Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.2, Apr. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.2.465

사이버 효과 지표를 활용한 사이버 전투 피해평가 시뮬레이션 도구의 설계 및 구현*

박 진 호,† 김 두 회, 신 동 일, 신 동 규‡
세종대학교

Design and Implementation of Simulation Tool for Cyber Battle Damage Assessment Using MOCE(Measure of Cyber Effectiveness)*

JinHo Park,† DuHoe Kim, DongIl Shin, DongKyoo Shin‡
Sejong University

요 약

최근 몇 년 사이에 사이버 공격의 보편화로, 사이버 공간내의 공격을 사이버전이라는 일종의 전쟁으로 간주하고 있다. 그러나 사이버전은 직접적인 피해 식별이 불가하여 공격에 대한 아군의 피해 파악이 어렵다. 사이버전에서 발생할 수 있는 공격에 대한 피해를 효과적으로 평가하기 위해, 본 논문은 MOCE(Measure of Cyber Effectiveness) 산출 식을 활용하여 사이버 공격에 대한 피해를 산출할 수 있는 DEVSim++ 기반의 사이버전의 피해 평가 시뮬레이션을 제시한다. 또한 사이버 지휘 통제 단계에서 지휘관의 판단을 돕기 위해, 공격 분류별 피해 받은 개체 수를 벤 다이어그램 형태로 표현하여 결과를 직관적으로 가시화한다.

ABSTRACT

In recent years, the cyber attack has become a universal phenomenon, and the attacks in cyberspace are regarded as a kind of war, cyber-warfare. However, cyber-warfare is difficult to identify the damage caused by the attack. In order to effectively evaluate the damage to the attack that may occur in the cyber-warfare, this paper describes the damage evaluation simulation of the cyber-warfare based on DEVSim++, which can calculate the damage to the cyber attack using the MOCE (Measure of Cyber Effectiveness). Also, in order to help the commander in the cyber Command&Control phase, the number of victims by attack classification is expressed in the form of Venn diagram.

Keywords: Cyber battle, Simulation, Network Security, MOCE(Measure of Cyber Effectiveness)

I. 서 론

최근 몇 년 사이에 사이버 공격이 점차 보편화되면서 이는 국가 안보에 심각한 위협이 되고 있다. 그렇기 때문에 사이버 공간에서 이루어지는 공격을 사이버전이라는 일종의 전쟁으로 간주하고 있는 상황이다[1]. 그러나 사이버전은 실제 물리전과는 달리 피해를 직접적으로 식별할 수 없기 때문에, 공격에 대한 아군의 피해를 파악하기 어렵다. 방위, 은행, 통신, 운송, 전력 및 기타 여러 시스템이 네트워크 인프라에 의존함에 따라, 시뮬레이션 방법론은 위협을 분류하고 결과를 평가하는데 필수적이다[2].

Received(02. 08. 2019), Modified(03. 27. 2019), Accepted(04. 04. 2019)
* 본 논문은 2018년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임

* 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).
† 주저자, sjaj123@naver.com
‡ 교신저자, shindk@sejong.ac.kr(Corresponding author)

본 논문은 사이버 공간에서 공격이 발생했을 때, MOCE(Measure of Cyber Effeciveness) 산출식으로 피해량을 산출하는 DEVSim++ 기반의 피해평가 시뮬레이션을 제시한다. 시뮬레이션을 실행하여 산출된 결과인 피해율을 토대로 지휘 통제 단계에서 최종적인 판단에 도움을 주는 지표가 되는 것을 목표로 한다.

2장에서는 피해평가 시뮬레이션에 사용하는 도구와 자산 중요도 설정 방법, MOCE 설정을 위해 사용한 사이버 공격 효과 분류 모델 및 기존 사이버 공격 분류 모델을 소개한다. 3장은 피해평가 시뮬레이션의 시스템 구조와 시뮬레이션의 실행 순서, 그리고 MOCE의 산출 식 및 가상 공격의 시나리오에 대해 설명한다. 4장에서는 시각화된 시뮬레이션의 최종 결과에 대해 설명한다. 5장에서는 결론 및 향후 연구를 내며 마친다.

