네트워크상에서의 징후를 기반으로 한 공격분류법

김 기 윤[†] · 최 형 기[††] · 최 동 현[†] · 이 병 희[†]
최 윤 성[†] · 방 효 찬[†††] · 나 중 찬[††††]

요 약

공격 발생시에 네트워크에 나타나는 징후정보를 수집하여 공격을 분류하는 징후기반공격분류법을 제안한다. 이 공격분류법은 공격 발생시 징후를 이용하므로 필요한 정보의 수집이 빠르고 알려지지 않은 공격에 대한 분류가 가능한 장점이 있다. 제안하는 공격법은 두 단계로 공격을 분류한다. 단일 공격자로부터 단일 공격대상에게 나타나는 단일 공격들을 먼저 분류하고 단일 공격들이 서로 연관성 없는 다른 공격들인지 아니면 동일한 하나의 공격을 구성하는 연관된 공격인지 판단하게 된다. 따라서, 이미 제안된 공격분류법보다 정확하게 분산서비스거부공격이나 웜, Bot과 같은 공격을 분류할 수 있게 되었다. 제안하는 분류법을 이용하여 웜과 분산서비스거부공격의 특징 및 근거리통신망에서 발생하는 공격의 특징을 도출하였고 이러한 특징들은 새로운 웜이나 분산서비스거부공격 또는 근거리통신망에서 발생하는 공격들도 공통적으로 가지는 특징임을 보였다.

키워드 : 네트워크 공격, 징후, 공격분류법, 네트워크 보안

A Symptom based Taxonomy for Network Security

Ki-Yoon Kim[†] · Hyoung-Kee Choi[††] · Dong-Hyun Choi[†] · Byoung-Hee Lee[†]
Yoon-Sung Choi[†] · Hyo-Chan Bang[†††] · Jung-Chan Na[††††]

ABSTRACT

We present a symptom based taxonomy for network security. This taxonomy classifies attacks in the network using early symptoms of the attacks. Since we use the symptom it is relatively easy to access the information to classify the attack. Furthermore we are able to classify the unknown attack because the symptoms of unknown attacks are correlated with the one of known attacks. The taxonomy classifies the attack in two stages. In the first stage, the taxonomy identifies the attack in a single connection and then, combines the single connections into the aggregated connections to check if the attacks among single connections may create the distribute attack over the aggregated connections. Hence, it is possible to attain the high accuracy in identifying such complex attacks as DDoS, Worm and Bot. We demonstrate the classification of the three major attacks in Internet using the proposed taxonomy.

Key Words : Network Attack, Symptom, Attack Taxonomy, Network Security

1. 서 론

네트워크에는 많은 공격이 존재하며 계속해서 새로운 공격들이 발견되고 있다. 시만텍이 2006년 3월에 발표한 보고서[1]에 따르면 사이버 범죄를 저지르기 위해 만들어진 보안 위협은 급격한 증가 추세를 보이고 있으며 조사 기간 동안 하루 평균 1402개의 서비스 거부 공격을 발견했다고 명시하고 있다. 공격들은 인터넷을 통해 제공되는 다양한 서비스를 정상적으로 이용할 수 없게 할 뿐만 아니라 개인정보나 군사정보와 같은 중요한 기밀을 훔치거나 경제적 손실을 유발하기도 한다. 국내에서는 키보드 입력정보를 공격자에게 전달하는 키로그라는 악성 프로그램을 이용하여 인터넷 뱅킹에 사용되는 사용자의 개인 정보를 탈취한 후 사용자의 은행잔고를 자신이 만든 계좌로 이체하는 범죄가 발생하기도 했다. 이처럼 네트워크 공격은 위협적이고 그 피해가 심각하므로 예방이나 방어를 통한 시스템의 보호가 절실히 요구된다.

※ 본 연구는 한국전자통신연구원 정보보호연구단의 위탁과제에 의한 것임.
†준 회 원 : 성균관대학교 컴퓨터공학과 석사과정
††정 회 원 : 성균관대학교 정보통신공학부 컴퓨터공학과 교수
†††정 회 원 : ETRI 능동보안기술연구팀 선임연구원
††††정 회 원 : ETRI 능동보안기술연구팀 팀장
논문접수 : 2006년 4월 20일, 심사완료 : 2006년 7월 10일

네트워크 공격들로부터 시스템을 효과적으로 보호하기 위해서는 공격들을 비슷한 유형으로 구분 짓고 공격 유형에 따라 적합한 예방이나 방어 방법을 선택, 적용하여야 한다. 비슷한 유형의 공격들이 포함하는 공통된 특징을 파악하면 해당 유형의 공격들은 그 특징을 이용하여 방어가 가능하기 때문에 효과적으로 시스템을 방어 할 수 있다. 또 새로운 공격이 나타나더라도 동일한 유형의 공격 방어법을 적용할 수 있다. 비슷한 유형으로 공격을 구분 짓기 위해 공격이 가지는 특징을 이용하여 공격을 분류하는 공격분류법들이 제안되었다. 공격분류법은 시스템 방어 방법의 적절한 적용을 위해 요구되는 중요한 항목이므로 시스템 보호를 위해 고려해야 하는 중요한 과정 중의 하나이다.

그러나 제안된 분류법들은 여러 가지 문제를 포함하고 있다. 공격의 분류를 위해 요구되는 정보를 분석하는데 많은 시간이 소모된다거나 정상적인 경우의 모든 시스템 패턴을 알고 있어야 공격분류결과를 신뢰할 수 있다. 공격분류법의 문제점은 곧 방어 방법의 선택에 영향을 미치기 때문에 시스템 방어의 문제점으로 드러난다. 이미 분석된 공격이 아닌 알려지지 않은 공격이 나타날 경우 분류결과를 얻는데 많은 시간이 소모된다는 것은 알려지지 않은 공격에 대한 방어 방법을 찾는데 많은 시간이 소모됨을 의미하며 이는 분석 시간 동안 해당 공격에 시스템이 노출되어 있다는 것을 의미한다. 또, 정상적인 시스템의 패턴을 모두 알지 못할 경우에는 정상적인 시스템의 동작도 공격으로 오인될 수 있으며 이는 방어 시스템에 대한 신뢰도를 떨어뜨리게 된다. 따라서 공격의 분류를 위해 공격을 분석하는데 많은 시간을 소모하지 않고, 정상적인 시스템의 패턴을 분류기준으로 사용하지 않으며 네트워크에 나타나는 공격에 대한 정보를 쉽게 수집하고 빠르게 분류할 수 있는 공격분류법이 요구된다.

