ISSN 2383-630X(Print) / ISSN 2383-6296(Online)
Journal of KIISE, Vol. 48, No. 9, pp. 1014-1026, 2021. 9
https://doi.org/10.5626/JOK.2021.48.9.1014

APT 공격 사례 기반 보안 요구사항 추천 프레임워크

(A Security Requirements Recommendation Framework Based on APT Attack Cases)

김 민 주 † 박 신 혜 †† 이 석 원 †††
(MinJu Kim) (Sihn-Hye Park) (Seok-Won Lee)

요 약 지능형 지속 위협(APT, Advanced Persistent Threat) 공격은 특정 대상에 지능적이며 지속적으로 공격을 가하는 기법이다. 분명한 공격 목적을 가지고, 공격 대상에 조직적이고 고도화된 기술을 사용하며, 특정 기간 동안 탐지되지 않고 지속적으로 공격을 시도하므로 탐지와 방어가 어려운 공격 중 하나이다. 본 논문은 APT 공격에 대한 선제적 방어 방법으로 실제 발생한 APT 공격에 대한 보안 요구사항을 추천하는 프레임워크를 제안한다. 제안하는 프레임워크는 특정 APT 공격에 대하여 시나리오를 기반으로 공격 요소를 도출하고 요소 간 관계를 분석한다. 분석 결과에 대한 사례 기반 추론을 통해 공격 패턴을 추론하고, 보안 요구사항을 추천한다. 사례 기반 추론과 보안 요구사항 추천을 위해 APT 공격 지식, 일반 보안 지식, 도메인 특화 지식을 포함하는 통합 지식 베이스를 구축하였다. 통합 지식 베이스는 지식별 온톨로지와 관련 데이터베이스로 구성된다. 본 프레임워크를 웹 어플리케이션으로 구현하여 특정 APT 공격에 대해 사례 연구를 수행하였다.

키워드: 지능형 지속 공격, 사례 기반 추론, 보안 요구사항, 문제 도메인 온톨로지

Abstract Advanced Persistent Threat (APT) attacks are intelligent and continuous attacks on specific targets. This type of attack is one of the most difficult attacks to detect and defend because it uses an organized and advanced technique for attacking targets, and it continuously attempts to attack the undetected for a certain period. In this paper, we propose a framework that recommends security requirements for real-world APT attacks as a proactive defense against APT attacks. The proposed framework derives attack elements based on scenarios for specific APT attacks and analyzes the relationships between elements. Through case-based reasoning of analytical results, attack patterns are deduced, and security requirements are recommended. For case-based reasoning and security requirements recommendation, we build an integrated knowledge base that includes APT attack knowledge, general security knowledge, and domain-specific knowledge. The integrated knowledge base consists of knowledge-specific ontology and related databases. We implement this framework as a web application to conduct case studies on specific APT attacks.

Keywords: advanced persistent threat, case-based reasoning, security requirements, problem domain ontology

· This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (NRF-2020R1F1A1075605).
· This work was supported by the BK21 FOUR program of the National Research Foundation of Korea funded by the Ministry of Education (NRF5199991014091)

† 정 회 원 : 아주대학교 컴퓨터공학과 학생
alswn0707@ajou.ac.kr
†† 정 회 원 : 아주대학교 인공지능학과 연구원
sinne@ajou.ac.kr
††† 종신회원 : 아주대학교 인공지능학과, 소프트웨어학과 교수
(Ajou Univ.)
leesw@ajou.ac.kr
(Corresponding author임)

논문접수 : 2021년 2월 17일
(Received 17 February 2021)
논문수정 : 2021년 6월 16일
(Revised 16 June 2021)
심사완료 : 2021년 7월 6일
(Accepted 6 July 2021)

정보과학회논문지 제48권 제9호(2021. 9)

1. 서 론

네트워크와 인터넷이 발전하면서 보안 사건 사고가 끊임없이 발생하고 있다. 정부 기관 및 기업은 보안 위협에 대응하기 위해 정보 보호에 많은 노력과 비용을 투자한다[1]. 그러나 보안 위협 또한 보안 대책을 우회하거나 방해하기 위해 지능적으로 진화하고, 지속적으로 시도되고 있다. 지능형 지속 위협(APT, Advanced Persistent Threat) 공격은 대표적인 사이버 보안 위협으로, 특정 대상에 지능적이며 지속적으로 공격을 가하는 기법이다[2,3]. 분명한 공격 목적을 가지고, 공격 대상에 조직적이고 고도화된 기술을 사용하며, 특정 기간 동안 탐지되지 않고 지속적으로 공격을 시도하여 탐지와 방어가 모두 어렵다. 또한 영향을 미치는 범위도 해당 조직만 아니라 공급망 내 조직까지 광범위하며 피해액도 막대하다[4-7].

본 논문은 이러한 APT 공격에 선제적으로 대응하기 위한 방법으로 APT 공격 사례로부터 보안 요구사항을 추천하는 프레임워크를 제안한다. 제안하는 프레임워크는 APT 사례 기반의 통합 지식 베이스와 APT 공격 패턴 추론 및 보안 요구사항 추천 과정을 포함한다. APT 공격은 시나리오 기반으로 분석되고, 공격 요소와 요소 간 관계에 대한 사례 기반 추론을 통해 APT 공격 패턴으로 추론된다. 통합 지식 베이스에서 제공하는 지식으로 기반으로 보안 요구사항 추천 프로세스를 통해 해당 APT 공격 패턴에 대한 보안 요구사항이 추천된다. 통합 지식 베이스는 APT 공격 사례와 도메인 정보를 가지고 있는 데이터베이스와 문제 도메인 온톨로지로 구성된다. 문제 도메인 온톨로지는 APT 공격 지식, 일반 보안 지식, 도메인 특화 지식으로 생성된다. 추천된 보안 요구사항은 분석된 APT 공격 요소 및 도메인 지식 내 인적, 비즈니스적 요소 등을 반영한다. 본 논문 2장에서는 관련 연구로서 APT 공격의 단계 모델과 보안 온톨로지 및 보안 요구사항에 대해 서술한다. 3장은 제안하는 APT 공격 사례 기반 보안 요구사항 추천 프레임워크, 4장은 사례 연구를 위한 웹 어플리케이션 구현, 5장은 사례 연구, 6장 결론을 서술한다.

2. 관련 연구

2.1 APT 공격 단계 모델

APT 공격 분석 방법에 대한 연구 중 하나로 APT 공격 생애 주기에 따른 단계 모델이 제안되었다. Chen et al.[2]은 APT 공격을 행동 목적에 따라 정찰 및 무기화(Reconnaissance and Weaponization), 전달(Delivery), 초기 침입(Initial Intrusion), 명령 및 제어(Command and Control), 내부 침입(Lateral Movement), 데이터 압축(Data Exfiltration) 6 단계로 구분하고, 4 가지 공격 사례를 단계 모델에 적용하여 단계 별 공격 방법과 대응을 정의하였다. LogRhythm[8]은 데이터 흐름과 로그 흔적을 통해 공격자 행동을 분석하여 APT 공격을 정찰(Reconnaissance), 손상(Compromise), 유지 보수 접근(Maintain Access), 내부 침입(Lateral Movement), 데이터 압축(Data Exfiltration) 5단계로 분류하였다. 공격 행동을 통한 APT 단계 모델은 행동 특성, 행동 분석 방법 등 구분 기준에 따라 모델이 만들어진다. APT 공격은 공격자, 공격 대상에 따라 공격 패턴이 다양하므로 공격 행동으로 APT 공격 모델을 제시하기 어렵다. Messaoud et al.[9]은 공격 목표를 단계 별로 나눈 모델을 제안하였다. 이 모델은 APT 공격 단계 별 사용되는 기법에 대한 보안 대응을 결정할 수는 있지만 APT 공격에 대한 종합적인 정보 보안 대책을 제안하기 어렵다. Li et al.[10]은 89개 APT 공격 사례를 분석하여 APT 공격 생애 주기 모델을 제안하고 단계 별 공격 기법을 분류하였다. Bere et al.[11]은 8개 APT 공격 사례를 단계 모델을 통해 공격 대상, 초기 침입 방식, 공격 목적, 고의성을 분석하였다. Ussath et al.[12]은 22개 APT 공격 사례를 분석하여 APT 공격 특성 별 방어 및 탐지 방법을 제안하였다. 이와 같은 사례 기반 분석 방법은 단계 별 사용 도구나 기법에 집중했기 때문에 공격 흐름에 대한 종합적이고 체계적인 이해를 통한 보안 대응 결정 또는 다음 행동 유추에 어려움이 있다. 이를 위해 공격 행동 간 연관 관계를 정의하고 공격 패턴을 분석할 수 있다.

