2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

웹 기반의 자동화된 로그 분석 시스템

임문희, 정태명**
성균관대학교 전자전기 및 컴퓨터 공학부
e-mail : mhim@rtlab.skku.ac.kr
tmchung@ece.skku.ac.kr

Web-based Automated Log Analysis System

Mun-Hui Lim, T. M. Chung**
Dept. of Electrical & Computer Engineering,
Sungkyunkwan University

요 약

정보 시스템의 눈부신 발전과 인터넷의 급속한 보급으로 인하여 누구나 웹상에서 그들의 정보 요구를 충족할 수 있게 되었다. 그러나 웹상에서의 정보 교환의 폭발적 증가로 인한 시스템의 중요 정보 및 자원 유출이 심각한 문제로 대두 되고 있다. 그러므로 관리자가 시스템에서 보유하고 있는 자원의 유출을 방지하고 시스템의 사용 원칙에 위배되는 해킹 행위를 추적하기 위한 감사 기능이 제공되어야 한다. 이에 본 논문에서는 감사 추적의 중요한 정보가 되는 유닉스 시스템의 로그 파일을 자동적으로 분석하는 시스템(WALAS)을 설계하였다. WALAS 는 UNIX 시스템 내의 방대한 로그 정보의 최적화를 통해 관리자가 해킹이나 사용자의 잘못된 시스템 사용 등을 효율적으로 감시하고 조사, 분석하는데 있어서의 자동화된 로그 파일 분석 시스템이다. WALAS 는 관리 대상 호스트의 로그 정보로부터 보안 정보를 추출하여 침입을 판단하며 침입으로 판정되면, 이를 웹 기반의 관리자 인터페이스로 전달하게 된다. 또한 방대한 양의 로그 정보를 적절히 분류하고 분석하며, 실시간으로 호스트 로그 파일을 모니터링하여 침입 발견 시 관리자의 즉각적 대응이라는 이점을 제공한다.

1. 서 론

최근 급속한 정보 통신 시스템의 발달과 인터넷의 확산으로 인하여 각 기관이나 업체 뿐 아니라, 각 가정의 컴퓨터 시스템도 바이러스나 인터넷 웜, 해킹 등의 위험에 노출되어 있다. 이러한 여러 가지 위험들로부터 시스템을 보호하기 위하여 각 시스템 운용자들은 침입 탐지 시스템, 방화벽, 바이러스 툴, VPN 등 여러 가지 보안 제품을 사용한다[1]. 이중 침입 탐지 시스템은 시스템 로그 파일을 분석하는 로그 분석 시스템, 네트워크 패킷을 분석하여 해킹 시도를 탐지하는 네트워크 기반 침입 탐지 시스템과 사용자 프로파일 등을 분석하여 해킹 시도를 탐지하는 호스트 기반의 침입 탐지 시스템 등으로 분류할 수 있다[2].

이중 로그 분석 시스템이란 호스트 로그 파일에 저장된 로그 데이터를 이용하여 사용자의 행위를 파악하고 분석하는 시스템이다. 그러나 시스템 자체적으로 저장되는 로그는 그 양의 방대함으로 인하여 관리자들이 수작업을 통해 분석하기에는 어려움을 준다. 이러한 관리자의 어려움을 줄이기 위해 자동화된 로그 분석 시스템이 필요하다. 로그 분석 시스템은 로그 데이터로부터 필요한 정보를 뽑아내어 분석 항목에 따라 분류하고 자동화된 감사 작업을 통하여 시스템 오류의 원인을 발견한다. 또한 사용자들의 잘못된 행위를 기록 및 분석하여 관리자가 이를 기반으로 시스템의 주요 정보를 수정, 변조하거나 해킹 하는 행위에 대한 사실을 발견할 수 있도록 해 준다.

본 논문에서는 UNIX 시스템에 기록되는 각종 로

그 파일의 종류와 각 로그의 의미, 로그 파일로부터 어떠한 방법으로 유용한 정보를 추출해내며, 그러한 로그 파일의 효과적인 분석을 통해 감사 작업에 어떻게 이용될 수 있는지에 대해 설명한다. 이러한 정보들을 바탕으로 기존에 관리자들이 수작업으로 수행해 오던 로그 분석 과정을 자동화할 수 있는 로그 분석 시스템과 이를 효율적으로 관리하기 위한 웹 기반의 인터페이스를 설계한다.

