JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 8, pp. 133-146, August 2025
https://doi.org/10.9708/jksci.2025.30.08.133

An Effective Visualization Method of Cyber Attack Modeling Technique to Improve Information Delivery using MITRE ATT&CK

Jae-Ho Lee*, Seok-Won Lee**

*Student, Dept. of Computer Engineering, Ajou University, Suwon, Korea
**Professor, Dept. of Software and Computer Engineering, Ajou University, Suwon, Korea

[Abstract]

In this paper, we propose a cyber attack model uniquely designed to improve understandings and usefulness for various computer system stakeholders. From various studies and researches, we elicited our research questions to solve a structural problem of Attack Trees and difficulties in understanding cyber attack reports. Our proposed model is designed to cooperate with MITRE ATT&CK cyber attack intelligence to provide a clear view of complex cyber attacks and enhanced information delivery both for experts and non-expert stakeholders. Additionally, our model ensures that each incident results in only one cyber attack model, eliminating ambiguity in cyber security assessment activities within an organization. We conducted a validity verification experiment to verify our method's efficiency against participants with various cyber security background knowledge. Our proposed model shows non-expert participants can understand cyber attack incidents with our model.

▸ **Key words**: Cyber Attack modeling, Visualizable Cyber Attack model, Graph Cyber Attack model, Cyber Threat Intelligence, Security assessment, Risk identification

[요 약]

본 논문에서는 다양한 컴퓨터 시스템의 이해 당사자들에게 보다 유용하도록 개선한 사이버 공격 모델을 제안한다. 다양한 연구들의 결과로부터 우리는 Attack Tree의 구조적 문제와 이해하기 어려운 사이버 공격 보고서의 문제를 발견하였고, 제안하는 모델은 MITRE ATT&CK 사이버 위협 인텔리전스를 활용하여 복잡한 사이버 공격에 대한 명확한 모델과 향상된 정보 전달이 가능하도록 하였다. 또한, 비전문가 이해 당사자들이 보다 쉽게 이해할 수 있도록 하였으며, 각 사이버 공격 사건이 하나의 모델로 귀결되도록 하여 조직 내 보안 사고 분석 활동 중에 발생하는 모호성을 제거한다. 본 모델의 기능 평가를 위하여 다양한 사이버 보안 배경 지식을 가진 참여자들을 대상으로 타당성 검증 실험을 수행하였으며, 비전문가 참여자들도 사이버 공격 사건을 충분히 이해할 수 있음을 보였다.

▸ **주제어**: 사이버 공격 모델링, 시각화 사이버 공격 모델, 공격 트리, 그래프 사이버 공격 모델, 사이버 위협 인텔리전스, 보안 사고 분석, 리스크 평가

• First Author: Jae-Ho Lee, Corresponding Author: Seok-Won Lee
*Jae-Ho Lee (infsynthesis@ajou.ac.kr), Dept. of Computer Engineering, Ajou University
**Seok-Won Lee (leesw@ajou.ac.kr), Dept. of Software and Computer Engineering, Ajou University
• Received: 2025. 06. 17, Revised: 2025. 07. 08, Accepted: 2025. 08. 07.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

현대 사회에서 컴퓨터 네트워크는 필수적인 부분으로 자리를 잡았으나, 사이버 공격의 위협에 끊임없이 노출되어 있으며 그 복잡성은 지속적으로 증대되고 있다. 초기에는 단순히 시스템을 파괴하는 행위에 그쳤으나, 오늘날의 사이버 공격은 고도화된 보안 체계도 돌파 혹은 우회하여 침투하여 피해를 입히며, 금전적 이득을 취하려는 등 방어 기술의 발전을 비웃듯 빠르게 발전하고, 그로 인한 피해 또한 이제는 단순한 데이터 파괴만이 아닌 막대한 금전적 및 사회적 피해를 유발하게 되었다. Stuxnet[1][2] 등의 Advanced Persistent Threat로 분류할 수 있는 사이버 공격들과 랜섬웨어들이 대표적이라고 할 수 있다. 이런 공격들을 정확하게 분석하고 이해하여야 유의미한 방어 전략을 세우고 피해가 최소화될 수 있도록 시스템을 설계하고 운영할 수 있을 것이다.

사이버 공격을 표현하기 위한 개념으로, 트리 형태로서 사이버 공격의 각 요소를 세부 사항으로 분해하며 분석하는 Attack Tree[3]가 있다. 이 모델이 발표된 이후, 다양한 연구자들이 이를 기반으로 하며 기능을 추가한 다수의 파생형 Attack Tree 모델들이 발표되었다. 이들 Attack Tree 기반 모델 이외에도 다른 개발 방향의 모델링 기법 또한 개발되었다. MITRE 사의 ATT&CK®[4]은 공격 기술과 대응책을 정리한 사이버 위협 인텔리전스이며, 사이버 공격 모델링의 기법으로서도 활용될 수 있다. 이는 보안 커뮤니티와의 지속적인 협업을 통하여 꾸준히 관리되고 갱신되며, 누구나 이용할 수 있도록 공개되어 있다. 그러나, ATT&CK과 같은 지식 베이스를 파생형 Attack Tree 등의 사이버 공격 모델링 분야에서 적극적으로 활용하는 사례는 그리 흔치 않았다.

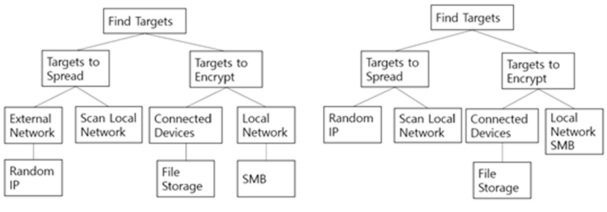

Fig. 1. Isomorphic Attack Trees

Attack Tree 및 이의 파생형 사이버 공격 모델들은 일반적으로 모델의 작성 규칙이 비교적 자유로운 편이다. Attack Tree에 대하여 원 저자 외의 시점에서 분석한 논문[5]에서 지적한 바에 따르면, 사이버 공격 모델을 작성한 사람이 평시 및 작성 당시에 중요시한 요소와 사용한 용어에 따라 같은 사건을 같은 그래프 형 모델로 작성하여도 의미는 같으나 외형과 내용이 일치하지 않는 서로 다른 모델, 즉 동형 트리가 제작될 수 있는 가능성이 존재한다. 이러한 문제는 여러 사람이 하나의 사건에 대하여 Attack Tree를 작성하여 분석할 경우는 물론, 한 사람이 하나의 사건을 다시 분석할 때에도 발생할 수 있다. 예를 들어, Fig. 1과 같이 Attack Tree의 규칙으로는 작성자의 시점에 따라 사용되는 용어에 차이가 존재하고, 구조가 다르지만 그 의미는 동일한 트리가 생성될 수 있다. 결국 하나의 형태로 수렴시키기 위해서는 추가적인 작업이 필요한 것이다. 또한, 사용하는 용어에 대한 기준이 명시되지 않으므로, 용어가 서로 다르게 작성되어 하나 이상의 사이버 공격 모델들을 읽어야 하는 이해 당사자들의 의사소통을 방해하게 된다. 또한, 이러한 모델들은 통일된 규격과 용어가 없어 보안 위협의 대응을 위한 시스템에 활용하려면 사전에 통일된 규격과 용어 규칙에 의한 데이터의 전처리 과정이 필요할 것이다.

보안 사고를 예방하거나 발생한 사고에 대응하는 과정에서는 인력과 복구비용 등의 상당한 비용 지출이 발생한다. 개인이 아닌 회사 등의 조직에서는 보안 사고에 대한 이해도가 낮은 구성원들에게도 관련 정보를 명확히 전달하여 구성원들이 비용 지출을 납득할 수 있어야 한다. 그러나 이를 위해 작성되어 제시되는 사이버 공격 보고서들에는 여러 가지 문제점들이 있다. 한 조사 결과[6]에 따르면, 사이버 공격 보고서가 일관성이 없는 서술 구조를 가지고 있거나, 과도하게 많은 정보를 담고 있는 경우가 많았으며, 이는 특히 조직에서 보안 문제에 대한 인식과 의사 결정을 어렵게 하였음이 확인되었다. 이는 보안 전문가가 아닌 이해 당사자들을 대상으로 하는 회의 자료 등을 작성할 때, 제공하는 정보의 양을 조절하여 이러한 문제점을 해결해야 한다는 것을 의미한다. 이 문제를 완화하기 위하여, 조직의 보안 전문가들은 사이버 공격 모델을 작성할 경우 사고 분석에 활용하기 위한 자세한 공격 모델과 더불어 앞서 언급한 조직의 비전문가 이해 당사자들이 이해할 수 있도록 기술적인 난이도를 낮춘 요약 모델을 각각 작성해야 한다. 그러나 Attack Tree와 이 모델의 파생형 모델들은 일반적으로 이러한 요구 사항에 대응하도록 개발되지 않았다. 또한, 이들 트리 형 모델들은 트리 구조에 익숙하지 않은 이해 당사자들이 잘못된 방향으로 인식을 시도할 수 있으며, 이는 이러한 이해 당사자들의 사건 이해 및 정보 전달을 저해하는 결과를 불러온다. 따라서, 우리는 Attack Tree 및 이를 기반으로 하여 개발된 많은 수의 사이버 공격 모델들에서 해결하지 않은 문제점들을 다

음과 같이 정의한다.

