전산망 사건을 이용한 침입 감지 및 감사 추적 시스템 설계

김 기 중[†] · 윤 상 훈[†] · 이 용 준[††] · 류 근 호[†††]

요 약

정보 산업의 급속한 발전에 따라, 컴퓨터 통신망을 통한 자료의 위협 및 손실에 대처하기 위한 방법중에 하나로서 현재 방호벽 시스템에 대한 연구가 활발히 진행되고 있다. 따라서, 이 논문에서는 효율적인 전산망 보호를 위하여 방호벽 시스템과 전산망 감사 추적 시스템과의 연계성을 통하여 전산망에 대한 위협 및 손실을 줄일 수 있는 방법 및 문제 발생시 사후 조치할수 있는 시스템 모델을 제시하고자 한다. 또한, 감사 자료 분석을 위하여 감사 분석기에서 사용되는 데이터베이스의 유형과 감사 분석기의 실행 모델을 제시한다. 전산망 감사 추적 시스템은 불법 침입자에 대한 모든 활동을 감시함으로서, 침입 유형을 식별하고, 감사 자료를 분석하는 기능을 갖는다.

Design of Intrusion Detection and Audit Trail System using Network Events

Ki Jung Kim[†] · Sang Hun Yun[†] · Yong Jun Lee[††] · Keun Ho Ryu[†††]

ABSTRACT

According to the outstanding development of information industry, a study of firewall is progressing as one of methods to cope with threat and loss of the data through computer network. For the secure network, this paper proposes the method diminishing threat and loss of the network using the correlation firewall with network audit trail system. Also, this paper suggests not only the audit analyzer execution model but also the type of databases used in audit analyzer to analyze the audit data. Network audit trail system has the function of identifing and analyzing of all intruder actions using audit records created by users.

1. 서 론

정보 산업의 급속한 발전으로 컴퓨터 시스템의 사용이 급격히 증가하고 있다. 이에 따라 사용자들은 전산망을 통한 정보 처리의 편의성을 누리는 반면 사용자 및 컴퓨터 시스템은 정보 보호상의 다양한 문제에 처하고 있다. 컴퓨터 통신망을 통한 해커등의 침입으로 시스템의 자원 및 중요한 자료들이 위협당하고 있으며 때로는 치명적인 손실을 입기도 한다. 따라서 전산망 시스템의 안정성 및 신뢰성을 확보하는 것을 목적으로하는 전산망 보안은 고도 정보화 사회의 필수 조건이다[1, 14, 16]. 전산망 보안에 대한 위협에 대처하기 위한 정보 보호 서비스의 필요성 또한

※이 연구는 1997년도 한국전자통신연구원의 연구비 지원으로 수행되었음
† 준 회 원:충북대학교 전자계산학과
†† 정 회 원:한국전자통신연구원 책임연구원
††† 종신회원:충북대학교 전자계산학과
논문접수:1997년 1월 6일, 심사완료:1997년 5월 29일

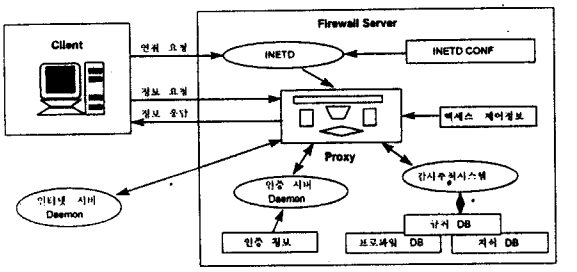
급격히 증가하고 있으며, 침입자의 방지책을 위한 방호벽 구축과 침입자나 허가받지 않은 사용자들을 추적하기 위한 감사 추적 서비스는 전산망에서 필수적인 서비스 중의 하나이다[10].

감사 추적을 위해서는 사용자에 의해 발생되는 각 사건을 기록하고 필요시 언제, 누가, 어떤 일을 수행했는지 추적할 수 있어야 한다. 또한 불법 침입을 예방하거나 침입시 그 사실을 감지하여 손실을 최소화하기 위해서는 시스템 내의 모든 활동들을 면밀히 조사 분석 해야 한다. 그러나 시스템 내에서 발생하는 사건 자료는 막대한 양이어서 수작업에 의한 자료의 수집 및 분석은 불가능하며 감사 자료를 필터링등의 방법으로 축소하여 자료의 저장 및 분석에 따른 오버헤드를 최소화시킬 필요가 있다. 최근 이에 대한 다양한 기법 및 모델들이 개발되어 왔으나 컴퓨터 통신망의 복잡성, 목적 시스템의 원초적 취약성, 정보 보호에 대한 이해 부족 및 불법적인 침입 기법들의 개발등으로 기존의 어떤 기법 또는 모델도 완전하지 못한 실정이다[8]. 전산망 시스템은 사용자의 신분 인증, 정보에 대한 접근 제어, 송수신 사실에 대한 부인 봉쇄, 저장 또는 전송 정보에 대한 비밀성과 무결성등 전산망 보안 기술과 더불어 모든 환경을 저장하여 향후 발생될 수 있는 분쟁에 대한 증빙 자료를 제시할 수 있는 전산망 감사 추적이 요구된다. 이러한 전산망 감사 추적은 다양하며 많은 자료가 시간적으로 계속하여 발생되기 때문에 다양한 형태의 정보들을 시간 정보와 함께 처리하여 효율적으로 저장 관리할수 있는 감사 추적 관리 시스템의 연구 개발이 필수적으로 요구된다[13]. 따라서 이 연구에서는 시간 정보와 함께 불법적인 침입자를 찾아 사후 조치와 아울러 분석 기능을 갖는 전산망 감사 추적 시스템 모델을 제시한다. 전산망 감사 추적 시스템은 전산망에서 발생된 감사 레코드를 바탕으로 사건 분류기, 감사 기록기, 감사 분석기, 그리고 감사 제공기등으로 구성되며, 감사 추적 시스템에서 사용되는 각종 데이터베이스의 제시와 감사 분석 실행 모델을 이 연구에서 제시하도록 한다.

