Journal of Convergence for Information Technology
Vol. 12. No. 4, pp. 126-132, 2022
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2022.12.04.126

능동적 탐지 대응을 위한 지능적 침입 상황 인식 추론 시스템 설계

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

Design of Intelligent Intrusion Context-aware Inference System for Active Detection and Response

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

요 약 현재 스마트폰의 급격한 보급과 IoT을 대상으로 활성화로 인해 소셜네트워크 서비스를 이용하여 악성코드를 유포하거나 지능화된 APT와 랜섬웨어 등과 같은 지능적인 침입이 진행되고 있고 이로 인한 피해도 이전의 침입보다는 많이 심각해지고 커지고 있는 실정이다. 따라서 본 논문에서는 이런 지능적인 악성 코드로 이루어지는 침입 행위를 탐지하기 위하여 지능적인 침입 상황 인식 추론 시스템을 제안하고, 제안한 시스템을 이용하여 지능적으로 진행되는 다양한 침입 행위를 조기에 탐지하고 대응하게 하였다. 제안 시스템은 이벤트 모니터와 이벤트 관리기, 상황 관리기, 대응 관리기, 데이터베이스로 구성되어 있으며 각 구성 요소들 사이에 긴밀한 상호 작용을 통해 기존에 인식하고 있는 침입 행위를 탐지하게 하고 새로운 침입 행위에 대해서는 학습을 통해 추론 엔진의 성능을 개선하는 기능을 통하여 탐지하게 하였다. 또한, 지능적인 침입 유형인 랜섬웨어를 탐지하는 시나리오 통하여 제안 시스템이 지능적인 침입을 탐지하고 대응함을 알 수 있었다.

주제어 : 악성코드, 상황 인식, 능동 탐지, 학습, 추론 엔진

Abstract At present, due to the rapid spread of smartphones and activation of IoT, malicious codes are disseminated using SNS, or intelligent intrusions such as intelligent APT and ransomware are in progress. The damage caused by the intelligent intrusion is also becoming more consequential, threatening, and emergent than the previous intrusion. Therefore, in this paper, we propose an intelligent intrusion situation-aware reasoning system to detect transgression behavior made by such intelligent malicious code. The proposed system was used to detect and respond to various intelligent intrusions at an early stage. The anticipated system is composed of an event monitor, event manager, situation manager, response manager, and database, and through close interaction between each component, it identifies the previously recognized intrusive behavior and learns about the new invasive activities. It was detected through the function to improve the performance of the inference device. In addition, it was found that the proposed system detects and responds to intelligent intrusions through the state of detecting ransomware, which is an intelligent intrusion type.

Key Words : Malware, Context-aware, Active Detection, Learning, Inference engine

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received February 24, 2022
Revised March 22, 2022
Accepted April 20, 2022
Published April 28, 2022

1. 서론

최근 들어 이전 시대에서 생각지도 못한 정보통신 기술들이 개발되어 우리 일상생활의 전반에 사용되어 편리함을 더해주고 있다. 그러나 이러한 기술 발전의 이면에는 발전된 기술을 이용하여 악의적인 방법으로 개인의 이익을 취하려는 행위가 더욱 지능적으로 이루어지고 있으며 이로 인하여 사회나 개인의 안위를 심각하게 위협하고 경제적 손실도 크게 입히고 있는 실정이다. 이러한 악성 코드를 이용한 침입 행위를 탐지하기 위해 사용되는 것이 침입 탐지 시스템이고 침입 패턴을 데이터베이스화하여 침입 여부를 판단할 수 있게 제작된 것이 대부분이기 때문에 현재 발생되고 있는 지능적인 침입을 탐지하는데 역부족이다[1]. 이러한 지능적인 악성 코드를 이용한 침입을 조기에 탐지하고 대응할 수 있는 시스템이 절실히 필요하다.