P1. 사이버 공격 모델에 사용하는 표준 용어를 지정하지 않아 동일한 개념에 동일한 용어가 사용되지 않을 수 있다.

P2. Attack Tree형 모델에서 작성자의 문제 이해 및 중요도 판단에 따라 서로 다른 외형의 동형 트리가 발생할 수 있다.

P3. 통일되지 않은 용어와 동형 트리 발생 가능성에 의하여 사이버 공격 모델을 검색하거나 학습, 혹은 검증 데이터로서 활용할 경우 특정 규칙에 의한 전처리가 요구된다.

P4. Attack Tree형 모델의 구조는 일반적으로 문자열을 읽는 방향과 다르므로 트리 구조에 익숙하지 않은 독자에게 효과적으로 정보를 전달하기 어려울 수 있다.

P5. 복잡도가 높은 사례의 모델은 일부 이해 당사자들의 사건 이해를 저해할 우려가 있다.

본 논문에서는 갈수록 위협적이며 복잡하게 진화하는 사이버 공격에 대항하는 방법론 중의 하나로서 보안 사고에 직면했거나 이를 예방하려는 컴퓨터 시스템의 모든 이해 당사자들이 정보를 효과적으로 교환하고 논의할 수 있도록 지원하며, 동시에 사이버 공격 모델로서 제공하는 정보의 양 및 품질을 저해하지 않는 새로운 그래프 기반 사이버 공격 모델을 제안한다.

본 논문의 이후 구성은 다음과 같다. 2장에서는 본 연구에 관련성이 있는 기존 사이버 공격 모델링 기법들과, 본 논문에서 제안하는 사이버 공격 모델에 활용되는 개념에 대하여 소개한다. 3장에서는 제안하는 사이버 공격 모델의 구조 및 모델링 작업 방법, 앞서 제시한 문제의 해결 방안에 대하여 설명한다. 4장에서는 제안하는 모델을 통하여 해결하고자 한 문제들의 실질적 효과를 확인하기 위한 타당성 검증 실험을 통하여 제안하는 모델의 기능을 평가한다. 마지막으로 5장에서는 결론 및 본 연구의 향후 연구 방향을 제시한다.

II. Related Works

1. Attack Tree

앞서 언급한 Attack Tree(공격 트리)[3]는 수많은 트리 구조의 사이버 공격 모델들의 기초가 된 트리 구조의 모델로 Bruce Schneier가 1997년에 공개하였다. 이 모델은 공격의 최종 목표를 루트 노드로 하며, 이 최종 목표로부터 이를 달성하기 위한 공격자의 행동을 하위 노드로 분할하며 사이버 공격을 표현한다. 이 모델은 트리의 깊이와 너비가 해당 공격의 복잡도를 표현하게 된다.

Attack Tree는 트리 내의 논리 구조로서 AND와 OR 연산을 사용하며, 외형이 트리 형태거나 개요 형식(outline form)으로 작성하는 것 외에는 내용 구성의 제약이 많지 않으며, 모델의 각 요소에 공격의 성공 가능성이나 공격 순서를 표기하는 등 여러 기능을 추가할 수 있다.

비록 개요 형식의 Attack Tree가 작성할 때 일반적으로 공격 행동의 순서를 표기하지만, 트리 구조로 작성할 경우 사이버 공격을 모델링하는 작업자의 우선 순위와 배경 지식, 분석하고자 하는 사이버 공격을 바라보는 시선 등의 변수에 의하여 하나의 사건을 그린 Attack Tree가 동일한 외형과 동일한 구조를 하지 않을 가능성이 존재[5]하며, 이 문제를 줄이기 위해서는 별도의 규칙을 적용하여야 한다.

2. Fault Tree Analysis

범용적인 사고 분석을 위한 방법으로서 Fault Tree 분석 방법은 표준화된 사용 방법이 존재한다.[7][8] 이 방법에서는 각 이벤트의 종류와 이벤트들을 잇는 게이트들을 지정된 문법에 따라 작성하여야 한다. 이 방법은 표준화된 문법을 통하여 작성되므로 정량적 분석 시 활용이 용이하나, 이해 당사자들이 Fault Tree 구조의 각 요소들에 대하여 숙지하여야만 이를 충분히 분석하고 적절한 의사 결정을 할 수 있다.

3. Attack-Defense Trees (ADTree)

이 모델[9]은 Attack Tree가 공격과 공격 목표가 된 시스템, 시스템의 방어 대책에 대한 상호 작용을 표현하는 기능을 추가한 Attack Tree의 파생형 모델이다. 이 모델은 Attack Tree를 기반으로 하지만 루트 노드가 공격자의 시점으로 고정되지 않고 방어자 시점으로도 작성할 수 있으며, 원형으로 표시하는 공격 노드와 사각형으로 표시하는 방어 노드를 이용하여 공격자와 방어자의 상호 작용을 표현한다. 이 모델에서 방어 노드는 트리 구조의 모든 수준에 표시할 수 있고, 각 공격 노드는 방어 노드로 이어지는 공격의 대응책 연결을 가질 수 있다. 또한, 공격 노드와 방어 노드가 서로 번갈아 가며 이어질 수도 있다. 이를 통하여 공격자와 방어자의 상호 작용을 표현한다. 이 모델은 공격자와 방어자의 상호 작용을 표현하는 기능을 추가하였으나, 이로 인해 개체 수가 증가하여 사이버 공격 사건 모델의 복잡도가 증대된다.

4. Boolean Logic Driven Markov Process (BDMP)

이 모델[10]은 Fault Tree Analysis[7][8]에서 사용하는 연산자를 Attack Tree에 차용하여 연산자 표기를 대체하고, 추가로 마르코프 연쇄 표현 및 연산 기능을 포함하였다. 연산자 기호와 공격 이벤트의 유형을 표현하는 아이콘이 사각형 안에 그려지고, 각 공격 행위에 대한 설명은 그 아래에 텍스트로 작성한 트리 구조에서, 이들 트리 구성 요소들이 실행되는 조건을 표기하는 화살표와 다음 이벤트를 지시하는 화살표로 각각의 공격 요소들을 추가로 연결하여 특정한 상태에서 미래에 어떤 공격이 발생할 것인지 파악할 수 있도록 하였다. 이 모델은 기능 추가를 위하여 추가된 트리의 각 개체를 가로지르는 화살표 및 논리 게이트의 표현 방식으로 인하여 모델의 복잡성이 증대되었다.

5. Cyber Kill Chain®

Lockheed Martin社가 개발한 하나의 공격 시나리오를 7단계로 분할하여 분석하는 이 개념은 각 공격 단계 중, 한 단계만이라도 실패한다면 해당 공격의 전체 목표가 완수되지 않는다는 개념인 Kill Chain을 사이버 공격에 맞게 이식한 사이버 공격 대응 프레임워크이자 모델링 방법이다[11]. 이 모델은 공격 과정을 총 7단계로 분류한다. 시작부터 순서대로 정찰 (Reconnaissance), 무기화 (Weaponization), 전달 (Delivery), 악용 (Exploitation), 설치 (Installation), 명령 및 제어 (Command & Control, C2), 그리고 목적 수행 (Action on Objectives)으로 구성한다. 이 모델의 핵심은 전체 공격 과정 중 어떤 단계에서 가장 효과적으로 방어할 수 있는지를 검토하고, 그에 맞춰 적재적소에 대응책을 실행하여 적은 손실로 효과적인 방어를 수행하는 것에 있다. 각 단계가 시간 순서에 따라 진행되므로 공격의 전체 개요를 파악하기 쉽다는 장점이 있다. 그러나, 이러한 비교적 단순한 구조라는 점은 한계로도 작용한다. 사건의 단계별 개요를 파악하는 데는 유용하지만, 세부 내용을 추가할 경우 충분한 구조화 없이 과도하게 많은 정보가 나열될 가능성이 있다. 또한, 이 모델은 그래픽 다이어그램 방식으로 표현하기 위한 설계가 아니기에, 정보의 접근성 문제는 전적으로 문서를 작성하는 사람의 역량에 의존한다.

6. MITRE ATT&CK®

MITRE ATT&CK®[4]은 모두가 접근할 수 있도록 공개된 사이버 공격의 전술과 기술을 집대성한 지식 베이스이다. 이는 실제 공격 사례를 바탕으로 구축되었으며, MITRE社와 참여하는 보안 커뮤니티에 의해 꾸준한 관리와 개선이 이어져 오고 있다. ATT&CK은 단순한 정보 축적 및 제공을 넘어, 이를 이용한 사이버 공격의 분류 및 활용 방법을 제시함으로써 종합 사이버 공격 대응 프레임워크 역할을 포함한다. ATT&CK 이 제공하는 공격 모델링 기법을 활용하면, 이 사이버 위협 지식 베이스에서 제공하는 공격 기술(Technique)과 공격 전술(Tactic) ID을 적극 활용하여 모델링하게 되므로 시스템의 이해 당사자 중 보안 실무자들의 정보 교환 시 정보의 기준이 되어 업무 효율의 개선이 가능할 것이다.

