韓國 컴퓨터情報學會 論文誌
第11卷 第5號, 2006. 11.

2006-11-5-2-1

인터넷 환경에서의 비정상행위 공격 탐지를 위한 위협관리 시스템

김 효 남*

Threat Management System for Anomaly Intrusion Detection in Internet Environment

Hyo-Nam Kim*

요 약

최근에는 대부분의 인터넷 공격은 악성코드(Malware)에 의한 잘 알려지지 않은 제로데이 공격 형태가 주류를 이루고 있으며, 이미 알려진 공격유형들에 대해서 탐지하는 오용탐지 기술로는 이러한 공격에 대응하기가 어려운 실정이다. 또한, 다양한 공격 패턴들이 인터넷상에 나타나고 있기 때문에 기존의 정보 보호 기술로는 한계에 다다르게 되었고, 웹기반 서비스가 보편화됨에 따라 인터넷상에 노출된 웹 서비스가 주공격 대상이 되고 있다. 본 논문은 인터넷상의 트래픽 유형을 분류하고, 각 유형에 따른 이상 징후를 탐지하고 분석할 수 있는 비정상행위공격 탐지기술(Anomaly Intrusion Detection Technologies)을 포함하고 있는 위협관리 시스템(Threat Management System)을 제안한다.

Abstract

The Recently, most of Internet attacks are zero-day types of the unknown attacks by Malware. Using already known Misuse Detection Technology is hard to cope with these attacks. Also, the existing information security technology reached the limits because of various attack's patterns over the Internet, as web based service became more affordable, web service exposed to the internet becomes main target of attack. This paper classifies the traffic type over the internet and suggests the Threat Management System (TMS) including the anomaly intrusion detection technologies which can detect and analyze the anomaly sign for each traffic type.

▸ Keyword : 비정상행위탐지(Anomaly Intrusion Detection), 조기경보(Early Warning Information), 위협관리(Threat Management)

• 제1저자 : 김효남
• 접수일 : 2006.09.11, 심사일 : 2006.09.23, 심사완료일 : 2006.11.18
* 청강문화산업대학 컴퓨터소프트웨어과 교수

Ⅰ. 서 론

최근 들어 인터넷이 급속하게 보급되면서 이를 이용한 스트리밍이나 P2P와 같은 새로운 애플리케이션들이 등장하였다. 이런 애플리케이션들은 대량의 네트워크 트래픽을 유발시키는 특징을 갖고 있다. 이와 더불어 최근에는 악성코드(Malware)와 인터넷 웜 혹은 기타 알려지지 않은 공격들이 대량의 네트워크 트래픽을 발생시켜 네트워크 가용성을 심각한 수준으로 떨어뜨리는 위협이 빈번하게 발생하고 있다. 대량 트래픽에 의한 네트워크 가용성 저하 문제를 해소하기 위해서는 조기에 위협 요인들을 탐지하여 적절한 조치를 취해야 한다. 그림 1은 공격을 막는 정보보호 기술보다 공격기술이 앞선 이유가 주로 제로데이(Zero-Day) 공격에 의한 악성코드의 공격과 사회공학공격이 주류를 이루고 있고, 가장 큰 문제점으로 취약점을 발견한 후 곧장 공격을 하는 제로데이 공격임을 보여주고 있다.

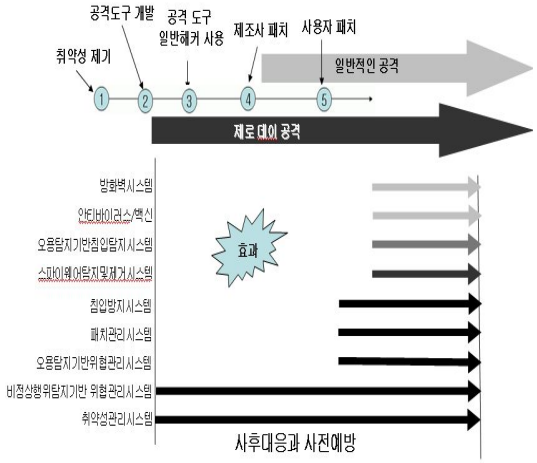


그림 1. 제로데이 공격과 정보보호기술
Fig 1. Zero-Day Attack and Information Security Technology

이와 같은 공격에 대해서 이상적인 침입 탐지 시스템은 공격탐지 비율이 100%이고 정상적인 행동을 잘못 분류하는(False Positive) 비율이 0%인 시스템이다. 침입 탐지 방법으로 크게 두 가지 기술로 분류된다. 오용탐지(Misuse Detection)와 비정상행위 탐지(Anomaly Detection)이다. 오용탐지는 기존의 공격을 탐지하는 방법으로 이미 알려진 공격기법들을 시그니처(Signature)로서 가지고 있어, 이를 기반으로 탐지하는 방법이다. 지금까지 대부분의 침입탐지 시스템에서는 오용탐지 방법을 적용하고 있기 때문에 제로데이 공격이 빈번해진 현재의 상황에서는 침입 탐지가 어려워 피해가 속출하고 있는 실정이다. 최근에는 오용탐지 방법을 보완하기 위하여 비정상행위 탐지 방법이 활발하게 연구되고 있다[1,12,13].

