디지털산업정보학회 논문지 제7권 제4호-2011년 12월

분산 환경에서 SysLog기반의 방화벽 통합로그관리시스템 개발

이 동 영* · 서 희 석** · 이 을 석***

Development of the SysLog-based Integrated Log Management System for Firewalls in Distributed Network Environments

Lee, Dong Young · Seo, Hee Suk · Lee, Eul Suk

〈Abstract〉

Application log files contain error messages; operational data and usage information that can help manage applications and servers. Log analysis system is software that read and parse log files, extract and aggregate information in order to generate reports on the application. In currently, the importance of log files of firewalls is growing bigger and bigger for the forensics of cyber crimes and the establishment of security policy.

In this paper, we designed and implemented the SILAS(SysLog-based Integrated Log mAanagement System) in distribute network environments. It help to generate reports on the the log fires of firewalls - IP and users, and statistics of application usage.

Key Words : SysLog, Firewall, Integrated Management System

Ⅰ. 서론

정보화 사회로 발전하면서 통신서비스 이용자들은 보다 신속하고 다양한 서비스를 요구하게 되고, 이에 부응하여 컴퓨터와 정보통신 기술의 발달은 전자 메일, 파일 전송 등과 같은 기본적인 서비스 뿐 만 아니라 분산 환경을 바탕으로 하는 멀티미디어, 전자 결재, 전자 상거래 등과 같이 복합적인 네트워크 서비스들로 확장되고 있다. 그리고 이와 같은 발전은 전송 속도의 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 일부 ISP(Internet Service Provider)의 국내 및 국제구간에서 UDP Flooding, Host Sweep과 TCP Syn Flooding DDoS(Distributed Denial of Service : 분산서비스거부공격)으로 인한 피해는 심각한 수준이다.

특히 국내 공공기관, 금융기관 및 주요 포털사이트를 대상으로 이루어지는 DDoS(Distributed Denial of Service : 분산서비스거부공격)으로 인한 피해는 심각한

* 명지전문대 정보통신과 부교수(교신저자)
** 한국기술교육대 컴퓨터공학부 부교수
*** (주)이너버스 대표이사

수준이다. <표 1>은 국내 주요 기관별 해킹사고 현황을 나타낸 것이다[1].

<표 1> 국내 주요 기관별 해킹사고 현황

기관	2010년		2011년			
	11월	12월	1월	2월	3월	4월
개인	885	800	615	480	619	641
기업	509	492	392	358	356	338
대학	10	6	8	8	21	15
비영리	6	9	10	8	6	5
연구소	2	0	0	0	0	0
총계	1,412	1,307	1,025	854	1,002	999

이에 정부기관에서는 정보시스템 구축 운영과 관련한 기술 가이드라인[2-3]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. 로그(Log)는 정보화 장비 및 네트워크 운영 과정에서 발생한 모든 내용들의 발생시간 등을 함께 기록한 자료를 말한다. 따라서 로그는 특수피해나 보안사고가 발생했을 경우 결정적인 증거가 될 수 있다. 이 때문에 대다수 금융권들은 로그를 법적인 규제를 통해 관리·감독하도록 되어있다. 그러나 금년 4월에 발생한 농협 전산망 장애 사건에서 볼 수 있듯이 매일 발생하는 많은 량의 로그정보를 체적으로 관리하기는 쉽지 않은 일이다.

또한, 통신망의 고도화, 지능화 추세에 따라 통신망의 관리 방식과 개념의 변화가 요구된다. 즉, 복잡하고 다양한 방식의 대규모 네트워크 환경에서 이종의 보안시스템과 라우터, 스위치와 같은 다양한 네트워크 장비에 대한 통합적인 관리가 요구되고 있다. 이에 따라, Web및 application기술의 발달과 함께 소비자의 정보 편재성(ubiquity)이 증가하면서 국내 로그 분석 서비스 가입자의 수가 급속도로 확대되고 있는 추세이다.

이벤트 로그(Event Log)는 SNMP, LEA, Syslog등의 형태로 관리대상시스템(MO: Managed Objects)의 이벤트 정보를 관리시스템(Manager System)에 전송하며, 해당 시스템에 대한 심각한 보안사고 및 Fault 발생시 매우 중요한 정보를 가지고 있다. 하지만 지금까지 대다수 기관에서 이러한 중요한 전산자원인 이벤트로그를 체계적으로 관리하지 못하고 방치하거나, 단순히 Storage장비에 보관만 하고 있는 상태이며 더 이상이 발생하였을 때 신속하게 대처하지 못하고 있는 실정이다.