2. 감사 추적 시스템과 방호벽 시스템과의 관계

2.1 감사 추적 시스템

전산망에서 감사 추적 시스템은 방호벽 시스템과 함께 위치하여 불법적인 침입자를 감지하는 역할을 한다. 그림 1은 이 연구에서 설계된 감사 추적 시스템과 방호벽 시스템과의 관계를 보여준다. 즉, 외부 전산망과 내부 전산망 사이에 외부로부터 사용자가 서비스 요청시 이에 대한 접근을 패킷 필터링을 통해 접근 통제할수있는 방호벽 시스템이 위치하고, 내부 전산망 서비스 요청을 감사 자료로 활용할 수 있는 감사 추적 시스템이 위치한다.



(그림 1) 전산망 감사 추적 시스템
(Fig. 1) Network audit trail system

전산망에 대한 감사 추적 시스템은 전산망에서 외부 사용자가 내부 전산망에 위치하는 UNIX 시스템에 의해 제공되는 서비스 요청시 이에 대한 요청 자료를 감사 자료로 활용하며, 시스템 문제 발생시 이를 해결할 수 있는 시스템이다. 감사 추적 시스템에서 활용될 수 있는 감사 자료로는 허가된 접근뿐만 아니라, 거절된 접근까지도 감사 정보에 포함된다[4, 8, 9, 11]. 이와 같은 감사 추적 시스템은 베스천 호스트, 이중 게이트웨이, 스크린드 호스트 게이트웨이, 응용 레벨 게이트웨이등의 4가지 방식으로 구성되는 방호벽 시스템에 확장하여 운영이 될 수 있다[12, 15].

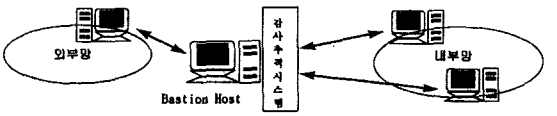
2.2. 방호벽 시스템과 연계성

방호벽 시스템은 외부 전산망과의 연결에 따르는 내부 전산망의 위험을 줄이고 보안 정책이 기본이 되어 외부 전산망과 내부망간의 보안 기능을 수행하는 시스템으로 외부 전산망 침입자로 부터 내부 전산망을 보호하고자 하는데 있다[11, 15]. 전산망 보호 기술의 한 분야로 내부 전산망과 외부 전산망 사이에 위치하여 사용자의 패킷을 필터링 하는 기능을 가진 방

호벽 시스템은 내부 전산망 보호를 위한 설계라고 정의할 수 있으며, 방호벽 시스템과 전산망 감사 추적 시스템과의 구성은 다음과 같다.

가. 베스천 호스트와 감사 추적 시스템

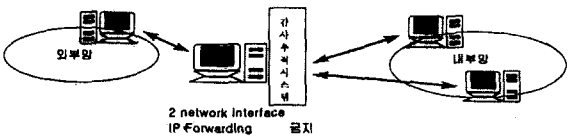
베스천 호스트는 전산망 보안의 중요한 부분으로 방호벽 관리자가 지정한 UNIX 시스템이다. 일반적으로 베스천 호스트는 보안을 위해서 특별히 주의가 필요하며, 내부 전산망으로 침입할 수 있는 영역으로 베스천 호스트를 경유하게 함으로서 위험 영역을 한정시키는 역할을 한다. 베스천 호스트는 높은 보안 상태를 유지하면서 감사 기능, 추적 기능을 가지고 있고 그림 2에서 보여주는 바와같이 2개의 패킷 필터링 라우터를 가지고 구현된다. 특징으로는 철저한 방어기능이 구현되는 시스템이며, 외부 전산망에서 내부 전산망으로의 처음 접속과 인증 부분, 외부의 침입자가 주로 노리는 시스템, 대용량의 로그 및 모니터링 그리고 비용이 많이 든다는 특징이 있다.



(그림 2) 베스천 호스트의 전산망 감사 추적
(Fig. 2) Network audit trail in Bastion host

나. 이중 게이트웨이와 감사 추적 시스템

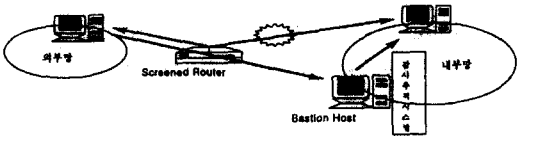
스크리닝 라우터없이 내부망과 외부망 사이에 시스템을 놓고 시스템의 TCP/IP forwarding 기능을 막음으로서 구현되는 방호벽 시스템이다. 일반적으로 내부망과 외부망 사이에 두개의 인터페이스를 가지고 있어 망 사이의 직접적인 트래픽은 불가능하다. 이 방식과 결합된 감사 추적 시스템의 구성은 그림 3에서 보여주는것과 같이 구성할수 있다.



(그림 3) 이중 게이트웨이의 전산망 감사 추적
(Fig. 3) Network audit trail in Dual homed gateway

다. 스크린드 호스트 게이트웨이와 감사 추적 시스템

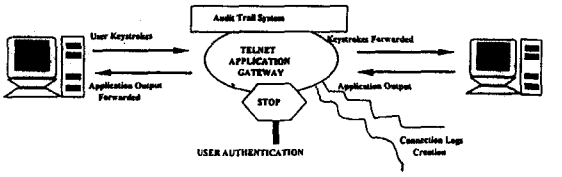
현재 가장 많이 사용하는 시스템으로 스크리닝 라우터와 베스천 호스트를 이용하여 구성되는 방호벽 시스템으로서 스크리닝 라우터와 베스천 호스트가 갖는 문제점을 해결할 수 있다. 이 시스템에서 베스천 호스트는 그림 4와 같이 내부 전산망의 안전한 곳에 위치하고, 스크리닝 라우터는 외부 전산망에서 접근 가능한 유일한 통로로 베스천 호스트를 지정한다.