따라서 본 논문에서는 이런 지능적으로 이루어지는 악의적인 행위를 탐지하기 위한 지능적인 침입 상황 인식 추론 시스템을 제안한다. 제안 시스템이 올바로 동작하기 위해서는 먼저 침입 상황에 대한 정의가 필요하고 기존에 알려져 있는 다양한 악성 코드의 특성 정보를 추출하고 분류하여 저장하는 일이 수행되어야 하고 분류된 특성 정보를 이용해 침입 유형을 판단하기 위해 머신러닝과 딥러닝을 기반으로 한 학습을 수행하여 지능적인 초기 추론 엔진을 만들어야 한다. 제안한 침입 상황 인식 추론 시스템은 의심되는 악성 코드를 지속적으로 탐지하는 이벤트 모니터와 탐지된 이벤트를 분석하고 추론하여 침입 여부를 판단하는 이벤트 관리기와 상황 정보를 관리하는 상황 정보 관리기와 상황 정보의 특성 정보와 대응 방식을 저장하는 데이터베이스, 침입 유형에 적합한 대응을 선택하여 실행하는 대응 관리기로 이루어져 있으며 침입 여부를 판단하는 추론 엔진은 기존 분류 범위를 벗어난 새로운 특성 정보가 입력되면 학습을 통해 판단 기능을 업그레이드하여 침입 여부를 판단하는 지능적 추론 엔진으로 설계하였다. 제안한 시스템을 이용하면 지능적으로 진행되는 다양한 침입 행위를 조기에 탐지하고 침입 유형에 가장 적합한 대응을 실행하게 함으로써 침입으로 발생 되는 피해를 최소화하고 침입을 조기에 예방할 수 있다.

논문의 구성은 다음과 같다. 2장에서는 관련 연구로 침입 상황과 상황 인식 컴퓨팅에 대해 살펴보고 3장에서는 지능적 침입 상황 인식 추론 시스템 제안하고 구성 요소와 동작 과정을 기술한다. 4장에서는 제안 시스템의 학습 과정과 랜섬웨어 탐지 시나리오를 사용하여 제안 시스템의 실행을 평가하고 5장에서는 연구의 의미와 향후 연구과제로 결론을 맺는다.

2. 관련연구

최근에 지능화되고 있는 대표적인 악성 코드 유형으로 소프트웨어 공급망과 사물인터넷을 대상으로 하는 악성 코드와 소셜네트워크 서비스를 이용한 악성코드 유포, 지능화된 APT와 랜섬웨어를 들 수 있다[2,3]. 이런 지능적인 악성 코드를 통한 침입을 조기에 식별하고 효과적으로 대응하기 위해서는 침입 상황을 사전에 정의하고 분류해야 하며 침입 상황이 발생하면 신속하게 인지하고 정확하게 침입 여부를 판단하는 침입 상황 인지 시스템이 필요하다.

2.1 침입 상황

침입 상황이란 인가되지 않는 사용자가 소유자 자원의 무결성과 기밀성, 가용성을 저해하는 행위들이나 소유자 시스템의 보안을 붕괴시키는 행위를 말하며, [4]에서 분류한 내용을 기반으로 침입 상황은 침입 자원과 침입자원에 대한 침입 유형, 침입의 진행 정도와 침입의 위험도 그리고 침입이 이루어지면 진행되는 행위로 분류할 수 있다. 침입자의 최종 목적지인 침입자원은 서비스와 네트워크, 엔드 포인트로 분류하고 침입자원에 대한 침입 유형은 기밀성, 무결성, 가용성으로 분류한다. 그리고 침입의 진행 정도는 시도, 진행, 완료로 나누어 분류되고 침입의 위험 정도는 주의, 경계, 심각으로 분류되며, 침입이 이루어지면 진행하는 행위는 서비스와 네트워크, 앤드 포인트에 대해 세부적으로 분류된다.