또한 다른 로깅 및 감사 도구들의 기능과 역할에 대해 살펴보고, 본문에서 설계된 WALAS과 비교하여 차이점과 한계들을 극복할 수 있는 방법에 대해서도 설명한다.

본 논문은 총 5 장으로 구성되어 있다. 2 장에서는 시스템 로깅 작업 및 각 로그 파일의 종류와 기능에 대해 설명하고 3 장에서는 WALAS 의 구성과 설계과정에 대해 설명한다. 4 장에서는 본 논문에서 설계한 WALAS 와 다른 분석 도구들을 비교 설명하며, 5 장에서는 WALAS 에 대해 요약하고 향후 연구 방향을 제시한다. 마지막으로, 본 논문의 작성을 위해 참고 된 참고 문헌을 기술한다.

2. 기존의 감사 추적과 로그 분석 기술

2.1 시스템 로깅 작업

외부로부터의 침입자 뿐 아니라, 시스템으로의 접근이 허용된 사용자에 의해서도 의도적인 행동이나 실수에 의해 시스템에 치명적인 피해가 야기될 수 있다[3]. 그런 경우에 시스템의 피해 정도와 누구에 의해서 언제 그러한 피해가 발생하였고, 피해가 미친 영향 범위가 어느 정도인지를 판단하여 최선의 복구 조치를 취해야 할 경우가 발생하게 된다. 그러한 상황에 대처하기 위한 방법은 매일, 매순간 보안과 관계된 시스템 이벤트들을 자동적으로 기록하고 안전한 형태로 저장하는 프로시저의 사용이다. 이러한 시스템의 주요한 이벤트의 기록 저장을 감사 추적이라 한다[4].

감사 추적은 언제, 누가, 어떤 자원을, 어떻게 이용하는가 하는 자료를 기초로 하여 다음과 같은 용도로 이용될 수 있다.

- 백업, 통계유지 등 시스템 사용 현황 파악 및 시스템 확장 기초 자료로 이용
- 시스템 자원 사용에 대한 모니터링 및 로깅에 의한 추적 자료로 이용
- 사용료 청구 등 회계 측면의 기초 자료로 이용

이러한 감사 기능 중 운영체제 자체적으로 생성된 감사 데이터를 가지고 침입을 탐지하는 것은 가장 기본적이 보안 방법이다[5]. 시스템은 시스템이 보호하는 모든 오브젝트에 대한 접근 사실이 기록되는 감사 추적을 유지해야 하며, 이러한 감사 추적 자료가 수정되지 않도록 보호해야 한다. 또한 이것은 TCSEC C2 수준의 평가를 위한 요구조건 중의 하나이다[6].

시스템이 관리하는 감사 레코드는 특정한 관리 권한을 가진 사용자만이 접근할 수 있도록 통제된다. 시스템이 기록해야 할 주요한 감사 자료는 다음과 같은 것들이 있다.

- 식별확인 메커니즘의 사용 (로그인)
- 사용자 영역 내의 오브젝트 사용 (파일 생성, 프로그램 수행)
- 오브젝트의 삭제 (파일 삭제, 프로세스 중단)
- 보안과 관련된 기타 이벤트 (로그인 시도 실패)

시스템에 의해 추적되어서 감사 기록으로 남게 되는 모든 이벤트에는 이벤트가 발생한 날짜와 시간, 이벤트의 종류와 이를 발생시킨 사용자, 이벤트의 성공 여부 등이 함께 기록되어야 한다.

이와 같은 이벤트에 대한 기록은 시스템이 특정 사용자별로 어떠한 작업들이 수행 되었는지를 선택하여 기록 할 수 있는 메커니즘이 제공되어야 한다.

2.2 UNIX 시스템의 주요 로그 파일

[표 1]은 UNIX 시스템에서의 주요한 로그 파일의 종류와 각 파일들의 기능을 나타내고 있다.

