Journal of Convergence for Information Technology
Vol. 9. No. 3, pp. 134-139, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.3.134

지능적인 침입 인지를 위한 침입 상황 분류 모델

황윤철[1], 문형진[2*]
[1]한남대학교 탈메이지 교양교육대학 강의전담교수, [2]성결대학교 정보통신공학부 조교수

Intrusion Situation Classification Model for Intelligent Intrusion Awareness

Yoon-Cheol Hwang[1], Hyung-Jin Mun[2*]
[1]Visiting Professor, Department of Talmage Liberal Arts College, Hannam University
[2]Assistant Professor, Department of Information & Communication Engineering, Sungkyul University

요 약 현대 사회의 발전이 급속하게 진행됨에 따라 이를 뒷받침 하는 사회 전반의 기술들도 전보다 한층 진보되고 지능화되고 있다. 특히 보안 분야에서도 기존의 공격보다 더 정교하고 지능화된 공격들이 새로 생성되고 있고 그 피해 상황도 전보다 몇 배나 크게 발생되고 있다. 기존의 침입에 대한 분류체계를 현시점에 맞게 재정립하고 분류할 필요가 있고, 현재 작동하고 있는 침입탐지 및 감지 시스템들에 이런 분류체계를 적용하여 지능화된 침입에 능동적으로 대응하여 침입 피해를 최소화하는 것이 요구되고 있다. 본 논문에서는 현재 지능적인 공격에 의해 발생하는 침입 유형을 분석하여, 목적하는 시스템의 서비스 안전성, 신뢰성, 가용성을 보장하기 위한 새로운 침입 상황분류 모델을 제안하고, 이 분류 모델을 사용하여 조기에 침입을 감지하여 침입 피해를 최소화하고 보다 능동적인 대응이 가능한 스마트한 침입 인지 시스템을 설계하고 구현하는 연구에 토대를 마련한다.

주제어 : 지능화된 침입, 침입 분류, 능동적인 대응, 침입 상황, 침입인지 시스템

Abstract As the development of modern society progresses rapidly, the technologies of society as a whole are progressing and becoming more advanced. Especially in the field of security, more sophisticated and intelligent attacks are being created. Meanwhile, damaging situations are becoming several times larger than before Therefore, it is necessary to re-classify and enhance the existing classification system. It is required to minimize the intrusion damage by actively responding to intelligent intrusions by applying this classification scheme to currently operating intrusion detection systems. In this paper, we analyze the intrusion type caused by intelligent attack We propose a new classification scheme for intrusion situations to guarantee the service safety, reliability, and availability of the target system, We use this classification model to lay the foundations for the design and implementation of a smart intrusion cognitive system capable of early detection of intrusion, the damages caused by intrusion, and more collections active response.

Key Words : Intelligent Intrusion, Intrusion Classification, Active response, Intrustion Situation, Intrusion Awareness System

*Corresponding Author : Hyung-Jin Mun (jinmun@gmail.com)
Received January 11, 2019 Revised February 12, 2019
Accepted March 20, 2019 Published March 28, 2019

1. 서 론

현대 사회의 기술이 급격하게 발전함으로써 사용자들 간의 정보 공유가 활발해지면서 정보의 노출 및 각종 침해 행위로 인해 개인이 사회생활을 하는 데 많은 어려움을 겪고 있고, 최근의 침해 방법들 또한 더 복잡하고 지능화되어 감에 따라 그 피해 규모 또한 심각해지고 있는 실정이다[1,2].

