사이버 전투 피해 평가 프레임워크

김두회*, 김용현**, 김동화**, 신동규*, 신동일*
세종대학교 컴퓨터공학과
e-mail:doo6310@gce.sejong.ac.kr

Cyber Battle damage assessment framework

Duhoe Kim*, Yonghyun Kim**, Donghwa Kim**, Dongkyoo Shin*, Dongil Shin*
*Dept of Computer Engineering, Se-jong University
**Agency for Defense Development

요 약

정보통신 기술의 발전으로 개인뿐만 아니라 경제, 행정, 국방 등 사회 전반에서 사이버 공간의 중요성이 대두되고 있다. 특히 국방부에서는 사이버 관련 공격들에 관한 피해를 평가하는 연구가 활발히 진행되고 있다. 본 논문에서는 사이버 전투 피해평가 프레임워크를 제안한다. 사이버 전투 피해평가 프레임워크는 아군이 사이버 공격에 의해 피해를 입은 뒤 지휘 통제실에게 아군의 피해를 알리고 장비의 손상도는 얼마인지 작전에 이상을 미치는 영향은 얼마인지 계산하여 제공한다. 본 프레임워크를 사용하면 현 상황을 아군의 사령부가 파악할 수 있게 되어 지휘 결심을 하는데 도움을 주어서 작전을 성공 시킬 수 있게 도와준다.

1. 서론

정보통신 기술의 발전으로 개인뿐만 아니라 경제, 행정, 국방 등 사회 전반에서 사이버 공간의 중요성이 대두되고 있다 [1]. 미군은 사이버공간을 지상 해상 공중 우주에 이은 5번째 전장으로 선언하여 사이버전 대비 능력을 강화하고 있으며, 우리 군도 사이버사령부를 신설하는 등 사이버 전력 보강을 본격화하고 있다 [2]. 국가는 사이버 공간에 점점 더 의존하고 있다. 국방부는 군대 중심의 물자 중심 전쟁 태세에서 기능 중심의 미션 중심 전쟁 태세로 전환함에 따라 군사를 지휘하는 지휘관, 분석가, 작전을 기획하는 군사 기획자 등이 중요해지고 있다.

국방부는 복잡하고 새로운 미션을 해결하기 위해 목표를 종합적으로 구성하고 엄격하게 지정하고 명시적으로 작성하는 합당한 프레임워크가 필요하다 [3]. 최근 사이버 공격을 당했을 때 피해를 평가하는 연구가 많이 진행되고 있다. 특히 국방부에서는 사이버 관련 공격들에 대비하여 사이버 피해를 평가하는 연구가 진행되고 있다 [4]. 이러한 사실에도 불구하고 기존 보안 분석은 시스템 상에선 자동적으로 할 수 없으며, 시스템이 가질 수 없는 통찰력을 지닌 보안 분석가들이 수동적으로 진행해야 한다.

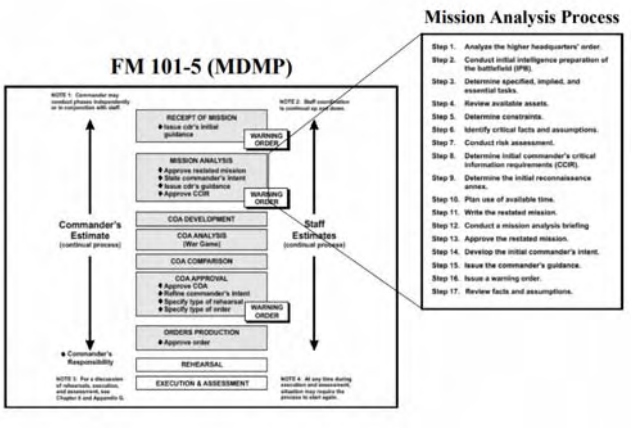
사이버 공격의 피해를 평가하는 것은 단지 사이버 공간상의 문제만이 아니라 물리전, 전자전, 기동화력 등과 같은 기존 전쟁에 영향을 미치는 것이 증명되었다 [5]. 러시아-그루지아전과 같이 실제 전쟁에서 사이버 공격을 이용한 전쟁이 시존 전쟁보다 피해를 효과적으로 가할 수 있기 때문에 전쟁에 국가별로 사이버 전쟁을 대비하고 있다. 사이버 전쟁을 위해선 사이버 피해에 관한 평가가 필요하다.

