https://doi.org/10.33778/kcsa.2024.24.2.189

국방 임무 종속성을 고려한 핵심 자산 도출 방안 연구★

김 준 석*, 엄 익 채**

요 약

최근 국방 기술의 발전은 인공지능이 탑재된 드론과 같은 첨단 자산의 도입으로 디지털화되고 있다. 이러한 자산들은 산업용 사물 인터넷, 인공지능, 클라우드 컴퓨팅 등의 현대 정보기술과 통합되어 국방 영역의 혁신을 촉진하고 있다. 그러나 해당 기술의 융합이 사이버 위협의 전이 가능성을 증가시키고 있으며, 이는 국방 자산의 취약성을 증가시키는 문제로 대두되고 있다. 현재의 사이버 보안 방법론들이 단일 자산의 취약점에 중점을 두는 반면, 임무 수행을 위해서는 다양한 군사 자산들의 상호 연동이 필요하다. 따라서 본 논문은 이러한 문제를 인식하고, 임무 기반의 자산 관리 및 평가 방법론을 제시한다. 이는 임무 수행에 중요한 자산을 식별하고, 사이버 보안 측면에서의 취약점을 분석하여 국방 부문의 사이버 보안성 강화를 목표로 한다. 본 논문에서는 임무를 수행하기 위한 기능과 자산 간의 연계분석을 통해 임무 종속성을 분류하며, 임무에 영향을 미치는 자산을 식별 및 분류하는 방안을 제안한다. 또한, 공격 시나리오를 통해 핵심 자산 식별 사례연구를 수행했다.

A Study on the Assessment of Critical Assets Considering the Dependence of Defense Mission

Kim Joon Seok*, Euom Ieck Chae**

ABSTRACT

In recent years, the development of defense technology has become digital with the introduction of advanced assets such as drones equipped with artificial intelligence. These assets are integrated with modern information technologies such as industrial IoT, artificial intelligence, and cloud computing to promote innovation in the defense domain. However, the convergence of the technology is increasing the possibility of transfer of cyber threats, which is emerging as a problem of increasing the vulnerability of defense assets. While the current cybersecurity methodologies focus on the vulnerability of a single asset, interworking of various military assets is necessary to perform the mission. Therefore, this paper recognizes these problems and presents a mission-based asset management and evaluation methodology. It aims to strengthen cyber security in the defense sector by identifying assets that are important for mission execution and analyzing vulnerabilities in terms of cyber security. In this paper, we propose a method of classifying mission dependencies through linkage analysis between functions and assets to perform a mission, and identifying and classifying assets that affect the mission. In addition, a case study of identifying key assets was conducted through an attack scenario.

Key words : Military Cyber Asset, Risk Assessment, Mission-based Risk Assessment, attack surface

접수일(2023년 10월 24일), 수정일(1차: 2024년 01월 17일), (2차: 2024년 04월 25일), 게재확정일(2024년 04월 30일)

★ 이 논문은 전남대학교 학술연구비(과제번호:2020-1952)지원에 의하여 연구되었음

★ 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된연구임(IITP-2022-0-01203)

* 전남대학교/정보보안융합학과(주저자)

** 전남대학교/데이터사이언스대학원(교신저자)

1. 서 론

정보기술(IT)의 진보는 6G를 지향하는 통신 기술의 발달로부터 비롯되며 이는 빅데이터, 인공지능, 클라우드, IoT와 같은 첨단 기술들과 함께 4차 산업 혁명을 선도하고 있다. 군사 분야 또한 이러한 기술들을 적극적으로 통합하며, 센서 기반의 의사결정 지원 시스템, 전술 통신, 정밀 타격 능력 향상 등 다양한 분야에서 IT의 적용을 확대하고 있다[1]. 이를 바탕으로 한 성능 개선 연구가 활발히 진행 중이다.

그러나 IT 기술의 채택은 사이버 보안이라는 복합적인 문제를 수반한다. 사이버 보안 위협은 IT 제품의 취약점을 통해 발생하며, 이는 악성코드, 랜섬웨어, DDoS 공격 등의 형태로 나타날 수 있다. 이러한 위협들은 IT 시스템의 신뢰성과 직결되어, 적절한 보안 관리가 필수적이다[2].

하지만 국방 분야에서는 임무 중심의 사이버 자산을 평가하는 방안이 부족한 실정이다. 따라서 임무 중심의 군사 자산 보안성을 강화하는 데 목적이 있다.

본 논문은 국방 장비의 사이버 보안을 위해 임무 중심의 접근 방법을 제안한다. 해당 접근법은 임무 수행에 결정적인 자산을 식별하고, 임무 영향성을 분석하여 사이버 보안의 우선순위를 결정하는 방식으로 구성된다. 해당 과정을 통해 임무 수행에 있어 문제가 될 수 있는 자산을 미리 식별함으로써, 임무 수행에 영향을 미칠 요소들을 효과적으로 파악할 수 있다.

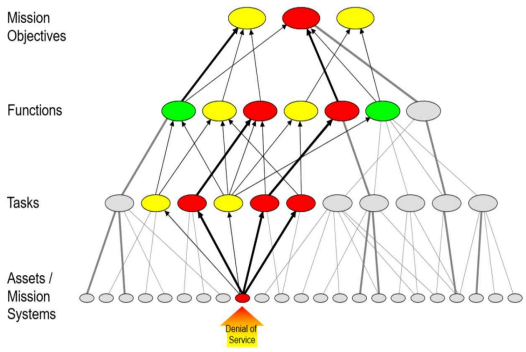
임무 영향성은 임무 수행에 필수적인 자산들의 가용성과 신뢰성을 확보하는 데 중점을 둔다. 특히 군사 자산의 경우, 보안성 확보는 인명 피해 방지 및 작전 수행 능력의 유지와 직결되는 중대한 요소이다.

본 논문은 임무 영향성 평가를 위한 체계적인 방안을 개발하고, 이를 통해 국방 장비의 사이버 보안을 강화하는 방향으로 연구를 진행한다. 서론에서는 임무 영향성 평가의 필요성과 관련된 선행 연구를 검토하며, 본론에서는 임무 영향성 평가를 위한 방법론을 상세히 설명한다. 이후 시나리오 기반 검증을 통해 방법론의 적용성을 평가하고, 결론에서는 연구 결과를 요약하고 향후 연구 방향을 제시한다.

