https://doi.org/10.33778/kcsa.2021.21.1.093

# 지능형 사이버 공격 경로 분석 방법에 관한 연구★

김 남 욱*, 이 동 규*, 엄 정 호**


## 요 약

지능형 사이버 공격으로 인한 피해는 시스템 운영 중단과 정보 유출뿐만 아니라 엄청난 규모의 경제적 손실을 동반한다. 최근 사이버 공격은 공격 목표가 뚜렷하며, 고도화된 공격 도구와 기법을 활용하여 정확하게 공격 대상으로 침투한다. 이러한 지능적인 사이버 공격으로 인한 피해를 최소화하기 위해서는 사이버 공격이 공격 대상의 핵심 시스템까지 침입하지 못하도록 공격 초기 또는 과정에서 차단해야 한다. 최근에는 빅데이터나 인공지능 기술을 활용하여 사이버 공격 경로를 예측하고 위험 수준을 분석하는 보안 기술들이 연구되고 있다. 본 논문에서는 자동화 사이버 공격 경로 예측 시스템 개발을 위한 기초 메커니즘으로 공격 트리와 RFI 기법을 활용한 사이버 공격 경로 분석 방법을 제안한다. 공격 트리를 활용하여 공격 경로를 가시화하고 각 공격 단계에서 RFI 기법을 이용하여 다음 단계로 이동할 수 있는 경로를 판단한다. 향후에 제안한 방법을 기반으로 빅데이터와 딥러닝 기술을 활용한 자동화된 사이버 공격 경로 예측 시스템의 메커니즘으로 활용할 수 있다.


# A Study on Mechanism of Intelligent Cyber Attack Path Analysis

Nam-Uk Kim*, Dong-Gyu Lee*, Jung-Ho Eom**


## ABSTRACT

Damage caused by intelligent cyber attacks not only disrupts system operations and leaks information, but also entails massive economic damage. Recently, cyber attacks have a distinct goal and use advanced attack tools and techniques to accurately infiltrate the target. In order to minimize the damage caused by such an intelligent cyber attack, it is necessary to block the cyber attack at the beginning or during the attack to prevent it from invading the target's core system. Recently, technologies for predicting cyber attack paths and analyzing risk level of cyber attack using big data or artificial intelligence technologies are being studied. In this paper, a cyber attack path analysis method using attack tree and RFI is proposed as a basic algorithm for the development of an automated cyber attack path prediction system. The attack path is visualized using the attack tree, and the priority of the path that can move to the next step is determined using the RFI technique in each attack step. Based on the proposed mechanism, it can contribute to the development of an automated cyber attack path prediction system using big data and deep learning technology.


**Key words : Intelligent Cyber Attack, Cyber Attack Path, Attack Tree, RFI, Path Prediction**

접수일(2021년 01월 19일), 수정일(1차: 2021년 03월 12일), 게재확정일(2021년 03월 22일)

★ 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019R1F1A1041782).

* 성균관대학교 컴퓨터공학과 박사과정

** 대전대학교 군사학과&안보융합학과 교수(교신저자)

# 1. 서 론

2020년도 사이버 공격 유형 중에 코로나-19와 관련된 이슈를 악용한 지능형 사이버 공격이 증가하였다. 사이버 공격자는 공격 대상 시스템에 침투하기 위해서 사용자가 가장 관심을 갖고 있는 화제나 언론에서 주요하게 다루는 이슈를 이용하여 악성코드를 유포하는 지능적인 방식을 활용하였다. 사용자가 부지불식간에 악성코드가 삽입된 첨부파일을 다운로드 받아서 실행할 경우에 사용자의 정보가 해커에게 넘어가게 된다[1,2].