[표 1] UNIX 에서의 로그 파일

로그 파일 종류	위 치	기 능
utmp /utmpx	/var/adm/	시스템에 현재 로그인한 사용자들에 대한 상태를 기록하며, utmpx 는 utmp를 확장하여 원격 호스트 관련 정보 등을 추가로 포함한다.
wtmp /wtmpx	/var/adm/	사용자의 로그인, 로그아웃 시간과 시스템의 시작, 종료 시간 등을 기록한다.
acct/pacct	/var/adm/	바이너리 형태로 사용자가 실행하는 단일 명령어들을 기록한다.
sulog	/var/adm/	슈퍼 유저 권한으로의 변환을 시도하는 su 명령어를 사용한 결과가 저장된다.
syslog	/var/log/	시스템 콘솔 정보 메시지와 로그인 시 에러 메시지, 로그 파일의 내용을 포함한다.
messages	/var/adm/	시스템의 콘솔에서 출력된 결과와 syslog에 의해 생성된 모든 메시지를 기록한다.
loginlog	/var/adm/	사용자의 로그인 시도 실패 시 그 정보를 기록한다.

그러나 이렇게 기록된 로그 파일은 매순간 급증하기 때문에 관리자가 원본 데이터 만으로 시스템을 분석하기에는 무리한 부담이 된다. 또한 매일, 매주 혹은 매달을 주기로 로그 파일을 순환시킨다 하더라도, 관리자의 관리 요구사항에 맞게 시스템 자체적인 로그 파일을 분류할 수 없다.

2.3 기존의 로그 분석 도구들

UNIX 시스템에서의 보안 문제와 시스템 로그로부터의 효율적인 감사 기능을 위해 많은 로그 분석 도구들이 개발되고 있다. [표 2]는 현재 배포되어 있는 도구들 중, 가장 널리 쓰이는 도구들이다[7,8,9,10,11].

[표 2] 로그 분석 도구들

분석 도구	기 능
Logcheck	시스템의 보안 취약성이나 비정상적인 행위를 발견하기 위해 로그 파일들을 자동으로 점검해 주는 패키지이다. Logcheck는 간단한 쉘 스크립트로써 cron 데몬에 의해 최소한 몇 시간마다 실행되어져야 한다.
Logsurfer	시스템에서 식별이 어려운 로그 파일들을 감시하고 분석하여 규칙으로 정의된 특정 조건이 발생하는 경우 경고를 하여 관리자가 적절한 행동을 취하도록 한다.
Swatch	로그 파일들을 감시, 기록하며 의도되지 않은 데이터는 필터링 하고 우선순위에 따라 사용자가 정의한 행위를 수행 하도록 한다.
Tripwire	유닉스 시스템 파일에서 파일크기, 링크, 디렉토리 등의 변화, 생성 및 삭제된 파일들을 감시하고 이전에 만들어진 데이터베이스에 저장된 정보와 비교하여 다른 점을 기록한다.
Watcher	시스템을 감시하고 있다가 잘못된 것을 발견하면 보고해 주는 프로그램이다. 주로 디스크 공간, 프로세스 부하, 시스템 상태 등과 같은 시스템 통계치를 감시한다.

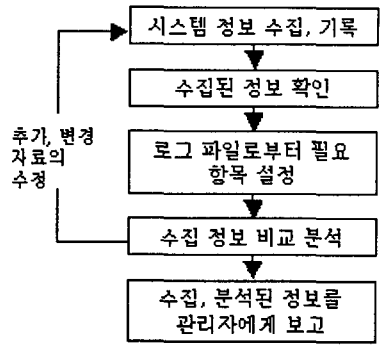
[표 2]에서 보여지는 것과 같은 기존의 로그 분석 도구들은 로그 파일을 자동으로 점검하거나 감시하는 기능만을 가지고 있다. 본 논문에서 제안하는 WALAS는 보안과 관련한 다양한 행위들에 대하여 관리자가 분석하는데 용이한 메커니즘과 실시간으로 탐지를 보고하는 시스템을 설계한다.

3. 본 논문에서 제안하는 WALAS

본 장에서는 기존의 UNIX 시스템에 저장된 로그 파일을 기반으로 웹 상에서 이를 자동적으로 분류하고 효율적으로 관리할 수 있는 메커니즘을 제시하고 웹 기반의 로그 파일 분석 시스템의 설계부터 기능과 장점에 대해 기술한다.