본 논문에서는 관리대상 시스템(MO: Managed Objects)에서 발생하는 이벤트로그 정보를 실시간으로 통합 모니터링하여 보안사고 발생시 이에 대한 경고 및 원인 규명의 근거 자료수집 및 재발방지를 위한 보안정책 수립 등의 기능을 수행하는 실시간 이벤트모니터링 시스템을 개발방안을 제시하고자 한다.

Ⅱ. 관련 연구

2.1 국내·외 실시간 이벤트 모니터링 시스템의 특징

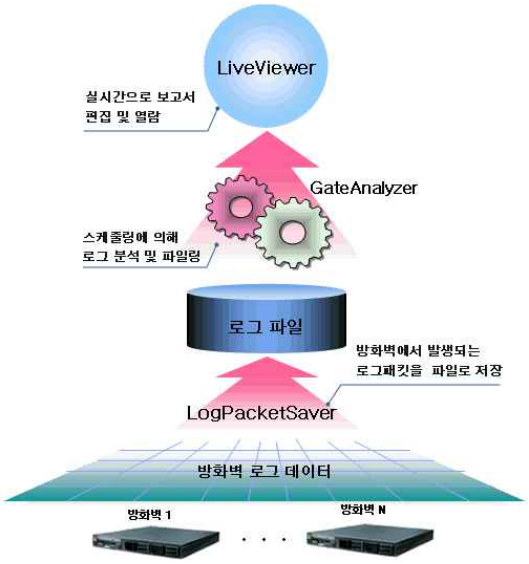
국내·외 실시간 이벤트 모니터링 시스템을 살펴보면 미국의 NetIQ사의 Security Reporting Center의 경우 세계 시장 점유율은 1위이나 국내 보안시스템에 대한 지원이 다소 미약하며 국내 실정에 맞지 않는 인테페이스 기능을 제공하고 있다. 또한, 국내의 경우 (주)이글루시큐리티의 경우 ESM(Enterprise Security Management)을 기반으로한 관제 솔루션으로 이벤트 모니터링 및 분석 기능이 다소 취약하며 시스템 가격이 고가여서 국내 중소기업환경에 적용하기에는 다소 어려움을 갖고 있다. 이에 본 연구에서는 이벤트 로그(Event Log)는 SNMP, LEA, Syslog등의 형태로 관리대상시스템(MO: Managed Objects)의 이벤트 정보를 관리시스템(Manager System)

에 전송하며, 해당 시스템에 대한 심각한 보안사고 및 Fault 발생시 매우 중요한 정보를 제공하고 이를 보안정책에 반영하는 하는 프로세스를 추가 하였다.

2.2 방화벽 로그분석시스템

기존의 로그분석시스템에서 가장 대표적인 보안장비인 방화벽로그분석시스템의 경우 방화벽 저장된 로그를 분석하여 보안상 문제가 될 수 있는 원인과 그에 대한 해결 방안을 제시할 수 있는 근거자료를 확보하고, 분석자료를 이용하여 체계적인 보안정책을 수립할 수 있는 기능을 수행하며 <그림 1>은 기본 구조를 나타낸 것이다 [4].

방화벽로그분석시스템의 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 구성된다.



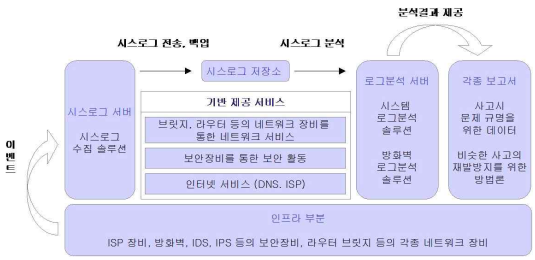
<그림 1> SILAS의 기본 구조

Ⅲ. 연구 내용

3.1 통합로그 관리 모형

SysLog[5] 장비의 에러 메시지나 보안사고시의 이벤트를 정확히 기록하여 문제발생 즉시 원인을 규명할 수 있는 근거 자료로 활용할 수 있다. 하지만 대부분의 기업에서 이러한 SysLog에 대한 관리가 제대로 이루어지지 않아 사고발생시 원인규명과 재발에 대한 대비책이 미약한 실정이다. 이렇게 SysLog의 관리가 제대로 되지 않는 이유는 일반적으로 스위치 라우터와 같은 네트워크 장비들은 저장장치 용량이 제한되어 SysLog 저장을 위한 공간적 한계를 가지며, 로그의 기록을 메모리에 함으로써 별도의 저장과정을 거치지 않고 재부팅하게 되면 모든 기록이 사라지게 된다는 기능적 한계를 가지고 있기 때문이다. 금년 4월에 발생한 농협 전산망 장애 사건에서 볼 수 있듯이 매일 발생하는 많은 량의 로그정보를 체적으로 관리하기는 쉽지 않은 일이다.

