creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

조선대학교
CHOSUN UNIVERSITY

[UCI]I804:24011-200000266480

2018년 2월

석사학위 논문

APT 공격 탐지를 위한 온톨로지 기반의 상황인지 모델

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 광 민

조선대학교
CHOSUN UNIVERSITY

APT 공격 탐지를 위한 온톨로지 기반의 상황인지 모델

Ontology-Based Context Awareness Model for APT Attack Detection

2018년 2월 23일

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 광 민

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

APT 공격 탐지를 위한 온톨로지 기반의 상황인지 모델

지도교수 김 판 구

이 논문을 공학석사학위신청 논문으로 제출함.

2017년 10월

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 광 민

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

김광민의 석사학위논문을 인준함

위원장 조선대학교 교수 정 일 용 (인)

위 원 조선대학교 교수 최 준 호 (인)

위 원 조선대학교 교수 김 판 구 (인)

2017년 11월

조선대학교 산업기술융합대학원

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

목 차

ABSTRACT

Ⅰ. 서론 ····· 1
A. 연구 배경 및 목적 ····· 1
B. 연구 내용 및 구성 ····· 2

Ⅱ. 관련 연구 ····· 3
A. 상황인지 ····· 3
B. 온톨로지 기반 상황인지모델 ····· 5
C. APT 공격 개념과 기존연구 ····· 7
1. APT 공격 개념 ····· 7
2. APT 공격 기존연구 ····· 9

Ⅲ. APT 공격 탐지를 위한 온톨로지 기반 상황인지 모델 ····· 11
A. 온톨로지 기반 상황인지 모델 필요성 ····· 11
B. 프레임워크 ····· 13
C. 온톨로지 설계 및 구축 ····· 15
1. APT 공격 온톨로지 - 클래스/계층 정의 ····· 15
2. APT 공격 온톨로지 - 속성 정의 ····· 22
3. APT 공격 온톨로지 - 관계 정의 ····· 22
D. 추론 규칙 설계 ····· 24
1. APT 탐지를 위한 추론 단계 정의 ····· 24
2. 추론 규칙 설계 ····· 26

Ⅳ. 실험 및 결과 ····· 28

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

A. 상황 시나리오 기반의 APT 공격 탐지 ····· 28
1. 상황 시나리오 구성 ····· 28
2. 상황정보에 따른 온톨로지 기반 클래스 추출 ····· 29
3. 시나리오 기반 추론식을 이용한 APT 공격 탐지 ····· 30
4. 추론엔진을 이용하여 평가 ····· 31
V. 결론 및 제언 ····· 32

참고문헌 ····· 33

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

표 목 차

[표 3-1] APT 공격의 특성 ····· 11
[표 3-2] 상황인지 모델링 기술과 요구사항 ····· 12
[표 3-3] Level 1 클래스와 Level 2 클래스 정의 ····· 15
[표 3-4] Means≡Behavior Level 2 클래스와 Level 3 클래스의 정의 ····· 17
[표 3-5] Means≡Behavior의 Level 3 클래스와 Level 4 클래스 정의 ····· 18
[표 3-6] Consequence의 Level 2 클래스와 Level 3 클래스 정의 ····· 19
[표 3-7] Consequence의 Level 3 클래스와 Level 4 클래스 정의 ····· 20
[표 3-8] LogicExploit와 하위 클래스 정의 ····· 21
[표 3-9] 보안위협 온톨로지 주요 Object Property의 정의 ····· 22
[표 3-10] APT 공격의 단계별 진행과정 ····· 24
[표 3-11] 공격단계 추론규칙 ····· 26
[표 3-12] 침투단계 추론규칙 ····· 27
[표 3-13] 수집단계 추론규칙 ····· 27
[표 4-1] 이상 상황 시나리오 구성 ····· 28
[표 4-2] 이상 상황정보의 온톨로지 클래스 정의 ····· 29
[표 4-3] 이상상황 시나리오 기반 추론결과 ····· 30

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

그 림 목 차

[그림 2-1] APT 공격 프로세스 ····· 8
[그림 3-1] 온톨로지 모델링 및 상황인지 추론 시스템 구성도 ····· 13
[그림 3-2] AttackTarget Level 1과 Level 2 관계 ····· 16
[그림 3-3] AttackPurpose Level 1과 Level 2 관계 ····· 16
[그림 3-4] AttackMethod sLevel 1과 Level 2 관계 ····· 17
[그림 3-5] Means≡Behavior 와 하위 클래스들의 관계 ····· 19
[그림 3-6] Consequence 와 하위 클래스들의 관계 ····· 21
[그림 3-7] Means, Consequence, Attackpurpose 클래스 관계 정의 ····· 23
[그림 4-1] SpearPhising_mail의 클래스 관계 ····· 29
[그림 4-2] SWRL을 이용한 추론식 ····· 31
[그림 4-3] 추론규칙 실행 결과 ····· 31

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

ABSTRACT

Ontology-Based Context Awareness Model for APT Attack Detection

KwangMin Kim
Advisor : Prof. Pankoo Kim, Ph.D
Department of Software Convergence Engineering
Graduate School of Industry Technology Convergence, Chosun University

With the Internet of cloud services, big data, machine learning, mobile technology, artificial intelligence, and similar new technologies providing the ability to connect and intelligently handle every aspect of our lives, these recent developments in IT technology have facilitated a highly personalized service and dramatically improved the productivity of industry, leading to a better quality of life. However, such changes have become the source of serious threats to cyber security. As everything is connected and intelligently handled, the importance of data has been thrown into sharper focus. Every company has invested heavily in protecting important data in the enterprise resources to encrypt key data, control access, and build security information and event management solutions to detect signs of an attack However, the advanced persistent threats (APT) attack, which can bypass security devices, hides malicious code in the system and steals information in a covert and continuous

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

manner, causing serious damage. APT attacks are one of the biggest challenges to conventional cyber security technology. this study constructed security threat ontology by analyzing and modeling the context information of a real APT attack, which is difficult to develop with security technology, and further designed reasoning rules based on inter-class relationships. The reasoning rules divide an APT attack into steps such as reconnaissance, attack using virus, acquisition of backdoor, action to achieve goal, acquisition of data after goal achievement, and finally, erasing traces of intrusion. Thus, to detect an anomaly in the context of an APT attack using the process of the APT attack, reasoning rules were designed by using Semantic Web Rule Language (SWRL) language for the context-aware reasoning of attack phase, penetration pahse, and collection phase based on the context information before and after the APT attack. Based on the SWRL language defined after designing the reasoning rules, the detection reasoning results for an APT attack context could be derived using the stepwise defined and designed rules. Future studies will continue to develop monitoring and context-aware control service systems with advanced functions to enable the integrated detection and control of various security threats using the application of various rules and the mapping of conventional designed ontologies via the modification and addition of rules.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Ⅰ. 서론

A. 연구 배경 및 목적

4차 산업혁명 시대의 도래와 더불어 우리의 삶은 점점 더 빠르게 변화하고 있다. 사물인터넷, 클라우드, 빅데이터, 머신러닝, 모바일 기술, 인공지능 등을 기반으로 모든 것들이 연결되고 지능적으로 처리되면서 고도의 개인 맞춤형 서비스가 가능해지고 산업의 생산성이 비약적으로 향상되는 시대를 맞이하고 있다. 그러나 이러한 환경 변화는 사이버 보안 측면에서는 더 큰 위협으로 작용하고 있다.

최근 데이터의 중요성이 부각되면서 각 기업들은 기업의 중요한 데이터를 보호하기 위하여 많은 비용을 투자하여 주요 데이터를 암호화하고, 접근을 제어하며, 공격 징후를 탐지하기 보안 정보 및 이벤트 관리 솔루션 Security Information and Event Management (SIEM)을 구현하는 등 많은 보안 대책을 세우고 있다[1]. 하지만 특정 국가, 기관 또는 단체를 표적으로 삼아 오랜 시간에 걸쳐 보안 장비들을 우회하며 시스템에 악성코드 자신을 숨기고 은밀하고 지속적으로 정보를 빼돌리는 형태의 공격으로 막대한 피해를 주고 있는 지능적 지속 위협 Advanced Persistent Threats (APT) 공격은 기존의 사이버 보안 기술로 대비하는데 한계가 있다. 국가 공공기관 및 금융기관 같은 특정 대상을 노린 공격, 혹은 사내에 직원의 작은 실수 하나가 원인 되어 벌어진 정보 유출 사고와 같은 사례를 보면, 기존의 백신 프로그램이 공격을 탐지하지 못하여 알려지지 않은 신종 악성코드의 감염으로 인해 큰 피해로 이어졌음을 알 수 있다[2]. APT 공격은 여러 보안장비와 함께 정보보호 관리 체계를 구축하며 운영하고 있더라도 조기에 식별 및 대응이 어려운 위협이라고 할 수 있다[3]. 최근 APT 공격 형태를 보면 공격 대상 목표에 따른 맞춤 맞춤화된 새로운 공격 툴을 생성할 수 있는 툴킷까지 제공되어 맞춤형 APT가 점점 증가하고 있는 상황이다. 따라서 기존의 침해지표기반분석대응 방식은 점점 더 진화되고 지능화 되어지는 APT 공격에 뒤처질 것이라고 전망하

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

고 있다[4][5].