이러한 침입 행위를 방지하고 효과적인 대응 방법을 마련하기 위해 다양한 정보보호기술들이 개발되고 있지만, 이러한 기술들은 알려진 또는 정의된 공격에 대해서만 효과적인 예방과 탐지를 제공할 뿐 알려지지 않은 취약점이나 공격에 대해서는 적절한 예방과 탐지를 제공하지 못한다는 한계점을 가지고 있다. 그러므로 알려지지 않은 취약점이나 새로운 공격에 의한 침해 사고를 방지하기 위한 기술이 필요하게 되었고, 이에 대한 한 가지 해결책으로 제시될 수 있는 기술이 지능화된 침입 인지 기술이다[3]. 지능화된 침입탐지 기술은 상당한 부분에서 이미 많은 연구가 이루어진 침입탐지 시스템이나 침입방지 시스템 기술에서 얻어진 개념과 기술을 이용한다. 그러나 이런 기술들은 시스템과 소프트웨어의 우발적인 결함과 악의적인 결함 즉 침입이나 바이러스, 웜 등과 같은 악성코드에 대한 기존의 침입형태에만 정상적인 탐지 서비스를 제공할 뿐 지능적인 공격에는 무용지물인 경우가 많다. 따라서 지능적인 공격에 대해서 능동적인 대응을 하기 위해서는 지능화된 새로운 침입탐지 기술 개발이 필요하고 이를 위해서는 기존의 침입 상황을 분류하고 있는 체계를 현시점에 맞게 침입 상황에 대한 개념과 분류가 재정의되어야 한다.

본 논문에서는 이를 위해 기존의 침입 유형과 분류체계를 분석, 검토하여 지능화된 침입 인지 시스템에 적용할 수 있는 침입 상황 분류체계를 제시한다. 이를 통해 서비스를 제공하는 시스템의 안전성, 신뢰성, 가용성을 보장하고 침입 행위에 따른 피해 자원의 신속한 파악과 피해의 최소화를 가져올 수 있다. 또한, 새로운 침입 상황 분류 속성에 기반한 지능화된 침입 인지 시스템을 설계하고 구현하는데 활용한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 침입 유형들을 살펴보고, 3장에서 지능화된 공격을 탐지할 수 있는 침입 상황 인지 프로세스를 제시하고 이 프로세스 과정을 통해 지능화된 공격을 신속하게 탐지할 수 있도록 침입 상황을 분류한 모델을 제안한다. 4장에서는 기존의 침입 분류체계를 제시한 모델에 적용하여 제안한 모델의 타당성을 보여준다. 마지막으로 5장에서는 연구에 대한 의의와 향후 연구 과제를 제시한다.

2. 관련 연구

현재 과거 꿈의 기술이었던 사물인터넷기술이 다방면에 접목되면서 우리들의 일상생활은 더욱 편해지고 있지만 다양한 사물들의 연결은 동시에 잠재적인 보안 및 개인 생활 침해를 야기하고 있다[4-6].

최근에 지능화되고 있는 대표적인 공격유형인 소프트웨어 공급망 대상 사이버 공격, 다양한 경로를 통한 크립토 재킹, 사물인터넷을 겨냥한 신종사이버 위협, 악성행위탐지를 우회하는 공격기법, SNS를 이용한 악성코드 유포, 지능화된 스피어피싱과 APT 공격 현황에 대해 살펴본다. 작년에 발생한 소프트웨어 공급망 대상 사이버 공격에는 웹 개발업체가 공격으로 인해 랜섬웨어에 감염되고 이를 통해 웹 서비스를 제공 받는 수천여 개의 홈페이지 서비스가 중단되는 사고와 파급력이 큰 웹 사이트 및 S/W 개발업체 등을 대상으로 하는 공격이 지속적으로 발생 되었다[7].

가상화폐는 온라인 개인 거래 및 익명성 보장 등의 이유로 여전히 인기가 있으며, 이에 공격자들은 가상화폐를 탈취하기 위해서 다양한 악성코드를 제작 및 유포하고 있다. 작년에는 특히 전용 채굴 시스템이 아닌 일반적으로 사용하는 시스템을 악성코드에 감염시켜 가상화폐를 채굴하는 크랩토재킹이 눈에 띄게 증가했으며, 다양한 경로를 통해 유포됐다[8-10].

