SysLog기반의 통합로그관리시스템에 관한 연구

이동영*, 이을석**, 김진철***
*명지전문대학 정보통신
**(주)이너버스 기술연구소
***명지전문대학
e-mail:dylee@mjc.ac.kr*, uslee@innerbus.com**,jj9636@yahoo.co.kr***

A Study on SysLog-based Integrated Log Management System.

DongYooung Lee*, Eul-Suk Lee** , Jin-Chul Kim***
*Dept of Information & Communication, MyongJi College
**Institute of Technology, Innerbus Company
***MyongJi College

요 약

주요 ISP(Internet Service Provider)와 금융기관 및 공공기관에서는 로그 분석에 대한 관심도가 높아지고 있다. 보안사고 발생시 원인 규명을 위한 근거자료와 재발방지를 위한 정보를 제공하고, 이를 기반으로 정보보호시스템 관리자에게 다양한 보안정책을 수립할 수 있는 기반자료로 활용 로그정보의 수집과 대용량의 로그정보를 백업할 수 있는 통합로그수집/백업시스템의 필요성이 절실히 요구되고 있다. 이에 본 논문에서는 로그메시지를 처리하기 위해서 제공하는 표준 인터페이스 중 하나인 SysLog를 기반으로 이종의 침입차단시스템의 로그를 통합관리하는 시스템을 설계·구현하였다.

1. 서론

정보화 사회로 발전하면서 통신서비스 이용자들은 보다 신속하고 다양한 서비스를 요구하게 되고, 이에 전송속도의 고속화, 대용량의 데이터 전송 등으로 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 거두고 있는 반면, Open Network인 인터넷의 개방으로 인한 외부자의 시스템 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 공격 등 부정적인 기능들도 날로 증대시킴으로서, 이로 인한 피해 규모는 심각한 수준에 이르고 있다. 특히 국내 공공기관, 금융기관 및 주요 포털사이트를 대상으로 이루어지는 DDoS(Distributed Denial of Service : 분산서비스거부공격)으로 인한 피해는 심각한 수준이다.

이에 정부기관에서는 정보시스템 구축 운영과 관련한 기술 가이드라인[1-2]에서는, "주요 시스템 및 장애에 대한 로그보관, 백업(backup) 및 분석지침을 수립하고 로그는 최소 6개월 이상 백업을 유지 관리하여 주요 보안시스템(Firewall, IDS, VPN)의 로그는 매일 분석"을 권고하고 있다. 이에 주요 ISP(Internet Service Provider)와 금융기관 및 공공기관에서는 로그 분석에 대한 관심도가 높아지고 있다. 보안사고 발생시 원인 규명을 위한 근거자료와 재발방지를 위한 정보를 제공하고, 이를 기반으로 정보보호시스템 관리자에게 다양한 보안정책을 수립할 수 있는 기반자료로 활용 로그정보의 수집과 대용량의 로그정보를 백업할 수 있는 통합로그수집/백업시스템의 필요성이 절실히 요구되고 있다.

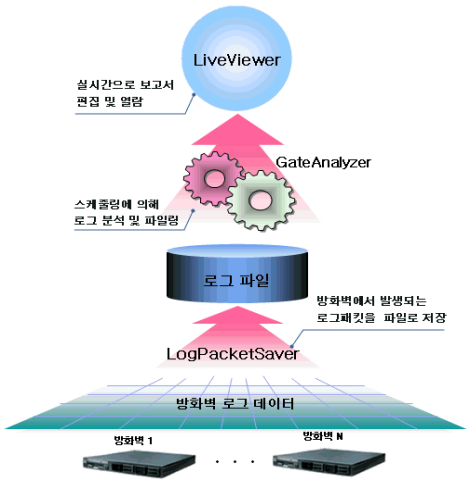
이에 본 논문에서는 각종 장비(방화벽, IPS, 라우터 및 네트워크 장비)의 SysLog를 전송, 저장, 백업하기 위한 SysLog 수집하고 분석하는 SysLog기반의 통합로그관리시스템(SILAS: SysLog-based Integrated Log mAanagement System)에서 가장 대표적인 네트워크보안시스템인 침입차단시스템(일명: 방화벽(Firewall))의 로그를 수집하고 분석하는 모델을 설계/구현하였다.

2. 연구내용

2.1 SysLog를 이용한 방화벽 로그분석시스템구조

본 연구에서 제안하는 통합로그분석시스템(SILAS)의 경우 방화벽 저장된 로그를 분석하여 보안상 문제가 될 수 있는 원인과 그에 대한 해결 방안을 제시할 수 있는 근거자료를 확보하고, 분석 자료를 이용하여 체계적인 보안정책을 수립할 수 있는 기능을 수행한다.