본 논문에서는 여러 APT 공격의 전후 맥락 속의 상황 정보를 분석하고 모델링 하여 APT 공격 온톨로지를 구축하고, 이를 기반으로 APT 공격상황을 추론할 수 있는 추론규칙을 설계 및 적용하여 APT 공격 상황을 인지하는 방법을 제안하고자 한다.

B. 연구 내용 및 구성

본 연구의 주요 내용은 여러 APT 공격 전후 상황 정보들을 분석하여, APT 공격 온톨로지를 설계하며, 설계된 온톨로지를 기반으로 APT 공격 추론 규칙을 적용하여 APT 공격 상황인지 및 추론하는 방법을 제안한다. 본 논문의 구성은 다음과 같다.

2장의 관련 연구에서는 상황인지와 상황 정보를 모델링하기 위한 지식표현의 체계인 온톨로지에 대한 정의와 추론규칙을 도입한 기존의 연구에 대하여 살펴본다.

3장에서는 본 논문에서 제안하는 APT 공격 추론을 위한 온톨로지 기반의 상황인식 모델 구축을 위해 여러 APT 공격들의 데이터를 수집하고, 분석을 통한 온톨로지 설계에 관하여 기술한다.

4장에서는 실험환경 및 추론 규칙 설계와 그 추론을 이용하여 테스트 실험을 이용하여 추론식을 확인하며, 마지막으로 5장에서는 결론과 향후 연구에 대하여 서술하며 본 논문을 마무리한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Ⅱ. 관련 연구

A. 상황인지

1. 상황인지

상황인지의 원론적인 개념은 “당신 주변에서 어떤 무언가가 진행되거나 발생하는 것을 인지하고 있느냐”가 상황인지의 원론적인 개념이다. 상황인지 기술이란 개개의 객체(이벤트, 사건)의 진위 여부를 판단하고 규명하기 그 개개의 객체들의 연관성과 전체적인 패턴들을 통하여 어떤 상황이 발생하고 있고, 무엇을 어떻게 해야 하는지를 알고자 함에서 출발하였다[6]. 상황인지 기술은 인문 · 사회과학에 있어서 과거부터 지금까지 연구되어온 학문 분야이며, 정보보안 관리에만 적용하거나 새로운 기술은 아니라고 할 수 있다. 상황인지의 단계는 3가지로 구성된다. (A) 식별(Perception), (B) 이해(Comprehension), (C) 예측(Projection)이 3가지로 구성된다.

(A) 식별(Perception) : 다수의 시스템에서 발생하는 이벤트를 수신/저장하는 단계로 발생한 이벤트의 시간과 종류와 시스템에 대한 정보를 갖고 있다. 이는 전체 상황을 인지하기 위한 준비 단계이다.

(B) 이해(Comprehension) : 이벤트들을 통합 및 혼합, 재배치, 연관성 분석 등을 수행하여 전체 상황을 표현할 수 있는 단계를 의미한다. 이때 피해 시스템, 취약 시스템, 도메인의 피해 정도를 직관적으로 표현한다.

(C) 예측(Projection) : 현재의 상황에서 피해 정도 또는 취약 정도를 기반으로 대응 행동을 결정하도록 돕는 단계이다. 현재 발생하고 있는 비정상적인 상황, 또는 취약성이 노출된 설계 상황을 토대로 공격대상이 될 수 있는 시스템을 파악하고 피해 가능성을 분석함과 동시에 취약성 보안 방안을 결정하도록 도와줄 수 있는 자료를 생성한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

상황인지는 시스템 중심의 상황 인지가 있다. 시스템 중심의 상황인지는 시스템의 기능 또는 시스템의 상태를 파악하여 이에 알맞게 시스템이 어떻게 수행하는지를 제시하는 것을 의미한다. 시스템이 정의된 기능만을 수행하려 하는지 지속적으로 확인하고 그에 알맞은 규칙에 의거하여 예외적인 기능을 시도하려 할 때 이를 인지하고 오류 사항을 보고하는 과정으로 상황인지가 잘 작동되고 있는가를 알 수 있다. 이 과정을 위해서 에이전트가 요구되는데 이는 시스템 자체가 정상적인 기능을 수행하지 못할 것을 대비하여 이원화된 상황인지 시스템으로 주요 정보를 전달하는 기능을 수행한다. 하지만 이러한 시스템 중심의 상황인지는 기존 범위가 아닌 예외 범위에 대한 기준 정의에 의거한 상태 판단이 모호해질 수 있는 단점이 있다. 이를 해결하기 위해 표준화된 보안기법을 기반으로 하여 시스템 허용범위를 명확히 정의하여야 한다. 또한, 에이전트가 정의되지 않은 상태의 문제를 허용할 경우 발생할 수 있는 문제를 해결하기 위한 방안으로 사용자가 시스템을 빠르고 지속적으로 조작과 관찰을 할 수 있고 사용자의 행동에 따른 피드백이 즉각적으로 발생하는 인터랙션 스타일인 Direct manipulation과 사용자가 심도 있게 디자인된 조작 인터페이스를 통해 만들어진 세부적인 명령을 통하여 기기를 조작하는 방식인 Command-Based 방식을 적용하여 관리자의 직접 명령 하달 방식을 융합한 시스템을 적용함으로써 보다 안전한 시스템 검증 및 관리를 할 수 있다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

B. 온톨로지 기반 상황인지 모델

온톨로지(Ontology)의 어원은 '존재론'이라 하며 원래 사물의 존재 의미를 논의하는 철학적인 연구 영역을 뜻하는 말이다. 이 존재론은 "이 세계에는 어떤 종류의 존재자들(물리적, 현상적, 개념적, 추상적, 감성적)이 존재하는가, 그들의 본질은 무엇인가, 그들 존재자들 사이에는 어떤 관계가 있는가"를 다루는 분야이다. 온톨로지는 '실제'라는 의미의 그리스어 'Onto'와 학문 또는 강연 등의 의미를 갖는 'logia'의 합성어로부터 유래되었다. 온톨로지는 사람들이 세상에 대하여 보고 듣고 느끼고 생각하는 것에 대하여 서로 간의 토론을 통하여 합의를 이룬 바를, 개념적이고 컴퓨터에서 다룰 수 있는 형태로 표현한 모델이다. 또한 어떤 관심 분야를 개념화하기 위해 명시적으로 정형화한 명세서(An Explicit and Formal Specification of a Conceptualization of a Domain of Interest) 이다[7]. 온톨로지 기반 상황인지에서 온톨로지는 앞에서 설명한 것처럼 어떤 관심 분야를 개념화하기 위해 명세서를 작성하는 작업이다. 특정 분야의 데이터를 모델을 기술하고 지식정보를 합의된 개념을 설계하여 개념과 개념 간의 관계를 기술한다. 온톨로지를 구축하고 추론하여 어떤 한 일이 존재하거나 발생하는 상황 관계를 조건으로 정의하여 기술적 관점에서 특성을 나열하여 관계를 정립한다면 상황을 사용자들에게 인지시켜 줄 수 있다. 하지만 이런 상황을 사용자들에게 인지시켜주기 위해서는 많은 데이터가 필요하며 데이터는 인간에 의해 입력되거나 센서의 값을 통해서 입력한다[8]. 온톨로지 기반의 상황인지는 보안 분야뿐만 아니라 서비스, 의료, 산업에 이르기까지 여러 분야에서 많은 연구가 이루어져 왔다. 서비스 분야의 온톨로지 기반 상황인지는 스마트폰의 위치기반서비스를 이용하여 움직임, 교통상황, 날씨, 시간, 개인정보 선호 등과 같은 정보를 이용하여 온톨로지를 구축 후 사용자 프로파일 온톨로지, 스케쥴 온톨로지, 과업 온톨로지를 구축하여 이를 기반으로 어플리케이션 제작을 통하여 사용자의 선호도 움직임에 따른 서비스 추천을 하고 있다. 또한, 자동차 블랙박스는 실시간 이벤트에 대해서 영상을 처리하여 메모리의 부족함이 있었다. 블랙박스의 충격이 발생하였을 때 기존에 저장되어있던 임계 값과 비교하여 현재 충격이 데이터