인터넷에 연결된 사물인터넷(IoT)가 급증하면서 IoT 기기를 통한 해킹이 자주 발생 되고 있으며, 개인 외부계정 탈취 및 DDoS 공격에서 DDoS에 활용하기 위한 좀비 기기화 및 IP 카메라의 영상 정보의 유출로 공격유형이 진화되고 있다. KISA에 따르면 2012년부터 IoT 취약점 접수가 해마다 2배 이상 증가하고 있다[11].

작년에 발견된 대형 사물인터넷 봇넷인 VPN 필터(VPNFilter)와 POS 단말기를 노리는 악성코드(PinkKite, TinyPOS 등)인 PinkKite, TinyPOS, 스팸 메일을 통해 유포된 신종 랜섬웨어인 파이록키(PyLocky)가 악성 행위탐지를 우회하는 공격 기법들이다[12].

소셜네트워크 서비스(SNS)를 대상으로 한 각종 보안 위협은 오랜 기간 지속적으로 발생하고 있으며, 사이버 공격자들은 가입 회원 수나 인기가 많은 서비스를 겨냥

해 다양한 방식으로 고유한 개인정보 탈취를 시도하고 있다. 특히, 한국에서는 유명 연예인의 인스타그램 계정을 해킹해 신분을 무단도용하거나 유명인의 지인을 사칭해 카카오톡 친구로 접근해 계좌 송금을 유도하는 피싱 사기도 보고되었다. 또한, 가짜 SNS 이벤트 내용으로 현혹해 불특정 다수에게 악의적인 링크를 클릭하도록 현혹하거나 보안위협에 노출될 수 있는 사이트로 접속을 유도하는 등 SNS를 기반으로 한 위협이 지속화되었다[13].

지능화된 스피어피싱과 APT 공격(하우리)으로 이력서 제출, 저작권 위반, 무료폰트 같은 일상적인 내용 들로 위장한 스피어피싱 메일과 특정 분야 웹 사이트의 방문객을 대상으로 하는 타겟형 공격인 "워터링홀" 공격, 국내 모 소프트웨어가 액티브엑스(ActiveX)의 취약점 이용하는 지능화된 APT 공격이 작년이 발생했다[14,15].

3. 능동적인 침입 인지를 위한 침입 상황분류 모델

지능적인 침입의 조기 식별 및 대응은 침입 상황을 신속하게 감지하고 침입 여부의 판단에 대한 정확성을 최적화하는데 달려있다. 지능적인 침입을 판단해서 처리하는 침입 상황 인지 처리 모델을 제안하고 이 모델을 통해서 침입을 판별할 수 있는 침입 상황을 지능적인 공격에 맞게 분류한다.

3.1 침입 상황 인지 처리 모델

침입 방법은 매우 다양하다. 일반적인 침입탐지 및 방지 시스템 측면에서는 침입의 주요 원인을 해커에 의한 공격과 악의적인 의도로 획득한 시스템 취약점으로 볼 수 있다. 여기서 시스템 취약점은 주기적인 패치로 다소간의 침입은 예방할 수 있지만, 해커에 의한 지능적인 침입은 발생 초기에 감지가 어렵고 침입이 발생하여 피해상황이 발생한 후에야 침입 발생을 알 수 있고 그 후에 방지법이 나오고 있다. 지능적인 침입은 조기에 탐지하고 신속한 사전 대응이 이루어지면 기존의 피해보다는 좀 더 피해를 최소화할 수 있다. 따라서 본 논문에서 기존의 침입탐지 과정에 지능적인 침입을 탐지할 수 있는 내용을 추가하여 Fig 1과같이 침입 상황 인지 처리 모델을 제안한다. 제안한 침입 상황 인지 처리 과정을 살펴보면 다음과 같다. 맨 먼저 침입이 의심되는 이벤트가 발생하면 우선 공격 요소가 있는 파일 및 패킷을 수집한다. 그 후 수집된 파일 및 패킷에 대해 연관 관계 분석과 시그니처 기반으로 공격 여부를 판별하여 알려진 침입에 대해 자동 삭제 또는 관리자에 보고하여 특정 파일을 일괄 삭제하거나 조치하는 자동 대응을 실행하고 알려지지 않은 새로운 공격 의심 파일 및 패킷에 대해서는 실행보류라는 사전 대응을 실행한다. 그런 다음 의심 부분을 추출하여 행위 기반으로 한 머신러닝 방법으로 보안 개념과 연계하여 학습하고 머신러닝을 기반으로 조사하고 분석하는 학습 단계를 거친다. 학습 단계에서 습득한 새로운 지식을 바탕으로 공격 의심 파일 및 패킷에 대한 공격 여부 판단이 이루어진다. 정상 파일로 판명되면 파일에 대해 실행을 진행하고 알려지지 않은 지능적인 침입으로 판명되면 의심 파일을 삭제한 후 새로 발견된 침입 상황에 대해 지식을 탐구하고 판단능력을 키우는 지속적인 학습을 진행하여 유사 침입에 대한 새로운 보안 지식을 축적하고 이를 새로운 침입이 발생 되었을 때 적용하여 전보다 신속한 침입탐지와 대응을 한다.