새로운 분류법을 구성하기 위해 공격이 발생할 때는 네트워크에 공격의 징후가 나타난다는 점[13][14]과 이기종 센서의 로그를 이용하면 네트워크에 나타나는 다양한 정보를 얻을 수 있다는 점에[12] 주목하였다. 이를 기반으로 본 논문에서는 이기종 센서의 로그에 담긴 네트워크 공격의 징후정보를 이용하여 공격을 분류할 수 있는 새로운 유형의 공격분류법인 징후기반분류법을 제안한다. 징후기반분류법은 공격 시 나타나는 다양한 징후정보를 공격의 분류기준으로 선택하였기 때문에 분류를 위한 정보를 쉽게 얻을 수 있으며, 수집된 정보는 분석을 위해 많은 시간을 소모하지 않고 분류법에 적용이 가능하므로 알려지지 않은 공격도 빠르게 분류가 가능하다. 또 정상적인 시스템의 패턴을 분류기준으로 사용하지 않으므로 정상적인 시스템의 모든 패턴을 미리 등록할 필요도 없다. 따라서 네트워크에 존재하는 이기종 센서의 로그를 이용하여 알려지지 않은 공격 역시 방어가 가능한 방어 시스템의 구축을 가능하게 하는 공격분류법이다. 제안하는 분류법을 이용하여 웜과 분산서비스거부 공격 및 근거리통신망에서 발생하는 공격의 특징을 분석하였으며 분석된 공격의 특징은 새로운 웜과 분산서비스거부 공격 및 근거리통신망에서 발생하는 공격에도 나타날 수 있는 공통적인 특성을 보여준다. 따라서 징후기반분류법을 이용하면 현재 널리 사용되는 침입탐지시스템의 문제점인 알려지지 않은 공격을 탐지하기 위한 공격 특징의 업데이트가 필요 없으므로 새로운 공격도 이미 알려진 공격과 마찬가지로 탐지가 가능할 것이다.

본 논문은 다음과 같이 구성되었다. 2장에서는 관련연구로 제안된 공격분류법에 대해 알아보고 3장에서는 징후기반분류법을 소개한다. 4장에서는 징후기반분류법에 웜, 분산서비스거부공격, 근거리통신망에서 발생하는 공격을 직접 적용해보고 5장에서 결론을 맺는다.

2. 관련연구

공격을 분류하는 기법은 크게 공격기반분류법과 방어기반분류법으로 구분이 가능하다. 공격 진행 과정에 나타나는 공격의 특징과 공격자가 이용하는 취약점이나 공격 방법을 분류 기준으로 선택하는 공격기반분류법은 공격에 대한 분석이 선행되어야 한다. 분류기준으로 공격에 사용되는 도구, 공격 목표, 공격에 이용하는 취약점 등과 같은 정보를 이용하기 때문이다. 따라서 공격기반분류법에 의해 공격을 분류하면 공격의 전체적인 흐름을 파악하기에 효과적이다. 방어기반분류법은 공격으로부터 시스템을 보호하기 위해 공격이 가지는 공격 패턴이나 특징을 분류 항목으로 이용하는 분류법이다. 방어기반분류법은 시스템의 정상적인 동작패턴을 미리 등록하고 공격 시 나타나는 비정상적인 패턴을 이용하여 공격을 분류한다. 따라서 공격기반분류법과는 달리 공격에 대한 분석에 소모되는 시간이 필요하지 않으며 알려지지 않은 공격도 비정상적인 패턴을 통해 분류가 가능하다는 장점이 있다. 그러나 정상적인 경우의 시스템 동작 패턴을 모두 등록해야 하며 누락된 정상패턴이 있을 경우 공격으로 오인될 수 있다는 단점이 있다.

2.1 공격기반분류법

공격기반분류법은 공격의 진행되는 과정에 나타나는 공격의 특징과 공격자가 이용하는 취약점이나 공격 방법을 분류 기준 선택하여 공격을 분류한다. 공격 기반 분류법으로 분류되는 공격 유형들은 공격자로부터 공격 대상까지 공격의 흐름이 자세히 드러나기 때문에 그로 인한 피해나 방어방법을 선택하기에 효과적이다. 그러나 공격자가 공격을 하는 과정이나 공격에 사용되는 도구, 공격의 목적 등 공격에 대한 자세한 정보를 이용하여 분류하기 때문에 새로운 공격에 대한 분류를 위해서는 반드시 공격에 대한 분석이 선행되어야 한다는 단점이 있다.

현재 CERT(Computer Emergency Response Team)에서 사용하는 공격 분류방법은 Howard[2] 가 제안하고 Sandia Lab[3]에서 수정한 공격 기반 분류법이다. 분류기준은 공격자의 유형, 공격에 사용되는 도구, 이용하는 취약점, 공격의

목적 등의 항목들로 구성되어 있다. 공격자의 유형이나 공격에 사용되는 도구와 같은 정보는 공격을 수행한 공격자가 알고 있는 정보이므로 공격을 분류하기 전에 공격을 수행하는 과정에 대한 분석이 요구된다. 따라서 CERT에서는 공격에 대한 피해사례를 리포트 형태로 수집하고 분석하는 과정을 거친다.

NIST(National Institute of Standards and Technology)[4]에서는 2004년에 Computer Security Incident Handling Guide를 통해서 공격 형태를 사용자가 입은 피해 형태에 따라 리소스를 고갈시키는 방식, 악성 코드로 호스트에 영향을 주는 공격, 비 인가된 접근권한(Unauthorized Access), 부적절한 행위(Inappropriate Usage), 복합적 요소 (Multiple Component)의 크게 5가지로 공격 유형을 미리 정의 하였다. 그리고 정의된 공격 형태별로 공격자가 취하는 공격의 방법에 따라 분류를 세분화 하였다. 공격의 결과를 이용하여 공격을 분류하였기 때문에 공격과정에 대한 정보 없이 공격의 결과만으로 쉽게 공격을 분류할 수 있다는 장점이 있으나 복합적 요소 유형의 공격은 분류결과만으로는 어떠한 공격의 특징이 나타나는지 판단하기 어렵다는 단점이 있다.

J. Anderson[5]과 그의 동료는 데이터나 프로그램 자원을 사용할 권한을 가지고 있는지 여부와 컴퓨터를 사용할 권한을 가지고 있는지 여부를 기준으로 공격자의 유형을 분류한 분류법을 제안하였다. 컴퓨터를 사용할 권한과 자원을 사용할 권한을 모두 가진 경우와 각각 한 가지 권한만 가진 경우, 그리고 어떠한 권한도 가지지 못한 경우의 4가지 유형으로 공격자를 분류하였다. 정당한 권한을 가진 사용자의 행위와 권한이 없는 사용자가 컴퓨터나 데이터에 접근하는 행위 등을 분류하기 위한 기준이기 때문에 접근권한에 따라 관리되는 기밀정보의 유출, 조작과 같은 공격들에 대한 분류 항목으로 적합하다. 그러나 사용자의 권한에 대한 자료만으로는 공격의 특징이나 공격의 결과, 이용하는 취약점과 같은 정보를 알기 어렵기 때문에 공격분류법으로 사용하기에는 어려움이 있다.