최근 사이버 공격의 양상을 살펴보면, 해커들은 뚜렷한 공격 목표를 갖고 지능화된 공격 도구와 기법을 활용하여 정확하게 공격 대상으로 침투하여 공격 목적을 달성한다. 이 과정에서 공격 대상 시스템에 설치된 보안 프로그램의 탐지로부터 벗어나기 위해서 고도화된 공격 기법으로 경로를 재설정하기도 한다. 점점 교묘해지는 지능형 지속 공격(APT: Advanced Persistent Threats)을 현재의 보안기술로는 탐지하기가 쉽지 않으며, 일단 공격을 받게 되면 시스템의 운영 중단과 정보 유출로 인해서 엄청난 경제적인 손실도 동반하게 된다. 최근에는 인공지능 기술을 활용하여 사이버 공격 경로와 의도를 공격 초기에 식별하여 공격을 차단하는 지능형 보안 시스템이 개발되고 있으며, 공격 진행 중에 탐지하여 핵심 공격 대상까지 침투하지 못하도록 차단하는 첨단 보안기술이 개발되고 있다[3-7].

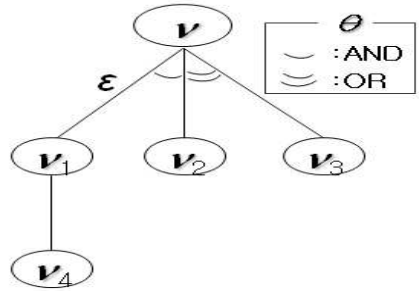
본 논문에서는 인공지능과 빅데이터를 활용한 자동화 사이버 공격 경로 예측 및 차단 시스템을 개발하기 이전에 예측 기술의 기초가 될 수 있는 경로 분석 방법을 제안하고자 한다. 제안한 방법은 공격 트리를 통해서 지능형 사이버 공격을 가시화하고 RFI 기법을 적용하여 공격 단계별로 이벤트 발생 값을 산출하여 공격 경로의 우선순위를 결정할 수 있도록 하였다. 논문 구성은 2장에서 관련 연구를 살펴보고 3장에서 제안한 방법을 설명한다. 4장에서는 APT 공격 시나리오를 이용한 실험을 하고, 5장에서 결론을 맺는다.

# 2. 공격 트리와 RFM 모델

## 2.1 공격 트리(Attack Tree)

Bruce Schneier가 제시한 'Attack Tree'[8]는 보안 위험평가, 접근제어, 침입탐지 기법 등 다양한 보안 분야에서 활용되고 있다. 공격 트리는 사이버 공격 절차에서 시작부터 최종 목표까지 공격 이벤트가 실행하는 것을 단계별로 트리 형태로 가시화할 수 있다. 최근에는 사이버 보안 기술에도 적용되고 있다. 예를 들어, 사이버 공격 절차를 단계별로 묘사하면, 각 단계에 따라 보안 기술을 매칭하여 공격의 최종 목적을 달성하지 못하도록 공격 과정에서 차단이 가능하다[9].

공격 트리는 아래 그림처럼 사이버 공격의 이벤트가 처음으로 실행하는 최하위 노드(Leaf Node)부터 각 공격 단계를 나타내는 중간 노드(Internal Node), 그리고 최종 공격 목표인 루트 노드(Root Node)로 구성된다. 공격 트리에서 동일 단계에서 반드시 실행해야 할 노드들은 'AND' 조합으로 구성하고 노드 실행을 선택적으로 할 수 있도록 'OR' 조합으로 구성된다. 공격 트리의 구조는 정점($\nu$), 앳지($\varepsilon$), 조합($\theta$)으로 이루어진다. 정점($\nu$)는 공격 이벤트나 공격 목적을 나타내는 노드들의 집합이고 앳지($\varepsilon$)는 자식 노드에서 공격 이벤트를 실행하여 부모 노드로 전이되는 상태들의 집합을 나타낸다. 조합($\theta$)은 공격 실행에 필요한 공격 이벤트를 선택할 수 있는 조건을 의미한다. 공격 트리 표현식은 Attack Tree = ($\nu$, $\varepsilon$, $\theta$)와 같다[10].




(그림 1) 공격 트리(Attack Tree)

사이버 공격 방식이 고도화되고 복잡해짐에 따라 이러한 사이버 공격을 표현하기에 'OR'와 'AND' 조합으로 구성된 초기의 공격 트리는 한계에 부딪혔다.