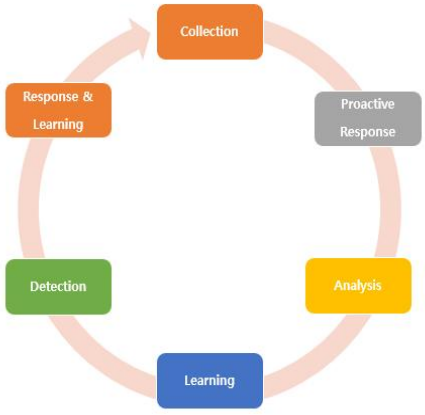

Fig 1. Intrusion Situation Awareness Process Model

3.2 능동적인 침입 인지를 위한 침입 상황분류 모델

침입 인지 시스템에서의 서비스 가용성과 기밀성은 대부분 시스템의 결함과 악의적인 목적을 가진 침입으로 인해 파괴된다. 이런 침입은 실시간적으로 탐지되고 해당 침입으로 인해 발생 되는 에러가 무엇이며, 어떤 자원에 손상을 입히는지 파악하여 그에 따른 대비 전략이 수립되어야 한다. 따라서 이러한 시스템에서 발생 되는 침입을 효율적으로 감지하기 위해서는 징후 감지 대상이 필요하게 되며, 이러한 감지에 필요한 대상을 어떤 유형의 침입이 어떠한 실행 단계와 행동 패턴으로 시스템이 가지고 있는 어떤 자원에 영향을 미치는가에 따라 분류

하면 좀 더 효율적이고 신속하게 침입을 탐지할 수 있다. 따라서 본 논문에서는 지능적인 침입도 조기에 탐지할 수 있는 침입 상황분류 모델을 Table 1과 같이 제안한다.

Table 1. Intrusion Situation Awareness Classification Model

Intrusion Resource	Intrusion Type	State	Risk	Intrusion Behavior
Service Network Endpoint (Drvice/ Sensor)	Confidentiality Integrity Availability	Complete Progress Try	serious alert caution	• Confidentiality / Integrity Infringement of data • Privacy Invasion • Data forgery / Modulation • Access to unauthorized applications and users • Confidentiality / Integrity infringement of signal data • Authentication interruption • Information Disclosure • Service interruption • Confidentiality / Integrity Infringement of device • Unauthorized Access • Cloning and disabling

제안한 모델은 정보관리자나 소유자의 관점에서 침입 상황을 판단할 때 고려되어야 할 요소를 침입 자원, 침입 유형, 진행상태, 위험 정도, 침입 행위와 같이 5가지 대그룹으로 분류했다. 제안한 모델은 외부의 침입에 대해 신속한 인지를 하도록 설계되었으며 침입이 일어나는 과정에서 접근해야 할 자원과 정보보호의 기본 요소의 정의를 기본으로 구분하여, 특정 침입이 진행되는 상태와 위험 정도를 추가하여 분류를 체계화하였으며, 침입 행위를 통해 같은 대응방안을 적용할 수 있는 침입들을 그룹화할 수 있게 하였다.