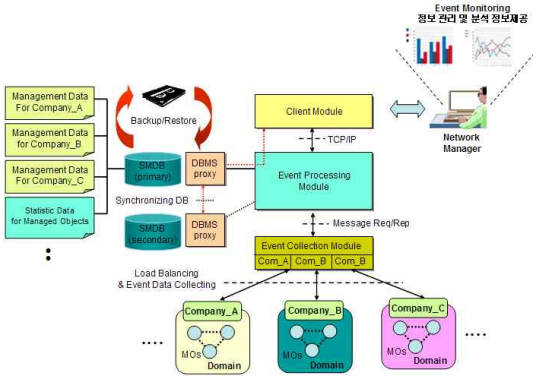
또한, 대부분의 기업에서 이러한 SysLog에 대한 관리가 제대로 이루어지지 않아 사고발생시 원인규명과 재발에 대한 대비책이 미약한 실정이다. 이렇게 SysLog의 관리가 제대로 되지 않는 이유는 일반적으로 스위치 라우터와 같은 네트워크 장비들은 저장장치 용량이 제한되어 SysLog 저장을 위한 공간적 한계를 갖고 있다. 이에 이러한 문제를 개선하기 위하여, 본 연구에서는 여러 장비의 로그를 하나의 서버로 모아서 관리하기 위한 SysLog 수집 기능과 로그 수집서버가 아닌 다른 장소에서도 로그 분석이 가능하도록 타 저장매체나 FTP로의 전송기능을 구현한 SysLog 수집 시스템을 구현에 필요한 로그정보의 수집과 대용량의 로그정보를 백업할 수 있는 통합로그수집/백업시스템을 추가한 통합 로그 관리 모형을 <그림 2>와 같이 정의하였다.



<그림 2> 통합로그관리 모형

3.2 실시간 이벤트 모니터링시스템 구조

실시간 이벤트 모니터링 시스템은 우선, 해당 관리대상 네트워크의 관리대상 시스템(MO: Managed Objects)들로부터 SNMP, LEA, Syslog로 통합 모니터링 장비에 이벤트 로그를 보내도록 설정한다.

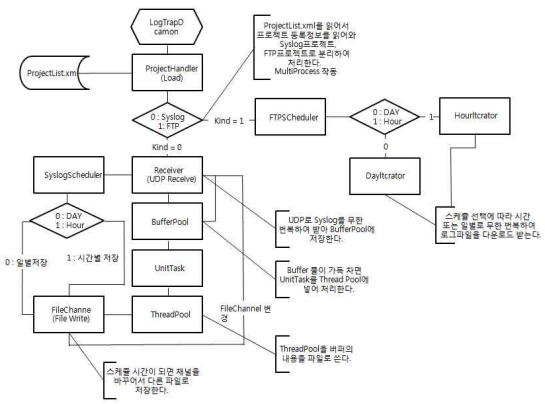


<그림 3> 실시간 이벤트모니터링 시스템 구조

연결된 서버, 네트워크 장비, 보안장비는 이상이 발생되게 되며 여러 가지 프로토콜의 형태로 모니터링 시스템으로 이벤트를 송신한다. 송신된 이벤트는 모니터링 시스템의 룰베이스 DB와 매칭하여 이상이 있는 이벤트인지를 필터링 한다. 이상이 발생되면 미리 지정된 관리자에게 경고 메시지를 SMS 또는 E-mail의 형태로 발신하게 된다. 경고를 받은 관리자는 모니터링 시스템에 웹 브라우저로 접속하여 어떤 이벤트가 발생되었는 지 확인한 후 중요 이벤트인 경우 해당 장비를 상세하게 조사하게 된다. <그림 2>는 실시간 이벤트모니터링 시스템 구조를 나타낸 것이다.

3.3 실시간 이벤트 모니터링시스템 구현

방화벽로그분석시스템(SILAS: SysLog-based Integrated Log mAanagement System)은 크게 Syslog 수집 부분과 수집된 로그를 전송하는 부분인 FTP 백업부분 구현하였으며 세부 프로그래밍 구조는 <그림 4>와 같다.