2. 관련 연구

본 장에서는 임무 종속성 및 임무 영향도에 관한 연구 동향을 분석하고, 이를 본 논문에서 제안하는 평가 방안에 적용할 수 있는 기술들을 살펴본다. 또한, 기존 연구들의 한계점을 식별하고, 이를 바탕으로 제안하는 방안에 대해 설명한다.

2.1 핵심 자산 분석 방법론(Crown Jewels Analysis, CJA)



(그림 1) 핵심 자산 분석 방법론 구조도

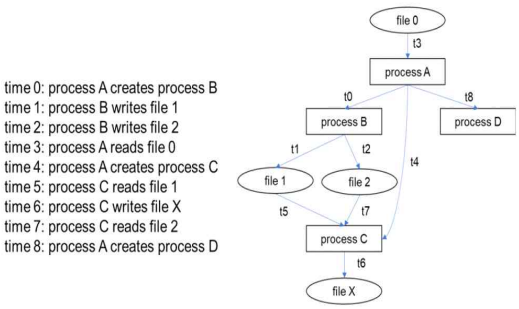
핵심 자산 분석 방법론(Crown Jewels Analysis, CJA)은 조직의 핵심 임무를 성공적으로 수행하는 데 중요한 사이버 자산을 도출하기 위한 체계적인 접근법을 제공한다[4]. 해당 방법론은 우선하여 조직의 주요 임무 목표를 규명하며, 이후 해당 임무를 유지 및 운영하기 위한 기능들을 상세히 분석한다. 그 과정에서 해당 기능들을 지원하는 필수 정보 및 사이버 자산을 선별하는 단계로 이어진다. 해당 분석을 통해 조직에 있어 필수적인 자산들이 도출된다.

(그림 1)에서 제시된 바와 같이, 각 자산 간의 상호 연결성을 시각화하여, 조직의 사이버 공간 내에서 임무 수행에 결정적인 역할을 하는 자산들을 명확히 식별하도록 한다.

본 논문에서는 임무, 기능 및 자산을 구조화하기 위한 방법론으로 CJA를 활용한다.

2.2 프로세스 데이터 종속성 구성 방안

2.2.1 출처 그래프(Provenance graph)



(그림 2) 출처 그래프

출처 그래프는 (그림 2)과같이 호스트 내의 개체(entity) 간 데이터, 정보 및 제어 흐름을 표현한 그래프이다[5]. 그래프의 노드는 개체를 표현하며, 프로세스는 주체(subject) 개체이며, 프로세스를 제외한 파일, 소켓 등은 객체(object) 개체이다. 그래프의 엣지는 주체 개체와 객체 개체 간의 흐름 또는 의존성을 나타내기 때문에 출처 그래프를 의존성 그래프라고도 한다.

출처 그래프를 이용하여 공격을 추적할 수 있는데 이 중 역방향 분석은 공격을 탐지한 이벤트와 관련한 개체 노드로부터 역으로 탐색하여 공격의 진입 지점을 식별하는 과정이며, 정방향 분석은 역방향 분석을 통해 식별한 공격의 진입 지점으로부터 출처 그래프를 추적하여 공격의 모든 영향 및 종료 지점을 식별하는 과정이다.

출처 그래프를 이용하여 이벤트 간의 인과관계를 분석하여 공격을 탐지하기 위한 다양한 연구가 진행되었다. 관련 연구를 종합하면 출처 그래프를 이용하여 APT 공격을 실시간으로 탐지하거나, 그래프를 이용한 이벤트 간 인과관계 분석을 통하여 공격 사후 침해사고를 분석하거나 추적하는 연구가 지속적으로 진행되고 있다[6].

본 논문에서는 부모/자식 프로세스 관계를 구성하기 위해 출처 그래프를 활용한다. 프로세스 연결성을 확인한 후 연계된 자산을 도출하는 방안으로 활용한다.

2.2.2 Sysmon

공격 발생의 증거로 다양한 보안 경고 도구를 활용해 수집할 수 있다. 본 논문에서는 알려진 취약점을 기준으로 해당 증거를 수집한다.

Sysmon은 마이크로소프트에서 제공하는 관련된 이벤트의 생성 및 로깅을 통해 네트워크 활동을 모니터링하기 위해 Windows 기반 도구이다. Sysmon의 이벤트 로거를 사용하여 원격 호스트의 작업을 모니터링할 수 있으며, Sysmon은 기존의 윈도우 이벤트 로그의 제한된 보안 로그를 확인할 수 있다. 프로세스 생성, 네트워크 연결 등 이벤트를 확인 가능하며, 활동 추적하여 이상 행위를 탐지할 수 있다.[7]

추출한 해쉬를 이용하여 평판 조회 사이트에서 악성코드 여부를 조회하여 확인할 수 있으며, 파일, 프로세스, 네트워크 생성, 수정, 삭제 등 변화를 이벤트로 식별되고, 필터링을 적용할 수 있다.

본 논문에서는 프로세스 호출 경로를 파악하기 위해 Sysmon을 활용하며, 연구 범위는 Window 운영 체제를 활용하는 자산을 대상으로 본 연구를 수행했다.

2.4 선행 연구 비교

본 절에서는 임무 영향 분석에 대한 선행 연구를 분석하여 비교한다. 핵심기반시설, 국방 및 IT 환경 등 다양한 분야에서 시행된 임무 영향 선행 연구 자료를 분석하고 한계점 및 연구 방향을 설명한다.

Olga Carvalho 외 연구진은[8] 핵심기반시설 영향 평가 방안을 개발했다. 핵심기반시설 영향 평가는 도구 및 표준들과 쉽게 통합될 수 있도록 개발되었다.

해당 방법론은 임무 지향 평가 모델을 기반으로 공격 영향력 전파 시뮬레이션 플랫폼을 설계하고, 원하는 위협 환경의 시뮬레이션에 의해 잠재적으로 영향을 받는 비즈니스 프로세스를 탐지하기 위한 상향식 계산 방법론을 제안했다.