(그림 4) 스크린드 호스트 게이트웨이의 전산망 감사 추적
(Fig. 4) Network audit trail in Screened host gateway

라. 응용레벨 게이트웨이(프럭시 게이트웨이)와 감사 추적 시스템

대부분의 인터넷상의 소프트웨어들은 자료를 모았다가 전달하는 방식으로 수행이 되는데 방호벽 시스템에서 동작하는 이러한 전달 서비스는 보안이 아주 중요시된다. 일반적으로 응용레벨 게이트웨이는 주로 방호벽을 가로질러 전달하는 종류(Telnet, FTP, Sendmail, www, …)를 말하며, 보안 관계의 잠재적인 가능성이 있으며 베스천 호스트에서 운영된다. 이 구성 방식에서는 응용 레벨에 위치하는 Telnet, FTP, mail, WWW 응용 게이트웨이에서 보안 정책에 따라 외부 전산망에서 연결 서비스를 요청하는 사용자의 감사 자료를 생성하고 관리한다. 그림 5는 이 시스템과 감사 추적 시스템과의 연동 구성을 보여준다.



(그림 5) 응용레벨 게이트웨이의 전산망 감사 추적
(Fig. 5) Network audit trail in Application gateway

3. 전산망 감사 추적 시스템 구조

전산망 감사 추적을 수행하기 위한 감사 추적 시스템은 사건 분류기, 감사 기록기, 감사 분석기, 감사 제공기등으로 구성된다. 사건 분류기는 전산망으로부터 가공되지 않은 데이터를 감사 분석기에서 필요로 하는 일정한 형태의 감사 자료로 변화시켜주며, 감사 기록기는 사건 분류기로부터 전달받은 감사 자료를 데이터베이스로 저장하는 기능을 수행한다. 그리고 감사 분석기는 사용자에 의해서 발생된 감사 자료를 통계적인 이상 상태 감지 기법 및 규칙 기반 침입 감지 기법을 이용하여 사용자의 행동이 정상적인 행동인지, 비정상적인 행동인지를 판단한다. 감사 제공기는 감사 분석기로부터 생성된 데이터베이스를 토대로 시스템의 이상 상태를 감사 서비스 요구자에게 서비스를 제공한다. 이 장에서는 감사 추적을 위한 기존의 기법을 분석하고 감사 추적 시스템을 제시한다.

3.1 감사 추적 기법

감사 추적을 위해 침입자의 공격을 감지하기 위한 침입 감지 기법들은 통계적 이상 상태 감지 기법, 규칙 기반 기법, 신경 회로망 기법, 지문 비교 침입 감지 기법 및 신경 회로망-지식 기반 융합 모델등이 있다 [11]. 이 절에서는 이들 기법들을 소개하고 각 기법들의 특성 및 문제점을 기술한다.

가. 통계적 이상 상태 감지 기법

통계적 이상 상태 감지 기법은 침입 방법의 통계적 특성을 쉽고 효율적으로 적용할 수 있기 때문에 많은 침입 감지 시스템에 적용되고 있다. 이 기법은 기본적으로 시스템이 생성한 감사 자료의 양적 및 유형적 변화를 측정하기 위하여 통계적 분석 방법을 사용하며 감사 자료의 분석은 개별 사용자의 감사 추적 또는 목적 시스템의 모든 감사 자료에 적용된다. 통계적 이상 상태 감지 기법은 임계치 감지와 프로파일 기반 기법으로 분류된다. 이 기법들의 공통적인 문제점은 정상 상태의 개념이 시간 변화에 따라 달라질 수 있으며 또한 시간대별로 다른 의미를 갖기 때문에 정상 상태의 기준 설정이 어렵다는 단점이 있다.

나. 규칙 기반 기법

규칙 기반 침입 감지 기법은 시스템상의 활동을 관찰하여 정상적인 패턴인지의 여부를 구분하는 규칙들의 집합으로 구성되며, 감사 자료의 분석을 통한 자동 규칙 생성 및 귀납 추리에 기초한 규칙 기반 이상상태 감지 기법과 전문가 시스템에 기초하여 자동 생성되지 않고 전문가에 의해 생성되는 규칙 기반 침입 감지 기법이 있다.

다. 신경 회로망 기법

신경 회로망은 상호 연결된 뉴런으로 구성된다. 각 뉴런은 연결상의 가중치를 통하여 다른 뉴런으로부터 입력을 받아 자체의 출력 값을 생성한다. 연결 가중치는 연결된 뉴런 사이의 활동 레벨 간의 상호 관계의 정도를 나타낸다. 따라서 가중치가 변함에 따라 각 뉴런의 그리고 전체 신경 회로망의 입력 처리 결과가 달라진다. 이와 같은 신경 회로망은 주어진 입력 자료 집단의 학습 패턴을 이용하여 지속적으로 가중치를 조절하는 알고리즘을 이용하여 학습할 수 있으며 전형적인 패턴 분류기로써 이용된다. 신경 회로망 기법의 예는 침입 감지 시스템의 한 요소로 사용되며 신경 회로망 요소와 전문가 시스템 요소로 구성되며 신경 회로망은 통계적인 자료 분석 단계를 담당하고, 전문가 시스템은 신경 회로망의 결과를 분석하고 침입 감지를 위한 형태로 변형시킨다.

라. 지문 비교 침입 감지 기법

지문 비교 침입 감지 기법은 복잡한 컴퓨터 네트워크 상에서의 침입 감지를 위한 기법으로 기존의 기법과는 달리 과거의 감사 기록에는 의존하지 않는다. 이 기법의 기본 개념은 연결 체인상의 다른 두 노드에서의 연결 활동 내용 즉, 지문은 동일하기 때문에 연결 체인의 시작을 찾을 수 있다는 개념을 이용한 기법이다. 즉, 어떤 사용자가 사용한 UNIX의 ls 명령은 연결 체인상의 모든 노드를 통과하며 동일하다는 것이다. 실제로 이 기법에서 지문은 사용자의 모든 명령을 이용하지 않고 자료의 체크섬과 같이 일정 시간 간격을 두고 채취되기 때문에 비교될 지문의 자료가 크지 않다는 장점이 있다.