그래서 'AND' 조합에서 공격 이벤트가 반드시 순서대로 발생하게 하는 순차 조합이 추가되거나 변형된 공격 이벤트가 발생할 경우에 예비 노드를 추가하여 결합시키는 조건 조합이 추가된 확장 공격 트리도 나타났다[11].

### 2.2 RFM 모델

RFM(Recency, Frequency, Monetary) 모델[12,13]은 백화점에서 주요 고객을 효과적으로 관리하기 위해서 3가지 지표인 시기, 빈도, 가치를 기준으로 주요 고객으로 분류하고 구매 가능성이 높은 고객을 선정하기 위한 데이터 분석 모델이다. 현재에는 마케팅 분야에서 주요 고객관리, 환자관리, 주문관리 업무에서 많이 사용되고 있는 분석 방법 중 하나이다. RFM 모델의 고객의 가치를 다음과 같은 3가지 요소로 평가한다.

- Recency(거래 시기): 고객이 최근에 언제 제품을 구입하였는가?
- Frequency(거래 빈도): 고객이 얼마나 자주 제품을 구입하였는가?
- Monetary(거래 가치): 고객이 구입한 제품의 가격은 어느 정도인가?

RFM 모델의 결과값은 위 3가지 요소의 곱으로 산출하되, 각 요소의 중요도에 따라 가중치를 부여하여 RFM의 최종 결과값을 도출한다.

- $RFM = a*R + b*F + c*M$ (1)
- $RFM\ Score = (RFM*100)/N$ (2)

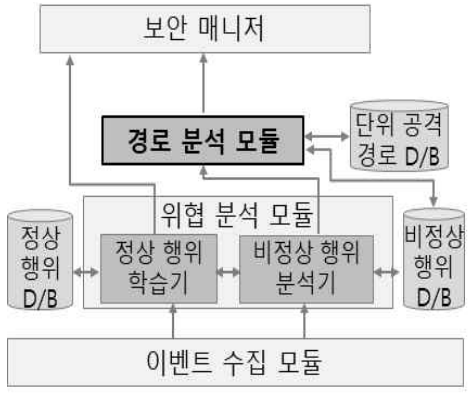
수식 (1)에서 a, b, c는 각 요소의 가중치를 의미하며, 일반적으로 시기, 빈도, 가치 순으로 큰 가중치를 부여하는데, 적용하는 방식에 따라 다를 수 있다. 수식 (2)에서 N은 세분화된 그룹 수를 의미한다. RFM 모델의 계산 방식은 Matrix Scaling 기법으로 요소별 각 5등급으로 나누어 점수를 부여하며, 3가지 요소를 비교하여 중요도에 따라 사용자가 가중치를 적용하기도 한다.

본 논문에서는 RFM 모델의 구성 요소 중에 거래 가치 대신에 사이버 공격으로 인한 피해 영향(Impact)으로 교체한 RFI 모델을 적용한다.

## 3. 사이버 공격의 경로 분석 방법

### 3.1 사이버 공격 경로 예측 시스템의 프레임워크

사이버 공격 경로 예측 시스템은 아래 그림과 같이 이벤트가 발생하면, 위협분석 모듈에서 비정상 행위 분석기를 통해서 비정상 행위 이벤트를 추출한 후 경로 분석 모듈에서 이후의 공격 경로를 분석/판단하여 사이버 공격이 핵심 시스템까지 침입하지 못하도록 차단하는 시스템이다[6].




(그림 2) 경로 예측 시스템의 프레임워크

이벤트 수집 모듈은 네트워크와 시스템에 설치된 감시 에이전트로부터 수집한 데이트를 종합하여 위협 분석 모듈로 전송한다.

위협 분석 모듈은 정상 행위 학습기와 비정상 행위 분석기로 구성된다. 정상 행위 학습기는 전송받은 이벤트를 정상 행위 DB를 참조하여 정상 행위 여부를 판단하고 새로운 정상 이벤트일 경우에는 자동학습을 통해서 정상 행위 범위를 확장하여 DB에 저장한다. 비정상 행위 분석기는 정상 행위 DB에 저장된 이벤트와 비교 분석하여 비정상 행위로 의심되는 이벤트를 추출하고 이를 그룹화하여 비정상 행위 DB에 저장한다.