Pranavi Appana 외 연구진은[9] 임무 영향도를 추적하기 위해 공격 그래프 생성기인 MulVAL을

활용한다. 임무 의존성 정보, 서비스 의존성 정보 및 공격 정보를 입력하여 생성한다. 순위 생성 프로세스는 두 단계로 제안했다.

1단계서는 일반적으로 .dot 파일인 추적 파일을 Perl 스크립트를 사용하여 구문 분석한다. 출력은 노드, 유형 및 종속성과 같은 정보로 구성된 텍스트 파일이다.

2단계에서는 파싱된 .txt 파일이 자바 프로그램으로 구현되는 순위 알고리즘의 입력으로 전송된다. 자바 프로그램은 노드들 사이의 의존성을 인접 매트릭스로 변환할 것이다. 정점 가중치뿐만 아니라 외부 이웃과 각 정점의 이웃에 따라 자산 순위 접근법을 기반으로 순위를 계산한다.

Alexander Motzek 외 연구진은[10] 임무에 미치는 영향을 평가하는 것은 지속적으로 관찰해야 하는 문제이며 알고리즘을 통한 임무 영향 평가 접근 방식은 잘못된 결과가 나올 수 있다고 설명했다. 임무 영향 평가를 위한 공식적이고 수학적인 모델을 제공한다. 확률론적 모델을 기반으로 임무 영향 평가를 수학적 문제로 줄이고 데이터 수준에서 검증했다.

Xiaoyan Sun 외 연구진은[12] 임무 영향 평가를 위해 베이지안 네트워크를 기반으로 한 확률론적 접근법을 제안한다. 베이지안 네트워크를 설정하고 시스템 객체 또는 임무 작업이 침해된 것과 같은 관심 이벤트의 확률을 추론하는 방식을 제안했다.

Laurin Buchanan 외 연구진은[12] 의사 결정자는 사이버 자산이 중요한 임무와 비즈니스 프로세스를 실행할 준비가 되었는지 알고 있어야한다고 제안한다. 네트워크 운영자는 장애가 발생한 네트워크 자산(예: IP 주소, 네트워크 서비스, 애플리케이션)에 의존하는 사람과 영향을 받는 데이터의 흐름을 파악해야 하고, 이를 위해서는 네트워크 자산과 이에 의존하는 중요한 작업의 연결성 분석이 필요하다고 제안했다.

앞서 분석한 선행 연구들의 특징으로는 위험 관리 측면에서 업무 연속성 문제를 달성하고자 각 분야에 맞도록 연구가 선행되었다. 본 논문의 연구 범위인 국방 분야 역시 임무 지속성을 중점으로 연구를 수행했다.

세부적인 평가 기준은 크게 임무 보증, 자산 중요도, 출처 그래프를 활용했다는 점이다.[11] 임무 보증은 사이버 보안의 기본 지표인 기밀성, 무결성, 가용성 중 임무 지속성을 고려하여 가용성에 초점을 맞춰 임무 보증이라는 요소가 도출되었다. 자산 중요도는 '2.1 핵심 자산 분석 방법론'에서 명시된 것과 같이 임무 지속성을 달성하기 위해 핵심 자산의 중요도를 도출한다. 마지막으로 출처 그래프는 자산 하위의 프로세스 및 시스템 호출 단위의 연결성을 파악할 수 있는 그래프로 중요한 요소로 도출되었다. 다음 <표 1>은 선행 연구들에 대한 비교·분석표이다.

<표 1> 임무 영향도 선행 연구 분석

Paper	Mission Assuarance	Asset Criticality Based	Provenance Graph Based
[8]	O	O	X
[9]	X	O	X
[10]	X	X	X
[11]	X	X	O
[12]	X	X	O
[13]	X	X	O

하지만 기존 연구들은 자산의 취약점 및 공격 경로에 관한 연구가 중심적으로 진행되었다. 임무 보증에 중심을 두고있지 않아 실제로 임무에 영향을 주는 자산 단위를 파악하는 것이 필요한다.

임무, 기능, 자산의 임무 종속성에 대해 연결된 자산의 단일 취약점 혹은 공격 침입 탐지에 중점을 두어 평가한다. 하지만 단일 취약점이나 공격 침입 탐지로 본 논문의 임무 수행에 영향을 미치는 자산을 파악하는 것과 차이가 있다. 우선순위로 평가할 수 있는 자산을 구분하는 것은 어려움이 있다.[14]

본 논문에서는 단일 취약점 및 사이버 공격에 의한 위험도를 평가하는 것이 아닌 관리 우선순위에 있는 자산을 평가하는데 중점을 둔다.

3. 임무기반 핵심 자산 평가 방안

본 논문에서 평가하는 임무 영향성이란 앞서 설명한바와 같이 사이버 공격으로 임무에 미치는 영향을 평가하는 것이다.

사이버 공격은 해당 조직의 업무에 영향을 미치게된다. 이는 곧 '임무에 영향을 미친다.' 라고 해석되며, 임무에 미칠 수 있는 영향을 미리 파악하는 것이 중요하다. 본 연구에서는 임무 영향성을 평가하기 위해 임무를 수행하기 위한 기능 및 자산간의 종속 관계를 정의한다.

다음 (그림 3)는 제안하는 임무기반 핵심 자산 평가 방안이다. 사이버 공격에 의한 임무 영향을 분석하기 위해 3단계의 과정을 통해 임무 영향도를 파악한다. 1단계는 시스템 개체 종속성 그래프이다. 2단계는 임무 연결성 분석으로 앞서 도출된 시스템 개체 종속성 그래프를 이용하여 서비스가 제공되는 지점을 연결하는 단계이다.

마지막 단계에서는 생성된 임무 종속성 구조도를 활용하여 영향 평가를 수행하는 단계이다. '정상 상태'와 '비정상 상태'로 나누어 임무 종속성 구조상 '비정상 상태'와 연결되는 자산들을 관리 대상으로 식별한다.

3.1 임무-기능-자산 종속 관계 정의

본 절에서는 임무, 기능 및 자산 간의 관계를 정의하는 방안에 대해 설명하는 단계이다.

