通信情報保護學會誌
第6卷 第3號, 1996. 9

침입 감지 기법의 분석

소 우 영*, 강 창 구**, 김 대 호**

요 약

정보산업의 급속한 발전에 따른 역기능적인 현상으로 컴퓨터 시스템의 사용자들은 정보 보호상의 다양한 문제에 처하고 있다. 컴퓨터 시스템은 네트워크를 통한 해커 등의 침입으로 시스템의 자원 및 중요한 자료들이 위협당하고 있으며 이러한 불법 침입에 대처하기 위한 침입 감지 시스템에 대한 연구가 절실히 요구되고 있다. 본 논문에서는 기존의 침입 감지 기법들을 조사하고 각 기법의 특성 및 문제점을 분석하고자 한다.

1. 서 론

정보산업의 급속한 발전으로 컴퓨터 시스템의 사용이 급격히 증가함에 따라 시스템 사용자들은 네트워크를 통한 정보처리의 편의성을 누리는 반면 사용자 및 컴퓨터 시스템은 정보 보호 상의 다양한 문제에 처하고 있다[1]. 컴퓨터 네트워크를 통한 정보의 위조 및 도청 등의 역기능적 불법 행위로 인한 많은 문제점들이 대두되었으며 이러한 위협에 대처하기 위한 정보 보호 서비스가 절실히 요구되고 수요 또한 급격히 증가하고 있다. 더욱이 컴퓨터 네트워크를 통한 해커 등의 침입으로 시스템의 자원 및 중요한 자료들이 위협 당하고 있으며 때로는 치명적인 손실을 입기도 한다. 따라서 고도의 정보 보호를 필요로 하는 시스템에 대한 불법 침입을 분석하고 감지하여 문제점을 사전에 방지 또는 대처하는 침입 감지 시스템(Intrusion Detection System)은 컴퓨터 네트워크에서 필수적인 보안 서비스로서 이에 대한 연구가 절실히 요구되고 있다.

침입 감지 시스템은 특정 대상 시스템에 대한 불법인 침입으로 시스템이 파괴될 수 있는 상황에서 이를 사전에 감지하여 조치를 취하는 역할을 수행한다. 어떠한 공격에 대해서도 안전한 시스템은 현실적으로 존재하기 어렵다. 왜냐하면, 그러한 이상적인 시스템의 설계에는 엄청난 재정이 소요되고, 시스템의 안전성은 사용 편리성과 서로 상반된 개념이며, 현존하는 첨단 기술로도 거의 불가능하기 때문이다.

대부분의 컴퓨터 시스템은 침입자에 대한 보안성이 적절히 고려되지 않았기 때문에 비합법적인 사용자에 의해 쉽게 악용될 여지를 갖고 있다. 이를 개선하기 위하여 기존 시스템의 소프트웨어 및 하드웨어를 교체하는 것은 어려운 실정이다. 또한, 현존하는 보안 메커니즘들은 패스 워드와 같은 액세스 제어 기법으로 비인가 사용자를 막고 있다. 신분 확인과 액세스 제어 기술은 외부의 침입을 막기 위한

* 한남대학교 전자계산공학과 부교수
** 한국전자통신연구소

1차적인 방어 수단이지만 타협이나 공모에 의해 파괴될 수 있으며 이 경우 악용 자가 비인가 액세스를 얻게 되어 피해 강도는 매우 증폭될 수 있다. 최근 기존의 감사 추적 기법에 통계적 전문가 시스템 기법, 인공 지능 및 신경망 기법 등 여러 첨단 기술을 적용하여 침입을 감지하는 시스템을 개발하게 되었다[3,4].