Jayaram[6]과 그의 동료는 실제로 컴퓨터의 부품을 훔치는 등의 행동을 통해 컴퓨터 보안상의 문제점을 야기하는 공격, 운영체제나 다른 시스템 소프트웨어의 취약점을 이용하는 공격, 바이러스 같은 악의적인 프로그램을 통하여 시스템의 데이터를 변경하거나 파괴하는 행위, 패스워드를 찾아내거나 비정상적인 방법을 이용해서 권한을 얻는 방법, 불법적인 정보 접근을 위해서 네트워크 접속가능성을 자유롭게 하는 공격과 같은 5가지의 공격유형을 공격 분류의 항목으로 정의한 분류법을 제안하였다. 물리적인 취약점까지 분류의 기준으로 사용하여 실제로 일어날 수 있는 보안 문제에 대한 분류항목을 포함하여 공격의 유형을 구체적으로 표현하였다. 하지만 공격의 유형이 중복되어 나타날 수 있다는 단점이 있다. 예를 들어 악의적인 프로그램을 통하여 시스템에 접근할 수 있는 권한을 얻어서 네트워크를 이용하여 허가되지 않은 정보에 접근 가능하도록 하는 공격을 수행한 경우에는 5가지 유형 중 정확히 하나의 유형으로 분류하기 어렵다.

IBM사의 침입탐지시스템인 Tivoli[9]는 공격에 이용되는 취약점과 공격발신지 주소정보와 목적지 주소정보를 이용하여 공격의 단계를 구분하고 단계별로 공격의 유형을 정의한다. 단계를 구분하는 기준은 단일 발신지로부터 시작되어 단일 목적지로 진행되는 공격, 단일 발신지로부터 시작되어 다수의 목적지로 진행되는 공격, 다수의 목적지로부터 시작되어 단일 목적지로 진행되는 공격 등 공격의 발신지와 목적지의 수와 공격에 이용되는 취약점의 종류를 정의하여 공격을 구분한다. 공격발신지 주소정보와 목적지 주소정보는 웜이나 분산서비스거부공격과 같은 공격을 분류하기에 적합한 분류기준이 된다. 웜의 경우 단일 발신지로부터 시작되어 다수의 목적지로 진행되며, 분산서비스거부공격의 경우 다수의 목적지로부터 시작되어 단일 목적지로 진행되는 특징이 있다.

2.2 방어기반분류법

방어기반분류법은 공격으로부터 시스템을 보호하기 위해 공격 시 나타나는 비정상적인 시스템 동작패턴을 분류 항목으로 이용하는 공격 분류법이다. 방어기반분류법은 정상적인 경우와 공격이 나타난 경우의 차이점을 이용하여 현재 공격이 나타나고 있음을 탐지해내고 유형별로 공격을 분류하는 방법이다. 이 방법은 공격자의 유형이나 공격에 사용되는 공격도구, 공격의 목적 등에 대한 정보는 필요하지 않으며 단지 공격 시 나타나는 비정상적인 패턴만을 이용하여 공격을 분류하는 방법이다. 이러한 분류법은 공격 피해사례 수집이나 공격의 분석과정이 요구되지 않기 때문에 새로운 공격이 나타나도 비교적 빠르게 분류가 가능하다는 장점이 있다. 대표적인 방어기반분류법으로는 시스템 콜의 패턴을 이용하는 방법이 있다.

Carnegie Mellon University 의 Killourhy[7]와 그의 동료는 정상적으로 동작하는 컴퓨터의 시스템 콜 패턴을 미리 기록해두고 공격 시 나타나는 비정상적인 시스템 콜의 패턴을 이용하여 공격을 분류하는 방법을 제안하였다. 하지만 시스템 콜을 이용하는 분류법은 호스트기반의 공격분류로 한정되며 정상적인 경우에도 미리 이 패턴이 등록되어 있지 않은 경우 공격으로 분류되는 문제점이 있었다.

University of Maryland, Baltimore County의 Undercoffer[8]와 그의 동료는 공격 대상에 따라 다양한 공격 형태가 나타나는 것을 분류항목으로 사용하는 공격대상기반분류법을 제안하였다. 공격대상기반분류법은 공격의 목표에 따라 공격의 유형이 다르게 나타난다는 점을 이용하여 공격을 분류하는 방법이다. 공격의 목표를 네트워크, 시스템, 프로세스로 구분하고 각 공격대상에 대한 공격의 패턴이 가지는 특징을 이용하여 공격을 분류하였다. 방어기반분류법과 유사하게 정상적인 패턴을 기준으로 공격 목표에 대한 비정상적인 패턴을 분류기준으로 사용한다. 하지만 공격으로 인한 피해가 네트워크와 시스템 모두에게 나타나는 경우처럼

그 대상을 정확하게 정의하기 어려운 경우가 있다는 문제점이 있다.

3. 징후기반 공격분류법

공격에 대한 방어를 위해서는 공격이 사용하는 취약점이나 공격이 띄는 특징을 이해할 필요성이 있다. 그리고 공격이 사용하는 취약점이나 특징을 찾아내기 위해서 공격에 대한 정보를 수집하여 공격을 분석하거나 공격분류법을 이용하여 분류하게 된다. 하지만 앞에서 설명한 공격법을 이용할 경우, 공격기반분류법은 알려지지 않은 공격을 분류하기 위해 공격에 대한 분석시간이 필요하기 때문에 새로운 유형의 공격이 나타날 경우 방어방법을 적용하기까지 그 피해가 확산될 가능성이 있다. 또 방어기반분류법은 정상적인 모든 동작패턴을 등록해야 하고 호스트에 기반한 패턴인식 방법이 사용되기 때문에 네트워크에 나타나는 공격에 대한 분류에 적합하지 않다. 따라서 본 논문에서는 빠른 속도로 새로운 유형의 공격을 분류할 수 있으며 호스트뿐만 아니라 네트워크 전반에 나타나는 공격들도 분류가 가능한 분류법을 제안하고자 한다. 제안하는 분류법은 공격의 대상 측에서 얻을 수 있는 다양한 공격의 징후정보를 이용한 징후기반분류법이다.

