제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

WAN 환경에서의 Syslog 관리 에이전트 시스템 설계

최강임*, 유황빈*
*광운대학교 컴퓨터과학과
e-mail : kichoi@netlab.kwangwoon.ac.kr
ryou@kwangwoon.ac.kr

Design of The Syslog Management Agent System in WAN

Kang-Im Choi*, Hwang-Bin Ryou*
*Dept of Computer Science, Kwangwoon University

요 약

Syslog는 Unix 시스템에서 로깅과 오류 보고를 위해 설계되었다. 즉, Syslog는 시스템 전반에 걸친 일상적 알림에서부터 치명적인 오류들과 네트워크 노드들 전반의 각종 행위들에 대한 감사 기록이다. 때문에 침해 사고 발생시 가장 우선적으로 사용되는 보안 감사 자료이며 장애나 침해가 발생하였음을 확인할 수 있는 유일한 증거이다. 그러나 기존의 Syslog 관리에서는 같은 WAN 환경에서도 로그 서버들 간의 로그 정보 공유가 제한적으로 행해지고 있다. 따라서 본 논문은 신뢰 가능한 로컬 네트워크로 구성된 WAN 환경에서 에이전트를 이용한 로컬 네트워크들 간의 원활한 로그 정보의 공유를 통해 보다 효과적인 Syslog 관리를 위한 시스템 모델을 제안하고자 한다.

1. 서론

네트워크 규모의 확대와 복잡화에 따라 네트워크를 구성하는 각 노드들의 자체 보안 및 전체적인 관리에 관한 관심이 증가하고 있다. 또한 정보통신 서비스의 급속한 확산에 따라 네트워크 환경에서 다양한 위험 요소가 증가하고 있다. 이에 침입으로부터 정보를 안전하게 보호하기 위해 침입탐지 시스템, 방화벽 시스템 등 다양한 네트워크 시스템에 대한 보호 장치들에 대한 개발과 연구가 진행 중이다.

네트워크/시스템 침입시도 또는 침해사고를 발견했을 경우 다양한 대응 방법들이 동원될 수 있다. 그 중에서도 Unix 시스템의 경우 가장 일반적이고 우선시 되어야할 대응 방법은 바로 시스템 로그 파일을 분석하고 그에 대한 대응책을 찾는 것이다.

네트워크의 다양한 노드들은 오류 메시지, 경고 메시지, 그 밖의 각종 정보 저장을 위한 로그 메시지들을 생성하게 되며, 이 메시지들은 침해 사고가 발생했을 때 또는 로그 정보를 이용한 정보 분석을 위해 파일로 저장되어야 할 필요가 있다. 이러한 로그 정보저장을 위해 Unix 시스템은 syslog를 제공한다[1].

즉, Syslog는 Unix 시스템에서 로깅과 오류 보고를 위해 설계되었으며 시스템 전반에 걸친 일상적 알림에서부터 치명적인 오류들과 네트워크 노드들 전반의 각종 행위들에 대한 감사 기록이다. 이러한 이유로 침해사고 발생시 가장 우선적으로 사용되는 보안 감사 자료이며 공격이 일어났음을 확인할 수 있는 유일한 증거이다. 따라서 Unix 시스템에서 로그 데이터를 관리하는 일은 시스템/네트워크 관리에 있어 가장 중요한 문제라고 할 수 있다.

로그 데이터를 보호하기 위한 여러 가지 방법 중 가장 일반적인 방법은 원격지에 로그 서버를 운영하는 방법이다[2][3]. 그러나 이 방법은 하나의 서버에 모든 호스트들의 로그 데이터를 저장하고 관리하고 있기 때문에 방대한 데이터로 인한 많은 어려움이 있다.

기존의 syslog 관리에서는 서로 신뢰가 가능한 네트워크로 구성된 WAN 환경에서도 로그 서버들

간의 로그 정보 공유가 제한적으로 행해지고 있다. 보안 사고가 일어났을 경우 우회적인 경로를 사용한 공격이나 공격 데몬이 상주하고 있는 호스트에 대해서는 메일이나 관리자의 양해를 구한 다음에 로그 데이터를 참조할 수가 있었다. 위와 같은 문제점들을 해결하기 위해 본 논문은 서로를 신뢰할 수 있는 네트워크들로 구성된 WAN 환경에서 에이전트를 이용한 로컬 네트워크들 간의 원활한 로그 정보의 공유를 통해 보다 효과적인 syslog 관리를 위한 시스템 설계를 제시하고자 한다.