초기의 침입 감지 연구는 주로 감사 추적 데이터의 분석에서 시작되었다. 그 중 J. Anderson은 일괄 처리 형식으로 설계된 추적 데이터의 분석 방법을 제시하였다[5]. 이러한 방법은 사후에 추적 감사하는 방법으로 침입이 일어난 후에 실시하는 오프라인 분석 과정을 자동화하는 작업이었다. 그후 이러한 불법인 침입을 분석하고 사전에 감지하는 첨단 기술이 발전을 거듭하여 시스템화되고 있다. 이러한 예로서 미국에서 연구되고 있는 IDES (Intrusion Detection Expert System), MIDAS(Multics Intrusion Detection and Alerting System), NAURS(Network Auditing Usage Reporting System), Discovery, NADIR (Network Anomaly Detection and Intrusion Reporter) 등을 들 수 있다.

미국의 SRI 인터내셔널에서는 IDES라는 침입 감지 시스템 프로토타입을 개발하였다. 이 시스템은 안전 문제를 위배하는 모든 형태의 침입을 감지하는 독립적인 메커니즘의 제공을 목적으로 하고 있다. IDES의 감지 설계를 위한 기본적인 개념은 사용자가 지금까지 시스템을 사용한 행위 형태들에서 정상 행위를 유도하여 비정상 행위 감지에 적용하는 것이며 대상 시스템과는 독립적으로 설계되는 Dorothy Denning이 제안한 모델[7]을 기초로 설계되었다.

일반적으로 침입 감지 시스템은 규칙을 기초로 설계되기 때문에 이러한 규칙의 정확한 설정이 매우 중요하며 예측에 대한 보다 높은 정확성과 최상의 신뢰성을 나타내어야 한다. 이러한 규칙은 추적 레코드 규칙, 정기적 활동 규칙, 비정상 레코드 규칙, 비정상 행위 분석 규칙 등이 있다. 또한 통계적 처리를 위한 실제 환경의 측정 기준(measure) 설정 문제가 매우 중요한 요소로써 이를 중점적으로 연구해 왔으며, 침입 감지 시스템이 다양한 형태의 내부적 또는 외부적 침입 행위와 컴퓨터 시스템을 악용하려는 모든 행위에 즉각적으로 반응하여 이를 감지하는 기능인 실시간 처리 분야에 대한 연구가 진행되고 있다[6].

이와 같은 침입 감지 서비스의 요구에 따라 최근에 다양한 기법과 모델들이 개발되어 왔으나 컴퓨터 통신망의 복잡성, 목적 시스템의 원초적 취약성, 정보 보호에 대한 이해 부족 및 불법 침입 기법의 개발 등으로 기존의 어떤 기법 또는 모델도 완전하지 못한 실정이다[3,8].

본 논문에서는 기존의 감사 추적 및 침입 감지를 위한 기법들을 소개하고 각 기법의 특성 및 문제점을 분석하여 새로운 기법 개발 및 기존 기법의 적절한 사용 또는 병용 방법을 고찰하고자 한다. 우선 침입 감지의 개념 및 문제점을 분석하고, 지금까지 연구된 침입 감지 기법의 개념 및 특성을 기술하며, 지금까지 개발된 대표적인 침입 감지 시스템을 소개한 후 침입 감지 시스템의 성능 향상을 위한 새로운 기법의 필요성 및 기존 기법의 병용 방법에 대하여 기술한다.

2. 보안 감사 추적 및 침입 감지

2.1 보안 감사 추적

보안 감사는 시스템 상의 보안 관련 활동을 기록, 조사 및 검토하는 과정을 의미하며 불법적인 정보 유출의 예방과 불법 행위의 추적을 목적으로 한다. 여기서 감사 대상이란 시스템의 사용자 및 프로세스 등의 주체, 단말기 및 통신 메시지 등의 객체, 인증 및 부인 봉쇄 등

의 보안 서비스 수행을 위한 해쉬, 인증 알고리즘 및 키 교환 알고리즘 등의 기법들을 의미한다[1].