본 논문에서는 피해 평가를 진행하여, 우리나라가 사이버 공격을 당했을 때, 물리전의 손실은 얼마나 일어나는지, 전자전의 손실은 얼마나 일어나는지, 사이버 공격으로 인해 미션의 성공률에 얼마나 영향을 미칠지를 평가하는 프레임 워크를 구성한다. 2장에서는 관련연구로 다른 프레임워크와의 비교를 통해 우수성을 증명하고, 3장에서는 본 논문에서 개발한 프레임워크를 소개하고 4장에서 결론을 내며 마친다.

2. 관련 연구

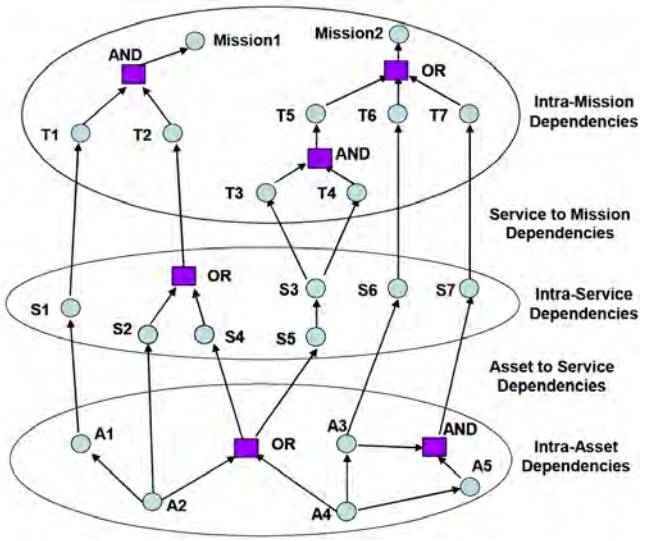
사이버 피해평가를 위해 미션을 측정할 수 있는 지표가 필요한데, 본 논문에서는 Measure Of Effectiveness(MOE) 와 Measure Of Performance (MOP)를 사용하였다. 미션 분석은 미션 결과의 측정을 달성하기 위해 작업을 패키지로 구성한다. 미션의 발전 과정은 capability 패키지를 운영에 할당하기 위해 MOP라는 측정을 사용하여 측정한다. 미션 분석 과정은 할당된 MOP들이 미션 요구사항을 충족시키고, 작업 실행을 가능하게 하는지 결정하기 위해 MOE라는 척도를 사용하여 측정한다 [3]. 그림 1은 MOE와 MOP의 처리 과정이다.

1) 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).