II. 관련 연구

기존 사이버 전투 피해평가 기술에 대해서 여러 연구가 진행되어왔다. Howard는 사이버 전투 피해평가를 위해 사이버 공격을 사건 단위로 분류하였다. 먼저 사이버 공격의 종류인 Action과 피해 대상인 Target을 Event로 소분류한다. 그리고 공격 도구인 Tool, 공격의 취약점인 Vulnerability, 비인가 공격 방법인 Unauthorized Result를 Event와 함께 Attack으로 중분류한다. 마지막으로 공격자인 Attackers, 공격의 주목적인 Objectives를 Attack과 함께 Incident로 대분류한다. Fig. 1.은 Howard 분류의 정리이다[3].

Horony는 사이버 공격을 받은 후의 Business Processes 피해 평가 모델을 제안하였다. 이 모델은 사이버 공격을 받은 정보 시스템이 평가해야할 8개의 평가 항목으로 구성된다. Recovery는 공격 이전의 상태로 복원하기 위해 수행하는 과정으로, 손상된 소프트웨어와 하드웨어의 수리를 의미한다. Education/Training은 정보 시스템의 새로운 절차나 프로세스에 대한 사용자의 숙지 필요성을 의미한다. Human Life는 인간의 삶이 정보 시스템에 의존하므로 사이버 공격에 의해 영향을 받을 수 있음을 의미한다. Data는 사이버 공격으로 인해 피해를 입은 데이터의 복구비용 및 복구능력에 대한 평가를 의미한다. Lost Revenue는 시스템이 피해를 받은 이후 조직의 수익 창출 방법의 평가 필요성을 의미한다. Reputation은 사이버 공격 이후의 조직의 평판을 피해평가 단계에서 고려해야함을 의미한다. Business Expenses는 사이버 공격의 피해로 인해 발생하는 직접적인 비용을 의미한다. Productivity는 정보 시스템의 성능 저하로 인한 조직의 생산성의 평가 필요성을 의미한다. Fig. 2.는 Horony의 정보 시스템 피해 평가 모델의 시스템 구조이다[4].

최근에는 공격자의 의도를 분석하여 사이버 공격의 효과를 분류하는 모델에 대한 연구가 진행되었다. Musman은 사이버 공격으로 인해 발생한 피해에 대한 효과를 DMIFUI(Degradation, Modification, Interception, Fabrication, Unauthorized use, Interruption)의 6가지로 분류하고, 이 효과가 임무 데이터에 미치는 영향에 대해서 설명하였다[5][6][7]. 사이버 지휘 통제 단계에서의 판단을 돕기 위해서는, 피해량을 보다 자세하게 공격자의 의도별로 나누어 산출하는 것이 필요하다. 이에 본 논문에서는 DMIFUI의 6 가지의 공격 의도 분

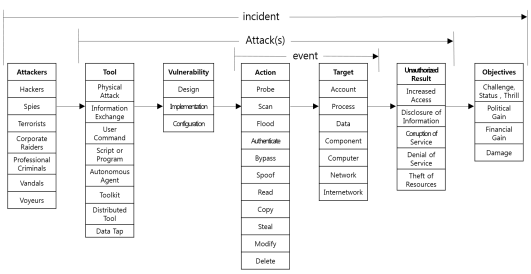

Fig. 1. Howard's Computer and Network Incident Taxonomy[3]

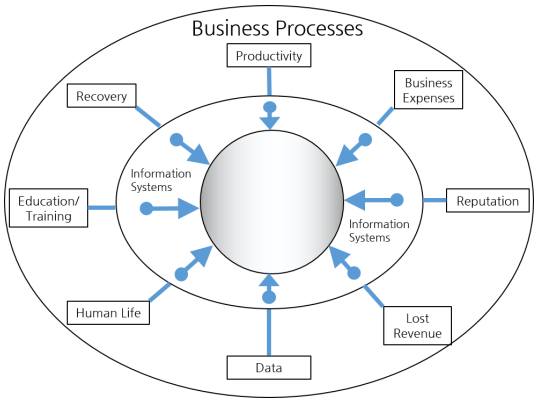

Fig. 2. Horony's Information System Damage Assessment Model[4]

류 기준 중 Interception, Modification, Interruption을 선택하여 공격 효과에 대해 최종적인 피해량 산출 분류 기준으로 사용한다. Unauthorized use는 Interception, Fabrication은 Modification, 그리고 Degradation은 Interruption의 범위 내에 한정이 가능하므로 기준에서 제외한다[8].