제안한 APT 공격 사례 기반 보안 요구사항 추천 프레임워크는 시나리오 기반 분석을 통해 공격 행동, 공격 목표, 생애 주기에 따른 단계 별 기법 등 다양한 APT 공격 특성을 반영하는 공격 요소와 공격 요소들 관계를 도출함으로써 이에 대한 종합적인 보안 대응을 할 수 있다.

2.2 보안 온톨로지와 보안 요구사항

시스템 개발 초기 단계부터 보안 요구사항을 도출하고 적용하면 운영 시 사이버 공격에 대한 피해를 최소화할 수 있다. Moffett el al.[13]은 보안 요구사항을 도출하는 프레임워크를 제안하고 사례 연구를 통해 보안 요구사항을 도출하는 과정을 보여주었으나, APT 공격과 같은 복잡한 공격에 대한 적용이 어렵고 인적 요소 등 공격에 사용되는 다양한 요소를 반영함에 있어 제한이 있을 수 있다. Elahi et al.[14]은 시스템 개발 과정 중 취약점 관련 경험 지식을 통합하기 위한 취약점 중심 모델링 온톨로지, 특히 취약점과 취약점이 시스템에 미치는 영향을 모델링하고 분석하는 방법을 제안하였다. 이 방법은 온톨로지를 통해 경험적 보안 지식을 효율적

으로 통합하고 활용하고자 하는 시도로 취약점에 집중되어 있다. Salini et al.[15]은 요구공학 단계에서 보안 요구사항을 도출하고 분석하기 위해 보안 요구사항 온톨로지를 통해 보안 요구사항을 재사용하는 온톨로지 기반 보안 요구공학 프레임워크를 제안하였다. 이 프레임워크는 보안 요구공학 지식을 명세 및 기술하고 구체화할 수 있는 온톨로지의 이점을 최대한 활용하였으나 이를 지원하는 효율적이고 체계적인 온톨로지를 구축하는데 어려움이 있다.

보안 요구사항을 정의하기 위한 다양한 요소와 관련 지식을 체계적으로 관리하고 활용하기 위해 온톨로지 지식 베이스를 구축하고 이를 활용하는 방법이 제안되었다. Lee et al.[16]은 보안 요구사항을 정의하기 위해 필요한 지식을 온톨로지 지식베이스를 통해 체계적으로 관리하고 활용하는 방법에 관한 연구로서 미 국방성 정보시스템 인증 및 증명 프로세스(DITSCAP, Department of Defense Information Technology Security Certification and Accreditation Process)를 기반으로 문제 도메인 온톨로지(PDO, Problem Domain Ontology)를 구축하고 보안 요구사항을 추천하는 방법을 제안하였다. 이는 특정 영역이나 세계를 개념과 개념과의 관계로 표현한 온톨로지를 보안 요구사항 추천에 이용하면 관련 지식을 정형화되고 명시적인 언어로 표현할 수 있으며, 표현된 지식을 재사용하고 공유할 수 있다는 장점이 있다. Kim et al.[17,18]은 문제 도메인 온톨로지를 통해 목적 기반 위험을 산정하고 보안 요구사항을 추천하는 3계층 프레임워크(PIC Framework)를 제안하였다. PIC 프레임워크를 통해 보안 요구사항을 추천하는 과정은 문제 도메인 온톨로지 생성, 문제 도메인 온톨로지 기반 위험 산정, 보안 요구사항 추천 단계로 구성된다. 문제 도메인 온톨로지는 지식 형태에 따라 물리 계층(physical layer), 정보-모델링 계층(information-modeling layer), 인지 계층(cognitive layer)인 3계층으로 관련 지식을 구체화하고 통합하여 생성된다. PIC 프레임워크에서는 문제 도메인 온톨로지 기반으로 시스템 위험을 산정하고 보안 요구사항을 추천하는 과정에서 시스템 취약점에 집중한다. APT 공격과 같은 지능화되고 복합적인 공격을 고려하는 보안 요구사항은 시스템과 시스템 관련 인적 요소도 포함해야 할 필요가 있다[19].

제안한 APT 공격 사례 기반 보안 요구사항 추천 프레임워크는 3계층 접근법을 통해 복잡하고 다양한 APT 공격 특성을 반영하는 종합적이고 체계적인 통합 지식 베이스를 구축함으로써 이를 통해 지능화되고 복합적인 공격을 수행하는 APT 공격에 대한 보안 요구사항을 추천할 수 있다.

3. APT 공격 사례 기반 보안 요구사항 추천 프레임워크

본 논문에서는 APT 공격 사례로부터 보안요구 사항을 추천하는 프레임워크를 제안한다. 추천된 보안 요구사항은 분석된 APT 공격 요소와 시스템 요소를 반영한다. 제안된 프레임워크는 APT 공격에 대한 문제 도메인 온톨로지를 포함하는 통합 지식 베이스와 이를 통한 APT 공격 패턴 추론 및 보안 요구사항 추천 과정으로 구성된다. APT 공격 사례를 기반으로 설계된 문제 도메인 온톨로지는 물리, 정보-모델링, 인지 계층으로 구성된 3계층 접근법[17,18]을 통해 생성된다. APT 공격은 시나리오 기반으로 분석되고, 공격 요소와 요소 간 관계들에 대한 사례 기반 추론을 통해 APT 공격 패턴으로 추론된다. 문제 도메인 온톨로지에서 보안 요구사항 추천 프로세스를 통해 해당 APT 공격 패턴에 대한 보안 요구사항이 추천된다.

3.1 시나리오 기반 APT 공격 분석

제안된 프레임워크는 APT 공격에 대한 보안 요구사항을 도출하기 위해 APT 공격 사례를 시나리오 기반으로 분석한다. 본 논문은 [20]에서와 같이 50개 APT 공격 사례를 대상으로 공격 단계를 정찰(Reconnaissance), 전달(Delivery), 초기 침입(Initial Intrusion), C&C 서버(C&C Server) 연결, 내부 침입(Lateral Movement), 정보 수집(Information Gathering), 공격 마무리(Completing the attack), 총 7 단계로 구분하고 단계 별 공격 요소를 도출하였다.

그림 1은 시나리오 기반 APT 공격 분석을 통해 각 단계 별로 공격 구성 요소와 요소 간 관계를 도출하는 방법을 표현한다(Scenario-based APT Attack Analysis to elicit Attack Elements and Inter-elements Relationships). 시나리오는 공격자가 공격을 시도하는 일련의 과정으로, 공격 목표 달성을 위해 수행하는 공격 방법 및 도구, 공격 수행 관계를 확인할 수 있다. 이러한 단계별 공격 목표, 방법, 도구 등 공격을 수행하는 요소들이 시나리오 분석을 통해 정의되는 공격 요소(Attack Element)가 되며, 공격 수행 관계는 공격 요소 간 관계(Attack Elements and Inter-elements Relationships)가 된다.

[21]에서 제안된 요구 공학 방법인 ScenID는 시나리오 분석을 위해 시나리오를 수행자(actor), 작업(task), 목표(goal), 목적(objectives), 방해물(obstacle)로 표현하는 의미론적 모델 스키마(semantic model schema)를 사용한다. 그림 1은 ScenID을 참조하여 공격 시나리오를 악의적 목표(Malicious Goal), 공격자(Attacker), 공격 목적(Objective), 공격 방법(Attack Method), 공격

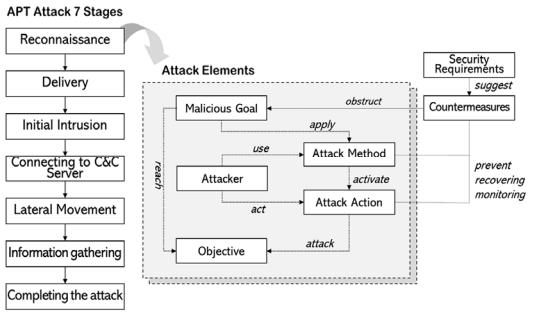

그림 1 시나리오 기반 APT 공격 분석을 통한 공격요소 및 요소 간 관계 도출

Fig. 1 Scenario-based APT Attack Analysis to Elicit Attack Elements and Inter-elements Relationships

행동(Attack Action)으로 구성한다. 공격 시나리오 분석을 통해 공격 요소뿐만 아니라 해당 시나리오에 대한 대응 방안(Countermeasures)과 보안 요구사항(Security Requirements)도 검토될 수 있음을 확인할 수 있다.