마. 신경 회로망-지식 기반 융합 모델

이 모델은 신경 회로망 패턴 인식 모델과 인공 지

능 패턴 인식 모델을 융합한 새로운 모델로서 기존의 패턴 인식 모델 중의 하나인 신경 회로망 패턴 인식이 갖는 학습시 주어진 과거 감사 자료의 패턴에 근거하여 정상, 또는 비정상 사용자를 분류해 내며 왜 그러한 결과가 도출되었는지에 대한 해설 방법이 없는 단점을 극복할 수 있다. 이 모델은 패턴을 인식할 때 각 단계에서 생기는 다양성, 애매성등을 다른 층의 지식을 이용하여 협조적으로 해결하며, 또한 인간처럼 직감적 처리와 논리적 처리를 상호 협조적으로 정보를 교환하여 패턴을 인식한다. 이 모델의 구조는 신경망을 이용한 표현 영역과, 지식 기반을 이용한 개념 영역의 두 영역으로 구성이 되며, 표현 영역과 개념 영역은 각각 여러개의 층으로 이루어진다.

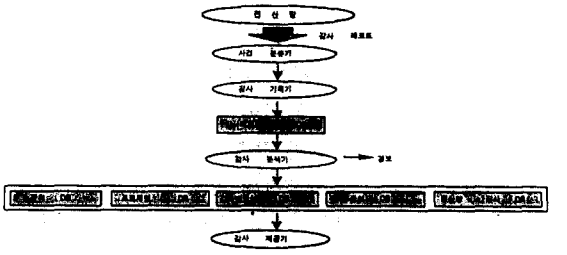
3.2. 감사 추적 자료 분류

전산망의 감사 추적은 전산망에서 외부 사용자에 의해 요청되는 각종 서비스 기능이 수행될 때 공격자의 분석 및 저해 요인에 대한 제어 절차 개발과 설정된 보호 정책을 허용하며 시스템 제어에서 부적절성을 지적할 수 있는 정보를 보고하고 제어, 정책, 절차상에서 요구된 변경 사항을 저장하도록 해야 한다. 전산망 보호와 관련된 사건은 감사의 대상 자료가 될 수 있는데, 감사 자료의 종류는 크게 두 가지로 분류된다[3, 8].

- 전산망 보안에 관련된 감사 자료
  - 시스템과 시스템들 사이의 접속
  - 시스템에 요청된 서비스 종류 (Ftp, Rlogin, Telnet ,..... 등).
  - 전산망에서의 Traffic 양.

- 시스템 보안에 관련된 감사 자료
  - 시스템 자원에 관련된 감사 자료(CPU 사용량,I/O 장치 사용량등).
  - 사용자 로그인 실패 횟수.
  - 사용자 패스워드 실패 횟수.
  - 파일 시스템에 관련된 감사 자료(Read, Write, Delete, Create, Append등).
  - 시스템 파일에 관련된 감사 자료.
  - 한 세션 안의 사용자의 지속 시간.
  - 한 세션 안의 사용자의 출력 데이터의 종류 및 양.

이러한 감사 자료를 바탕으로 감사 추적 기법을 이용, 사용자의 행동 패턴 분석을 통하여 시스템 사용에 대한 감사 추적을 수행할 수 있다. 전산망에서 감사 추적을 위하여 제시된 감사 추적 시스템 모델은 그림 6과 같다.



(그림 6) 전산망 감사 추적 시스템 모델
(Fig. 6) Network audit trail system model

3.3 감사 추적 모듈 기능

가. 사건분류기

사건 분류기에서 실행될 수 있는 일반적인 기능으로는 외부로부터 사용자가 내부 시스템에 접근하여 시스템 자원을 사용한후에 최종적으로 시스템을 빠져나가는 시간까지 사용자에 대한 흔적을 감시하여 감사 자료를 생성한다. 이러한 감사 자료는 UNIX Audit System이 사용하는 시스템 파일인 /var/adm/lastlog, /var/adm/acct, /var/adm/ wtmp, /etc/utmp와 방호벽 시스템이 관리하는 각 프럭시 서버의 로그 정보로부터 생성되는데, 이들 감사 자료는 감사 분석기에서 사용하는 형태인 다음과 같은 6개의 감사 자료 항목으로 정의한다[6, 7, 8, 11].

〈시스템 사용자(subject), 행동(Action), 시스템 자원(Object), 예외 조건(Excepti on-condition), 시스템 자원 사용량(Quantity), 행동 시간(Time)〉

- 시스템 사용자 : 시스템에서 서비스를 요청하고 수행하는 사용자이다.
- 행동(Action) : 사용자가 시스템 자원을 사용하기 위한 수단으로 Login, Logout, Read, Write, Execute, Telnet, Ftp등이다.
- 시스템 자원 : 사용자가 행동을 하는데 있어서 수반되는 시스템 자원이다.

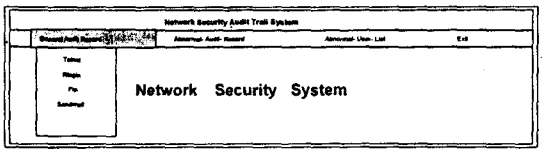
· 에러 조건:시스템 자원 요청 및 명령어 실행 결과에 대한 상태값.
· 시스템 자원 사용량:사용자에 의해서 사용된 시스템 자원 사용량으로 사용된 CPU시간, I/O 단위 시간, 세션의 지속 시간, 읽고 쓰여진 레코드 수, 프린트된 페이지 수 등이 된다.
· 행동 시간:사용자에 의해서 행동이 일어난 시간이다.

나. 감사 기록기

감사 기록기는 전산망에서 감사 자료를 수집하는 사건 분류기로부터 분류된 감사 자료를 파라미터로 입력받아 데이터베이스 관리시스템(DBMS)을 이용하여 감사 레코드 데이터베이스를 생성, 감사 자료를 저장한다.