3.1 징후기반 공격분류법 소개

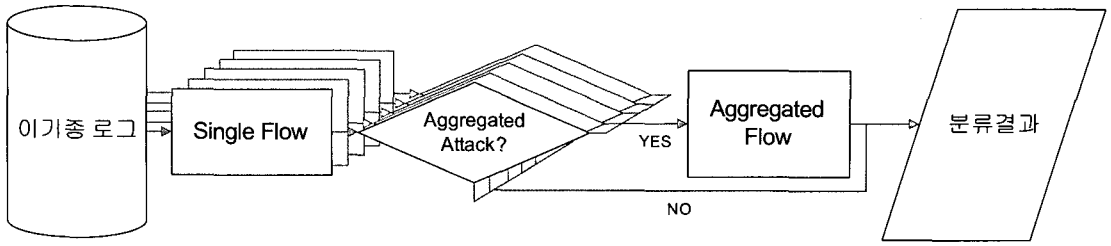
공격이 발생할 때는 공격의 징후가 나타난다. 공격의 징후는 공격 발생 전부터 시작하여 공격이 진행되는 동안에 나타나는데[13][14] 네트워크에 존재하는 다양한 센서들의 로그정보를 이용하면 손쉽게 징후정보를 얻을 수 있다. 징후기반 분류법은 수집한 로그로부터 얻은 징후정보를 이용하여 공격을 분류한다. 징후정보는 네트워크 트래픽의 흔적이나 호스트에 대한 접근기록 또는 침입탐지시스템이나 침입차단시스템과 같은 방어 시스템에 남겨지는 스캐닝, 공격과정에서 발생하는 비정상적인 트래픽의 증가 기록 등이 있으며[13][14] 이러한 기록들은 로그로 남겨진다[12]. 즉, 남겨진 로그를 이용하여 공격의 특징을 찾아내고 찾아낸 특징을 이용하여 공격을 분류할 수 있다는 점에 착안한 분류법이다. 공격기반분류법과는 다르게 피해사례 분석이나 공격에 대한 분석 시간을 소모할 필요가 없으며, 방어기반분류법과 같이 시스템의 모든 정상적인 패턴을 미리 등록해야 할 필요도 없다. 또 알려지지 않은 공격이 나타나더라도 공격의 징후정보를 다양한 센서들의 로그 정보를 통해 수집이 가능하기 때문에 정확한 공격 명칭을 알 수는 없지만 유사한 공격의 징후를 보이는 공격유형에 포함시킬 수 있다. 따라서 알려지지 않은 새로운 유형의 공격에 대한 빠른 대처가 어려운 공격기반분류법이나, 호스트기반에 하며 모든 정상적인 시스템의 동작 패턴을 등록해야만 사용 가능한 방어기반분류법의 한계를 해결할 수 있는 분류법이다.

<표 1>은 공격기반분류법과 방어기반분류법 그리고 징후기반분류법의 특징을 나타낸다. 표에서 알 수 있듯이 징후기반분류법은 기존의 두 분류법의 단점인 공격에 대한 분석시간 요구와 모든 정상패턴에 대한 등록 없이도 알려지지 않은 공격에 대한 분류가 가능하다는 특징을 가진다.

징후기반분류법은 Single-flow와 Aggregated-flow 두 단계의 분류과정을 통해 공격을 분류한다. 첫 번째 단계인 Single-flow는 서비스거부공격(Denial of Service)의 경우처럼 단일 공격자로부터 단일 공격대상에게 나타나는 공격들을 분류한다. 분류 기준은 공격대상, 이용하는 취약점, 공격 시 나타나는 현상, 공격의 결과로 구성된다. 두 번째 단계인 Aggregated-flow는 첫 번째 단계에서 분류된 단일 공격들이 서로 연관성 없는 다른 공격들인지 아니면 동일한 하나의 공격을 구성하는 연관된 공격인지 판단하기 위해 사용된다. 분산서비스거부공격(Distributed Denial of Service)과 같은 공격은 동시에 여러 노드로부터 공격이 발생하는데 이때 각각의 노드로부터 발생하는 단일 공격은 Single-flow에서 분류가 되지만 분산서비스거부공격임을 판단하기 위해서는 분류된 단일 공격들의 특성을 이용하여 다시 한 번 공격형태에 대한 분류를 진행하여야 한다. 특히 두 번째 단계인 Aggregated-flow는 공격 발신지 정보와 목적지 정보를 이용하여 공격을 분류하도록 구성하였다. Aggregated-flow 분류기준은 나타나는 Single-flow 공격들이 각기 다른 공격인지 아니면 공통된 특성을 가지는 동일한 공격의 한 부분인지 구분하기 위해 사용되므로 단일 공격의 분류만으로는 분류해내기 어려운 분산서비스거부공격이나 웜, Bot과 같은 공격을 분류하기 위해 사용된다. Aggregated-flow 공격분류

〈표 1〉 공격분류법들의 특징

분류법	특 징
공격기반	• 공격의 과정에 나타나는 특징과 이용하는 취약점, 공격 방법을 분류 기준으로 선택 • 공격자로부터 공격 대상까지 공격의 흐름이 자세히 드러남 • 피해사례분석이나 공격에 대한 분석 시간이 요구됨
방어기반	• 공격 시 나타나는 비정상적인 시스템 동작패턴을 분류 항목으로 이용 • 공격 분석과정이 요구되지 않으므로 새로운 공격이 나타나도 빠르게 분류가 가능 • 정상적인 시스템 동작패턴이 모두 등록되어 있지 않을 경우 등록되지 않은 동작 역시 공격으로 분류됨
징후기반	• 공격 시 나타나는 징후를 네트워크에 존재하는 센서 로그로부터 수집하여 분류 • 피해사례 분석이나 공격에 대한 분석 시간을 소모할 필요가 없음 • 모든 정상적인 패턴을 미리 등록해야 할 필요도 없음 • 알려지지 않은 공격도 수집된 로그를 이용하여 유사한 형태의 공격으로 분류가 가능



(그림 1) 징후기반 분류법 적용 흐름도

단계는 IBM사의 Tivoli[9]의 공격탐지방법에서 사용하는 공격분류방법을 적용한 분류항목이다.

(그림 1)은 징후기반 분류법을 적용하는 과정을 나타내고 있다. Single-flow를 통해 이기종 센서의 로그로부터 단일한 공격을 분류해 낸다. Single-flow 분류 결과들은 Aggregated-flow 적용 기준에 해당하는지 판단하는 과정을 거친다. 만약 다양한 공격이 단일한 호스트를 향해 같은 시간대에 나타나거나 웜과 같이 동일한 유형의 트래픽이 단위 시간당 비정상적으로 발생할 경우에는 두 번째 단계를 적용한다. 예를 들어 분산서비스거부공격의 징후정보가 담긴 로그로부터 Single-flow 단계를 거쳐 분류된 단일 공격들은 발신지는 다르지만 공격의 목표는 동일한 형태를 띈다. 따라서 공격이 단일한 호스트를 향해 같은 시간대에 나타나므로 Aggregated-flow 적용을 통해 분산서비스거부공격임을 분류해 낸다. 또, 웜의 경우 전파되는 패킷이 가지는 동일한 특징을 가진 단일 공격들이 분류된다. 패킷의 크기와 프로토콜의 종류, 목적지 포트와 같은 항목이 동일한 단일 공격들이 동시에 나타나면 Aggregated-flow 적용을 통해 웜 임을 분류해 낸다. Aggregated-flow 적용 여부를 판단하는 기준은 네트워크의 특성에 따라 통계치를 이용하여 조절할 수 있다. 첫 번째 단계에서 공격의 분류가 종료되거나 두 번째 단계까지 거쳐서 공격의 분류가 종료되면 공격이 유형별로 분류되어 나타난다. 각 단계별 분류 항목에 대해서는 (그림 2), (그림 3)을 통해 상세히 나타낸다.