2장에서는 syslog의 개념과 중요성 및 syslog 감사 자료별 저장 파일의 종류들에 대해 살펴보고 syslog를 관리하는 안전한 로그 서버에 대해 기술한다. 3장에서는 syslog 관리 에이전트 시스템의 구성과 에이전트의 기능에 대해 기술한다. 마지막으로 4장에서는 결론 및 향후 연구 방향에 대하여 언급한다.

2. Syslog 개념

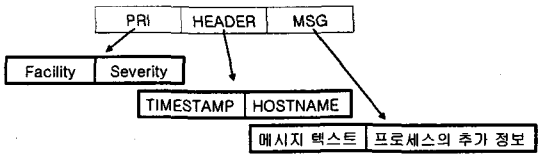
2.1 syslog

Syslog는 Unix 시스템에서 로깅과 오류 보고를 위해 설계되었으며 시스템 전반에 걸친 일상적 알림에서부터 치명적 오류까지에 대한 감사 기록이므로 침해 사고가 발생 했을 경우 가장 우선적으로 사용되는 중요한 자료이다.

Syslog 시스템은 다른 운영체제에 비해 Unix에서 보다 유용한 서비스이다. 다른 운영체제들이 로그를 제한된 범위 안에서 사용하도록 제공하는 것과는 달리 Unix는 커널 수준에서 상위 서비스까지 모든 로그를 남길 수 있다. 일반적인 Unix 시스템은 로그 데이터가 제공되므로 관리자가 로그 설정을 하기만 하면 된다. 이와 같은 이유로 syslog는 침해 사고의 발생 시 중요한 감사 자료로 쓰이고 있다.

표준문서에 따른 syslog의 패킷 형식과 내용은 UDP 포트 514번을 사용하여 메시지를 전송하며 메시지는 PRI, HEADER, MSG 이 세부분으로 구성된다. 첫 번째 부분인 PRI는 syslog 메시지의 기능별 구성요소(facility)와 위험도(severity)를 표현하는 우선순위이다. 두 번째 부분인 HEADER는 TIMESTAMP와 HOSTNAME으로 불리는 두 가지 필드를 포함한다. 마지막으로 MSG는 메시지 텍스트와 메시지를 생성했던 프로세스의 추가적인 정보를 포함한다. 부가적으로 syslog 메시지의 전체 길이는 1024 바이트를 초과해서는 안된다[4][5].

(그림 1)은 syslog 패킷 형식과 내용을 표현한 것이다.



(그림 1) syslog 패킷 형식과 내용

<표 1>은 syslog 메시지의 기능별 구성요소를 표현한 것이고 <표 2>는 syslog 메시지의 위험도를 표현한 것이다.

<표 1> syslog 메시지기능별 구성요소(Facility)

숫자 코드	기능별 구성요소(Facility)
0	커널 메시지
1	사용자 레벨 메시지
2	메일 시스템
3	시스템 데몬들
4	보안/인증 메시지
5	syslogd 내부 메시지
6	라인 프린터 서브시스템
7	네트워크 뉴스 서브시스템
8	UUCP 서브시스템
9	clock 데몬
10	보안/인증 메시지
11	FTP 데몬
12	NTP 서브시스템
13	로그 감사
14	로그 경고
15	clock 데몬
16~23	local 사용 0~7

<표 2> syslog 메시지 위험도(Severity)

숫자 코드	위험도(Severity)
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

2.2 syslog 감사 자료별 저장 파일

로그 데이터를 이용하여 시스템 버그의 원인과 침입자의 출처 및 침해 사고의 범위를 알 수 있다. <표 3>은 syslog 감사 자료별 저장 파일 종류 및 기본적인 기능을 요약한 것이고 이는 시스템에 따라

약간씩의 차이가 있다.