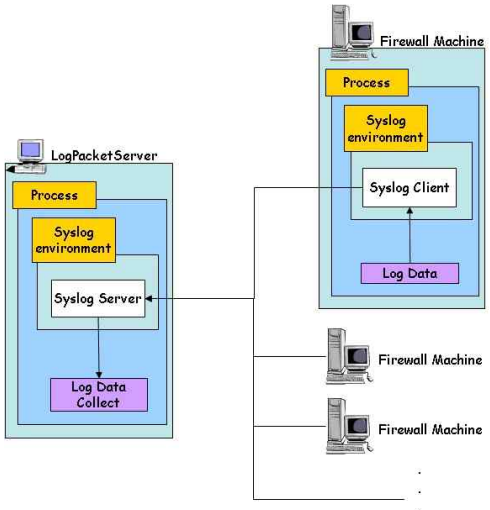


<그림 4> 프로그래밍 구조

3.3.1 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[6-8]. 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 5>는 SysLog를 이용한 방화벽 로그 수집모듈의 구조를 나타낸 것이다.



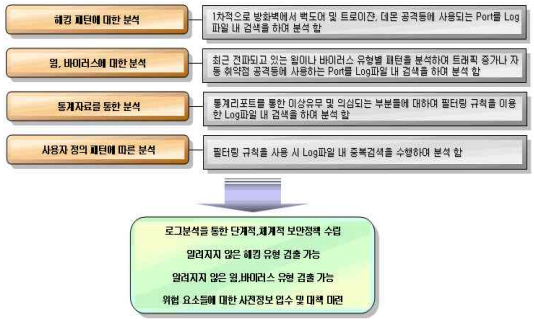
<그림 5> SysLog를 방화벽 로그 수집모듈의 구조

<그림 5>에서 보는 바와 같이 SysLog Client는 관리대상 방화벽시스템으로부터 로그데이터를 수집하고 이를 SysLog Server에게로 전송하는 기능을 수행한다.

3.3.2 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 6>은 다양한 로그패턴을 분석하는 동작 메커니즘이다.



<그림 6> 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)

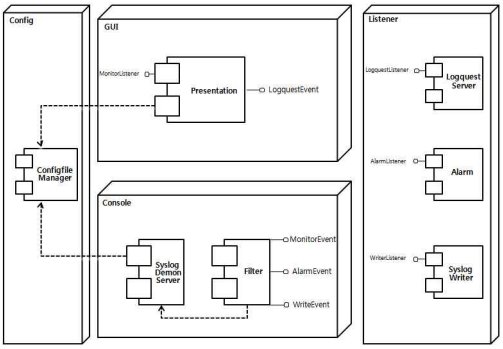
```
id=firewall time="2010-10-28 19:37:24" fw=firew4 pri=6 proto= 445/TCP
src=192.168.47.250 dst=158.216.65.1 sent=2592 msg= "ALLOW SESSION"
id=firewall time="2010-10-28 19:37:27" fw=firew4 pri=6
proto=4444/TCP src=192.168.47.250 dst=158.216.65.1 sent=2592 msg=
"ALLOW SESSION"
```

• 분석결과

```
-srcip=SRCPORT, srcport=any, dstip=DSTIP, dstport=445, action=any
-srcip=SRCPORT, srcport=any, dstip=DSTIP, dstport=4444, action=any
```

3.3.3 방화벽 로그 분석 관리 모듈

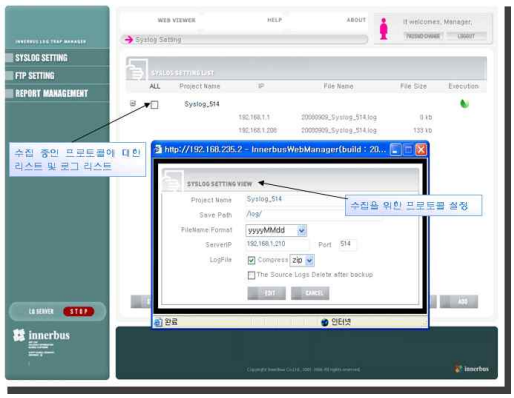
방화벽로그 분석모듈에서 수집된 SysLog를 분석한 후 결과는 방화벽로그뷰어를 통해서 제공된다. 본 논문에서 구현한 방화벽 로그뷰터는 방화벽 시스템별 상이한 로그 단일 형태로 변환하고 이를 정기적으로 침입유형별로 분