경로 분석 모듈은 비정상 행위 분석기로부터 전송받은 의심 이벤트를 단위 공격 경로 DB를 참조하여 공격 트리로 공격 경로를 가시화하고 RFI 기법을 통해서 공격 진행 가능성이 높은 경로를 판단한다.

### 3.2 사이버 공격의 경로 분석 프로세스

사이버 공격 경로 예측 시스템에서 핵심 모듈은 공격 경로 분석 모듈로 프로세스 아래 그림과 같이 실행한다.


(그림 3) 경로 분석 모듈의 프로세스

이벤트 연관성 분석은 비정상 행위 DB에 저장된 비정상 이벤트 그룹을 바탕으로 이벤트가 발생한 순서와 각 이벤트들의 연관성을 분석한다. 그리고 각 비정상 이벤트 그룹에는 위험 수준과 공격 가능성에 따라 우선순위를 설정하며, 비정상 행위 DB에 저장된 비정상 행위 그룹들과의 연관성 분석을 통해 특정 비정상 행위 그룹에 속하는지 판단한다.

이벤트 진행 경로 가시화는 이벤트 연관성 분석을 통해 확인된 비정상 행위를 단위 공격 경로 DB와 매칭시킨다. 만약, DB에 없는 비정상 행위 그룹이라면, 새로운 그룹을 생성하여 저장한다. 공격 경로 가시화는 공격 트리를 이용하여 인과적/시간적 순에 따라 그래프 형태로 표현된다.

단계별 이벤트 진행 경로 예측은 그래프 형태로 표현된 이벤트들의 진행 경로와 동일한 단계에서 발생할 할 수 이벤트들의 발생 우선순위를 결정한다. 우선순위는 앞서 설명한 RFM 모델의 변형 모델을 이용하여 산출한다. 본 논문에서는 RFM 모델에서 거래 가치 요소 대신에 NIST의 위험관리 가이드[14]에서 제시한 위협분석 요소인 영향(Impact)을 적용한다. 즉, 공격을 받았을 때 네트워크나 시스템에 발생하는 피해 영향을 사용한다[15]. 변경된 모델은 RFI 모델로 구성 요소는 다음과 같다.

- Recency(발생 시기): 이벤트가 최근에 발생한 시기는?
- Frequency(발생 빈도): 이벤트가 얼마나 자주 발생하였는가?
- Impact(피해 영향): 이벤트 발생으로 인한 피해 영향은 어느 수준인가?
- $RFI = a*R + b*F + c*I$ (3)

사이버 공격 경로는 경로 가시화와 RFI 값을 기반으로 차후 이벤트가 진행할 가능성이 높은 경로들을 예측한다. 공격 경로 예측은 최종 공격 목표까지 침입하지 못하도록 공격 진행 단계에서 차단하기 위한 목적을 갖고 있다.

## 4. 사이버 공격의 경로 분석 실험

### 4.1 APT 공격 시나리오

최근에 지능형 공격을 대표하는 공격 방식은 APT 공격이다. 그래서 제안한 분석 방법의 실험은 APT 공격 시나리오[6]를 기반으로 공격 경로를 판단한다.

<표 1> APT 공격 개요

| |
|---|
| • 목적 및 대상 : 정보 유출 / 서버<br><br>• 공격 절차<br>① 사전정찰 : Search Engine이나 Crawler, Social Network 등을 활용<br>② 1차 침투 : (P1&P2) \| (P5&P2) \| (P3&P4)<br>③ 은닉 및 정보수집 : (S1 \| S2 \| S3 \| S4 \| S5)&(G1 \| G2 \| G3 \| G4 \| G5)&((S1 \| S2 \| S3 \| S4) & ( G6 \| G7 ))<br>④ 권한 획득 : (A1 \| A2 \| A3 \| A4 \| A5) |

<표 1>의 공격 절차에서 이벤트가 발생하는 시점은 ①부터이지만, 본 논문에서는 실질적으로 공격이 이루어지는 ②부터 실험에 활용한다. <표 1>의 1차 침투부터 권한 획득 단계까지의 이벤트는 다음과 같다.