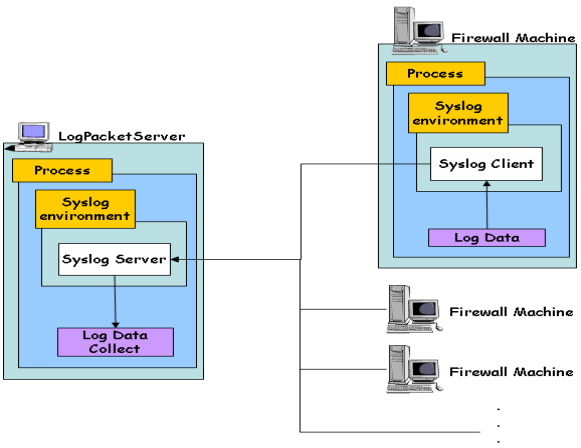
SILAS의 구성은 크게 방화벽으로부터 로그패킷을 수집하는 로그 수집 모듈(LogPacketSaver), 수집된 로그파일을 분석하는 로그 분석 모듈(GateAnalyzer), 로그 분석 모듈에서 분석된 보고서를 열람 및 편집할 수 있는 모듈(LiveViewer)로 구성되어있으며 [그림 1]은 기본 구조를 나타낸 것이다.



(그림 1) SILAS의 기본 구조

2.2 방화벽 로그 수집 모듈

SysLog[3]는 Unix 시스템에서 로그메시지를 처리하기 위해서 제공하는 표준 인터페이스 중 하나이며 이를 이용하여 시스템이나 응용 프로그램에서 발생하는 각종 메시지를 체계적으로 관리할 수 있다. 또한 운영체제에 관계없이 동일하게 사용할 수 있다는 장점도 갖고 있으며 이를 이용하여 다양한 장비(방화벽, IPS, 라우터 및 네트워크 장비)의 에러 메시지나 보안사고시 이벤트를 정확히 기록하여 문제 발생 즉시 원인을 규명할 수 있는 근거 자료로 활용이 가능하다[4-6]. 그러나 실제 기업의 네트워크 환경에서는 네트워크 장비들의 저장장치 용량이 제한되어 SysLog 저장을 위한 공간적 한계를 갖고 있어서 이에 대한 효율적인 관리에 어려움을 겪고 있는 실정이다. (그림 2)는 SysLog를 이용한 방화벽 로그 수집모듈의 구조를 나타낸 것이다.



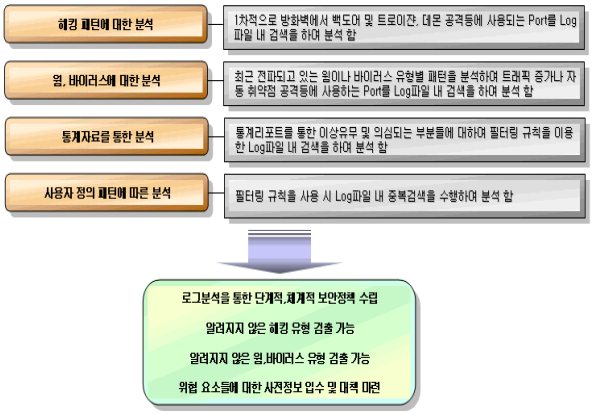
(그림 2) SysLog를 방화벽 로그 수집모듈의 구조

(그림 2)에서 보는 바와 같이 SysLog Client는 관리대상 방화벽시스템으로부터 로그데이터를 수집하고 이를 SysLog Server에게로 전송하는 기능을 수행한다.

2.3 방화벽 로그 분석 모듈

로그 분석 모듈은 일별 로그파일이 10Gbyte 이상의 대용량 로그파일 분석 기능과 멀티쓰레드, 멀티프로세스 환경을 지원함으로써 포괄적인 트래픽 분석과 해킹 패턴이나 최근 전파되고 있는 웜이나 바이러스 유형별 패턴을 분석한다.

그리고 분석된 정보를 기반으로 시스템 사용자의 이상증후를 조기에 발견하고, 시스템으로의 침입시도를 파악할 수 있게 된다. 따라서 분산되어 있는 방화벽의 활동에 대한 종합적인 분석정보를 얻을 수 있으며, 공격의 원천과 위험수준 모두를 식별하고, 네트워크를 보다 더 쉽게 방어할 수 있는 정보를 고객에게 제공한다. 또한 위험요소 분석을 통해 최적의 보안정책을 수립할 수 있다. (그림 3)은 다양한 로그패턴을 분석하는 동작 메커니즘이다.



