Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 12 pp. 8908-8914, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.12.8908
ISSN 1975-4701 / eISSN 2288-4688

악성코드 감염방지 및 사용자 부정행위 방지를 위한 통합 관리 시스템 구현

민소연[1*], 조은숙[2], 진병욱[3]
[1]서일대학교 정보통신과, [2]서일대학교 컴퓨터소프트웨어과, [3]숭실대학교 컴퓨터학과

A Implement of Integrated Management Systems for User Fraud Protection and Malware Infection Prevention

So-Yeon Min[1*], Eun-Sook Cho[2], Byung-Wook Jin[3]
[1]**Department of Information and Communication, Seoil University**
[2]**Department of Computer Software, Seoil University**
[3]**Department of Computer Science, Soongsil University**

요 약 인터넷이 지속적으로 성장과 발전을 거듭해가고 있는 이면에는 이를 악용하기 위한 다양한 인터넷 공격들이 발생하고 있다. 초기 인터넷 환경에서는 공격자가 역량과시 및 취미 등으로 인터넷 환경을 악용한 공격이 존재하였지만, 금전적인 이득을 목적으로 각종범죄와 연관된 체계적으로 복잡한 공격들이 발생하고 있다. 최근 들어서 바이러스나 웜과 같은 구조가 단순한 소스 멀티타깃(one source multi-target)의 형태가 존재하였지만, 멀티소스 싱글타깃(multi-source single target)의 형태를 갖는 APT(Advanced Persistent Threat, 지속적인 지능형 공격)으로 사용자들로 하여금 막대한 피해를 입히고 있다. 그러므로 본 논문에서는 Agent 및 관리 시스템은 악성코드 감염을 사전에 예방하는 기능을 고도화하여 사용자의 부정행위를 통한 자료유출을 감시할 수 방지 시스템을 설계 및 구현하였다. 성능평가에서는 감사데이터 생성 여부, 무결성 침해 발생 시 탐지 여부, 정상트래픽 오탐 여부, 프로세스 탐지 및 차단 기능 설정, Agent 정책 적용 가능여부에 대해서 기능을 분석하였다.

Abstract The Internet continues to grow and develop, but there are going to generate a variety of Internet attacks that exploit it. In the initial Internet environment, the attackers maliciously exploited Internet environments for ostentations and hobbies. but these days many malicious attempts purpose the financial gain so systematic and sophisticated attacks that are associated with various crimes are occurred. The structures, such as viruses and worms were present in the form of one source multi-target before. but recently, APT(Advanced Persistent Threat, intelligent continuous attacks) in the form of multi-source single target is dealing massive damage. The performance evaluation analyzed whether to generate audit data and detect integrity infringement, and false positives for normal traffic, process detecting and blocking functions, and Agent policy capabilities with respect to the application availability.

Keywords : Integrated Management, Malware Infection Prevention, User Fraud Protection

1. 서론

최근 발생하는 인터넷 해킹 피해 사례들이 갈수록 증가하고 있으며, 기존 시스템을 해킹하던 단계에서 개인 단말기를 해킹하여 다양한 피해를 유발 시키고 있다[1~2]. 사용자 개인 PC의 중요 정보 유출이나, 농협 해킹

본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0236185)의 연구수행으로 인한 결과물임을 밝힙니다.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
Tel: +82-2-490-7583 email: symin@seoil.ac.kr
Received November 25, 2015 Revised December 3, 2015
Accepted December 4, 2015 Published December 31, 2015

(2011.4)처럼 사용자 단말기를 이용한 내부 중요 시스템 접근, 악성코드에 감염된 개인 사용자 PC를 이용한 분산 서비스거부(DDoS) 공격 등, 점점 진화하는 악성코드에 대한 피해는 개인적인 피해에 그치지 않고 기업적인 피해, 더 나아가 사회적인 피해로 확산 되고 있다[3].