3.2.1 침입 자원

공격자의 최종 목적지는 네트워크와 방화벽, 라우터 뒤의 호스트, 서버, 엔드 포인트다. 이를 구분하기 위한 분류이다. 서비스는 진행하고 있는 서비스의 애플리케이션을 통해 이루어지는 침입으로 침입에 대한 대응이 웹 서비스를 하는 애플리케이션이나 특정 프로그램 단에서 조치가 이루어져야 하는 침입상황분류이고 네트워크는 침입이 네트워크를 통해 이루어지고 이에 대한 대응이 네트워크 단에서 이루어져야 하는 침입 상황분류이다. 앤드 포인트는 단말이나 장치에서 이루어지는 침입으로 침입에 대한 조치가 단말이나 센서에서 이루어져야 하는 침입 상황분류이다.

3.2.2 침입 유형

자신의 정보자산에 대해 침입의 원인이 정보보호의 3가지 주요 속성인 가용성, 기밀성, 무결성 중 어떤 속성에 관련된 공격인지를 파악하기 위한 분류이다. 기밀성은 접근이 인가된 자만이 접근 가능함을 보장하는 것이고 무결성은 정보 및 처리 방법의 정확성 및 완전성을 보장하는 것이다. 또한, 가용성은 인가된 사용자가 필요한 정보 및 관련 자산에 접근하는 것을 보장하는 것이다.

3.2.3 진행 상태

침입이 정보소유자의 정보자산에 침입이 얼마나 진행되었는지를 구분하기 위한 분류이다. 시도는 침입 시도에 대한 사전 차단 대응이 필요한 침입 상황분류이고 진행은 침입 시도 후 추가적인 침입이 발생할 가능성이 있는 침입 상황분류이다. 완료는 침입이 이미 이루어졌을 가능성이 있으며 사후 대응이 필요한 침입 상황에 대한 분류이다.

3.2.4 위험 정도

침입이 얼마나 위험한가를 구분하기 위한 분류로 최대한 복잡도를 줄이기 위해 침입의 위험도를 주의, 경계, 심각으로 구분한다. 주의는 위험 정도가 가장 낮은 단계로 침입의 사전 준비 징후나 탐지와 같이 침해 효과가 미미한 것으로 관리자의 관심이 요구되는 침입 상황이다. 경계는 침입에 대한 파급효과나 심각도가 중간 정도로 사전 대응 후 추가 분석이 필요한 침입 상황이고, 심각은 가장 위험도가 높은 상황으로 즉각적인 대응이 필요한 침입 상황으로 관리자에게 즉각적으로 보고되고 대응 조치가 이루어져야 하는 침입 상황이다.

3.2.5 침입 행위

침입이 이루어지면 행해지는 행위를 위한 구분으로 침입 자원에 대한 침입 행위를 세분화한 구분으로 서비스에 대한 침입 행위로는 데이터의 기밀성/무결성 침해, 프라이버시 침해, 데이터 위•변조, 비인가 된 애플리케이션 및 사용자의 접근으로 분류되며, 네트워크에 대한 침입 행위로는 신호 데이터의 기밀성/무결성 침해, 인증

방해, 데이터 위•변조, 정보유출, 서비스 거부로 분류된다. 앤드 포인트에 대한 침입 행위로는 장치의 기밀성/무결성 침해, 비인가 접근, 복제 및 무력화로 분류된다.

4. 침입 상황 분류 모델의 적용

제안한 침입 상황분류 모델을 이용하여 가장 최근에 화제가 되고 피해도 크며 자주 발생하는 소프트웨어 공급망 대상 사이버 공격과 가상화폐를 탈취하기 위해서 다양한 악성코드를 제작 및 유포하는 크랩토재킹에 적용하여 분석해 본다.