(그림 3) 다양한 로그패턴을 분석하는 동작 메커니즘

다음은 “MS04-011 취약점을 가진 lsasrv.dll 에 대해 버퍼오버플로우 공격을 시도하는 패턴”에 대한 로그파일 분석하는 예를 나타낸 것이다.

- 예제로그(Sample Log)

```
id=firewall time="2010-10-28 19:37:24" fw=firew4 pri=6
proto=445/TCP src=192.168.47.250 dst=158.216.65.1
sent=2592 msg="ALLOW SESSION"
id=firewall time="2010-10-28 19:37:27" fw=firew4 pri=6
proto=4444/TCP src=192.168.47.250 dst=158.216.65.1
sent=2592 msg="ALLOW SESSION"
```

- 분석결과

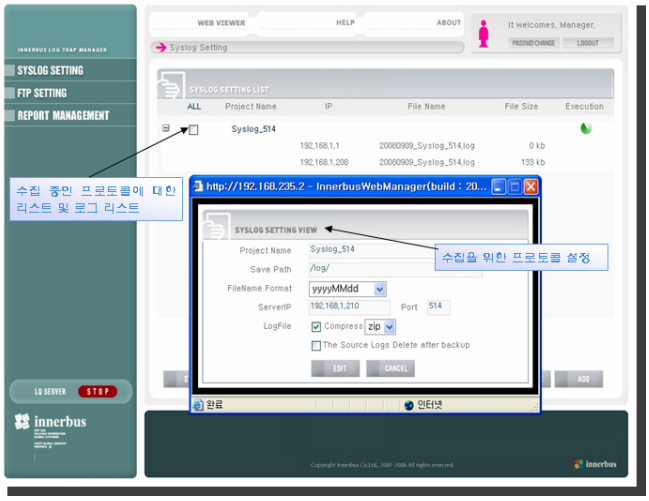
-srcip=SRCPORT, srcport=any,dstip=DSTIP, dstport=445, action=any

-srcip=SRCPORT, srcport=any, dstip=DSTIP, dstport=4444, action=any

2.4 방화벽 로그뷰어(LiveViewer)모듈

방화벽로그 분석모듈에서 수집된 SysLog를 분석한 후 결과는 방화벽로그뷰어를 통해서 제공된다. 본 논문에서 구현한 방화벽 로그뷰터는 방화벽 시스템별 상이한 로그 단일 형태로 변환하고 이를 정기적으로 침입유형별로 분류하여 MS Word또는 Excel파일 형태로 보안관리자에게

제공하는 기능 갖는다. (그림 4)는 본 연구를 통해서 구현된 방화벽 로그뷰어(LogViewer)시스템을 나타낸 것이며, ava/xml로 개발하여 모든 플랫폼을 지원할 수 있도록 구현하였다.



(그림 4) 방화벽 로그뷰어(LogViewer)시스템

3. 결론 및 향후계획

본 연구에서는 대용량의 방화벽에서 발생하는 로그패킷을 실시간으로 저장하고 SysLog기반으로 이를 분석 및 관리하는 통합로그관리시스템(SILAS: SysLog-based Integrated Log mAanagement System)을 설계하고 프로토타입(prototype)으로 구현하였다. 또한 통합로그관리시스템에서 도출된 결과는 실제 방화벽을 운영하고 있는 네트워크 보안정책 수립에 기반자료로 활용이 가능하다.

향후계획으로는 네트워크장비의 로그파일이 대용량화는 경향을 고려하여 대용량 로그파일 분석하고 신속하게 처리할 수 있는 알고리즘 개발과 실제 환경에서 성능 분석을 통한 시스템 안정화 작업이 요구된다.

참고문헌

[1] 정보통신부, 정부혁신지방분권위원회, 한국전산원 제정, “정보시스템 구축 운영과 관련한 기술 가이드라인 버전 1.0”, 2004. 4.

[2] 행정자치부 보안관리팀, 개인정보 침해유형 및 취약점 보안대책, 2007. 7.

[3] Chris Fry. Martin Nystrom. "Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks", O'Reilly.

[4] Qiang Fu Jian-Guang Lou Yi Wang Jiang Li "Execution Anomaly Detection in Distributed Systems through Unstructured Log Analysis", IEEE Conference ICDM'09, Dec. 2009.

[5] Herrerias, J. Gomez, "Log Analysis Towards an Automated Forensic Diagnosis System", IEEE ARES'10, 15-18 Feb. 2010.

[6] Matsumoto, S. Sato, A. Shinjo, Y. Nakai, H. Itano, K. Shomura, Y. Yoshida,"A Method for Analyzing Network Traffic Using Cardinality Information in Firewall Logs", Applications and the Internet (SAINT), 2010 10th,