<표 2> APT 공격 절차의 이벤트

〈Penetration Methods〉
P1 : Spear-phishing email with malicious link
P2 : Drive-by Download
P3 : Spear-phishing email with malicious attachment
P4 : Malicious cod installation through software vulnerability
P5 : Water Hole attack

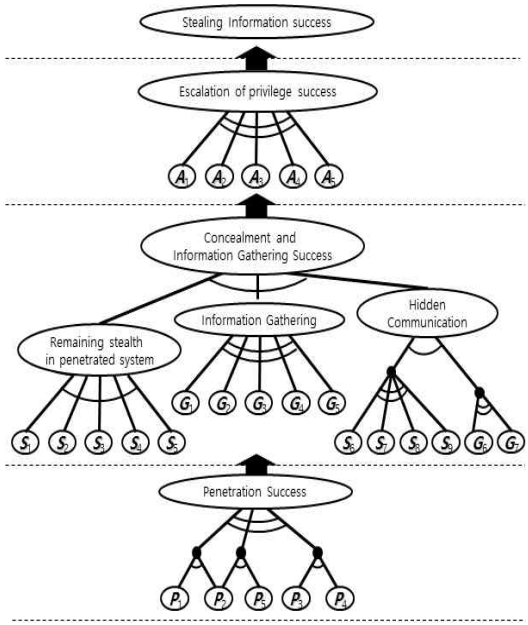
〈Concealment& Hidden Comm. Methods〉
S1 : Logic bomb
S2 : Rootkits
S3 : Binary packing
S4 : Polymorphic malware
S5 : Fileless malware
S6 : Network Fast Flux
S7 : Encrypted Communication
S8 : Anonymous Communication
S9 : Covert Communication

〈Information Gathering Methods〉
G1 : Port Scanning
G2 : Vulnerability Scanning
G3 : Service Scanning
G4 : Host Scanning
G5 : Directory Guess
G6 : Backdoor
G7 : C&C Communication

〈Privilege Escalation Methods〉
A1 : Dictionary / Brute force attack
A2 : Key Logging
A3 : Screen Capture
A4 : Man-in-the Browser
A5 : Directory/File Search

## 4.2 공격 경로의 가시화 및 예측

<표 2>를 참고하여 APT 공격을 공격 트리로 표현하면 다음 그림과 같다. 이러한 공격 트리는 사이버 공격 경로 예측 시스템에서 단위 공격 경로 DB에 저장된다. 공격 트리는 공격 경로를 가시화하는데 가장 유용한 방법으로 공격 진행을 쉽게 알 수 있다.




(그림 4) APT 공격 트리

단계별 이벤트 진행 경로의 판단은 앞서 설명한 바와 같이 RFI 모델을 이용한다. 이때, 공격 트리에서 'AND' 조합으로 구성된 이벤트(노드)들은 모두 발생해야 하기 때문에 RFI 결과값을 산출할 필요가 없고 'OR' 조합으로 구성된 이벤트만 RFI 결과값을 산출한다.

우선 RFI의 요소들의 판단 기준은 다양한 방법으로 결정할 수 있으며, 본 논문에서는 Matrix Scaling 기법으로 판단 기준을 정한다. 예를 들어 발생 시기(R)와 빈도(F)는 아래 표와 같이 선정할 수 있다.

<표 3> 발생 시기와 빈도 값 선정 기준

| R값 | 발생 시기(T) | F값 | 발생 빈도(월) |
|---|---|---|---|
| 1 | 5M≤T | 1 | 1〈N |
| 2 | 1M≤T〈5M | 2 | 1≤N〈3 |
| 3 | 1W≤T〈1M | 3 | 3≤N〈5 |
| 4 | 24H≤T〈1W | 4 | 5≤N〈10 |
| 5 | T〈24H | 5 | 10≤N |

위의 표에서 발생 시기는 월, 주, 시간 단위로 기준을 정했으며, 발생 빈도는 월 단위로 이벤트의 발생 숫자로 기준을 설정하였다. 하지만, 머신러닝과 빅데

이터 기술을 활용하여 메커니즘을 구현할 경우에는 기준만 정해주면 학습을 통해서 자동적으로 설정이 가능하다.