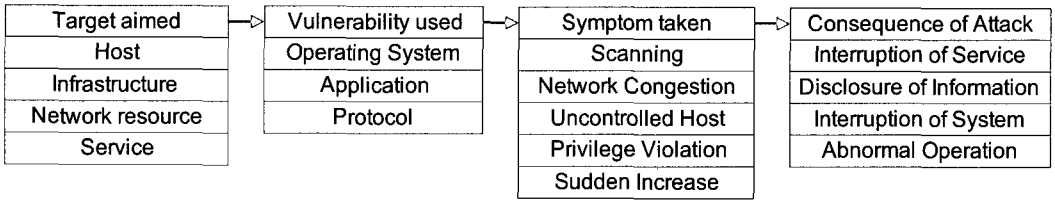
징후기반 분류법의 기준들은 네트워크를 통해 얻을 수 있는 징후정보를 다수 사용하기 때문에 네트워크를 통해 전파되지 않는 바이러스와 같은 공격은 분류법에 적용하기 어렵다. 또, 징후기반 분류법은 전송되는 데이터를 보지 않고 공격을 분류하도록 구성되었기 때문에 네트워크에 나타나는 징후가 정상적인 트래픽의 경우와 구분되는 특징이 없는 공격은 분류법에 적용하기 어렵다. E-메일을 통해 전파되거나 트로이목마처럼 시스템에서 동작하는 공격은 시스템 로그 이외의 정보는 얻기 어렵고, 하드웨어에 대한 물리적인 공격이나 사용자의 실수로 발생하는 사회공학적인 공격 역시 분류하기 어렵다.

3.1.1 Single-flow

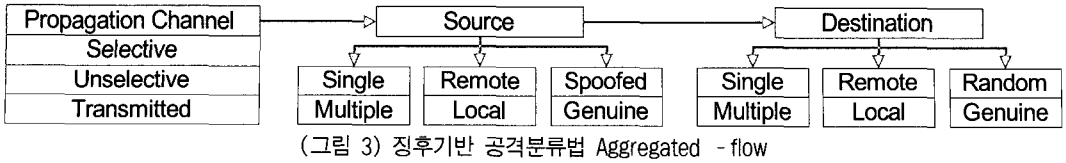
제안하는 분류법의 첫 번째 단계는 Single-flow의 공격 형태를 구분하기 위해 정의된 분류기준이다. 공격이 이용하는 취약점과 공격의 대상, 공격의 결과와 같은 공격 시 나타나는 징후를 이용하여 공격의 유형을 구분하기 위해 사용된다. 분류항목은 Target aimed, Vulnerability, Symptom taken, Consequence of Attack의 4개 항목으로 구성된다. 각 항목에 사용된 분류기준들은 공격을 분류법에 적용할 때 공격분류의 결과가 두 가지 이상의 분류기준에 중복되지 않도록 작성하였다.

1) Target aimed

공격의 대상을 나타내는 것으로 Host, Infrastructure, Network resource, Service 항목으로 구성되어 있다. 실제 공격의 목표가 되는 대상을 파악하여 공격이 나타났을 경우 피해가 발생하는 범위나 방어 대상을 선택하기 위해 요구되는 기준이다.



(그림 2) 징후기반 공격분류법 Single-flow



(그림 3) 징후기반 공격분류법 Aggregated - flow

〈표 2〉 Target aimed 항목

Host	공격의 대상이 되는 네트워크 종단의 단말기
Infrastructure	네트워크 서비스를 지원하는 장비. 예)라우터, 허브
Network resource	대역폭과 같은 네트워크 자원
Service	서버나 개인용 PC에서 제공하는 서비스

〈표 3〉 Symptom taken 항목

Scanning	공격 대상 혹은 취약점 정보를 얻기 위한 행위
Network Congestion	네트워크 대역폭과 같은 자원을 고갈시켜는 행위
Uncontrolled Host	호스트가 비정상적으로 동작하거나 제어되지 않는 경우
Privilege Violation	접근권한이 없으나 비정상적인 방법으로 호스트에 접근
Sudden Increase	트래픽의 양이 급증하여 공격과 유사한 형태가 되는 경우

〈표 4〉 Consequence of Attack 항목

Interruption of Service	정상적으로 제공되던 서비스를 사용이 불가능하도록 했을 경우
Disclosure of Information	접근 권한이 주어지지 않은 정보의 내용을 유출 또는 조작
Interruption of System	시스템을 파괴하거나 손상시켜 사용이 불가능하도록 하는 행위
Abnormal Operation	시스템이 비정상적으로 동작하도록 하는 경우

〈표 5〉 Propagation Channel 항목

Selective	정해진 공격 목표가 있는 경우
Unselective	불특정 다수에 대한 공격
Transmitted	공격 전파 과정에 이용되는 경우. 예) 분산서비스거부공격의 Agent

2) Vulnerability used

공격에 사용되는 운영체제나 응용프로그램 또는 프로토콜 상의 취약점들의 집합을 의미한다. 공격의 특징 중에서 공격의 상세분류나 방어를 위해 유용하게 사용될 수 있는 징후정보이다. 공격을 방어하기 위해서는 공격이 이용하는 취약점을 보완하여 공격을 막는 경우가 많은데 이 분류항목에서 공격에 이용되는 취약점에 대한 분류를 진행함으로써 공격의 방어를 위해 유용하게 사용될 수 있다. 취약점 항목은 Operating System, Application, Protocol의 3가지로 구성된다.

3) Symptom taken

비정상적인 트래픽이나 공격을 받은 대상으로부터 발생하는 비정상행위를 의미한다. Scanning, Network Congestion, Uncontrolled Host, Privilege Violation, Sudden Increase 의 항목으로 구성되어 있다. 공격의 목적이나 결과를 파악하기 위해 사용되는 정보이며, 공격이 시작되기 전에 나타나는 비정상적인 트래픽의 흔적을 포함하고 있다.

4) Consequence of Attack

공격의 진행 결과를 의미하며 공격자의 공격 목적이 드러나는 분류항목이다. 서비스를 정상적으로 사용하지 못하도록 하는 경우나 기밀 정보 혹은 금융 정보와 같이 접근 권한이 주어지지 않은 중요한 정보의 내용을 유출 또는 조작하는 행위, 또 시스템 자체를 파괴하거나 손상시키는 행위나 시스템이 비정상적으로 동작하도록 하는 공격 결과의 항목들을 나타낸다.

3.1.2 Aggregated - flow

두 번째 단계는 Aggregated-flow 형태의 공격을 탐지하기 위해 이용되는 분류항목이다. 첫 번째 단계를 통해 Single-flow 형태의 공격을 분류해 내고 분류된 공격들이 동일한 공격 대상에 대해 반복적으로 나타나거나 동일한 Single-flow 형태의 공격들이 반복적으로 나타날 경우 적용되는 단계이다. Aggregated-flow 형태의 공격은 Single-flow 형태의 공격인 서비스거부공격이 다른 발신지로부터 동일한 대상에게 반복적으로 나타나는 분산서비스거부공격이나 동일한 취약점을 이용하여 시스템을 감염시키는 패킷들이 같은 시간대에 서로 다른 발신지와 목적지로 나타나는 웜과 같은 공격을 의미한다. 이런 공격의 유형은 Single-flow 형태의 공격이 결합된 형태를 띄기 때문에 두 번째 단계를 이용해야 분류가 가능하다.

