JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 11 : 2067~2072 Nov. 2016

IOA 기반의 지능형지속위협 대응 위한 지능형 정보보호시스템

류창수*

The IOA-Based Intelligent Information Protection System for Response of Advanced Persistent Threats

Chang-su Ryu*

Department of Cartoon & Game Animation, Yewon Arts University, Seoul 11429, Korea

요 약

최근 기존 정보보호시스템을 우회하는 공격 기법의 발달로 사용자가 인식하지 못하는 형태의 정보자산에 대한 지속적인 공격으로 위협이 되고 있다. 이는 기존 시스템의 단일 대응이 어려운 APT 공격, 우회접근공격 및 암호화 패킷에 대한 공격 등에 대한 침해예측 시도에 대한 즉각적인 대응을 지원하고 공격지표 위주의 방어 전략으로 정보보호시스템에 대한 지속적인 모니터링의 수행이 요구되고 있다. 본 논문에서는 지능형지속위협 공격경로차단을 위해 정보자산에 대한 업무영향평가를 통한 예방통제로 중요한 자산 식별하고 위험을 미리 제거하기 위하여 취약성 분석, 위험분석을 통한 정보통제 정책을 수립하고 서버접근에 대한 내‧외부 우회네트워크 통제, 암호화통신 감시를 통해 탐지통제를 수립하고 백업과 복구를 통해 연계 제어된 교정통제를 하여 지능화된 침해대응 할 수 있도록 중앙집중식 지능형 정보보호시스템을 제안한다.

ABSTRACT

Recently, due to the development of attack techniques that can circumvent existing information protection systems, continuous threats in a form unrecognized by the user have threatened information assets. Therefore, it is necessary to support the prompt responses to anticipated attempts of APT attacks, bypass access attacks, and encryption packet attacks, which the existing systems have difficulty defending against through a single response, and to continuously monitor information protection systems with a defense strategy based on Indicators of Attack (IOA). In this paper, I suggest a centralized intelligent information protection system to support the intelligent response to a violation by discerning important assets through prevention control in a performance impact assessment about information properties in order to block the attack routes of APT; establishing information control policies through weakness/risk analyses in order to remove the risks in advance; establishing detection control by restricting interior/exterior bypass networks to server access and monitoring encrypted communications; and lastly, performing related corrective control through backup/restoration.

키워드 : 공격지표, 지능형지속위협, 정보보호시스템, 공격경로차단

Key word : Indicator Of Attack, Advanced Persistent Threat, Information Security System, Attack Routes Block

Received 01 November 2016, **Revised** 06 November 2016, **Accepted** 12 November 2016

* **Corresponding Author** Chang-Su Ryu(E-mail:twin4me@hotmail.com, Tel:+82-32-869-0571
Department of Cartoon & Game Animation, Yewon Arts University, Seoul 11429, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.11.2067 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

최근 정보보안 환경 변화에 따른 사이버 침해, 사업 기밀유출, 글로벌 보안위협 등의 정보자산에 대한 지속적인 공격으로 위협이 되고 있으며, 기존의 정보보호 시스템을 우회하는 공격 기법의 발달로 사용자가 인지하는 못하는 공격 형태로 진화되고 있다[1]. 또한 단일 보안 기술로는 모든 보안위협을 제거할 수 있는 방안을 기대하기는 현실적으로 불가능하다[2, 3]. 현재 발생하고 있는 대부분의 사이버침해가 지능형 지속 위협(Advanced Persistent Threat)공격을 시작하여 공격대상을 찾아 침투하여 주요정보 및 접근권한을 탈취하는 방식으로 사이버침해를 하고 있다[4]. 본 논문에서는 지능형지속위협 공격경로차단을 위한 예방통제(Prevention Control)로 중요한 자산 식별하고 위험을 미리 제거하기 위하여 취약성 분석, 위험분석을 통한 정보통제 정책을 수립하고 서버접근통제, 암호화통신 감시를 통해 탐지통제(Detection Control)를 수립하고 패킷 태깅, 보안플랫폼, 시스템백업 복구를 통해 교정통제(Corrective Control)를 하여 지능화된 침해대응(Intelligent Violation of Response) 할 수 있도록 정보보호시스템 설계를 제안한다.