피해 영향(I) 값은 과거 피해 사례를 경제적 손실로 환산한 금액으로 기준을 설정할 수도 있으며, 정성적인 방법으로 선정할 수도 있다. 예를 들어 정성적인 방법으로 시스템이 조직에서 얼마나 중요한가를 기준으로 설정한다면 다음 표와 같이 설정할 수 있다.

<표 4> 피해 영향 값 선정 기준

| I값 | 중요도 |
|---|---|
| 1 | 사이버공격을 받았을 때나 오류가 발생할 경우에 복구가 바로 가능하고 즉시 대체 자산으로 바꿀 수 있으며, 업무에 거의 영향을 받지 않음. |
| 2 | 사이버공격을 받았을 때나 오류가 발생할 경우에 확인 절차가 필요하며, 업무 진행에 차질(지연, 변경 등)을 초래할 수 있음. |
| 3 | 사이버공격을 받았을 때나 오류가 발생할 경우에 업무 진행이 잠시 중지되고 조직에 상당한 손해를 초래할 가능성이 있음. |
| 4 | 사이버공격을 받았을 때나 오류가 발생할 경우에 업무 진행이 상당기간 중지되고 조직에 현저한 손해를 초래할 수 있음. |
| 5 | 사이버공격을 받았을 때나 오류가 발생할 경우에 업무가 정지되고 조직에 치명적인 손해를 초래할 수 있음. |

가중치는 일반적으로 사이버 공격의 심각 수준이나 위협 평가를 진행할 때, 빈도와 피해 영향을 주요한 요소로 판단하기 때문에 본 실험에서도 빈도와 피해 영향에 가중치를 높게 하고 빈도와 피해 영향 중에는 피해 영향에 가중치 값을 높게 부여한다[14]. 가중치도 머신러닝 기반으로 구현할 경우에는 기존의 데이터를 활용하여 학습함으로써 자동적으로 산출이 가능하다. 본 실험에서는 방법의 적용 방안을 증명하는 것에 중점을 두었기 때문에 위협 평가 요소를 고려하여 피해평가, 빈도, 시기 순으로 가중치를 부여하였다.

- $RFI = 1*R + 2*F + 3*I$ (5)

공격 예상 경로를 판단하기 위해서 우선, 1차 침투 단계에서 5개의 이벤트 중에서 각 2개씩 'AND' 조합으로 구성되어 3개의 이벤트 그룹이 생성되었다.

Penetration Success(PS)={P1,P2,P3,P4,P5}

$PS_1$={P1∧P2} / $PS_2$={P1∧P2} / $PS_3$={P1∧P2}

$PS_{EG}$={$PS_1$, $PS_2$, $PS_3$}

1차 침투에서 이벤트 그룹 중에서 발생 가능성이 높은 경로를 예측하기 위해서는 각각의 이벤트들의 RFI 값을 산출한다.

예를 들어, 스피어 피싱 링크나 이메일을 자주 사용하고 다음으로 드라이브 바이 다운로드를 사용하며, 피해도 악성코드 파일이 첨부된 스피어 피싱에 의한 감염이 가장 크고, 한 달 이내에 발생한 사례가 있다고 가정하고 R 값을 3, F 값을 3, I 값을 4로 선택해서 RFI 값을 산출하면 다음과 같다.

RFI($PS_1$)=*1*3 + 2*3 + 3*4 = 21*

동일한 방식으로 PS2과 PS3의, R, F, I 값을 선택하여 RFI 결과값을 구한다면 다음과 같다.

RFI($PS_2$)=*1*2 + 2*2 + 3*3 = 15*

RFI($PS_3$)=*1*3 + 2*2 + 3*4 = 19*

위의 1차 침투의 이벤트 그룹별로 RFI 값을 비교했을 때, PS1의 값이 21로 가장 크기 때문에 PS1={P1∧P2}이 발생 가능성이 높은 경로로 예측할 수 있다.