다. 감사 분석기

감사 분석기는 사건 분류기에 의해서 생성된 감사 자료의 조사, 평가, 분석을 통해 시스템 사용에 대한 위협 요소를 식별하고 불법 침입자를 감지하여 시스템 관리자에게 보고함으로서 시스템 위협에 대하여 능동적으로 대처할 수 있는 기능을 제공한다. 또한 시스템이 가지고 있는 보안 취약점을 제거함으로서, 외부 사용자로부터 발생할 수 있는 공격에 대하여 시스템을 안전하게 관리할 수 있다. 감사 분석기는 분석 데이터베이스 갱신기, 비정상 탐지기, 프로파일 갱신기, 규칙 생성기등의 프로세스 부분과 감사 레코드 데이터베이스, 분석 데이터베이스, 전산망 감사 데이터베이스, 비정상 데이터베이스, 프로파일 데이터베이스, 규칙 데이터베이스등의 데이터베이스 부분으로 구성이 된다.



(그림 7) 전산망 감사 추적 시스템 사용자 인터페이스
(Fig. 7) Network audit trail system user interface

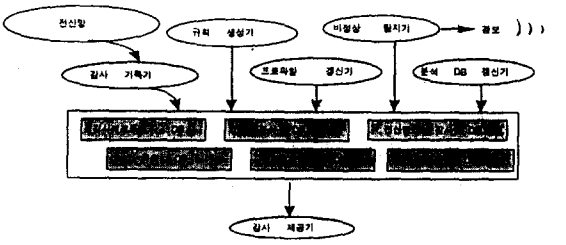
라. 감사 제공기

감사 제공기는 그림 7과 같이 윈도우 환경 사용자 인터페이스로 제공이되며, 감사자로부터 감사 서비스 요청시 감사 분석기에 의해서 현재까지 수행된 감사 결과 및 감사 자료, 비정상적인 사용자에 대한 감사 자료를 제공하는 역할을 한다.

4. 감사 분석기 실행 모델

4.1. 감사 분석기 모델

감사 분석기는 감사 기록기를 통해 구축된 감사 자료의 기록을 조사, 평가, 분석한다. 그리고 분석 결과를 이용하여 각종 보안 위배와 불법 침입자를 감지하고 분석 결과 및 침입 감지 내용을 감사자에게 보고함으로서 침입자에 대해 능동적으로 대처하게 하여 사전에 보안 사고 예방 및 취약점등을 제거하여 전산망에서 시스템의 효율적인 운영을 도모한다. 이러한 감사 분석기 모델은 그림 8과 같다.



(그림 8) 감사 분석기 모델
(Fig. 8) Audit analyzer model

4.2. 감사 분석기 프로세서

가. 분석 데이터베이스 갱신기

분석 데이터베이스 갱신기는 감사 기록기에 의해 감사 레코드 데이터베이스에 저장된 감사 자료중에서 사용자별, 시스템 자원 종류 그리고 사용자가 목적 시스템에 요청한 서비스 종류에 따라서 주기적으로 분석 데이터베이스로 감사 자료를 갱신하는 역할을 한다. 분석 데이터베이스를 갱신하면서 감사 자료 종류에 따라 사건을 발생시키는데, 로그인에 관련된 감사 자료인 경우 Login 사건을, 시스템에 로그인한 후 활동에 대한 감사 자료인 경우 Activity 사건을, 로

그아웃에 관련된 감사 자료인 경우 Logout 사건을 발생시킨다.

나. 비정상 탐지기

비정상 탐지기는 분석 데이터베이스에서 발생한 Login, Activity, Logout 사건을 감지한후 분석 데이터베이스에 저장된 감사 자료에 대해서 비교, 분석 기능을 수행하여 감사 자료의 이상 유무를 판단한다. 이때 사용자의 시스템 사용 패턴을 정의한 프로파일 데이터베이스와 과거의 시스템 침입 패턴, 시스템 보안 정책 및 관리 사항들에 대한 휴리스틱 규칙을 갖는 규칙 데이터베이스를 이용한다.

다. 프로파일 갱신기

프로파일 갱신기는 시스템 clock을 이용, 규칙 데이터베이스에 저장된 시간값을 주기로 전산망 감사 데이터베이스 및 비정상 데이터베이스의 감사 자료를 이용하여 사용자, 사용자 그룹 및 시스템 자원에 대한 프로파일을 갱신하는 기능을 수행한다.

라. 규칙 생성기

규칙 생성기는 시스템 clock을 이용, 규칙 데이터베이스에 저장된 시간값을 주기로 과거의 사용자에 의해서 발생한 전산망 감사 데이터베이스, 비정상 데이터베이스, 과거의 시스템 침입 방법, 시스템 보안 정책 및 시스템 관리 사항들에 대한 정보를 이용하여 규칙을 생성하는 기능을 수행한다. 규칙 생성기에 의해서 생성되는 규칙들은 과거의 감사 자료를 이용하기 때문에 전문가도 예측하지 못하는 사항들을 포함할수도 있다[2, 5].

4.3. 비정상 탐지기의 분석 기능

비정상 탐지기는 4. 2절에서 설명한바와 같이 감사 자료의 이상 유무를 판단하는데 분석 데이터베이스에서 발생한 3가지 사건 즉, Login, Activity, Logout 별 감사 자료에 대한 비교, 분석 기능을 아래와 같이 수행한다.