최근 발생하는 악성코드는 평균 3분마다 기업에 대한 공격이 발생되며, 산업별 특성에 따라 악성코드 비율은 상이하다. 기술 기업의 경우 1분당 한 번의 보안 위협을 경험하고 있으며, 지적재산권이 많은 기술 기업에 공격 집중되고 있다[1,4~5][11]. 지적재산권이 많은 기술 기업은 공격에 가장 타깃화된 산업군으로, 악성코드와 같은 보안 위협에 집중적인 공격을 받는다.

그리고 사용자 부정행위에 의한 사례를 살펴보면 2014년 3월에 외부와 연동되는 KT 홈페이지를 정상적으로 로그인한 뒤, 홈페이지 조회란에 고유숫자 9개를 무작위 자동입력 시키는 방법으로, 약 1천2백만 명의 개인정보를 탈취한 사고가 내부직원에 의해 발생 되었다[1,6]. 이처럼 내부 직원 또는 시스템 접근이 허용된 사용자에 의한 부정행위를 통해, 정보가 유출 되는 사례가 지속적으로 증가 하고 있다[7].

그러므로 사용자의 네트워크 사용 및 프로세스 사용 현황을 수집하고 이를 Agent 통합 관리 시스템으로 전송하고 수집된 다양한 이벤트 정보를 기반으로, 내부사용자의 부정행위를 분석하고 방지하는 시스템 설계 및 구현 하고자 한다.

2. 제안된 시스템 설계 및 개발

제안된 시스템은 기존의 백신과 같은 악성코드에 대한 기존 대응의 한계점을 극복하고, 악성코드의 감염 유형 이상행위를 탐지, 분석 하는 새로운 방식을 통해, 악성코드 감염을 예방 하고, 이를 통해 사용자 단말기의 악성코드에 대한 피해를 최소화하도록 개발한다.

2.1 Agent 통신 모듈 설계

이상 행위 유형 탐지기술은 일반적으로 DDoS 공격툴(악성코드)인 트로이목마, 백도어, 루트킷, 키로거, 웜, 바이러스 등의 악성 프로그램들이 일반적인 프로그램이 하지 않는 일련의 작업 및 행위를 탐지 하는 기술이다. 탐지 및 차단하는 일련의 행위는 API후킹, 신규파일 생성, 신규프로세스 생성, 서비스숨기기, 백도어 외부접속, 이름 없는 프로세스, 드라이버로딩, 타 프로그램 침범하여 실행, 실행 파일 변경, 실행중인 타 프로세스 중지, 레지스트리 경로 은닉, 타 프로세스 메모리 공간 침범 및 행위, OS 주요함수 테이블 침범 등 다양한 유형을 통해 감염된다. 본 시스템에서는 Agent 통신 소켓 모듈인 TCP/255를 활용하여 설계하며, [Fig. 1]과 같은 프로토콜을 활용하여 정책을 반영한다.

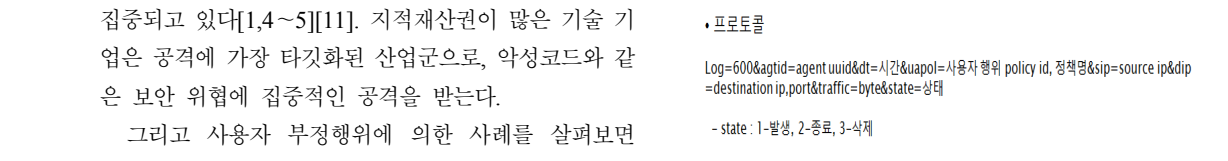


Fig. 1. Protocol structure to reflect the policy

시스템의 관리서버의 데이터베이스 테이블 구조를 설계하였으며, Agent와 관리서버의 암호화 통신을 적용하기 위해서 비밀성은 AES-CBC(256bit), 무결성은 SHA-256(256bit), 키교환은 RSA(2048bits)로 수행하며, OpenSSL 1.0.1e-fips을 활용하여 시스템을 설계한다[8].