Fig. 3.는 본 논문에서 사용한 사이버 공격이 발생하기 전과 후의 상황 및 대처에 대한 사이버 전투 피해 평가 프레임워크이다. 프레임워크에서 사이버 공격이 발생하기 전에는, 공격에 대한 피해율 산출을 대비하여 자산 평가, MOP(Measure of Performance) 정의, 공격 유형 분류, MOCE 산출 식 정의를 미리 준비한다. 사이버 공격이 발생한 후에는, C&C로부터 피해율의 요청을 받고 공격 탐지 및 공격 유형 식별을 시작한다. 또한 MOCE의 피해량 데이터를 수집하고, MOCE를 계산하여 산출한다. 그리고 저장된 평가 데이터와 계산된 MOCE를 가시화하여 C&C의 요청에 응답한다[9].

Fig. 3.의 프레임워크처럼 사이버 공격으로 인한 피해가 발생하기 전에 미리 사이버 자산의 중요도를 평가해놓는다면, 피해를 받은 사이버 자산의 중요도를 피해 산출 식에 대입하여, 결과로 산출된 피해의 정확도를 높일 수 있다. Fig. 4.은 본 논문에서 설계한 사이버 자산의 중요도를 산출하는 자산 평가 시스템 구조이다. 자산의 중요도를 크게 기밀성, 무결성, 가용성의 세 분류로 나누어 평가한다. 기밀성은 군사 기밀 등급과, 무결성은 자산의 생성 날짜와 수정된 날짜의 기간차이, 가용성은 자산의 백업 파일 개수로 중요도를 산출한다[10].

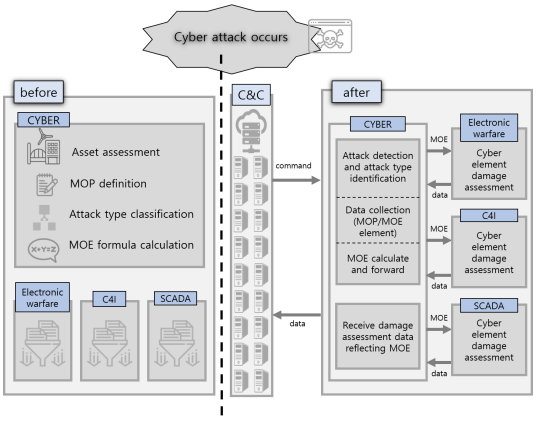

Fig. 3. Cyber Damage Assessment Framework[9]

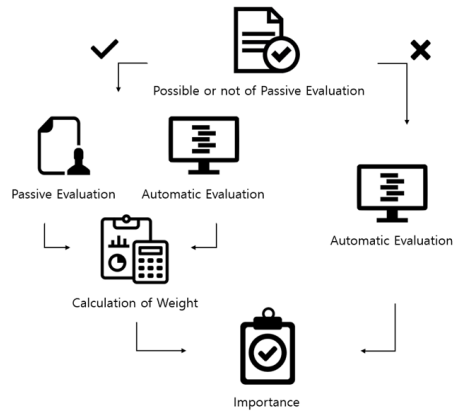

Fig. 4. Cyber Asset Assessment System[10]

2.1 시뮬레이션 구현 도구

본 논문에서는 사이버 피해평가 시뮬레이션 구현 도구로 DEVSim++을 사용하였다. DEVS (Discrete Event System Specification)는 계층형태의 모듈 방식을 사용하는 추상적인 이산 이벤트 모델이다. 이를 기반으로 하여 시뮬레이션을 위한 모델링 및 추상 시뮬레이터 개념을 C++언어로 구현한 도구가 DEVSim++이다. 시뮬레이션의 실시간 상호작용 시스템을 표현하기 위해, DEVSim++은 계층적 스케줄링 알고리즘을 구현한다. 또한 모델링을 위해 Atomic 모델과 Coupled 모델을 DEVS 프레임워크 내에서 방향 그래프 형태로 제공한다[11]. Atomic 모델은 입력 사건에 대한 상태 변화를 나타내는 개체로, 시뮬레이션에서는 하나의 PC로서 사용된다. Coupled 모델은 개체간의 관계를 나타내는 모델로, 시뮬레이션에서는 한 부대에 속

