사용자별 권한이동 이벤트 모델링기반 침입탐지시스템의 체계적인 평가*

박혁장[0] 정유석 노영주 조성배

{twinkler, j8508, yjnoh, sbcho}@candy.yonsei.ac.kr

A Systematic Evaluation of Intrusion Detection System based on Modeling Privilege Change Events of Users

Hyuk-Jang Park, Yoo-suk Jung, Young-Joo Noh and Sung-Bae Cho
Computer Science Department, Yonsei University

요 약

침입탐지 시스템은 내부자의 불법적인 사용, 오용 또는 외부 침입자에 의한 중요 정보 유출 및 변경을 알아내는 것으로서 각 운영체제에서 사용자가 발생시킨 키워드, 시스템 호출, 시스템 로그, 사용시간, 네트워크 패킷 등의 분석을 통하여 침입여부를 결정한다. 본 논문에서 제안하는 침입탐지시스템은 권한 이동 관련 이벤트 추출 기법을 이용하여 사용자의 권한이 바뀌는 일정한 시점만큼 기록을 한 후 HMM모델에 적용시켜 평가한다. 기존 실험에서 보여주었던 데이터의 신뢰에 대한 단점을 보완하기 위해 다량의 정상행위 데이터와 많은 종류의 침입유형을 적용해 보았고, 그밖에 몇 가지 단점들을 수정하여 기존 모델에 비해 향상된 성능을 보이는지를 평가하였다. 실험 결과 호스트기반의 침입에 대해서 매우 좋은 탐지율을 보여 주었고 F-P error(false positive error) 또한 매우 낮은 수치를 보여 주었다.

1. 서 론

침입탐지 시스템이란 내부자의 불법적인 사용, 오용 또는 외부 침입자에 의한 중요 정보 유출 및 변경을 알아내는 것으로서 각 운영체제에서 사용자가 발생시킨 키워드, 시스템 호출, 시스템 로그, 사용시간, 네트워크 패킷 등의 분석을 통하여 침입여부를 결정한다. 요즘 사용되고 있는 대부분의 서버 컴퓨터 시스템은 시스템 내에서 발생한 행동에 관한 자세한 정보를 얻을 수 있는 C2이상의 보안 감사 프로그램을 자체적으로 지원하여 잠재적으로 보안에 영향을 주는 모든 이벤트를 기록한다. 이러한 감사 프로그램을 사용하여 사용자의 행위시퀀스를 관찰함으로써 사용자의 행위 특성을 파악할 수 있는 모델을 구축할 수 있다. 본 논문에서 제안한 침입탐지 시스템은 권한 이동 관련 정보만을 추출하는 모듈을 두어 정상으로 사용되는 권한이동을 수집한 후 HMM을 이용하여 사용자의 정상행위 모델을 구축하였다. 또한, 실험을 통하여 비정상적인 권한이동이 있을 경우 제안한 시스템이 적절히 탐지할 수 있는지 평가하는데 정확한 평가를 위해 다양한 공격을 적용시켜 보았다.

2. 관련연구

침입탐지 기술의 세계적인 현황은 아직 기술적 미성숙 상태이지만 역동적으로 다양한 실험적 제품이 개발되고 있다. 국내의 경우 대부분의 시스템들이 오용탐지 기법 중 하나인 규칙기반의 침입탐지 시스템을 개발하고 있기 때문에 새로운 침입에는 취약하다는 문제점이 있다. 미국은 수년간의 DARPA 프로젝트 수행으로 보다 우수한 침입탐지 시스템 개발을 위한 실험을 가능케 하였고, 이는 향상된 기능과 성능의 상용제품 개발로 이어지고 있다. 미국 DARPA에서는 현재 침입탐지 관련 기술의 측면에서 오용탐지와 비정상행위 탐지에 대한 연구가 계속적으로 수행되고 있고 최근에는 각 연구기관 사이의 정보 공유를 쉽게 하기 위해 Intrusion Detection Message Exchange Format(IDMEF)으로 공격행위 데이터를 표준화하거나, Traffic 발생 소프트웨어 등을 개발하여 연구자들이 새로운 DARPA 프로젝트에 참여할 필요 없이 가상의 네트워크 공간에서 발생한 데이터를 이용하여 침입탐지시스템을 평가할 수 있게 하였다[1]. 대표적인 침입탐지 시스템으로는 NIDES, EMERALD, STAT등을 들 수 있다. NIDES(Next-generation IDES)는 미국의 SRI(Stanford Research Institute) International에서 초기 연구인 IDES를 기반으로 개발한 침입탐지시스템으로 통계학적인 비정상행위 탐지 및 침입행위의 특성을 규칙으로 나타낼 수 있는 PBEST 시그네처 분석도구를 결합하여 만들었다. NIDES의 후속 시스템인 EMERALD는 네트워크 기반의 분석과 상호 연동성을 증가시키고 분산 컴퓨팅 환경으로의 통합을 편리하게 하기 위해서 만들어졌다. STAT는 침입을 상태 전이 다이어그램으로 표현하며, 전문가 시스템을 이용한 실시간 처리 시스템으로서 다중 사용자의 감사 기록 분석을 위해 규칙기반의 분석방법을 사용한다.