각 공격 진행 단계별로 RFI 값을 위의 방식으로 산출할 수 있다. 단, 하위 단계에서 판단된 이벤트 경로와 차상위 단계에서 이벤트들간의 상관관계를 반드시 고려해야 한다. 만약에 하위 단계를 고려하지 않고 각 공격 단계별로 이벤트 진행 경로를 판단할 경우에는 하위 단계와 차상위 단계 이벤트간의 연관성이 낮아져서 공격 경로를 제대로 예측할 수 없다.

계속해서 은닉 및 정보 수집 단계에서 정보 수집은 G1이 선택되고 숨겨진 통신에서는 S7과 G6이 선택되었다고 가정하면, 다음과 같이 표현이 가능하다.

Remaining Stealth(RS)={S1∧S2∧S3∧S4∧S5}

Information Gathering(IG)={G1}

Hidden Comm.(HC)={S7∧G6}

Concealment and Information Gathering(CIG)={RS∧IG∧HC}

CIG={S1∧S2∧S3∧S4∧S5∧G1∧G6}

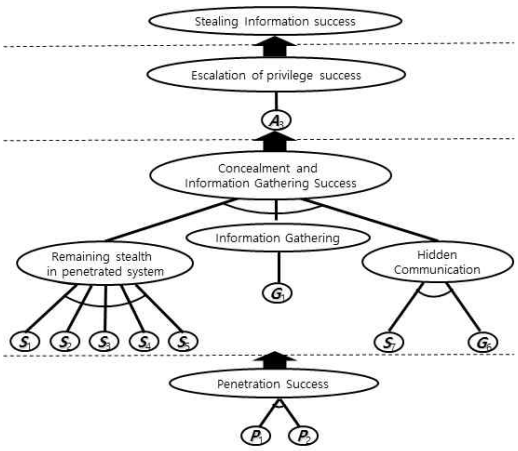
권한 획득 단계에서는 A4가 선택되었다고 가정하면, Escalation of Privilege(EP)={A4}가 된다.

APT 공격의 다양한 경로는 Path of APT={PS∧CIG∧EP}으로 표현할 수 있다. 본 논문에서 제시한 방식으로 예측한 공격 경로를 종합해 보면 다음과 같다.

$P_{APT}$={$PS_1$∧RS∧IG∧HC∧EP}

$P_{APT}$={(P1∧P2)∧(S1∧S2∧S3∧S4∧S5)∧G1∧S7∧G6∧A4}

위의 표현식을 공격 트리로 묘사하면 아래 그림과 같다.




(그림 5) APT 공격의 예측 경로

제안한 방법으로 공격 경로를 예측하면, RFI 값과 하위단계와 차상위단계의 연관성 분석 결과에 의해서 다양한 공격 경로 중에서 발생 가능성이 높은 공격 경로를 판단할 수 있다. 사이버 공격 발생 이전이나 공격 초기에 공격 경로를 예측할 수 있다면, 공격 경로에 맞게 대응책을 적용함으로써 공격 피해를 최소화할 수 있게 된다.

## 5. 결 론

4차 산업혁명 기술과 접목한 사이버 공격 기법은 점점 고도화되고 첨단화되고 있다. 이러한 공격 양상을 차단하고 탐지하기에는 기존의 보안 기술로는 어렵다. 그래서 보안 기술에도 이러한 지능형 사이버 공격을 탐지하기 위해서 인공지능 기술을 접목시키고 있다. 사이버 공격을 공격 발생 이전에 예측하고 탐지하기는 쉽지 않다. 그래서 사이버 공격으로 인한 피해를 최소화하기 위해서 핵심 시스템까지 침투하지 못하도록 공격 초기나 중간 단계에서 차단해야 한다.