그림 2는 시나리오 기반 APT 공격 분석을 통해 도출한 단계 별 공격 요소와 공격 요소 간 관계에 대한 개념도(The Concept of the Relationships between APT Attack and Inter-elements)이다. 도출된 공격 요소는 단계 전후 공격 요소 간에도 연결된다. 시나리오 분석 결과인 공격 요소와 요소 간 관계는 APT 공격 패턴 추론 및 보안 요구사항 추천을 위해 통합 지식 베이스에 저장된다.

3.2 APT 공격 패턴 추론 및 보안 요구사항 추천을 위한 통합 지식 베이스

제안하는 프레임워크의 통합 지식 베이스는 그림 3과 같이 APT 공격 온톨로지(APT Attack Ontology), 일반 보안 온톨로지(General Security Ontology), 도메인 특화 온톨로지(Domain Specific Ontology)가 통합된 문제 도메인 온톨로지(Problem Domain Ontology)와 이를 지원하는 APT 공격 사례 데이터베이스(APT Attack Cases Database), 도메인 특화 데이터베이스(Domain Specific Ontology)로 구성된다. APT 공격 사례 데이터베이스는 APT 공격 사례를 시나리오 기반으로 분석한 결과가 저장되며 사례 기반 추론을 하는데 사용된다. 도메인 특화 지식 데이터베이스는 도메인 내 조직의 비즈니스 관련 모든 정보를 포함하며 이 정보를 기반으로 도메인 특화 온톨로지를 생성한다.

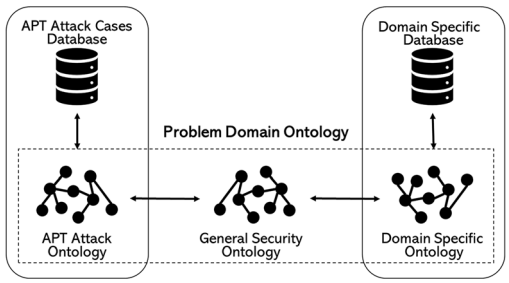

그림 3 통합 지식 베이스

Fig. 3 Integrated Knowledge Base

APT 공격 패턴에 대한 보안 요구사항을 추천하기 위한 주요 지식 베이스인 문제 도메인 온톨로지는 [17,18]에서 제안된 3계층 접근법으로 생성된다. 3계층 접근법은 지식을 모델링하고 통합하기 위해, 자료나 데이터 등 개별 지식을 포함하는 물리 계층, 개별 지식이 개념 단위로 분류되고 모델링된 정보-모델링 계층, 개념과 개념 간의 관계를 포함하는 인지 계층의 3계층으로 표현하는 방법이다.

문제 도메인 온톨로지는 APT 공격 지식(APT Attack Knowledge), 일반 보안 지식(General Security Knowledge), 도메인 특화 지식(Domain Specific Knowledge)을 포함한다. 각 지식은 3계층 접근법을 통해 APT 공격 온톨로지, 일반 보안 온톨로지, 도메인 특화 온톨로지로 생성된다. 그림 4는 3계층 접근법을 통해 문제 도메인 온톨로지의 각 지식 별 온톨로지를 생성하는 개념이다. 각 지식에 대하여 물리 계층 지식을 수집 및 분석

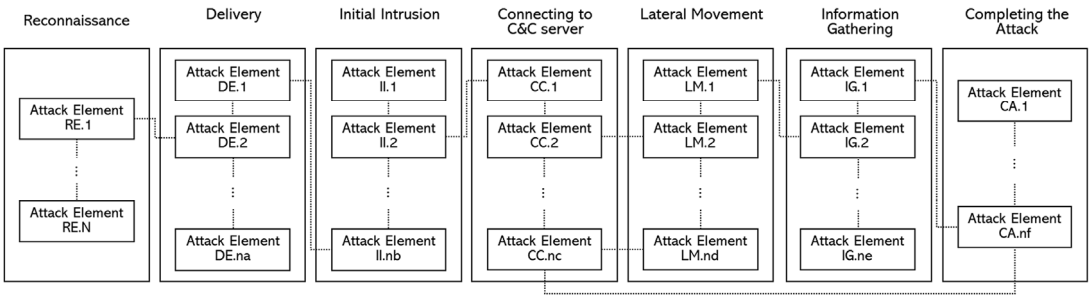

그림 2 APT 공격요소와 요소 간 관계 개념

Fig. 2 The Concept of the Relationships between APT Attack and Inter-elements

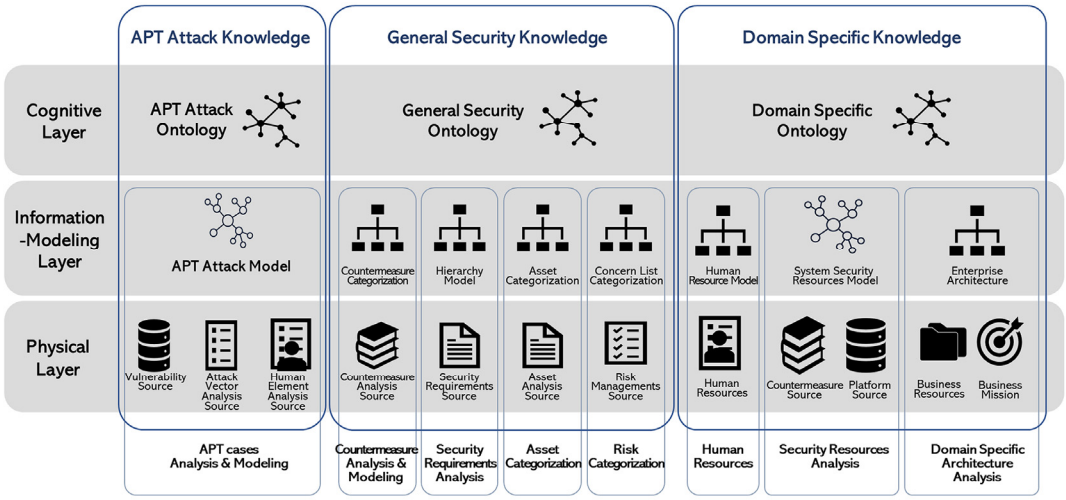

그림 4 3계층 접근법 통한 문제 도메인 온톨로지의 지식 별 온톨로지 생성 개념

Fig. 4 The Concept of Building Individual Ontologies of Problem Domain Ontology with a 3-Layer Approach

하고, 분석 결과를 분류 및 모델링을 거쳐 개념 별 모델로 구성한 후 개념과 개념 간 관계를 통해 지식 별 온톨로지가 생성되는 과정을 통해 문제 도메인 온톨로지를 구성하는 각 지식 별 온톨로지가 생성된다.

APT 공격 온톨로지는 APT 공격 사례로부터 도출할 수 있는 지식으로 시나리오 분석을 통한 공격 요소와 요소 간 관계를 포함한다. 일반 보안 온톨로지는 보안 요구사항을 추천하기 위해 필요한 보안 지식으로 자산, 보안 목표, 공격 벡터, 보안 대책, 공격 목적, 악의적 목표 등을 포함한다. 범용적인 지식으로 도메인에 상관없이 재사용 가능하다. 도메인 특화 지식과 연계하여 APT 공격 지식을 이해할 수 있도록 함으로써 보안 요구사항 도출을 가능하게 한다. 도메인 특화 온톨로지는 도메인 관련 지식으로 도메인 내 비즈니스 목표, 자산, 위험 요소 등을 포함한다. 특정 도메인 내 조직에 대한 정보-모델링 단계를 거쳐 온톨로지로 표현된다.