Agent의 개발 내용은 관리서버와의 통신모듈을 수정하고, Agent 환경설정에 대한 기록을 암호화, IP목록에서 수신 정책 블랙 및 목적지 차단 기능 수정, 이벤트 로그 수집 주기 및 성능을 개선한다. 관리서버에서는 로그 수신 성능, 데이터베이스 쿼리 속도를 개선 후 보고서 생성 기능을 추가한다. Agent 전송 환경설정 페이지 및 배포 설치 유도 데몬을 설계하여 Agent 배포 IP 검출 기능을 개발한다[12].

2.2 사용자 부정행위 방지 모듈 설계 및 개발

Agent 설치 및 로그 수집과 관리 서버에서 탐지 정책을 수립하여 사용자의 부정행위를 방지하고자 한다. 우선 Agent별로 네트워크를 수집 후 NIC 정보를 추가적으로 수집하여 전송한다. 세부적인 내용을 살펴보면 5초마다 Agent를 수집 후 30초에 한 번씩 관리서버로 로그를 전송한다. NIC에서는 목록별로 테이블로 별도 기록하고 고유한 값을 식별하기 위해 전역고유 식별자를 전송한다. 정책설정화면은 Fig. 2와 같으며, 보고서는 Fig. 3과 같이 출력된다.

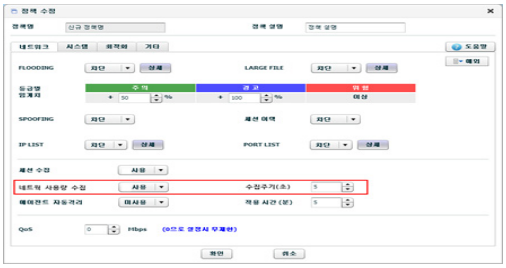


Fig. 2. Policy setting screen for detecting fraud user

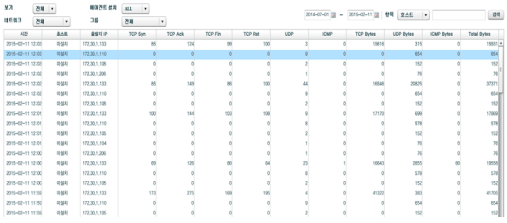


Fig. 3. Detection of connection information using the filter settings

2.3 프로세스 관리 모듈 설계 및 개발

사용자의 단말기의 프로그램을 관리에 필요한 하기 위해서 프로세스 관리 모듈을 설계한다. 화이트 프로세스 목록설정을 설계한다. 설계내용에서는 실행 경로 및 프로그램 경로 정보를 포함한다. 관리시스템 화면 구성 위치를 추가하여 정책, 시스템 보호, 프로세스 보호를 추가한다. 프로세스 Flow는 Fig. 4와 같다.

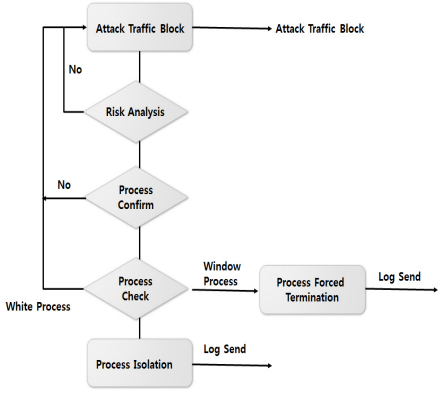


Fig. 4. Flowchart based on process management module design

관리시스템 프로세스의 입력 값의 유효범위를 지정하고 입력 값에 결과 메시지가 출력된다. tasklist를 통하여 실행 프로세스 목록을 생성하여 PID정보를 수집한다. 실행된 프로세스 목록 및 결과에 대해 관리시스템으로 로그를 전송하는데 [Fig. 5]와 같다. 관리자 설정에서 등록한 유해프로세스의 경우 실행 후 탐지 및 차단이 되어야 하나, 차단에 이르는 시간이 다소 소요된다.