3.1.1 임무-기능-자산 정의

해당 프로세스를 수행함에 앞서 임무, 기능, 자산을 정의해야 한다. 국방부 아키텍쳐 프레임워크는 목적은 각 프레임워크 산출물의 정의와 목적을 설명하고, 산출물을 상세하게 제시하는 데에 있다[15].

해당 절차에서 임무란 조직단위 또는 부대에 부여된 주요 과업으로 정의된다. 기능은 해당 임무를 수행하기 위한 기술적 수단을 의미하며 자산은 해당 기능을 수행하기 위한 단말기를 의미한다.

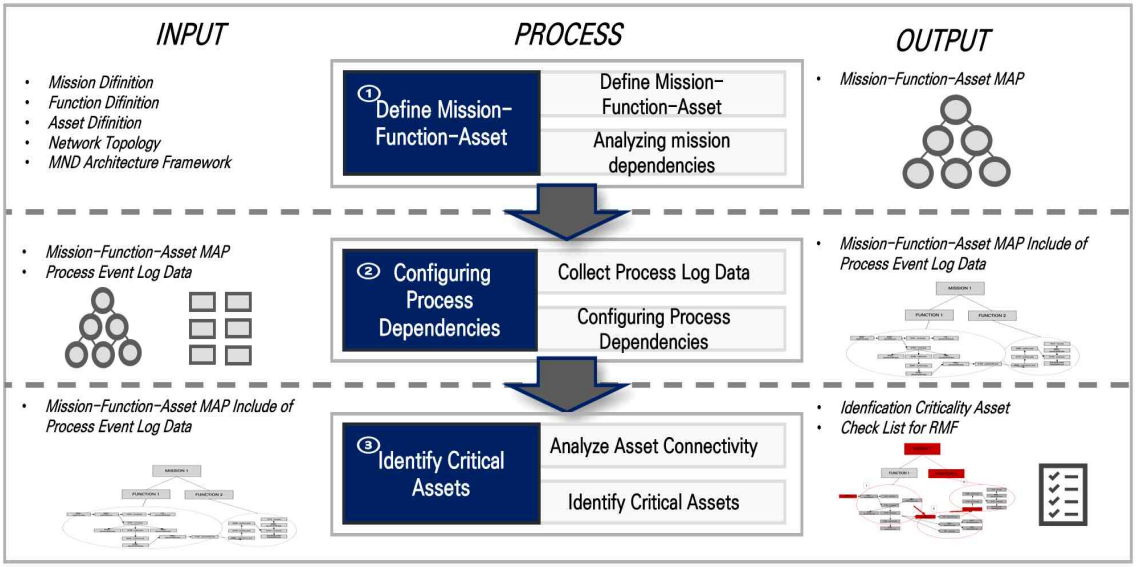
3.1.2 임무 종속성 분석

임무 종속성은 임무를 수행하기 위한 각 기능 및 자산과 연결시키는 것이다. 해당 작업을 수행하기 위해서 3계층으로 나누어 수행한다. 임무 종속성 그래프는 임무, 기능, 자산을 구조화한 그래프로 임무와 관련된 모든 기능 및 자산을 추상화한 것이다.

본 논문에서는 핵심 자산 분석 방법론(CJA)를 활용하여 임무 영향 평가를 수행한다.

기존 임무-업무-기능-자산 4가지 계층이 아닌 임무-기능-자산 계층으로 구성하여 해당 임무와 연관된 자산을 분류하는 작업을 가장 먼저 실시한다.

기존 CJA의 4가지 계층이 아닌 3가지 계층을 활용한 업무와 기능의 경계가 모호함에 있다. 핵심 자산 분석 방법론에서 업무 '특정 임무나 비즈니스 목표를 수

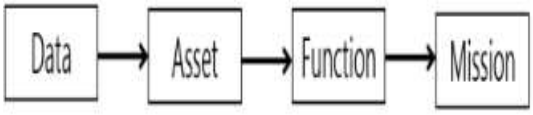


(그림 3) 임무기반 핵심 자산 평가 방안

행하기 위해 필요한 활동' 로 정의하고 있으며, 기능(Function)은 '특정 임무나 비즈니스 목표를 달성하기 위한 일련의 작업'으로 정의하고 있다.

자산을 활용하여 임무 수행의 활동 및 작업을 세분화하는 것보다 본 논문에서는 특정 자산에 해당하는 임무 파악을 중점으로 두기 때문에 임무-기능-자산 3계층으로 설정하여 절차를 진행한다.

임무 종속성 구성은 시스템 개체를 임무 및 기능과 연결하는 것이다. 앞서 설명한바와 같이 기존 핵심 자산 분석 방법론을 활용하여 임무 종속성을 하향식으로 구성할 때, 각 임무 및 기능에 대한 아키텍처 요구사항이 정확해야한다.



(그림 4) 임무 연결성

다음 (그림 4)는 임무 연결성을 표현한 도형이다. 시스템 개체 종속성 관계를 정의하면서 종속되는 구조를 알 수 있었다. 개별 개체가 아닌 네트워크에 속해 있는 모든 관계를 정의하여 최종적으론 자산, 기능, 임무에 도달하게 된다.

임무 연결성이 구성된 후에는 잠재적으로 침해된 자산을 식별하기 위해 정방향 또는 역방향으로 추적할 수 있다. 공격으로 인해 보안 센서에서 경보가 발생할 수 하는 경우 관련된 시스템 개체를 침해당한 프로세스로 간주하여 트리거 지점으로 사용할 수 있다.

예를 들어, 무결성 점검 도구의 점검 결과에서 특정 파일이 비정상적으로 수정되었다는 경고를 표시하는 경우 해당 파일을 트리거 포인트로 간주 할 수 있다. 따라서 시스템 개체 출처 그래프에서 파일은 침해당한 것으로 표시된다.

3.2 프로세스 종속성 구성

본 절차에서는 3.1 임무-기능-자산 정의로 구성된 임무 종속성 구조도 및 프로세스 데이터를 이용하여 자산 하위 계층인 프로세스 데이터 흐름에 대한 연결성을 분석하는 단계이다.