그림 5는 문제 도메인 온톨로지를 구축하는 과정(Building Process of Problem Domain Ontology)으로

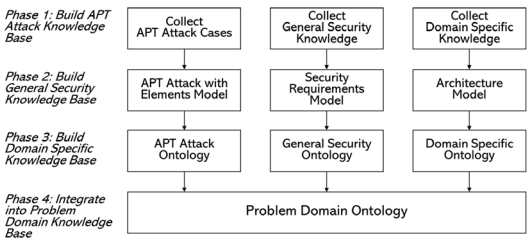

그림 5 문제 도메인 온톨로지 구축 과정

Fig. 5 The Building Process of Problem Domain Ontology

3계층 접근법을 통해 생성된 APT 공격 온톨로지, 일반 보안 온톨로지, 도메인 특화 온톨로지를 통합하여 문제 도메인 온톨로지가 구축됨을 표현한다.

APT 공격 온톨로지, 일반 보안 온톨로지, 도메인 특화 온톨로지를 통합한 문제 도메인 온톨로지는 세 가지 유형의 지식을 통해 APT 공격 및 보안 상황을 이해하고 보안 요구사항 추천을 지원한다. 다음은 각 온톨로지의 상세 구성 요소를 서술한다.

3.2.1 APT 공격 온톨로지

APT 공격 온톨로지는 APT 공격 정보를 담고 있는 지식 베이스이다. 제안된 프레임워크를 통해 특정 APT 공격이 시나리오 기반으로 분석되고 해당 공격 요소와 요소 간 관계가 사례 기반 추론에 의해 유사 사례 결정 및 보안 요구사항이 추천되는 일련의 과정이 완료되면, 사례 기반 추론의 대상이 되었던 공격 요소와 요소 간 관계는 새로운 공격 패턴으로, 추천되어 전문가 검토를 마친 보안 요구사항은 해당 공격 패턴에 대한 보안 요구사항으로서 기존 APT 공격 온톨로지에 축적된다.

기존 APT 공격 온톨로지에 추가되는 공격 패턴은 APT 공격에 대한 시나리오 기반 분석 결과인 공격 요소와 요소 간 관계이다. 공격 요소는 공격 목적 및 방법에 따라 분류된다. 공격 목적 및 방법은 온톨로지 클래스 계층 구조를 이루고, 공격 요소는 인스턴스로 정의된다. 인스턴스 간 연결은 프로퍼티로 정의된다.

그림 6은 APT 공격 온톨로지의 개념 모델이다. APT 공격 사례(APT Attack Cases)에 포함되는 APT 공격 사례 인스턴스는 APT 공격 목적(APT Attack Purpose) 내에서 정의된 공격 목적 인스턴스를 가지고,

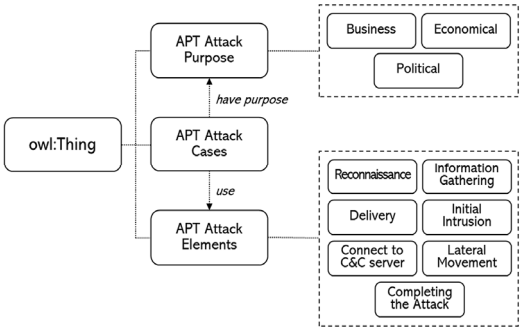

그림 6 APT 공격 온톨로지 개념 모델
Fig. 6 The Concept Model of APT Attack Ontology

APT 공격 요소(APT Attack Elements)에서 정의된 공격 요소 인스턴스를 사용한다. 공격 목적 인스턴스는 비즈니스(Business), 경제적(Economical), 정치적(Political) 목적으로 구분되고, 시나리오 분석 결과인 공격 요소는 APT 공격 7단계에 대한 사례 별 공격 요소를 가진다. 이와 같은 특정 APT 공격 사례, 공격 목적, 공격 요소는 APT 공격 패턴의 기본이 된다.

3.2.2 일반 보안 온톨로지

일반 보안 지식은 보안 요구사항 추천을 지원하기 위한 범용적인 보안 지식이다. 일반 보안 온톨로지는 일반 보안 지식에 속하는 개념[22]을 정의하고, 개념 간 연결을 통해 보안 요구사항을 추론할 수 있도록 한다.

본 논문은 [16]과 [23]을 참조하여 보안 요구사항을 구성하는 요소와 요소 간 관계를 정의한 [17]에서 제안한 모델에 APT 공격 사례와 인적 취약점을 이용하는 사회 공학적 요소 [24]를 포함하여 요소와 요소 간 관계를 재정의하였다. 그림 7은 본 논문에서 사용한 일반 보안 온톨로지 개념 모델로 이러한 구성 요소와 요소 간 관계를 보여준다.

일반 보안 온톨로지에서의 자산(Assets/Human Resource)은 조직 내에서 보호하고자 하는 대상으로, 자산 유형에 따라 분류된다. 자산은 노출된 취약점에 대해 공격 목적을 반영한 공격 벡터 및 공격 방법(Attack Vector/Attack Method)에 의해 공격 대상이 된다. 취약점(Technical/Human Vulnerability)은 자산 플랫폼 및 유형에 따라 분류된다. 공격 벡터는 APT 공격 패턴을 분석하기 위한 CAPEC[25] 공격 패턴을 반영하며, 공격 방법은 APT 공격에서 사용되는 공격 도구 및 기법이다. 악의적 목표(Malicious Goal)는 공격자가 목적을 달성하기 위해 취하는 행동 목표로 보안 목표와 대치한다. 보안 목표(Security Goal)는 보안의 3원칙인 기밀성, 무결성, 가용성, 악의적 목표는 노출, 수정, 파괴로 구성된다. 악의적 목표에 대한 보안 대응(Countermeasures)은 감시, 방어, 복구가 된다. 보안 요구사항은 미국 국방 정보 시스템국(Defense Information Systems Agency, DISA)에서 권장하는 보안 기술 구현 가이드(Security Technical Implementation Guide, STIG)[26]를 기반으로 정의하였다.

일반 보안 온톨로지를 구성하는 개념 간 미치는 영향은 개념 간 관계로 표현된다. 일반 보안 온톨로지에서 확인할 수 있는 개념 간 관계를 통해 공격 관련 개념인 공격 목적, 취약점, 공격 벡터, 공격 방법이 자산에 미치는 영향과 해당 자산을 보호하기 위한 보안 요구사항을 추천할 수 있다. 이를 위해 공격 목적, 악의적 목표, 기술/사람 취약점, 공격 벡터/공격 방법의 인스턴스는 APT 공격 지식, 자산/인적 자원은 도메인 특화 지식과 연결된다. 일반 보안 온톨로지는 도메인 특화 온톨로지와 독립적으로 관리될 수 있으며, 도메인 특화 온톨로지가 새로 생성되는 경우 일반 보안 지식을 재사용할 수 있다.

3.2.3 도메인 특화 온톨로지

도메인 특화 지식은 APT 공격이 영향을 미치는 특정 도메인 지식으로, APT 공격으로부터 공격 대상이 될 수 있는 조직의 비즈니스와 연관된 모든 자산에 대한 정보를 포함한다.

그림 8은 제안하는 프레임워크에서 사용하는 도메인 특화 온톨로지의 개념 모델(The Concept Model of Domain Specific Ontology)로, 보안 요구사항을 추천하

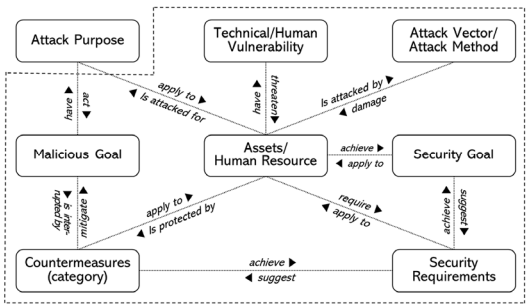

그림 7 일반 보안 온톨로지 개념 모델
Fig. 7 The Concept Model of General Security Ontology

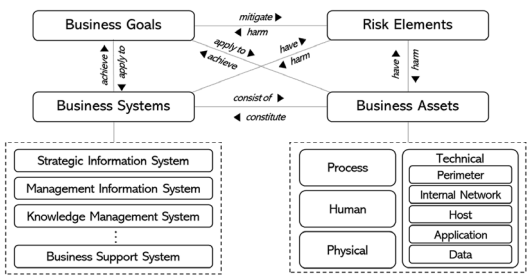

그림 8 도메인 특화 온톨로지 개념 모델
Fig. 8 The Concept Model of Domain Specific Ontology

기 위해 필요한 구성 요소를 도메인 관점에서 분류하고 정의한다. 도메인 특화 온톨로지는 비즈니스 목표(Business Goal)와 이를 지원하는 비즈니스 시스템(Business System), 비즈니스 시스템을 구성하는 비즈니스 자산(Business Assets)과 공격에 대한 위험을 검토할 수 있는 위험 요소(Risk Elements)로 구성되어 있다. 비즈니스 시스템은 도메인 내 비즈니스를 지원하는 시스템군으로 분류되며, 비즈니스 자산은 다양한 자산 유형과 이에 대한 심층 보안을 반영하는 자산군으로 분류된다. 도메인 특화 온톨로지의 구성 요소는 일반 보안 온톨로지와 연계하여 APT 공격에 대한 보안 요구사항을 추천한다. 도메인 특화 온톨로지는 적용되는 도메인, 조직 특성에 따라 새롭게 생성되어야 하며, 일반 보안 온톨로지와 독립적으로 도메인 지식 관리자에 의해 관리될 수 있다.