1) 서비스에 대한 침입 상황 : 데이터의 기밀성/무결성 침해, 프라이버시 침해, 데이터 위•변조, 비인가된 애플리케이션 및 사용자의 접근
2) 네트워크에 대한 침입 상황 : 신호 데이터의 기밀성/무결성 침해, 인증방해, 데이터 위•변조, 정보유출, 서비스 거부
3) 앤드 포인트에 대한 침입 상황 : 장치의 기밀성/무결성 침해, 비인가 접근, 복제 및 무력화

2.2 상황 인식 컴퓨팅

상황 인지 시스템은 현재 발전하고 있는 사물인터넷

(IoT)을 인간이 접근하기 어려운 환경에 접목하여 사용하기 위해 많은 연구들이 진행되고 있으며, 상황 인식 시스템의 최소 데이터 단위는 상황 정보이며 상황을 표현하는 모든 물체 및 이들 간의 관계 정보가 상황 정보가 될 수 있다. 상황 인식 시스템에서 가장 중요한 구성요소는 컴퓨터가 주변 상황 정보를 복합적으로 정확하게 이해하고 그 상황에 적합한 서비스를 제공하는 것이다[5].

상황 인식 컴퓨팅은 현실 세계의 모든 상황을 표현하는 기술적 수단을 제시하며 이를 기반으로 상황을 인식하고 상황 중 특징을 추출하여 학습하고 추론하는 등의 지능화된 기법을 적용하여 인간 중심의 자율적인 서비스를 가능하게 하는 기술을 의미하며 인간 세계의 의사 소통과 거의 동일한 수준으로 인간과 컴퓨터 간의 의사 소통이 가능하도록 하는 것이 목적이다[6]. 상황 인식 컴퓨팅은 입력정보가 들어오면 상황 정보를 이용해 제작된 상황 인식 시스템에서 입력 정보에 해당하는 상황을 판단하여 사용자에게 알려주는 형태로 동작한다. 이를 표현하면 Fig 1과 같다.

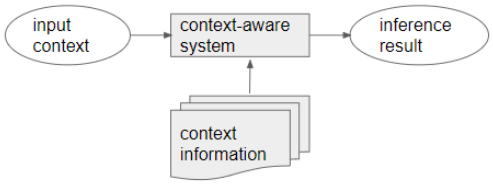

Fig 1. context-aware system

상황 인식 컴퓨팅에서 사용하는 상황 정보로는 사용자의 상황과 물리적 환경 상황, 컴퓨팅 시스템 상황과 사용자와 컴퓨터 상호 작용 이력, 기타 미분류 상황 등이 있으며 상황 인식 컴퓨팅에서는 사용자에게 정보와 서비스를 제공할 뿐만 아니라 사용자를 위한 서비스를 자동으로 실행할 수 있고 이후 검색을 위한 상황 정보를 표현하는 서비스를 제공할 수 있다.

3. 지능적 침입 상황 인식 추론 시스템

침입 상황 인지 추론 시스템은 침입 행위가 발생하면 이를 탐지하기 위해 사용하는 시스템으로서 침입을 탐지했을 때 가장 먼저 침입 유형을 분석하여 판별한 다음 각 침입 유형별로 대응 방법을 제공해야 한다[7]. 제안하는 침입 상황 인식 추론 시스템은 지능적 침입 탐지 서비스와 네트워크, 앤드 포인트에 대한 침입 행위를 상황 정보로 사용하여 상황을 추론하고 가공하는 추론 엔진을 공유된 상황 정보를 이용하여 학습시킨 다음 추론 엔진을 통하여 현재 탐지된 상황을 도출하여 결과를 시스템 관리자에게 보고하는 서비스를 제공한다. 지능적 추론 엔진은 보다 정확한 침입 탐지를 위해 머신러닝이나 딥러닝을 조합한 앙상블로 학습하고 입력된 특성 정보에 대해 침입 유형을 분류하고 대응 방법을 선택하고 추천하는 판단 기능을 수행한다. 지능적 침입 상황 인식 추론 시스템은 Fig 2와 같이 이벤트 모니터, 이벤트 관리기, 상황 관리기, 대응 관리기, 데이터베이스로 이루어진다.