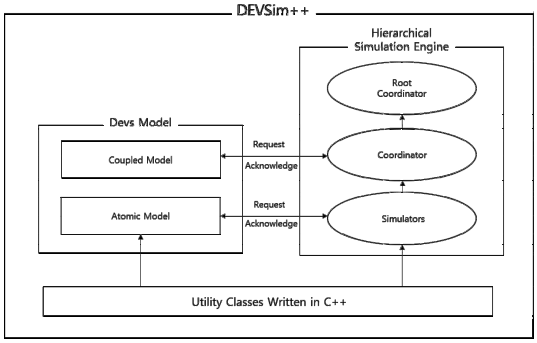

Fig. 5. DEVSim++ Simulation System Structure[11]

한 PC Atomic 모델들을 연결하는 역할을 한다. Fig. 5.는 DEVSim++의 시뮬레이션 시스템 구조다. 이는 C++로 구현된 클래스가 시뮬레이션 엔진과 Atomic, Coupled 모델 간의 상호작용 스케줄링에 영향을 미치는 것을 보여준다.

III. 사이버 전투 피해평가 시뮬레이션 시스템

본 논문의 사이버 피해평가 시뮬레이션의 실행은 먼저 피해평가에 필요한 파일의 입력으로 시작한다. 입력 파일은 Fig. 4.의 사이버 자산 평가 시스템을 이용하여 산출한 사이버 자산의 중요도, 보유한 사이버 자산의 개수 및 데이터의 크기 등을 속성으로 갖는다.

파일의 입력 이후에는 Fig. 6.의 가상 네트워크 구조에 따라 Cyber_Generator 모듈에서 공격 시나리오가 생성되며 사이버 공격이 시작된다. 공격 시나리오는 외부 네트워크를 통해 공용서버로, 공용서버를 통해 내부 네트워크로 침투한다.

시나리오를 통해 공격을 받은 부대 단위 유닛 내의 PC들은, 공격의 종류마다 범위가 다르게 정해진 피해를 받는다.