ISO(International Organization for Standardization)에서는 보안 감사 모델을 기본적으로 사건식별부, 감사 레코드 생성부, 보안 감사추적부, 감사 분석부, 감사 공급부, 보안 감사 기록부 등으로 나누어 구성하는 방법을 국제 표준으로 제안하고 있다[8]. 그림 1에서는 ISO 제안 모델을 기초로 하여 감사 모델을 구성하는 기본 요소의 연관 관계를 나타내고 있다. 구성 요소들로는 보안 관련 사건, 보안 감사 메시지, 보안 감사 경보, 보안 감사 레코드, 보안 감사 추적 기록부, 감사 추적 보고부 등이 있다.

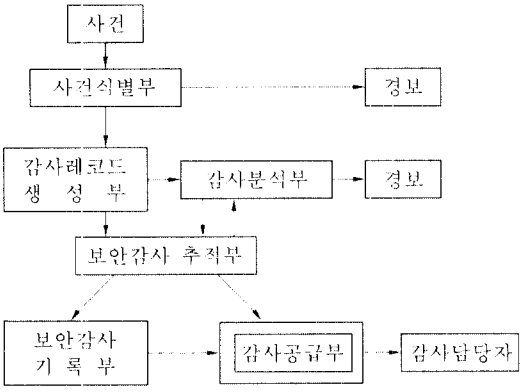


그림 1. 보안 감사의 기본 구성

감사 추적은 발생된 거래에 대하여 필요 시 주체가 객체에 접근한 시간 등의 상황 기록 및 불법 접근 기록 등을 원시 거래 자료를 추적하며 근거를 제공해 주는 과정을 의미하며, 다음과 같은 감사 자료를 취급할 적절한 방법이 요구된다.

- 자료 수집 : 감사 자료의 수집 방법
- 자료의 축소 : 막대한 양의 감사 자료를 필터링하고 필요한 자료를 추출하기 위한 방법
- 자료의 분류 : 해당 사건에 필요한 자료의 분류 및 침입자의 인식 방법
- 결과보고 : 보고서 작성 등 처리 결과의 보고 방법
- 응답 : 침입 감지의 경우 취할 행동 방법

감사 자료는 시스템의 OS(Operating System)가 제공하는 로그 화일을 이용하거나 또는 감사 추적 및 침입 감지를 위하여 별도로 정의하여 생성 수집된다[9]. 광역 망과 같이 이종 호스트 시스템이 연결된 경우 감사 자료는 보안 서비스가 수행되는 도메인 내의 호스트 상호간의 협조를 위하여 표준화될 필요가 있다[10]. 감사 자료는 막대한 양이 생성되며 처리 시간, 통신 오버 헤드 및 저장 공간의 문제가 발생하게 된다. 실시간 처리가 요구되는 경우는 물론 일괄 처리되는 경우에도 자료의 양을 축소시킬 필요가 있으며 다음과 같은 축소 방법이 요구된다[11].

- 필터링 : 불필요한 자료의 제거 및 유용한 자료의 추출 방법
- 클러스터링 : 자료의 특징을 정렬하여 군집화함으로써 새로운 패턴을 추출 생성하는 방법
- 특징(Feature)선택 : 감사 자료 중 불필요한 부분의 제거 방법

2.2 침입 감지

침입 감지란 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법인 침입의 예방에 실패한 경우 취할 수 있는 방법으로서 일반적으로 실시간 처리를 목표로 한다[12]. 침입 감지는 처리 목표 및 단계별로 다음과 같은 기능이 요구된다.

- 침입 예방 : 가장 높은 수준의 침입 방지 대책
- 침입 감지 : 침입 예방이 실패했을 경우 가능한 한 신속히 침입 사실을 감지하여 손실을 최소화하는 대책
- 복구 : 이미 침입하여 공격이 이루어진 경우 시스템 손상을 복구할 대책

침입 감지를 수행하기 위해서는 시스템의 감사 대상에 대한 거래 자료 즉, 감사 자료를 수집해야 하며, 감사 자료를 감사 추적 목적 또는 침입 감지 목적으로 수집 처리하느냐에 따라 이들 3 과정은 동일 시스템에서 통합 운영될 수도 있다.