3.2.1 프로세스 로그 데이터 수집

시스템 개체 간의 상호 작용을 통해 공격을 통한 침입이 발생 시 다른 개체로 전파 될 수 있다. 일반적으로 침입은 공격자가 직·간접적으로 생성하거나 주입한 서비스 프로그램이거나 바이러스와 같은 손상된 파일로 시작된다. 이후, 시스템 호출 과정을 통해 다른 시스템 개체와 상호작용하여 다른 개체에도 영향을 미치게되는 침입 전파과정을 가지게된다. 해당 절차에서는 프로세스 단위의 로그 데이터를 분석한다.

로그 데이터 분석 절차에서는 Sysmon을 활용해 자산에서 수행된 프로세스 로그 이벤트를 수집하는 것으로 시작한다. 해당 데이터를 분석하여 단위공격을 탐지하는 과정으로 수집/저장된 이벤트를 활용한다.

3.2.2 프로세스 종속성 구성

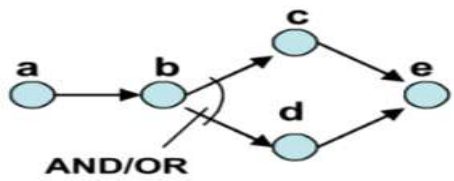
프로세스 기반 인과관계는 동일 호스트에서 발생하는 데이터를 분석한다. 프로세스 연결성을 확인하여 부모/자식 프로세스를 연결함으로써 해당 과정으로 어떤 명령어를 주입하였고 최종적으로 어떤 자산에 영향을 미치는지 확인할 수 있다[16].

시스템 개체 종속성 관계 구성은 앞서 설명된 시스템 호출 구문 분석과 시스템 호출 도형을 이용하여 종속성 관계를 나타낼 수 있다.

(그림 5)는 프로세스의 순차 흐름을 나타낸다. 임무는 흐름도에서 설명하는 순서대로 실행되는 이러한 모든 단계에 따라 달라진다. 흐름도에는 병렬 분기가 포함될 수 있다.

(그림 5) 프로세스 순차 흐름 관계

(그림 6)은 시스템 개체 종속성 관계를 AND 또는 OR 노드로 정의할 수 있다. AND 노드는 두 분기가 모두 실행되어야 하는 반면 OR 노드는 적어도 하나의 분기를 수행해야 한다.



(그림 6) AND/OR 흐름 관계

시스템 개체 종속성 그래프에서 기능을 추출한 다음 임무와 연결하는 상향식 방법을 제안한다. 시스템 개체 종속성 그래프에서 실제로 일어나는 데이터 및 제어 흐름을 반영하므로 정확한 식별이 가능하다.

다음 (그림 7)은 해당 절차에서 연결성을 분석하는 임무, 기능 및 자산의 구조를 나타내며, 임무 종속성 구조에 사용되는 엣지를 구조화한 것이다. 해당 과정을 통해 타 자산으로 명령 및 제어 기능을 수행하는 프로세스의 경우 핵심 프로세스 데이터로 정의해야한다.

시스템 내부의 문제가 있더라도 전파가 되지 않는다면 피해가 최소화되어 고려하지 않을 수 있지만 타 자산으로 연계가 된다면 직·간접적인 피해를 줄 수 있다고 판단한다.

3.3 사이버보안 측면 위험 관리 대상 도출

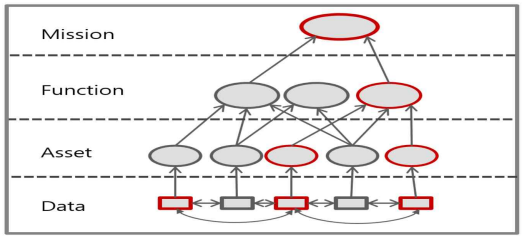
본 절에서는 임무 종속성 구조도를 통해 '정상 상태'와 '비정상 상태'에 있는 자산들을 분석하고, 이를 기반으로 최종 평가를 수행하는 단계이다. 특히, '비정상 상태'에 있는 자산들을 중점적으로 살펴보며, 이들 중 임무 수행에 중대한 영향을 끼칠 가능성이 있는 핵심 자산들을 선별하는 과정이다. 해당 과정은 임무 종속성 구조상 자산 간 연결성을 이해하고, 잠재적 위협으로부터 우선적으로 보호해야 할 자산들을 명확히 식별하는 데 중점을 뒀다.

결과적으로 해당 자산들을 위험 관리의 주요 대상으로 식별하여, 전체 시스템의 안정성을 강화하고, 임무 수행의 연속성을 보장하기 위해 우선 관리가 필요한 자산으로 식별된다[17].

'정상 상태'는 사이버 공격 시 임무에 영향을 미칠 수 있는 기능 및 자산으로 분류되지 않는다. 반대의 경우'비정상 상태'는 사이버 공격에 의하여 임무에 영향을 미칠 수 있는 기능 및 자산으로 분류된다.

3.3.1 자산 연결성 식별

3.2 프로세스 종속성 구성 단계에서 식별된 핵심 프로세스 데이터와 임무 종속성 관계를 활용하여 타 자산에 영향을 미치는 자산의 연결성을 식별해야한다. 임무-기능-자산-프로세스 데이터 간 연계 분석을 통해 프로세스 단위부터 임무 단위까지 상향식 방식으로 '비정상 상태'을 확인할 수 있다.



(그림 7) 임무 종속성 및 관리 대상 식별 방안

3.3.2 사이버보안 측면 위험 관리 대상 식별

앞서 구성한 시스템 종속성 관계를 활용하여 침입 탐지 이벤트 목록을 통합하여 임무에 직·간접적으로 영향을 미치는 자산을 목록화 할 수 있다. 해당 목록을 통해 자산 관리 수행하기 앞서 우선순위가 되는 자산 목록을 도출하고, 본 논문에서는 개별 자산의 중요도는 모두 같은 조건에 있다는 명시하에 임무 영향성 평가를 마친다.