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

가 임계 값을 초과할 경우, 이벤트 발생과 함께 영상 정보를 메모리에 저장하여 다수의 영상정보를 저장하는 문제점을 해결하기 위해 가중치를 매겨 낮은 가중치를 가지는 데이터를 우선 삭제할 수 있는 온톨로지 기반의 상황인지 알고리즘도 있었다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

C. APT 공격 개념과 기존 연구

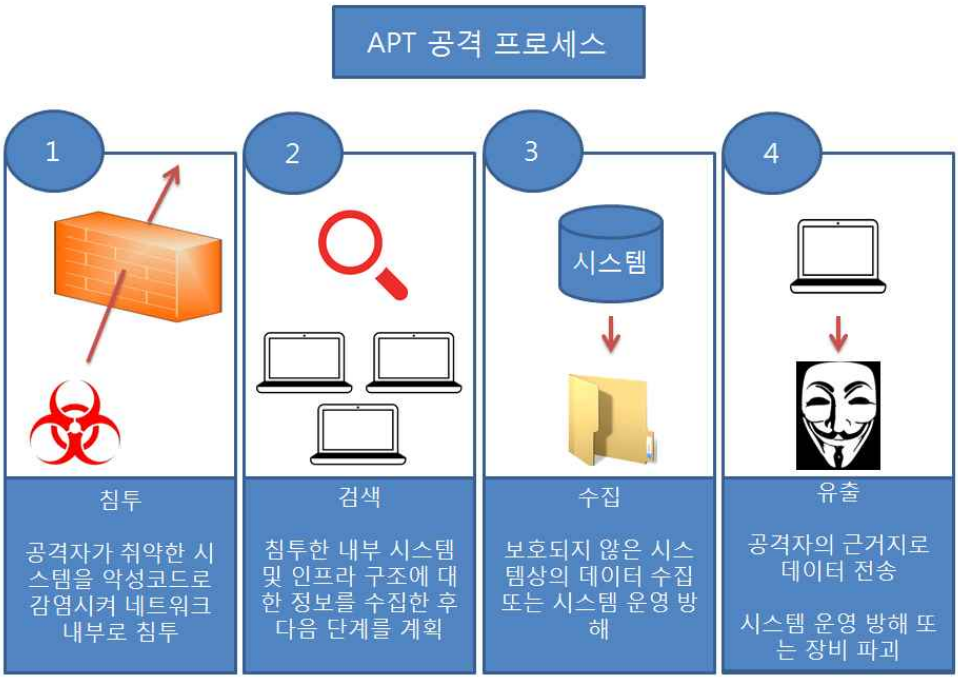
1. APT 공격 개념

APT 공격은 전문지식과 많은 자원을 가진 공격자가 여러 다른 공격 경로를 통하여 사용자 컴퓨터에 대한 목적을 달성시키는 공격을 말한다. APT 공격은 공격에 대한 전문적인 지식을 가지고 있음과 동시에 많은 자원을 가지고 있고 이를 이용하여 여러 다른 공격 경로를 통하여 목표 상대방에게 목적을 달성하는 공격이다. 여기서 말하는 목적은 중요정보를 탈취하기 위하여 지속적으로 조직의 정보기술 인프라 내부에 기반을 마련하거나 확장을 하며, 공격 목표 대상의 임무나 계획 또는 조직 자체를 약화시키거나 방해한다. APT 공격은 방어자가 방어하려고 시스템을 구축해놓으면 이에 대응하여 공격자의 목적을 실행하기 위하여 방어 시스템과 상호작용을 유지하면서 오랜 기간 동안 반복적으로 목적을 달성하기 위하여 공격을 시도한다[9]. APT 공격은 2010년 중국발 구글 해킹 사고에서부터 APT라는 용어가 빈번하게 사용되기 시작하였다. APT 공격의 프로세스 단계는 4단계로 이루어져 있다. 1단계 침투 단계에서는 타깃으로 하는 조직 내부로 침투하는 단계이다. 해커들은 사전에 사회 공학적 기법을 이용하여 해당 조직이나 특정 개인에 대해 정보를 파악하며, 연구 조사를 한다. 이런 연구 조사를 바탕으로 해커들은 페이스북이나 소셜 네트워크 사이트를 통하여 특정 개인에 대한 정보를 수집하여 맞춤형 공격을 실행한다. 2단계는 검색 단계이다. 검색 단계에서는 정보 검색을 통하여 공격 환경에 대한 전반적인 프로파일링을 통해 민감한 정보가 어디에 있는지 먼저 파악할 수 있다. 이를 통하여 해커들은 어떤 정보를 탈취할 것인지 계획을 세운다. 3단계는 정보 수집 단계로 보호되지 않은 시스템 주요 저장데이터는 공격자에게 노출되게 된다. 이 단계에서 APT 공격은 조직 내 데이터와 명령어 수집을 통하여 표적 시스템이나 접속 포인트에 정보를 탈취할 수 있는 악성코드를 감염시킨다. 마지막으로 4단계에서 APT 공격 공격자들은 표적 시스템에 제어권을 장악한다. 이를 통하여 APT 공격자들은 표적 시스템 안에 있는 정보를 유출시킬 뿐만 아니라 시스템까지 손상시킨

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

다. [그림 2-1]은 APT 공격 프로세스를 나타낸다.



[그림 2-1] APT 공격 프로세스

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2. APT 공격 기존 연구

APT 공격은 주요 사례연구, 공격 탐지 연구, 대응 기술 연구 등 많은 연구가 진행되어 왔다. 이문구외 1 명은 APT 공격의 주요 사례에 관하여 연구를 진행하였다. APT 공격의 해외 피해사례를 보자면 1999년에 미국 국방부와 항공우주국 해킹사고와 2010년 이란의 원자력 발전소 사고 등 여러 사례가 있었다. 1999년 미국 국방부, 항공우주국의 사고 사례를 보면 국가기밀 핵무기 정보, 군사 시설 지도, 병력 구성 등 한 나라에서 특급 기밀정보로 판단되는 정보를 유출 시키는 사고였다. 실제 인지 한 것은 1999년 이지만 첫 공격은 1998년부터 1년 동안 지속되어 왔다는 걸 알 수 있었다. 2010년 이란의 원자력 발전소 사고는 원자력 발전소가 일부 마비되는 사고였다. 핵발전시설의 주요 시설인 원심분리기가 출처불명의 악성코드에 의해 작동이 정지되었고 우라늄 원심분리기 약 1,000여대가 APT 공격에 의해 작동불능 상태에 빠졌다. 최초의 감염은 USB를 통하여 시작되었고, 내부 시스템을 장악하기 위해 4개의 제로데이 취약점(Zero Day Vulnerability)을 이용하여 복합적이고 지능적으로 공격을 진행 하였다. 또한, 내부의 백신정보를 스캔하고 자신을 은닉하거나 스스로 삭제하는 등 APT 공격의 주요 특징인 은밀함이 나타나는 공격이었다. 또한 이 공격은 2010년이 아닌 2009년부터 공격이 시작됐다는 게 밝혀졌다[10]. APT 공격의 사례를 연구하면 APT 공격의 주요 특징과 공격 기법 등을 알 수 있다. 이렇게 APT 공격의 사례뿐만 아니라 APT 공격 탐지에 대한 연구도 많이 진행 되어왔다. APT 공격은 알려지지 않은 다양한 공격기법을 활용하며 또한 보안솔루션을 우회하며, 장기간에 걸쳐 취약점을 조사하고 이에 맞는 공격으로 기존의 보안기술 및 제품으로 이를 찾아내고 대응에 대한 많은 어려움이 있었다[11]. APT 탐지는 APT 공격으로 인하여 시스템에 대한 원치 않는 조작을 탐지한다. 이에 대한 연구로 보안로그 연관분석을 통한 공격 탐지 연구가 있다. 보안로그 연관분석의 연구는 IT시스템에서 발생하는 로그들을 분석하기 위하여 로그간의 연관성(Correlatgion)을 분석함으로써 유사속성을 비교하고 이를 기반으로 유사도를 측정하여 필요한 이벤트를 미리 설정하여 탐지하는 시나리오 기반 접근방법이다[12, 13, 14]. 이렇게 보안 로그분석에서의 분석뿐만 아니라 빅 데이터 기반의 탐지기법도

