사이버전 피해 평가를 위한 사이버 공격의 분류 체계 제시

박진호*, 김용현**, 김동화**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소

A Proposal of Classification System on Cyber Attack for Damage Assessment of Cyber Warfare

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

요 약

최근에는 랜섬웨어의 일종인 '워너크라이' 등의 바이러스로 인한 피해도 기하급수적으로 증가하고, 그 수법도 사용자가 파일에 접근하면 감염되던 형태에서 인터넷에 접속되기만 하면 감염되는 형태로 진화하면서 사이버전에 사용되어질 수 있는 사이버 공격에 대응하는 방어 및 회복 방책에 대한 관심이 한층 더 증폭되고 있다. 하지만 일반적으로 방어, 회복 등의 대응 과정은 공격의 피해를 평가하여 결과로 산출된 피해 정도를 전제 조건으로 가지기 때문에 먼저 해킹 공격의 피해를 평가하여야 한다. 본 논문에서는 사이버전에서 사용되어질 수 있는 해킹 공격 및 위협의 피해를 공격의 종류별로 평가하기 위해, 피해 정도를 수치화할 수 있는지의 여부 등을 기준으로 하여 총 3가지 Interruption, Modification, Interception 로 구성된 해킹 공격의 분류 체계를 제시한다.

1. 서론

현재 우리는 '4차 산업혁명의 시대', 사물과 사물, 인간과 사물이 연결되는 초연결성을 기반으로 하여 '초연결시대'라고도 불리는 시기에 도래하였다. 하지만 초연결성의 순기능을 추구하지 않고 악의적인 의도를 포지한다면 단순 사이버 공격에 그치지 않고 범국가적인 사이버 위협을 초래할 수 있다.

사이버전의 배경이 되는 사이버 공간은 상당히 개방적이고 상호의존적이기 때문에 앞서 말한 악의적인 사이버 위협을 통해 대규모의 이익을 취하려는 시도가 점진적으로 증가하고 무방비하게 위협에 노출된다면 국가 안보에 있어서도 큰 문제를 발생시킬 가능성이 높다.

최근에는 랜섬웨어의 일종인 (그림 1)의 '워너크라이' 등의 바이러스로 인한 피해도 기하급수적으로 증가하고, 그 수법도 사용자가 파일에 접근하면 감염되던 형태에서 인터넷에 접속되기만 하면 감염되는 형태로 진화하면서 사이버전에 사용되어질 수 있는 사이버 공격에 대응하는 방어 및 회복 방책에 대한 관심이 한층 더 증폭되고 있다.[1]

하지만 일반적으로 방어, 회복 등의 대응 과정은 공격의 피해를 평가하여 결과로 산출된 피해 정도를 전제 조건으로 가지기 때문에 먼저 해킹 공격의 피해를 평가하여야 한다. 그러나 사이버 공격의 종류는 굉장히 많기 때문에 공식을 하나만 산출하여 사이버 공격에 대한 피해를 평가할 경우 시스템의 피해 정도에 대한 정확도가 감소할 확률이 크다. 그래서 정확도가 감소하지 않고, 필요 이상으로 세분화되지 않으며, 모든 종류의 공격을 포함할 수 있는 새로운 사이버 공격의 분류체계가 필요하다.

(그림 1) 랜섬웨어 '워너크라이'의 감염 화면

이에 본 논문에서는 사이버전에서 사용되어질 수 있는 각종 사이버 공격의 피해를 평가하기 위해 공격의 종류를 피해 정도를 수치화할 수 있는지의 여부, 분류 간의 목적과 개념이 분명하게 상이한지의 여부, 사이버전에서 사용 가능한지의 여부 등을 기준으로 한 사이버 공격의 분류 체계를 제시한다.

2. 관련연구

사이버 공격을 공격받은 시스템의 피해를 평가할 만큼 큰 범주로 분류하기 위해서는 근간으로 삼을 수 있는 공격을 분류할 기준이 필요한데, 개개의 공격 기법들을 분류하는 기준이 되기 때문에 본 논문에서 분류할 기준보다 더욱 세분화된 해킹 기법들을 대상으로 하는 해킹 기법의 분류 기준은 기준 선정에 근간이 된다고 할 수 있다. 하지만 해킹 기법의 분류 기준에는 필요 이상으로 세분화된 기법들이 속하기 때문에, 그에 맞춰서 공식을 산출하기에는 어려움이 따를 수 있다.

해킹 기법 분류의 기준은 분류 대상이 세분화되어 있는 해킹 기법들이기 때문에 이에 맞춰서 공식을 산출하기 어렵다는 것에 반해, (그림 2)와 <표 2>의 분류에서는 보다 큰 범주를 가진 분류에 대해 다룬다.