침입 감지 시스템은 의심스러운 행위를 감지하여 가능한 한 침입자를 조기에 발견하는 것이 목적이지만 분석할 자료의 양이 많기 때문에 그러한 의심스러운 행위가 동시 다발적으로 발생할 경우 감지의 가능성은 적어진다. 따라서 침입 감지 시스템은 이러한 동시 다발적인 침입의 감지 능력이 요구된다.

침입 감지는 그 목적 및 시스템의 처리 능력에 따라 일괄처리 또는 실시간 처리로 이루어진다. 일괄처리 형태의 감사 추적 및 침입 감지는 감사 자료가 수집된 후 중앙 처리기 사용률이 낮은 시간 또는 다른 시스템에서 수집 및 분석된다. 일괄처리 시스템은 주기적으로 의심스러운 시스템 사용에 대한 요약 보고로 충분한 환경에 적합하다. 실시간 침입 감지 시스템은 감사 자료를 축적해 두지 않고 생성 즉시 시스템의 입력으로 처리되며 처리 성능이 중요한 문제가 된다. 따라서 고속 처리 하드웨어, 대용량 저장 장치 및 고도의 신뢰도가 필수적으로 요구된다.

침입 감지 시스템은 운영될 목적 시스템의 환경에 따라 독립형(stand-alone) 다중 사용자 시스템과 분산형 시스템으로 구분된다. 독립형 시스템 환경의 경우 감사 자료가 단일형 레코드로 단일 생성 기법에 의해 수집된다. 분산형의 경우에는 감사 자료가 다수의 상이한 레코드 형식으로 다른 기법에 의하여 생성 수집될 수 있다. 이 경우 반드시 감사 레코드 형식을 통일해야 할 필요는 없으나 상이한 호스트간의 협조를 위한 오버 헤드가 발생할 수 있다. 분산형 환경의 경우 원격 시스템간의 감사 자료 전송을 위한 통신 프로토콜이 요구된다. 이러한 프로토콜은 감사 자료의 무결성과 기밀성을 고려해야 한다. 또한 분산형 환경의 경우 감사 자료의 수집 및 분석을 하나의 시스템으로 집중하거나 다중 시스템으로 분산할 수 있다. 다중 분석 시스템의 경우 전체 시스템을 위한 감사 자료 생성을 위하여 분산형 환경하에서는 통신 프로토콜이 필요하다. 각 시스템의 가능한 침입 형태에 전체 시스템 내에 존재하는 침입 형태가 추가되기 때문에 감지해야 할 침입 유형이 증가하게 된다. 또한 분석할 감사 자료가 증가하게 되며 이에 따른 저장 장치 및 복잡한 압축 기법이 필요하다.

침입 감지 시스템은 특정 목적 시스템에 관련된 사항(예 : 시스템의 취약성)외에 일반적인 사항을 다루게 된다. 따라서 이러한 시스템은 설계 시 다른 목적 시스템에의 이식성을 고려해야 한다. 또한 시스템이 적용되는 환경은 변화될 수 있기 때문에 필요 시 조정 및 확장될 수 있도록 설계되어야 한다. 침입 감지를 위해서는 준비된 자료를 분류하여 비정상적인 행위 또는 불법 침입을 구별할 수 있는 방법이 필요하다.

Denning은 시스템에 대한 불법 사용 또는 침입의 유형을 다음과 같이 분류했다[2].