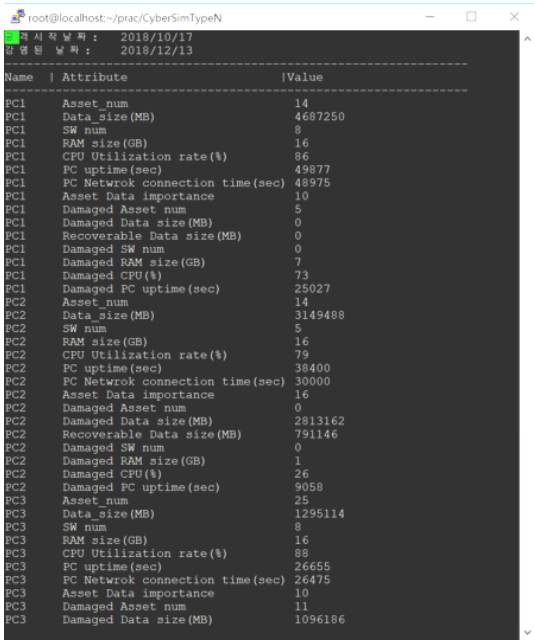

Fig. 7. Simulation Output File

공격이 모두 종료되면 피해를 받은 각 유닛마다 피해량을 Fig. 7.과 같은 텍스트 파일 형태로 출력

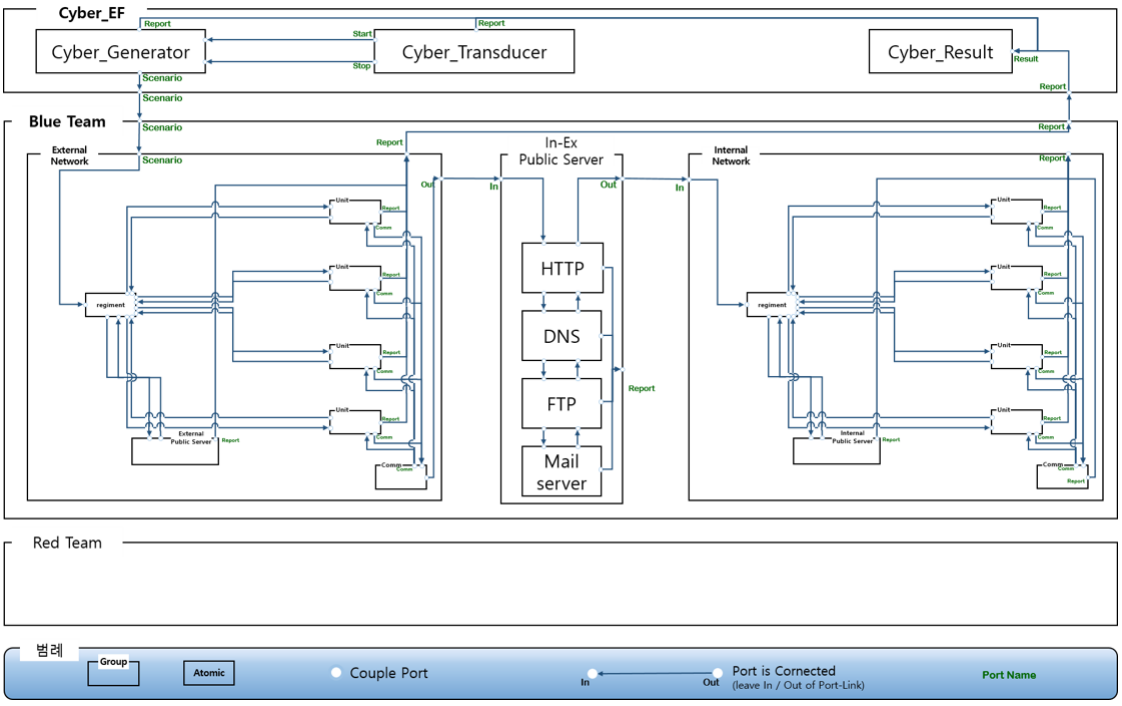

Fig. 6. Virtual Network System Structure for Cyber Damage Assessment Simulation

한다. 피해를 받지 않은 유닛은 파일을 출력하지 않는다. 파일의 출력 이후에는 DMIFUI 기반으로 제작한 공격 효과 분류 기준마다 최종 MOCE 피해율을 산출한다.

Fig. 8.은 그림으로 표현한 사이버 피해평가 시뮬레이션의 실행 순서이다. 시뮬레이션의 실행 순서를 정리하면 크게 유닛 데이터 입력, 가상 네트워크 공격 시뮬레이션, 피해율 계산 및 출력의 세 단계로 구성된다. 먼저 시뮬레이션에 사용되는 가상 네트워크 내의 유닛을 구성하는 PC의 속성을 입력한다. 그리고 가상 네트워크에 공격을 수행하여 각 PC 속성의 수치에 피해를 입혀 시뮬레이션을 실행하여, 공격에 대한 피해량을 Cyber_Result 모듈에 저장하고, 3.1의 MOCE 산출 식을 통해 최종 피해율을 출력한다. 마지막으로 산출된 피해율, 피해량 및 MOCE 피해 비율을 기반으로 하는 시뮬레이션 결과를 대시보드 형태로 가시화한다.

본 논문의 시뮬레이션에서는 피해 평가를 위해 APT(Advanced Persistent Threat) Stuxnet 공격 피해 시나리오를 적용하였다. APT Stuxnet 공격은 다양한 보안 위협을 지속적으로 가하는 공격으로, MOCE에 복합적으로 피해를 받을 수 있기 때문에 선정하였다. 공유 서버 내의 Windows 커널 모드 드라이버가 개체에 대한 참조 수를 적절하게 유지하지 않는 권한 상승 취약점을 통해 사이버 공격 및 전파 활동을 수행한다고 가정하였다. 그로 인해