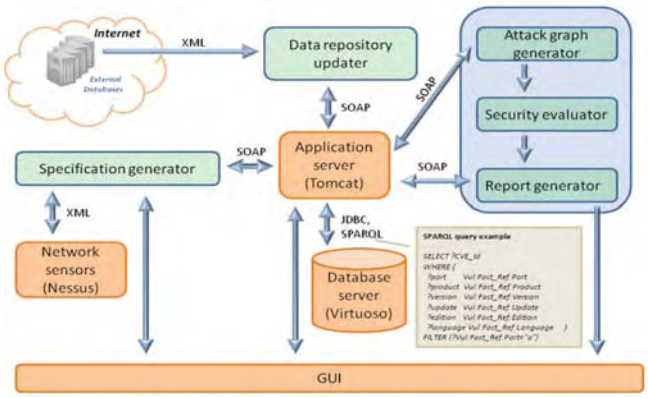
(그림 1) MOE, MOP Process

Jakobson, Gabriel 은 사이버 자산, 서비스 및 임무에 미칠 수 있는 영향을 평가하기 위한 개념적 틀과 방법을 제안한다. 또한 확장된 개념 그래프를 기반으로 한 사이버 공격 모델을 설명한다. 사이버 공간의 개념을 자산과 서비스 및 상호 의존성을 포함하는 다단계 정보 구조로 소개한다. 또한 임무 모델과 임팩트 종속 그래프를 통해 일관된 방식으로 사이버 공간과 임무간의 종속성을 제시한다. 그림 2는 Jakobson이 제안한 Impact Dependency Graph 이다. 사이버 공격이 직접적으로 공격받은 자산에 미치는 영향을 계산하는 방법, 사이버 공격이 자산, 서비스 및 미션 종속성, 진행 중인 임무의 운영능력에 어떤 영향을 미치는지 알고리즘 기반으로 제시한다 [6]. 본 논문에서는 사이버 자산뿐 만 아니라 물리전, 전자전, Supervisory Control And Data Acquisition(SCADA) 시스템까지 아우르는 시스템을 제안한다. 또한 지휘 통제부와의 소통할 데이터를 정의함으로써 지휘 결심을 더 정확하게 할 수 있도록 도와준다.



(그림 2) Impact Dependency Graph

Igor Kotenko는 사이버 공격 모델링 및 영향 평가를 위한 프레임워크를 제안한다. 공격 모델링 및 영향 평가에 대한 일반적인 접근 방식은 공격 그래프를 생성하며 보안 메트릭을 계산하고 위험 분석 절차를 제공하는 것을 기반으로 한다고 가정한다. 실시간 모드 이벤트 분석 및 예지 메커니즘, 보안 및 피해 평가를 달성하는 것이다. 공격 그래프 생성 및 보안 평가를 최적화하기 위해 다른 타임 라인 및 정밀도의 알고리즘 세트를 적용하여 결과를 얻을 수 있는 접근 방식을 적용한다. Cyber Attack Modeling and Impact Assessment Component(CAMIAC)의 아키텍처를 제안했다 [4]. 그림 3은 Igor Kotenko가 제안한 CAMIAC의 프로토타입 아키텍처이다.