Ⅱ. 관련연구

2.1. 지능형지속위협

정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 명확한 목적을 가지고 특정 대상을 겨냥하여 지능적이고 복합적인 방법을 동원하여 지속적으로 공격하는 위협형태의 목표를 지속적으로 추구하는 것을 말한다. 이러한 APT의 의미는 지능형(Advanced), 지속형(Persistent), 위협(Threat)으로 정의할 수 있다[5, 6].

Advanced(지능형) APT : 공격자는 표적의 취약점을 악용할 수 있는 정도의 탁월한 기술로 취약한 대규모 데이터베이스에 액세스하거나 정보 착취 및 코딩 등을 할 수 있다.

Persistent(지속) APT : 장기간에 걸쳐 이루어지는 것으로 인터넷 기반 공격에서 스마트디바이스를 통한 공격까지 총망라한 다양한 공격 경로가 사용될 수 있으며, 데이터에 액세스하기 위해 단순한 보안 침해로 위장해 침입을 시도할 수 있다.

Threat(위협) APT: 취약한 시스템에 항상 공격의 동기와 공격에 대한 능력을 갖고 있으며 침입 시스템 또는 공격자가 존재한다[6, 7].

일반적인 지능형지속위협은 정찰, 최초 진입, 권한상승 및 제어확대, 지속적인 안용의 4가지이며, 지능형 지속위협은 그림 1과 같이 4단계이다.

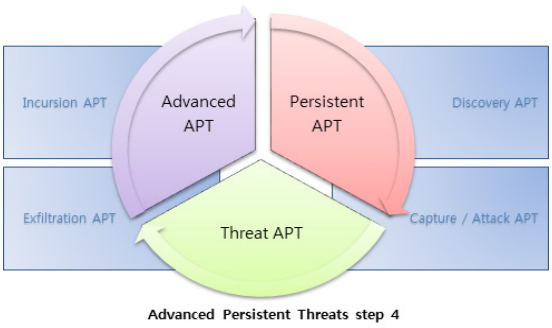

Fig. 1 Advanced Persistent Threat Step 4

2.2. 정보보호시스템

허가되지 않은 접근을 통한 정보의 손상이나 변형, 파괴시키는 행위로부터 정보를 보호하고 무결성, 기밀성, 가용성, 인증, 부인방지, 접근통제를 제공하는 시스템을 말한다. 정보보호시스템은 데이터관점, 시스템관점(네트워크보호, 서버보호), 서비스관점에서의 의미이다. 범용적인 시스템의 보호보다는 특정 서비스의 보호에 특화된 시스템이다[8]. 정보보호시스템은 웹 방화벽, 네트워크 접근 통제, 자료유출방지, 정보보호관리체계 강화, 침입차단시스템, 침입방지시스템, DDos 대응, 가상사설망, 서버보안 등을 포함한다.

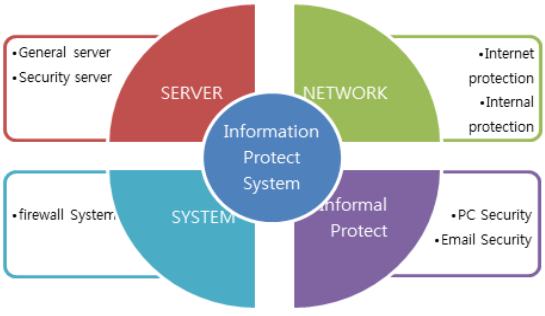

Fig. 2 Information Protect System

그림 2는 정보보호시스템의 의미를 도식화한 것이다.

Ⅲ. 지능형 정보보호시스템 관리방안

3.1. 필요성

기존 정보보호기술을 우회하는 공격 기법의 발달로 사용자가 인식 못하는 공격 형태로 진화하고 있고, 암호화된 트래픽과 서버의 정상 접근에 대한 정보 누출 그리고 사용자의 정상적인 트래픽을 이용한 정보 누출, 다중 공격과 같은 기존의 사이버침해 공격대응 방식에서의 한계점을 가지고 있다. 표 1과 같이 DDos 공격이 발생하였으며 84.8%는 3개국에 집중 발생하고 있다[7, 9]. 따라서 침해예측 시도에 즉각적인 대응을 지원하는 관리시스템이 필요하다.