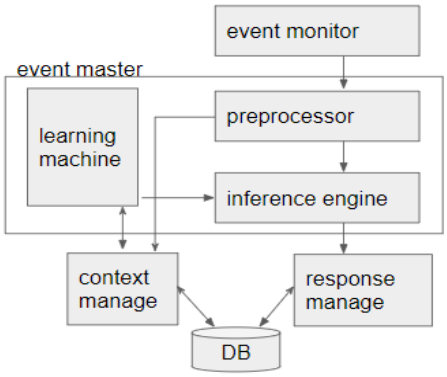

Fig 2. intrusion context-aware inference system

이벤트 모니터는 침입 상황이 발생했는지를 감시하며 침입 상황이 발생하면 침입 정보를 이벤트 관리기의 전처리기로 전송하는 기능을 수행한다. 이벤트 관리기는 이벤트 모니터에서 전송된 침입 상황을 처리하여 침입 여부를 판별하고 새로운 침입 유형에 대해서 학습하는 기능을 수행하며 전처리기와 학습기, 추론 엔진으로 구성된다. 전처리기는 이벤트 모니터에서 전송받은 침입 상황 정보에서 침입 상황에 관련된 특징 정보를 추출하는 기능을 수행하고 추론 엔진은 기본적으로 데이터베이스에 저장된 이전 침입 상황들의 특징 정보를 이용해 침입 여부를 판단할 수 있게 만들어진 지능화된 추론 엔진으로 전처리기에서 전송된 특징 정보를 이용하여 침입 상황을 추론하여 침입 여부나 유형을 판별한다. 또한, 침입 판별이 모호한 새로운 특징 정보는 전처리기에서 상황 관리기로 전송하게 하는 기능을 수행한다. 학습기는 상황 관리기에서 받은 특징 정보를 이용

하여 새로운 특징 정보를 평가하기 위한 학습을 진행하여 새로운 특징 정보를 평가하고 추론 엔진의 성능을 업그레이드 시키는 기능을 수행한다. 상황 관리기는 전처리기에서 추출된 특징 정보가 기존의 침입 상황이 아닌 경우 추출된 특징 정보를 이벤트 관리기의 전처리기에서 전송받고 이 특징 정보를 데이터베이스에 저장한 다음 학습기에 전송하여 학습을 수행하여 새로운 특징 정보를 평가하게 하고 그 결과를 바탕으로 대응 방식을 결정하여 해당 특성 정보에 대한 데이터베이스의 대응 정보 필드에 저장한다. 데이터베이스는 침입 유형별 악성 코드들의 특징과 침입 유형별 대응 방법이 저장된다. 대응 관리기는 이벤트 관리기의 추론 엔진에서 전송받은 침입 유형을 이용하여 데이터베이스에서 침입 유형에 맞는 대응 방법을 요청하고 대응 결과를 전송받아 대응 결과에 따라 침입 행위에 대한 대응을 실행하고 관리자에게 침입을 보고하는 등의 침입에 적합한 대응을 수행한다.

제안한 시스템의 가장 큰 특징은 학습 과정을 반복적으로 실시하여 정확한 침입 여부를 판단 추론 엔진의 성능을 지속적으로 향상시키고 침입에 가장 적합한 대응을 선택하여 수행함으로써 침입에 대한 피해를 최소화하도록 설계되었다. 제안한 침입 상황 인지 추론 시스템은 아래와 같은 단계로 동작하여 침입 여부 판단과 대응 한다.

단계 1: 지속적으로 감시 기능을 수행하는 이벤트 모니터에 침입 행위가 감지된다.

단계 2: 감지된 침입 행위는 이벤트 모니터에서 이벤트 관리자의 전처리기로 전송된다.

단계 3: 침입 행위를 받은 전처리기에서는 침입 행위에 대한 특성 정보를 추출한다.

단계 4: 전처리기는 추출된 특성 정보를 추론 엔진으로 전송한다.