3.1 WALAS의 로그 분석 과정

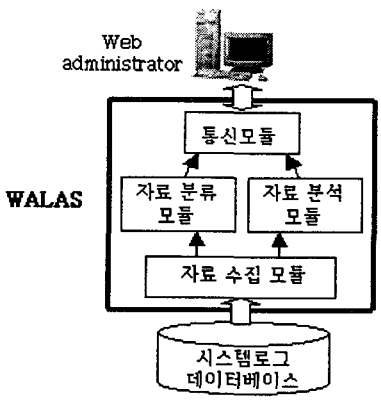
WALAS는 시스템에 의하여 기록된 로그 정보를 이용하여 관리자에 의해 정의된 설정을 기반으로 로그를 분류하고 자동으로 분석하여 침입이라 판단되는 행동에 대해 실시간으로 관리자의 인터페이스에 보고하는 기능을 제공한다.



[그림 1] 로그 분석 과정

[그림 1]은 로그 분석 과정을 도식화 한 것이다. 이에 대한 상세 설명은 다음과 같다.

- 시스템의 구성 데이터베이스로부터 사용자에 의해 제공되는 시스템 호출이나 라이브러리 호출 등의 원시 데이터를 수집하여 효율적인 시스템 관리에 필요한 정보를 결정한다.
- 수집된 정보가 적절한 형태로 어떤 로그 파일에 존재하는지에 대한 검사를 수행한다. 대부분의 유닉스 시스템에서는 syslog.conf를 통하여 로그 파일의 위치를 설정하고 이를 관리한다.
- 확인된 로그 파일로부터 시스템 관리와 침입의 탐지 등에 이용할 수 있는 항목들을 선택한다.
- 가장 최근에 수집된 정보와 새로 수집된 정보를 비교하여 추가, 삭제, 변경 등에 대한 상세 정보를 생성한다. 여기서 추가되거나 변경된 정보는 시스템의 기초 정보 수집 단계에 자동적으로 반영될 수 있다.
- WALFAS로부터 수집, 분석을 통한 결과를 관리자의 화면에 출력하게 된다. 여기서 관리자는 시스템의 사용 현황과, 잘못된 사용 등을 판단하는 근거 자료로써 로그 파일 생성을 구성할 수 있다.



[그림 2] 분석 에이전트 설계

[그림 2]는 WALAS의 로그 분석 에이전트의 내부 설계를 나타내고 있다. WALAS를 구성하는 각 모듈에 대한 기능은 다음과 같다.

- 시스템 로그 데이터베이스 : WALAS의 효율적인 기능 수행을 위해 시스템 정보와 기타 필요한 정보를 공급한다.
- 자료 수집 모듈 : 시스템 데이터 베이스에 기록된 로그 정보를 수집한다.
- 자료 분류 모듈 : 관리자 인터페이스 설정 창에서 관리자의 요구사항에 맞게 설정 된 로그 자료를 각 로그 파일로 분류한다.
- 자료 분석 모듈 : 자료를 분류함과 동시에 자동으로 분석하는 기증을 수행한다.
- 통신 모듈 : 자료 분류, 분석 모듈로부터 분석된 시스템 상태 정보를 관리자 인터페이스에 전송하는 기능을 수행한다.
- 웹 기반 관리자 인터페이스 : 관리자는 어느 곳에서나 관리자의 권한을 가지고 시스템을 감시할 수 있다. 침입 발견 시 즉각적인 대응을 위해 관리자에게 메일을 보내거나 경보를 울린다.

3.2 WALAS 의 관리자 인터페이스

WALAS는 분석되어 통신 모듈을 통해 관리자 인터페이스로 전달된 정보를 관리자가 효율적으로 관찰할 수 있게 한다. WALAS 인터페이스는 닫기, 설정, 통계, 관리 옵션으로 이루어져 있으며 설정 옵션에서 관리자는 시스템의 사용 현황과 보안 체크에 필요한 설정을 할 수 있다.