소프트웨어 공급망 대상 사이버 공격은 침입자들이 불특정 개인보다는 영향력이 있는 기업을 공격목표로 삼는 것이 더 효과적인 결과를 얻는다고 판단하고, 기업고객 또는 어느 특정 회사 네트워크와 유기적으로 연결된 관계사, 협력업체 등을 대상으로 하는 침입을 시도하는 방식이다. 많은 기업들이 사용하는 SW의 공급망을 통한 침입, 특정 대상을 침입하기 위한 최초단계로 대상의 협력업체를 1차로 노리는 침입들이 대표적으로 침입자들은 기업 SW 공급망을 장악하기 위해 다양한 형태의 APT 침입을 시도하고 있다. 이런 종류의 침입들은 침입 자원이 네트워크이고 침입 유형은 기밀성과 무결성을 가지며 진행상태는 시도이면은 위험 정도가 경계이고 진행상태가 완료나 진행이면 위험 정도는 심각하게 분류할 수 있으며 침입 행위로는 신호 데이터의 기밀성/무결성 침해, 정보유출, 서비스 방해로 구분하여 분류할 수 있다. 이를 표로 표현하면 Table 2와 같다.

Table 2. SW Service Network Classification according to proposed classification Model

Intrusion Resource	Intrusion Type	State	Risk	Intrusion Behavior
Network	Confidentiality Integrity	Complete Progress	serious	• Confidentiality / Integrity infringement of signal data • Information Disclosure • Service interruption
		Try	alert	

크립토재킹은 암호화폐를 뜻하는 단어 ‘crypto-currency’와 납치를 뜻하는 ‘hijacking’의 합성어로, 공격자가 몰래 PC에 침입하여 암호화폐 채굴 용도로 사용자의 PC를 활용하는 최신형 사이버 범죄를 말하는 신조어이다. 공격자는 사용자 PC에 몰래 잠입하여 암호화폐 채굴 악성코드를 설치하고 채굴한 암호화폐를 본인의 전자지갑으로 전송하는 방식으로 이뤄지는 게 전형적인 방식이다. 크래토재핑은 침입 자원은 최종적으로 앤드 포인트인(장치)로 볼 수 있고 침입 유형은 기밀성과 무결성을 가지며 진행상태가 시도, 진행, 완료이면 위험 정도는 심각하게 분류할 수 있으며 침입 행위로는 비인가 접근과 복제 및 무력화로 구분하여 분류 할 수 있다. 이 같은 분류는 Table 3과 같다.

Table 3. Cryptojacking Classification according to proposed classification model

Intrusion Resource	Intrusion Type	State	Risk	Intrusion Behavior
Endpoint (Drvice)	Confidentiality Integrity	Complete Progress Try	serious	• Unauthorized Access • Cloning and disabling

5. 결론

지능화된 침입 인지 시스템을 구축하기 위해서는 침입 인지를 위해 취급해야 하는 ‘침입 상황’이 어떤 것인지를 가장 먼저 식별되고 정의되어야 한다. 서비스를 제공하는 시스템의 중요한 서비스가 정상적으로 유지되기 위한 조건은 서비스의 가용성과 서비스의 신뢰, 서비스의 안전성, 그리고 서비스의 보안성이 유지되어야 한다. 이런 특성을 한 가지라도 만족하지 않는다면 해당 서비스는 안정적인 상태라고 볼 수 없다. 이런 특성을 해치는 가장 기본적인 유형은 시스템의 자체 결함과 비인가자에 의한 비정상적인 사용이다. 이를 공격 또는 침입이라고 정의할 수 있다. 시스템의 결함은 매우 다양한 종류의 원인으로 발생할 수 있으나 이는 예방하고 복구하는 방법들이 대부분 구축되어 있어 크게 문제가 되지 않는다. 그러나 두 번째 요인인 공격 또는 침입은 기존의 식별된 것 이외에는 탐지도 어렵고 지능화되어 가고 있어 개인이나 사회, 그리고 국가에도 커다란 문제점이 되고 있다.