본 논문에서는 인터넷 환경에서의 네트워크 트래픽 유형을 다양하게 분류하여 위험지표로 선정하였으며, 각 위험지표별로 가중치를 적용하여 최종적으로 위험경보 단계 값을 보안 관리자에게 알려줄 수 있다는 점이 기존 연구와 다른 점이다. 그리고 네트워크 트래픽의 이상 징후를 탐지하고 분석하여 조기에 알려지지 않은 비정상행위공격(Anomaly Intrusion)을 탐지할 수 있는 비정상행위 기반의 탐지기술을 포함한 위협관리 시스템(Threat Management System : TMS)을 제안한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 비정상행위 탐지기술, 조기경보시스템, 위협관리시스템에 대한 관련 연구에 대하여 기술한다. 제 3장에서는 위협관리시스템 설계 및 구현에 대한 내용을 기술한다. 제 4장에서는 실험 후 결과분석에 대하여 기술한다. 제 5장에서는 결론 및 향후 연구 과제를 기술한다.

Ⅱ. 관련 연구

2.1 비정상행위탐지(Anomaly Detection)

비정상행위 탐지는 극히 정상적인 사용에 대해서 사용자나 그룹, 프로그램, 시스템 자원에서 비정상적인 행위가 일어나는 지를 탐지하는 방법이다. 최근에는 오용탐지 방법을 보완하기 위하여 비정상행위 탐지 방법이 활발하게 연구되고 있다.

2.1.1 비정상행위 탐지 유형

비정상행위 탐지 방법 유형들에 대해서 살펴보면 다음과 같다.

- 먼저 수용할 수 있는 값을 설정하고, 이를 위반하는지 탐지하는 방법으로서, 매우 명확하며 탐지 수용범위를 명확하게 구분하여 준다. 하지만 근사치로 설정된 이러한 값은 높은 false positive and false negative의 가능성이 있다.
- 사용자의 업무 흐름이나 일어날 수 있는 일에 대한

분석 정보를 가지는 방법이 있다. 변경된 가장 최근의 행동 패턴은 다음의 행위에 대한 예측 자료로 사용된다.

- ○ 그룹 사용자의 일반적인 행동패턴을 만들고 이를 분석 정보로 활용하는 방법이다. 정보는 그룹 전체사용자의 기록 정보를 기반으로 추출해 낸다.
- ○ 사용자, 애플리케이션, 저장 매체, 프로토콜, 통신포트 등 시스템 리소스 모니터링 정보를 활용하는 방법이 있다.

이상같이 비정상행위에 대한 탐지 유형들에 대한 내용들이며, 실제적으로 적용되는 비정상행위 침입 탐지 방법 예로는 네트워크 패킷에 대한 데이터 마이닝(data mining), 감사 레코드들에 대한 통계적인 분석, 운영체제 시스템 call에 대한 순서 분석 등이 있다. 그러나 비정상행위 탐지 방법은 기본적으로 통계적 비정상행위 탐지 방법과 규칙기반 비정상행위 탐지 방법으로 분류할 수 있다.

2.1.2 통계적 비정상행위 탐지(Statistical Anomaly Detection)

이 방법은 시스템에 관련된 명령어를 관찰하는 임계값(Threshold Value) 탐지와 사용자 행동이 기록된 속성파일(Profile) 혹은 로그 파일에 대한 통계적인 탐지 방법이 이에 속한다. 빈번한 공격유형 중의 하나로 웹의 취약성을 이용하여 다양한 기술을 바탕으로 하는 웹 기반의 공격을 탐지하기 위하여 CLF (Common Log Format) 형식으로 기록되어 있는 웹 서버 로그 파일의 내용을 분석하여 anomaly score를 산출하여 적용하는 방법이다. 이는 비정상행위 탐지에 적용하기 위한 threshold 값으로 적용되며 실제적으로 입력되는 웹 요청 속성에 대해서 계산된 값을 threshold 값과 비교하여 비정상행위 여부를 판단하는 방법이다[2].

2.1.3 규칙기반 비정상행위 탐지 (Rule-based Anomaly Detection)

규칙기반 변화 탐지 방법은 행위기반 모델(Behavior-based Model) 중의 하나로 과거에 만들어진 감사(Audit) 자료로부터 얻은 시스템 사용자의 정상적인 행위 사용패턴을 규칙으로 만들어 이에 맞지 않으면 침입으로 간주하는 방법이다. 모델 구축 방법에 따라 machine learning model과 specification-based model로 분류될 수 있다[3].