- 침입 시도 : 시스템에 불법으로 로그인 하려다 실패함
- 신분 위장 또는 성공적 침입 : 비인가자가 인가 자의 계좌에 불법 로그인 함
- 합법적 사용자의 불법 침입 : 시스템 사용

인가 자가 비인가 사항에의 침입
- 합법적 사용자의 기밀 정보 유출 : 합법적 사용자가 시스템 내의 기밀 정보를 외부로 유출
- 합법적 사용자의 정보 추론 : 합법적 사용자가 데이터베이스에서 인가되지 않은 레코드를 불법으로 취득
- 트로이 목마 : 유용한 프로그램 내에 숨겨진 유해한 기능
- 바이러스 : 다른 프로그램 또는 시스템에 유해한 기능을 수행하고 자신을 복제하는 프로 그램
- 서비스 부인 : 자원을 독점함으로써 시스템의 서비스를 방해함

이와 같은 공격에 대처하는 침입 감지 기법들은 다음 장에서 자세히 살펴본다.

침입의 여부를 판정하기 위한 측정 기준은 사용자의 한 세션 내에서 연속성을 가지면서 변하게 되는 ordinal 측정 기준과 한 세션이 시작될 때 측정되는 불연속적인 categorical 측정 기준으로 나누어진다. 불연속적인 측정 기준은 특정 행위의 category가 발생한 회수를 셀 수 있는지의 여부에 따라 선형 불연속 기준과 이진 불연속 기준으로 설정할 수 있다. 선형 불연속 측정 기준으로는 일정 기간에 일어나는 로그인 시간과 로그인이 발생한 터미널의 위치, 각종 응용 소프트웨어 사용 등이 있다. 이진 불연속적 측정 기준으로는 디렉토리나 화일 의 사용 여부 등을 들 수 있으며, 한 세션 동안 각 사용자 세션에 대해 누적되는 연속적인 측정 기준은 세션 연결 시간, CPU 사용량, 입출력 사용량, 명령어나 프로그램의 사용 빈도, 프로텍션 규칙 위반 회수 등을 들 수 있다.

현재 사용되는 측정 기준의 발생 확률이 특정 기준에 미달되면 해당 측정 기준을 제외시키고 연구 결과에 따라 새로운 측정 기준을 추가할 수 있다. 그리고 한 측정 기준을 모든 사용자에게 일률적으로 적용할 경우 사용자의 특성상 여러 문제점이 나타날 수 있으며 사용자들을 그룹별로 다른 측정 기준들을 적용하는 것이 바람직하다. 또한 측정 기준들을 감사 추적 자료의 생성 원인이 되는 사용자, 대상 시스템, 원격 호스트로 나누어 다음과 같이 분류하여 기술할 수 있다.

〈 사용자 측정 기준 〉

- 사용 빈도 : CPU, 입출력, mailer, editor, 컴파일러, 쉘, 프로그램, 디렉토리, 명령어, 윈도 우 명령어, 시스템 호출, 화일, 임시화일등의 사용 횟수
- 디렉토리: 생성, 삭제, 읽기, 수정 등이 수행된 디렉토리의 수
- 연결 회수: 사용처
- 화일 : 생성, 삭제, 읽기, 수정 등이 수행된 화일 의 수
- 사용자 ID: 바뀐 회수, 읽혀졌는지의 여부
- 에러 : 시스템 에러, 유형별 발생 에러 등의 회수
- 추적 레코드 : 추적 레코드의 수(시간, 일), 추적 레코드의 발생 기록, 발생 빈도
- 원거리 네트워크 : 활동량, 유형별 활동량, 호스트별 활동량
- 근거리 네트워크 : 활동량, 유형별 활동량, 호스트별 활동량
- protection 규칙 위반 회수

〈 대상 시스템 〉

- 레코드 생성 수
- 사용 빈도: CPU, 입출력
- login: 실패 회수, 시간별 실패 회수
- 에러: 시스템 에러, 유형별 발생 에러, 시간별 발생 에러 등의 회수
- 네트워크: 활동량, 유형별 활동량, 원격지 호스트별 활동량