본 논문에서 제시한 침입 상황 분류체계는 이런 침입 인지 시스템을 구축하기 위한 첫 단계로써 침입이 발생하는 원인을 정확히 파악하고 침입으로 인해 생길 수 있는 시스템의 피해를 효과적으로 인지하여 시스템의 안전성과 가용성을 보장하는 데 그 목적이 있다. 제시한 분류체계는 어떤 유형의 침입이 어떠한 실행 단계와 행동 패턴을 지니고 있으며 시스템이 가지고 있는 어떤 자원에 영향을 미치는가에 따라 침입 유형을 몇 가지 범주로 나누어 구분하였다. 이는 어떤 침입이 어떤 단계로 실행되

는지 또 시스템의 어떤 부분에 영향을 미치는지를 정확히 판단하고 확인한 후 여기에 상응하는 신속한 대응이 이루어지면 침입으로 인해 발생 되는 피해를 줄이는데 도움이 될 것이다.

향후 연구로는, 먼저 침입을 인지한 스마트한 침입차단 뿐만 아니라 제안된 분류체계를 이용하여 스마트한 침입 인지 프레임워크와 침입 인지 시스템을 설계하고 개발하는 연구가 필요하다.

REFERENCES

[1] R. Von Solms & J. Van Niekerk. (2013). From information security to cyber security. *computers & security*, 38, 97-102.

[2] K. Panetta. (2017). 5 Trends in Cybersecurity for 2017 and 2018. *Smarter with Gartner.*

[3] Symantec. (2017). *2017 Internet Security Threat Report. 22.*https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[4] Y. X. Meng. (2011). The practice on using machine learning for network anomaly intrusion detection. *In Machine Learning and Cybernetics (ICMLC), 2011 International Conference on, 2(1),* 576-581.

[5] H. J. Seo, D. G. Lee, J. S. Choi & H. W. Kim.(2013). IoT Security Technology Trend. *Journal of KIEES, 24(4),* 27-35.

[6] M. Abomhara. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security, 4,* 65-88.

[7] H. H. Lee, Y. Y. Lee & J. S. An. (2016). Commercial and Public Software Intentional Security Weakness Trend. *Journal of Information Security, 26(1),* 9-19.

[8] W. S. Choi, H. S. Kim & D. H. Lee. (2018). Cryptojacking Research Trends. *Journal of Information Security, 28(3),* 33-37.

[9] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology, 8(3),* 85-90.

[10] H. J. Mun, Y. C. Hwang & H. Y. Kim. (2015). Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey. *Journal of Convergence for Information Technology, 5(2),* 1-6.

[11] K. S. Kim & M. S. Kang. (2014). Next Generation Cyber Security Issues, Threats and Countermeasures. *Journal of Electrical Engineering, 41(4),* 69-77.

[12] AhnLab. (2018). *security threat trend.*

[13] C. T. Lim, J. H. Oh & H. C. Jung. (2010). Trend of Malicious Code Technology and Analysis Method. *Information Science Society, 28(11),* 117-126.

[14] M. S Gu & Y. Z. Lee. (2015). A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code. *Journal of Convergence for Information Technology, 5(4),* 37-42.

[15] H. J. Mun, S. H. Choi & Y. C. Hwang. (2016). Effective Countermeasure to APT Attacks using Big Data. *Journal of Convergence for Information Technology, 6(1),* 17-23.

황윤철(Hwang, Yooncheol) [정회원]

- 2008년 2월 : 충북대학교 전자계산학과 (이학박사)
- 2005년 9월 ~ 2007년 2월 : 충북대학교 IT 누리 초빙교수
- 2017년 9월 ~ 현재 : 한남대학교 탈메이지 교양교육대학 강의전담교수

- 관심분야 : 네트워크 및 웹보안, IDS, ITS, Fusion IT Technology
- E-Mail : dolpin98@nate.com

문형진(Mun, Hyung Jin) [종신회원]

- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
- 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수

- 관심분야 : 정보보안, 네트워크 보안, 빅데이터분석
- E-Mail : jinmun@gmail.com