ATT&CK을 이용한 시각화 모델은 Attack Tree와 같은 트리 형태와 같은 공격 개념도가 아닌 14종의 전술 분류와 기술들로 구성된 표에서 각각의 공격 행동과 전체 공격 시나리오에서 사용된 기술을 표기하는 ATT&CK Matrix이다. 이것은 ATT&CK Navigator를 통하여 서비스되는 상호 작용이 가능한 웹 서비스로서 제공되며, ATT&CK Matrix은 해당 사이버 공격이 사용한 기술을 한 눈에 보기 위한 개요 및 개별 사용된 기술에 대한 링크만 제공하며, 해당 사이버 공격에 대한 설명과 참조 자료는 별도의 문서에 정리한다. 문서 [1]은 MITRE 및 ATT&CK 기여자들이 ATT&CK을 활용하여 Stuxnet 악성 코드의 정보를 분석하여 정리한 문서이며, [12]는 해당 사건의 개요를 시각화하여 보여주는 ATT&CK Matrix이다.

7. Miller's Law

Miller's Law[13]은 보통 사람은 5~9개의 객체만 단기 기억(Short-term memory)으로 기억할 수 있음을 의미하며, 해당 연구는 이를 실험 결과로 제시하였다. 피실험자들은 숫자열과 같은 정보에서 대략 7개 정도를 기억하는 경향이 있었으며, 개별 항목을 각 항목들보다 큰 단위로 묶을 경우 단기 기억의 병목 현상을 완화할 수 있음을 보였다.

8. Cognitive Load Theory

인지 부하 이론(Cognitive Load Theory)[14]는 단기 기억, 혹은 작업 기억(Working memory)의 특징으로부터 이들이 겪는 인지 부하의 종류를 파악하고, 교육 설계에 활용하여 학습 효과를 높이는 방법에 대하여 논한 이론이다. 이 이론에서는 단기 기억 혹은 작업 기억에서 Miller's Law에서 제시한 개념과 함께, 작업 기억이 정리, 비교, 처리 등의 연산 작업에도 활용되므로 사람이 동시에 처리할 수 있는 정보는 2~3종으로 제한될 것으로 예상하였다. 이를 바탕으로 효과적인 교육 설계를 위하여 제시할 정보를 보다 작은

단위로 나누어 제공하고, 시청각 자료를 활용하여 인지 부하를 줄이고 학습 효과를 높일 수 있음을 보였다.

III. Proposed Method

1. Background

Attack Tree[3]가 공개된 이후 많은 연구자들에 의해 각각의 기능 개선 시도가 있었으나, 필요한 기능의 추가, 특정 상황에 대한 공격 모델의 사용 방법의 연구가 다수를 차지하였으며 이들은 심지어 비과학적이라는 비판까지 받기도 하였다[15]. 뿐만 아니라, 앞서 이 논문에서 제기한 문제점들은 깊이 있게 다루어지지 못하였다. 또한, 사이버 공격을 체계적으로 분석하고 표현하기 위해 고안된 그래프 기반의 공격 모델링 기법들이지만 각종 매체에 공개되는 사고 보고서에서도 이러한 사이버 공격 모델이 시각화된 형태로 적극적으로 활용되는 사례는 많지 않고, 대신 필요한 경우 전체 혹은 일부분의 정보를 크게 축약한 인포그래픽의 형태로 제공되는 경우가 존재하였다[2].

Attack Tree는 개별 공격 사건이 어떠한 공격 기술을 통하여 목표를 달성하고자 하는지 분석할 수 있으나, 이 방법으로는 사건의 복잡도가 증가할수록 모델의 복잡도 또한 비례하여 증가하기 때문에 복잡도가 크게 증가한 Stuxnet[1][2] 등의 Advanced Persistent Threat에 대하여 서로 다른 배경 지식을 가진 이해 당사자들에게 충분한 정보를 제공하기 쉽지 않다. 따라서 Attack Tree의 구조에 개선 사항을 적용함과 동시에 이로 인하여 증가하는 모델의 복잡도를 D. Moody[16]에서 제시한 바와 같이 최소화하여야 한다는 결론에 도달하였다.

본 논문에서는 이러한 문제를 해결하기 위하여 복잡한 사이버 공격을 Attack Tree보다 간결하게 표현하고, 일관된 규칙에 따라 작성되도록 하여 동형 트리와 같은 사례가 발생하지 않도록 하며, 사이버 공격 모델로서의 공격 표현 능력과 정보 전달 능력, 그리고 조직의 협업 과정에서 상호 호환성을 극대화할 수 있도록 설계한 Attack Tree 구조 기반의 복합적 그래프 형 사이버 공격 모델인 Attack Forest를 제안한다.

본 모델은 다수의 고유 명칭을 사용하므로, 이들을 Table 1에 정리하였다.

Table 1. Terminology used in Attack Forest

Term	Description
Attack Forest	A cyber attack modeling framework proposed by this paper
Sapling	Sub-tree, Small tree structure describes each attack behavior
Leaves Leaf node	Sub-nodes under Sapling trees
Phase	Cyber attack phase that includes one or sequentially connected Saplings
Level of Detail	4 levels of detail preset to control amount of information
Outline form	Model as textual form
Tactic (Tactics)	Cyber attack strategies (Refers MITRE ATT&CK® Tactics)
Technique (Techniques)	Cyber attack methods (Refers MITRE ATT&CK® Techniques)
Impact	Direct damages what cyber attack inflicts to victims (Refers MITRE ATT&CK® Tactics - Impact)

2. Attack Forest

2.1 Overview of Attack Forest

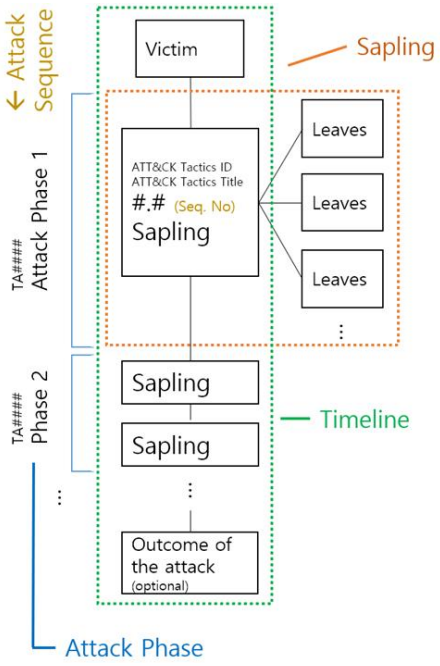

Fig. 2. Overview of Attack Forest

Attack Forest는 사건의 구성 요소들을 여러 개의 Sapling들로 분할하여 Fig. 2와 같이 시간 순서와 사건의 기승전결(起承轉結)에 따라 배치하여 사이버 공격을 표현한다. 그리고 각 공격 행위의 정보 추적성을 부여함과 동시에 참조 가능한 정보를 제공하기 위하여 각각의 공격에 대하여 해당 개체에 알맞은 ATT&CK의 사이버 공격 지식 베이스의 Tactics 및 Techniques의 ID를 찾아 표기한다. 이

러한 방법을 통하여 Cyber Kill Chain[11]이 제시하는 공격 단계의 개념과 Attack Tree가 가진 직관적인 디자인, 그리고 사건을 개요 목록으로 표기할 경우 얻을 수 있는 사건의 기승전결과 시간 순서에 따른 서술, 그리고 제공하는 정보의 추적 기능을 하나의 시각화 모델에 통합하였다.

2.2 Optimized information delivery: Level of Detail

Attack Forest는 사이버 공격 모델의 사건 서술 구조를 시간 순서에 따라 배치하도록 하고 정보의 일관성을 유지하기 위하여 지식 베이스에서 각각의 공격 행위에 대한 자세한 정보를 확인할 수 있도록 각 공격 행위에 대하여 적합한 항목의 연결을 제공한다. 단, 이 과정에서 충분한 지식을 전달하기 위하여 Attack Forest가 표현하고자 하는 사이버 공격의 규모에 따라 공격 행위를 설명하는 개체의 수가 늘어나게 된다. 이로 인하여 제안하는 모델이 앞서 소개한 'Miller's Law' [13]과 인지 부하 이론[14]에서 제시하는 정보의 단기 기억량과 처리량의 문제에 직면할 수 있으며, 이는 모델을 읽는 이해 당사자의 사건 이해 수준을 저해할 가능성이 있다. 이 문제를 완화하기 위하여 Attack Forest는 전체 모델을 특정 이해 당사자의 요구사항에 맞추어 다시 작성하는 대신, 가장 자세히 작성한 모델에서 정해진 기준에 의하여 일괄적으로 조정할 수 있도록 설계되었다. 서술되는 정보의 상세도는 기본적으로 3단계로 구분하며, 보안 실무를 수행하여야 하는 이해 당사자에게는 축약하지 않은 모델을 제공하고, 많은 정보가 과하다고 느껴질 수 있는 이해 당사자에게 요점만 제공할 수 있도록 단순화한 모델을 모든 내용이 포함된 모델에서 규칙에 의한 일괄적인 삭제를 통하여 쉽게 만들어 배포할 수 있도록 한다. 이 기능은 이후 설명할 각각의 공격 사건을 표현하는 Sapling 구조의 작성 규칙을 준수하여 모델을 작성함으로서 가능해진다.

다음 Table 2는 이 Level of Detail을 지정하기 위한 기본 규칙이다. 이 표의 Level of Detail 기준과 이해 당사자들이 별도 합의한 기준에 따라 전체 모델의 정보 밀도를 일괄적으로 조정할 수 있다. 이 규칙에 따라 Level of Detail 2~3단계는 Fig. 2의 개별 Sapling들의 하위 노드들(Leaves)을 조정하며, 0~1단계는 전반적으로 조정한다.

