내부자 감사를 위한 클라이언트/서버 구조의 네트워크 트래픽 포렌식 시스템 설계

오형준○ 장성민 안현태 원유헌
홍익대학교
{hjoh○, smjang, vmasta}@cs.hongik.ac.kr, yhwon@hongik.ac.kr

A Design of Network Traffic Forensic System For Insider Auditing based on Client/ Server System

HyungJun Oh○, SungMin Jang, HyunTae An, YooHun Won
Hongik University, Dept.of Computer Engineering

1. 서 론

정보화 사회의 발달로 인해 보안의 중요성이 더욱 커지고 있다. 그로 인해 많은 보안 솔루션이 연구, 개발되고 있다. 이러한 보안 솔루션은 크게 공격의 방지 및 탐지를 위한 방어벽 및 침입탐지 시스템과 공격에 대한 사후 조치 및 증거 확보를 위한 포렌식 시스템 등으로 구분할 수 있다.

침입탐지기법은 크게 오용탐지기법과 비정상행위 탐지 기법으로 분류할 수 있다. 오용탐지 기법은 이미 알려진 공격 유형들을 정의해 놓고 그에 해당하는 공격을 탐지해 내는 침입탐지 기법이다. 그러나, 최근의 인터넷 공격은 대부분의 경우 악성코드를 이용한다. 악성코드를 이용한 공격의 경우 기존에 알려진 공격과는 달리 잘 알려지지 않은 제로데이 공격 형태를 나타내기 때문에 오용탐지 기법만을 적용해서는 적절한 대응을 하기 어려운 상황이다. 따라서, 사용자의 정상행위를 기반으로 정상적인 행동패턴에 어긋나는 행위를 침입으로 간주하는 비정상행위 탐지기법을 적용한 침입탐지 시스템의 필요성이 증대되고 있다.

포렌식 시스템은 범죄의 대처 관점에서 증거 확보 및 분석을 하기 위한 시스템으로 최근 범죄 수준의 악의적인 목적의 해킹이 빈번히 발생하고 산업 스파이에 의한 정보 유출 등이 발생함에 따라 많은 연구가 활발히 진행되고 있다.

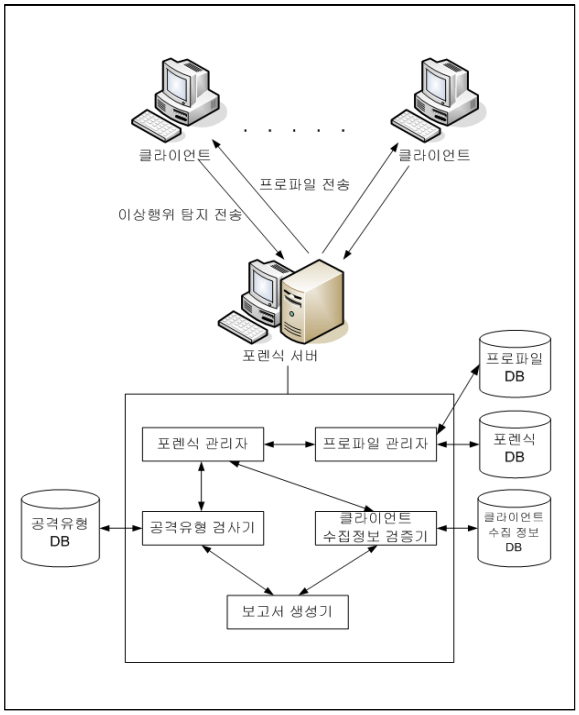
그러나, 이러한 보안 해결 방안으로 제시된 대부분의 기술은 외부로부터의 공격에 대해서는 많은 관심을 기울이고 해결하려고 하는 반면, 내부자에 대한 분석 및 감시에는 취약점을 보이고 있다. 본 논문에서는 내부자에 대한 분석 및 감시를 위해 내부자가 사용하는 클라이언트 시스템의 네트워크 트래픽을 모니터링하여 비정상행위 탐지 기법을 적용해 내부자 행동에 대한 이상 징후를 판단하는 시스템을 설계하였다. 또한, 이 시스템은 침입탐지 시스템의 탐지 로그 기록을 포렌식 정보로 이용하여 내부자 감사에 대한 증거 자료를 확보하는 포렌식 시스템의 역할을 담당하도록 하였다.