단계 5: 특성 정보를 받은 추론 엔진은 기존의 학습한 내용을 기반으로 특성 정보에 대한 침입 여부와 침입 유형을 다음과 같이 두가지 유형으로 판단하고 분류한다.

a. 기존 학습한 내용으로 판단이 가능하면 침입 여부와 침입 유형을 판단하여 대응 관리기로 결과를 전송한다.(단계 6으로 진행)

b. 기존의 학습한 내용으로 판단하기 어려운 변형된 침입 유형이나 새로운 침입 유형이면 특성 정보를 상황 관리기로 보낸다.(단계 7로 진행)

단계 6: 추론 엔진으로부터 판단 결과를 받은 대응 관리기는 침입 유형에 맞는 대응 방식을 데이터베이스에 요청해서 받고 그에 적합한 대응을 수행한다.

단계 7:

a. 특성 정보를 받은 상황 관리기는 새로운 특성 정보를 데이터베이스에 저장하고 특성 정보를 학습기로 보내 특성 정보에 대하여 기존의 학습 정보와 더불어 학습을 진행하여 침입 여부와 유형을 학습기에서 판단하고 분류하는 추론 엔진을 생성한다. 학습기는 생성된 추론 엔진으로 기존의 추론 엔진을 업그레이드하고 판단 결과를 상황 정보기에 전송한다.

b. 새로운 특성 정보에 대한 판단 결과를 전송 받은 상황 관리기는 그에 적절한 대응 정보를 생성하여 데이터베이스 해당 특성 정보에 해당하는 필드에 저장한다.

c. 업그레이드된 추론 엔진으로부터 판단 결과를 받은 대응 관리기는 침입 유형에 맞는 대응 방식을 데이터베이스에 요청해서 받고 그에 적합한 대응을 수행한다.

4. 학습 과정과 실행 성능 평가

제안한 침입 상황 인식 추론 시스템의 추론 엔진이 만들어지는 학습 과정을 살펴보면 Fig 3과 같다.

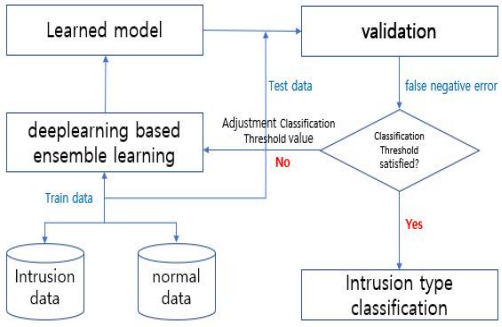

Fig 3. intrusion context-aware inference system learning process

기존에 발생하였던 침입 상황을 유형별로 수집하여 수집된 데이터에서 침입에 관련된 특징 정보를 추출한 다음 추출한 데이터를 침입 데이터로 분류하고 침입 유형에 관련된 정상적인 행위에 대한 특징 정보들을 수집하여 정상 데이터로 분류한다. 분류된 데이터를 섞은

다음 훈련 데이터와 테스트 데이터로 분할 한 후 10-fold 교차검증을 이용하여 딥러닝 기반의 모델들을 통해 학습을 진행한다. 학습이 마치고 생성된 모델은 침입 탐지의 정확성을 높이기 위하여 침입을 침입으로 탐지 못하는 에러(false negative error)의 임계값을 0.3~0.7로 조정해 가면서 검증 단계를 진행한 후 최적의 모델을 생성한다. 이렇게 최종 선정된 모델을 침입 여부와유형을 판단하는 추론 엔진으로 사용한다.

제안 시스템의 실행 평가는 현재 가장 지능적으로 진행되어 사회와 개인에게 큰 피해를 야기하고 있는 랜섬웨어에 대한 침입 상황 시나리오를 사용하여 평가해 보겠다. 랜섬웨어는 공격 대상 시스템이나 파일들을 인질로 잡고 시스템이나 파일 소유자에게 금전적인 요구를 하는 악성코드로 피해를 입는 산업 분야도 에너지, 식량, IT, 제조, 서비스, 운송 분야 등으로 다양해지고 있다[8,9]. 그리고 국내 랜섬웨어 신고 건수와 공격자의 요구 금액 및 실질적 기업의 피해 금액을 살펴보면 Table 1과 같다[10].