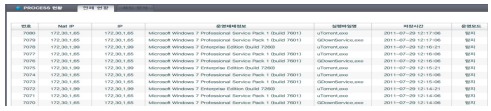


Fig. 5. Management report for current status

2.4 DLL 인젝션 탐지 모듈 설계 및 개발

윈도우 시스템 환경에서 DLL 인젝션 탐지 모듈을 설계하기 위해서 Hooking을 사전 차단한다. 관리서버 환경에서는 정책설정-시스템보호- DLL 인젝션 방어 추가하며, Policy_tbl - protopt 필드 사용하여 데이터베이스를 설정한다. DLL 인젝션 함수를 구하기 위해서는 CreateRemoteThread()함수를 이용하여 Loadlibrary()함수를 호출하여 인젝션 시키는 방법 설계한다. NewLdrLoadDll() 함수 작성 및 시작주소얻기-Detoured Function을 사용하며 수행과정은 Fig. 6과 같다.

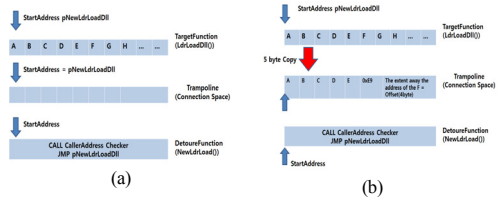


Fig. 6. DLL injection detection module design
(a) DLL injection function setup before
(b) DLL injection function setup after

NewLdrLoadDll()함수, virtaulAlloc() 함수, LdrLoadDll() 함수를 사용하여 인젝션 공격 방어 소스를 설계한다. Fig. 7과 같이 API_Hooking()함수를 작성한다. 쓰레드의 시작 주소 얻는 방법 설계 후 Anti_dll Injection()함수 호출을 하여 인젝션 탐지 모듈에 대한 설계를 끝낸다.

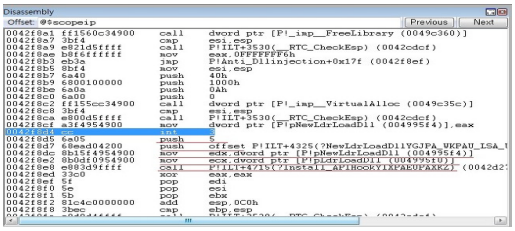


Fig. 7. Value following the JMP instruction in hooking operation is specified in the offset

3. 성능평가

본 장에서는 악성코드 감염방지 Agent 및 사용자 부정행위 방지 시스템을 설계된 시스템에 관하여 성능을 평가한다. 제안된 시스템의 권고사양은 CPU Intel Pentium4 3Ghz 이상, Memory는 1Gb이상, HDD 120GB이상, NIC 10/100/1000 Base-T 이상을 요구하며 운영체제는 CentOS-6.0(64bit), DBMS MySQL 5.1을 사용한다. Agent는 CPU Intel Pentium4 2Ghz 이상, Memory 512MB 이상, 10GB 이상 여유공간, 10/100Mbps * 1의 Nic을 요구하며 윈도우 XP이상 환경에서 구동된다. 네트워크의 구성도는 [Fig. 8]과 같으며 요구사항은 Table 1과 같다[9-10].