Table. 1 Infringement Indicator of DDos Attack Rate

DDos Attack Rate	2015 year	2016 year
China	56.1%	55.4%
South Korea	18.4%	20.4% △
USA	11.2%	9.0%
Russia	2.1%	1.9%
Vietnam	1.6%	1.4%
Japan	0.7%	1.0%
Hong Kong	0.8%	0.8%
Other	9.1%	10% △

3.2. 예방통제(Prevention Control)

정보에 대한 영향평가로 중요자산정보에 대한 식별과 위험분석을 통한 취약성 파악과 분석을 통한 정보통제정책을 정의하며 이를 정책에 반영한다[10].

3.3. 탐지통제(Detection Control)

관리자 계정을 관리하고 모니터링 하는 것으로 APT에 대응하려면 최대한 빨리 위협을 감지할 수 있어야 한다. 듀얼 인증관리를 통한 사용자 업무 데이터 관리, 주요보안 사항 로그관리, 주기적 점검사항 로그관리를 통한 비정상적 암호화 패킷 모니터링을 하며 유해사이트 및 P2P 접근관리, 권한 상승, 권한 무단 사용 시도 감시 및 기록을 통한 통제정책을 관리하고 모니터링 한다.

3.4. 침해대응(Intelligent Violation of Response)

초기 시스템에 침입이 발생 했을 때 최적의 전략을 결정하고 관리자 승인을 획득하여 실행하는 것으로 액세스되고 사용되고 이동하며 저장되는 데이터를 파악하여 관련 데이터를 수집하고 침입 탐지 로그와 데이터 식별을 위한 네트워크 기반의 로그 분석과 동시에 네트워크 구조와 접근 통제 리스트를 분석하여 통제정책과 시스템 구성 정보 기반의 회피 기법을 비교 분석을 한다[6, 7].

3.5. 교정통제(Corrective Control)

침입이 발생 했을 때 듀얼인증을 통한 관리자에게 통보하고 로그를 저장하며 네트워크 트래픽을 집중 감시하며 침입자 네트워크를 차단하고 포렌식을 위한 이미지를 보관 및 결과를 통제정책에 반영하고[8] 시스템이미지를 복구하고 보안 에이전트 플랫폼을 동작시킨다.

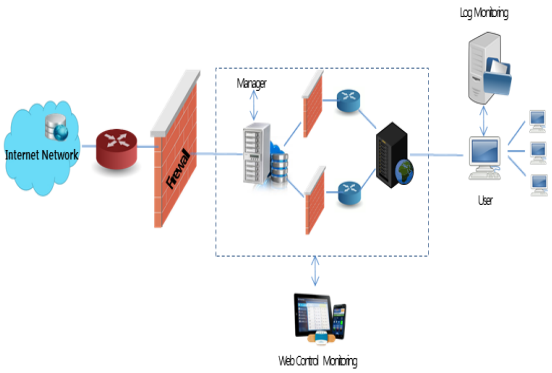

Fig. 3 Visible Integrated Information Protection System

3.6. 정보보호시스템 운영관리

그림 3은 가시적 정보보호시스템을 설명하고 있으며, 물리적 중요 시설물에 대한 출입통제 및 보호가 이루어지며 관련 중요자료는 백업을 한다. 시스템 관리자는 서버의 업데이트 구성변경 등 설치에 필요한 권한에 한정되어 있으며 보안관련 로그 파일정보는 확인할 수 없으며, 모든 액세스 권한은 읽기 전용으로 보안 관리자 역할을 하며, 감사 담당자는 로그 파일을 볼 수만 있으면 시스템 변경은 수행할 수 없다. 지능형지속위협 공격경로차단 위한 정보보호시스템에 대한 것으로 시스템 관리에서 보안을 분리하며 지능형지속위험을 제거하기 위한 사고 유형을 분류하고 공격환경과 대응 능

력을 부여한 적절한 통합 운영 관리한다.

Ⅳ. 제안하는 APT 정보보호시스템

4.1. 구현환경

기존 정보보호시스템의 문제점인 주요정보 및 접근권한이 탈취되는 문제점을 극복하기 위해서는 네트워크 침입과 악성코드에 대응하고 다중공격을 방어 할 수 있는 디지털 포렌식에 표준화되었으며 공격지표의 대응이 적용된 유무선 접속에 보안이 강화된 정보보안시스템을 구축한다.