Table 1에서 보는 것과 같이 국내의 경우 2019년 KISA에 신고된 랜섬웨어는 39건이지만, 2020년에는 127건으로 3배 이상 급증했고 2021년에는 55건이지만 피해액은 전년도보다 늘어났다.

Table 1. Reports of Ransomware Infringement

year	number of reports	Average Damage Negotiations (per case)
2018	22 case	$41.198
2019	39 case	$84.116
2020	127 case	$154.108
2021	55 case	$220.298

제안 시스템이 랜섬웨어를 탐지하기 위해서는 제안 시스템의 추론엔진이 랜섬웨어에 대해 미리 학습하는 과정이 필요하고 이 과정에서 랜섬웨어의 특징 정보가 필요하다. 따라서 이 논문에서는 랜섬웨어의 특징 정보를 [11-17]에 있는 주요 랜섬웨어를 기반으로 유입 방식, 유입 시기, 공격 대상 OS, 공격 대상 파일 확장자, 사용 암호화 방식, 암호화 후 생성하는 파일 확장자, 요구 금액, 랜섬웨어 유형으로 추출해서 학습과정을 거쳤다고 가정하고 CERBER 랜섬웨어의 침입 상황이 발생되었을때 제안 시스템이 이를 탐지하는 과정을 살펴보겠다.

CERBER 랜섬웨어는 스팸 메일이나 익스플로잇 킷(Exploit Toolkit)을 이용하여 유포되고 2016년 3월에 발생되었고 windows를 공격대상으로 대상 파일을 AES-128이나 RSA-2048로 암호화한 후 파일의 확장자를 .cerber로 바꾸고 1.2 비트코인을 요구한다. Table 2는 CERBER 랜섬웨어의 특징 정보를 나타낸 것이다.

Table 2. CERBER ransomeware feature information

Inflow method	Spam / Malvertising
spread	March 2016
target OS	windows
file extention of attack	about 450
encryption method	AES-128, RSA-2048
file extensions created after encryption	.cerber
request amount	1.2 (BTC)
type	CERBER

CERBER 랜섬웨어로 의심되는 침입 상황이 발생하면 침입 상황 인식 추론 시스템의 이벤트 모니터에서 이를 감지하고 이벤트 관리자의 전처리기로 이 상황을 보낸다. 전처리기에서는 전송받은 상황 정보에서 랜섬웨어에 대한 특징 정보를 추출한 다음 추론 엔진으로 보낸다. 추론엔진은 전송 받은 특징 정보를 기반으로 침입 상황에 대한 유무와 유형을 판단한다. 기존에 CERBER 랜섬웨어에 대한 학습이 진행되어 있다면 지금 상황을 침입 상황으로 판단하고 침입 유형으로 랜섬웨어라는 것을 판별하여 대응 관리자에게 결과를 전송한다. 침입 유형을 전송받은 대응 관리자는 침입 상황이 아니면 정상적인 상황으로 현 상황 판단을 종료하고 침입이면 상황 정보를 관리하는 데이터베이스에 판단된 침입 유형에 해당하는 대응 방식을 요청하여 그 결과를 전송받아 침입 상황에 대한 대응을 진행한다. 만약에 기존에 CERBER 랜섬웨어에 대한 학습이 진행되어 있지 않다면 전처리기는 전송받은 상황 정보를 상황 관리자에 보낸다. 특징 정보를 받은 상황 관리자는 이를 데이터베이스에 저장하고 학습기에 이 정보를 전송한다. 상황 관리자로부터 특징 정보를 받은 학습기를 이 특징 정보를 바탕으로 구축되어 있는 학습기를 통해

학습을 진행한다. 학습이 종료되면 학습기는 학습 결과인 침입 유무와 침입 상황이 어떤 유형인지를 상황 관리기에 전송하고 기존의 추론 엔진도 업그레이드 한다. 그리고 학습 결과를 전송 받은 상황 관리자는 판단된 결과에 해당되는 대응 방식을 선택하여 데이터베이스에 저장한다. 업그레이드된 추론 엔진에서는 지금 상황을 다시 판단하여 대응 관리자에 전송한다. 침입 유형을 전송 받은 대응 관리자는 침입 상황이 아니면 정상적인 상황으로 현 상황 판단을 종료하고 침입이면 상황 정보를 관리하는 데이터베이스에 판단된 침입 유형에 해당하는 대응 방식을 요청하여 그 결과를 전송받아 침입 상황에 대한 대응을 진행한다.