<표 3> syslog 감사 자료별 저장 파일

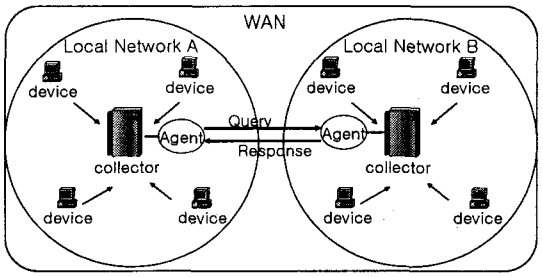
파일명	기 능
acct 또는 pacct	사용자별로 실행되는 모든 명령어 기록
aculog	다이얼-아웃 모뎀 관련 기록
lastlog	각 사용자의 가장 최근 로그인 시간 기록
loginlog	실패한 로그인 시도 기록
messages	부트 메시지 등 시스템의 콘솔에서 출력된 결과를 기록하고 syslog에 의해 생성된 메시지도 기록
sulog	su 명령 사용 내역 기록
utmp	현재 로그인한 각 사용자의 기록
utmpx	utmp 기능 확장, 원격 호스트 관련 정보 등 자료 구조 확장
wtmp	사용자의 로그인, 로그아웃 시간과 시스템의 종료 시간 시작 시간 등을 기록
wtmpx	wtmp 확장
vold.log	플로피 디스크나 CD-ROM과 같은 외부 매체 사용에서 발생하는 에러 기록
xferlog	FTP 접근 기록

2.3 syslog 서버

로그 데이터를 보호하기 위한 일반적인 방법은 다음과 같다. 첫째, 오직 로그 수집용으로 사용되는 별도의 호스트에 로그 데이터를 저장한다. 이 호스트는 네트워크를 통한 불법적인 접근이 불가능하도록 충분히 안전하여야만 한다. 둘째, 특정 데이터는 한번 쓰여진 데이터가 수정될 수 없는 장치에 기록한다. 셋째, 시스템에서 지원이 된다면 설정된 로그 파일 속성을 새로운 정보를 로그 파일에 추가할 수는 있지만 기존에 있는 정보를 수정할 수 없도록 설정한다. 넷째, 로그 파일을 암호화한다.[2][3] 이상의 네 가지 방법 중 가장 현실적이고, 일반적으로 사용되는 방법은 첫 번째 방법인 원격지에 로그 서버를 운영하는 것이다. 이에 본 논문에서는 Unix 시스템이 원격 로그 서버를 운영할 경우 에이전트를 이용하여 좀 더 효과적으로 syslog를 관리할 수 있는 시스템 모델을 제시하려고 한다.

3. 에이전트를 이용한 syslog 관리 시스템 설계

현재 로그 데이터를 관리하는 로그 서버는 네트워크 노드들의 각각의 로그 데이터를 수집하는 기능만을 가지고 있다. 한대의 로그 서버에 모든 호스트들의 로그 데이터를 관리하고 있기 때문에 단시간의 로그 데이터의 확대와 방대한 데이터로 인해 너무나 많은 정보를 빠르게 보여주는 등 많은 문제점들이 야기 되고 있다. 따라서 필요한 정보만을 검색하고 분석할 수 있도록 하여 트래픽 문제를 개선하기 위해 에이전트 기법을 도입했다. 로그 데이터의 중요성으로 인해 환경은 서로 신뢰 가능한 로컬 네트워크로 구성된 WAN에서의 공유로 제한한다. 각각의 로컬 네트워크들의 로그 서버에 에이전트를 연결하여 방대한 로그 데이터들 중에서 필요한 정보만을 선택적으로 택하여 자료를 공유하고 분석할 수 있도록 돕고자 한다. 또한 침해 사고가 발생했을 경우 연결된 다른 로컬 네트워크들의 에이전트에 경고 메시지를 전송함으로써 침해 사고에 빠르게 대응할 수 있는 근거자료를 제시하고자 한다.



(그림 2) syslog 관리 에이전트 시스템

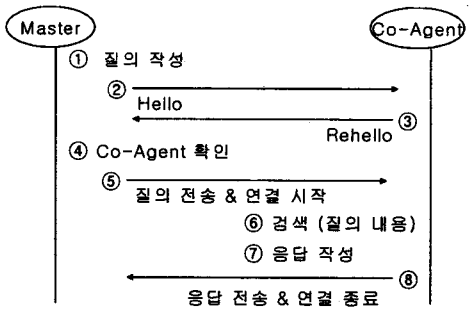
3.1 syslog 관리 에이전트 시스템의 구성

(그림 2)는 syslog 관리 에이전트 시스템을 나타낸다. 다음은 간단한 용어 정의이다[4][5].