Table 2. Level of Detail

Level of Detail	Description
0	Attack phase, attack sequence, simplified information of attack behavior, ATT&CK Tactics ID
1	Includes all of above, ATT&CK Techniques ID, damages caused by cyber attacks within the scope of TA0040 Impact
2	Includes all of above, Objects related with attack techniques, vulnerability management ID(CVE Record ID, etc), name of other cyber attacks used in current cyber attack
3	Includes all of above, Additional details, etc

Level of Detail 규칙을 사용하여 정보의 밀도를 낮추더라도 시야에 들어오는 정보의 양이 과도하게 많은 경우 시각화 모델이 여전히 복잡하게 느껴질 수 있다. 본 모델에서는 각각의 공격 사건을 Fig. 2에 표시된 Sapling들로 구성하며, 공격의 세부 내용을 파악하기 위하여 탐색할 때에는 각 Sapling의 루트 노드에 연결되어 오른쪽에 배치된 하위 노드들을 탐색하게 된다. 이 과정 중에는 인접한 다른 Sapling들을 잠시 무시할 수 있다. 이 경우, 시선 안에 들어오는 개체의 수는 일반적으로 Miller's Law[13]의 단기 기억량 문제를 크게 상회하지 않는다.

본 모델의 시간 순서에 따른 서술 구조는 Fig. 2의 Timeline에 해당한다. 개별 사건을 나타내는 Sapling들이 위에서 아래로 시간 순서에 따라 배치하여 이를 위에서 아래로 내려오면서 읽는 구조이다. 트리 구조의 서술 방향에 익숙하지 않은 사용자가 트리를 잘못 읽을 수 있는 문제[15]가 미연에 방지된다. 이 탐색 방향의 배치를 통하여, 사람이 속한 문화권과 경험에 따라 눈의 움직임과 문서를 읽는 눈의 움직임 패턴이 영향을 받는다는 점을 증명한 연구[17] 및 언어 문화에 따라 이미지의 인식 방향 선호도가 영향을 받는다는 연구[18]의 결과를 반영함으로써 보다 자연스럽게 읽을 수 있도록 유도하여 시각화 모델로서의 사용성을 개선하고자 하였다.

2.3 Attack Sapling (Sub-tree)

사이버 공격 사건은 시간 순서에서 인접한 시기에 발생하는 여러 개의 공격 행위가 같은 전술로 대표되는 하나의 그룹으로 묶어질 수 있다. 예를 들어, 피해자의 정보를 수집하는 과정은 정찰(reconniassance)의 개념으로 묶을 수 있으며. 여기에 포함되는 공격 기술로는 피싱(phishing) E-mail, 피해자 시스템의 취약점 탐지, 피해자

의 인적 정보 수집 등이 해당한다. Attack Forest에서는 이러한 한 단위의 공격 행위를 표현하는 작은 Sub-tree 구조를 Attack Sapling, 줄여서 Sapling으로 정의한다. Attack Forest는 이 Sapling들의 루트 노드들을 사건의 시간 순서에 맞게 위에서 아래 방향으로 배치하고, 세부 정보를 포함한 하위 노드들을 오른쪽에 배치하여 정보를 습득할 시 인식해야 할 개체 수를 제한할 수 있도록 한다. 본 모델에서는 사건의 순서는 세로로 배치되며, 세부 내용은 가로로 배치되므로 특정 공격 행위의 세부 정보를 확인하는 동안 다른 단계의 타임라인 및 공격 전술을 표기하는 그래픽 구성 요소를 잠시 주시할 필요가 없도록 한다. 동시에, 왼쪽에서 오른쪽으로 읽는 문자 시스템을 사용하는 사람들의 문자 및 도표 읽기 작업 중 시선의 방향[17]에 다른 공격 행위의 정보가 시야에 들어와 단기 기억에 방해가 되는 경우의 수를 경감한다. 이를 통하여 규모가 큰 사건의 시각화 모델이더라도 한 번에 접할 수 있는 정보의 양을 적절히 제한하여 인식하도록 유도함으로써 사건의 개요 파악 및 세부 내역 파악 등의 작업 부하를 경감할 수 있도록 한다.

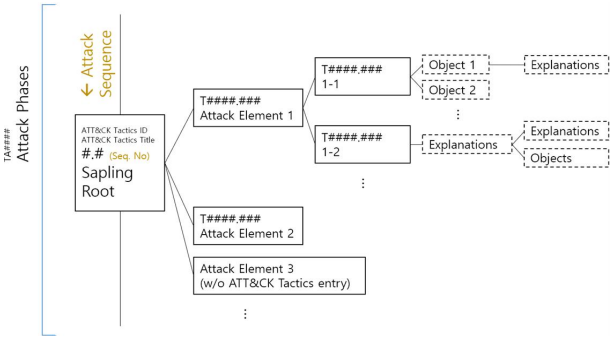

Fig. 3. Attack Sapling

하나의 공격 사건을 세부 항목으로 분할하여 Sapling으로 만들게 되며, 해당 사건의 최상위에 위치하는 개념은 Sapling의 루트 노드(Root node, 트리 구조의 최상위 개체)가 된다. 각 Sapling은 이러한 각각의 최상위 개념의 공격 요소들을 루트 노드로서 구성하며, 해당 Sapling이 가지는 전술(Tactics) ID가 하나인 경우 Sapling의 루트 노드가 아닌 그 왼쪽의 Phase에 표시한다. 만약, Sapling이 가진 Tactics ID가 공격 단계의 Tactics ID와 같은 경우 Sapling은 중복된 Tactics ID를 표기하지 않고, 중복되지 않은 Tactics ID만 표기하여 불필요한 시각적 부하가 감소하도록 한다.

Sapling 구조에서, 공격을 설명하기 위한 잎사귀 노드(Leaves, Leaf node, 하위 노드)에는 3종의 구조가 있으며, 각각 실선 사각형, 점선 사각형, 그리고 사각형 테두리가 없는 문장으로 되어 있다. 시스템 취약점의 사용, 공격 기술의 사용에 대한 정보는 실선 사각형으로 표기하며, 공격 행위의 영향을 받는 개체, 파일의 종류, 짧은 텍스트로 구성한 상세 설명의 테두리는 점선으로 표기한다. 이들보다 더 자세한 설명이 필요한 경우, 테두리와 실선 없이 해당 노드의 하위 노드의 위치에 작성한다.

각 Sapling 및 하위 노드의 공격 행위에 표기하는 공격 순서는 다음과 같이 표기한다. 순서는 1부터 시작하여 각 Sapling마다 1씩 더하여 표기하는 것을 기본으로 한다. 단, 둘 이상의 Sapling의 공격 행위들이 동시에 발동하는 공격 행위인 경우 순서 번호를 정수는 동일하게 하고 소수점 자리로 구분하며 이에 대한 서술 순서의 차이는 별도의 정의를 하지 않는 한 의미를 가지지 않는다. 예를 들어, 2.1과 2.2는 1의 다음에 동시에 실행되며 2.1과 2.2의 공격 순서의 차이는 없다. 이러한 동시 공격이 있는 경우 해당 공격 순서의 정수 번호는 사용하지 않는다. 즉, 2.1, 2.2가 존재할 때 정수 번호 2는 사용하지 않는다. 공격 순서 번호가 Sapling의 루트 노드의 하위에서 필요한 경우 루트 노드에 지정한 번호에 -를 붙여서 표기한다. 예를 들면, 2.1 하위의 1번은 2.1-1이 된다. 번호가 있는 경우 해당 번호의 순서가 공격 순서가 되며, 없는 경우 각각의 노드는 순서가 없음을 의미한다. 또한, 루트 노드의 동시 공격 순서 번호 규칙을 그대로 적용하므로 2.1-1.1, 2.1-1.2는 2.1의 1번째 순서로 둘이 동시에 실행되는 것을 의미한다. 이 명명 규칙은 본 모델에서 기본으로 사용하는 규칙이며, 필요한 경우 -를 다른 문자로 변경하되 이 변경 사항을 표기하여 혼동이 발생하지 않도록 하여야 한다.

사이버 공격 모델링 과정 및 전산 처리를 위한 데이터화에는 Fig. 3과 같은 시각화한 데이터보다 Fig. 4와 같은 텍스트 계층 구조 및 이와 유사한 형태의 데이터가 활용하기에 유리하다. Fig. 4는 Fig. 3의 Sapling 구조를 개요 형식의 텍스트 데이터로 변환한 것이다. 이 데이터 구조는 구성 요소를 유지하는 한 탭 및 띄어쓰기 문자를 사용하여 구조화한 텍스트뿐만 아니라, 객체 지향형 구조의 데이터 형식(JSON 등)으로도 구성하여 사용할 수 있다.