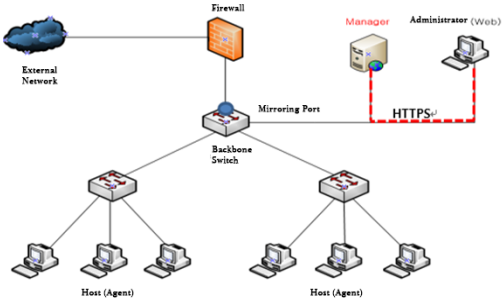


Fig. 8. Network configuration diagram of the proposed system

Table 1. Proposed system of requirement

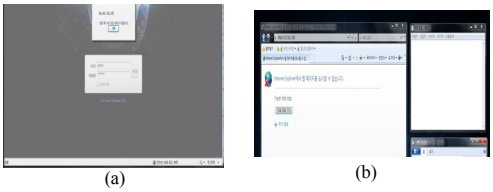
	Requirement
OE.Physical Security	Agent, manager, and log DB must be located in physically secure environments that only authorized administrators can access.
OE. Trusted Administrator	The administrator authorized by Pre-Guard must be not mali- cious, receive proper training on Pre-Guard management and perform the duties in accordance with the administrator instructions.
OE.TimeStamp	Per-Guard must be provided with reliable timestamp from OS server.
OE.Secure Channel	Pre-Guard must use encrypted communication channel to protect the information transferred between Pre-Guard components, and Pre-Guard and administrator from damage, and alteration
OE.Save LogDB	LogDB must protect and store securely the monitoring data generated from Pre-Guard
OE. MainTain Security	When internal network environments are changed, Authorized Pre-Guard must apply changed environments and security policies to Pre-Guard operational policy to maintain the same security level as before

감사대상 사건 발생 시 감사데이터 생성 여부 검증에 대한 기능을 평가하고자 한다. 목적은 사건 발생 시 OE가 정상적으로 감사기록을 생성하는지 확인하며, 감사대상 사건을 임의로 발생시킨 후 감사기록 생성여부를 Manager에서 확인한다.

(a) (b)

Fig. 9. Verification as to whether or not to generate audit data
(a) Creating a log list and threshold exceeded log generation
(b) Generation and verification of audit log

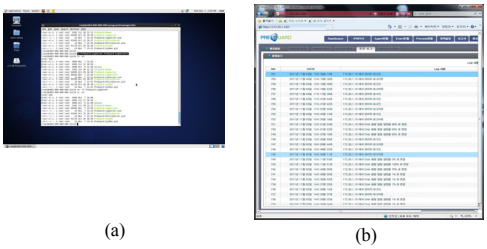
보안위반사건 발생 시 대응행동 점검을 수행하기 위해서 잠재적인 보안 위반을 임의로 발생 후 알림창이 여부에 대해서 기능성능 평가하였다. 시험 초기 선행조건에서는 TCP SYN Attack, IP Spoofing에 대해서 분석하였다.



(a) (b)

Fig. 10. Check the corresponding behavior at the time of security violations occur
(a) Pop-up settings when administrator 5 times authentication failure
(b) Host access control policy violation Alulim chan setting

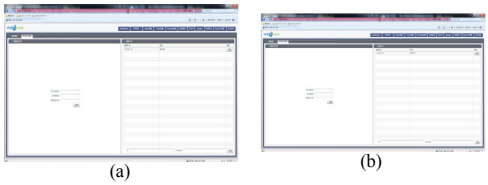
무결성 침해사건 발생 시 정상 탐지 여부를 점검하기 위해서 Manager에 로그인하여 kill, ps, cp 그리고 reboot 명령어를 사용하여 프로세스를 강제 종료 후 Manager의 대응행동을 확인하였다. 무결성을 임의로 변조하여 무결성 침해에 대한 로그를 확인하였다.



(a) (b)

Fig. 11. Whether to detect when integrity violations occur
(a) Consistency modulation
(b) Check the infringement modulation log of consistency

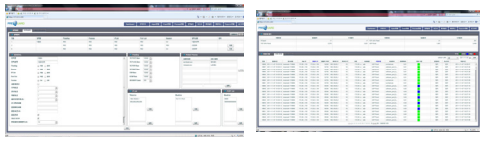
관리자 IP 등록 제안 개수를 검증하기 위해 관리자만이 접속할 수 있는 관리자 접속 IP의 등록제한 개수가 존재하는 지 확인하였다. 관리자 PC에서 IP를 지속적으로 추가하여 IP 여부를 확인하였다.



(a) (b)

Fig. 12. Verification of administrator IP list
(a) IP settings from the administrator PC
(b) Change and add the IP configuration

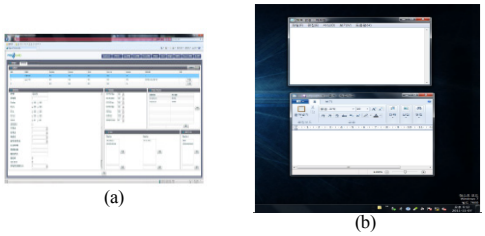
정상트래픽의 오탐 여부를 점검하기 위해서 Flooding 정책을 임계치까지 설정 후 정상트래픽을 발생하여 도달되지 않은 트래픽이 유해트래픽으로 탐지될 경우 오탐으로 판단하는 성능을 평가하였다.