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

있었다. 김도근 외 2명은 빅데이터 분석기술을 기반으로 APT 공격 대응 기술에 관한 방안 연구를 진행하였다. 빅 데이터는 2011년도 메켄지에서 인터넷 데이터의 증가가 전 세계에 미치는 영향에 대한 보고서를 빅 데이터라고 하였다. 빅데이터는 대용량 정보를 실시간 처리하는 기술이며 빅데이터 분석기술인 SIEMD을 구축하여 원본 로그자료 및 비정형 데이터 자체를 분석하여 APT공격을 탐지하는 연구가 진행되었다[15]. 많은 APT 공격의 탐지 방법이 있지만 점점 지능화 되고 또한 은밀함을 갖춘 APT 공격에는 탐지하는 게 매우 어렵다. 사례에서 보다시피 피해는 최근에 받았지만 실질적으로 공격은 그보다 1년 전이나 몇 개월 전에 일어난다는 것을 알 수 있었다. 이런 APT 공격에 특징에 맞춰 본 연구에서는 APT 공격의 특징과 사전 데이터들을 모아 실제로 내부 데이터가 유출되기 전 APT 공격 상황을 인식 할 수 있는 온톨로지 추론 모델을 제안한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Ⅲ. APT 공격 탐지를 위한 온톨로지 기반 상황인지 모델

A. 온톨로지 기반 상황인지 모델 필요성

상황인지기술이란 상황에 맞게 사용자에게 최적화된 기능을 도출함으로써 사용자의 요구를 사전에 예측 및 제시하는 소프트웨어 및 하드웨어 기술을 의미한다[16]. 본 연구에서의 상황인지는 기존의 상황인지와 차이점이 있다. 기존의 상황인지기술은 생활패턴/생체신호/주변 환경 등을 분석하여 상황에 맞게 사용자의 삶을 편안하게 해주지만 본 연구에서의 상황인지는 여러 보안 문서들을 취득하고 이를 이용하여 주요 정보를 추출 후 APT 공격자의 의도를 분석하여 사용자에게 APT 공격 상황을 인지시켜주는 연구를 진행하였다. APT 공격은 지능형 지속적 위협 공격이라고 한다. 이 공격은 특정 조직, 국가, 공공기관, 기업 및 개인에 이르기까지 다양한 목표로 하여 이제까지 알려지지 않거나 또는 기존에 사용해왔던 방식들을 다양하게 이용하여 공격하는 기법을 활용하여 공격자의 경제적 또는 정치적 목적을 달성할 때까지 장기간에 걸쳐서 지속적으로 정교한 공격을 하며 말한다.

[표 3-1] APT 공격의 특성

다양한 공격 방법	공격 경로	다양한 대상	기간	목적
Watering Hole, DDos, Zero-day attack, Key Logger, Spear-Phishing	웹사이트, 기업 홈페이지, 이메일, 메신저, P2P, SNS	학교, 은행, 기업, 기관, 국가, 언론사, 공공기관	수개월 ~ 수년	정치 경제 보복 염탐

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

APT 공격은 [표 3-1]과 같이 다양한 공격 방법과 여러 공격 경로를 가지고 있다. APT 공격의 이러한 공격 특성은 기존의 공격방법에 비해서 보다 정밀화 되었고 지능화된 공격방식을 가지고 있으며 해커들은 표적타깃에 대해 성공적으로 APT 공격을 수행하기 위해서 보다 더 정교하고 지능화된 기술을 이용한다. APT 공격의 효과적인 대응을 위해서는 APT 공격자보다 전략적이고 체계적으로 접근하는 것이 중요하다. 상황인지의 핵심기술인 온톨로지에 주목을 하는 이유는 온톨로지는 클래스와 관계들로 구성되어 있으며 일종의 사전으로서 그 안에는 특정 도메인에 관련된 단어들이 계층적으로 표현되어 있고 추가적으로 이를 확장할 수 있는 추론 규칙이 포함되어 있으며, 웹 기반에서 지식을 처리하거나 응용 프로그램 사이에 지식을 공유하고, 또 재사용이 가능하도록 설계되어 있고 [표 3-2]와 같은 이유로 본 실험에서는 APT 공격에 대한 상황을 인지할 수 있도록 보안 온톨로지를 모델링하였다[17].

[표 3-2] 상황인지 모델링 기술과 요구사항

모델/요구사항	분산 조합	표현되는 정보의 질	불명확한 정보 대처능력	표현의 정규도	응용 가능성
키값 기반 모델	X	△	△	△	O
마크 업 기반 모델	O	X	X	O	O
그래픽 기반 모델	△	O	X	O	O
객체지향 기반 모델	O	O	O	O	O
로직 기반 모델	O	X	X	O	△
온톨로지 기반 모델	O	O	O	O	O

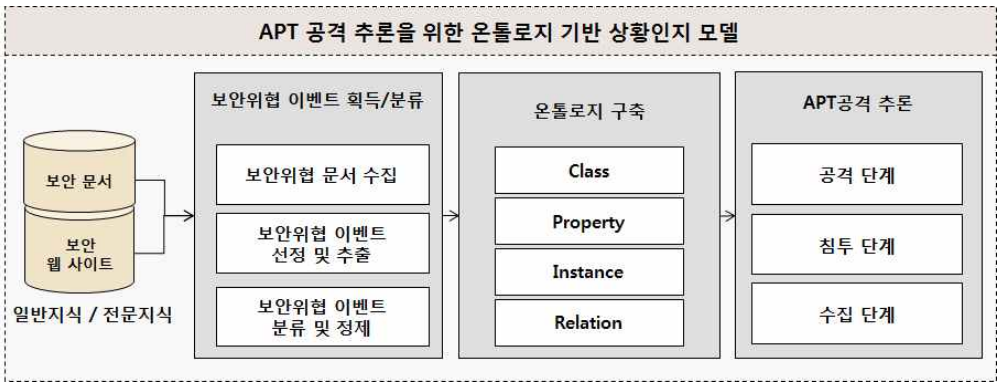
Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

B. 프레임 워크

온톨로지는 사람과 컴퓨터 사이에 정보 공유 및 재사용을 위한 시맨틱웹의 핵심으로써 컴퓨터가 정보의 의미를 이해하여 사람에게 제공할 수 있도록 데이터, 정보, 지식 등의 개념 간 관계를 표현한다.

본 논문에서는 보안 문서, 보안 웹 사이트 등 보안 관련 일반지식과 전문지식을 분석하여 APT 공격 단계별 상황 정보를 정형화 및 개념화하여, 보안 위협 온톨로지를 설계 및 구축함으로써 APT 공격 상황(단계)의 이해를 위한 도구로 사용하며, APT 공격 상황 정보 기반의 추론 규칙을 적용하여, APT 공격 상황 정보 간의 관계를 검증하고자 한다. [그림 3-2]는 APT 공격 추론을 위한 온톨로지 기반 상황인지 모델의 전체 구성도이다.



[그림 3-1] 온톨로지 모델링 및 상황인지 추론 프레임워크

정보 수집 단계에서는 보안 문서, 보안 사례, 보안 웹사이트 등에서 [그림 3-2]와 같이 여러 자료를 모아 본 연구에서 필요한 데이터들을 수집하였다. 본 연구에서 필요한 데이터는 온톨로지를 구축함에 있어 여러 공격 행위들과 공격이 어떻게 진행되는지 공격으로 인하여 어떤 피해를 입었는지에 대하여 중심적으로 데이터를 수집하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

정보 분류 단계에서는 정보 수집 단계에서 모은 데이터들을 온톨로지 모델링을 하기 위하여 공격 행위, 공격 방법, 공격에 대한 피해 정도, 공격으로 이용한 취약점 컴퓨터의 보안 점수, 보안 소프트웨어 업그레이드 상태, 공격 목적, 공격 목표, 공격당한 후 상태 등 데이터를 분류하였다.