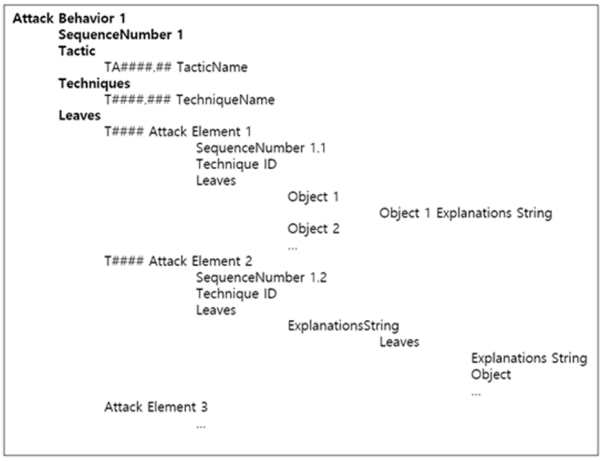

Fig. 4. Attack Sapling Outline Form

2.4 Priority of ATT&CK Tactics Tags

MITRE ATT&CK®: Design and Philosophy[4]에 의하면, ATT&CK Tactics는 Tag의 개념으로 사용되는 공격자의 전술 목표이며 하나의 행동에 부여하는 단일 분류가 아니다. 이는 하나의 공격 기술이 여러 종류의 Tactic을 포함할 수 있음을 의미하며, 이는 설계 및 적용의 오류가 아니다. 따라서 Attack Forest에서도 Tactics는 Tag의 개념으로 사용하되, 공격의 단계를 구분할 수 있도록 하기 위하여 각 공격에 ATT&CK Tactics을 지정하기 위한 규칙이 필요하다.

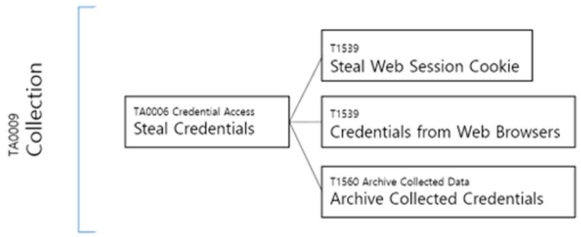

Fig. 5. Attack Sapling with two ATT&CK Tactics tags

Fig. 5의 경우 좌측의 Phase에 표기된 Tactic과 Sapling의 루트 노드의 Tactic은 그 위치를 변경하여도 의미가 변하지 않는다. 이와 같은 문제를 사전에 방지하기 위하여 Attack Forest의 시각화 모델은 Tactic 태그를 표기할 때 Fig. 6과 같은 방향으로 탐색하며 표기한다. 작성 시, Techinique 및 Tactic들을 가장 오른쪽의 말단 노드부터 왼쪽의 상위 노드로 올라가면서 작성하며 가장 좌측에 위치한 Phase의 Tactics는 직전, 직후 단계의 Sapling들과 현재 Sapling의 최종 전술이 동일한지 여부를 확인하고, 동일할 경우 Phase에 작성한다. 따라서 각 Sapling의 Tactic은 해당 공격 행동의 의미를 포함하며 그 의미가 최대한 근접한 전술이 되도록 하며, 가장 좌측의 Tactic는 공격 전반의 단계(Phase)를 표기하게 된다.

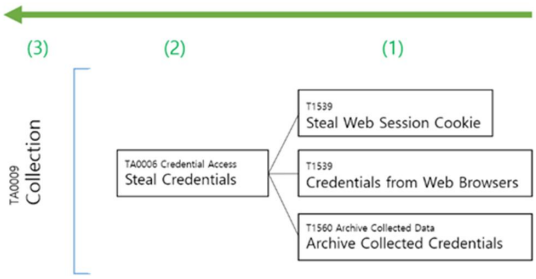

Fig. 6. Sequence to write Tactics on visualized model

2.5 Modeling Cyber Attack using Attack Forest

여기서는 사이버 공격 사건을 Attack Forest로 작성하는 방법에 대하여 설명한다. 사건을 Attack Forest로 작성하기 위하여, 각종 증거 자료 및 분석 자료로부터 사건의 순서 타임라인, 공격자가 사용한 전술, 악용한 취약점들을 확인하고, 사이버 공격 지식 베이스에 명시된 각각의 공격 행위, 전술, 기술, 해당 공격이 사용한 다른 악성 코드 등의 정보를 찾아 공격자의 공격 행위들에 연결한다. 이 정보들을 바탕으로 하여 사건의 타임라인의 개별 공격 행위를 Attack Sapling Outline Form으로 작성하고, 이들 Sapling들을 순서에 맞게 나열하여 Attack Forest Outline Form을 구축한다.

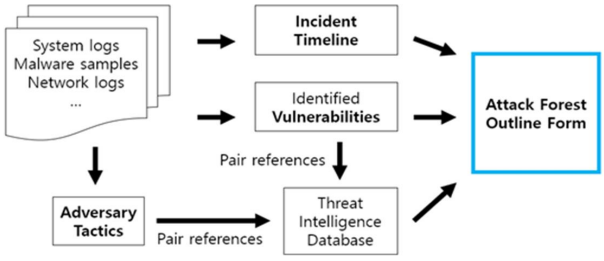

Fig. 7. Sequences to create Attack Forest from a Cyber Attack Incident

이렇게 구성한 Attack Forest는 문자열 데이터에서 시각화 과정을 거쳐 본 모델이 제공하는 모든 기능을 제공할 수 있다. 단, 시각화 전 마지막 단계로 어떠한 정보를 Level of Detail 2 및 Level of Detail 3에 추가로 지정하거나 해제할지에 대한 문제를 이해 당사자들과 협의하여 결정하여야 한다. 협의를 통하여 변동사항이 발생한 경우 합의된 규칙에 따라 Level of Detail이 조정된 개체에 별도의 표기를 추가하여 합의 사항을 알아볼 수 있도록 한다. 별도 합의를 제외하면, 이 단계에서 사용하는 기본

Level of Detail 규칙은 Table 2에서 확인할 수 있다.

이 과정을 통하여 구성한 Attack Forest는 이 모델을 읽어야 하는 이해 당사자에 맞추어 필요한 Level of Detail에 맞추어 제공함으로써 각 이해 당사자들의 단기 기억의 부하를 조절하고 필요한 정보를 충분히 제공할 수 있도록 한다. 다음 Fig. 8은 스트리밍 서비스 채널의 탈취 공격을 모델링한 Attack Forest이며, Level of Detail 2를 적용한 예제이다.

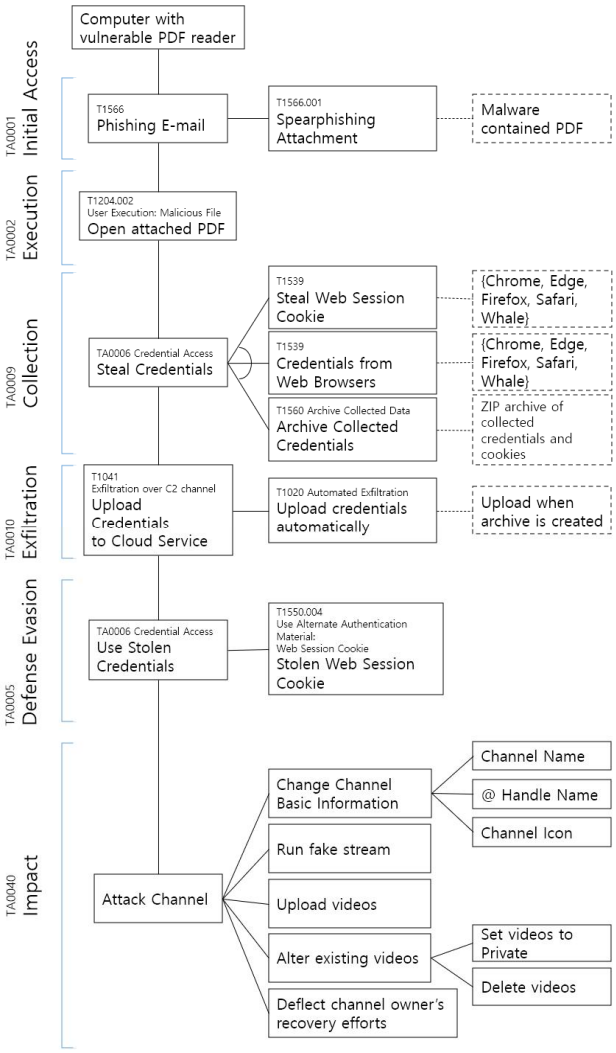

Fig. 8. Attack Forest example on Level of Detail 2

이 공격은 취약한 PDF Reader가 설치된 컴퓨터에서 피해자가 피싱 목적의 악성 이메일을 여는 것으로 시작된다. 악성코드는 PDF Reader 프로그램의 취약점을 이용하여 권한을 상승시키고, 로그인 세션 정보 등을 수집하여 C2로 사용하는 클라우드 서비스에 업로드한다. 공격자는 이를 수신한 후 스트리밍 서비스 채널에 탈취한 정보를 사용하여 계정을 탈취하여 각종 공격을 수행한다. 이 모델을 Level of Detail 1으로 표현할 경우, 이 시각화 모델에서 점선과 점선 테두리의 사각형으로 표기된 Level of Detail 2 이상의 모델에 포함되는 개체를 일괄적으로 삭제할 수 있다.