하드웨어 사양은 Max 3000 EPS, CPU : 3.2 GHz 8-Core, Memory : 32GB, HDD : 2 x 600GB, 랜카드 : 4-port 10/100/1000 Copper, 전원 : Dual, Throughput : 250Mbps 이다. 프로그램은 Windows 환경에서 Visual Studio 2010 툴을 사용하여 C# 언어로 프로그램하고 Windows 서버와 MS SQL Server로 작성하였으며, IEEE802.16 ITU, ITU-T, IEEE, ITU-R IETF, ITU-T IETF 등이 가능한 표준화 설계를 하였다.

4.2. 예방통제시스템

안정적 시스템 운영하기 위하여 보안 관리에 집중 대상이 되는 중요 자산을 식별하고 정보자산의 조사 및 등록을 위해 각 사이트 특성에 맞는 정보자산에 대한 조사 양식 문서를 생성하고 관리, 정보자산 분석가에 의해 식별된 중요 자산에 대해 취약성 분석 도구를 이용하여 잠재적 위험 요소를 분석을 통해 위험 분석 후 예방통제를 마친 중요 자산에 대해 탐지통제를 수행할 수 있도록 통제정책 관리 기능과 공격자가 중요 자산의 통제 정책을 무단으로 변경하지 못 하도록 관리자 Log을 통한 안전한 정책 설정으로 사고 발생 시 감사를 위한 통제정책에 대한 내부 결제 및 감사 로그 저장 및 검색 기능을 제공되어 내재되어 있는 잠재적 위험을 제거하는 기능을 수행한다.

그림 4와 같이 예방통제를 위한 관리자가 사용자가 보안 공지의 확인 여부를 파악하기 위한 통계 로그와 통제정책을 리뉴얼하며 피드백을 처리할 수 있는 시스템이다.

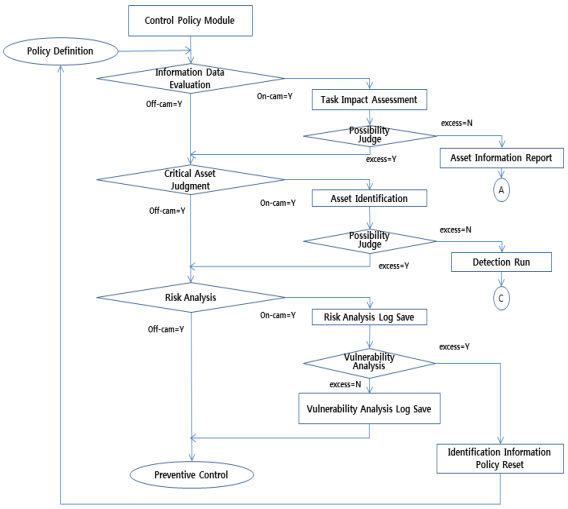

Fig. 4 Preventive Control System Diagram

4.3. 탐지통제시스템

공격이 예측되는 APT 공격의 호스트 역할을 하는 C&C 서버 IP 목록을 관리하고 공격자가 중요 자산에 접속할 때 관리자가 의도한 접근인지를 파악하기 위해 해당 그림 5의 서버 접속 빈도와 서버의 접속 시간 및 포트를 정하는 공지 메시지를 탐지하여 관제시스템에 전송하고 중요 자산에 대한 모든 네트워크 트래픽을 로깅하기 위해 멀리 프로세싱 기법을 적용한 고성능 모니터링과 공격 이용 대상이 될 수 있는 클라이언트 PC의 탐지와 APT 공격 의심 여부를 파악하기 위해 네트워크 트래픽을 분석하고 제거하는 역할을 수행하다.

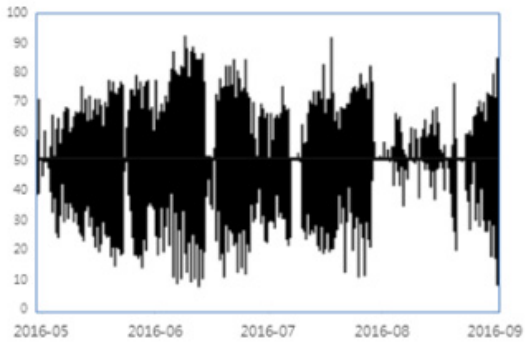

Fig. 5 Server Access Frequency

그림 6은 탐지통제를 위한 서버의 접근 통제를 관리하는 시스템 도식도로 IP 기반 C&C 서버 탐지 기법을 사용하여 일반 패킷뿐만 아니라 암호화 통신을 통해 전달되는 비밀 패킷을 감시와 URL과 IP의 매핑 사전을 이용하여 white url로 등록된 사이트에 대해서는 패킷 감시를 수행하지 않지만 로그는 기록한다.