위에 단계에서 여러 정보들을 취합하여 분류한 여러 데이터들을 이용하여 온톨로지의 모델링의 규칙에 맞게 온톨로지를 모델링 하였다. 온톨로지의 모델링 규칙은 첫 번째 단계에서 온톨로지의 도메인과 범위를 결정하여야 한다. 구축하고자 범위를 설정하여야 하며, 사용하고자 하는 목적, 제공하고자 하는 목적 또한 사용하는 사람이 누구인지 명확하게 결정하여야 온톨로지 구축을 할 수 있다. 본 실험에서는 사이버 공격 행위에 대하여 범위를 설정하였고 여러 사례들과 공격 행위에 관한 데이터들을 이용하여 도메인을 결정하였다. 두 번째 단계에서는 기존의 온톨로지 구축이 되어 있는지 확인하여 재사용 가능 여부를 고려하여 자원의 낭비를 막아야 한다. 본 실험에서는 기존에 사용되었던 보안 온톨로지를 이용하여 APT 공격 행위, 특성, 목표와 APT 공격 목적을 삽입하여 온톨로지를 재구축 하였다. 세 번째 단계에서는 주요 항목들을 열거하여 주요한 문장으로 나열함으로써 온톨로지에서 하고 싶은 것이 무엇인지, 여러 항목들이 가진 특성이 무엇인지, 어떤 행위나 행동, 서비스 등을 이야기하고 싶은 것인지를 리스트로 나열하여야 한다. 네 번째 단계에서는 온톨로지의 클래스와 계층 간의 관계를 정의하는 단계에다. 본 실험에서는 공격자의 클래스가 있으면 공격자가 몇 번의 공격을 시도하였는지와 어떠한 공격을 시도하였는지 등과 같은 클래스와 계층 간에 관계를 정의하였다. 마지막 단계로 클래스와 클래스 간의 인스턴스 생성을 하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

C. 온톨로지 설계 및 구축

1. APT 공격 온톨로지 - 클래스/계층 정의

이 단계에서는 클래스, 클래스의 계층, 클래스의 관계를 정의하였다. 보안위협에 대한 주요 객체를 클래스로 정의하고, 각 클래스의 계층 및 클래스 간의 관계를 정의함으로써 온톨로지를 설계하였다. 상위 클래스와 하위클래스는 Level로 표기하였으며 Level 1은 최상위 클래스를 가리키며 그 다음 Level은 하위클래스를 가리킨다. [표 3-3]은 Level 1의 클래스와 Level 2의 클래스의 정의를 보여준다.

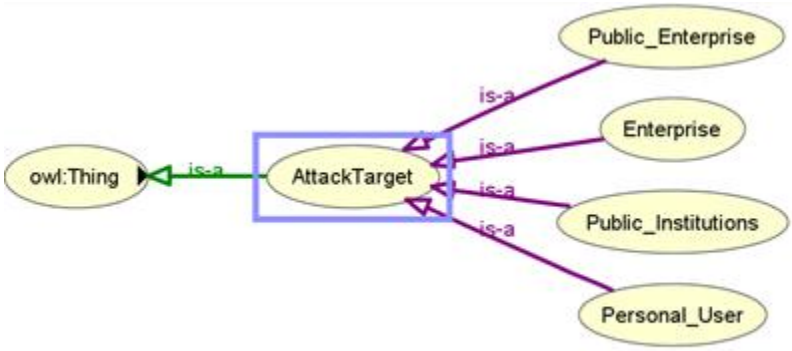
[표 3-3] Level 1 클래스와 Level 2 클래스정의

Class	Level	Class	Level
AttackTarget	1	Public_Enterprise	2
		Enterprise	
		Public_Institutions	
		Personal_User	
AttackPurpose	1	System_Control	2
		Server_Connect	
		Id/Password_Change	
		System_Penetration	
		Malware_Drop	
		System_Destruction	
		Information_Leakage	
AttackMethods	1	Means≡Behavior	2
		Consequence	

AttackTarget은 공격 목표물을 정의하며 Public_Enterprise, Enterprise, Public_Institutions, Personal_User의 하위 클래스를 가진다. AttackTarget과 하위 클래스들의 관계를 표현하면 [그림 3-2]와 같다.

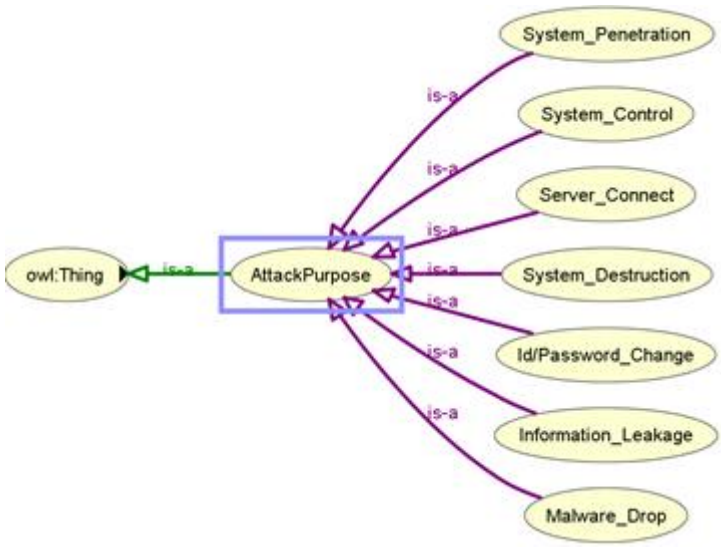
Collection @ chosun

조선대학교
CHOSUN UNIVERSITY



[그림 3-2] AttackTarget Level 1과 Lvel 2 관계

AttackPurpose는 공격에 대한 목적을 정의하며 System_Control, Server_Connect, Id/Password_Change, System_Penetration, Malware_Drop, System_Destruction, Information_Leakaged와 같은 하위클래스를 가진다. AttackPurpose와 하위 클래스들의 관계를 표현하면 [그림 3-3]과 같다.

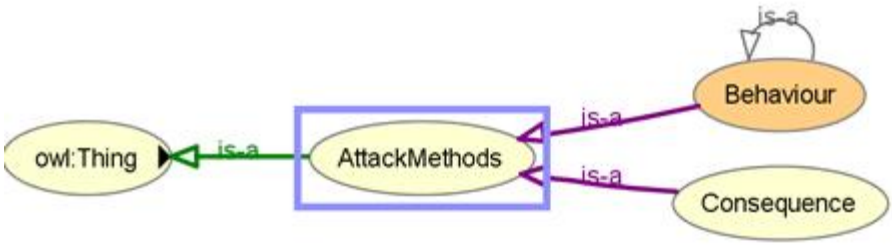


[그림 3-3] AttackPurpose Level 1과 Lvel 2 관계

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

AttackMethods는 공격의 방법에 대해서 정의하며 Means≡Behavior, Consequence의 하위 클래스를 가진다. AttackMethods와 하위 클래스들의 관계를 [그림 3-4]와 같다.



[그림 3-4] AttackMethods Level 1과 Lvel 2 관계

[표 3-4]는 Means≡Behavior의 2 Level의 클래스와 3 Level의 클래스의 정의를 보여준다.

[표 3-4] Means≡Behavior Level 2 클래스와 Level 3 클래스의 정의

Class	Level	Class	Level
Means≡Behavior	2	BufferOverFlow	3
		ConfigurationError	
		ExICMPEchoReq	
		ExIPPacketSize	
		InputValidationError	
		MaliciousCodeExecution	
		SocialEngineering	
		SynFlood	

Means≡Behavior는 공격에 대한 행위를 의미하며 BufferOverFlow, ConfigurationError, ExICMPEchoReq, ExIPPacketSize, InputValidationError, MaliciousCodeExecution, SocialEngineering, SynFlood의 하위클래스를 가진

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

다. [표 3-5]는 Means≡Behavior의 3 Level의 클래스와 4 Level의 클래스 정의를 보여준다.

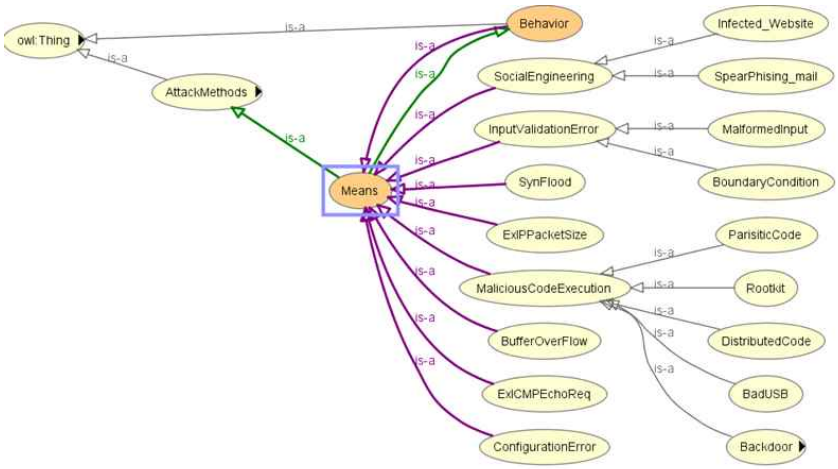
[표 3-5] Means≡Behavior의 Level 3 클래스와 Level 4 클래스 정의

Class	Level	Class	Level
InputValidationError	3	BoundaryCondition	4
		MalformedInput	
MaliciousCodeExecution	3	BadUSB	4
		DistributedCode	
		ParisiticCode	
		Rootkit	
SocialEngineering	3	Infected_Website	4
		SpearPhising_mail	

InputValidationError는 입력에 대한 유효성 검사 오류를 정의하며 BoundaryCondition, MalformedInput의 하위 클래스를 가진다. MaliciousCodeExecution는 악성코드를 삽입하는 공격을 정의하며 BadUSB, DistributedCode, ParisiticCode, Rootkit의 하위 클래스를 가진다. SocialEngineering은 사회공학 공격을 정의하며 Infected_Website, SpearPhising_mail의 하위 클래스를 가진다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY



[그림 3-5] Means≡Behavior 와 하위 클래스들의 관계

[표 3-6]은 Consequence의 2 Level의 클래스와 3 Level의 클래스의 정의를 보여준다.