2.6 Contributions of Attack Forest

Table 3. Problems and Solutions of Attack Forest

Problem	Solution
P1. Terminology inconsistency	Resolved terminology inconsistency and provides references by referencing knowledge base entities
P2. Isomorphic trees and structural inconsistency	Apply chronological sequence and cyber attack phases to minimize inconsistency
P3. Inefficient data structure for reuse	Terminology consistencies, references, and formal outline form structure
P4. Reduced understandings by stakeholders unfamiliar with the structure of the graphic model used	Mitigated or resolved through narrative direction derived from the design of the visualization model and the optimization of the Level of Detail functionality
P5. Reduced understandings by stakeholders due to the complexity of the graphic model	

앞서 제시한 문제들을 본 모델은 다음과 같은 방법으로 해결하였다. Attack Forest는 각 공격 행위의 표기 시 해당 항목이 직접적으로 설명된 MITRE ATT&CK의 문서를 최대한 명시하도록 함으로써, 이를 통하여 정보의 표준 및 출처를 확보한다. 이에 따라 ATT&CK에서 사용하도록 한 용어를 표준 용어로써 사용하게 되므로 문제 P1이 해결된다. 사건을 시간 순서와 공격 단계를 고려하여 배치하여야 하므로 하나의 사건에 하나의 형태의 트리가 존재하도록 하며, 앞서 언급한 정보 출처 확보 및 용어 표준 확립 과정을 통하여 각 구성 요소가 통제되어 동일한 의미를 가지는 두 가지 이상의 표현이 발생하지 않아 문제 P3를 해결한다. 단, 시간 순서에 따른 사건의 배치를 사용하기에 동시에 실행되는 공격 행위의 서술 순서 차이는 발생할 수 있다. 이는 Fig. 1의 사례와 같은 동형 트리의 사례가 아닌 루트 노드의 동일 시간대 내 위, 아래의 배치만 섞일 수 있는 예외 사항이 되므로, 이는 각 소규모 트리의 데이터가 Fig. 1의 예제처럼 다른 데이터가 되지 않기 때문에, 이러한 상황에서는 영문 알파벳 순서와 같은 언어 순서로 지정하거나, 같은 시간 순서 안에서 배치 순서를 변경하여 대응할 수 있다. 따라서 앞서 해결한 문제들을 통하여 정보의 표준, 용어의 표준, 모델 구조 표준화의 달성이 가능하

므로, 문제 P2를 해결할 수 있다. 문제 P4와 문제 P5는 Attack Forest의 디자인 설계에 의한 서술 방향 및 독자의 지식 수준과 요구 사항에 맞추어 미리 지정한 기준을 통하여 간단하게 실행할 수 있는 Attack Forest의 Level of Detail 기능으로 인한 정보 제공량 최적화를 통하여 모델의 전체 재작성 과정 없이 해결 혹은 완화를 달성할 수 있을 것으로 예상하였다.

IV. Validity Verification Experiment

1. Experiment Setup

1.1 Experiment Preparation

앞서 제시한 문제 중 문제 P4와 P5를 해결하려면 Attack Forest가 다양한 사이버 보안 지식 배경을 가진 사람들에게 정확하고 충분한 정보를 제공할 수 있어야 하므로, 이를 확인하기 위하여 소수의 실험 참여자들을 모집하여 타당성 검증 실험을 수행하였다. 이 실험에서는 Attack Tree와 Attack Forest의 기능적 차이에 의한 정보 전달력, Attack Forest가 제공하는 각 기능의 실효성을 확인하고자 하였다. 이번 실험의 실험 문제와 가설은 다음 Table 4에 정리하였다.

Table 4. Experiment problems and hypotheses

Experiment Questions	Hypotheses
SQ1. Can Attack Forest improve understanding of the cyber attack case more efficiently than Attack Tree for individuals with diverse levels of computer security knowledge?	**SH1**. Attack Forest improves understanding for the cyber attack case for individuals with lower level of computer security knowledge.
SQ2. How do the sequence and layout direction of information provided by the graph model affect the reader's understanding?	**SH2**. The proposed method improves information understanding more effectively than the Attack Tree model.
SQ3. Is it possible to deliver the essential aspects of a cyber attack incident despite limiting the amount of information provided?	**SH3**. The proposed approach can deliver the essential aspects of a complex cyber attack incident even when the amount of information is limited.
SQ4. How does the variation in the amount of information provided by the graph model affect participants' understanding of the incident?	**SH4**. References from the knowledge base in the proposed method will facilitate a more detailed understanding of the cyber attack incident.

모든 참여자는 전원 본 연구와 무관한 외부 참여자 총 6명으로 구성하였다. 실험에 앞서 모든 참여자들의 대면 및 비대면 인터뷰, 설문조사를 통하여 컴퓨터 보안과 사이버 공격에 관한 배경 지식을 확인하여 결과 분석 시 활용하였다.

본 실험은 각각 복잡도 및 주제에 차이가 있는 가상의 사이버 공격 5종을 표현한 Attack Tree 및 Attack Forest 그래프 모델을 이용한다. 각 사이버 공격 모델은 다음 Table 5에서 설명한 소재를 이용하여 모델링하였다. 문항 Q1부터 Q4까지는 각각 하나의 Attack Tree와 Attack Forest를 제시하며, 여기서 사용된 Attack Forest은 모두 Level of Detail 2를 적용하였다. Q5에서는 Level of Detail 1과 Level of Detail 2를 적용한 Attack Forest을 순차적으로 제시하여 참여자들이 제출한 답안에 발생한 차이를 확인하였다.

Table 5. Virtual cyber attack cases used in the experiment

Q	Description
Q1	A malware that deletes specific files on specific date based on system clock Detection name for inspired malware: W95.CIH, Win32/Parite
Q2	Simplified malware based on Slammer worm that caused 1.25 Internet Outage in South Korea. Detection Name: W32.Slammer References: https://www.f-secure.com/v-descs/mssqlm.shtml http://www.itdaily.kr/news/articleView.html?idxno=212839
Q3	Simplified malware inspired from Stuxnet. Has capabilities to intrude air-gapped systems and cause industrial system destruction. Inspired and referenced items: [1], [2]
Q4	A cyber attack hijacks video streaming service account. Uses E-mail phishing and PDF vulnerability to use infostealer malware. References: [19], videos featuring victims sharing their experiences of this cyber attack.
Q5	Simplified WannaCry ransomware incident References: https://attack.mitre.org/software/S0366/ and references within the page above.

실험에서 Q1, Q2는 비교적 단순한 사이버 공격 사례로, 참여자에게 Attack Tree와 Attack Forest 중 하나를 먼저 제시하고 이에 대하여 참 또는 거짓인 명제 15종을 제시한다. 이후, 제시하지 않았던 다른 모델을 제시하여 일부 지문과 정답이 다른 명제 15종을 제시한다. 명제를 제시할 때, 명제의 구성은 해당 사이버 공격에 대한 명제 10종, 해당 사이버 공격을 방어하는 방법에 대한 명제 5종으로 하였다. 이를 통하여, 두 모델 중 어떤 모델을 제공받았을 때에 정보의 전달이 효과적인지, 그리고 참여자가 더 선호하는 모델을 확인한다. Q3와 Q4에서는 Q1, Q2와 유사한 난이도 및 상대적으로 복잡한 사이버 공격에 대하여

Attack Tree와 Attack Forest를 동시에 제공하고, 각각 10종의 해당 사이버 공격에 대한 명제를 제시하고, 해당 사이버 공격을 방어하는 방법에 대한 명제는 상대적으로 복잡한 사건을 소재로 한 Q3에 8종, Q4에 5종을 제시하였다. Q1부터 Q4까지는 각각 답한 후 어떠한 모델을 선호하는지, 어떠한 문제가 왜 어려웠는지를 묻는 등의 실험 참여 경험을 묻는 주관식 질문들을 통하여 추가 의견을 수집하였다. 마지막으로, Q5에서는 Attack Forest의 일괄적인 정보 제공량 조절 기능에 의한 영향을 확인하기 위하여 주관식 문제로 구성하였다.

실험에서 모든 참여자는 그래프 사이버 공격 모델의 트리 구조의 AND 조건 및 OR 조건의 하위 노드를 올바르게 이해하는 방법, Attack Tree와 Attack Forest의 구조에 대한 간략한 설명 자료를 제공받았다. 단, 제공된 정보는 각 공격 모델을 읽고 이해하는 데에 필요한 지식으로 한정하였으며, 본 실험에서 모델을 작성하는 실험 단계는 없으므로 Attack Tree 및 Attack Forest를 작성할 때에 필요한 규칙에 관한 설명은 제외하였다.

1.2 Scoring

본 실험은 Q1부터 Q4까지 해당 사이버 공격에 대한 명제에 대하여 참, 거짓, 혹은 선택할 수 없음의 3가지 선택지를 선택하는 문항으로 구성되었으며, Q5에서는 해당 사이버 공격에 대한 주관식 질문들로 문항을 구성하였다. Q1부터 Q4까지의 문항의 답안은 참과 거짓을 가리는 것과 동시에 참여자가 답안에 얼마나 확신을 가질 수 있는지를 동시에 확인하기 위하여 선택한 답안에 확신 여부를 포함하도록 하였다. Level of Detail의 차이에 의한 효과를 확인하는 실험의 Q5는 Level of Detail 1의 Attack Forest를 확인하고 1회, Level of Detail 2의 모델을 확인하고 1회씩 제공하는 모델의 정보량에 차이를 두어 동일한 문항을 2회 답변하도록 구성하여 참여자의 답안에서 차이를 확인할 수 있도록 하였다. 본 실험에서는 Q1부터 Q4까지의 모든 문항은 참 또는 거짓으로 구성하였으며, 정답은 1점, 오답은 0점으로 처리하고 확신에 대한 평가는 점수와 별도로 계산하였다. 주관식 문항은 중요한 정답 요소를 포함하는 경우 1점, 중요한 요소를 놓쳤으나 오답이 아닌 내용을 포함할 경우 0.5점, 오답인 내용이 답안에 포함되어 작성된 경우 부분 점수 없이 0점 처리하여 평가하였다.

