피해시스템 기반의 확장형 공격 분류기법

최윤성*, 최동현, 조혜숙, 이영교, 김승주, 원동호**

성균관대학교 정보통신공학부 정보보호연구소

Extendable Victimized-System-Based Attack Taxonomy

Younsung Choi*, Donghyun Choi, Heasuk Jo, Younggyo Lee, Seungjoo Kim, Dongho Won**

Information Security Group, School of Information and Communication Engineering, SungKyunKwan University

요 약

컴퓨터의 정상적인 활동을 방해하는 공격행위는 네트워크로 연결된 컴퓨터를 기반으로 하는 사회 활동이 증가함에 따라 심각한 문제를 유발하고 있다. 하지만 기존의 네트워크 및 시스템 공격에 대한 분류기법은 주로 공격자 입장에서 연구되어서 피해를 입은 시스템이 사용하기에는 부족하였다. 그래서 피해시스템 입장에서 공격을 정확히 분류하고 탐지할 수 있는 분류기법을 개발하는 것은 중요하다. 본 논문에서는 기존의 공격 분류방식을 분석하여 문제점을 발견한 후, 공격 분류방식이 가져야할 요구사항을 도출한다. 공격 분류기법의 요구사항을 만족하면서, 피해시스템의 관리자가 공격에 대한 대책수립에 도움이 되는 공격 분류기법을 제안한다. 제안하는 분류기법은 공격방식에 따라 확장이 가능하므로 복합적 공격을 보다 정확하게 분류할 수 있다.

I. 서론

오늘날 사회는 수많은 컴퓨터가 연결되어 거대한 네트워크를 이루고 있다. 컴퓨터를 통한 조직과 개인의 사회 활동의 증가에 따라 컴퓨터에 대한 생활 의존도가 점차 증가하고 있다. 이러한 관점에서 볼 때, 컴퓨터 시스템에 불법적으로 침입하는 공격자의 존재는 매우 심각한 문제를 유발한다.

기존의 공격 분류기법은 공격자 관점의 간단한 공격 분류기법들이다. 이러한 분류기법에 의한 공격의 분류는 제한적이고, 공격자의 관점이기 때문에 IDS를 통한 공격 탐지나 피해를 입은 시스템에 대한 대책수립에 이용하기에는 효율적이지 못한 구조이다.

피해시스템 입장에서 시스템과 네트워크의 침해 사항들에 대해 신속하게 대처할 수 있는 공격 분류기법에 관한 연구가 필요하다.

* 주저자 : yschoi@security.re.kr
** 교신저자 : dhwon@security.re.kr
본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(ITRC) 육성·지원사업의 연구결과로 수행되었음.

기존의 공격자 관점의 공격 분류기법의 문제점을 분석하여, 공격 분류기법이 가져야할 요구사항들을 도출할 필요성이 있다. 그 요구사항에 부합하면서, 피해시스템 관점의 공격 분류기법을 본 논문에서 제안하고, 이에 따른 확장성과 정확성을 보다 높은 분석을 통해 제시한다.

본 논문은 다음과 같이 구성된다. 2장에서 기존의 공격분류방법에 대해 분석한 후, 문제점과 그것을 보안하는 공격 분류방법의 요구사항을 다룬다. 그리고 3장에서 제안하는 공격분류방법에 대해 설명한다. 4장에서는 제안하는 기법의 성능 평가 및 분석을 한다. 5장에서 결론 및 향후 과제에 대해 알아본다.

II. 기존의 공격 분류방법

2.1 Howard의 공격분류

John Howard가 제안한 이 분류법은 1989년 ~ 1995년 사이에 CERT에 보고된 컴퓨터와 네트워크 관련 사고들을 분류하는데 사용되었다. 시스템에 침입이 발생한 이유와 시스템 접근

시 무엇이 사용되었는지, 공격의 결과가 무엇인지, 그리고 공격의 목적이 무엇인지 등을 사용하여 분류법을 정의하였다[1,4].