3.3 APT 공격 패턴 추론 및 보안 요구사항 추천

본 논문에서는 사례 기반 추론(CBR, Case Based Reasoning)을 통해 APT 공격 패턴을 추론한다. 제안된 사례 기반 추론 프로세스는 기존 사례에서 분석하고자 하는 APT 공격 사례에 대한 유사 사례를 추론할 수 있게 한다. 사례 기반 추론을 통해 얻은 유사 공격 사례, 즉 APT 공격 패턴은 보안 요구사항을 추천하는 기준 정보가 된다.

그림 9는 사례 기반 APT 공격 패턴 추론을 포함한 보안 요구사항 추천 프로세스(The Process of APT Attack Pattern Reasoning and Security Requirements Recommendation)이다. APT 공격 패턴은 사례 기반 추론 4단계인 검색(Retrieve), 재사용(Reuse), 수정(Revise), 유지(Retain) 단계에 따라 추론되며, 문제 도메인 온톨로지에서 해당 공격 패턴에 대한 보안 요구사항이 추천된다. 통합 지식 베이스 내 APT 공격 사례 데이터베이스에는 공격 시나리오와 해당 공격 패턴이 저장되고, 문제 도메인 온톨로지에는 APT 공격 패턴을 포함한 보안 요구사항 추천 관련 정보가 저장된다.

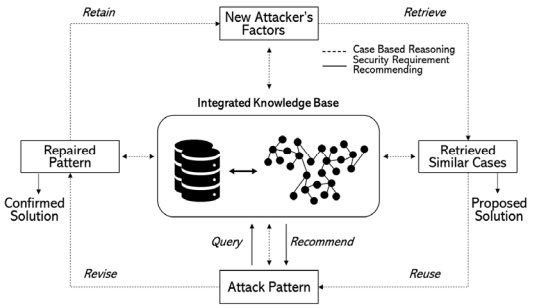

그림 9 APT 공격 패턴 추론과 보안 요구사항 추천 프로세스
Fig. 9 The Process of APT Attack Pattern Reasoning and Security Requirements Recommendation

시나리오 기반으로 APT 공격이 분석되면 공격 요소와 요소 간 관계가 도출된다. 도출된 공격 요소와 요소 간 관계로 통합 지식 베이스에서 사례 기반 추론 프로세스를 통해 사례 간 유사도 검사를 수행한 후 APT 공격 패턴(Attack Pattern)이 추론된다. 사례 간 유사도는 동일 공격 요소, 동일 그룹, 동일 범주 내 공격 요소 사용 여부 등을 통해 계산된다. 유사도 계산을 통해 획득한 유사 공격 사례는 APT 공격 패턴으로서 APT 공격 사례에 대한 보안 요구사항을 추천하는데 이용된다. 기본적으로 APT 공격 패턴으로 정의된 유사 공격 사례에 대한 기존 보안 요구사항이 분석 대상 APT 공격 사례에 대한 보안 요구사항으로 추천된다.

사례 기반 추론 및 보안 요구사항 추천에 적용에 APT 공격 패턴은 통합 지식 베이스에 포함되어 재사용된다. 따라서 보안 요구사항 추천 과정이 여러 번 수행될 수록 지식 베이스의 다양성과 규모가 증가한다.

4. 사례 연구를 위한 웹 어플리케이션 구현

제안하는 프레임워크에 대한 사례 연구를 위해 웹 어플리케이션을 구현하였다. 웹 어플리케이션은 APT 공격요소를 입력했을 때 유사 사례를 검색하고, 보안 요구사항을 추천한다.

그림 10은 제안된 프레임워크의 웹 어플리케이션 구조(Web Application Structure for the proposed framework)이다. MVC(Model, Controller, View) 구조로, 사용자 인터페이스(View)는 HTML 템플릿 엔진인 Pug와 CSS, Javascript로, Model과 Controller는 Javascript 기반 웹 프레임워크인 NodeJS의 Express로 구현되었다. APT 공격 사례 데이터베이스(APT Attack Case Database)는 MongoDB이고, NodeJS 모듈인 Mongoose를 통해

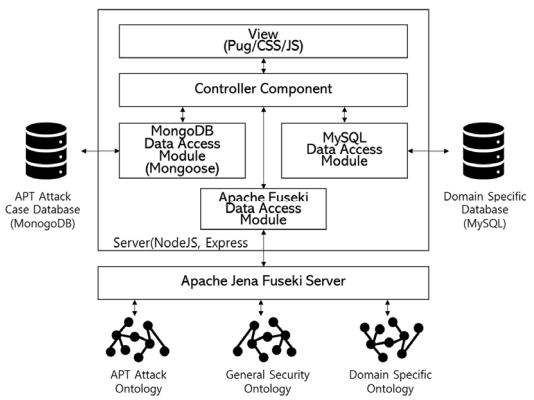

그림 10 제안된 프레임워크 웹 어플리케이션 구조
Fig. 10 The Web Application Structure for the Proposed Framework

접근한다. 도메인 특화 데이터베이스(Domain Specific Database)는 MySQL DB로, MySQL 쿼리를 통해 접근한다. APT 공격 온톨로지, 일반 보안 온톨로지, 도메인 특화 온톨로지는 그림 11과 같이 Protégé로 구현되었고, Apache Jena Fuseki Server에서 SPARQL 쿼리를 통해 접근한다. 보안 요구사항 추천은 데이터베이스에 저장된 사례와 온톨로지 간 지식 연계를 통해 수행된다.

5. 사례 연구

본 사례 연구는 제안하는 프레임워크를 통해 Copy-Kittens 그룹의 Operation Wilted Tulip 공격에 대한 보안 요구사항을 추천하는 과정을 서술하고 분석한다. 본 프레임워크는 기존 APT 공격 사례가 축적된 통합 지식 베이스를 포함한다. (1) 시나리오 기반 Operation Wilted Tulip 공격 분석, (2) 통합 지식 베이스 업데이트-가상 조직에 대한 도메인 특화 온톨로지, (3) 공격 패턴 추론-유사 APT 공격 패턴 검색, (4) 보안 요구사항 추천 순으로 진행된다.

5.1 시나리오 기반 Operation Wilted Tulip 공격 분석

Operation Wilted Tulip은 사이버 스파이 행위를 수행하는 CopyKittens 그룹에 의한 공격이다[27]. 다음은 Operation Wilted Tulip 공격 흐름과 특징을 반영한 주요 시나리오 중 하나로 이 시나리오를 기반으로 공격 요소와 요소 간 관계를 도출한다.

- 경쟁사의 핵심 기술 정보 획득을 목적으로 공격 대상 조직 내 영업 부서 소속 직원 E1의 개인 정보와 관심사 등을 SNS를 통해 수집한다.
- E1이 자주 사용하는 웹사이트 GEN_WEB을 해킹하여 악의적인 스크립트를 업로드한다.
- E1이 GEN_WEB에 접속하면 스크립트가 실행되고, E1의 PC에 Cobalt Striker가 설치된다.
- Cobalt Striker를 통해 E1의 사내 메일 계정 정보를 획득한다.
- E1 계정으로 메일 서버에 접속하여 다른 계정에 악성 메일을 전송하여 다른 PC에도 Cobalt Striker를 설치한다.
- 연속 감염과 탐색을 통해 핵심 기술을 관리하는 E2의 PC를 감염시키고, 핵심 기술 데이터에 대한 접근 권한을 획득한다.
- 핵심 기술 데이터를 수집하고, 수집한 정보를 압축하여 공격자 서버로 보낸 후, 흔적을 삭제한다.