〈 원격 호스트 〉

- 사용자 account : 읽혀진 회수
- 네트워크: 유형별 활동량, 시간별 활동량, 유형/시간별 활동량
- login: 실패 회수

3. 기존 침입 감지 기법 분석

앞장에서는 감사 추적 및 침입 감지 기법의 개념 및 요구 사항을 고찰했다. 이러한 요구 사항을 위한 다양한 기법들이 개발되고 있으나 어느 한 기법도 이들 요구 사항을 모두 만족하지는 못한다. 기존의 여러 기법들을 통합 적용한 모델들이 개발되었으나 아직 완전한 시스템과는 거리가 멀다. 여기서는 지금까지 개발된 기법들 중 대표적인 기법들을 소개하고 각 기법들의 특성 및 문제점들을 분석한다.

3.1 통계적 이상 상태 감지 기법

통계적 이상 상태 감지 기법(Statistical Anomaly Detection Technique)은 기존의 침입 감지 기법중 가장 널리 알려져 있으며, 이미 알려진 침입 방법의 통계적 특성을 쉽고 효율적으로 적용할 수 있기 때문에 많은 침입 감지 시스템에 적용되고 있다. 이 기법은 목적 시스템의 취약성에 대한 지식을 요구하지 않으며 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 감지(Threshold Detection)와 프로 파일 기반(Profile-Based)기법으로 대별된다. 이 기법들의 공통적인 문제점은 정상 상태의 개념이 시간 변화에 따라 달라질 수 있으며 또한 시간대별로 다른 의미를 갖기 때문에 정상 상태의 기준 설정이 어렵다는 점이다.

3.1.1 임계치 감지 기법

임계치 감지 기법은 가장 초보적인 형태의 침입 감지 기법으로서 우선 모든 사건의 발생을 기록하고 각 사건들에 대한 정상 상태의 발생 량을 통계적으로 조사 분석하여 각 사건들이 정상 상태에서 허용될 수 있는 발생량 즉, 임계치를 결정한다. 만일 어떤 시점에서 일정 시간 특정 사건의 발생 량이 그 사건의 임계치를 초과할 경우 침입이 발생할 수 있는 것으로 판단한다. 예를 들어 적법한 사용자가 로그인 할 경우 정상상태내에서 USER-ID 또는 PASSWORD의 입력 오류로 실패하는 횟수를 통계적으로 분석하여 임계치를 설정한 후, 어떤 사용자의 로그인 실패 횟수가 설정된 임계치를 초과할 경우 가능한 침입자로 판단할 수 있다. 임계치 감지 기법의 적용 가능한 감시 대상 사건은 로그인 실패 횟수 외에 입출력 오류의 수, 과다한 양의 화일 삭제 및 참조, 그리고 대량의 원격 출력 등이 있다.

임계치 감지 기법은 알려진 침입 기법이 분석될 경우 쉽게 적용할 수 있으며 오버 헤드가 비교적 적다는 장점이 있다. 그러나 이 기법의 성능은 매우 제한적이기 때문에 효율적인 침입 감지를 위한 방법으로는 단독으로 사용되지 못하며, 특정 사건에 대한 임계치와 윈도우 크기 결정이 어렵다는 단점을 가지고 있다. 대개의 경우 이 기법은 침입 감지 시스템의 한 요소를 위한 방법으로 사용된다. 예를 들면 실시간 침입 감지 도구 MIDAS 와 실시간 감사 분석 도구 NADIR에서 시스템의 부분 요소를 위한 기법으로 사용되고 있다.

3.1.2 프로 파일 기반 기법

가장 널리 사용되는 침입 감지 기법의 하나

로서 통계적 프로 파일 방법과 규칙 기반 프로 파일 방법으로 개발되었다. 이 기법은 개인 또는 그룹 사용자의 과거 행동 특성 패턴을 생성하여 관찰된 행동이 과거 행동 패턴과 심한 차이가 있을 경우 침입으로 판단한다. 프로 파일은 대개 침입 감지의 정확성을 높이기 위하여 다수의 파라미터로 구성된다.