[표 3-6] Consequence의 Level 2 클래스와 Level 3 클래스 정의

Class	Level	Class	Level
Consequence	2	Watering_Hole	3
		Backdoor	
		Infected_I/O_Device	
		BotnetAttack	
		Networktraffic_increase	
		DenialOfService	
		LossOfConf	
		LossOfIntegrity	
		RemoteAccess	
		SelfPropagatingCode	
		TriggeredCode	
		Trojans	

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Consequence는 Means≡Behavior에서 정의한 공격에 대한 결과를 의미하며 Watering_Hole, Backdoor, Infected_I/O_Device, BotnetAttack, Networktraffic_increase, DenialOfService, LossOfConf, RemoteAccess, SelfPropagatingCode, TriggeredCode, TriggeredCode, Trojans의 하위클래스를 가진다. [표 3-7]은 Consequence의 3 Level의 클래스와 4 Level의 클래스 정의를 보여준다.

[표 3-7] Consequence의 Level 3 클래스와 Level 4 클래스 정의

Class	Level	Class	Level
DenialOfService	3	ExcessForks	4
		MemoryConsumption	
		NetFlood	
		PingOfDeath	
		SysCrash	
LossOfConf	3	DirectoryExposure	4
LossOfIntegrity	3	DataCorruption	4
SelfPropagatingCode	3	Virus	4
		Worm	
TriggeredCode	3	Logic	4
Backdoor	3	ChangeSystem_Backdoor	
		False_Update	
		Local_Backdoor	
		Password_Cracking _Backdoor	
		Remote_Backdoor	

DenialOfService는 서비스 거부 공격을 정의하며 ExcessForks, MemoryConsumption, NetFlood, PingOfDeath, SysCrash의 하위 클래스를 가진다. LossOfConf는 파일의 손실 공격을 정의하며 DirectoryExposure의 하위 클래스를 가진다. LossOfIntegrity는 무결성 손실 공격을 정의하며 DataCorruption의 하위 클래스를 가진다. SelfPropagatingCode는 자체적으로 증식하는 악성코드 공격을 정의하며 Virus, Worm의 하위 클래스를 가진다. TriggeredCode는 코드를 변환시키는 공격을 정의하며 Logic의 하위 클래스를 가진다. Backdoor는 공격자가 시스템에 통로를 만드는 것을 의미하며

Collection @ chosun

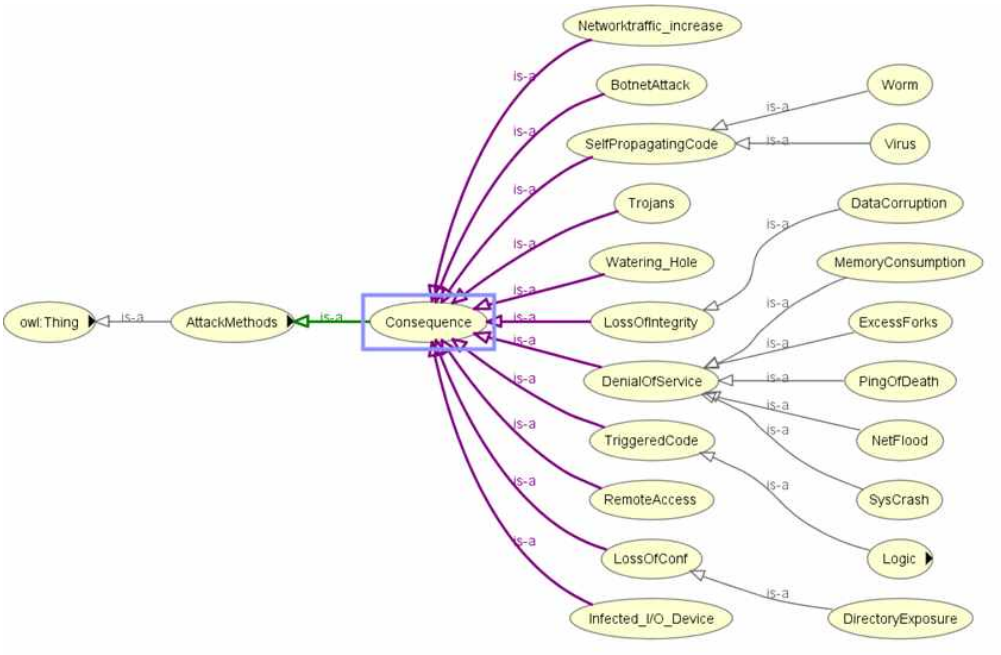
조선대학교
CHOSUN UNIVERSITY

ChangeSystem_Backdoor, False_Update, Local_Backdoor, Password_cracking_bBackdoor, Remote_Backdoor을 하위클래스로 가진다. Logic은 논리적 공격으로 정의하며 LogicExploit의 하위클래스를 가지며 LogicExploit는 AtError, ExceptionCondition, RaceCond ition, SerialError의 하위클래스를 가지며, [표 3-8]과 같이 정의하였다.

[표 3-8] LogicExploit와 하위 클래스 정의

Class	Level	Class	Level
LogicExploit	5	AtError	6
		ExceptionCondition	
		RaceCondition	
		SerialError	

Consequence와 하위 클래스 관계를 표현하면 [그림 3-6]과 같다.



[그림 3-6] Consequence 와 하위 클래스들의 관계

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2. APT 공격 온톨로지 - 속성 정의

앞 장에서는 APT 공격 온톨로지의 클래스와 계층에 관하여 정의를 하였으며, 본 장에서는 클래스 속성을 정의한다. [표 3-9]는 APT 공격 온톨로지 클래스의 Object Property의 정의이다.

[표 3-9] 보안위협 온톨로지 주요 Object Property의 정의

Property	Name	Type	Range
behavior	행위	ObjectTypeProperty	Means
isResultOf	결과에 대한 행위	ObjectTypeProperty	Consequence
resultsIn	행위에대한 결과	ObjectTypeProperty	Means
hasImpact	영향	ObjectTypeProperty	Means
hasIntendedEffect	의도한 효과	ObjectTypeProperty	Means
hasType	타입을 가진다	ObjectTypeProperty	Means
isPurpose	결과에 대한목적	ObjectTypeProperty	Attack PurPose

3. APT 공격 온톨로지 - 관계 정의

보안위협 온톨로지 속성 정의에서는 클래스와 계층간의 속성을 정의하였다. 관계 정의 단계에서는 속성 단계에서 정의한 Property를 가지고 클래스와 클래스간의 관계를 정의 해주었다. [그림 3-7]은 클래스와 클래스를 이어주는 속성을 이용하여 관계를 정의하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

[그림 3-7] Means, Consequence, Attackpurpose 클래스 관계 정의

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

D. 추론 규칙 설계

1. APT 탐지를 위한 추론 단계정의

추론 규칙 설계는 상황인지에서 매우 중요한 작업이다. APT 공격은 다양한 경로와 복합적인 공격방법을 사용하여 타겟에 대한 은밀한 공격을 진행한다. 이러한 이유로 공격방법과 경로 타켓을 모두 고려하여 추론 규칙을 설계하여야만 APT 공격에 대한 상황인지가 가능하다. 본 실험에서는 APT 공격 진행 과정을 인지하며 실험에 진행하였으며 APT 공격의 단계별로 진행 과정은 [표 3-10]과 같이 표현된다.