Table 3는 기존 침입탐지 시스템과 제안 시스템을 5개의 성능측면에서 비교분석하였다.

Table 3. Performance evaluation of the proposed system

Item	Existing intrusion detection system	Proposal system
known intrusions	detect all	detect all
new intrusions	undetectable	detect all
transformed intrusions	some detection	detect all
engine improvement	manual	automatic
response time	somewhat slow	fast

Table 3에서 보듯이 기존 방식은 탐지했던 침입에 대해서만 완전히 탐지하지만 새로운 침입이나 변형된 침입은 탐지에 어려움이 있고 탐지 엔진도 수동으로 업그레이드 해야되고 대응 시간도 그리 빠르지 않다. 그러나 제안 시스템은 학습이 제대로 진행되었다면 기존의 침입 뿐만 아니라 새로운 침입이나 변형된 침입도 빠르게 인식하고 그에 따른 대응도 빠르며 침입을 판단하는 엔진도 지속적으로 자동 업그레이드가 가능하다.

5. 결론

오늘날 새롭게 등장하고 있는 정보 통신 기술을 사용하여 모든 사물들이 서로 연결되는 초연결사회로 진행되고 있는 상황을 이용하여 사회와 개인을 위협하는 다양한 유형의 지능적인 침입이 발생되고 있는데 기존의 탐지 시스템으로는 탐지가 어려워 여러 분야에서 많은 불안감을 가지고 있는 실정이다.

따라서 본 논문에서는 기존의 보편적인 침입 상황 뿐만아니라 현대에 들어서 만연하고 있는 지능적인 악성 코드를 이용한 침입 상황까지도 조기에 탐지하고 대응할 수 있는 지능적 침입 상황 인식 추론 시스템을 제안하였다. 제안한 시스템은 이벤트 모니터와 이벤트 관리기, 상황 관리기, 대응 관리기, 데이터베이스로 로 구성되어 있으며 각 구성 요소들 사이에 긴밀한 상호 작용을 통해 기존에 인식하고 있는 침입 행위를 탐지하게 하고 새로운 침입 행위에 대해서는 학습을 통해 추론 엔진의 성능을 개선하는 기능을 통하여 탐지하게 하였다. 그리고 지능적인 침입 유형인 랜섬웨어를 탐지하는 시나리오 통하여 제안한 시스템이 지능적인 침입을 적절하게 탐지하고 대응할 수 있음을 알 수 있었다. 그리고 현재에 만연하고 있는 지능적인 악성 코드를 이용한 침입을 쉽게 탐지하고 침입에 의한 피해를 최소화하기 위해서는 제안 시스템과 같은 지능적인 침입 상황 인식 추론 시스템이 적실히 필요하다는 것을 실감하였다.

이 논문에서 제안한 시스템을 실제로 구현하기 위해서는 침입 상황별 특징 정보를 추출하는 방법과 추출된 특징 정보들을 가지고 최적의 추론 엔진을 생성하기 위한 딥러닝 기반 앙상블 학습 방법에 대한 연구가 선행적으로 진행된 다음에 전체적인 시스템을 구현하는 것이 순차적으로 이루어져야 한다.

REFERENCES

[1] D. H. Lakshminarayana, J. Philips & N. Tabrizi. (2019). A survey of intrusion detection techniques. *In 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)* (pp. 1122-1129). IEEE. DOI : 10.1109/ICMLA.2019.00187.