2.2 조기경보시스템(Early Warning Information System)

조기경보 시스템은 해킹, 바이러스, 웜 등의 다양한 전자적인 침해사고에 대한 이벤트 정보를 수집, 분석하여 문제가 확산되기 전에 보안 관리자나 사용자에게 공격의 위협을 사전에 제거할 수 있도록 정보를 제공하는 시스템이다. 현재 한국 정보보호진흥원의 인터넷침해사고 대응지원센터에서는 주요 보안관제 기관 및 IPS, IDC 업체로부터 수집되는 위협정보 및 트래픽정보 등을 수집, 분석하여 일반 업체에게 조기에 정보를 제공할 수 있는 시스템을 구축하고 있다[4].

2.2.1 조기경보시스템 관련 연구

조기경보시스템을 보다 더 효율적으로 운용하기 위한 능동적인 대응방법을 보안 관리자에게 제시하는 자동화된 프레임워크 연구가 있다.

트래픽 양과 플로우(Flow) 분석과 같은 트래픽 추이분석 방법을 통하여 정상 트래픽 패턴과 비교하여 현재 트래픽의 이상을 조기에 알리는 방법이 있다[6].

최근 연구에서는 네트워크에서 실시간 탐지용인 N-IDS (Network Intrusion Detection System)의 위협 탐지 정보와 정기적인 보안감사용으로 운영되는 VAS(Vulnerability Analysis System)의 취약점 탐지 정보간 상관속성을 산출하여 자산에 발생할 수 있는 위협유형에 따라 대응방안을 결정하는 네트워크위험 조기 경보시스템 연구가 있다[5].

2.3 트래픽분석시스템(Traffic Analysis System)

최근 인터넷이 크기 측면이나 복잡도 측면에서 급속하게 성장하면서 네트워크를 통해 전달되는 데이터 량이나 데이터의 복잡도 또한 증가하고 있으며 악성코드인 웜 등은 트래픽 분석에 대한 특징이나 이해, 그리고 모델링하는데 어려움을 초래하고 있다. 따라서 인터넷상의 트래픽의 모델링은 실험실이나 테스트베드 수준의 제한된 데이터 량으로 시뮬레이션 하는 것이 일반적인 추세이다[6].

네트워크 트래픽 분석 방법은 크게 2가지로 실시간 분석 방법과 일괄처리 분석방법이 있다[7]. 네트워크 트래픽 감시 및 분석 정보는 네트워크 상태와 문제점을 파악, 트래픽이 증가하는 경우 원인을 분석, 네트워크 회선 계획 등이 필요하다. 하지만 기존의 네트워크 분석의 문제점으로서 패킷 손실로 인한 트래픽 분석의 부정확성, 대용량 트래픽 처리의 한계, 장기간 트래픽 감시 및 분석을 지원하지 않음, 주로

잘 알려진 서비스만 분석하는 등의 문제점을 갖고 있다.

최근 몇 년 동안 여러 연구자들이 인프라 구조를 보호하는 많은 방어 장비와 방법에 대해 연구하고 있지만 실세계 데이터 부재로 인해 장비의 효용성과 다양한 분야에 쉽게 사용할 수 있도록 평가하는 작업이 계속되고 있다[8]. 그리고 다양한 분야의 네트워크 행위를 분석하기 위하여 한 순간의 네트워크 행위를 포획하기 보다는 진행되는 네트워크 트래픽 데이터를 수집하는 것을 시도하였다[9]. 일반적으로 수동적인 형태의 가장 인기 있는 측정 시스템으로는 SNMP, tcpdump, NetFlow 등이 있다[10,11].

2.3.1 네트워크 트래픽 추이 형태

네트워크 트래픽 수집 분석도구로는 웹 기반의 모니터링 및 분석 애플리케이션인 Ntop을 비롯하여 tcpdump, ethereal, FlowScan, CoralReef, PMA, IPMON, snort 등이 있다. 이 중에서 snort는 실시간 트래픽 분석과 패킷 로깅을 수행하는 시그너처 기반 혹은 규칙 기반의 네트워크 침입 탐지 시스템으로 오픈 소스 기반의 도구이다. 아래 그림 2는 snort 시스템을 이용한 특정 포트별 네트워크 트래픽 추이를 보여주는 그래프이다.