본 논문에서는 핵심 목표 시스템까지 침입하지 못하도록 공격 초기나 중간 단계에서 차단할 수 있도록 공격 경로를 분석하고 예측하는 방법을 제안하였다. 우선, 공격 트리를 이용해서 공격 절차를 가시화하고 RFI 기법을 적용하여 각 공격 단계별 동일 단계에서 다양한 공격 경로 중에서 발생 가능성이 높은 경로를 판단할 수 있도록 하였다. 각 공격 단계에서 다양한 방식으로 공격을 진행할 수 있기 때문에 이 모든 경로를 차단하는 것은 쉽지 않다. 그래서 가장 발생 가능성이 높은 공격 경로를 판단하여 우선적으로 대응하는 것이 피해를 최소화할 수 있다. 본 논문에서는 제안한 메커니즘의 적용 방법을 중심으로 다루었다. 차후 연구에서는 이러한 메커니즘을 머신러닝 기법에 접목하여 자동화 공격 경로 예측 시스템 개발하고자 한다.

## 참고문헌

[1] “코로나19 금융부문 사이버 위협 동향”, 금융보안원, 2020.

[2] 김홍준, 엄정호, "코로나19 대응을 위한 책임 있는 디지털 기술의 활용 방안", 융합보안논문지, 20(3), pp.99-108, 2020.

[3] 국경완, 공병철, “인공지능을 활용한 보안기술 개발 동향”, 정보통신기획평가원 주간기술동향 1913호, pp.2-15, 2019.

[4] Jung ho Eom, "Modeling of Cyber Attack Intentions Analysis reflecting Domestic / International Situations", International Journal of Control and Automation, 11(2), 2018.

[5] 권혁천, 이용준, 박원형, "한국의 사이버공격 비교 분석과 정책적 대응방안", 융합보안논문지, 20(5), pp.19-26, 2020.

[6] 김남욱, 엄정호, “APT 공격 탐지를 위한 공격 경로 및 의도 인지 시스템,” 디지털산업정보학회 논문지 16(1), pp.69-80, 2020.
[7] 이종관, 문미남, 신규용, 강성록, "공개출처정보의 정량화를 이용한 인공신경망 기반 사이버위협 예측 모델", 융합보안논문지, 20(3), pp.115-123, 2020.
[8] B. Schneier, “Attack Trees," Dr. Dobb's Journal, 24(12), pp.21-29, 1999.
[9] 김남욱, 엄정호, "A situation-Flexible and Action-OrientedCyber Response Mechanism against Intelligent Cyber Attack", 디지털산업정보학회 논문지, 16(3), pp.69-80, 2020.
[10] 엄정호, “공격트리를 이용한 위협평가방법에 관한 연구”, 보안공학연구논문지 9(1), pp.45-52, 2012.
[11] 엄정호, “능동적인 사이버 공격 트리 설계-애트리뷰트 접근”, 정보보호학회논문지 21(3), pp.67~74, 2011.
[12] 구수연 외 2명, “RFM 모델을 활용한 No-Show 방지 모바일 예약 플랫폼”, 한국정보과학회 학술발표 논문집, pp.33-35, 2016.
[13] 이영호 외 2명, “RFM 모델 기반의 병원고객 세분화 전략”, 정보과학회논문지:기술교육 2(1), pp.25-33, 2005.
[14] NIST, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, 2001.
[15] 엄정호, “SFI 분석 기법을 이용한 내부자 활동 수준의 정량적 평가”, 보안공학연구논문지 10(2), pp.113-122, 2013.

## [저 자 소 개]

엄 정 호 (Jung-Ho Eom)
1994년 2월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
2011년 3월~현재 대전대학교 군사학과&안보융합학과 교수
email : eomhun@gmail.com

김 남 욱 (Nam-Uk Kim)
2009년 2월 성균관대학교 컴퓨터공학과 학사
2012년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2012년 3월~현재 성균관대학교 전기전자 및 컴퓨터공학과 박사과정
email : nukim8275@gmail.com

이 동 규 (Donggyu Lee)
2016년 8월 성균관대학교 소프트웨어학과 학사
2016년 9월~현재 성균관대학교 전자전자컴퓨터공학과 석박사 통합과정
email : raymondlee@skku.edu