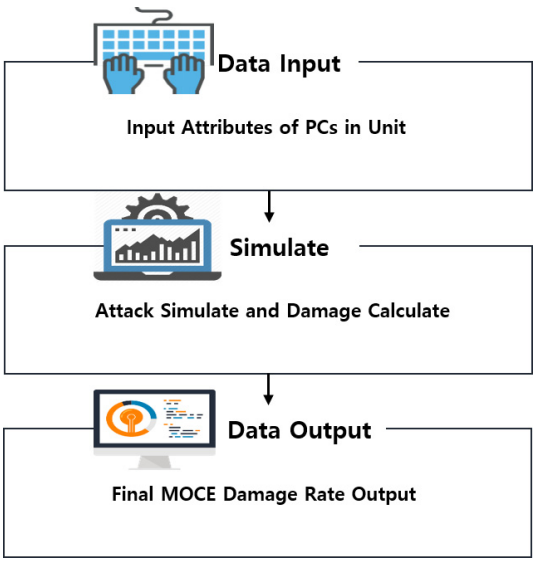

Fig. 8. Simulation of Execution Flow

아군의 사이버 네트워크 가운데 임의로 선정된 다수의 Unit에 대한 Interruption, Interception, Modification 공격을 성공하였다고 시나리오를 설정하였다.

3.1 피해평가 시뮬레이션의 피해율 산출 식

피해율, 즉 MOCE의 산출 식은 전체 개체와 피해를 입은 개체의 해당 MOCE의 피해 요소 비율로 구성한다. 세 개의 산출 식이 모두 포함하는 R_i는 해당 개체의 사이버 공격에 대한 피해 여부를 나타내는 연산 항으로, 1(true) 혹은 0(false)의 값을 가진다.

$$\left\{\left(\sum_{i=1}^{n} W_i \times D_i \times R_i\right) \div \left(\sum_{j=1}^{n} W_j \times D_j\right)\right\} \times 100 \quad (1)$$

수식 1의 MOCE Interception은 탈취된 데이터의 양 및 중요도로 피해율을 산출한다. W_i는 i번째 데이터의 중요도, D_i는 i번째 데이터의 크기, R_i는 i번째 데이터의 탈취 여부를 의미한다. 데이터 탈취 공격의 직관적인 피해 지표는 탈취당한 데이터가 얼마나 크고 중요한지의 여부이다. 그렇기 때문에 해당 PC가 사이버 공격을 받아 데이터가 탈취된 경우, 탈취된 데이터의 크기와 중요도가 높을수록 MOCE가 증가한다.

$$\left\{\left(\sum_{i=1}^{n} DT_i \times DS_i \times R_i\right) \div \left(\sum_{j=1}^{n} DT_j \times DS_j\right)\right\} \times 100 \quad (2)$$

수식 2의 MOCE Interruption은 시스템의 성능 저하와 그에 따른 작업 속도의 지연율로 피해율을 산출한다. DT_i는 i번째 PC(서버)의 피해 시간, DS_i는 i번째 PC(서버)의 피해 입은 시스템 가용메모리 크기, R_i는 i번째 PC(서버)의 네트워크 피해 여부를 의미한다. 시스템의 성능 저하에 대한 가장 큰 원인으로는 가용메모리가 있고, 이를 얼마나 사용할 수 없는지도 성능에 큰 영향을 미친다. 그렇기 때문에 해당 서버 혹은 PC가 공격을 받은 경우, 서버를 사용할 수 없는 피해 시간과 사용할 수 없는 메모리의 크기가 클수록 MOCE가 증가한다.

$$\left\{\sum_{i=1}^{n}(W_i \times D_i + S_i) \times R_i \div \sum_{j=1}^{n}(W_j \times D_j + S_j)\right\} \times 100 \quad (3)$$

수식 3의 MOCE Modification은 공격자에 의해 기존과 다르게 변경된 데이터의 양 및 중요도로 피해율을 산출한다. W_i는 i번째 데이터(소프트웨어)의 중요도, D_i는 i번째 데이터의 크기, S_i는 i번째 소프트웨어의 크기, R_i는 i번째 데이터(소프트웨어)의 수정 및 삭제 여부를 의미한다. 데이터 탈취 공격과 마찬가지로 데이터 변조 공격의 직관적인 피해 지표는 탈취당한 데이터가 얼마나 크고 중요한지의 여부이다. 그렇기 때문에 해당 PC 혹은 서버가 공격을 받아 데이터가 변조된 경우, 변조된 데이터의 크기와 중요도가 높을수록 MOCE가 증가한다.