2. Experiment Result

Table 6. Experiment Scoreboard

SE	Highest Group		High	Medium		Low	-
ID	Si	Sc	Zx	Pp	Ke	Ji	*Avg*
Q1-1	10	12	14	11	9	9	10.8
Q1-2	11	14	14	9	10	11	11.5
Q2-1	12	10	8	11	10	10	10.1
Q2-2	12	9	7	9	6	9	8.66
Q3	14	16	10	13	8	16	12.8
Q4	11	12	9	9	12	13	11
Q1-4 Sum	70	73	62	62	55	68	65
Q1-4 %	75%	78%	67%	67%	59%	73%	70%
Q5-1	5.5	7	7	6	6.5	5	6.16
Q5-2	5.5	8	8	7.5	7.5	5	6.91
Q5 Sum	11	15	15	13.5	14	10	13
Q5 %	68%	93%	93%	84%	87%	62%	81%

Table 7. Model Preferences Per Question

SE	ID	Q1 P	Q2 P	Q3 R	Q3 U	Q4 R	Q4 U
Highest	Si	AF	AF	AF	AF	AF	AF
	Sc	AF	AF	AF	AF	AF	AF
High	Zx	AF	AF	AT	AF	AT	AF
Med	Pp	AF	AF	AF	AF	AF	AF
	Ke	AF	AF	AF	AF	AT	AT
Low	Ji	AF	AT	AT	AF	AT	AT
Forest%		**100**	**83**	**66**	**100**	**50**	**66**

Table 8. Confidence Levels for each questions

SE	Highest Group		High	Medium		Low	-
ID	Si	Sc	Zx	Pp	Ke	Ji	평균
Q1-1	0	5	8	12	3	1	4.83
Q1-2	6	12	13	13	9	0	8.83
Q1-D	6	7	5	1	6	-1	4
Q2-1	4	12	11	12	7	0	7.66
Q2-2	0	10	13	14	6	0	7.16
Q2-D	-4	-2	2	2	-1	0	-0.5
Q3-C	3	16	10	18	5	3	9.16
Q4-C	5	14	15	15	11	6	11

Table 6은 객관식 및 주관식 득점과 정답률, 주관식 득점과 정답률을 정리한 평가 점수표이다. SE는 보안 관련 배경지식으로 참여자를 분류한다. Table 7에서는 문제별로 참여자가 보다 선호한 모델을 표기한다. P는 선호 조사로 Q1과 Q2에서 사용되었다, R은 읽기 쉬운 모델, U는 이해하기 쉬운 모델을 선택하도록 한 결과로 Q3와 Q4에서 사용되었다. Table 8은 참여자들이 제출한 각각의 문제에 대한 답안에 확신을 가진 수를 정리하였다. Q1-D, Q2-D

는 각각 제공하는 모델에 따라 변화한 확신 계수의 차를 표기한다.

Q1에서는 한 명의 참여자를 제외하면 Attack Forest를 제공받은 후 하나 이상의 평가 점수가 향상되었다. 반면, Q2에서는 반대로 Attack Forest로 문제를 푼 다음 Attack Tree를 제공받은 후의 정답률이 한 명의 참여자를 제외하면 1점 이상 낮아지는 결과를 보였다. 문제 Q1의 결과는 Attack Forest가 제공될 때 사건의 이해도가 증가하는 경향을 보였고, Q2의 결과는 정보량이 많아질 경우 오히려 혼란을 유발할 수 있음을 보인 Attack Tree보다, Attack Forest를 이후에 제공할 경우 이해도를 끌어올릴 수 있음을 보였으며, 이 효과는 보안 지식의 수준이 높은 참여자들과, 보안 지식의 수준이 중간 수준인 참여자 중 1명, 낮은 수준의 참여자로부터 관측되었다. Table 8과 같이, Q1에서는 1명을 제외한 모든 참여자들이 답안에 확신을 가진 비율이 증가하였고, Q2에서는 오히려 3명의 참여자가 여러 문제에서 자신의 답안에 대한 확신을 잃었다. 확신한 답안이 늘어난 사례는 2명뿐이었으며, 이들 중 한 명은 오히려 점수가 가장 낮았다. 점수가 가장 낮았던 참여자는 해당 문제에서 제시된 두 모델 모두 충분히 이해하지 못하였음을 밝혔다.

문제 Q3은 비교적 복잡한 문항이었으나, 참여자 중 보안 지식의 수준이 가장 낮았던 참여자가 최고 득점자의 결과와 동률을 기록하였다. 해당 참여자는 대부분의 답안에 확신하지 못 하였으나 제시된 사이버 공격 사건에 대한 높은 이해도를 달성하였다.

문제 Q4는 비교적 논리 구조가 단순한 사이버 공격에 대한 문제로 구성 요소의 수는 적지 않았으나 복잡하지 않았던 구조로 인하여 단순함이 드러났으며, 모델을 읽을 때 상대적으로 쉬웠던 모델로서 Attack Tree를 고른 참여자가 전체의 50% 비율을 기록하였다. 반면, 이번 문제에서 이해하기에 더 좋았던 모델링 방법의 선택에서는 2명만이 Attack Tree를 선택하였다. 해당 문항에서 Attack Tree를 선호한 참여자들은 '한 눈에 보기 편했다', '전체 구조를 빠르게 파악할 수 있었다', '복잡하지 않은 직관적인 공격 구조였으므로 추가 정보가 많이 필요하지 않았다'는 피드백을 제공하였다. Attack Forest를 선택한 참여자들은 '주요 진행 구조가 명확하다', '인과 관계나 전체를 파악할 때, 방어에 관하여 파악할 때 Attack Forest가 좋았다'는 피드백을 남겼다.

Q5에서는 Level of Detail 2 모델을 제공받은 후의 답안이 좀 더 높은 정확도를 보였는데, 이에 대하여 Level of Detail 1 모델에 이 사이버 공격 사건의 각 공격 행위의 진행을 이해하는 데에 필요한 정보가 제공되지 않았다는 피드백이 있었다. 이 문제의 사이버 공격은 다소 복잡한 구성이었으며, 이는 참여자의 보안 배경 지식이 사건의 요점을 파악하는 데에 영향이 있었음을 의미할 수 있다. 본 실험에서 참여자들에게 밝히지 않았으나, 이 문제에서 소재로 활용한 WannaCry 랜섬웨어 공격이 크게 전파되기 시작한 시점으로부터 7년 이상 경과했음에도 불구하고 한 명의 참여자가 이 문제로부터 이 사이버 공격의 이름을 유추하였다. 해당 참여자는 보안 지식의 수준이 매우 높은 참여자였다.

실험 결과로부터 시각화 사이버 공격 모델의 정확한 이해 여부, 참여자의 사이버 보안 배경 지식의 수준, 사이버 공격 사례의 복잡도는 크게 의미가 두드러지는 패턴이 존재하지 않았으며, 참여자가 문제와 그 문제의 사건에 관하여 어떠한 관심이 있고 얼마나 이해하는가에 따라 크게 차이가 발생하였음을 확인할 수 있었다. 어떤 참여자는 일반적인 사이버 보안 지식이 부족한 편이지만 복잡한 사건 중 하나에서 높은 이해도를 보이며 최고 득점과 동일한 점수를 내었으나, 상대적으로 더 높은 지식 수준을 가진 일부 참여자들은 해당 문제에서 오히려 더 낮은 점수를 기록하였다.

실험에 앞서 Table 4에서 제시한 가설에 대하여 결과와 함께 정리하면 다음과 같다. 가설 SH1은 참여자 중 가장 사이버 보안에 관한 지식을 적게 보유한 참여자가 객관식 문항에서 평균 이상의 점수를 획득하였으며, 해당 참여자가 별도로 관심이 있거나 추가적인 배경 지식을 갖추지 않은 문제에서도 점수의 차이가 발생하여 이 가설의 유효성을 확인한다. 이 점은 해당 참여자가 대부분의 답안에 확신을 가지지 못한 점이 뒷받침한다. 가설 SH2는 다음과 같은 결과와 피드백으로 검증되었다. 사건이 단순한 구조일 경우 Attack Tree를 선호하는 참여자들이 존재하였으나, 대체로 모든 참여자들이 Attack Forest를 선호하는 경향을 보였다. 각 문항별 선호 모델로서 Attack Forest를 선택한 참여자들의 피드백에 의하면, '사건의 발생 순서에 따른 서술', '주요한 사건 흐름이 명확함', '세부 정보를 원할 경우 시선의 방향을 바꾸어 확인할 수 있었음' 등을 선택한 이유로 들었으며 이는 본 모델이 제공하는 기능과 일치한다. 비교적 단순하고 직관적이었던 문제 4에서는 모델의 인식은 Attack Tree가 용이했으나, 사건을 이해하기 위하여 유용한 모델은 Attack Forest였다는 피드백이 있었다. 다음으로, 모든 참여자가 Level of Detail 1 모델을 읽고 답한 점수와 Level of Detail 2 모델을 읽고 답한 점수의 차이가 0점에서 1.5점 차이(정답 1개와 부분 점수 1개)에 그쳤으며 8개 문항 중 평균 6점 이

상의 결과를 내어 사건을 이해하기에 지장이 없었음을 보임으로 인하여 가설 SH3가 검증되었다. 마지막 가설인 SH4는 일부 참여자들에게 효과가 있었음을 확인할 수 있었다. MITRE ATT&CK® Tactics ID 및 Techniques ID를 정보 수집에 활용하였음을 명시한 참여자가 1명 있었으며, 개별 인터뷰를 통하여 수집한 추가 피드백에서 3명으로 늘어났다. 이들은 모두 보안 지식 수준이 높은 참여자들이었으며, 반면 보안 지식이 상대적으로 낮은 참여자들은 모델 그 자체에서만 정보를 습득하려고 한 경향이 있었음을 피드백 및 개별 인터뷰를 통하여 보였다.