서술된 시나리오를 기반으로 APT 공격 7 단계 별 공격 요소와 요소 간 관계를 도출할 수 있다. 그림 13은 전달(Delivery) 단계에서의 공격 요소와 요소 간 관계 일부를 보여준다.

모든 단계에서 공격 요소와 요소 간 관계를 도출하면 시나리오에 대한 전체 공격 요소와 요소 간 관계를 얻을 수 있다. 그림 12는 Operation Wilted Tulip 공격

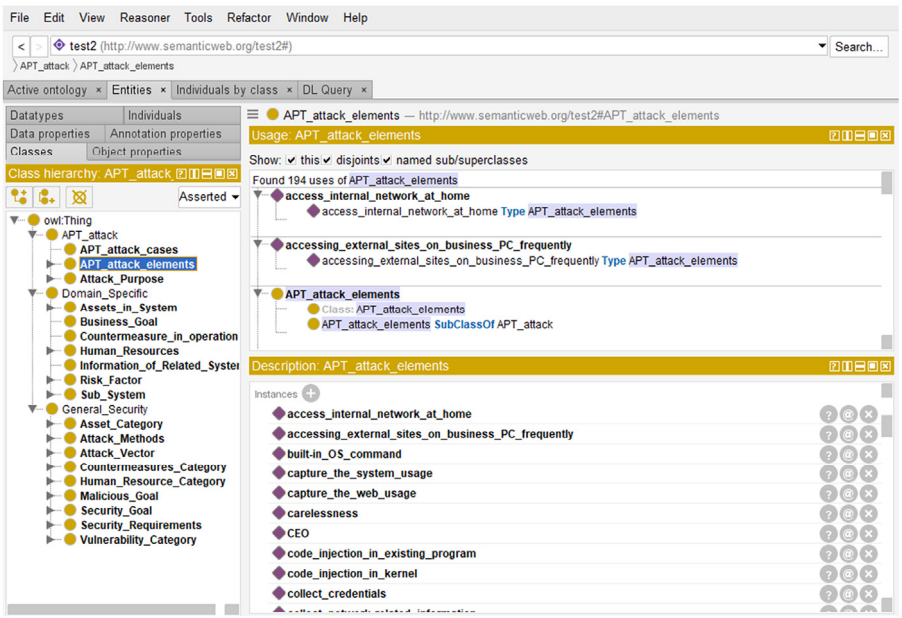

그림 11 문제 도메인 온톨로지

Fig. 11 Problem Domain Ontology

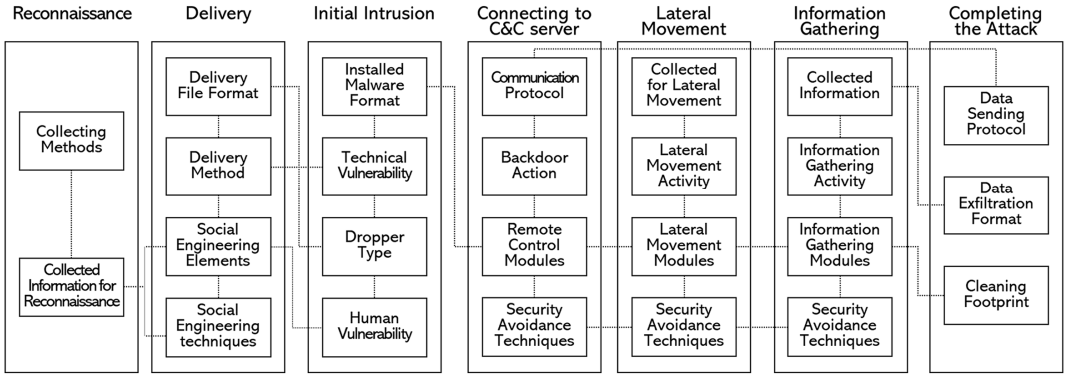

그림 12 Operation Wilted Tulip 공격 요소와 요소 간 관계

Fig. 12 Attack Elements and Inter-elements Relationships of Operation Wilted Tulip

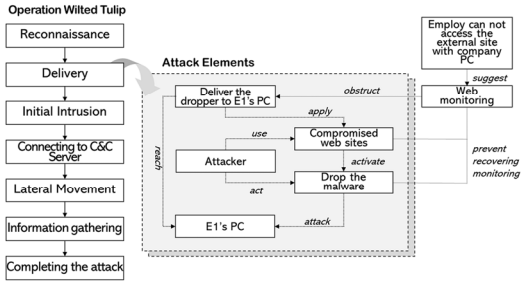

그림 13 Operation Wilted Tulip 시나리오 분석을 통한 공격 요소 및 요소 간 관계 도출

Fig. 13 Elicitation of Attack Elements and Inter-elements Relationships by Scenario-based Analysis of Operation Wilted Tulip

시나리오에 대해 얻을 수 있는 공격 요소와 요소 간 관계의 일부이다.

5.2 통합 지식 베이스 업데이트-도메인 특화 온톨로지

상기 Operation Wilted Tulip 공격에서 공격 대상이 되는 조직에 대한 도메인 지식을 준비하고, 제안된 프레임워크 내 도메인 특화 온톨로지를 업데이트 한다. 공격 대상이 되는 조직은 사례 연구를 위해 그림 14와 같이 구성된 가상 조직이다. 도메인 특화 온톨로지는 그림 8과 같이 구성된 온톨로지 개념에 가상 조직의 자산을 인스턴스로 포함한다.

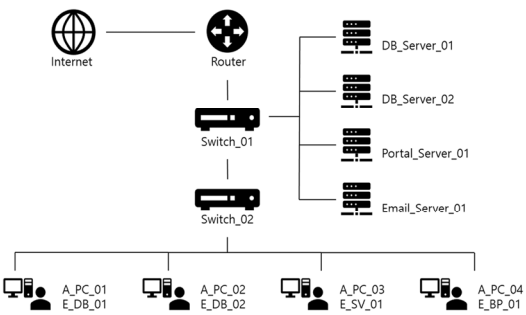

그림 14 조직 내 자산 구조도

Fig. 14 Asset Structures in the Organization

가상 조직은 데이터베이스 서버 DB_Server_01, DB_Server_02와 포탈 서버 Portal_Server_01, 메일 서버 Email_Server_01로 구성된다. DB_Server_01은 고객 정보, DB_Server_02는 사업 정보를 저장하고, Portal_Server_01은 기업 포탈 등 기업 내부 서비스, Email_Server_01은 메일 서비스를 제공한다. 네 명의 직원은 Portal_Server_01과 Email_Server_01 계정을 가지고 있으며, 직책과 직무에 따라 관련 시스템에 접근할 수 있다. 직원 E_DB_01과 E_DB_02는 각각 DB_Server_01, DB_Server_02를 관리하는 데이터베이스 관리자로 각 데이터베이스 서버에 대한 접근 권한 및 관리자 권한을 가진다. E_SV_01은 Portal_Server_01을 관리하며 메인 서버의 접근 권한과 관리자 권한을 가진다. E_BP_01은 사업 플랜 문서를 작성 및 관리하는 직원으로 DB_Server_02로의 접근 권한을 가진다. 직원 모두 개인 PC, A_PC_01, A_PC_02, A_PC_03, A_PC_04를 가진다.

5.3 공격 패턴 추론-유사 APT 공격 패턴 검색

제안한 프레임워크 내 통합 지식 베이스에서 Operation Wilted Tulip을 시나리오 기반으로 분석한 공격 요소와 공격 요소 간 관-계에 대한 공격 패턴을 추론한다.