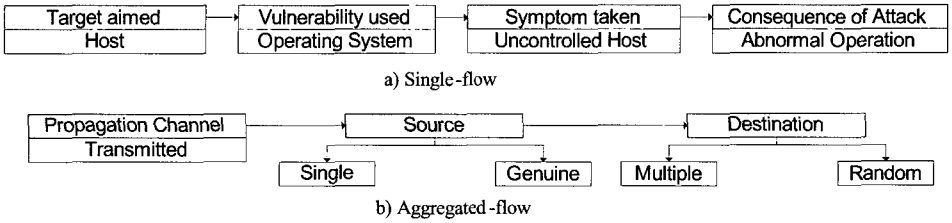
두 번째 단계의 항목들은 Propagation Channel, Source Address, Destination Address로 구성되어 있다. 첫 번째 단계의 항목들처럼 공격이 사용하는 취약점이나 징후정보와는 달리 공격의 확산 과정이나 공격이 시작되는 곳과 목표가 되는 곳의 정보를 이용하여 Aggregated-flow 형태의 공격을 구분하기 위한 항목들로 구성되어 있다. 항목 중 Source Address 및 Destination Address 항목은 주소의 수, 주소의 위치, 주소의 신뢰성을 나타내는 세 가지 하위 항목을 포함하고 있다. 이처럼 세 가지 하위항목을 공격분류의 기준으로 이용하는 이유는 공격이 띄는 특징을 보다 세분화하여 분류하기 위함이다. Aggregated-flow 형태의 공격은 공격 발신지와 공격 목적지에 대한 정보가 그 유형을 구분하는데 중요한 정보가 된다. 이 분류기준들은 세 가지 하위 항목의 정보를 모두 얻지 못하더라도 하나 이상의 정보만 얻을 수 있다면 분류의 적용은 가능하다.

1) Propagation Channel

공격이 전파되는 경로를 나타낸다. Selective, Unselective, Transmitted로 구성되며 첫 번째 단계의 분류결과로 나타나

〈표 6〉 Source Address 항목

Number	Single Address : 발신지 주소가 단일 개 Multiple Address : 발신지 주소가 복수 개
Location	Remote Area : 발신지 주소가 원격지에 있음을 의미 Local Area : 발신지 주소가 같은 네트워크에 있음을 의미
Trust	Spoofed Address : 실제 발신지 주소와 패킷 해더의 발신지 주소가 다름을 의미 Genuine Address : 실제 발신지 주소와 패킷 해더의 발신지 주소가 같음을 의미



(그림 4) 웜의 특징을 나타내는 징후기반 분류법

는 공격들이 분류의 적용 대상이 된다.

2) Source Address

공격의 발신지 주소의 특징을 나타낸다. 발신지 주소의 수, 발신지 주소의 위치, 패킷을 전송한 발신지 주소와 패킷 해더에 명시된 발신지 주소와의 일치 여부를 이용하여 공격의 특징을 구분한다. 다만 로그로부터 얻는 정보에 이와 같은 세 가지 정보가 모두 포함되어 있지 않을 수 있기 때문에 세 가지 하위 항목 중 하나의 항목만 사용해도 무방하다. 발신지 주소의 Trust 항목은 웜이나 분산서비스거부공격과 같은 공격을 구분하는데 중요한 정보이다. 웜의 경우 공격 패킷이 정상적인 통신과정을 거쳐 전송되기 때문에 Genuine Address에 해당되지만 분산서비스거부공격의 경우 실제 공격에 사용되는 공격 머신보다 훨씬 많은 발신지로부터 패킷이 전송되는 효과를 낼 수 있도록 임의의 발신지 주소를 생성하여 사용하므로 Spoofed Address 에 해당된다. 이처럼 공격에 사용되는 주소 정보는 공격의 유형을 구분하는데 중요한 정보가 된다.

3) Destination Address

공격의 목적지 주소의 특징을 나타낸다. 목적지 주소의 수, 목적지 주소의 위치, 전송되는 패킷의 목적지가 실제로 존재하는지에 대한 정보를 이용하여 공격의 특징을 구분한다. 분류항목은 Source Address 의 항목과 동일하다. Source Address 항목과의 차이점은 Trust 항목의 Spoofed Address가 Random Address로 대체된다. 목적지 주소는 패킷 해더의 주소와 실제 목적지 주소가 다를 수 없으며 실제 존재 여부를 알 수 없는 목적지로 전송됨을 나타내기 때문에 Random Address를 사용한다.

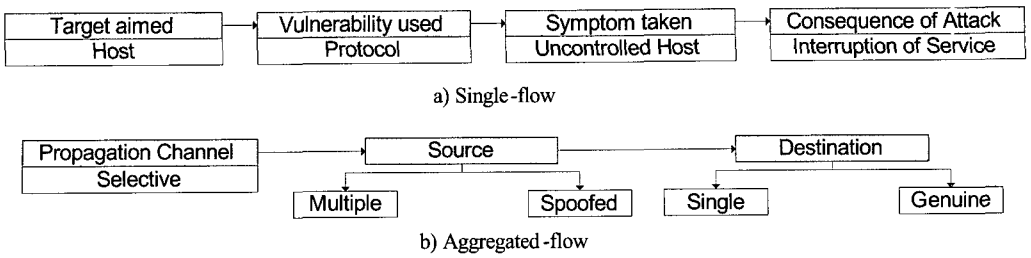
4. 징후기반 분류법을 이용한 공격분류

징후기반 분류법의 두 번째 단계까지 이용하여 공격을 분류하게 되면 공격의 전파형태와 발신지, 목적지 주소의 형태에 대한 특징이 나타난다. 이러한 분류 결과를 이용하여 적절한 방어방법을 선택할 수 있다. 소개한 징후기반 분류법을 이용하여 실제 웜과 분산서비스거부공격 그리고 근거리통신망에서 발생하는 공격을 분류하면 다음과 같다.

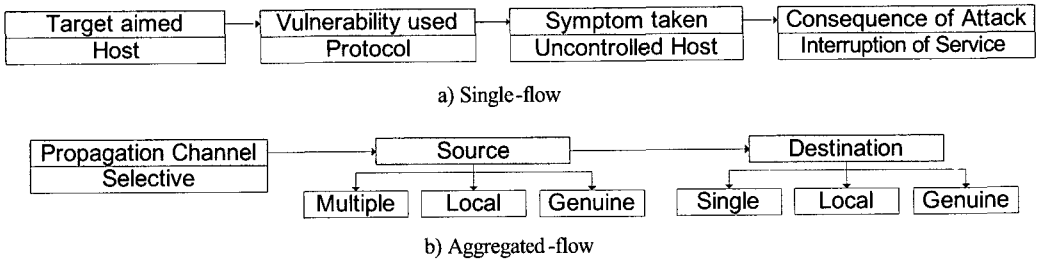
4.1 웜의 징후기반 분류법 적용

웜은 감염된 호스트로부터 다른 호스트를 감염시키기 위해 패킷을 전송하게 되는데 감염된 호스트가 많아지면 다량의 웜 전파 패킷으로 인해 네트워크 자원이 고갈된다. 따라서 웜은 동일한 프로토콜 유형, 패킷 사이즈, 목적지 포트번호를 띄는 패킷이 다량으로 전송되는 특징을 가진다. 그리고 불특정 다수로 전파되도록 랜덤한 다수의 목적지로 패킷이 전송되며 공격 코드의 성공적인 전송을 위해 발신지 주소를 속이는 Spoofing이 나타나지 않는 특징을 가진다. (그림 4)는 징후기반 분류법을 이용하여 웜을 분류한 결과를 나타낸다.