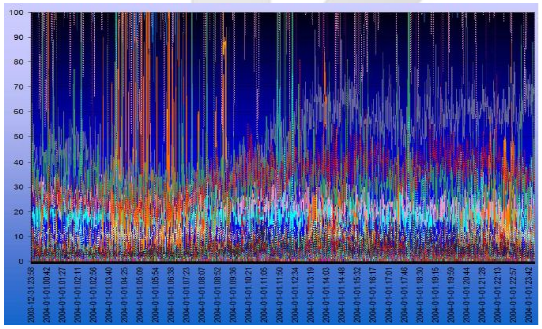


그림 2. 포트별 네트워크 트래픽 추이 그래프
Fig 2. Network Traffic Change Graph based on Port

그림 2에서 보는 것과 같이 일반적인 네트워크 트래픽은 간헐적으로는 최고 임계치(Threshold)에 근접하기는 하나 전반적으로 볼 때 유순한 곡선을 나타내는 형태로 파악된다. 물론 업무량이 증가하거나 특정한 응용을 사용할 경우에 있어서는 갑작스런 네트워크의 증가를 보이기도 하나 이는 일정시간이 경과하면 다시 정상적인 행태로 복귀하는 것을 알 수 있다. 그림 3에서는 이미 알려진 포트 정보에 대해서는 Snort에서 필터를 사용하여 정상적이라고 판단되는 트래픽은 제거한 후에 네트워크 트래픽 추이를 보여주는 그래프이다.

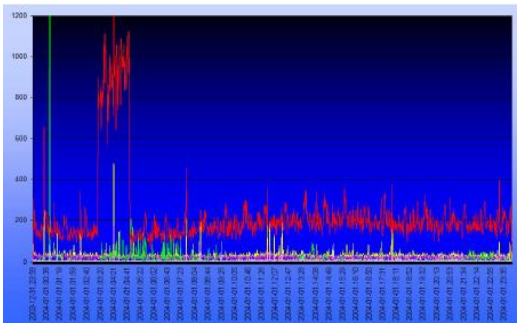


그림 3. 필터를 통한 추이 그래프
Fig 3. Network Traffic Change Graph based on Filter

그림 3의 그래프에서 보여주듯이 뚜렷하게 이상 징후에 대한 내용을 확인할 수 있다. 이때 이상 징후에 해당하는 부분을 보다 눈여겨 볼 필요가 있다.

2.4 위협관리시스템 (Threat Management System : TMS)

기존의 오용탐지 기반 보안 솔루션들은 알려진 공격에 대해서만 대응 가능하기 때문에 제로 데이 위협에 대해 처리의 취약성을 갖는다. 결국 이런 위협이 확산되어 네트워크 장애나 트래픽 폭주 등의 현상이 나타나기 전까지는 인식조차도 어려운 상황이다. 그리고 최근의 웜이나 바이러스는 피싱(phishing)과 같은 기법을 이용함으로 탐지를 위한 패턴을 정의하기도 불가능하다. 이런 사이버 위협을 효과적으로 대처하기 위해 발생될 위협을 조기에 탐지하고 발생될 위협을 완화하거나 확산을 방지하며 피해를 최소화 시키는 방안이 필요하다.

위협 관리란 시스템 상태를 위협하거나 영향을 미치는 악성 코드 등을 탐지하고, 제거하는 것을 의미한다. 현재의 초고속 통신망 환경 하에서는 짧은 기간 내에 다량의 의심스러운 이벤트들이 발생되고, 이를 보안 담당자, 시스템 담당자, 네트워크 관리자 등이 관리하고 대처하는 데는 한계가 있으며, 매우 비효율적이다. 이를 보다 효과적이면서 자동화되고, 체계적으로 대응하고 보안 도구가 위협 관리 시스템이다. 이 시스템은 효과적으로 적절한 시간 내에 침입을 탐지하고 대처한다. 이 시스템은 여러 독립적인 장치로부터 시스템 로그를 수집하고, 여러 의심스러운 이벤트들을 계산하는 중앙 집중 방식으로 동작한다.

2.4.1 위협 관리 처리 모델

그림 4는 위협 관리 처리 모델을 보여준다. 각종 장치로

구성되는 device 모듈에서 각종 로그 정보들이 수집되어 이후 모듈에서 처리되어 네트워크에 영향을 주는 위협을 포착하면 즉시에 위협 경고를 보안 관리자에게 전달하여 관리자로 하여금 적절한 조치를 내릴 수 있도록 돕는다.