가. Login 사건

사용자가 새로운 login 세션을 open할때 발생하는 사건으로 로그인 및 패스워드 실패 횟수, 시스템 접속수, 서비스 종류, 로그인 사이트에 대한 분석 기능을 수행한다. 다음 알고리즘은 로그인 실패 사건을 감지한후, 주어진 시간(duration)동안의 사용자의 로그인 실패 횟수를 누적하여 임계치(maxtimes)를 초과하면 비정상으로 판단하는 과정의 일부이다.

```
procedure count_rule(countdown, expiration)
int countdown, expiration; /* countdown: 로그인 실패 횟수 카운트 변수 */
/* expiration: 현재 시간값으로 감시 단위 시간 체크 */
{
    if(audit_record → action = 'login' and audit_record
    → condition = 'failure'
      and (time( ) < expiration))
    {
      if countdown > 1
        count_rule(countdown − 1, expiration);
      else if countdown = 1
      {
        printf("Too much login failed \n");
        audit_record → flag = abnormal;
        alarm( );
      }
    }
    if(time( ) > = expiration)
      break;
};
```

나. Activity 사건

사용자가 login 세션상에서 시스템 자원을 사용할 때 발생하는 사건으로 데이터의 송수신(traffic) 양, CPU 사용량, I/O 장치 사용량, 수행되는 명령어에 대한 분석 기능을 수행한다. 다음 알고리즘은 사용자가 자주 사용하지 않는 터미널 및 비 시간대에 로그인하는 사건을 감지하고, 비합법적인 사용자를 감지하기 위하여 정상적인 사용자의 시스템 사용 패턴을 정의한 프로파일을 이용, 명령어 실행 횟수를 감시한다. 이때 명령어의 실행 횟수가 임계치를 초과하면 비정상으로 판단한다.

```
procedure monitor(profile, suspected_userid)
```

```
struct PROFILE profile;
int suspected_userid;
{
    int maxtimes, duration;
    /* maxtimes: 임계치, duration: 로그인 실패 감시
    단위 시간 */
    if(userid = suspected_userid and is_an_entry_in
    (profile, event))
    {
      maxtimes = select(profile, event);
      duration = time( ) +3600;
      count_rule(suspectid, maxtimes, duration, event);
    }
};

procedure count_rule(suspectid, countdown, expiration,
command)
int suspectid, countdown, expiration;
 char *event;
{
      if(userid = suspectid and audit_record→action
      = command
        and expiration < time( ))
      {
        if countdown > 1
    count_rule(suspectid,countdown-1, expiration,
    command);
        else if countdown = 1
        {
          printf("Unusal behavior occurred for
          %d\n", suspectid);
          audit_record→flag = abnormal;
          alarm( );
        }
      }
      if(time( ) > = expiration)
        break;
};
```

다. Logout 사건

사용자가 login 세션 종료로 발생하는 사건으로 사용자에 의해서 발생된 감자 자료를 정상, 비정상 여부에 따라 전산망 감사 데이터베이스 및 비정상 데이터베이스에 기록한다. 이에 대한 알고리즘은 다음과 같다.

```
procedure logout_check( )
{
      if audit_record→flag = normal
      {
        open_DB(전산망 감사 DB);
        audit_write(audit_record, 전산망 감사 DB);
        close_DB(전산망 감사 DB);
        exit( );
      }
      else if audit_record→flag = abnormal
      {
        open_DB(비정상 DB);
        audit_write(audit_record, 비정상 DB);
        close_DB(비정상 DB);
        exit( );
      }
};
```

4.4. 감사 분석기 데이터베이스

가. 감사 레코드 데이터베이스

감사 레코드 데이터베이스는 사용자가 시스템에 서비스를 요청하거나 시스템을 이용할때 발생되는 계속적인 활동에 대한 감사 자료로 감사 분석기의 입력 자료로 이용된다. 감사 자료는 시스템에서 생성되는 Native Audit Record와 사건 분류기에서 일정한 형태로 만들어주는 Detection-Specific Audit Record로 구분된다[11].

Native Audit Record는 Unix 운영체제의 감사 패키지에 의해서 생성되는 모든 사용자의 활동에 대한 로그 정보다. 이것을 감사 분석기에서 이용하게 되면 추가적으로 감사 자료를 수집하는 절차가 필요 없지만 감사 분석기에서 필요로 하는 감사 자료를 가지고 있지 않거나, 감사 분석을 하는데 있어서 사용하기에 편리한 형태로 구성이 되어있지 않기 때문에 효율적으로 사용자에 대한 감사 분석을 수행할수가 없다. 따라서 이 연구는 이러한 Native Audit Record를 감

사 분석기에서 필요로하는 형태로 감사 레코드를 구성, 감사 기록기를 통하여 감사 레코드 데이터베이스에 이를 저장하여 사용한다.

나. 분석 데이터베이스

분석 데이터베이스는 감사 레코드 데이터베이스로부터 분석 데이터베이스 갱신기를 통하여 갱신되어 비정상 탐지기에 의해 비교, 분석 과정이 수행된다.

다. 전산망 감사 데이터베이스

전산망 감사 데이터베이스는 전산망을 통하여 발생한 감사 자료가 비정상 탐지기의 분석 과정을 거쳐 최종적으로 감사 자료가 저장되는 데이터베이스로 필요시에 비정상 탐지기에 의해서 참조 되어질수도 있다. 후에 감사자로부터 감사 자료 제공을 요청 받으면 비정상 데이터베이스와 마찬가지로 정보를 제공할수있는 데이터베이스로서 비정상 탐지기에 의해서 계속적으로 갱신이 일어난다.

라. 비정상 데이터베이스

비정상 데이터베이스는 비정상 탐지기에 의해서 분석 데이터베이스내에 있는 감사자료 분석 결과로 이상 상태가 탐지되었을때 비정상 탐지기에 의해서 비정상 감사 자료가 저장되는 데이터베이스로서 규칙 데이터베이스를 생성하는데 이용이 된다. 감사자로부터 감사 자료 제공을 요청받으면, 전산망 감사 데이터베이스와 마찬가지로 정보를 제공할수있는 데이터베이스로서 비정상 탐지기에 의해서 계속적으로 갱신이 일어난다.

마. 프로파일 데이터베이스

사용자의 행동이 정상적인지, 비정상적인 행동인지를 결정하기 위하여 평상시에 사용자가 시스템을 사용하는 습관 또는 패턴을 정의하는데 이용되는 데이터베이스이다. 여기에서 사용할 수 있는 프로파일로는 시스템 접속에 대한 프로파일, 명령어에 대한 프로파일, 파일에 접근에 대한 프로파일등을 정의하여 사용할 수가 있다. 이때 사용자 프로파일을 정의하는데 Metrics변수를 이용하여 표현하며, Metrics변수는 고정된 시간이나 관련된 세션들 사이의 사용자에 의해서 발생되는 측정치로, 새로이 발생하는 사용자의 행동이 정상적인지, 비정상적인지를 결정하기 위하여 통계적인 모델을 적용하는데 이용이 되며 Metrics변수는 다음과 같이 분류된다[8][11].