3.2 시뮬레이션 결과 시각화

시뮬레이션의 최종단계인 MOCE 최종 피해율 산출 이후에는 시각화 프로그램을 통해 이를 가시화한다.

사이버 지휘 통제 단계에서의 판단에 도움이 될 수 있도록, Fig. 9.과 같이 전체 피해율뿐만 아니라 각 유닛 별로 수식 (1), (2), (3)의 피해율을 가시화한다. 또한 하나의 PC보다 서버에 가해지는 피해가 더욱 치명적이므로, PC와 서버의 피해율을 각 공격의 분류 별로 나누어 표현한다. APT Stuxnet 공격 피해 시나리오를 시뮬레이션에 적용했기 때문에, 공격의 특성상 시스템 마비로 인해 Interruption 수치가 높은 것을 알 수 있다.

또한 각 Unit내에서 피해를 받은 공격분류 마다

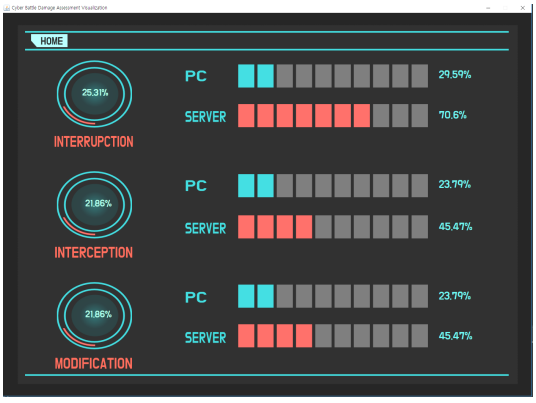

Fig. 9. Cyber Battle Damage Rate Visualization

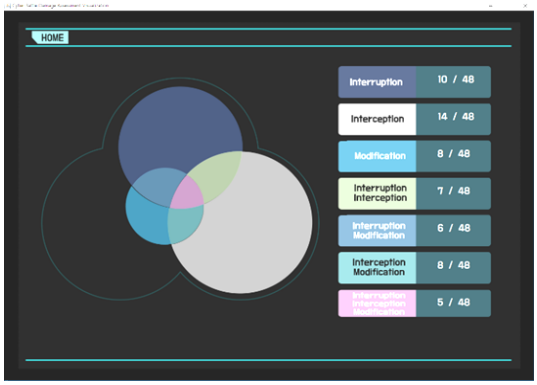

Fig. 10. Unit&Server MOCE Ratio

의 PC와 서버 개수를 알게 되면, 피해 분류 별로 대처가 가능하다. 그렇기 때문에 Fig. 7.과 같이 각 공격의 효과 분류, 즉 MOCE의 분류별로 피해를 받은 PC와 서버의 개수를 표현한다.

기존의 시뮬레이션은 공격의 분류별로 피해를 받은 개체의 수를 단순히 number of failures(피해 개체 수/전체 개체 수) 형태로 표현한다. 그러나 본 논문의 시뮬레이션에서 선정한 APT Stuxnet 공격은 복합적인 공격이다. 그렇기 때문에 공격의 한 분류에만 국한되지 않고, 동시에 다수의 공격 분류의 피해를 입힐 수 있다. 이를 기존 시뮬레이션의 표현 방식으로는 동시에 피해를 입힌 공격 분류 별 피해를 표현할 수 없다. 그러므로 사이버 지휘 통제 단계의 판단에 직관적인 도움이 되기도 어렵다. 그러하여 본 논문에서는 공격 분류별로 피해를 받은 개체의 수를 벤 다이어그램 형태로 표현한다. 이 표현 방식을 사용하면 각 개체별로 동시에 어느 공격 분류의 피해를 받았는지 파악하기 쉽다. 또한 이런 직관적인 형태의 표현으로 인해 지휘관이 사이버 지휘 통제 단계에서 판단의 지표로 사용하기 용이하다.

IV. 결 론

본 논문에서는 MOCE 산출 식을 통해 사이버 공격에 대한 피해를 산출할 수 있는 사이버전의 피해평가 시뮬레이션 시스템을 설계 및 구현했다. 또한 사이버 지휘 통제 단계에서 지휘관의 판단을 돕기 위해, 공격 분류별 피해 받은 개체의 수를 벤 다이어그램 형태로 표현하여 직관적으로 가시화하였다.