- device : 로그 데이터를 입력하는 모듈(방화벽, 라우터, NIDS, HNIDS, 호스트와 응용로그 등)
- aggregation : 다양한 정보를 수집, 정규화 모듈
- correlation: 이벤트를 처리하고 그들 간에 상관관계를 발견하는 모듈
- analysis : 상관 관계 정보를 호스트 중요성, 제공되는 네트워크 서비스, 다른 호스트와의 관계, 호스트 취약성 등과 비교하는 모듈
- alert : 특정 이벤트 경고를 발생시키는 모듈
- reporting : 오랜 기간 동안의 추세와 적절한 관리 정보를 제공하는 모듈

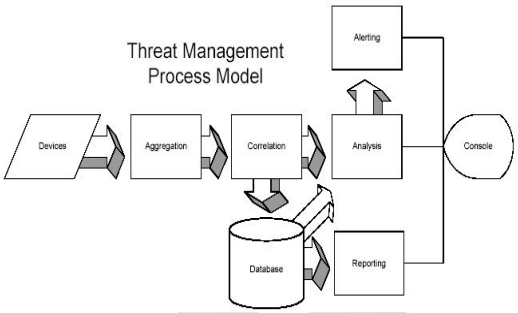


그림 4. 위협 관리 처리 모델
Fig 4. Threat Management Processing Model

III. 시스템 구현

3.1 위협관리시스템의 구조

본 논문에서 제안하는 위협관리시스템(TMS)의 상세 구조는 그림 5와 같다.

그림 5에서 보는 바와 같이 데이터 생성부, 데이터 수집부, 데이터 분석부 그리고 데이터 표현부로 구성된다.

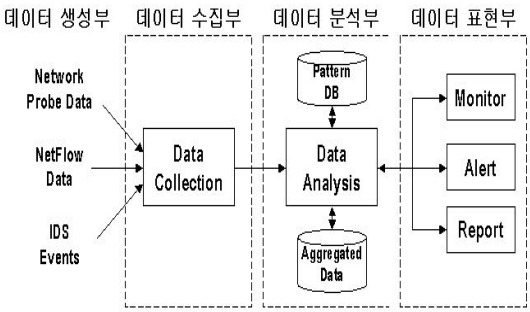


그림 5. TMS 구조
Fig 5. Structure of TMS

3.2 데이터 생성부

데이터 생성부는 Network Probe를 통한 실시간 트래픽 데이터, 라우터 혹은 NetFlow 호환 시스템을 통한 NetFlow 데이터, 그리고 IDS 나 IPS 등을 통한 공격이벤트 데이터를 생성한다.

3.3 데이터 수집부

데이터 수집부는 NetFlow 데이터와 공격이벤트 데이터를 수집하여 저장한다. NetWork Probe로부터의 데이터는 실시간 처리를 위하여 직접 데이터 표현부(콘솔)로 전달한다. 1차 수집된 Raw 데이터로부터 전체 트래픽(inbound/outbound), 프로토콜별, 서비스별, 패킷크기별, 출발지IP 및 목적지IP별 트래픽량(flows, packets, bytes)을 추출하여 DB에 저장한다.

그림 5는 NetFlow 데이터 수집모듈의 구조를 보여준다. 수집모듈은 NetFlow 내부 모듈인 cflowdmux, cflowd, cfdcollect 단위 모듈로 구성되며, 본 논문에서는 cflowdmux와 cflowd 모듈을 사용하여 NetFlow 데이터를 수집한다.

3.4 비정상행위 탐지를 위한 데이터 분석부

데이터 분석부는 데이터 수집부에서 수집한 데이터 즉 전체 트래픽(inbound/outbound), 프로토콜별, 서비스별, 패킷크기별, 출발지IP 및 목적지IP별 트래픽 량(flows, packets, bytes)을 위험지표로 선정한다. 각 위험지표에 대해서 아래의 트래픽 추이분석 식을 적용하여 추이값을 만들어내고 각각의 추이값에 가중치를 부여하여 최종적으로 위험경보 단계 값을 만들어 보안 관리자에게 보안 정보를 제공할 수 있도록 한다. 다음 절에서 데이터 분석부에 대한 내용에 대해서 자세하게 기술하고 있다.

3.4.1 트래픽 추이분석

특정 서비스(포트)에 대한 트래픽 추이값은 t_p으로 나타내며, 다음 식(1)에서와 같이 계산한다.

$$t_p = log\left(\frac{R^* r_p}{r^* R_p}\right) \quad \cdots\cdots (1)$$

R=최근 한달(4주)간 트래픽량(flows, packets, bytes)

r = 하루동안 트래픽량

R_p = 특정 포트에 대한 최근 한달(4주)간 트래픽량

r_p = 특정 포트에 대한 하루동안 트래픽량

트래픽 추이값(t_p)은 특정 서비스(포트)의 트래픽이 급격히 증가할 경우, 양(+)의 값을 가지며, 반대의 경우는 음(-)의 값을 가진다. 트래픽 량의 변화가 없을 경우 0에 가까운 값으로 나타나고, 트래픽의 급격한 변화가 있을 때 증감하므로, 트래픽 추이값을 통해 네트워크 트래픽의 이상 징후를 탐지할 수 있다.