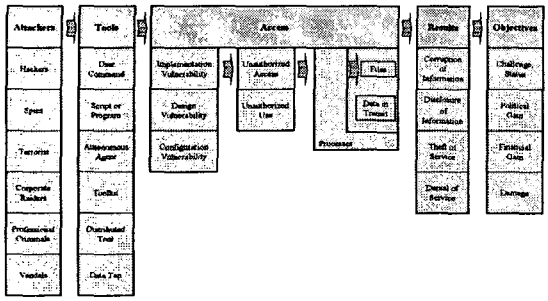

그림 1. Howard's Process Based Taxonomy

2.2 Jayaram & Morse의 공격분류

Jayaram과 Morse는 네트워크 시스템을 손상시킬 수 있는 방법들을 기준으로 공격기법을 분류하였다. 자세한 분류는 표 1과 같다[2].

표 1. Jayaram & Morse의 공격분류

공격분류	설명
Physical	실제로 컴퓨터의 부품을 훔치는 등의 행동을 통해 컴퓨터 보안상의 문제점을 야기함
System Weak Spots	운영체제나 다른 시스템 소프트웨어의 취약점을 이용함
Malign Programs	바이러스 같은 악의적인 프로그램을 통하여 시스템의 데이터를 변경하거나 파괴함
Access Rights	패스워드를 Crack 하거나 트랩을 이용해서 권한을 얻는 방법
Communication-base	불법적인 정보 접근을 위해서 네트워크 접속가능성을 자유롭게 하는 공격함

2.3 Curtis A. Carver의 공격분류

Curtis A. Carver는 기존의 공격 분류기법을 분석하여 새로운 공격 분류기법을 제안하였다. Curtis A. Carver가 제안하는 방식은 크게 6가지 기준을 사용한다.

첫 번째 분류기준으로는 탐지시점(Timing)을 제시하였다. 두 번째로는 공격의 유형이다. 이 분류에서는 Lindqvist와 Jonsson의 분류 방식을 도입하였다. 세 번째 기준은 공격자의 유형이다. 즉 공격하는 사람이 속해 있는 기관이나 조직에 따라 분류한 것이다. 네 번째는 공격의 강도(Degree of Suspicion)이다. 즉 공격의 피해 정도에 따라서 분류하는 것이다. 다섯 번째 분류기준은 공격의 영향(Implication of Attack) 이다. 같은 공격이라도 단일 워크스테이션이 받는 영향과 DNS 서버가 받는 영향은 다른 것이기 때문이다. 마지막 기준은 환경적 제약(Environmental Constraint)이다[3].

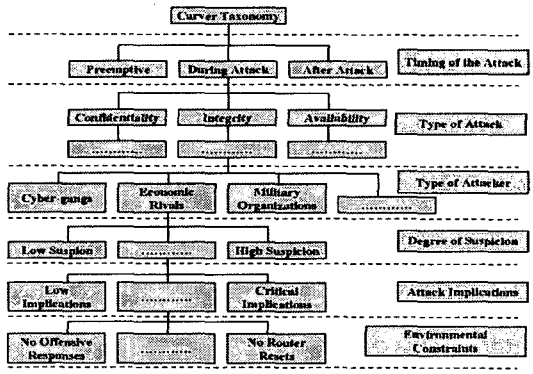

그림 2. Curtis A. Carver's
An Intrusion Response Taxonomy

2.4 공격분류 방법의 문제점

가. 공격자 중심적이다.

피해를 입은 시스템 기반이 아니라, 공격자 입장에서 분류되어서 IDS를 통하여 공격을 탐지하거나, 피해를 입은 시스템에 대한 대책 수립하기에는 불충분하다.

나. 상호배타적이지 못하다.

하나의 공격이 여러 범주에 속하게 된다. 예를 들어, Howard의 분류법에서 Tools 카테고리 내에 Toolkit은 Script or Program과 Autonomous Agent를 결합하여 만든 하나의 소프트웨어 패키지이므로 Script or Program과 서로 배타적이지 못하다.

다. 모든 공격에 적용하지 못한다.

Howard의 분류법은 컴퓨터 보안상의 취약점이나 시도 가능한 공격기법들을 모두 열거하기 보다는 공격의 진행과정(process)에 초점을 맞추어 분류하였다.

III. 요구사항 및 공격 분류기법 제안

본 절에서는 공격 분류기법이 가져야할 요구사항에 따른 새로운 공격 분류기법을 제안한다. 제안하는 공격 분류기법은 크게 Level 1의 시스템 피해 와 Level 2의 공격방식으로 독립적으로 구분된다.