3. 권한 이동 이벤트를 이용한 침입탐지

선행연구에서는 대부분의 침입형태에서 보이는 권한이동에 중점을 두어 권한이동시 사용자의 행위를 추적, 수집하고 다양한 시퀀스 크기의 로그파일들을 모델링 하였다[2]. 실험결과 대부분의 침입이 일반 사용자의 정상적인 권한이동과 다르다는 것을 알 수 있었다. 본 논문에서는 기존 실험에서 보여주었던 데이터의 신뢰에 대한 단점을 보완하기 위해 보다 다양한 종류의 침입유형을 적용하여 테스트 데이터를 완성하였으며, 다수의 인원이 전문화된 작업을 하여 약 100메가의 정상행위 모델을 만들 수 있었다. 그밖에 몇 가지 단점들을 수정하여 기존 모델에 비해 향상된 성능을 보이는지를 평가하였다.

3.1 전처리 모듈

감사 자료 수집 단계에서는 침입 탐지의 근거 자료가 되는 감사 자료를 수집, 축약하는 과정을 통해 침입 여부를 판단할 수 있는 데이터를 제공한다. 가장 쉽게 이용할 수 있는 감사

*본 논문은 (주)정보보호기술의 지원에 의한 것임

자료는 시스템 로그 파일이다. 유닉스 시스템의 경우 /var/log/message나 /var/adm/ 디렉토리의 wtmp, utmp, sulog 등에서 사용자 로그 정보를 확인할 수 있다. 이와 같이 기본적인 로그 파일을 이용할 경우 특별한 작업 없이 손쉽게 감사 자료를 얻을 수 있다는 장점이 있지만 반면에 대부분의 로그파일에서는 Buffer Overflow로 인한 권한 취득의 증거를 찾기가 쉽지가 않고 침입자들이 침입에 성공한 경우 주요 로그파일에서 자신의 흔적을 손쉽게 지울 수 있다. 이러한 단점 때문에 사용되는 것이 시스템 호출(system call)레벨의 감사 자료이다[3].

본 논문에서는 호스트 안에서 발생하는 다양한 권한 이동의 정보를 추출하기 위해 SunOS의 BSM(Basic Security Module)을 사용하였다. BSM 데이터를 통하여 추출되는 막대한 양의 데이터를 이용하기 위해서는 설정파일 조정 등을 통하여 정보의 손실을 최소화시키고 탐지에 필요한 효율적인 대표 값들을 추출하는 작업이 필요하다[4]. 최근 버전인 2.7 이상의 Solaris버전에서는 BSM 데이터의 정보확장을 위해 몇 가지 감사 토큰들이 32bit에서 64bit로 확장되었다. 기존 실험환경은 Solaris 2.5.1에서만 국한되어 있었지만 확장된 환경에서 모든 버전의 Solaris를 대상으로 실험하기 위해서는 32bit와 64bit의 Audit Token을 시스템에 맞게 읽어 들일 필요가 있다. 이를 위해 전처리 부분에서 BSM 추출 모듈을 수정하였다. BSM에서 발생되는 토큰타입은 모두 81개인데 전처리 단계에서는 수집해놓은 정상행위와 침입행위 이벤트들을 분석하여 그중 호스트 침입탐지를 위해 사용되는 토큰만 재 정렬하였다.