(a) (b)

Fig. 13. Check whether the normal traffic Autumn
(a) Setting the threshold
(b) Setting of normal traffic harmful traffic detection

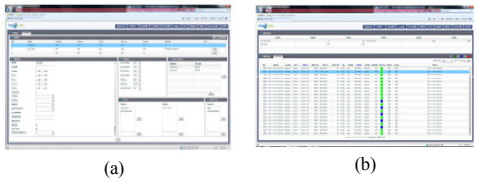
프로세스 탐지 및 차단기능 정상동작 여부 검증을 수행하기 위해 관리자가 설정한 유해프로세스가 호스트에서 실행되었을 경우 실시간으로 탐지 및 차단되는 지 확인하였다.



(a) (b)

Fig. 14. Detection and block function check of the process
(a) Policy settings
(b) Real-time block confirmation

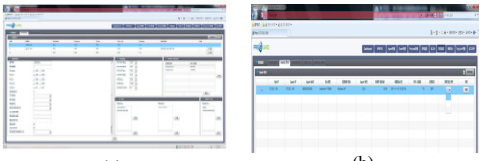
IP 및 Port 탐지 및 차단기능 정상동작 확인하기 위해서는 정책설정에서 Blacklist 등록 후 Agent가 설치된 호스트에서 해당 IP를 사용하여 외부와의 통신을 시도하여 비 인가된 IP 차단에 대해서 검증하였다.



(a) (b)

Fig. 15. IP and Port detect and block function
(a) Modify the Normal policy
(b) Block log generation

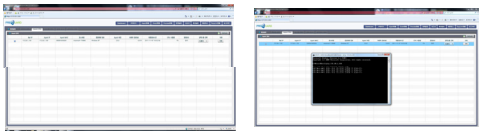
Agent 정책 적용 가능여부 검증을 확인하기 위해서 [정책설정]메뉴에서 정책수정 후 [환경설정] → [Agent 관리]에서 수정된 정책을 적용한다. 이후 정책수정 후 수정된 정책을 Agent에 정상적으로 적용할 수 있는지 확인한다.



(a) (b)

Fig. 16. Application verification of Agent policy
(a) Change of policy changes
(b) Apply the modified policy

Agent 삭제 후 자동등록 가능 여부 확인을 검증한다. 네트워크에 연결되지 않은 Agent를 관리자가 보안관리 화면에서 삭제 시 추후 Agent가 네트워크에 연결될 경우 자동으로 등록되는 지 확인함으로써, Agent를 삭제 후 재등록여부를 확인한다.



(a) (b)

Fig. 17. After the agent removed, and confirm whether you want to register
(a) Remove the Agent in the Preferences
(b) Check whether to remove Agent through the options of Delete prevention

4. 결론

본 논문에서는 악성코드 감염방지 Agent 및 사용자 부정행위 방지 시스템을 설계 및 구현하여 사용자 단말기에서 악성코드의 침투 행위 및 감염 형태를 분석 후 악성코드 탐지 및 차단과정을 확인할 수 있었다. 기존의 악성코드에 대한 사후대응 솔루션들의 한계점을 보완하고, 사용자 단말기의 악성코드 감염에 대한 사전대응 기능을 추가하였다.

또한, 악의적인 DLL 인젝션과 유해 프로세스에 대한 탐지 및 차단 기능 개발, 유해 프로세스의 시스템 파일 변조 탐지 및 차단하는 기능 개발, 그리고 Agent 관리 시스템기능을 개발하여 악성코드 침투 및 감염 형태를 분석할 수 있었다. 또한 제안된 시스템을 기초로 Agent와 통합관리 시스템 간 통신 프로토콜 및 로그 포맷 및 이벤트 저장 DB 구조 설계, 기능 설명, 시스템 구조 설계 등에 대하여 기술이 활성화 될 것으로 예상한다.