V. Conclusions and Remarks

본 논문에서는 Attack Tree와 이의 파생형 사이버 공격 모델이 가진 용어의 통일성, 동형 트리 발생 가능성의 문제를 해결함과 동시에 시각화 모델의 정보 제공량을 자연스러운 시선의 이동 방향[17][18]과 모델에 포함될 수 있는 과다한 정보로 인한 인지 부하 문제[13][14]를 고려하여 설계한 Attack Forest를 제안하였으며, 제한된 인원의 타당성 검증 실험을 통하여 Attack Forest가 사용자의 지식 수준의 제약에 의한 영향을 최소화하고 모든 이해 당사자들이 의사 결정을 내리기 위한 충분한 사이버 공격 사건의 정보 제공을 가능하게 함을 확인하였다. 본 논문이 제시한 Attack Tree 및 이로부터 발전한 Attack Tree형 모델들의 문제점과 본 연구에서 적용한 해결 방안은 앞서 Table 3에 비교 및 정리하였다.

본 연구에서 제시하는 Attack Forest는 다음과 같은 한계점을 포함하고 있다. 본 연구에서는 MITRE ATT&CK® 프레임워크를 기반 지식 베이스로 활용하였으며, 이는 MITRE ATT&CK®의 대규모 업데이트를 통하여 발생하는 변경점이 구조의 변경을 동반할 경우 본 모델의 규칙과 충돌할 가능성이 있어 Attack Forest 규칙의 개선이 필요할 수 있다. 또한, MITRE ATT&CK의 서비스가 중단될 경우 본 모델을 활용하려면 중단되기 전의 MITRE ATT&CK의 백업 및 최신화된 정보를 별도로 준비하여야 한다. 또한, 본 모델은 작성자의 높은 전문성이 요구되며, 참조하는 지식 베이스의 정보가 불완전할 경우 이를 보완하기 위하여 작성자의 전문성이 더 크게 요구된다. 본 연구에서는 모델의 성능을 평가하기 위하여 제한된 구성원으로 타당성 검증 실험을 수행하였기에, 현업 환경에서의 성능 및 사용성을 검증하기 위한 추가적인 필드 테스트를 통하여 모델의 기능성과 실용성을 평가하고 피드백을 통하여 개선할 수 있을 것이다. 마지막으로, 본 연구에서는 과학적 이론을 바탕으로 복잡성을 완화할 수 있도록 디자인하였고, 이를 실험을 통하여 관련 지식 수준이 높지 않더라도 사건에 대한 높은 이해도를 달성할 수 있음을 확인하여 이러한 설계가 효과가 있었음을 보였으나, 본 모델과 인지 능력에 대한 과학적 분석은 이번 연구의 주요 목적 범위에 포함되지 않아 이러한 디자인이 인지 능력과 정보 습득에 주는 영향에 대한 자세한 평가가 수행되지 아니하였다. 향후 연구의 한 방향으로서, 이러한 점을 시각화 사이버 모델의 평가 및 개선에 활용할 수 있을 것이다.

ACKNOWLEDGEMENT

Seok-Won Lee's work was supported by the BK21 FOUR program of the National Research Foundation of Korea funded by the Ministry of Education(NRF5199991014091) and the Institute of Information & communications Technology Planning & Evaluation (IITP) under the Artificial Intelligence Convergence Innovation Human Resources Development (IITP-2025-RS-2023-00255968) grant funded by the Korea government(MSIT).

REFERENCES

[1] The MITRE Corporation, "Stuxnet, Software S0603 | MITRE ATT&CK®," 2020. *https://attack.mitre.org/software/S0603/*

[2] N. Falliere, L. O. Murchu and E. Chien, "W32.Stuxnet Dossier (Version 1.4)," Symantec Corporation (Broadcom Inc.), 2011. *https://docs.broadcom.com/docs/security-response-w32-stuxnet-dossier-11-en*

[3] B. Schneier, "Attack Trees," Dr. Dobb's Journal, 1999.

[4] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, MITRE ATT&CK®: Design and Philosophy, Revision v1.2, The MITRE Corporation, 2020.

[5] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," Information Security and Cryptology - ICISC 2005, 2006. DOI: 10.1007/11734727_17

[6] J. Boehm, T. Poppensieker, R. Riemenschnitter and T. Stähle, "Cyber risk measurement and the holistic cybersecurity approach," Nov. 2018. *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cyber-risk-measurement-and-the-holistic-cybers*

ecurity-approach#.

[7] E. Ruijters and M. Stoelinga, “Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools,” Computer Science Review, Vol. 15-16, pp. 29-62, Feb-May 2015. DOI: 10.1016/j.cosrev.2015.03.001

[8] International Electrotechnical Commission (IEC), “Fault Tree Analysis,” International Electrotechnical Commission, 2006.

[9] B. Kordy, S. Mauw, S. Radomirović and P. Schweitzer, “Attack-defense trees,” Journal of Logic and Computation, Vol. 24, No. 1, April 2014. DOI: 10.1016/S0167-4048(03)00313-4

[10] S. Kriaa, M. Bouissou and L. Piètre-Cambacédès, “Modeling the Stuxnet Attack with BDMP: Towards More Formal Risk Assessments,” 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), Oct 2012. DOI: 10.1109/CRISIS.2012.6378942

[11] E. M. Hutchins, M. J. Cloppert and R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Leading Issues in Information Warfare & Security Research, Vol. 1, Issue 1, p. 80, Jan 2011.

[12] The MITRE Corporation, “ATT&CK Navigator - Stuxnet, Enterprise Layer,”, *https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0603%2FS0603-enterprise-layer.json*

[13] G. A. Miller, “The magical number seven, plus or minus two: Some limits on our capacity for processing information,” Psychological Review, Vol. 63, Issue 2, pp. 81-97, 1956. DOI: 10.1037/h0043158

[14] P. Kirschner, “Cognitive load theory: implications of cognitive load theory on the design of learning,” Learning and Instruction, Vol. 12, No. 1, pp. 1-10, Feb 2002. DOI: 10.1016/S0959-4752(01)00014-7

[15] H. S. Lallie, K. Debattista and J. Bal, “A review of attack graph and attack tree visual syntax in cyber security,” Computer Science Review, Vol. 35, Issue C, Feb 2020. DOI: 10.1016/j.cosrev.2019.100219

[16] D. Moody, “What Makes a Good Diagram? Improving the Cognitive Effectiveness of Diagrams in IS Development,” Advances in Information Systems Development: New Methods and Practice for the Networked Society, 2007, pp. 481-492. DOI: 10.1007/978-0-387-70802-7_40

[17] Y. Ishii, M. Okubo, M. E. Nicholls and H. Imai, “Lateral biases and reading direction: A dissociation between aesthetic preference and line bisection,” Journal of Brain and Cognition, Vol. 75, Issue 3, pp. 242-247, April 2011. DOI: 10.1016/j.bandc.2010.12.005

[18] F. Abed, “Cultural Influences on Visual Scanning Patterns,” Journal of Cross-Cultural Psychology, Vol. 22, Issue 4, pp. 525-534, Dec 1991. DOI: 10.1177/0022022191224006

[19] J. Luna, “Linus Tech Tips' YouTube channels were hacked due to a session hijacking attack - Neowin,” Mar 24, 2023. *https://www.neowin.net/news/linus-tech-tips-youtubechannels--were-hacked-due-to-a-session-hijacking-attack/*

Authors

Jae-Ho Lee received a B.S. degree in Computer Science from Yong In University, Korea, in 2016. He received a M.S. degree in Computer Engineering at Ajou University, Korea 2025.

His research interests are computer security, software engineering, and artificial intelligence.

Seok-Won Lee is currently a Full Professor and Chair in the Dept. of Software & Computer Engineering and Dept. of Applied Artificial Intelligence, and Vice President for International Affairs at Ajou University, Republic of Korea since 2012. Before his move to Korea, he was a faculty member at the University of North Carolina at Charlotte, University of Texas at San Antonio, and a research staff at IBM T.J. Watson Research Center. His areas of specialization include software engineering with specific expertise in ontological requirements engineering and domain modeling, and knowledge engineering with specific expertise in knowledge acquisition, machine learning and knowledge-based systems, and information assurance with specific expertise in software security & privacy. He has published more than 250 peer reviewed articles. He is a professional senior member of IEEE, ACM and AAAI.