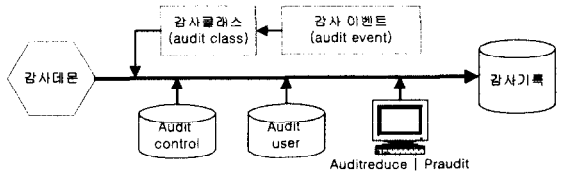

그림 1. BSM 감사기록의 생성과정

3.2 사용된 침입패턴

표 1. 침입 유형

Solaris 버전	침입 형태
2.5.1 sparc	Solaris ufsrestore vulnerability
	rpcbind file overwrite Vulnerability
	Libc (getopt() bug) stack overflow
	Eject exploit
	Passwd stack overflow
	Buffer overflow in /bin/fdformat
	CGI Exploit
2.7 sparc	OpenView xlock Heap Overflow
	Lpset -r Buffer Overflow Vulnerability
	DTMail Mail Environment Variable Buffer Overflow
	libc2_list_devices exploit
	ufsrestore Vulnerability
2.8	OpenView xlock Heap Overflow
	whodo Buffer Overflow Vulnerability
	kcms_configure KCMS_PROFILES Buffer Overflow
	mailx -F Buffer Overflow Vulnerability
	libsldap Buffer Overflow Vulnerability

기존 실험에서의 단점을 보완하기 위해 이미 DARPA 프로젝트에서 사용되어진 침입과 그 외 다양한 침입패턴들을 적용 시켜보았는데 대표적인 침입유형으로는 버퍼 오버플로우(Buffer Overflow), 레이싱 컨디션, CGI 취약점을 이용한 침입이다. 대부분의 호스트기반 침입은 일반 사용자에서 루트로 권한을 옮기는 U2R형태의 침입이고 BSM을 통한 네트워크로부터의 침입탐지 가능성을 알아보기 위해 R2U 침입형태도 시도하여 보았다. 또한 Solaris의 다양한 버전에 대해 평가를 하기 위해 모두 4개의 호스트에서 Test 데이타를 수집하였다.

3.3 권한 이동 탐지 모듈

일반적으로 보안에 관련되어 파일의 권한이 문제가 되는 경우는 대부분 파일을 실행할 때이다. SETUID로 설정된 실행 파일은 프로그램이 실행중일 때만 다른 사용자의 권한을 지니므로 다른 작업은 수행하지 못하고 해당 프로그램이 제공하는 기능만 수행할 수 있지만 프로그램이 정상적으로 동작하지 않고 다른 작업을 수행한다면 큰 문제가 발생할 수 있다. 대부분의 침입은 SETUID로 설정된 이러한 파일의 버그를 이용하여 권한을 획득하게 된다. 그림 2는 fdformat 버퍼 오버플로우를 이용한 공격 시 권한 이동의 예를 보여 준다.

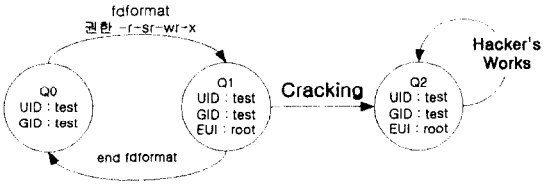

그림 2. 버퍼 오버플로우 공격시 권한이동 예

이외에도 유닉스의 파일 시스템 보안과 관련하여 허점을 가지고 있는 것으로는 링크(symlink) 메커니즘을 들 수 있다. 이렇듯 SETUID나 Symblic Link등을 통하여 잠시 바뀌는 권한 이동 전의 행동들은 정상행위와 비정상 행위를 구분하는 중요한 시점이 되는데, 권한 이동을 탐지하기 위해서는 BSM Audit Data를 통하여 정상적인 권한이동에 쓰이는 정보들을 현재 시점으로부터 과거 일정한 기간동안 기록하여 저장하고 있어야 한다.

제안한 권한 이동 모듈은 BSM 데이터에서 발생되는 EUID와 UID가 변경되었을 경우 그 시점을 기준으로 전에 사용되었던 일정양의 데이터 시퀀스를 가지고 평가를 하게 된다. 하지만 수집한 공격행위 분석 시 사용자의 변화뿐만 아니라 때로는 그룹 사용자가 변화하여 시스템을 침범 후 관리자 권한을 획득하는 경우가 있다. 이를 위해 본 시스템에서는 사용자와 그룹 모두의 권한이동을 탐지하였다.