공격의 분류는 Level 1에서 Level 2의 순서로 진행되며, Worm와 같은 복합적 공격은 Level 2에서 다시 Level 1으로 반복 진행된다.

◇ 공격분류기법의 요구사항

기본적인 공격 분류기법의 요구사항과 2.4절에서 분석한 기존 공격 분류기법의 문제점을 분석하여 새로운 요구사항을 도출하였다.

- Accepted : 공격 분류기법들은 명확하게 구조화되어 있어서 모든 공격들을 분류할 수 있어야 한다.
- Determinism : 공격을 분류하는 처리과정이 명확해서 해당 공격의 특징을 뽑아낼 수 있어야 한다.
- Mutually exclusive : 하나의 공격은 하나의 범주 안에만 포함되어 분류되어야 한다.
- Unambiguous : 어떤 공격이 어느 범주에 포함되는지 애매모호함이 없도록 분류기법 내의 범주는 명확히 정의되어야 한다.
- Useful : 정의된 분류기법들은 보안 관련 산업에 유용하게 이용될 수 있어야 한다.

3.1 공격 분류기법 (Level 1 : 시스템 피해)

시스템이 입은 피해는 매우 다양하고. 모든 피해를 열거하여 분류한다면 그 분류범위가 너무 방대할 것이다. 그래서 Level 1에서는 시스템의 실질적 피해를 중심으로 다음과 같이 5개로 나누었다.

가. 서비스 중단
나. 악의적 코드의 저장
다. 공격자의 불법적 권한 획득
라. 시스템의 비정상적인 행동
마. 정보의 누출 및 수정

3.2 공격 분류기법 (Level 2 : 공격방식)

Level 2에서는 공격의 분류를 정확하게 하기 위해서, 시스템의 피해분류 뿐만 아니라 피해 시스템 입장에서 보는 공격방식을 4단계로 나누어 분류한다. 공격의 4단계인 취약점, 피해대상, 침투방법, 경로는 공격의 종류가 증가함에 따라 확장이 가능하다.

가. 1단계 - 경로

유선네트워크, 무선네트워크, 시스템에 물리적으로 접근 등과 같은 공격이 시스템에 피해를 입힌 공격경로를 말한다.

나. 2단계 - 침투방법

공격에 사용된 프로토콜(TCP, UDP 등)이나 바이러스가 저장된 USB 이동저장장치와 같은 공격되는 침투방법을 말한다.

다. 3단계 - 피해대상

Software(MS-office 등), Hardware(HDD, 네트워크카드 등), 시스템이 제공하는 서비스와 같은 피해가 발행한 대상 시스템을 말한다.

라. 4단계 - 취약점

Buffer Overflow, guest 계정 등과 같은 공격의 원인이 된 시스템 취약점을 말한다.

IV. 제안 기법의 성능평가 및 분석

이 절에서는 제안한 공격분류기법을 사용하여 Mass-Mailing worm, Trinoo(DDOS), SYN Flooding Attack에 제안하는 공격 분류기법을 적용시켜보겠다.

4.1 피해에 따른 공격 분류기법(Level 1) 적용

Level 1에서는 시스템의 피해를 공격의 분류를 시스템의 피해상황만을 가지고 간단히 정리할 수 있다. 시스템이 입은 피해만을 분석하면 다음과 같이 간단히 작성할 수 있다.

가. Mass-Mailing worm

Mass-Mailing worm 공격을 받은 시스템 A에 한순간에 수많은 E-mail이 전달됨으로 써 시스템에 비정상적인 행동을 하게 된다. 그리고 E-mail을 보내온 시스템 B에게 E-mail를 보내게 하는 악의적 코드가 저장된 것이 원인이었다. 그림 3은 Mass -Mailing worm 공격으로 분류하는 과정을 도식화한 것이다.

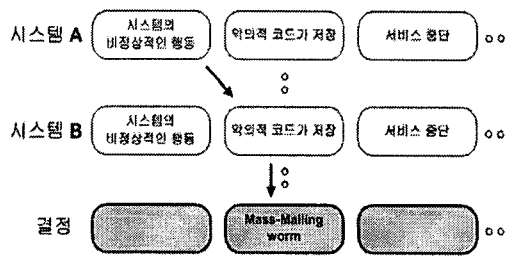

그림 3. Mass-Mailing worm의 분류과정

나. Trinoo(DDOS)

Trinoo(DDOS) 공격을 받은 시스템 A은 제공하던 서비스가 중단되는 현상이 발생했다. 그 이유는 다른 시스템 B에서 시스템 A의 자원을 소비시키는 비정상적인 행위를 하였기 때문었다. 그리고 그 이유는 공격자가 시스템 B의 접근권한을 불법적으로 얻었기 때문이다. 아래 <그림 4>는 Trinoo(DDOS) 공격으로 분류하는 과정을 도식화한 것이다.