첫 번째 단계에서는 웜 전파 패킷의 특징을 나타낸다. 웜 전파 패킷은 다른 호스트를 감염시키기 위해 발생되므로 공격목표는 호스트에 해당되고, 운영체제에 존재하는 취약점 또는 응용프로그램에 존재하는 취약점을 이용하여 전파된다. 윈도우 운영체제의 취약점을 이용하는 웜의 종류가 상당수이며 웜에 감염될 경우 사용자가 의도하지 않은 웜의 동작들이 진행된다. 공격을 당하게 되면 다른 호스트로 웜을 전파하는데 사용자가 제어하지 않은 동작이 진행되는 것이다. 두 번째 단계에서는 감염을 위해 전파되는 패킷들이 네트워크의 자원을 고갈시켜 피해를 입히는 형태를 나타내므로 Propagation Channel 항목의 Trasmitted에 해당된다. 즉 선택한 대상이나 임의의 대상을 향해 공격이 진행되는 과정보다 계속해서 다른 호스트로 전파되는 과정에서 피해가 발생한다. 또 Source 는 감염된 호스트로부터 발생하고 Spoofing되지 않은 주소를 사용하므로 Single과 Genuine에 해당된다. Destination은 임의의 목적지로 전송되므로 Multiple과 Random 에 해당된다. 따라서 웜의 종류에 따라 사용하는 취약점에 대한 차이는 있지만 두 번째 단계의 특



(그림 5) 분산서비스거부공격의 특징을 나타내는 징후기반 분류법



(그림 6) Smurf 공격의 특징을 나타내는 징후기반 분류법

징을 동일하게 나타나므로 새로운 유형의 웜이 나타나더라도 두 번째 단계의 분류결과를 통해 웜의 한 종류임을 분류해 낼 수 있다.

4.2 분산서비스거부공격의 징후기반 분류법 적용

분산서비스거부공격은 하나의 공격 목표에 대해 여러 공격 노드로부터 공격 패킷이 전송되는 특징을 가진다. 일반적으로 TCP 프로토콜의 취약점을 악용한 공격 패킷이 사용된다. UDP나 ICMP와 같은 프로토콜 역시 분산서비스거부공격에 사용될 수 있으나 이와 같은 프로토콜을 사용할 경우 공격 노드도 자원을 소비해야 하므로 TCP 프로토콜을 사용해서 공격하는 유형이 빈번하게 나타난다. TCP 프로토콜을 이용한 분산서비스거부공격에는 Syn Flooding, Ack Flooding, Syn-Ack Flooding, Naptha와 같은 공격유형이 있는데 네트워크 자원의 고갈보다는 공격 대상의 CPU와 메모리 자원을 고갈시키는 공격 방법이다.

분산서비스거부공격은 공격자가 확보한 Agent 머신을 통해 최종 공격목표로 공격이 행해진다. 이 과정에서 보다 많은 호스트로부터 패킷이 전송되는 것처럼 공격을 진행하기 위해 Agent당 여러 개의 Spoofed Source Address를 이용하여 패킷을 전송한다. 이러한 특징은 분산서비스거부공격을 탐지해 낼 수 있는 중요한 정보로 활용할 수 있으며 특히 징후기반 분류법에서는 Aggregated-flow 에서 이러한 특징을 통해 공격을 구분한다. (그림 5)는 징후기반 분류법을 이용하여 Tcp-Syn Flooding 분산서비스거부공격[10]을 분류한 결과를 나타낸다.

첫 번째 단계에서는 Tcp-Syn Flooding의 특징을 이용하여 공격을 분류한다. 공격의 목표는 호스트이며 TCP프로토콜의 취약점을 이용한다. 공격받은 호스트에게는 CPU와 메모리 자원이 고갈되고 정상적으로 통신을 할 수 없는 현상이 나타난다. 결과적으로 네트워크 서비스를 사용할 수 없게 된다. 두 번째 단계에서는 선택된 공격 목표에게 공격이 집중되어 나타나므로 Propagation Channel의 Selective에 해당된다. 즉 선택한 하나의 공격 대상에게 공격이 진행되며 다른 호스트로 확산, 전파되지는 않는다. 또 발신지 주소를 Spoofing하는 공격형태를 띄기 때문에 Multiple 와 Spoofed에 해당된다. Destination은 선택된 하나의 목적지로 전송되므로 Single과 Genuine 에 해당된다. 다른 유형의 분산서비스거부공격의 경우 첫 번째 단계의 분류결과는 차이점이 존재할 수 있다. 그러나 두 번째 단계에서는 동일한 공격으로 분류되므로 새로운 유형의 분산서비스거부공격 역시 분산서비스거부공격의 특징을 나타내는 분류결과로 인해 분산서비스거부공격의 형태로 분류가 가능하다.

4.3 근거리통신망에서 발생하는 공격의 징후기반 분류법 적용

근거리통신망에서 발생하는 공격은 침입탐지시스템이나 침입차단시스템이 설치된 위치에 따라서 대응이나 방어가 불가능할 수 있다. 특히 근거리통신망에서 발생하는 공격에 대해서 발생한 위치 정보를 모를 경우 계속해서 공격에 노출될 수 있다. 이러한 문제점을 해결하기 위해 징후기반 분류법에서는 두 번째 단계에서 공격이 발생하는 위치를 Local Area와 Remote Area로 구분하는 분류항목을 이용한다. 근거리통신망에서 발생하는 대표적인 공격으로 Smurf 공격[11]이 있다. Smurf 공격은 공격자가 ICMP Request Broadcast 메시지를 마치 공격대상이 전송한 것처럼 발신지 주소를 Spoofing 하여 많은 ICMP Reply 메시지를 공격대상에게 전송되도록 하는 공격이다. Router는 ICMP Broadcast 메시지를 다른 네트워크로 전송하지 않기 때문에 공격은 내

부에서 내부로만 가능하다. 만약 외부에서 내부로 ICMP Reply 패킷을 유도하는 공격이 진행된다면 침입탐지시스템이나 침입차단시스템을 이용하여 대응이 가능하지만 내부에서 발생할 경우 적절한 대응이 어려울 수 있다. (그림 6)은 징후기반 분류법을 이용하여 Smurf 공격[11]을 분류한 결과를 나타낸다.