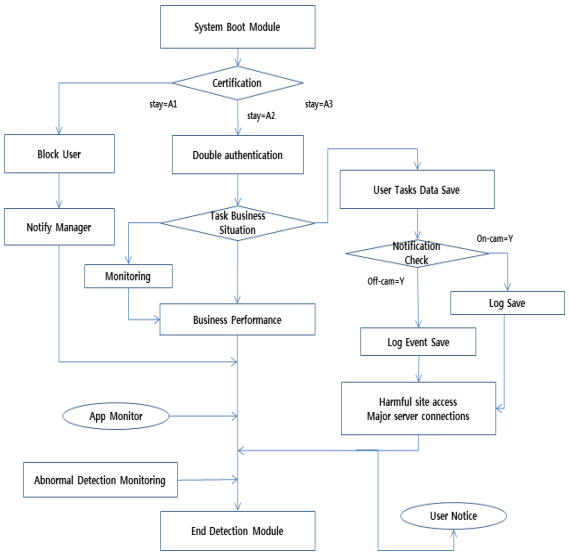

Fig. 6 Detection Control System Diagram

4.4. 교정통제시스템

보안 위험이 되는 사용자 PC를 정확히 판별하여 공격 징후에 대한 1차적인 대응을 수행하는 것으로 공유기를 사용하는 PC에서 발생한 네트워크 패킷을 보안 서버에서 구별하기 위해 사용자 PC에서 발생한 모든 TCP 패킷에 고유 ID를 태깅하고 에이전트가 설치되지 않은 PC에서 해당 에이전트를 자동 배포하고 사용자 PC가 중요 자산에 접근할 경우 공격으로 간주하고 해당 PC의 네트워크 통신 및 주요 매체 접근을 즉각적으로 차단과 동시에 위험 요소로 분리된 프로세스의 실행을 강제 종료하거나 해당 프로세스의 실행을 방지하는 기능을 한다.

그림 7과 같이 교정통제를 위해 해당 PC가 공격자에 의해 탈취된 것으로 판단되면 가용성 확보가 즉각적으로 이루어질 수 있도록 사용자 PC를 항상 안전한 상태로 복원할 수 있도록 표준 시스템 이미지를 저장하고 패치 또는 신규 소프트웨어가 설치된 경우 표준 시스템 이미지를 자동으로 업데이트하고 안정적인 백업 및 복원 작업을 수행한다.

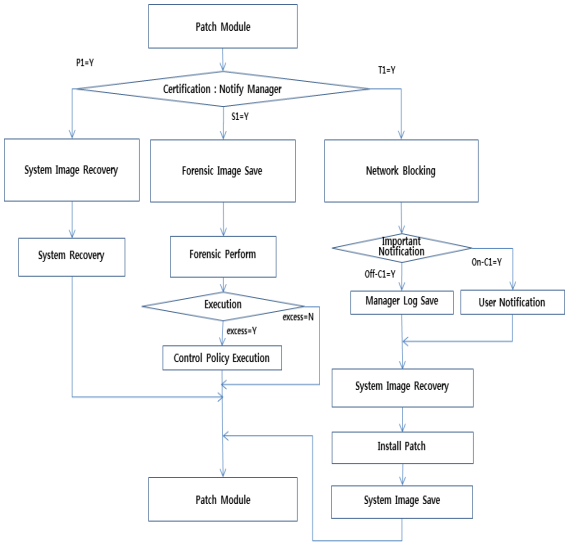

Fig. 7 Corrective Control System Diagram

4.5. 통합된 지능형 정보보호시스템

통합 보안 관리를 위해 각 시스템이 보안에 안정적으로 통신하고 관리자 인증 시 공격자의 계정 탈취에 대한 위험을 원천 차단하기 위해 2채널 인증 체계로 정보를 관리하며 안전한 네트워크 통신을 보장하기 위해 최신 SSL 프로토콜인 TLS 1.2을 지원할 수 있도록 구현한 관리자를 인증할 수 있도록 하는 모듈이다.