통합 지식 베이스에는 이미 Operation Wilted Tulip 사례가 포함되어 있고, 27가지 공격 요소를 가진다. 분석하고자 하는 공격 시나리오(Operation Wilted Tulip)에서 공격 요소와 공격 요소 간 관계가 도출되면 공격 패턴 추론을 위한 입력으로 사용된다. 입력되는 공격 요소는 Operation Wilted Tulip 공격 요소 27가지 중 같은 공격 단계 내 5개 공격 요소가 다른 공격 요소로 구

Test #	Input Case	Output Case	Attack Pattern
Test 01	Change few elements	Wilted_Tulip_01, Wilted_Tulip_02, Wilted_Tulip_04	Wilted_Tulip
Test 02	Delete few elements	Wilted_Tulip_01, Wilted_Tulip_04	Wilted_Tulip
Test 03	Change many elements	Wilted_Tulip_05	Wilted_Tulip
Test 04	Delete mant elements	Wilted_Tulip_01, Wilted_Tulip_04, APT_1_04	Wilted_Tulip, APT_1

그림 15 APT 공격 사례 유사도 분석 결과
Fig. 15 Results of Similarity Analysis for APT Attack Cases

Asset	Vulnerability	Attack Vector	Attack Purpose	Total
A_PC_01	0	60	0	60
A_PC_02	0	60	0	60
A_PC_03	0	60	0	60
A_PC_04	3	60	1	64
DB_server_01	0	16	1	17
DB_server_02	3	21	1	25
Main_Server_01	3	31	0	34
Email_server_01	3	20	0	23

그림 16 공격 요소에 대한 자산 분석 결과
Fig. 16 Results of Asset Analysis for Attack Elements

성된 공격 요소 집합으로, 그림 15에서 Test 01에 해당한다. Test 02, Test 03, Test 04는 이 외 유사 APT 공격 패턴 검색 결과 확인을 위해 생성한 임의의 공격 요소 집합으로, Test 02는 27가지 공격 요소 중 같은 공격 단계 내 5개 공격 요소를 삭제한 공격 요소 집합, Test 03은 임의의 여러 공격 단계에서 10가지 공격 요소를 변경한 공격 요소 집합, Test 04는 임의의 여러 단계에서 10가지 요소를 삭제한 공격 요소 집합이다.

유사 APT 공격 패턴 검색 결과는 그림 15와 같다. 분석하고자 하는 공격 Operation Wilted Tulip을 시나리오 기반으로 분석하여 도출한 공격 요소 집합 Test 01에 대하여 추론된 공격 패턴은 “Wilted_Tulip”이고, 구성 사례가 되는 공격 요소 집합으로 “Wilted_Tulip_01”, “Wilted_Tulip_02”, “Wilted_Tulip_04”이 있음을 확인할 수 있다. Test 02, Test 03, Test 04는 본래의 Operation Wilted Tulip 공격 요소를 부분 변경한 것으로 결과를 통해 유사 APT 공격 패턴 검색 기준을 확인할 수 있다. 이 과정은 그림 9의 사례 기반 추론 중 검색(retrieve) 과정에 해당된다. 추론된 공격 패턴은 보안 요구사항 추천을 위해 재사용(Reuse)된다. 보안 요구사항 추천이 완료되면 피드백을 통해 수정(Revise)될 수 있고, 통합 지식 베이스 업데이트를 통해 유지 (retain)된다.

5.4 보안 요구사항 추천

제안한 프레임워크 내 통합 지식 베이스에서 Operation Wilted Tulip을 시나리오 기반으로 분석한 공격 요소와 공격 요소 간 관계에 대한 공격 패턴이 추론된 후 추론된 공격 패턴에 대한 보안 요구사항을 추천한다. 통합 지식 베이스에서 “Wilted_Tulip_01”, “Wilted_Tulip_02”, “Wilted_Tulip_04”에 대한 보안 요구사항을 검토한다. 요구 사항 검토를 위해 요구 사항이 적용되어 있는 자산을 검색한다.

분석에 사용된 시나리오는 Operation Wilted Tulip을 통해 대상 기업의 고객 정보를 포함한 비즈니스 정보 유출을 목적으로 하므로 공격 요소 중 특정 자산 취득이 목적인 공격 요소를 통해 이 공격에 노출될 위험 이 높은 자산을 검색한다. 그림 16은 보안 요구사항 추천을 위해 공격에 노출될 위험이 높은 자산을 검색한 결과이다. 입력한 공격 요소와 연관된 취약점, 공격 벡터, 공격 목적, 관련 자산이 검색된다. 검색된 횟수는 DB_Server_01 17번, DB_Server_02 25번, Email_Server_01 23번, Portal_Server_01 34번으로, 포탈 서버가 입력된 공격 요소에 노출될 확률이 높다. 개인 PC는 A_PC_01, A_PC_02, A_PC_03이 모두 60번, A_PC_04는 64번으로 개인 PC 자산이 다른 자산에 비해 검색 수가 높다. 자산의 위험 노출도 분석 결과 공격 목표와 관련된 자산이 많이 검색되며, APT 공격 특성 상 내부 망 탐색에 용이한 자산이 상대적으로 많이 검색된다. 위험도가 높은 자산 순으로 보안 요구사항을 검색하고 검토한다.

결과적으로 시나리오를 분석하여 도출된 공격 요소에 의해 추론된 공격 패턴에 추천되는 보안 요구사항은 기술적 보안 요구사항과 인적 보안 요구사항으로 구분된다. 기술적 보안 요구사항은 적용 목적에 따라 보안 3요소로 분류된다. 본 사례 연구에서는 입력한 공격 요소가 개인 PC를 공격할 가능성이 높기 때문에 관련된 보안 요구사항이 추천된다. 특히 공격 목적이 정보 획득이므로 기밀성과 관련된 보안 요구사항이 다수 검색된다.

그림 17은 기술적 보안 요구사항 추천 결과이다. 개인 PC에 대한 보안 요구사항은 220번, 데이터베이스 관련 요구사항과 서버 관련 요구사항이 보안 목표에 따라 11번씩 검색된다. 통합 지식 베이스에 설정한 개인 PC 관련 요구사항은 10개, 데이터베이스, 서버 관련 요구사항은 모두 20개로 상대적으로 적은 수의 지식이 있었음에도 공격 패턴과 관련 자산에 대해 개인 PC에 집중되어 보안 요구사항이 추천된다.

인적 보안 요구사항은 인적 자원에 적용되는 보안 요구사항이다. 인적 자산에 대한 보안 요구사항 추천은 그림 18과 같다. SESR_03이 1188로 가장 많이 검색되었는데 이는 개인 PC와 관련된 보안 요구사항이다. 기술적 보안 요구사항 결과와 같이 개인 PC 자산이 공격에 노출될 가능성이 높기 때문에 해당 보안 요구사항에 대한 검색 수가 높다.

이와 같이 제안한 프레임워크에서 시나리오 기반 Operation Wilted Tulip 공격 분석, 통합 지식 베이스 업데이트-가상 조직에 대한 도메인 특화 온톨로지, 공격 패턴

security_requirement	security goal	num
DBSR_01	C	22
DBSR_02	C	44
DBSR_03	C	22
DBSR_04	C, I	88
DBSR_05	I	44
DBSR_06	C	22
DBSR_07	C	44
DBSR_08	I	22
DBSR_09	A	22
DBSR_10	A	44
DBSR_11	C	22
DBSR_12	C	22
DBSR_13	A	22
DBSR_14	C, I	44
DBSR_15	C, I	44
DBSR_16	C, I	44
DBSR_17	C, I	44
DBSR_18	C	22
DBSR_19	C	22
DBSR_20	C	22

security_requirement	security_goa	num
SVSR_01	C	22
SVSR_02	C	11
SVSR_03	A	22
SVSR_04	C, I	66
SVSR_05	I	11
SVSR_06	C, I	44
SVSR_07	C, I	44
SVSR_08	A	11
SVSR_09	C, I	22
SVSR_10	C	11
SVSR_11	C	22
SVSR_12	C	22
SVSR_13	C	11
SVSR_14	C	11
SVSR_15	C	11
SVSR_16	C	11
SVSR_17	C	11
SVSR_18	C, I	22
SVSR_19	C, I	22
SVSR_20	C	11

security_requirement	security_goal	num
PCSR_01	C	220
PCSR_02	C	220
PCSR_03	C	220
PCSR_04	C	220
PCSR_05	C	220
PCSR_06	C	220
PCSR_07	C	220
PCSR_08	C	220
PCSR_09	C	220
PCSR_10	C	220

그림 17 공격 요소에 대한 기술적 보안 요구사항 추천 결과
Fig. 17 Results of Technical Security Requirements Recommendation for Attack Elements

security_requirement	description	num
SESR_01	The employees must take at least one of security education course	594
SESR_02	The employees must change the password of their company account regulary	891
SESR_03	The employees must not access to internal server in outside without VPN	1188
SESR_04	The employees must not save their account information (ID, password) on non-encryption file.	891
SESR_05	The employees must log-out the internal server when they do not use.	889
SESR_06	The organization must provide the data encryption policy.	230
SESR_07	The organization must provide the education course about the email security.	593
SESR_08	The organization must provide the server authorization policy	297
SESR_09	The organization must provide policy for using mobile computers outside.	296
SESR_10	The organization must provide the network device that provide encryption network communication.	297

그림 18 공격 요소에 대한 인적 보안 요구사항 추천 결과
Fig. 18 Results of Human Security Requirements Recommendation for Attack Elements

추론-유사 APT 공격 패턴 검색, 보안 요구사항 추천 과정을 통해 입력한 공격 요소에 적합한 보안 요구사항이 추천됨을 확인할 수 있다.