나타나는 ICMP Reply는 호스트에게 전송되며 Broadcast 메시지처리에 대한 프로토콜의 취약점을 이용한 공격형태이다. 또 공격을 받으면 통신이 불가능해지거나 시스템이 재시작 되며 결과적으로 네트워크 서비스를 정상적으로 사용하지 못하게 된다. 두 번째 단계에서는 정해진 공격 목표에게 전송되는 공격이므로 Selective에 해당하며 발신지는 Multiple이며 Local Area에 존재하는 주소들이다. 목적지는 Single이며 역시 Local Area에 해당된다. 분류결과를 통해 해당 공격이 Local Area에서 나타남을 알 수 있으며 적절한 방어 방법을 선택하는데 중요한 정보를 제공해준다.

5. 결 론

네트워크에는 많은 수의 공격이 존재하며 지금 이 순간에도 새로운 공격들이 발견되고 있다. 이러한 공격들로부터 시스템을 보호하기 위해서는 공격들을 비슷한 유형으로 구분 짓고 그 결과에 따라 적절한 방어 방법을 선택, 적용하여야 한다. 현재 대부분의 보안 시스템들이 이와 같은 절차를 따르지만 여전히 네트워크 공격으로 인한 피해는 발생하고 있다. 그 이유는 일반적으로 널리 사용되는 침입탐지시스템이나 침입차단시스템과 같은 네트워크 보안 시스템들 대부분이 공격기반분류법을 사용하기 때문이다. 결과적으로 알려지지 않았거나 또는 새로운 공격에 대한 방어를 위해서는 많은 시간이 소모되며, 해당 공격에 대한 분류에 소모되는 시간 동안은 시스템을 보호할 수 없게 된다.

본 논문에서는 공격을 받는 피해자의 입장에서 공격 시 나타나는 다양한 징후들을 수집하고 이 징후정보를 이용하여 이상행위에 대한 분석 및 분류를 수행하는 징후기반 분류법을 제안하였다. 제안하는 분류법은 공격의 피해사례를 수집, 분석하고 분석한 자료를 토대로 공격자 관점에서 공격 진행 과정을 분류기준으로 사용하는 공격기반 분류법과는 달리 공격 피해사례를 수집, 분석하는데 시간이 소모되지 않는 장점이 있다. 또 정상적인 패턴을 모두 등록해두고 이를 기반으로 비정상적인 패턴을 이용하여 공격을 탐지하는 방어기반 분류법과는 달리 사전에 정상적인 패턴을 등록할 필요가 없으며 네트워크에 존재하는 이기종 센서들로부터 쉽게 얻을 수 있는 로그정보를 이용한다는 장점이 있다.

결과적으로 알려지지 않은 공격에 대해서도 피해사례 수집이나 분석과 같은 절차 없이 공격을 분류해 낼 수 있으며, 쉽게 얻을 수 있는 정보를 이용한 공격분류법을 제안함으로써 새로운 공격에 대해서도 빠르게 대처할 수 있는 방안을 마련할 수 있게 되었다.

참 고 문 헌

[1] Dean Turner et al., "Symantec Internet Security Threat Report Trends for July 05 - December 05 Volume IX, March 2006," Symantec, March, 2006.

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

[3] John D. Howard and Thomas A. Longstaff, "A Common Language for Computer Security Incidents," Sandia Report SAND98-8667, October, 1998.

[4] Tim Grance, Karen Kent and Brian Kim, "Computer Security Incident Handling Guide," NIST Special Publication 800-61, January, 2004.

[5] James P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Fort Washington, PA, April, 1980.

[6] N. D. Jayaram and P. L. R. Morse, "Network security: A taxonomic view," In European Conf. Sec. and Detection, IEEE, pp.124-127, April, 1997.

[7] Kevin S. Killourhy, Roy A. Maxion, and Kymie M. C. Tan, "A defence-centric taxonomy based on attack manifestations," In Proceedings of the International Conference on Dependable Systems and Networks 2004, June, 2004.

[8] Jeffrey Undercoffer and John Pinkston, "Modeling Computer Attacks: A Target-Centric Onto-pogy for Intrusion Detection," CADIP Research Symposium 2002, October, 2002.

[9] Catherine Cook et al., "An Introduction to Tivoli Enterprise," IBM, pp. 679 - 726, October 1999, available at http://www.redbook-s.ibm.com/redbooks/pdfs/sg245494.pdf

[10] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," CERT/CC, September, 1996, available at http://www.cert.org/advisories/CA-1996-21.html

[11] CERT, "CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks," CERT/CC, January 1998, available at http://www.cert.org/advisories/CA-1998-01.html

[12] Cristina Abad, Jed Taylor, Cigdem Sengul, William Yurcik, Yuanyuan Zhou, and Ken Rowe, "Log Correlation for Intrusion Detection: A Proof of Concept," Computer Security Applications Conference, December, 2003.

[13] Nong Ye, Joseph Giordano and John Feldman, "A Process Control Approach to Cyber Attack Detection," Communications of the ACM, Vol 44 No 8, pp 76-82, August, 2001.

[14] Akira Kanamaru, Kohei Ohta, Nei Kato, Glenn Mansfield and Yoshiaki Nemoto, "A simple packet aggregation technique for fault detection," International Journal of Network Management 2000, Vol.10, Issue 4, pp.215~228, August, 2000.

김 기 윤

e-mail : doogysp@ece.skku.ac.kr
2005년 성균관대학교 정보통신공학부 (공학사)
2005년~현재 성균관대학교 정보통신공학부 컴퓨터공학과 석사과정
관심분야 : 인터넷 보안, 홈네트워크 등

최 윤 성

e-mail : yschoi@security.re.kr
2006년 성균관대학교 정보통신공학부 (공학사)
2006년3월~현재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 사이버 포렌식

최 형 기

e-mail : hkchoi@ece.skku.ac.kr
1992년 성균관대학교 전자공학과(공학사)
1996년 Polytechnique University 전기전자(공학석사)
2001년 Georgia Institute of Technology 전기전자(공학박사)
2001년~2004년 미국 Lancope. Inc. 연구원
2004년~2006년 성균관대학교 정보통신공학부 전임강사
2006년~현재 성균관대학교 정보통신공학부 조교수
관심분야 : 인터넷 보안, 모바일 커뮤니케이션 등

방 효 찬

e-mail : bangs@etri.re.kr
1995년 홋카이도공업대학 경영공학과 (공학사)
1997년 홋카이도공업대학 기계시스템공학과(공학석사)
1997년~1999년 한국통신 운용연구단 전임연구원
2000년~현재 ETRI 능동보안기술연구팀 선임연구원
관심분야 : 네트워크보안, 액티브네트워크

최 동 현

e-mail : dhchoi@security.re.kr
2005년 성균관대학교 정보통신공학부 (공학사)
2005년 9월~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, DRM, 워터마킹

나 중 찬

e-mail : njcg@etri.re.kr
1986년 충남대학교 계산통계학과(이학사)
1989년 숭실대학교 전자계산학과(공학석사)
2004년 충남대학교 컴퓨터과학과(이학박사)
1989년~현재 ETRI 능동보안기술연구팀 팀장
관심분야 : 네트워크 트래픽 및 공격상황 분석

이 병 희

e-mail : bhlee@security.re.kr
2005년 성균관대학교 정보통신공학부 (공학사)
2005년 3월~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 정보보안, 네트워크 보안, 해킹