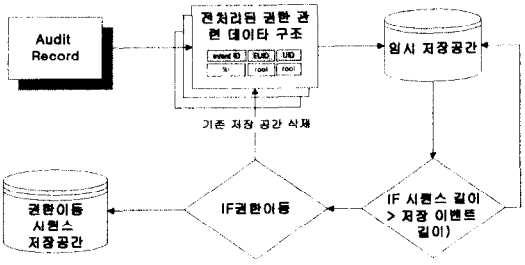

그림 3. 권한이동 침입시스템 구조

3.4 HMM를 통한 모델링

정상행위 평가는 이미 구축되어 있는 정상행위 모델에 사용자행위 시퀀스를 HMM 입력으로 넣어 각 정상행위에서 현재 행위가 생성되었을 확률을 계산한다[2]. 이때 심볼의 크기가 크

기 때문에 평가에 따른 확률 값이 매우 낮아지는 단점이 있다. 이를 위해 결과 값에 로그를 취하는 방식을 사용하였다. 정상행위 평가에 의해 수치화된 평가 값은 현재 행위가 기준이 되는 모델, 즉 정상행위로부터 생성되었는지를 나타내는 확률 값으로 다른 평가 값과의 산술적인 직접비교가 가능하다. 따라서 정상행위로 볼 수 있는 가장 낮은 임계값을 결정하고, 현재 행위의 평가 값을 임계값과 산술 비교하여 더 낮으면 현재 행위를 비정상행위로 판정한다.

4. 실험 및 결과

실험을 위해 10명의 사용자가 참여를 하였으며, 정상행위의 경우 한 달에 걸쳐 8명의 사용자가 일정한 패턴을 가지고 수집하였다. 주로 사용된 프로그램은 Mail Server, 홈페이지 접속, 유닉스 명령어 실행, FTP 데이터 전송 등이다. 다양한 상황 구성을 위해 매번 다른 방법으로 프로그램을 실행시켰으며 총 수집된 데이터는 90메가바이트이다. 시스템 호출의 개수는 767,237 개로 기존 정상행위 데이터에 비해 약 20배 이상 늘어났다. 테스트에서는 6명의 사용자가 참가하였으며, 그 중 3명이 각 Exploit에 대해서 2~3번씩 침입을 시도하였다. 사용된 침입은 총 17개, 시도된 침입은 50차례이며 다양한 Solaris버전에서 실험되었다. 침입에 사용된 호스트는 표2와 같다.

표 2. 운영체제 분류

장비명	운영체제 버전	플랫폼
Ultra sparc 1	Solaris 2.5.1	sparc
Ultra sparc 10	Solaris 2.7	sparc
PC	Solaris 2.8	intel
Ultra-Enterprise	Solaris 2.5.1	sparc

HMM를 통한 모델링시 최적의 성능을 보일 수 있는 매개변수를 결정하기 위해 상태는 3~15, 시퀀스는 15~50사이를 설정하였다. 실험결과 기존 실험과 비슷하게 상태 5~7, 시퀀스 25~30정도에서 최적의 성능을 나타냈고 HMM 판정 모듈을 통해 나온 정상행위 시퀀스 값은 평균 -58.2정도였으며 임계값은 약 -66.8이었다. 그림 4는 상태 5, 시퀀스 27에서 발생된 평가 값들의 빈도수를 보여준다. 테스트 시 침입을 시도한 시간에서는 약 -69의 평가 값이 나오기 때문에 편차가 심함을 알 수 있었다.