3.4.2 조기경보를 위한 위험지표

위험지표는 네트워크 트래픽의 이상 징후에 따른 위험의 정도를 나타내는 측정값(metrics)이다. 위험지표를 구하기 위하여 본 논문에서 고려한 측정대상 및 측정값(metrics)은 표 1과 같다.

표 1. 측정값과 위험지표
Table 1. Measurement Value and Risk Index

대상	측정값	위험지표
전체 트래픽	인바운드 및 아웃바운드 트래픽의 량	t_i, t_o
서비스(포트)	서비스별(목적지 포트) 트래픽의 량	t_p
프로토콜	프로토콜별(TCP, UDP, ICMP 등) 트래픽의 량	t_P
패킷 사이즈	패킷 사이즈별 분포(비율)	t_{ps}
출발지 주소	출발지 주소별 트래픽의 량, 목적지 주소의 수, Top 10 목적지 주소별 트래픽의 량	t_s
공격 이벤트	공격 유형별 이벤트 수(공격시도횟수)	t_a
목적지 주소	목적지 주소별 트래픽의 량, 출발지 주소의 수, Top 10 목적지 주소별 트래픽의 량	t_d

3.4.3 위험경보 및 조기경보

위험경보는 트래픽 폭주 등으로 실제 위험상황이 발생하기 전에 사전대응(주의, 경계)할 수 있도록 알리는 행위 혹은 신호이다. 위험경보는 측정한 위험지표를 종합적으로 분석하여 최종적으로 4단계(정상, 주의, 경고, 위험)를 가진다. 위험경보 단계는 각 위험지표별 가중치를 부여하고, 임계값을 초과하는 위험지표와 정도, 빈도, 지속시간 및 상황지수를 고려하여 식 (2)에 따라 결정된다.

$$R = \sum (t_i, t_o, t_p, t_P, t_{ps}, t_s, t_a, t_d)^*(w, i, f, d, C) \quad \cdots\cdots (2)$$

R = 위험경보단계

t_x = 각 위험지표

w_{xy} = 각 위험지표에 대한 위험지표별 가중치(weight)

i_{xy} = 각 위험지표에 대한 위협의 강도(impact)

f_{xy} = 각 위험지표에 대한 위협의 빈도(frequency)

d_{xy} = 각 위험지표에 대한 위협의 지속시간(duration)

C = 상황지수(context index)

3.5 데이터 표현부

데이터 표현부는 그림 6의 실시간 트래픽 모니터링, 통계 및 분석, 네트워크 서비스별 상세 추이 분석, 그림 7의 공격이벤트 분석, 리포팅 기능을 수행한다.

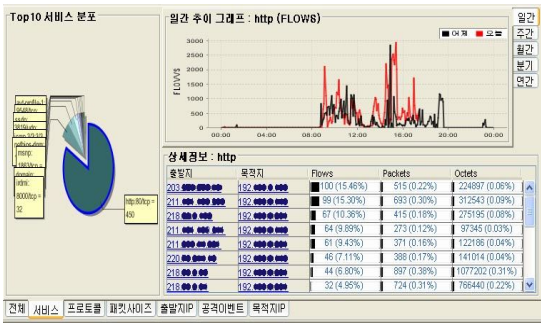


그림 6. 네트워크 서비스별 상세 추이분석
Fig 6. The Detailed Change Analysis based on Network Service

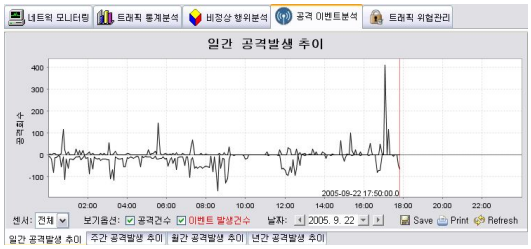


그림 7. 공격이벤트 분석
Fig 7. Attack Event Analysis

IV. 실험분석

국내 모 대학 연구실에서 한달간 설치 운영한 결과 다음과 같은 트래픽 현황을 보았으며, 웜 트래픽이 상당한 비율을 차지함을 짐작할 수 있었다. 즉 UDP 트래픽 양은 적지만, 엄청난 플로우 수를 볼 때 확인되는 것이다.