[2] E. J. Khaleefa & D. A. Abdulah. (2022). Concept and difficulties of advanced persistent threats (APT): Survey. *International Journal of Nonlinear Analysis and Applications, 13(1),* 4037-4052. DOI : 10.22075/IJNAA.2022.6230

[3] 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),* 7-23. DOI : 10.221 56/CS4SMB.2016.6.1.017

[4] Y. C. Hwang. & H. J. Mun (2019). Intrusion

Situation Classification Model for Intelligent Intrusion Awareness. *Journal of Convergence for Information Technology, 9(3),* 134-139.
DOI : 10.22156/CS4SMB.2019.9.3.134

[5] Charith Perera, et al. (2014). Context Aware Computing for the Internet of Things: A Survey. *Communications Surveys & Tutorials, IEEE. 16(1).* 414-454.
DOI : 10.1109 /SURV.2013.042313.00197.

[6] Y. Wang, W. Ji & J. Wang. (2012). Design and Implementation of Inference Engine for Conflict Resolution. *In 2012 Second International Conference on Intelligent System Design and Engineering Application (pp. 220-223).* IEEE.
DOI : 10.1109/ISdea .2012.677.

[7] S. Park. (2014). Current Status and Analysis of Domestic Security Monitoring Systems. *Journal of the Korea Institute of Electronic Communication Sciences, 9(2),* 261-266.
DOI : 10.13067/JKIECS.2014.9.2.261

[8] J. Y. Moon. & Y. H. Jang. (2016). Ransomware Analysis and Method for Minimize the Damage. *The Journal of the Convergence on Culture Technology (JCCT), 2(1),* 79-85.
DOI : 10.17703/JCCT.2016.2.1.79

[9] AhnLab. (2017). *Latest Ransomware Trend Analysis Report.* Seongnam : AhnLab.

[10] KISA. (2021). *Ransomware Special Report.* KISA(Online). https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=36211

[11] KISA. (2017). *Cyber Threat Trend Report for the first quarter of 2017.* KISA(online). https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=25623&queryString=cGFnZT03JnNvcnRfY29kZT0mc29ydF9jb2RlX25hbWU9JnNlYXJjaF9zb3J0PXRpdGxlX25hbWUmc2VhcmNoX3dvcmQ9.

[12] CERT-EU. (2017). *WannaCry Ransomware Analysis Propagated to Windows SMB Vulnerabilities.* RedAlert.

[13] Kenet. (2017). *Petya Ransomware v0.3 National KE-CIRT-CC Report.* ThaiCERT(Online). https://cert. kenet.or.ke/node/2.

[14] HAURI. (2017). *SECURITY MAGAZINE ViRobot.* HAURI(Online). http://www.hauri.co.kr/EBook/zoom.html?intSeq=99.

[15] TACHYON & ISARC. (2017). *Analysis of sage ransomware that appeared in version 2.0.* (Online). https://isarc.tachyonlab.com/1085.

[16] Korea Ransomware Infringement Response Center. (2017). *CryptoShield.* rancert(Online). https://www.rancert.com/bbs/bbs.php?bbs_id=case&mode=view&id=64.

[17] M. C. Lim. (2017). *Ransomware Infected Linux Servers, What Happens?.* ZDNet Korea(Online). https://zdnet.co.kr/view/?no=20170613100723.

황 윤 철(Yooncheol Hwang) [정회원]

· 2008년 2월 : 충북대학교 전자계산학과(이학박사)
· 2019년 3월 ~ 2021년 2월 : 가천대학교 소프트웨어 중심대학 사업단 소프트웨어교육센터 초빙교수
· 2021년 3월 ~ 현재 : 한남대학교 탈메이지 교양교육대학 조교수
· 관심분야 : 네트워크 및 웹 보안, IDS, ITS, Fusion IT Technology(AI)
· E-Mail : dolpin98@nate.com

문 형 진(Hyung-Jin Mun) [종신회원]

· 2008년 2월 : 충북대학교 전자계산학과(이학박사)
· 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수
· 관심분야 : 정보보안, 네트워크 보안, 빅데이터분석
· E-Mail : jinmun@gmail.com