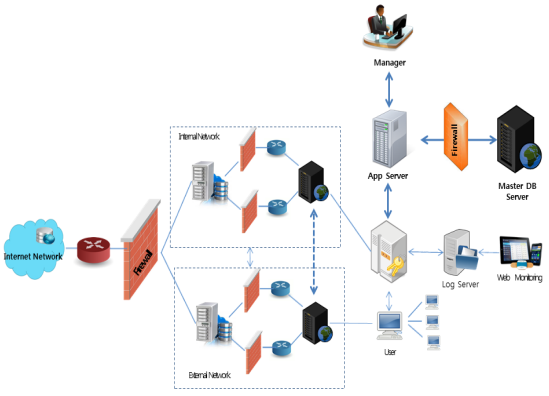

Fig. 8 Integrated Intelligent Information Protection System

그림 8은 네트워크 침입과 악성코드에 대응하며 디지털 포렌식에 표준화되었으며 유무선 접속에 보안이 강화된 정보보안시스템이며 정보자산의 정보를 극대화 할 수 있을 것으로 보인다.

Ⅴ. 결 론

APT에 대응하는 데 반드시 필요한 핵심은 방어책이다. 거의 모든 공격의 성공 여부는 권한 있는 아이덴티티에 대한 액세스 권한을 확보하는 중간 단계에 의해 결정된다.

그러므로 지능형지속위협 공격경로차단을 위한 예방통제와 탐지통제를 통해 교정통제 된 침해대응 할 수 있도록 네트워크 침입과 악성코드에 대응하며 디지털 포렌식에 표준화되었으며 유무선 접속에 보안이 강화된 정보의 보안관리 된 지능형 정보보호시스템 운영관리 하여야 한다. 향후에는 IOA 기반의 지능형지속위협 공격경로차단 기법에 대한 수집 및 공격에 대한 자동보호시스템을 연구할 것이다.

REFERENCES

[1] M. G. Lee, and C. S. Bae, “Next Generation Convergence Security Framework for Advanced Persistent Threat,” *Journal of The Institute of Electronics Engineering of Korea*, vol. 50, no. 9, pp. 92-99, Sep. 2013.

[2] Y. S. Lim, “Review on the Cyber Attack by Advanced Persistent Threat,” *Journal of The Korean Association for Terrorism Studies*, vol. 6, no. 2, pp. 158-178, Jun. 2013.

[3] S. H. Lee, and M. S. Han, “A Study of Defense Method through APT(Advanced Persistent Threat) Penetration Path Analysis in Industrial Network,” *The Journal of Korean Association for Industry Security*, vol. 5, no. 1, pp. 223-253, Jun. 2015.

[4] M. S. Gu, and Y. Z. Li, “A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code,” *Journal of IT Convergence Society for SMB*, vol. 5, no. 4, pp. 37-42, Aug. 2015.

[5] H. W. Kim, J. S. Ryu, and D. S. Kim, “Personal Information Protection by Privacy Impact Assessment in Information System Audit,” *The Journal of the Korea Contents Association*, vol. 11, no. 3, pp. 84-99, Mar. 2011.

[6] NIA, *2015 National Informatization White Paper*, National Information Society Agency, 2015.

[7] KISA, *2016 the first quarter Cyber Threat Trend Report*, Korea Internet & Security Agency, 2016.

[8] CA Technologies. Target Attack 2012 [Internet]. Available: http://www.ca.com/.

[9] Publication 800-30 Revision 1. Guide for Conducting Risk Assessments [Internet]. Available: http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf.

[10] C. S. Ryu, “Operation Plan for the Management of an Information Security System to Block the Attack Routes of Advanced Persistent Threats,” in *Proceeding of the 39th Conference of the Korea Institute of Information and Communication Engineering*, Catholic University of Pusan, pp. 759-761, 2016.

류창수(Chang-Su Ryu)

2003년 목원대학교 컴퓨터교육과 공학사
2006년 목원대학교 컴퓨터교육과 교육학석사
2010년 숭실대학교 수학교육과 교육학석사
2014년 목원대학교 IT공학과 공학박사
2011년~현재 예원예술대학교 만화게임영상학과 조교수
※관심분야 : 클라우드 컴퓨터보안, 모바일 프로그래밍, XML, 5G 모바일 네트워크, 3D 모델링, 증강현실, 사물인터넷