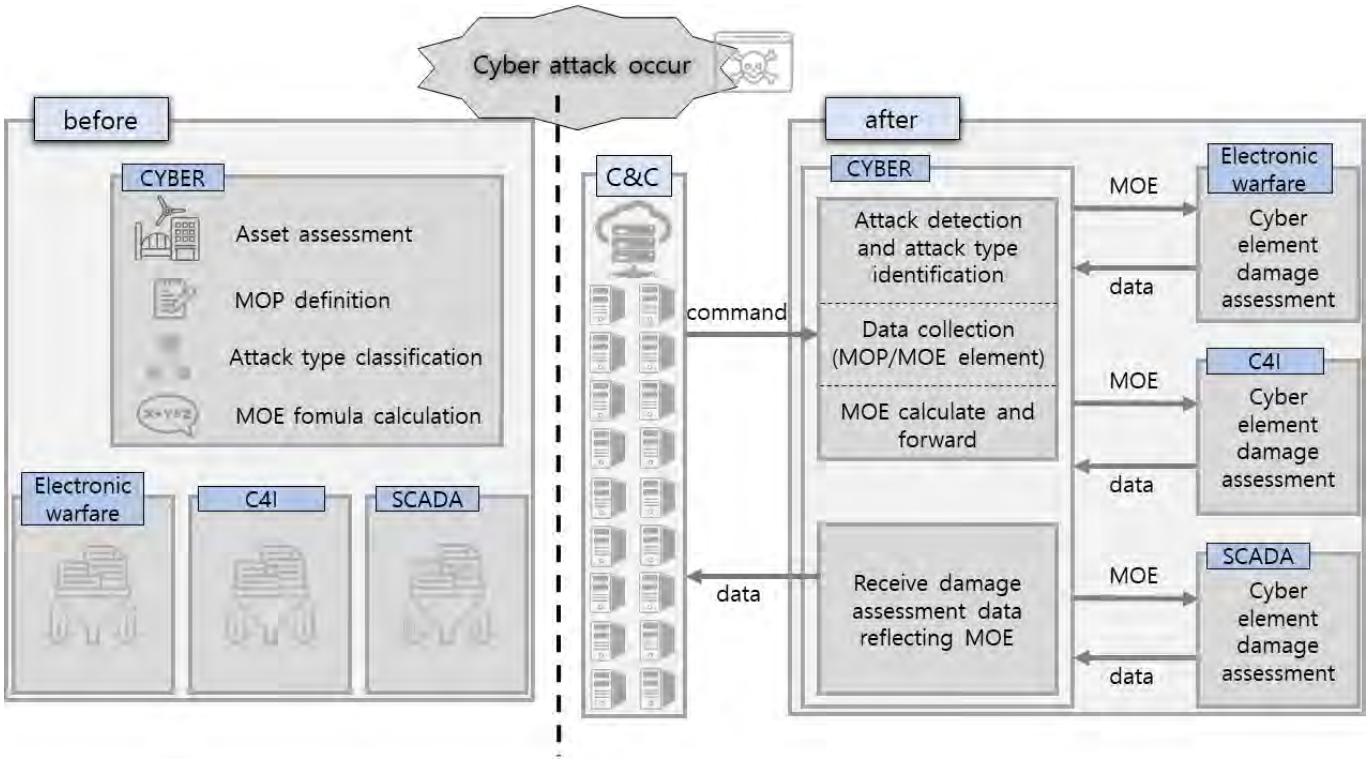


(그림 3) CAMIAC 프로토타입 아키텍처

3. 피해 평가 프레임워크

본 논문에서 제안하는 프레임워크는 크게 두 부분으로 볼 수 있다. 사이버 공격이 발생하기 전과 나머지 한 부분은 사이버 공격이 발생한 이후로 나누어진다. 사이버 공격이 발생하기 이전은 공격이 일어나기 전 준비해야 할 사전단계로 공격이 일어나기 전 기존의 시스템 정보 수집이나 자산평가, MOE 공식산출, 공격체계 분류 등 미리 여러 가지 지표를 설정해 놓는다. 사이버 공격이 발생한 후에는 어떤 공격이 진행되었는지 감지한다. 감지한 공격은 공격자의 목적을 파악하여 분류한다. 분류한 후에는 MOP와 MOE를 산출하여 사이버전자전, 물리전, SCADA 피해를 평가하는 모듈로 보낸다. 각 모듈에서는 사이버 공격으로 산출된 MOE를 입력받아 각 모듈에 해당하는 피해관련 수치들을 산출하여 지휘통제실로 보낸다. 지휘 통제실에선 수집된 피해 평가 자료들로 미션을 기획하고 만들어낸다. 피해 평가 자료들을 이용하면 더 성공적인 미션을 만들 수 있고 상황에 따라 지휘결심을 더 정확하게 만들 수 있는 지표가 된다. 그림 4는 본 논문에서 개발한 사이버 전투 피해 평가 프레임워크이다. 개발한 사이버 전투 피해 평가 프레임워크는 여러 가지 모듈들로 구성이 되어 있다. 최종적으로 계산한 데이터들은 사이버 사령부나 지휘통제실로 보내지며 작전 설계나 지휘에 영향을 미친다.