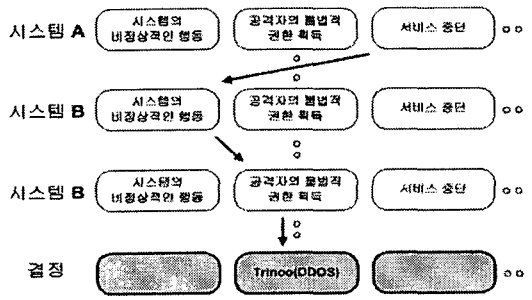

그림 4. Trinoo(DDOS)의 분류과정

4.2 피해에 따른 공격 분류기법(Level 1,2) 적용

SYN Flooding 공격을 받은 시스템 A는 제공하던 서비스가 중단되는 현상이 발생했다. 분석해보니 공격이 들어온 경로는 유선네트워크인 걸로 밝혀졌다, 그 침투방법은 TCP 프로토콜이고, 피해대상은 HTTP 서비스를 제공하는 서버였다. 시스템을 분석해보니 공격자는 SYN 메시지를 받기 전에 통신이 끊지 않는 TCP 자체적 연결 취약성을 이용한 것이 발견되었다. 아래 그림 5는 SYN Flooding 공격으로 분류하는 과정을 도식화한 것이다.

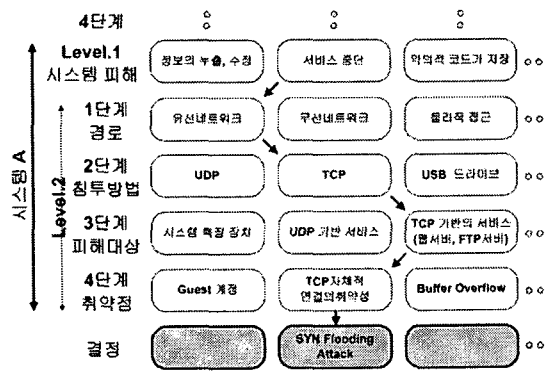

그림 5. SYN Flooding 공격의 분류과정

4.3 제안하는 공격분류 기법의 분석

표 2는 제안하는 공격분류 기법과 기존의 것들을 비교한 결과이다.

표 2. 기존의 공격분류 기법과의 비교

	Howard	NIST	Curtis A. Carver	제안하는 분류방식
Accepted			○	○
Determinism	○		○	○
Mutually Exclusive		○	○	○
Unambiguous	○	○		○
Useful	○	○	○	◎

제안하는 분류방식은 공격방식이 증가함에 따라 확장이 가능하다. 그리고 피해 시스템을 기준으로 하여 시스템 관리자에게 매우 유용하다.

V. 결론

본 논문에서는 기존의 공격분류기법의 문제점을 분석하고, 요구사항을 도출하였다. 그리고 요구사항을 만족하며 시스템의 피해를 중심으로 공격하는 확장형 공격분류 기법을 제안하였다. 제안하는 공격 분류기법이 발전하여, 공격에 대한 대책 수립에 도움이 되었으면 한다.

[참고문헌]

[1] John D. Howard. An Analysis Of Security Incidents On The Internet 1989-1995. PhD thesis, Carnegie Mellon University, 1997

[2] C.A. Carver and U.W. Pooch, An intrusion response taxonomy and its role in automatic intrusion response, Proceeding of the 2000 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2000

[3] Jayaram, N. D. and Morse, P. L. R. Network security: A taxonomic view. In European Conf. Sec. and Detection, IEEE, Apr. 1997

[4] S. Nielson, S. Crosby, D. Wallach. A Taxonomy of Rational Attacks. IPTPS 2005

[5] J. Howard and T. Longstaff, A Common Language for Computer Security Incidents, Sandia Report SAND98-8667, Oct 1998