해킹 기법은 공격할 때의 동작방식, 공격의 목표, 즉 해커가 얻고자 의도한 것, 그리고 사용하는 취약점 등을 기준으로 분류한다.

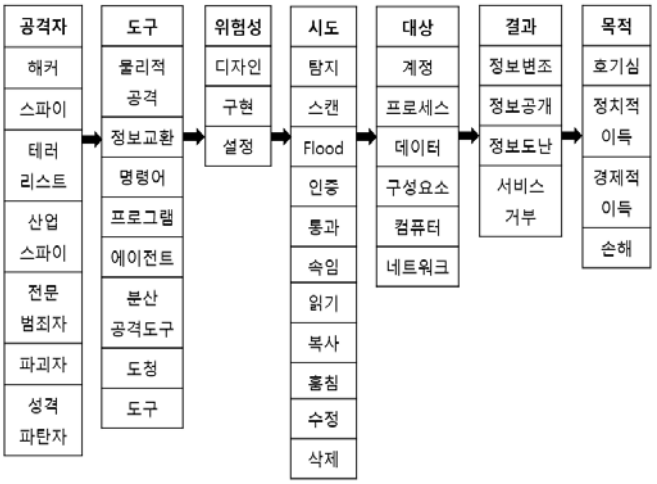
해킹 기법의 분류에서 한 해킹 기법은 여러 분류에 포함될 수 있다. 분산 서비스 거부 공격(DDos Attack)을 예로 들면, 아래의 <표 1>에 명시된 기준 1,2의 공격의 목적, 그리고 사용하는 취약점의 종류, 총 두 가지의 기준에 모두 속할 수 있다. 이런 경우에는 우선순위에 따라 해킹 기법을 분류한다.[2]

<표 1> 해킹 기법 분류 기준

분류기준	내 용
기준 1	공격의 목적
기준 2	사용하는 취약점의 종류
기준 3	기준 1, 2외의 기법은 기타로 분류

이렇듯 세워놓은 분류의 기준에서 2 가지의 기준에 모두 부합할 경우에는 우선순위에 따라 기준에 하나만 속하도록 정의하는 것을 알 수 있는데, 이에 따라 큰 범위 내에서 목적이나 개념이 유사한 범주들은 우선순위에 따라 택일하여 분류체계에 포함한다.

해킹 사건은 악의적인 목적으로 사이버 공격, 즉 해킹을 시도하여 발생하는 것을 의미한다. 2-1에서의 세분화된 해킹 기법 분류의 기준은 실제로도 바로 사용이 가능한 사이버 공격 기법의 기준을 나타내지만, (그림 2)의 해킹 사건의 분류는 좀 더 포괄적이고 큰 범주로, 해킹 사건이 발생하였을 때에 사건을 구성할 수 있는 모든 요소들을 분류한다. 그리고 분류한 항목이 될 가능성이 있는, 즉 후보가 될 수 있는 것들을 포함한다.



(그림 2) 해킹 사건의 분류

(그림 2)에서는 해킹 사건의 분류를 크게 공격자. 도구, 위험성, 시도, 대상, 결과, 목적으로 나누고 있다. 본 논문에서는 결론적으로 사이버 공격을 분류해야하기 때문에, 이 항목들 중에서 필요한 항목은 '시도'다. 이 항목에 포함된 해킹 시도의 종류는 다음의 <표 2>와 같다.[3]

<표 2> 해킹 시도의 종류

종류	설 명
탐지	특성을 알기 위해 목표에 액세스
스캔	명확한 특성을 가진 목표 식별을 위해 순차적으로 일습의 목표에 액세스
Flood	목표의 용량에 과부하를 주기 위해 반복적으로 목표에 액세스
인증	목표에 접근하기 위해 신원 증명
통과	목표에 접근하기 위해 대체 방법을 사용하여 인증 과정을 회피
속임	네트워크 내의 다른 개체로 가장
읽기	저장 장치 혹은 다른 데이터 매체 내의 데이터를 획득
복사	원래 목표의 변경 없이 목표를 복사
훔침	목표의 복사 없이 목표를 획득
수정	목표의 내용 또는 특성을 변경
삭제	목표를 삭제하거나 복구 불가 상태로 만듦

해킹 기법의 분류보다는 광범위하지만 해킹 시도의 분류에서도 그 피해의 정도를 수치화할 수 없고, 수행하는 일이나 개념 및 목적이 중복되는 항목이 있으며, 항목들의

수가 많아서 피해를 평가하기에 적합한 분류체계라고는 말할 수 없다.

<표 2>의 항목들을 그 개념과 목적, 실제 수행하는 일, 피해 정도의 수치화 가능 여부 등에 따라서 선택한다면, 분류 체계에 적용이 가능하다.