- 사건 카운터 변수: 주어진 기간 동안에 발생한 사건의 수로 사용자가 시스템에 Login한 수, 한 세션 동안에 임의의 명령어가 실행된 횟수, 패스워드 입력 실패수, 화일 접근 위반수 등이 있다.
- 시간 간격 변수: 두개의 관련된 사건들 사이의 시간 간격을 나타내는 변수로 하나의 Account에 계속하여 Login하는 경우, Login 사이 시간 간격등이다.
- 시스템 자원 측정 변수: 주어진 기간 동안에 사용자에 의해서 사용된 시스템 자원양을 의미하는 변 수로 사용자에 의해서 인쇄된 페이지수, 읽혀진 레코드수, 사용된 CPU 시간등이 있다.

위에서 정의된 임의의 Metrics변수에 통계적인 모델을 적용하여 사용자에 의해서 발생하는 새로운 측정치가 정상적인지, 비정상적인지를 결정할수있는 기준으로 이용한다. 이런 목적을 위하여 이용되는 통계적인 모델로는 운영적 모델, 평균 및 표준 모델, 다변량 모델, 마코브 모델, 타임-시리즈 모델등을 적용할수있다.

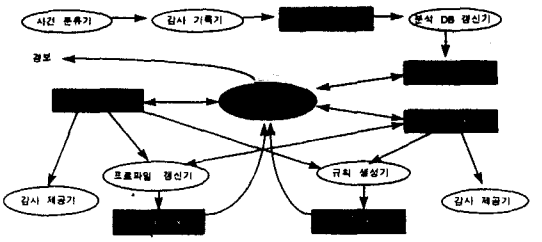
바. 규칙 데이터베이스

규칙 데이터베이스는 주어진 사용자의 행동 패턴이 정상적인지, 비 정상적인지를 결정할수있는 휴리스틱 규칙을 과거의 감사 자료, 시스템의 보안 정책, 과거의 침입 방법 및 시스템 관리 사항들의 정보를 통하여 시스템 사용 패턴을 분석하고, 이런 사용 패턴을 활용하여 자동으로 규칙을 생성한다. 규칙 데이터베이스에 생성될수있는 규칙들은 사용자, 프로그램, 권한, 타임 슬롯, 터미널등의 과거 행동 및 사용 패턴을 묘사한다. 이런 규칙을 토대로 현재 사용자의 행동이 감시되고 사용자의 행동이 침입을 판단 할 수 있는 규칙 데이터베이스내의 규칙 집합과의 비교를

통하여 시스템 이상 상태를 감지하게 된다.

4.5 감사 분석기 실행 모델

전산망 보안에 관련된 감사 자료 및 시스템 보안에 관련된 감사 자료 발생시, 사건 분류기는 이에대한 로그 정보로부터 시스템 사용자 및 위치, 행동, 시스템 자원, 에러조건, 시스템 자원 사용량, 행동 시간등으로 구성되는 감사 자료를 생성한다. 프로세스 및 데이터베이스로 이루어지는 감사 분석기의 실행 과정은 그림 9와 같다.



(그림 9) 감사 분석기 실행 모델
(Fig. 9) Audit analyzer execution model

감사 분석기의 실행 과정의 예를 들어보면 다음과 같다. 사용자 홍 길동이가 IP 주소 203, 255, 71, 102인 시스템으로부터 IP 주소가 203.255.71.20인 시스템으로 Telnet 서비스를 1996년 12월에 요청하는 경우에 있어서 감사 자료는 〈홍 길동(203.255.71.102), Telent, 203.255.71.20, 0, (Telnet Login-Time-Telent Logout-Time), Login-Time〉와 같은 형태로 구성이 된다. 사건 분류기에 의해서 생성된 감사 자료는 감사 기록기에 의해서 감사 레코드 데이터베이스에 저장을 하고, 분석 데이터베이스 갱신기는 감사 레코드 데이터베이스로부터 사용자별, 시간대별, 서비스별등으로 분석 데이터베이스에 감사 자료를 전달한다. 비정상 탐지기는 프로파일 데이터베이스, 규칙 데이터베이스, 비정상 데이터베이스에 저장된 정보를 이용하여 분석 데이터베이스에 저장된 감사 자료의 비교, 분석 과정을 수행한다. 프로파일 데이터베이스에는 각 사용자에 대한 시스템 사용 패턴을 Metrics 변수를 이용하여 표현하는데, 감사 자료의 특정 필드값이 Metrics 변수값의 한계를 초과하는 경우 시스템 침입으로 간주한다. 이때 침입 판정의 오차를 줄이기 위하여 비교, 분석 결과로 대응되지않는 사건에 일정한 비율을 적용하여 그 비율이 일정 수준을 초과하면 최종적으로 시스템 침입으로 간주한다. 시스템 침입 감지시, 이에 대한 상황을 시스템 관리자에게 보고함으로서 침입자에 대하여 적절한 행동을 취할수 있다.

5. 결 론

전산망 감사 추적 시스템은 방호벽 시스템과 상호 연동되어 수행됨으로서 한층더 전산망 보안을 강화시킬 수 있다. 방호벽 시스템은 공격자에 의해서 시스템이 공격을 받아 이상 현상 발생시 이에 대한 적절한 조치를 능동적으로 취할수 없는데 반하여, 감사 추적 시스템은 감사 추적 기법을 이용하여 시스템 침입자를 감지하고, 침입자 발견시 이에 대한 적절한 행동을 취할수 있는 능동성을 제공한다.