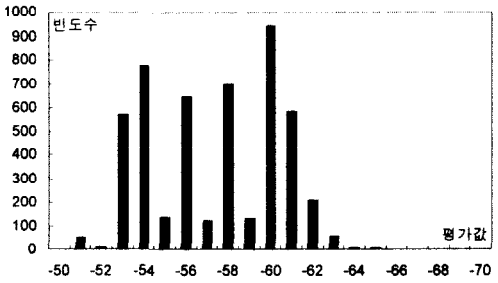

그림 4. 권한 이동 평가값 빈도수

표 3은 각각의 테스트에서 상태와 시퀀스에 따른 최적의 실험 결과를 보여주는데 2.5.1 버전에서 사용된 침입은 모두 탐지를 하였고 F-P error 또한 매우 낮은 수치를 보여주었다. 하지만 2.8 버전의 경우 실험에서 사용된 많은 행위들이 윈도우 환경(CDE)에서 발생하였기 때문에 수집된 정상행위와는 많은 차이점을 보였고 따라서 높은 F-P 오류가 나왔다. 이 문제를 해결하기 위해서는 버전별 정상행위를 따로 모아야 할 것으로 사료된다. 또한 2.5.1에서 CGI 버그를 통한 내부 프로세스 사용을 탐지해보았지만 탐지가 불가능함을 알 수 있었다. 이 문제는 외부의 접속 또한 Nobody라는 계정으로 작업을 하기 때문에 권한이동이 일어나지 않아 탐지를 못하는 것으로 추정된다.

표 3. F-P error를 이용한 침입탐지시스템 성능비교

운영체제	상태/시퀀스	HMM 임계값	침입횟수/유형	탐지율	F-P error
2.5.1	5/27	-66.8	10/local	100%	1.049%
2.5.1	5/25	-63.5	8/local	100%	1.079%
2.5.1	5/25	-66.8	3/remote	0%	100%
2.7	5/27	-68.6	20/local	100%	2.14%
2.8	7/27	-71.6	8/local	100%	23.478%

그림 5는 각각의 운영체제에서 실험한 데이터의 탐지율과 F-P 오류를 보여주고 있다.

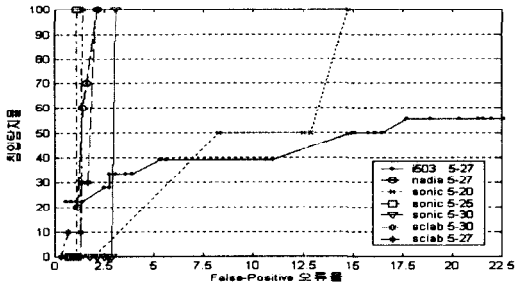

그림 5. 권한 이동 관련 침입 탐지율

5. 결론 및 향후연구

본 논문에서는 기존 실험에 비해 다양한 침입패턴과 고용량의 데이터를 이용하여 평가를 해보았다. 실험결과 매우 좋은 성능을 보여 주었지만 보다 정확한 탐지를 위해서는 모델링 문제뿐만 아니라 감사수집단계에서의 설정 또한 매우 중요하다. BSM 데이터 분석결과 감사 설정에 따라 임계값의 편차가 매우 다양화되는 것을 알 수 있었는데 이를 해결하기 위해서 다량의 정상행위를 수집, 분석하여 최적의 이벤트들이 무엇인지를 파악해야 할 것이며, 여러 종류의 침입패턴을 수집 후 침입의 시도 시에 발생하는 증거물들을 분석할 필요가 있다. BSM의 경우 로그파일 생성시 감사적용 대상 범위와 커널레벨과 사용자레벨의 감사이벤트들을 설정할 수 있다. 이러한 설정을 얼마나 적절히 설정하느냐에 따라 침입을 탐지하기 위한 최적을 환경을 만들 수 있을 것이다. 차후 시스템에서 이러한 평가 작업들을 적용할 경우 보다 좋은 탐지율을 얻을 수 있을 것이다.

6. 참고 문헌

[1] J.W. Haines, L.M. Rossey, and R.P. Lippmmann, "Extending the DARPA off-line intrusion detection evaluations," *DISCEX '01. Proceedings*, pp. 35-45, 2001

[2] 박혁장, 정유석, 조성배, "권한 이동 이벤트를 이용한 은닉 마르코프 모델 기반 침입탐지 시스템," *정보과학회*, 제28권 1호, pp 769-771, 2001.

[3] D. Endler, "Intrusion detection: Applying machine learning to Solaris audit data," *Proces of Computer Security Applications Conference*, pp 268-279, 1998.

[4] M. Schonlau, and M. Theus, "Detecting masquerades in intrusion detection based on unpopular commands," *Information Processing Letters*, pp 33-38, November 2000.