프로 파일은 감사 기록을 분석하여 다양한 정량적 계량 단위를 이용하여 사용자의 전형적인 행동 패턴을 생성한다. 생성된 사용자 행동 패턴을 침입 감지 시 입력 감사 기록을 분석하여 현 사용자의 행동이 평균적 행동 즉 프로 파일로부터 이탈되는지를 결정하는데 이용된다.

주체와 객체의 집합체로 객체에 대한 주체의 행동을 결정하는 구조인 프로 파일은 변수 이름, 행위 패턴, 예외 패턴, 자원 사용 패턴, 측정을 위한 시간 간격인 주기, 통계적 모델의 특별한 타입을 정의하는 추상적인 데이터 타입(예, 평균과 표준편차 모델을 갖는 이벤트 카운터)을 나타내는 변수 타입, 임계치, 주체 패턴, 객체 패턴, 측정값 등의 구성 요소를 가진다.

프로 파일 기반 침입 감지에 유용한 통계적 계량 단위의 예는 다음과 같다[1].

- 카운터 : 특정 시간 동안 발생한 사건의 총수 예를 들면, 한 시간 동안 사용자가 로그인 한 수, 사용자 세션 동안 명령 수행 횟수, 일분 동안 패스 워드 실패 횟수 등이 있다.
- 게이지 : 특정 개체의 현재 값 예를 들면, 사용자의 논리적 접속 수, 큐에 대기 중인 사용 자 메지수등이 있다.
- 간격 타이머 : 두 관련 사건 사이의 시간 예를 들면, 동일 사용자 계정에의 로그인 사이의 시간 등이 있다.
- 자원 이용 : 특정 시간 동안 소비된 자원의 양 예를 들면, 사용자 세션 동안 인쇄된 페이 지수, 프로그램 실행 시간 등이 있다.

이와 같은 계량 단위를 이용하여 사용자에 대한 통계적 분석을 통하여 사용자 패턴 즉 프로 파일을 작성한다.

작성된 프로 파일은 새로운 측정값과 비교하여 정상 여부를 결정하게 되며 다음과 같은 운용적 모델, 평균 및 표준편차 모델, 다중 확률 변수 모델, 마코브 프로세스 모델, 타임 시리즈 모델 등의 프로 파일 모델을 이용하여 통계적 테스트가 이루어진다[1].

- 운영적 모델 : 제한 값을 미리 계산하여 정해 놓고 새로운 측정값을 제한 값과 비교하는 모델이며 패스 워드 실패의 수에 대한 이벤트 카운트와 같은 Metric 모델 형태처럼 경험적으로 침입을 예측하게 된다.
- 평균과 표준편차 모델 : 비정규적인 행위를 평균과 표준편차에 의한 신뢰 구간으로 결정하는 모델이며 이벤트 카운트, interval time, resource measure 등에 적용이 가능하다. 이 모델은 운영적 모델의 제한 값을 정하기 위한 정규 행위에 관한 사전 지식이 없어도 가능하며 신뢰 구간이 측정된 데이터들에 의존함으로 사용자별로 다르게 정의될 수 있게 된다. 하지만 오래된 측정값과 최근의 측정값이 같은 영향을 줄 수 있으므로 최근 측정값에 더 많은 가중치를 주도록 설계할 수 있다.
- 다중 확률 변수 모델 : 다중 확률 변수 모델은 두개 이상의 metric들이 상호 관계를 갖는 것으로 표준편차 모델을 이용하며 경험적인 데이터가 여러 측정값들의 조합에서 더 좋은 식별력으로 얻어지는 결과를 이용하여 결정하는 형태의 모델이다.
- 마코브 프로세스 모델 : 마코브 프로세스 모델은 이벤트 카운트에만 적용되는 모델

이며 상태 변수가 이벤트 형태가 되며 상태 사이의 전이 빈도를 상태 전이 행렬로 구성된다. 이 모델은 명령어 순서가 중요한 명령어들 사이의 전이를 조사함에 유용하게 사용된다.