시뮬레이션 형태로 사이버 공격에 대한 피해를 평가하는 시스템이 기존에 공개되어 있지 않기 때문에

비교 및 신뢰도 검증이 어렵다. 그러므로 추후에 시뮬레이션을 반복 수행하여 산출한 결과물과 실제 사이버 공격으로 피해를 입은 결과물로 데이터셋을 구성하여, 시뮬레이션에 대해 신뢰성을 증명할 예정이다.

References

[1] O. A. Hathaway, et al. 2012. "The Law of CyberAttack." California Law Review 100 (4), pp. 817-885. Aug. 2012.

[2] Sung-Do Chi, et al. "Network Security Modeling and Cyber Attack Simulation Methodology." Springer, 6th Australasian Conference, ACISP 2001, pp. 321-333 Jul. 2001.

[3] J. D. Howard and T. A. Longstaff, "A Common Language for Computer Security Incidents," Sandia Report: SAND 98-8667, Sandia National Laboratories,http://www.cert.org/research/taxonomy_988667.pdf, Oct. 1998.

[4] M. D. Horony, "Information System Incidents: The Development Of A Damage Assessment Model". Department of Engineering and Management. Wright Patterson Air Force Base, OH, Air Force Institute of Technology, Dec. 1999.

[5] S. Musman, et al. "Computing the impact of cyber attacks on complex missions." Systems Conference (SysCon), 2011 IEEE International. IEEE, pp. 46-51, Apr. 2011.

[6] S. Musman, A. Temin, M. Tanner, D. Fox, and B. Pridemore. "Evaluating the Impact of Cyber Attacks on Missions." MITRE Technical Paper, pp. 09-4577, Jul. 2010.

[7] S. Musman, A. Temin. "A cyber mission impact assessment tool." Technologies for Homeland Security (HST), 2015 IEEE International Symposium on. IEEE, 2015.

[8] Jinho Park et al. "A Proposal of Classification System on Cyber Attack for Damage Assessment of Cyber Warfare." The Korea Information Processing Society Fall Conference 2017. KIPS, pp. 235-238, Nov. 2017.

[9] Duhoe Kim et al. "Cyber Battle Damage Assessment Framework and Detection of Unauthorized Wireless Access Point Using Machine Learning." The 7th International Conference on Frontier Computing - Theory, Technologies, and Applications, FC 2018, pp. 41-49, Jul. 2018.

[10] Jinho Park et al. "Suggestion of Measurement to Calculating the Importance of Cyver Assets." 2018 Korea Information and Communications Society, KICS 2018, pp. 365-366, Jun. 2018.

[11] T. G. Kim, C. H. Sung, S.-Y. Hong, J. H. Hong, C. B. Choi, J. H. Kim, K. M. Seo, and J. W. Bae, "DEVSim++ Toolset for Defense Modeling and Simulation and Interoperation." The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, pp. 129-142, Nov. 2010.

〈저자소개〉

박 진 호 (JinHo Park) 학생회원
2017년 8월~현재: 세종대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 사이버보안, 사이버전, 사이버 피해평가, 머신러닝

김 두 회 (DuHoe Kim) 학생회원
2015년 2월: 세종대학교 컴퓨터공학과 졸업
2015년 3월~현재: 세종대학교 컴퓨터공학과 석박사과정
〈관심분야〉 정보보호, 사이버 피해평가, 머신러닝

신 동 일 (DongIl Shin) 종신회원
1988년 2월: 연세대학교 컴퓨터과학과 졸업
1993년 2월: Washington State University 컴퓨터과학과 석사
1997년 2월: North Texas University 컴퓨터과학과 박사
1998년 3월~현재: 세종대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 생체신호 데이터처리, 데이터마이닝, 머신러닝

신 동 규 (DongKyoo Shin) 종신회원
1986년 2월: 서울대학교 계산통계학과 졸업
1992년 2월: Illinois Institute of Technology 컴퓨터과학과 석사
1997년 2월: Texas A&M University 컴퓨터과학과 박사
1998년 3월~현재: 세종대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 유비쿼터스 컴퓨팅, 생체신호 데이터처리