018). *Malicious code hidden site detection trend report Second half of 2018.* Seoul : Korea Internet & Security Agency Publishing.

[13] SK Infosec. (2018) *Evolution of information deception and malicious code emote in 2018.* http://blog.naver.com/PostView.nhn?blogId=skinfosec2000&logNo=221260804498&categoryNo=0&parentCategoryNo=0&viewDate=&currentPage=1&postListTopCurrentPage=1&from=postView

[14] KOREA COMMUNICATIONS COMMISSION. (2017). *Virtual currency trading site <BISSUM> Personal information leak in 2017.* https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=1&ctx=ALL&searchKey=ALL&searchVal=%EB%B9%97%EC%8D%B8&boardSeq=45265

[15] S. H. Kim (2016). *The Critical Information and Communication Infrastructure Technical Field Vulnerability Assessment Improvements Research.* master dissertation. Konkuk University, Korea.

[16] KISA. (2017). *Critical Information Infrastructure Protection technical vulnerabilities analyze and evaluate Detail Guide in 2017.* Seoul : Korea Internet & Security Agency Publishing.

[17] STIG. (2018). *Windows 10 Security Technical Implementation Guide in 2018. Security Technical Implementation Guide Viewer.* https://www.stigviewer.com/stig/windows_10/

[18] ACSC (2019). *Hardening Microsoft Windows 10 in 2019. Australian Cyber Security Center.* https://www.acsc.gov.au/publications/protect/hardening-win10.htm

조 진 근 (Cho, Jin Keun) [학생회원]

- 2016년 8월 : 세종사이버대학교 정보보안학과(공학사)
- 2017년 3월 ~ 현재 : 고려대학교 소프트웨어보안학과 석사과정
- 관심분야 : 정보보호 관리체계, 인프라 취약점 점검
- E-Mail : gogg08@korea.ac.kr