4. 임무기반 핵심 자산 평가 사례연구

본 장에서는 임무 영향성 평가 사례 연구를 수행한다. 드론 탐지 체계의 공급망 공격에 의한 침해 사고 시나리오로 MITRE 社에서 제공하는 APT 29 시나리오를 활용한다.[18] APT(Advanced Persistent Threat)는 침입자가 장기간에 걸쳐 중요한 데이터를 훔치기 위해 네트워크에 탐지되지 않은 프로세스 및 실행 파일을 설정하는 지속적인 사이버 공격이다. APT 공격은 특정 조직에 침투하여 기존의 보안 조치를 회피하기 위해 계획된 공격 기법이다. APT 공격을 실행하기 위해 기존 공격보다 높은 수준의 정교함이 요구된다.[19]

APT 29는 Cozy Bear라고도 불리며, 2008년부터 러시아 정부와 관련이 있다고 여겨지는 러시아 해커 그룹이다. 러시아 해킹 그룹 이름에 따라붙는 APT는 지능형 지속 공격을 의미한다. 우리에게 익숙한 디도스(DDoS) 공격과 함께 지금은 사이버 공격의 주류로 평가받고 있다.[20]

4.1 임무 영향성 평가 시나리오

00부대는 서해 최북단에 위치한 군 부대로 해안 경계 작전을 수행한다. 주요 임무로 해수면 경계 작전을 수행하며, 지상 전자정보 수집체계와 드론봇 경계체계를 활용하여 임무를 수행한다.

드론봇 경계 체계의 주요 기능은 레이더 방출 차단 및 분석 기능과 통신 가로채기 기능이 있다. 해당 기능을 통해 해수면 경계 임무를 수행한다.

00부대에서 드론봇 임무를 수행하는 중사 김00은 드론봇 운용 및 관리용 단말기의 소프트웨어 업데이트가 필요한 사실을 알게되어, 기존 소프트웨어 판매 업체에 업데이트 요청을 하게된다.

소프트웨어 판매 업체는 군 특성상 USB 반입이어렵다는 것을 알고 CD를 이용해 소프트웨어 업데이트를 수행하려고 한다. 이때, 공격자가 업데이트 요청 사실을 알게되어 악성코드를 기입한 조작된 CD를 개발한 후 00부대에 반입하게 된다.

조작된 CD에는 공격 지속성을 위해 'javamtsup'라는 서비스를 등록하여 시스템 시작 시 서비스가 자동 실행되도록 한다. 'hostui.lnk'라는 파일을 생성하여 재시작 시 'hostui.exe'라는 파일이 자동 실행되도록 설정한다. 이를 통해서 침해 대상 PC의 관리자 권한을 획득하게 되어 지속적으로 드론봇 운용에 관한 정보를 입수 할 수 있게된다.

4.2 시나리오 기반 임무 영향성 평가

4.2.1 임무-기능-자산 정의

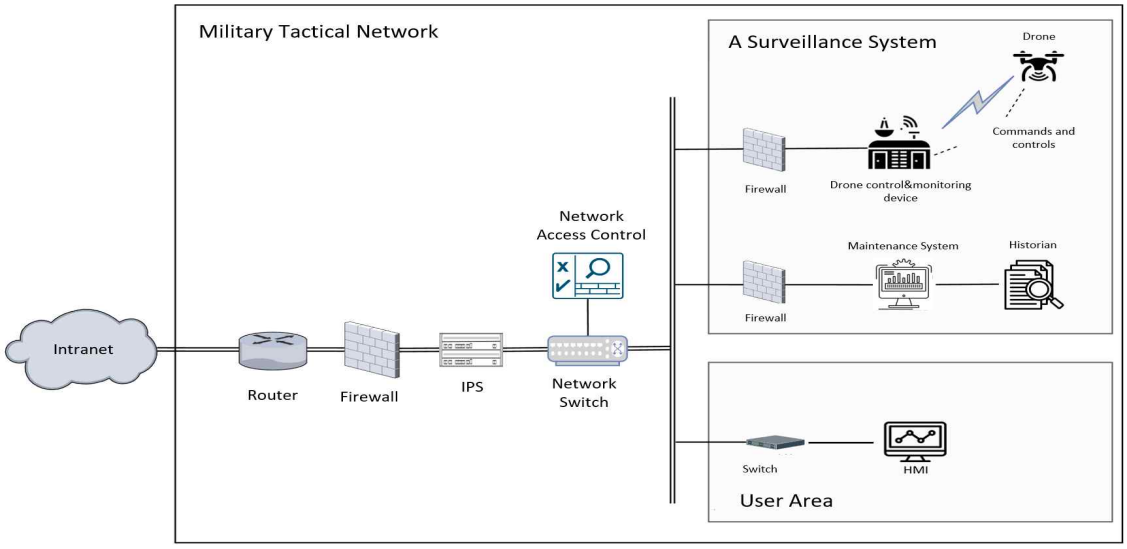
해당 절차는 임무-기능-자산 간의 관계를 정의하고 임무 종속성을 구성하는 단계이다. 해당 절차를 수행하기 위해 임무, 기능, 자산의 정의와 네트워크 토폴로지 자료가 필요하다.

<표 2> 임무-기능-자산 정의

Category	Description
Mission	Coast guard operations
Function	Radar emission blocking and analysis
	Communication intercept
Asset	HMI(Human-Machine Interface)
	Data Historian
	ESM(Electronic Support Measure)
	ECM(Electronic Counter Measure)
	Drone bot

00부대의 해안 경계 작전을 임무-기능-자산 관계도를 구성하는 것으로 평가가 시작된다. 다음 <표 2> 는 00부대의 해안 경계 작전에 해당하는 임무, 기능, 자산을 정의한 표이다.

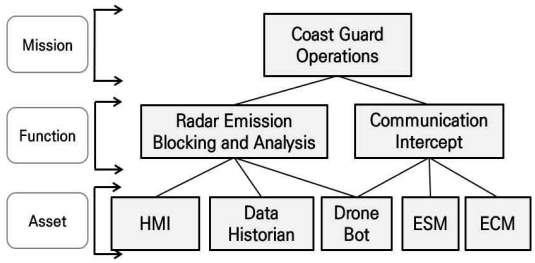
(그림 8)는 00부대 드론봇 운용 네트워크 토폴리지이다. 사용자 영역의 사용자 단말기를 통해 감시



(그림 8) 네트워크 구성도

체계 망으로 접속하여 드론/제어 감시 장비를 활용하여 감시 드론을 운용하거나 통신 주파수 감시를 수행 할 수 있다. 해당 네트워크 구성도 내용 중 감시체계 망 내부의 두 가지 기능이 포함되며 사용자 영역 망 내부에는 자산들이 포함된다. 해당 정보를 기반으로 임무 종속성 관계도를 구성한다.