본 논문의 결과물은 향후 Agent와 통합관리 시스템 연동을 위한 통신 프로토콜 설계, 정책 파일 포맷 및 이벤트 저장 DB 설계, DLL 인젝션 방지 기능 정의 및 설계, 프로세스 관리 기능 정의 및 설계, 프로세스 디스크 쓰기 방지 기능정의 및 설계, 보고서 및 관리 기능 정의 및 화면 설계와 관련하여 각 기능 모듈별에 대한 상세부분부터, 전체 시스템 구성 등 세부적으로 개발되어 상용화를 할 계획이다.

References

[1] Saint Security, Malware analysis report, malwares.com, 2015. 7. 13

[2] Jae-Kyung Park, A Realtime Malware Detection Technique Using Multiple Filter, KSCI, Vol.19, No. 7. 2014. 7.

[3] Jaeho Lee, Sangjin Lee, A Study on Unknown Malware Detection using Digital Forensic Techniques, , JKIISC, Vol24, No. 1, 2014. 2.

[4] JesseBurns,“DevelopingSecureMobileApplications forAndroid:AnintroductiontomakingsecureAndroidapplications”,Dec2009.

[5] A.Shabtai,Y.FledelandU.Kanonov,Y.EloviiandS.Dolev. “GoogleAndroid:AState-of-the-ArtReview ofSecurityMechanisms.”IEEE SecurityandPrivacy,vol.8,issue2,pp.35-442010.

[6] James M. Aquilina, Eoghan Casey, Cameron H. Malin, MalwareForensics-InvestigatingandAnalyzingMaliciousCode”, 2008.

[7] Brett Stone-Gross, Ryan Abman, Richard A. Kemmerer, ChristopherKruegel,DouglasG.Steigerwald,andGiovanniVigna, “TheUndergroundEconomyofFakeAntivirusSoftware”, 2012.

[8] Sang Min Lee, Hwa Sun Kim, Hune Cho, “Study on OWL-based database built for the efficient operation of human resources bank,” *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.5, No.3, pp.55-64, June 2015. DOI: http://dx.doi.org/10.14257/AJMAHS.2015.06.27

[9] Sattarova Feruza, “Secure Multi-Party Computation in Networks Over A Cross Domain Privacy Preserving Firewall Optimization,” *Asia-pacific Journal of Multimedia*

Services Convergent with Art, Humanities, and Sociology, Vol.1, No.1, pp.91-98, Dec. 2011.
DOI: http://dx.doi.org/10.14257/AJMAHS.2011.12.06

[10] Zita Maria Almeida do Vale, Carlos Ramos, Rosslin John Robles, "Effective Use of Multiple Random Walks in P2P Networks," *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.4, No.1, pp.1-8, June 2014.
DOI: http://dx.doi.org/10.14257/AJMAHS.2014.06.04

[11] Farkhod Alisherov, "The Security in the Vehicular Ad Hoc Network (VANET) Using Expedite Message Authentication Protocol (EMAP)," *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.1, No.1, pp.99-106, Dec. 2011.
DOI: http://dx.doi.org/10.14257/AJMAHS.2011.12.03

[12] Chul-Woo Park, Ji-Woong Son, Hyun-Ki Hwang, Ki-Chang Kim, "Detection of systems infected with C&C Zeus through technique of Windows API hooking," *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol.5 No.2, pp.297-304, April 2015.
DOI: http://dx.doi.org/10.14257/AJMAHS.2015.04.11

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

조 은 숙(Eun-Sook Cho) **[정회원]**

- 1993년 2월 : 동의대학교 전산통계학과 (이학사)
- 1996년 2월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2000년 2월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
- 2000년 9월 ~ 2005년 2월 : 동덕여자대학교 강의전임교수
- 2005년 3월 ~ 현재 : 서일대학교 컴퓨터소프트웨어과 부교수

<관심분야>
Soft Engineering, Embedded Software, Mobile Computing

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과

<관심분야>
사물지능통신, USN, 네트워크 통신