0



(그림 4) Cyber Battle damage assessment framework

3.1 Before Cyber Attack Occur

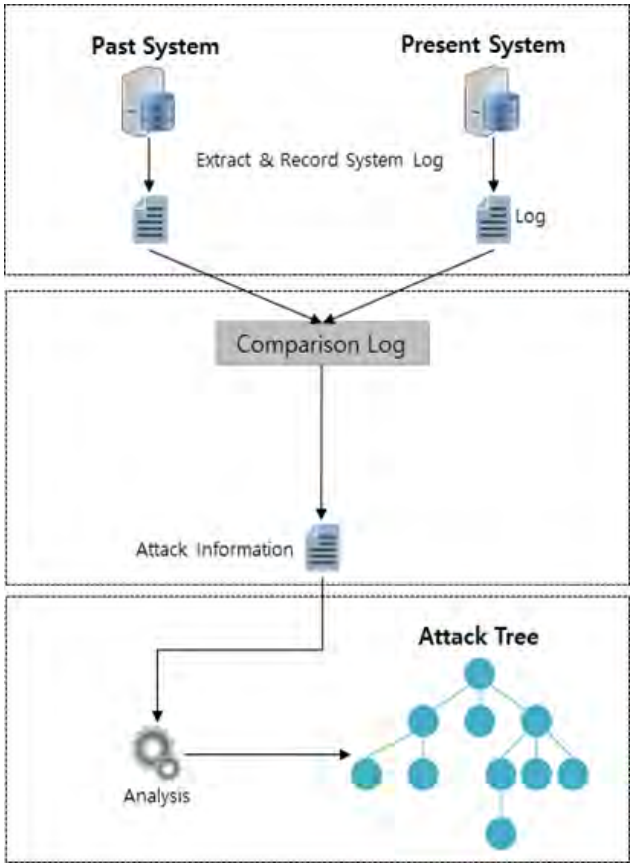
사이버 공격이 일어나기 전에 준비해야 할 것들은 총 4가지이다. 첫 번째는 자산 평가다. 자산평가를 위해 먼저 자산을 분류한다. 자산은 유형과 무형으로 분류하고, 그 안에서 또 카테고리를 만들어 분류한 뒤 각 카테고리마다 중요도를 부여할 수 있는 설문조사를 만들어 중요도를 결정한다. 각 중요도는 공격을 당한 뒤에 피해평가에서 가중치로 쓰인다. 두 번째는 MOP를 정의해야 한다. 본 논문에서 사용하는 MOP는 목적 달성을 위해 필요한 척도 MOE를 구성하는 변수로써 소프트웨어 손상도, 복구불능 데이터의 양, 인터넷 의존도 등이 있다. MOP는 자산평가에서 사용하는 척도를 많이 가져왔다. 세 번째는 공격을 분류한다. 공격을 분류하는 기준은 공격자가 의도하는 목적을 기준으로 삼는다. 본 논문에서는 공격자의 의도를 세 가지로 분류한다. 세 가지는 Interruption, Interception, Modification이다. 각 분류 안에 공격이 중복해서 들어갈 수도 있다. 예를 들면 Backdoor나 APT 공격은 세 가지를 다 목표로 할 수 있기 때문에 세 카테고리에 다 포함된다. 표 1은 공격 분류의 일부이다. 네 번째는 MOP와 여러 요소들을 조합하여 사이버 공격에 대한 피해량을 측정할 수 있는 MOE를 수식으로 만든다. MOE 수식은 총 3가지로 각 수식은 세 번째에 공격자의 목표가 MOE 값으로 표현된다. 예를 들면 ARP Spoofing 공격이 일어났을 때 ARP Spoofing으로 인한 정보 손실이 얼마나 되는지 수식화 하는 것이다. 이 4가지 사전 작업을 거쳐 사이버 공격을 당했을 때, 사이버 피해 평가를 할 수 있게 된다.

<표 1> 공격 데이터 분류

Class	Attack
Interception	Backdoor, APT, Footprinting, ARP Spoofing, Phishing, Scanning 등
Interruption	DDOS, APT, Backdoor, Bufferoverflow, Smurf, UDP Flood 등
Modification	APT, Backdoor, Ransomware, SQL Injection 등