이와같은 역할을 수행하기 위하여 이 연구는 전산망에서의 시스템이 가지고 있는 취약점 및 감사 추적 기법들을 검토하였고, 시간정보와 함께 불법적인 침입자를 찾아 사후 조치와 아울러 사전에 분석 기능을 갖는 감사 추적 시스템을 설계하였다. 설계된 전산망 감사 추적 시스템은 사건 분류기, 감사 기록기, 감사 분석기 및 감사 제공기로 구성되었으며, 감사 추적 시스템의 주요 요소중에 하나인 감사 분석기의 세부 구조와 비정상 탐지기의 감사 자료에 대한 분석 기능의 예를 들었다. 감사 분석기는 분석 데이터베이스 갱신기, 비정상 탐지기, 프로파일 갱신기, 규칙 생성기등의 프로세서등으로 구성이되며, 분석에 관련된 데이터베이스를 사용한다. 감사 추적 시스템의 수행을 보이기위하여 감사 분석기의 세부 프로세서들과 각종 데이터베이스와의 연관 관계로서 감사 분석기 실행 모델을 설계하였다.

이 연구에서는 실시간 경계 조치를 위한 완전한 실시간 기능을 수행하지는 못하였다. 현재 이와 같은 미비된 기능의 보완과 아울러 감사 추적 시스템의 기본 구조 설계를 바탕으로 구현된 시스템의 안정성을 위하여 검증 평가 기법의 연구가 추가로 수행되어야 한다. 또한 전산망에서 유통되는 데이터의 양이 매우 방대함으로 효율적인 감사 추적을 위하여 전산망 보안 및 시스템 보안에 관련된 감사 자료만을 추출할 수 있는 기법에 대한 연구가 함께 이뤄져야 한다.

참 고 문 헌

[1] Anderson, J. Computer Security Threat Monitoring and Surveillan ce. Fort Washington, PA:James P. Anderson Co., April 1980.

[2] Bauer, D., and Koblentz, M. NIDX-An Expert System for Real-Time Network Intrusion Detection. Proceedings, Computer Networking Symposium, April 1988.

[3] Denning, D. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, February 1987.

[4] Heberlein, L.;Mukherjee, B.;and Levitt, K. Internetwork Security Monitor:An Intrusion-Detection System for Large-Scale Networks. Proceedings, 15th National Computer Security Conference, October 1992.

[5] Lunt, T., and Jagannathan, R. A Prototype Real-Time Intrusion-Detection Expert System. Proceeding, 1988 IEEE Computer Society Symposium on Research in Security and Privacy, April 1988.

[6] Porras, P. STAT:A Stat Transition Analysis Tool for Intrusion Detection. Masters Thesis, University of California at Santa Barbara, July 1992.

[7] Simon Garfinkel and Gene Spafford, "Practical UNIX Security", O'Relilly and Associates,Inc, 1994.

[8] Silvana Castano, Maria Grazia Fugini, Giancarlo Martella, Pieranglela Samarati, "Database Security", ACM Press, 1995.

[9] Snapp, S., et al., A System for Distributed Intrusion Detection. Proceedings, COMPCON Spring 91, 1991.

[10] Stoll, C. Stalking the Wily Hacker. Communications of the ACM, May 1988.

[11] William Stallings, "Network and Internetwork Security", Prentice-Hall, Inc. A Division of Simon and Schuster,Inc. Englewood Cliffs, New Jersey 07632, 1995.

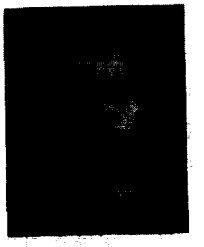
[12] William R. Cheswick, Steven M. Bellovin, "Firewall and Internet Security", AT&T Bell Laboratories. Inc, 1994.

[13] 김기중, 류근호, "시간지원 정보와 EDI 보안감사 추적", 안전한 EDI 관련 심포지움, 한국전자통신연구소,1995.

[14] 신순자, 김홍근, 이재우, "정보화 역기능 현황 및 분석", 한국정보과학회 학술발표논문집 제14권 3호, 1996. 3.

[15] 이재광, 이용준, 박성열, "인터넷 방화벽과 네트워크보안", 이한출판사, 1996.

[16] 정경자, 김기중, 서경란, 류근호, 강창구, "EDI 보안 감사 추적 서비스 시스템 구현", 한국정보처리학회 논문지 제4권 제3호, 1997.



김 기 중

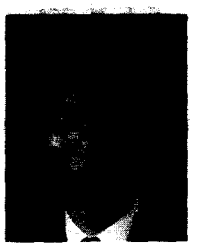
1983년 공군사관학교졸업
1987년 서울대학교 계산통계학과 졸업
1995년 충북대학교 대학원 전자계산학과 졸업(이학석사)
1995년~현재 충북대학교 대학원 전자계산학과 박사과정
관심분야:시간지원 데이터베이스, 데이터베이스 보안, 전산망 보안

윤 상 훈

1996년 군산대학교 컴퓨터과학과 졸업
1996년~현재 충북대학교 대학원 전자계산학과 석사과정
관신분야:시간지원 데이터베이스, 데이터베이스 보안, 전산망 보안

이 용 준

1984년 광운대학교 전산학과 졸업
1987년 연세대학교 전산학과 졸업(석사)
1993년 정보처리기술사(전자계산조직응용)
1997년 충북대학교 전자계산학과 박사과정
1984년~현재 한국전자통신연구원 책임연구원
관심분야: 전산망보안/데이터베이스 보안, 시간지원 데이터베이스, 객체지향 데이터베이스



류 근 호

1976년 숭실대학교 전산학과 졸업
1980년 연세대학교 산업대학원 전산전공(공학석사)
1988년 연세대학교 대학원 전산전공(공학박사)
1976년~1986년 육군군수 지원사 전산실(ROTC장교), 한국전자통신연구소(연구원), 한국방송통신대 전산학과(조교수) 근무
1989년~1991년 Univ. of Arizona TempIS 연구원
1989년~1991년 Univ. of Arizona TempIS 연구원 (TempIS 연구원, Temporal DB)
1986년~현재 충북대학교 전자계산학과 교수겸 컴퓨터 정보통신 연구소장
관심분야: 시간지원 데이터베이스, 시공간 데이터베이스, DBMS 및 OS, 객체 및 지식베이스 시스템