[표 3-10] APT 공격의 단계별 진행과정

1	2	3	4	5	6
정찰	Varous Attack	Back Door	Movement	Data Gathering	흔적 삭제
검색 사이트, Target 기업 홈페이지, SNS, Scanning …	Zero-day Attack, 외부 Update Server, E-mail, Messenger, USB, SNS …	Keylogger, 원격제어	취약점 공격, 서버 공격	서버 접근, 정보획득	악성 툴 자동 삭제, 악성 파일 삭제

APT 공격은 정찰에서부터 바이러스를 이용한 공격, 백도어 확보, 목적달성

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

을 위한 행동, 목적 달성 후 데이터 취득, 마지막으로 자신이 침입한 흔적을 지우는 단계로 나누어진다. 본 실험에서 추론 규칙 설계 단계에서는 APT 공격의 공격단계와 침투, 수집, 유출에 해당되는 상황을 고려하여 추론 규칙을 설계하였다. 정찰단계에서는 공격자가 검색사이트나 기업 홈페이지 등 여러 방법으로 공격할 대상을 찾는데 이때의 흔적은 공격당하는 당사자가 정해져 있지 않고 또한 정해져 있다 해도 공격자가 자기 자신을 공격대상으로 정한다는 행위를 감지하지 못하므로 정찰 단계는 추론 규칙에서 제외하였다. 또한, 흔적 삭제 단계에서는 공격자는 모든 공격을 끝내고 자신의 흔적을 지우는 단계이기 때문에 추론에서 제외하였다. 정찰 단계와 흔적 삭제 단계를 제외한 나머지 VirousAttack, Backdoor, Movement, Data Gathering 단계를 이용하였고 APT 공격상황에서 이상 상태를 감지하기 위하여 APT 공격의 전후 맥락 속의 상황 정보를 기반으로 공격단계(VirousAttack), 침투 단계(Backdoor, Movement), 수집 단계(Data Gathring)와 같이 단계별로 나누어서 추론 규칙을 설계하였다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2. 추론 규칙 설계

본 장에서는 APT 공격상황에서 이상 상태를 감지하기 위하여 APT 공격의 전후 맥락 속의 상황 정보를 기반으로 공격단계, 침투단계, 수집단계에 대한 상황인지 추론을 위한 SWRL 언어로 추론규칙을 설계하였다.

2.1 공격단계

공격단계는 공격자가 바이러스를 침투시키는 단계이다. 타켓을 지정하고 타겟에 대한 공격행위를 선택하며 그 행위에 대한 결과를 알 수 있으며 그 결과로 인해서 공격단계인지 확인이 가능하다. [표 3-11]은 공격단계에서의 추론규칙을 나타낸다.

[표 3-11] 공격단계 추론규칙

Result	Reasoning Rules
이메일 공격	(?T behaviour Spearphising_mail)∧(Spearphising resultIn RemoteAccess)∧(RemoteAccess resultIn System_Control) ⇒ (?T step VariousAttack)
웹 사이트 공격	(?T behaviour InfetedWebsite)∧(InfetedWebsite resultIn RemoteAccess)∧(RemoteAccess resultIn System_Control) ⇒ (?T step VariousAttack)

2.2 침투단계

침투단계에서는 Backdoor단계와 Movement 단계로 나누어진다. 공격 단계를 통해 바이러스가 침투되었으며 그 바이러스를 이용하여 직접적으로 시스템을 장악해나가는 단계다. 개인의 PC를 공격자는 장악하고 그 PC를 이용하여 공격자는 자신이 시스템을 Backdoor 단계인 계속 사용할 수 있도록 통로를 만들며 PC 제어를 한다. Movement 단계에서는 공격자가 개인의 PC를 가

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

지고 그 상위 타겟인 기업 서버로 들어가기 위한 공격을 시도하며 서버로 침투한다. [표 3-12]는 침투단계에서의 추론규칙을 나타낸다.

[표 3-12] 침투단계 추론규칙

Result	Reasoning Rules
네트워크 트레픽 증가	(?T behaviour RemoteAccess)∧(RemoteAccess resultIn System_Control)∧(System_Control resultIn Networktraffic_increase) ⇒ (?T step Backdoor)
서버 공격	(?T behaviour DenialOfService)∧(DenialOfService resultIn LossOfIntegrity)∧(LossOfIntegrity resultIn MaliciousCodeExecution) ⇒ (?T step Movement)

2.3 수집단계

수집단계에서는 Data Gathering 단계로 정의하였다. Data Gathering 단계에서는 공격자가 서버에 접근하고 마지막 목적을 실행하는 단계이다. 이 단계에서는 공격자가 기업의 기밀정보를 유출하거나 기업에 피해를 주기 위해 시스템을 파괴하는 단계이다. [표 3-13]은 수집단계에서의 추론규칙을 나타낸다.

[표 3-13] 수집단계 추론규칙

Result	Reasoning Rules
서버 접속 후 정보유출	(?T behaviour Server_Connect)∧(Server_Connect resultIn Information_Leakage) ⇒ (?T step Data Gathering)
서버 접속 후 시스템 파괴	(?T behaviour Server_Connect)∧(Server_Connect resultIn System_Destruction) ⇒ (?T step Data Gathering)

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

Ⅳ. 실험 및 결과

A. 상황 시나리오기반의 APT공격 탐지

1. 상황 시나리오 구성

[표 4-1]은 실제 일어난 APT 공격의 보안 사례를 기반으로 실제 상황에서 있을 수 있는 상황으로 시나리오를 구성하였다.

[표 4-1] 상황 시나리오 구성

시나리오
건실한 IT 회사를 다니던 ‘A’씨는 최근 몇 일간 이상한 상황을 겪었다. 같은 회사에 다니는 상사인 부장 ‘B’씨에게 중요 메일로 “연말 정산서 빠른 확인 바람.” 이라는 메일을 받아 확인하였고 메일 안에는 연말정산서.xlsx라는 파일이 있어 다운을 받아 파일을 열어 보았지만, 연말정산서 파일이 아니었다. 그 일을 겪고 그다음 날 ‘A’ 씨는 평소처럼 출근하였고 자신의 PC를 켜서 비밀번호를 쳤지만 사용하던 비밀번호로 자신의 컴퓨터에 접속하지 못하였다. 같은 날 ‘A’ 씨와 같은 회사에 다니는 ‘B’ 씨는 고객에 대한 정보를 입력하기 위해 회사 서버에 접속을 시도하였지만 서버에 대한 접속에 실패 하였다. ‘B’ 씨는 이상하게 생각하여 서버에 대한 네트워크 로그를 확인해본 결과 ICMP 프로토콜로 용량이 큰 패킷이 들어오면서 핑이 계속 찍히고 있었다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

2. 상황정보에 따른 온톨로지 기반 클래스 추출

[표 4-2]는 보안 상황 온톨로지를 이용하여 이상 상황 정보를 기반으로 상황 정보에 대하여 온톨로지에서의 클래스를 추출해 놓았다.

[표 4-2] 시나리오 상황정보 온톨로지 클래스 정의

상황정보	Class
부장 'B' 씨에게 메일을 받아 확인하였으며 내용과 다른 첨부파일이 있었다.	SpearPhising_mail
자신의 사용하던 비밀번호로 컴퓨터에 접속하지 못하였다.	Password_Cracking_Backdoor
서버 접속에 실패 하였다.	DenialOfService
ICMP 프로토콜로 용량이 큰 패킷이 들어오며 핑이 계속해서 찍힘.	ExIPPacketSize, PingOfDeath

[그림 4-1]은 이상 상황정보에서 정의된 클래스들이 온톨로지에서 어떤 관계로 이루어져있는지 SpearPhising_mail을 예시로 하여 표현하였다.

[그림 4-1] SpearPhising_mail의 클래스 관계

dCollection @ chosun

조선대학교
CHOSUN UNIVERSITY

3. 시나리오 기반 추론식을 이용한 APT공격 탐지

SWRL언어를 기반으로 각 단계별 정의된 설계된 규칙을 통하여 APT 공격 상황에 대한 탐지 추론식을 [표 4-3]과 같이 도출할 수 있었다.