다음 (그림 9)은 임무, 기능 및 자산의 구조도를 설명한다.



(그림 9) 임무 종속 구조도

임무는 해양 경계 작전으로 기능은 레이더 방출 차단 및 분석과 통신 가로채기 기능이 있다. 해당 기능에 연결되는 자산으로는 데이터 방출 차단 및 분석에는 관리자용 휴먼 머신 인터페이스(Human-Machine Interface, HMI), Data Historian 및 드론봇이 있으며, 통신 가로채기 기능에 연결되는 하위 자산으로 ESM, ECM 및 드론봇이 있다.

4.2.2 프로세스 종속 관계 구성

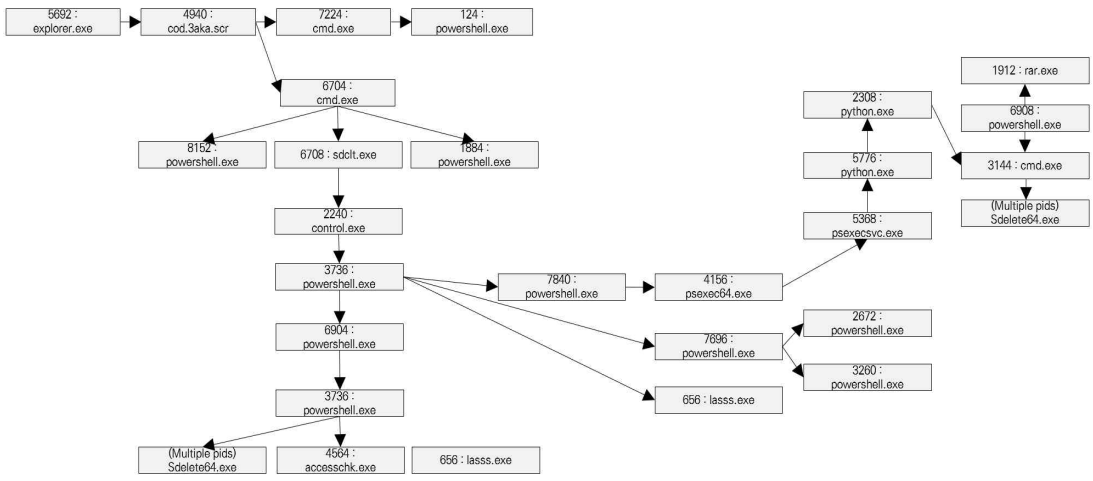
Sysmon을 활용하여 프로세스가 수행과정을 파악할 수 있다. 실행된 프로세스와 실행된 프로세스의 부모 프로세스 정보를 알 수 있어 전체 구문을 분석하여 공격 경로를 파악할 수 있다.

본 사례에서 핵심이 되는 구간은 초기에 악성코드('rcs.3aka3.doc' 파일)가 초기에 시작한 구간과 사용자 계정 컨트롤(UAC, user account control) 우회(bypass)를 통하여 높은 수준의 권한으로 Power Shell이 실행된 단계, 이후 얻은 PowerShell로부터 다른 PowerShell을 실행한 단계이다. 앞서 도출된 시스템 개체 종속성 구조의 프로세스 및 파일들이 제공하는 서비스를 통해 타 자산에 연결되는 지점을 식별한 것이다. 다음 (그림 11)는 Sysmon에서 탐지된 프로세스를 부모/자식 종속 관계를 구현한 것이다.

해당 종속 관계도를 통해 임무 종속성 관계도와 연결하여 자산 별로 발생하는 프로세스와 연계된 자산의 관계 및 영향을 미치는 임무를 포함한 전체 구성도를 파악할 수 있다.

첫 번째는 초기 진입 지점이다. 공격자는 'rc3.3aka 3.doc' 파일을 목표 대상 PC에 설치하였고, 사용자는 이를 실행시켜 공격자가 초기진입이 가능하게 하였다.

두 번째는 권한 탈취 지점이다. 공격자는 사용자 계정 제어 우회를 통해 권한 탈취를 이후, 'Powershell'이 실행되는 단계이다. 해당 단계로 시스템 전반에 명령 및 제어가 가능한 상황이다.

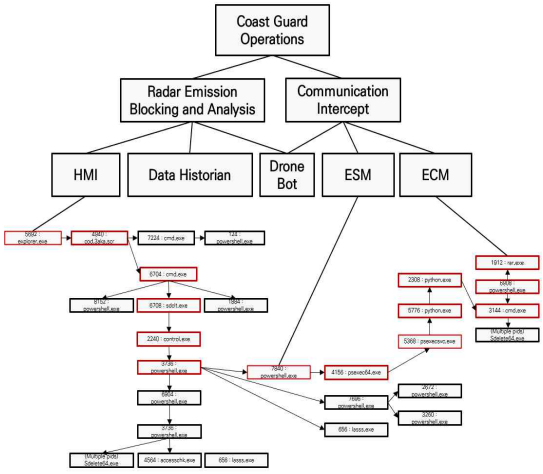


(그림 10) 시스템 호출 구조 다이어그램

세 번째는 지속성 공격 실행 지점이다. APT29의 최종 목적지이며, 사용자 PC가 재부팅을 할 때마다 실행 파일이 자동적으로 실행되도록 설정한 것이다.

4.2.3 사이버보안 측면 위험 관리 대상 도출

다음 (그림 11)는 임무-기능-자산 정의 및 프로세스 종속 관계 구성 단계에서 도출된 임무 구조도 및 그에 따르는 프로세스 종속 관계를 표현한 그림이다. 프로세스 종속 관계에서 공격자가 임무 및 타 자산에 연계하여 영향을 미칠 수 있는 구간을 도출하였다.



(그림 11) 핵심 임무 종속성 구성 도출

다음 <표 3>는 본 시나리오의 최종 결과이다. 5가지의 장비 중 우선적으로 관리해야하는 장비는 총 3개로 관리자가 사용하는 HMI와 ESM, ECM은 우선 관리가 필요한 자산으로 도출된다.