2. 본 론

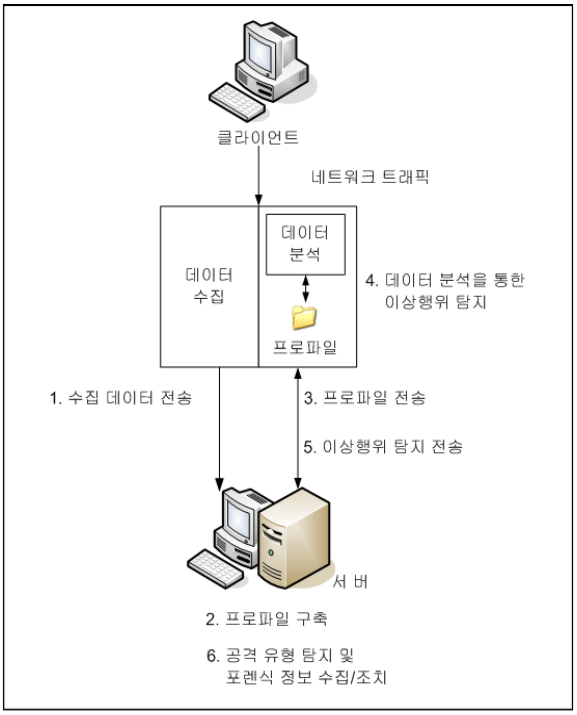
내부자 감사를 위한 네트워크 포렌식 시스템의 구성은 서버와 클라이언트 구조로 이루어진다. 대부분의 침해 탐지 시스템 및 포렌식 시스템이 서버를 통한 모니터링 및 실시간 제어가 이루어지는 것과는 달리 클라이언트에서 네트워크 트래픽에 대한 실시간 모니터링을 통해 이상 여부를 판단하고 이에 대해 이상 징후가 발견된 내용만 서버에게 전달한다. 서버는 해당 정보를 근거로 공격 행위의 발생 여부를 판단하고 공격 행위라고 판단 될 경우 클라이언트의 정보를 증거로 수집한다. 그리고, 공격 행위에 대한 내용을 상위 기관에 보고하여 해당 클라이언트에 대한 조치를 취하도록 한다. 서버의 상세 구성은 <그림 1>과 같다. 포렌식 관리자는 클라이언트로부터 받은 정보를 초기 분석하고 프로파일 관리자로 전달하는 역할을 담당하고 프로파일 관리자는 포렌식 관리자로부터 받은 프로파일 자료를 수집하여 포렌식 데이터베이스와 프로파일 데이터베이스에 저장하고 관리하며 일정 주기로 각각의 클라이언트에게 해당 프로파일을 전송한다. 공격유형 검사기는 이상 징후가 탐지된 클라이언트의 패킷을 공격유형 데이터베이스와 비교하여 공격 패턴을 탐지하는 기능을 수행하고 클라이언트 수집 정보 검증기는 공격 및 이상행위가 발견된 클라이언트의 각종 정보들을 수집하여 데이터베이스에 저장하고 관리하는 역할을 담당한다. 보고서 생성기는 클라이언트 상에서 공격행위가 발생되었다고 판단되는 상황에 대한 보고서를 생성하여 상위기관에 보고하고 상위 기관은 이 보고서를 토대로 적절한 대응을 취한다.

서버에서의 중요한 기능 중의 하나가 프로파일 데이터의 구축이다. 관리 대상인 내부의 클라이언트의

네트워크 비정상 행위를 탐지하기 위해서는 일정기간의 정상적인 트래픽의 프로파일링 단계를 수행해야 한다. 프로파일링 기간은 최소 한 달 이상으로 정하도록 한다. 그 이유는 각 클라이언트마다 시스템의 사용 목적에 따라 일별, 요일별 트래픽 유형이 달라질 수 있기 때문이다. 프로파일링 기간 동안에 클라이언트의 실시간 모니터링/제어기는 정상적이고 일상적인 클라이언트의 트래픽을 수집하여 서버로 전송한다. 서버의 프로파일 관리자는 각 클라이언트의 네트워크 프로파일을 날짜, 주간, 그리고 한달 간격으로 생성하여 데이터베이스에 저장한다. 전체 시스템이 탐지모드로 동작하게 되면 프로파일링 기간 동안에 생성된 프로파일 데이터는 날짜와 요일을 지정하여 매일 0시를 기점으로 클라이언트 실시간 모니터링/제어기로 전송되어지고 클라이언트 시스템에서 실시간 네트워크 트래픽과 비교하는 정상적인 트래픽 값으로 사용한다.



<그림 1> 내부자 감사를 위한 포렌식 시스템



<그림 2> 클라이언트 모듈의 내부 구성/동작

클라이언트에서 동작하는 내부 모듈은 <그림 2>와 같은 구성과 처리 과정을 보여준다. 클라이언트의 실시간 모니터링/제어기는 클라이언트의 네트워크 트래픽에 대해 실시간으로 모니터링을 하여, 데이터를 수집하고 비정상 행위를 분석한다. 실시간 네트워크 트래픽 분석에 필요한 프로파일 데이터는 서버로부터 일정 주기 단위로 수신한다. 프로파일을 이용한 데이터 분석 시 비정상행위 침입탐지시스템의 통계적 기법을 적용한다. 이 때, 트래픽 플로우 값(t_p)을 계산하기 위해 사용하는 식은 다음과 같다.

$$t_p = \log(R * r_p / r * R_p) \quad \text{.....(1)}$$

식 (1)에서 R은 최근 한 달간 트래픽량, r은 하루동안의 트래픽량, R_p는 특정 포트에 대한 최근 한 달간 트래픽량, r_p는 특정 포트에 대한 하루동안의 트래픽량을 의미한다. 여기서의 모든 트래픽량은 클라이언트의 네트워크 트래픽을 의미한다. 트래픽 플로우 값은 특정 포트의 트래픽이 급격히 증가할 경우 양의 값을 가지며, 반대의 경우는 음의 값을 가지게 된다. 따라서 트래픽량의 변화가 없을 경우는 0에 가까운 값으로 나타나고, 트래픽의 급격한 변화가 있을 경우에는 증감하게 되므로, 트래픽 플로우 값을 통해 네트워크 트래픽의 비정상 행위의 징후를 탐지할 수 있다.

3. 결 론

보안의 중요성이 증가함에 따라 많은 보안 솔루션이 등장하고 있다. 그러나, 대부분의 보안 솔루션은 외부로부터의 공격을 탐지하고 방지하는 것이 주요 목적으로 내부자의 이상 행위를 간과할 수 있다.

본 논문에서는 내부자 감사를 위한 시스템을 설계, 제시하였다. 내부자의 이상 행위를 판단하는 기준으로는 내부자 시스템(클라이언트)의 네트워크 트래픽을 사용한다. 즉, 내부자의 네트워크 트래픽을 이용하여 비정상행위 탐지 기법을 적용한 데이터 분석을 실시하고, 이상 징후 발견 시 컴퓨터 포렌식을 적용하는 시스템을 설계하였다. 향후, 기존의 보안 솔루션과의 결합 시 보다 안정적인 보안 시스템의 구축이 기대된다.