[표 4-3] 이상상황 시나리오 기반 추론식

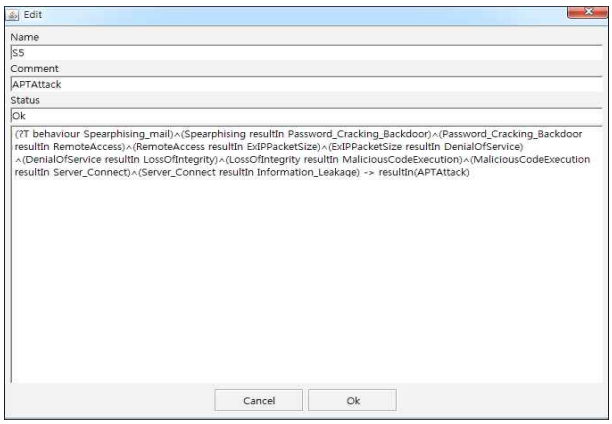
VariousAttack	(?T behaviour Spearphising_mail)∧(Spearphising resultIn Password_Cracking_Backdoor)∧(Password_Cracking_Backdoor resultIn RemoteAccess) ⇒ (?T step VariousAttack)
Backdoor	(?T behaviour RemoteAccess)∧(RemoteAccess resultIn ExIPPacketSize)∧(ExIPPacketSize resultIn DenialOfService) ⇒ (?T step Backdoor)
Movement	(?T behaviour DenialOfService)∧(DenialOfService resultIn LossOfIntegrity)∧(LossOfIntegrity resultIn MaliciousCodeExecution) ⇒ (?T step Movement)
Data Gathering	(?T behaviour MaliciousCodeExecution)∧(MaliciousCodeExecution resultIn Server_Connect)∧(Server_Connect resultIn Information_Leakage) ⇒ (?T step Data Gathering)
APT Attack	(?T behaviour VariousAttack)∧(?T behaviour Backdoor)∧(T behaviour Movement)∧(?T behaviour Data Gathering) ⇒ (?T behaviour APT Attack)

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

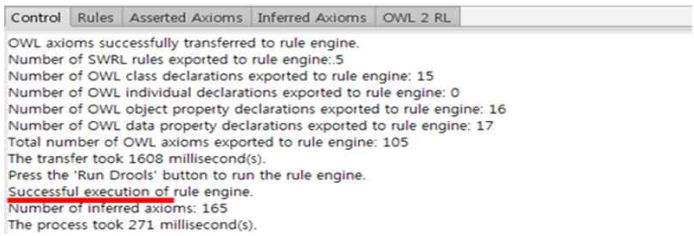
4. 추론엔진을 이용하여 평가

실제 Protege안에 있는 SWRL 추론엔진을 이용하여 추론식을 작성하여 실험을 진행하였다. APT 공격은 공격 특성상 여러 공격들이 복합적으로 구성되어 단계별로 진행되며, 이 여러 단계들이 모여 APT 공격이 진행되므로 추론식을 복합적으로 구성하여 단계별 진행 시켜 APT 공격을 탐지할 수 있는 식을 그림[4-2]와 같이 구성하였다.



[그림 4-2] SWRL을 이용한 추론식

실험 진행 결과 APT 공격 온톨로지 위에 SWRL기반 추론 엔진을 실행하여 온톨로지 기반 추론식이 실제 실행하는지를 확인하였으며, 그림[4-3]과 같이 추론식이 성공적으로 실행됨을 확인할 수 있었으며, 이를 이용하여 APT 공격행위가 보일 경우 추론식에 의해서 APT 공격을 탐지 할 수 있었다.



[그림 4-3] 추론규칙 실행 결과

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

V. 결론 및 제언

본 논문에서는 여러 APT 공격의 전후 맥락 속의 상황 정보를 분석하고 모델링하여 APT 공격 온톨로지를 구축하고, 이를 기반으로 APT 공격상황을 추론할 수 있는 추론규칙을 설계 및 적용하여 APT 공격 탐지 서비스를 적용하고 구현하는 것을 목적으로 하였다.

본 논문에서 제안하는 APT 공격 온톨로지 설계는 보안 위협 정보 모델링을 토대로 하여 이를 APT 공격 도메인에 적용한 것으로 OWL DL을 이용한 스키마 기반의 상황 모델링에 주안점을 두었다. 스키마를 이용한 추론을 바탕으로 한 모델 구조는 개별 상황들의 조합으로 정찰, 공격, Back door, Movement 등의 단계를 정의할 수 있다.

이를 위하여 본 논문에서는 APT 공격 탐지를 위해 필요한 요소 및 요소들의 관계를 정의하고 온톨로지를 통해 구축함으로써 의미적 접근법을 제안하였다. 이는 APT 공격 전후 환경에 대하여 지식 정보의 기초를 정의함으로써 추후 추가 및 수정, 확장을 위한 온톨로지 설계의 지표로 활용될 수 있다.

또한, 온톨로지 설계는 비슷한 도메인의 컨텐츠 매핑에서도 장점을 발휘한다. 동일한 의미를 갖는 용어에 대해서 서로 다른 어휘를 사용하는 문제를 해결하기 위해 각각 다른 도메인 온톨로지 상의 개념 간에 관계를 매핑하는 작업을 거쳐 필요·충분조건 등의 조건식을 거치면 각각 의미가 같은 어휘끼리 매치가 되어 매핑이 가능하다. 이는 기존에 구축된 온톨로지와 다른 온톨로지나 시소러스, 사전 등과 같은 다른 자원들에 의존하여 확장할 수가 있음을 나타낸다.

향후 연구 방향은 규칙의 수정 및 추가를 통하여 다양성을 갖춘 Rule 적용과 기존의 설계된 온톨로지의 매핑을 통하여 다양한 보안위협에 대해 통합적인 탐지 및 제어를 할 수 있도록 모니터링 및 상황인지 제어 서비스 시스템을 개발하여 기능의 고도화를 목표로 한다.

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

참고문헌

[1] 한은혜, 김인석, “효율적인 APT 대응 시스템 운영 모델”, 정보보호학회논문지, 제 27권, 제 3호, pp. 501-518, 2017

[2] 박형수, 김휘강, 김은진, “사례기반추론기법을 적용한 해킹메일 프로파일링”, 한국정보보호학회논문지, 제 25권, 제1호, pp. 107-122, 2015

[3] Sung-Baek HAN, Sung-Kwon Hong, "Measures against the APT attack in the financial sector“, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 1, pp. 44-53, 2013

[4] Kaspersky Security Bulletin. Predictions for 2017 “Indicators of Compromise are dead” By Juan

[5] Andrés Guerrero-Saade, GReAT, Costin Raiu on November 16, 2016

[6] 장범환, 나중찬, 장종수, “보안 이벤트 시각화를 이용한 보안 상황 인지기술”, 한국정보보호학회지, 제 16권, 제2호, pp. 18-25, 2006

[7] Knowledge Systems Laboratory, A Translation Approach to Portable Ontology Specifications, KSL-9271, 1993

[8] 이승철, 김치수, 임재현, “의도추론의 모허성 해결을 위한 온톨로지 기반 상황해석 구조의 설계 및 구현”, 한국컴퓨터종합학술대회 논문집, 제 34권, 제 1호, pp. 208-213, 2007

[9] 문대성, 이한성, 김익균, “APT 공격 탐지를 위한 호스트 기반 특징 표현 방법”, 한국정보보호학회, 제 24권, 제 5호, 2014

[10] 이문구, 배춘석, “APT 공격의 주요사례에 대한 연구”, 2013년 대한전자공학회 추계학술대회 논문집, pp. 939-942, 2013.

[11] 손경호, 이태진, 원동호, “트래픽 분석을 통한 악성코드 감염PC 및 APT 공격탐지 방안”, 정보보호학회논문지, 제 24권, 제 3호, pp. 491-298, 2014

[12] S. Cheung, U. Lindqvist, M.W. Fong, “Modeling multistep cyber attack for scenario recognition”, DARPA Information Survivability Conference and Exposition, pp. 284-292, 2003

Collection @ chosun

조선대학교
CHOSUN UNIVERSITY

[13] H. Debar, A. Wespi, “Aggregation and correlation of intrusion detection alerts”, Proceedings of the International Symposium on Recent Advances in Intrusion Detection, pp. 85-103, 2001

[14] B. Morin, L. Me, H. Debar, M. Ducasse, “M2D2: A formal data model for IDS alert correlation”, Proc. Recent Advances in Intrusion Detection, pp. 115-137,k 2002

[15] 김도근, 표성빈, 김창희, “빅데이터 분석기술을 기반으로 하는 APT공격 대응 기술에 관한 방안 연구”, 융복합지식학회논문지, 제 4권, 제 1호, pp. 29-34, 2016

[16] 김정기, 박승민, 장재우, “상황인식(Context-Awareness) 처리 기술”, 정보처리학회지, 제 10권, 제 4호, pp 182-188, 2003

[17] S. Chan and Q. Jin, “Enhancing Ontology-based Context Modeling with Temporal Vector Space for Ubiquitous Intelligence.”, In 20th Int'l Conf. on Advanced Information Networking and Applications, pp. 669 - 674, Apr 2006.

Collection @ chosun