<표 3> 관리 필요 자산 도출

Asset	Need to be managed
HMI(Human-Machine Interface)	O
Data Historian	X
ESM(Electronic Support Measure)	O
ECM(Electronic Counter Measure)	O
Drone bot	X

5. 결론

본 논문에서는 임무 수행에 영향을 줄 수 있는 군사 자산을 파악하기 위한 임무 영향성 평가 방안을 제안하였다. 임무 수행을 위한 기능 및 자산을 정의하고 해당 자산에 문제가 되는 데이터 흐름을 분석하여 임무에 영향을 미칠 수 있는지에 대한 문제를 가지고 분석하였다.

본 논문 2장에서는 임무 영향 관련 연구사례에서는 임무 종속성을 중심으로 대표적으로 연구된 논문을 통해 프로세스 단위에서 시행되어야하는 필요성을 나타냈다.

3장에서는 임무 영향도를 평가하는 이론적인 방법에 대해서 기술하였다. 임무 종속성 및 시스템 출처 그래프를 활용하여 어떻게 자산과 연결하여 임무에 미치는 영향을 파악하는지 연구했다.

4장에서는 3장에서 제안한 임무 영향 평가 방법을 APT29라는 알려진 공격 기법을 활용해 공격 시나리오를 구성하였다.

향후 연구방향은 본 논문에서 다뤄지는 시스템 출처 그래프를 구성하는 자동화 프로그램을 연구하는 것이다. 공격 그래프를 그리는 자동화 도구로는 MulVAL, TVA, NetSPA 등이 있으며, 이 중 오픈소스이며 소프트웨어의 버그와 시스템 및 네트워크 설정 간의 상호 관계를 모델링하는 것으로 MulVAL을 활용한 연구를 진행할 예정이다.

참고문헌

[1] 김두환; 박호정. 4 차 산업혁명에 따른 군사 보안 발전방안 연구. 융합보안논문지, 2020, 20.4: 47-59.

[2] 신미주, 윤성수, 엄익채. (2022). 국내 원자력 시설 통합 취약점 분석 프레임워크 연구. 융합보안논문지, 22(1), 11-17.

[3] 이승운, et al. 국방 소프트웨어의 현대화 및 공급망 보안을 위한 DevSecOps 도입 방안 연구. 정보보호학회지, 2022, 32.5: 67-73.

[4] ORCE, Joint Task. Risk management framework for information systems and organizations. NIST Special Publication, 2018, 800: 37.

[5] ROESCH, Martin, et al. Snort: Lightweight intrusion detection for networks. In: Lisa. 1999. p. 229-238.

[6] 이종범; 엄익채. 사물인터넷 기기 침해사고 데이터 수집 방안 연구. 정보보호학회지, 2023, 33.3.

[7] CARVALHO, Olga, et al. CIIA: critical infrastructure impact assessment. In: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. 2022. p. 124-132.

[8] APPANA, Pranavi; SUN, Xiaoyan; CHENG, Yuan. What To Do First: Ranking The Mission Impact Graph for Effective Mission Assurance. In: 2019 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2019. p. 567-571.

[9] CAO, Chen, et al. Assessing attack impact on business processes by interconnecting attack graphs and entity dependency graphs. In: IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham, 2018. p. 330-348. network security: principles and practices, 4th Ed., Prentice Hall, Nov. 2005.

[10] DOUTHWAITE, Mark. The Assurance of Bayesian Networks for Mission Critical Systems. 2018. PhD Thesis. University of York.

[11] SUN, Xiaoyan; SINGHAL, Anoop; LIU, Peng. Towards actionable mission impact assessment in the context of cloud computing. In: IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham, 2017. p. 259-274.

[12] MOTZEK, Alexander; MÖLLER, Ralf. Context-and bias-free probabilistic mission impact assessment. computers & security, 2017, 65: 166-186.

[13] UN, Xiaoyan; SINGHAL, Anoop; LIU, Peng. Who touched my mission: Towards probabilistic mission impact assessment. In: Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense. 2015. p. 21-26.

[14] BUCHANAN, Laurin; LARKIN, Mark; D'AMICO, Anita. Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users. In: 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE, 2012. p. 298-304.

[15] DAI, Jun, et al. Gaining big picture awareness through an interconnected cross-layer situation knowledge reference model. In: 2012 International Conference on Cyber Security. IEEE, 2012. p. 83-92.

[16] XIE, Peng, et al. Using Bayesian networks for cyber security analysis. In: 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). IEEE, 2010. p. 211-220.

[17] OU, Xinming; BOYER, Wayne F.; MCQUEEN, Miles A. A scalable approach to attack graph generation. In: Proceedings of the 13th ACM conference on Computer and communications se

curity. 2006. p. 336-345.
[18] MOREAU, Luc, et al. The open provenance model: An overview. In: International provenance and annotation workshop. Springer, Berlin, Heidelberg, 2008. p. 323-326.
[19] 윤성수; 엄익채. 시계열 특성 기반의 공격자 기술 수준을 고려한 취약점 심각도 평가 방안 연구. 정보보호학회논문지, 2023, 33.2: 281-293.
[20] MAVROEIDIS, Vasileios; JØSANG, Audun. Data-driven threat hunting using sysmon. In: Proceedings of the 2nd international conference on cryptography, security and privacy. 2018. p. 82-88.

〔저자소개〕

김 준 석 (Joon-seok Kim)

2018년 2월 전북대학교 학사
2023년 2월 전남대학교 정보보안협동과정 석사
2023년 9월 ~ 현재 전남대학교 박사
<관심분야> 산업제어시스템보안, 위험평가

email : jss8707@jnu.ac.kr

엄 익 채 (Ieck-chae Euom)

2018년 2월 전남대학교 컴퓨터정보학부 학사
2023년 2월 한국과학기술원 소프트웨어대학원 석사
2019년 10월 ~ 현재 전남대학교 데이터사이언스대학원, 교수
<관심분야> 산업제어시스템보안, 데이터 보안, 취약점연구

email : iceuom@jnu.ac.kr