6. 결 론

본 논문에서는 APT 공격 사례를 포함하는 지식 베이스를 구축하고, 특정 APT 공격을 시나리오 기반으로 분석하여 공격 요소 및 요소 간 관계를 도출, 사례 기반 추론을 통해 공격 패턴을 추론하고 이에 대한 보안 요구사항을 추천하는 APT 공격 사례 기반 보안 요구사항 추천 프레임워크를 제안한다. 3계층 접근법 기반으로 생성된 통합 지식 베이스는 APT 공격 지식과 일반적 보안 지식, 도메인 특화 지식으로 구성되어 APT 공격에 대한 보안 요구사항을 추천하기 위한 관련 지식 및 분류로 정의되었다. 사례 기반 추론 프로세스는 APT 공격 요소와 요소 간 관계를 기반으로 유사 사례를 도출하는 과정을 통해 공격 패턴을 추론한다. 이를 위해 APT 공격에 대해 시나리오 기반으로 단계 별 공격 요소와 요소 간 관계를 도출하는 시나리오 기반 APT 공격 분석을 수행했다.

제안한 프레임워크는 APT 공격 사례를 기반으로 보안 요구사항을 추천하는 프레임워크로 실제 공격 위협과 자산에 대한 위험 노출도 평가를 하나의 프레임워크를 통해 자동화할 수 있다. 새로운 APT 공격에 대한 지식이 입력되었을 때 사례 기반 추론 프로세스를 통해 공격 패턴을 추론하고 통합 지식 베이스에 지식을 추가하여 공격에 대한 지식을 축적한다. 또한 도메인 지식을 기반으로 한 보안 요구사항 추천을 통해 실제로 적용할 수 있고 평가를 할 수 있다.

APT 공격 요소 및 요소 간 관계, 관련 자산의 공격에 대한 위험 노출도에 대한 범위와 분류를 다각화하면 보다 복잡한 보안 상황을 이해하고 이를 반영한 보안 요구사항을 추천할 수 있다. 특히 사람 취약점 또는 사람 성격 및 행동 요소 정의에 있어 실제 사용자 로그를 분석하여 반영하는 등 새로운 시도가 필요하다. 향후 이와 같은 통합 지식 베이스의 고도화를 통해, 제안된 보안 요구사항 추천 프레임워크는 공격 사례를 기반으로 복잡한 APT 공격에 대해 선제적 방어를 수행할 수 있도록 지속적으로 개선될 것이다.

References

[1] Ponemon Institute, "2011 cost of data breach study: United states," Ponemon Institute, 2012.

[2] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," *IFIP International Conference on Communications and Multimedia Security*, pp. 63-72, 2014.

[3] N. Virvilis, D. Gritzalis, and T. Apostolopoulos, "Trusted computing vs. advanced persistent threats: Can a defender win this game?" *IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, pp. 396-403, 2013.

[4] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 537-540, Apr. 2016.

[5] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey," *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 4, pp. 2091-2121, 2013.

[6] F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat: A case study of malware for political espionage," *2011 6th International Conference on Malicious and Unwanted Software*, October 2011, Available: https://ieeexplore.ieee.org/document/6112333. DOI: 10.1109/MALWARE.2011.6112333.

[7] D. N. Pande and P. S. Voditel, "Spear phishing: Diagnosing attack paradigm," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, March 2017, Available: https://ieeexplore.ieee.org/document/8300257. DOI: 10.1109/WiSPNET.2017.8300257.

[8] LogRhythm, "The APT lifecycle and its log trail," LogRhythm, 2013.

[9] B. I. D. Messaoud et al., "Advanced persistent threat: New analysis driven by life cycle phases and their challenges," *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)*, 2017.

[10] Meicong Li et al., "The study of APT attack stage model," *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, June 2016, Available: https://ieeexplore.ieee.org/document/7550947. DOI: 10.1109/ICIS.2016.7550947.

[11] M. Bere et al., "How Advanced Persistent Threats Exploit Humans," *International Journal of Computer Science Issues*, Vol. 12, No. 6, 2015.

[12] M. Ussath et al., "Advanced persistent threats: Behind the scenes," *2016 Annual Conference on Information Science and Systems (CISS)*, pp. 181-186, 2016.

[13] J. D. Moffett, C. B. Haley, and B. Nuseibeh, "Core security requirements artefacts," Department of Computing, The Open University, Milton Keynes, UK, 2004.

[14] G. Elahi, E. Yu and N. Zannone, *A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[15] P. Salini and S. Kanmani, "A novel method: Ontology-based security requirements engineering framework," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1-5, Feb. 2016.

[16] S. Lee et al., "Building problem domain ontology from security requirements in regulatory documents," *Software Engineering for Secure Systems*, pp. 43, 2006.

[17] B. Kim and S. Lee, "Analytical study of cognitive layered approach for understanding security requirements using problem domain ontology," *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*, pp. 97-104, 2016.

[18] B. Kim and S. Lee, "Understanding and recommending security requirements from problem domain ontology: A cognitive three-layered approach," *The Journal of Systems & Software*, Vol. 169, 2020.

[19] A. Suleimanov, M. Abramov, and A. Tulupyev, "Modelling of the social engineering attacks based on social graph of employees communications analysis," pp. 801, 2018.

[20] M. Kim and S. Lee, "Analysis and Modeling of Advanced Persistent Threat through Case Study," *Journal of KIISE*, Vol. 46, No. 2, pp. 1328-1338,

2019.
[21] C. Potts, "ScenIC: A strategy for inquiry-driven requirements determination," *Proc. IEEE International Symposium on Requirements Engineering (Cat.no. PR00188)*, pp. 58-65, 1999.
[22] A. Avizienis et al., "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 1, pp. 11-33, 2004.
[23] Common Criteria, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*, Common Criteria, 2012.
[24] S. Kim and S. Lee, "Social engineering based security requirements elicitation model for advanced persistent threats," *Communications in Computer and Information Science*, Vol. 809, pp. 29-40, 2018.
[25] *The MITRE Corporation, Common Attack Pattern Enumeration and Classification(CAPEC)*. Available: https://capec.mitre.org/. (Accessed Jul. 7, 2021)
[26] C. E. P. DoD, "Security Technical Implementation Guides, Https://Public.Cyber.Mil/Stigs/Srg-Stig-Tools/, 2021. (Accessed Jul. 7, 2021)
[27] ClearSky Cyber Security Trend Micro, "Operation wilted tulip [white paper]," ClearSky Cyber Security, Trend Micro, 2017.

김 민 주

2017년 아주대학교 소프트웨어학과 졸업(학사). 2019년 아주대학교 컴퓨터공학과 졸업(석사). 관심분야는 소프트웨어공학, 정보보안, 지식기반 시스템

박 신 혜

1999년 아주대학교 정보컴퓨터공학부 졸업(학사). 2004년 아주대학교 정보통신공학과 졸업(석사). 2016년~현재 아주대학교 인공지능학과 박사과정. 관심분야는 소프트웨어공학, 정보보안, 인공지능

이 석 원

1992년 동국대학교 전자계산학과 졸업(학사). 1995년 Univ. of Pittsburgh, Computer Science (Artificial Intelligence) 졸업(석사). 2003년 George Mason Univ. Computer Science (Software Engineering) 졸업(박사). 1999년~2000년 IBM Thomas J. Watson Research Center 연구원. 2000년~2003년 Science Applications International Corporation (SAIC),수석연구원. 2003년~2010년 Univ. of North Carolina at Charlotte Software and Information Systems 교수 2010년~2012년 Univ. of Texas at San Antonio Information Systems and Cyber Security 교수. 2012년~2017년 아주대학교 소프트웨어융합학과 교수, 소프트웨어 특성화대학원장. 2017년~현재 아주대학교 소프트웨어학과, 인공지능학과 교수. 관심분야는 기계학습, 인공지능, 요구공학, 소프트웨어공학, 정보보안