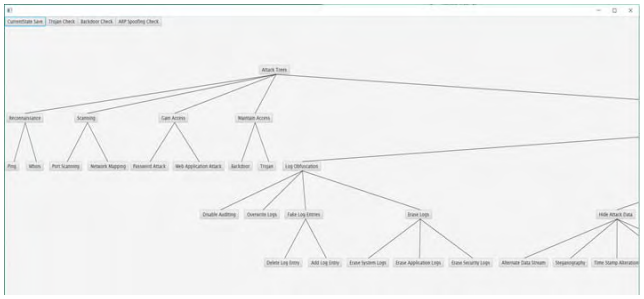
3.2 After Cyber Attack Occur

사이버 공격이 일어난 뒤에 피해평가를 위해서 사이버 사령부나 지휘통제실에서 명령을 받은 뒤 피해를 당한 시스템의 여러 가지 정보를 수집한다. 그 후에 어떤 사이버 공격을 당했는지 확인한다. 확인하는 방법은 사이버 공격을 당하기 전의 로그와 사이버 공격을 당한 후의 로그를 비교 분석하여 어떠한 공격을 당했는지 추적한다. 이 작업을 위해선 사전에 모든 공격 정보를 수집하고 데이터베이스화 하여 가지고 있어야 하며, 사이버 공격이 일어나기 전의 시스템에 관한 로그 수집이 필요하다. 로그를 비교 분석해서 검출해 내는 방법은 공격마다 알고리즘이 있으며, 공격마다 반드시 이전로그와의 비교를 요구하지는 않는다. 그림 5는 어떤 공격인지 검출해내는 과정을 보여주는 그림이며 사전 작업은 표시되어 있지 않다.



(그림 5) 공격 검출 과정

어떤 공격인지 검출한 후에는 앞서 만든 MOE 공식에 대입하여 결과를 산출한다. 산출한 MOE 지표는 전자전, 기동화력, SCADA 모듈에 전송한다. 전자전과 기동화력, SCADA 모듈 에서는 전송 받은 MOE를 토대로 각자에게 어떤 영향을 미치는지 데이터를 산출한다. 결과적으로 나온 사이버 피해 평가 데이터를 사이버 모듈에서 수집하여 피해 요소와 전송받은 데이터들을 포맷에 맞춰 사령부나 지휘통제실로 전송한다. 포맷은 TAXII나 IOC 등 일정한 데이터 포맷을 사용한다. 사이버 사령부나 지휘통제실에서 전송받은 데이터를 토대로 미션을 설계하거나 지휘 결심에 반영한다. 그림 6은 검출한 그림을 그래프로 표시하는 프로그램이며 공격자가 어떤 경로로 침입했는지 알 수 있다.



(그림 6) 검출된 공격 및 공격 경로 표시 그래프

4. 결론

본 논문에서는 사이버 전투 피해 평가 프레임워크를 제안했다. 사이버 전투 피해 평가 프레임워크는 크게 두 부분으로 구성되어 있으며 여러 가지 모듈들로 이루어져 있다. 각 모듈은 사이버 피해 평가를 진행하는데 중요한 역할을 하는 것을 실험을 공격 검출을 통해 증명했으며, 최종적으로 계산된 피해 평가 데이터는 사이버 사령부나 지휘통제실로 전송되어 작전 설계나 지휘에 영향을 미친다.

본 논문에서 개발한 프레임워크를 사용하면 전시에 사이버 공격을 당하더라도 정확한 계산을 통해 피해를 수치화하여 지휘관이 내부 전력을 파악하여 미션구성과 지휘결심에 직간접적인 도움을 줄 수 있다.

추후에는 사이버 전투 피해 평가 프레임워크 내 각 모듈의 세부적인 부분에 대해서 개발할 예정이며, MOE 수식이 좀 더 정확한 수치를 반영할 수 있도록 개선할 예정이다. 또한 다른 세부 모듈들을 실험을 통해 데이터를 분석할 예정이다. 더불어 모든 모듈들이 작동하여 전체적인 프레임워크가 작전 지휘와 미션 구성에 도움이 되는지 증명할 예정이다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] Cashell, B, et al. “The economic impact of cyber-attacks”. Congressional Research Service Documents. CRS RL32331 (Washington DC). 2004.

[2] 김두회, et al. “공격 트리 시나리오의 생성 및 분석을 이용한 침입 경로 예측 시스템”. 한국인터넷정보학회 학술발표대회 논문집. 17.2 2016: 13-14.

[3] Sheehan, Jack H. et al. “The military missions and means framework”. No. AMSAA-TR-756. ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY ABERDEEN PROVING GROUND MD. 2004

[4] Kotenko, I, and Andrey C. “A cyber attack modeling and impact assessment framework”. Cyber Conflict (CyCon). 2013 5th International Conference on. IEEE. 2013.

[5] Deibert, Ronald J, Rafal R, and Masashi C. “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war”. Security Dialogue. 43.1 2012: 3-24.

[6] Jakobson, Gabriel. “Mission cyber security situation assessment using impact dependency graphs”. Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on. IEEE. 2011.