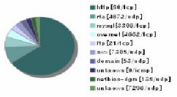
- Flows 기준: TCP -74%, UDP-24%
- Packets : TCP-95%, UDP-4%
- Octets: TCP-98%, UDP-1%

프로토콜	Flows	패킷수	바이트(GB)
TCP	309,750,819 (74.01..	51,710,401,847 (95...	51,928 (98.79%)
UDP	102,832,255 (24.57..	2,566,495,970 (4.72..	631 (1.20%)
ICMP	5,952,725 (1.42%)	148,553,057 (0.27%)	6 (0.01%)
SIP	3,690 (0.00%)	129,418 (0.00%)	0 (0.00%)
SIPP-ESP	780 (0.00%)	456,063 (0.00%)	0 (0.00%)
GRE	143 (0.00%)	320,401 (0.00%)	0 (0.00%)
RSVP	128 (0.00%)	6,596 (0.00%)	0 (0.00%)
246	1 (0.00%)	1 (0.00%)	0 (0.00%)
247	1 (0.00%)	1 (0.00%)	0 (0.00%)
249	1 (0.00%)	1 (0.00%)	0 (0.00%)

그림 8. 프로토콜 량 분석
Fig 8. Protocol Volume Analysis

또한 어플리케이션 사용량을 분석하면 다음과 같다.

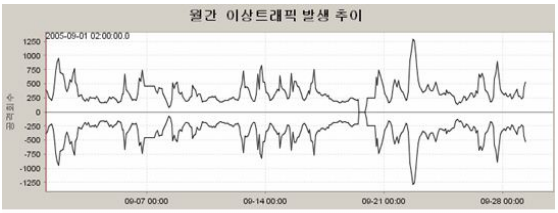
- http: 65%
- E-donkey 및 P2P: 15%
- MySQL: 5%
- ftp: 5%



서비스명	Flows	패킷수	바이트(GB)
http[80/tcp]	146,798,015 (65.34..	4,748,549,010 (61.3..	1,874 (44.22%)
rfa[4672/udp]	20,727,539 (9.23%)	51,002,065 (0.66%)	3 (0.06%)
sygvsql[3306/tcp]	12,493,158 (5.56%)	28,479,101 (0.37%)	4 (0.11%)
overnet[4662/tcp]	10,416,731 (4.64%)	2,682,616,528 (34.6..	2,343 (55.27%)
ftp[21/tcp]	7,262,275 (3.23%)	7,895,561 (0.10%)	0 (0.01%)
sygn[7306/udp]	6,306,641 (2.81%)	6,309,131 (0.08%)	0 (0.02%)
domain[53/udp]	5,856,645 (2.61%)	81,448,369 (1.05%)	4 (0.12%)
unknown[0/icmp]	5,350,723 (2.38%)	123,972,229 (1.60%)	5 (0.14%)
netbios-dgm[138/udp]	5,066,112 (2.25%)	6,969,427 (0.09%)	1 (0.03%)
unknown[7296/udp]	4,457,664 (1.98%)	4,458,751 (0.06%)	0 (0.01%)

그림 9. 어플리케이션 사용량 분석
Fig 9. Application Amount Used Analysis

또한 IPS에 의한 비정상행위 트래픽을 분석한 내용은 다음 그림과 같다.



발생시각	트래픽	서비스명	출발지주소	프로..	목적..	출발..	패킷수	바이트	초스..	소요..
2005-09-12 23:50:...	Scan	MySQL Vulnerability Scan	210.110.14...	tcp	1433	15498	30458	1461984	15498	2
2005-09-12 23:50:...	Scan	MySQL Vulnerability Scan	210.110.15...	tcp	1433	15596	30688	1964032	15595	3
2005-09-12 23:50:...	-	-	203.247.20...	tcp	1000	13503	13687	658976	13503	0
2005-09-12 23:50:...	P2P	파일구리	203.247.19...	tcp	9493	6752	26679	3049468	6752	0
2005-09-12 23:50:...	P2P	파일구리	210.110.15...	tcp	9493	2366	55932	2943430	2366	0
2005-09-12 23:50:...	DoS[...	Microsoft DS	210.110.19...	tcp	445	3429	7464	383753	3429	3
2005-09-12 23:50:...	Scan	MySQL Vulnerability Scan	210.110.19...	tcp	1433	2700	5244	251712	2700	2
2005-09-12 23:50:...	DoS[...	NetBIOS Session OR Netbio	210.110.19...	tcp	139	229	608	28912	229	6
2005-09-12 23:50:...	DoS[...	Microsoft DS	210.110.15...	tcp	445	2239	6927	394623	2232	7
2005-09-12 23:50:...	DoS[...	NetBIOS Session OR Netbio	210.110.15...	tcp	139	704	1844	86872	703	5
2005-09-12 23:50:...	DoS[...	Microsoft RPC	210.110.15...	tcp	135	495	1415	67848	495	8
2005-09-12 23:50:...	Scan	MySQL Vulnerability Scan	210.110.14...	tcp	1433	2593	5008	240384	2593	2
2005-09-12 23:50:...	Scan	MySQL Vulnerability Scan	210.110.14...	tcp	1433	2656	4557	218736	2656	2
2005-09-12 23:50:...	DoS[...	Microsoft RPC	210.110.15...	tcp	135	2648	5200	332800	2648	2