로그 파일의 구성 형태는 트리 형태로 나열되어 있으며 어떤 로그 파일을 선택하더라도 바로 '로그 보기' 화면에서 로그 정보를 확인할 수 있다. 관리자에 의해 설정된 로그 파일의 저장 형식에 따라 로그 정보는 다를 수 있다. 그러나 기본적으로 이벤트 사용자, 터미널, 이벤트의 발생 날짜와 시간, 출발지 주소와 목적지 주소를 포함한다[12].

4. 평 가

기존의 로그 분석 도구들은, 각 도구마다 차이는 있지만, 기본적으로 분석의 자동화와 시스템 문제 발생 시 관리자에게 메일을 보내는 등의 메커니즘을 가지고 있다. [표 3]은 그러한 차이점과 함께 WALAS 의 기능과 이점을 설명하고 있다.

[표 3] WALAS와 다른 도구들과의 차이점

기 능	WALAS	분석 도구들
로그 분석의 용이성	자동화된 로그 정보의 분류, 분석 기능으로 관리자가 로그 파일의 관찰, 감시에 용이하며 실시간 알림 기능을 포함한다.	시스템 파일 및 시스템의 상태에 대한 다각적 분석 요소들을 모두 수용하지는 못한다.
관리의 용이성	웹 기반의 관리자 인터페이스를 제공함으로써 관리자의 위치에 관계없이 어느 곳에서나 시스템의 상황을 감시, 관리할 수 있다.	원격 시스템이나 콘솔을 통해 호스트 시스템을 감시할 수 있다.
환경 구성의 용이성	시스템 관리 요구사항을 관리자가 인터페이스 상에서 용이하게 설정할 수 있다.	시스템 콘솔상에서 제어가 이루어지며 그 과정이 복잡하다.

5. 결론 및 향후 연구 방향

인터넷과 웹 브라우저의 급속한 발전 속에서 정보 시스템의 보안에 대한 위협 또한 증가하고 있다 이러한 상황에서 웹 기반의 UNIX 시스템에 기록되는 로그 정보를 이용하여 시스템내의 보안 상황을 감시하고 관리자가 무리한 부담 없이 효율적으로 관리할 수 있는 메커니즘이 개발되어야 한다.

이에 본 논문에서는 UNIX 시스템을 기반으로, 발생하는 침입에 대한 감사 추적과 효율적인 시스템 관리 기능을 수행할 수 있는 WALAS를 설계하였다. 이는 기존의 많은 감사 도구와 로그 분석 도구에 비해 관리자가 쉽게 로그 정보를 파악할 수 있도록 로그 정보를 최적화하고 관리자의 필요에 따라 항목들을 설정할 수 있다. 또한 침입의 발견 시 관리자에게 실시간으로 통보해 줌으로써 즉각적인 침입 조치를 취할 수 있게 한다.

향후 연구 방향은 사용자 정의 메커니즘에 대한 연구와 시스템으로부터의 효율적인 정보 추출 방법에 대한 연구를 수행할 것이다. 본 논문에서 제시한 시스템은 그러한 실제 구현에 있어서의 발판이 될 것이다.

참고 문헌

[1] Bishop, Matt, S. Cheung, J. Hoagland, S. Samorodin, C. Wee, "The Threat from the Net", IEEE Spectrum 34, 1997.
[2] D. E. Denning, "An Intrusion-Detection Model", In Processing of the IEEE Symposium on Security and Privacy, 1986.
[3] Teresa F. Lunt, "Automated Audit Trail Analysis and Intrusion Detection: A Survey", 11th National Computer Security Conference, October 1988.
[4] Rebecca Gurley Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000.
[5] Aurubindo Sundaram. "An Introduction to Intrusion Detection", 1996.
[6] "Trusted Computer System Evaluation Criteria (TCSEC)", DOD Standard 5200.28-STD, National Computer Security Center (NCSC), Orange Book, 1985.
[7] Psionic company web page <http://www.psionic.com>
[8] Web page <http://www.cert.dfn.de/eng/>
[9, 10] Simson Garfinkel & Gene Spafford, "Practical UNIX & Internet Security", OWEILLY, Second Edition, April 1996.
[11] Kenneth Ingham web page <http://www.i-pi.com>
[12] 이경준, "Security+ for UNIX", POSTECH Laboratory for UNIX Security.