<그림 7> 방화벽로그분석시스템의 S/W구조

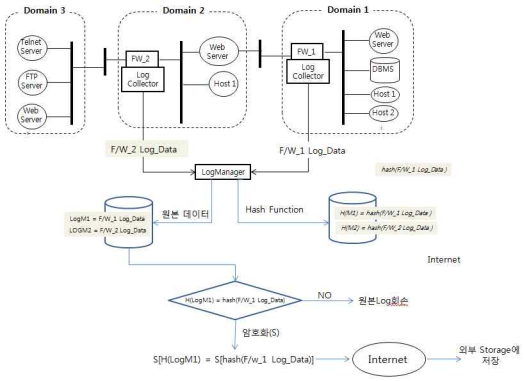
류하여 MS Word또는 Excel파일 형태로 보안관리자에게 제공하는 기능 갖는다. <그림 7>은 방화벽로그분석시스템의 S/W 모듈의 기본구조를 나타낸 것이다.

그리고, (그림 7)의 S/W구조를 기반으로 구현된 방화벽 로그뷰어(LogViewer)시스템을 나타낸 것이며, ava/xml로 개발하여 모든 플랫폼을 지원할 수 있도록 구현하였으며 <그림 8>은 방화벽로그분석시스템의 통합관리 뷰를 나타낸 것이다.



<그림 8> 방화벽 로그뷰어(LogViewer)시스템

또한, 따라서 최근의 국내 금융권의 보안사고 발생시 이를 해결하는 과정에서 로그파일의 중요성은 대두되었으나 기존의 로그분석시스템은 보안시스템들로부터 로그를 단순히 수집해서 저장하는 기능을 수행하였다. 해커들이 자신의 로그파일 기록을 삭제 및 변조하는 경우 이를 적절히 대처할 수 없는 실정이다. 이에 본 시스템은 로그파일 자체에대한 무결성을 확보하기 위해서 수집된 로그파일을 해쉬함수 H(M)를 적용하여 저장함으로써 기존 로그분석시스템의 무결성 문제를 다소 해결하였다. <그림 9>는 자체 제작한 테스트환경에서 해쉬함수를 적용한 무결성 검사를 하는 과정을 나타낸 것이다. 또한 해쉬함수를 적용한 로그값 H(M) = hash(F/W_Log_Data) 값에 암호 알고리즘을 적용 S[H(M)] = S(hash(F/W_Log_Data)한 로그파일을 외부 스토리지 장비에 저장할 수 있다.



<그림 9> 해쉬함수를 적용한 무결성 검사

Ⅳ. 결론

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

대한 무결성을 확보하기 위하여 해쉬함수를 적용하였다.

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] 인터넷침해사고 동향 및 분석 통계, 인터넷침해대응센터(http://www.krcert.or.kr/index.jsp)

[2] 정보통신부, 정부혁신지방분권위원회, 한국전산원 제정," 정보시스템 구축 운영과 관련한 기술 가이드라인 버전 1.0", 2004. 4.

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

[4] 이동영・이을석, 김진철 "SysLog기반의 통합로그관리시스템에 관한 연구," 한국정보처리학회, 학술발표논문집, 제23권, 제2호, 2011, pp. 1030-1032.

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

[6] 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.

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

[8] 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,

■ 저자소개 ■

이 동 영
Lee, Dong Young

2002년 3월~현재 명지전문대 정보통신과 부교수
2002년 2월 성균관대학교 전기전자컴퓨터공학과(공학박사)
1998년 2월 성균관대학교 정보공학과(공학석사)
1993년 2월 동아대학교 전자공학학과(공학사)

관심분야 : 네트워크관리, 정보보호, 클라우드컴퓨팅
E-mail : dylee@mjc.ac.kr

이 을 석
Lee, Eul Suk

2001년 10월~현재 (주)이너버스 대표이사
1999년 6월 한국트랜드마이크로 솔루션 개발팀장
1996년 3월 삼성전자 연구원
1996년 2월 아주대학교 전자공학과(공학사)

관심분야 : 로그분석 및 관리, 정보보호, 클라우드컴퓨팅
E-mail : uslee@innerbus.com

서 희 석
Seo, Hee Suk

2005년 3월~현재 한국기술교육대학교 컴퓨터공학부 (부교수)
2005년 2월 성균관대학교 전기전자및컴퓨터공학과 (공학박사)
2002년 2월 성균관대학교 전기전자및컴퓨터공학과 (공학석사)

관심분야 : 네트워크보안, 보안시뮬레이션, USN
E-mail : histone@kut.ac.kr

논문접수일 : 2011년 8월 20일
수 정 일 : 2011년 10월 04일(1차), 10월 16일(2차)
게재확정일 : 2011년 10월 21일