3. 본론

사이버 공격의 분류는 크게 Degradation(저하), Modification(수정), Interruption(중단), Fabrication(위조), Unauthorized use(비인가사용), Interception(도청)으로 분류할 수 있다. 이 분류에 대한 개념 및 목적은 다음과 같다.

<표 3> 사이버 공격의 분류

종류	설 명	시도 종류	
저하	목표 시스템의 정보 전달 비율, 품질, 정밀도 감소	Flood	탐지, 스캔
수정	목표 시스템의 내용 또는 특성을 변경	수정, 삭제	
중단	목표 시스템에 과부하를 주어 목표의 프로세스 실행 불가	Flood	
위조	목표 시스템에 거짓된 정보를 삽입 혹은, 목표의 정보를 위·변조	수정	
비인가 사용	인증과정 없이 목표 시스템에 접근	인증, 통과	
도청	목표 시스템의 정보를 사용하거나 획득	속임, 읽기 복사, 훔침	

<표 3>에서 사이버 공격의 분류의 개념을 해킹 시도의 분류의 개념과 비교해봤을 때, 탐지와 스캔의 개념은 사이버 공격 분류의 모든 항목에 포함되고, Flood의 개념은 저하와 중단에, 수정과 삭제의 개념은 수정에, 수정의 개념은 위조에, 인증과 통과의 개념은 비인가 사용에, 속임과 읽기와 복사, 훔침의 개념은 도청에 포함된다. 포함되는 관계를 보면 사이버 공격의 분류에 해킹 시도의 분류가 포함되므로 더 큰 범위임을 알 수 있다.

피해를 평가하는 공식에 시스템의 각종 피해 수치를 삽입하여 최종적으로 피해를 산출해야하기 때문에, 분류체계의 가장 중요한 조건은 수치화의 가능 여부이다. 그렇기 때문에 비인가 사용은 단지 목표 시스템에 별도의 인증 과정 없이 접근하는 항목으로, 인증 과정을 회피하기 위한 권한 획득은 수치화하기 불분명하고, 권한을 얻는 목적이 다른 항목들과 중복되며, 그 외에도 수치화할만한 요소를 내포하지 않기 때문에 조건에 부합하지 않는다.

또, 그 개념이나 목적, 수행하는 공격의 과정이 중복되지 않아야 하는데 저하와 중단은 두 항목 모두 Flood가 속하며 목표 시스템의 프로세스 혹은 정보 전송을 중단시켜 지연하는 목적을 가지는데, 근본적인 목적은 중단이고 총 중단된 시간 등의 수치화할 수 있는 요소들을 포함하므로 중단을 분류체계에 포함한다. 이와 유사하게 수정과 위조도 두 항목 모두 수정이 포함되고 시스템 내 정보의 정확성에 영향을 미친다는 목적을 가지는데, 시스템의 정보 및 특성을 변경하는 수정 항목이 더 포괄적이므로 수정을 분류체계에 포함한다.

<표 3>에서 분류된 사이버 공격의 항목들을 수치화 가능 여부, 개념 및 목적의 중복 여부 등의 조건을 통해 <표 4>로 수정(Modification), 중단(Interruption), 도청(Interception)으로 구성된 피해를 평가하기 위한 분류체계를 산출했다.

<표 4> MOE 설정을 위한 사이버 공격의 분류

종류	설 명
수정 (Modification)	목표 시스템의 정보 혹은 특성을 수정
중단 (Interruption)	목표 시스템에 반복적으로 액세스하여 목표의 프로세스 및 정보전송 중단, 지연
도청 (Interception)	목표 시스템의 정보를 사용하거나 획득

4. 결론

본 논문에서는 최종적으로 공격자의 의도를 파악하고 의도별로 사이버 공격으로 인한 피해를 평가하기 위해 공격의 분류 기준을 세우고 이에 부합하는지를 가려 수정(Modification), 중단(Interruption), 도청(Interception)의 총 3가지 항목으로 분류한다.

결과로 도출된 분류체계의 각 항목들에 속하는 요소들을 조사하고 이를 연산하는 피해 평가 공식을 산출하면, 실제 사이버전에서 받은 공격의 피해를 공격자의 의도에 맞춰 분류하고 평가할 수 있을 것이다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] 정대장, 배우정, 이성호, 전영조. (2017). “4차 산업혁명 시대의 사이버전 위협과 우리 군의 대응” 국방과 기술,

(462), 114-121.
[2] 최양서, 서동일, 손승원. (2001). “네트워크 보안평가를 위한 해커 및 해킹기법 수준 분류” 정보보호학회지, 11(5), 63-74.
[3] Ryan T. Ostler, Captain, USAF “Defensive cyber battle damage assessment through attack methodology modeling” Department of the Air Force. Air University.