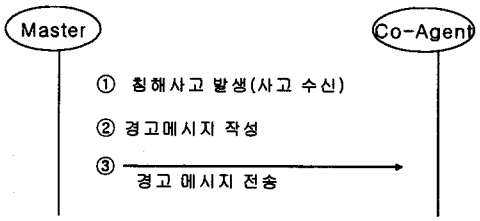
- device- 메시지를 생성할 수 있는 호스트
- relay- 메시지를 수신할 수 있고 그것을 다른 호스트에 전송할 수 있는 호스트
- collector- 메시지를 수신하고 다른 호스트에 그것을 전송하지 않는 호스트, 일반적으로 "syslog server"이라고 칭함
- sender- device나 relay가 메시지를 전송할 때 "sender"가 될 수 있음
- receiver- relay나 collector는 메시지를 수신할 때 "receiver"가 될 수 있음

syslog 관리 시스템은 에이전트를 이용하여 로그 데이터를 저장하기만 하는 로그 서버에 에이전트를 이용하여 같은 WAN 상에서는 로그 데이터를 공유함으로써 시스템을 관리하고 분석하는데 도움을 주고 침해 사고 발생시 이에 좀 더 빠르게 대처할 수 있는 근거 자료를 제공하는 기능을 가진다.

3.2 에이전트 기능



(그림 3) 에이전트의 질의-응답 기능



(그림 4) 에이전트 경고 메시지 기능

(그림 3)과 (그림 4)은 syslog 관리 시스템에서 에이전트의 기능을 표현한 것이다. (그림 3)는 에이전트의 질의-응답 기능으로서 Master에서 Cooperative-Agent에 시스템 분석과 관리에 도움되는 로그 데이터를 얻고자 할 때 필요한 기능이다. 우선 Master는 Co-Agent에 요청할 로그 데이터를 질의 형식에 맞춰 작성을 하고 Co-Agent에 연결 요청(Hello)를 한다. Co-Agent는 연결 요청에 따른 답(Rehello)을 보내고 Master는 Rehello로 Co-Agent임을 확인하고 질의를 전송하면서 연결을 시작한다. Co-Agent는 로그 서버를 통해 질의에 해당하는 내용을 검색하고 응답을 작성한다. 그 후에 Co-Agent는 응답을 Master에 전송하면서 연결을 종료하게 된다. (그림 4)은 에이전트의 경고 기능으로서 Master에 침해 사고가 발생시 WAN에 연결되어 있는 모든 로컬 네트워크들의 로그 서버에 맞물려 있는 에이전트에 경고 메시지를 전송함으로써 빠른 대응을 할 수 있도록 돕는 역할을 한다. 처음에 Master는 네트워크기반 침입탐지시스템이나 호스트기반 침입탐지 시스템으로부터 침입이 발생했다는 사고를 수신한다. 이에 Master는 그에 해당하는 로그 데이터로 경고 메시지를 작성한다. 그 후에 $Co\text{-}Agent_1$에서 $Co\text{-}Agent_n$까지 모든 연결된 에이전트에 경고 메시지를 보낸다.

4. 결론 및 향후 연구 방향

본 논문에서는 syslog 관리 에이전트 시스템을 이용하여, 로그 서버에서의 대규모의 로그 데이터의 관리와 제한된 공유로 인한 문제점을 해결하였다. 이것은 서로 신뢰 가능한 네트워크로 구성된 WAN 환경에서는 로그 데이터를 수집하여 사용 유형을 분석하여 관리에도 도움을 줄 뿐만 아니라 침해 사고가 발생했을 시 보다 빠른 대응 방법을 제시할 수 있는 근거 자료를 제공 한다.

그러나, 에이전트 상호간의 메시지 전송 시 안전성에 대한 문제가 제기 된다. 따라서 향후 보다 강력한 보안요구를 충족하기 위해서 상호 인증과 비밀성을 보장할 수 있는 로그 데이터의 축약, 암호화 기능과 같은 보다 특화된 보안 서비스를 추가하기 위한 연구를 시행하여 syslog 관리 에이전트 시스템의 성능한계를 보완할 예정이다.

참고문헌

[1] Scott Mann, Ellen L. Mitchell, Mitchell Krell "Linux System Security" 2nd Ed. Prentice Hall, pp.179~195, 2003

[2] 정현철, "Unix 로그분석을 통한 침입자 추적 및 로그 관리: Part Ⅰ", URL: http://www.certcc.or.kr, CERTCC-KR-TR-2001-11, 2001

[3] 정현철, "Unix 로그분석을 통한 침입자 추적 및 로그 관리: Part Ⅱ", URL: http://www.certcc.or.kr, CERTCC-KR-TR-2001-13, 2001

[4] "The BSD syslog Protocol", URL: http://www.ietf.org/rfc/rfc3164.txt?number=3164, RFC 3164, IETF, August 2001

[5] "Reliable Delivery for syslog", URL: http://www.ietf.org/rfc/rfc3195.txt?number=3195, RFC 3195, IETF, November 2001