그림 10. 비정상행위 탐지 자료
Fig 10. Data of The Anomaly Detection

위 실험 결과 그림 8, 9, 10에 대한 분석 내용은 적용한 대학의 경우 기존에 파악하지 못한 위협에 대하여 다음과 같은 정보를 제공할 수 있었다. 웜 트래픽 사이즈는 1%이지만 약 24%의 플로우를 가지고 있었으며, E-Donkey 및 P2P 등과 MySQL 등의 악성트래픽이 매우 많았다. 특히 비정상행위로 분석한 내용 중 90%는 공격이었으며, 단 10%만이 네트워크 오류임을 보안 관리자에게 보안 정보를 제공할 수 있었다. 본 시스템은 공격 트래픽을 탐지 못하는 false negative와 오탐인 false positive를 최소화하기 위하여 다양한 위험지표를 기반으로 위험단계 정보를 산출하였다.

V. 결 론

본 연구에서는 악성코드와 인터넷 웜 혹은 기타 알려지지 않은 공격들이 대량의 네트워크 트래픽을 발생시켜 네트워크 가용성을 심각한 수준으로 떨어뜨리는 위협에 대하여 적절하게 대처할 수 있도록 보안 관리자에게 공격 정보들을 조기에 알려주는데 있다. 그리고 제안하고자 하는 위협관리시스템은 알려지지 않은 비정상행위공격을 탐지할 수 있는 비정상행위 기반의 탐지기술을 포함하고 있으며, 위협이 되는 공격 정보들을 조기에 보안 관리자에게 제공할 수 있었다.

향후 인터넷 환경에서의 비정상 행위 공격에 대한 탐지 효율을 높이기 위하여 위협관리시스템을 보다 우수하게 수행하기 위한 자동화 프로세스 연구와 탐지 규칙 자동 생성 시스템을 개발할 필요가 있다.

참고문헌

[1] U. Lindqvist and P.A. Porras. Detecting Computer and Network Misuse with the Production-Based Expert System Toolset (P-BEST). In IEEE Symposium on Security and Privacy, pages 146-161, Oakland, California, May 1999.

[2] Christopher Kruegel and Giovanni Vigna. Anomaly Detection of Web-based Attacks. CCS'03 Washington, DC, October 2003.

[3] Juan M. Estevez-Tapiador and Pedro Garcia-Teodoro and jesus E. Diaz-Verdejo. Anomaly Detection Methods in Wired Network: a Survey and Taxonomy. In Computer Communications. July 2004

[4] 인터넷침해사고 대응지원세터, "KrCERT/CC", http://www.krcert.or.kr

[5] 문호건 외3명, "취약점 위협의 상관성 분석을 통한 네트워크 위험 조기경보 시스템 설계", 한국정보보호학회지, 제15권, 제1호, 2005년 2월.

[6] Christopher Kruegal, Giovanni Vigna, William Robertson, "A multi-model approach to the detection of web-based attack", Computer Network: The International Journal of Computer and Telecommunications Networking, Jan 2005

[7] 홍순화, 로드 분산 방법을 이용한 네트워크 트래픽 모니터링 및 분석, 석사논문, 2002

[8] Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher. Internet Denial of Service: Attack and Defense Mechanisms. Prentice-Hall, Upper Saddle River, NJ, 2004.

[9] Alefiya Hussain 외 5인, Experience with a Continuous Network Tracing Infrastructure, ACM SIGCOMM'05 Workshops, 2005

[10] C. Fraleigh, C. Diot, B. Lyles, S. Moon, P. Owezarski, D. Papagiannaki, and F. Tobagi. Design and deployment of a passive monitoring infrastructure. Lecture Notes in Computer Science, 2170:556-567, 2001

[11] Anukool Lakhina 외 5인, Structural Structural Analysis of Network Traffic Flows, ACM SIGMETR ICS/CS/Performance 2004

[12] 이창우 외3명, "분산환경에성의 침입방지를 위한 통합 보안 관리 시스템 설계", 한국컴퓨터정보학회 논문지, 제11권 2호, pp. 75~82, 2006.5.

[13] 오승준, 원민관, "텍스트 마이닝을 이용한 컴퓨터 네트워크의 침입 탐지", 한국컴퓨터정보학회 논문지, 제10권 5호, pp. 27~32, 2005.11.

저 자 소 개

김 효 남

1988 홍익대학교 전자계산학과 (이공학사)

1990 홍익대학교 전자계산학과 (이공석사)

2002 홍익대학교 전자계산학과 박사수료

현재 청강문화산업대학 컴퓨터소프트웨어과 부교수

<관심분야> OOP, Mobile, 컴퓨터 보안, 게임 보안