- 타임 시리즈 모델 : 타임 시리즈 모델은 관찰된 측정값 각각의 순서와 도착 시간 간격을 이용하여 결정하는 모델이다.

프로 파일 기반 이상 감지 기법의 장점은 목적 시스템의 취약성에 대한 사전 지식이 거의 필요치 않으며 단지 과거의 감사 기록으로부터 정상적인 행동에 대한 통계자료를 이용하기 때문에 다른 시스템에 쉽게 이식될 수 있으며, 특히 불법 신분 위장 침입의 감지에 강하다.

한편 프로 파일의 생성 관리에는 몇 가지 단점이 있다. 첫째, 사용자가 아주 많은 대형 시스템에서는 프로 파일의 크기 때문에 개인별 프로 파일보다는 그룹별 프로 파일의 관리가 필요하며, 이 경우 개인별 행동 패턴의 고려가 어렵다. 둘째, 대형 시스템의 프로 파일 작성시 개인 및 그룹의 유형별 사용 습관 등이 고려되어야 한다. 예를 들면, 사용자의 수행 업무의 성격, 근무 시간대, 책임 및 권한 등을 고려해야 사용자 그룹의 정확한 프로 파일을 작성할 수 있다. 그러나 사용자의 그룹화는 개별 사용자의 특성 및 습관을 고려하기 어렵고 프로 파일이 위에 열거한 사용자의 유형보다는 실제 관찰된 습관에 따라 작성되어야 하기 때문에 수작 업에 의한 분류는 결과적으로 잘못된 프로 파일을 생성하여 시스템의 성능을 저하시킬 수 있다. 셋째, 목적 시스템의 상황이 바뀔 경우 새로운 통계 처리 알고리즘 개발이 요구될 수 있으며 이 경우 고가의 개발비가 소요된다.

3.2 규칙 기반 기법

규칙 기반 침입 감지 기법은 시스템 상의 활동을 관찰하여 정상적인 패턴인지의 여부를 구분하는 규칙들의 집합으로 구성되며, 감사 자료의 분석을 통한 자동 규칙 생성 및 귀납 추리에 기초한 규칙 기반 이상 상태 감지 기법과 전문가 시스템에 기초한 규칙 기반 침입 감지 기법으로 나뉜다.

3.2.1 감지 규칙

감지 규칙을 설정하기 위해 먼저 일상적이고 일시적인 관찰을 통하여 패턴을 찾아낸다. 여기서 패턴은 되풀이되는 행동을 나타내며 높은 정확도를 갖는 예측을 사용할 수 있다. 관찰에서 얻어진 자료에서 일반화된 가정을 설정하고 얻어진 자료를 논리적 추론을 통하여 변형된 형태의 새로운 패턴을 생성한다. 설정된 가정도 여러 수정을 거쳐 동적으로 유지하며 궁극적으로 보다 정확한 규칙만을 남게 한다. 여기서 가정은 예측에서의 정확성이 높고 신뢰성이 최상이어야 하며 많은 관찰에 의해 추론된 가정이어야 신뢰성이 높아지게 된다. 그리고 설명한 예측의 정확성은 "엔트로피(entropy)"로 표현된다.

침입 감지는 사전에 설정된 행위 규칙에 따라 감사 레코드와 프로 파일의 패턴을 비교함으로 수행된다. 행위 규칙의 형태는 다음과 같이 감사 레코드 규칙, 주기적 행위 갱신 규칙, 비정상 레코드 규칙, 주기적 비정상 분석 규칙 등으로 구분되며 각 규칙들은 조건 부분과 본체 부분으로 구성된다[2].

- 감사 레코드 규칙 : 감사 레코드 규칙은 새로운 감사 레코드와 활동 프로 파일의 패턴이 일 치될 때 발생되며 프로 파일을 갱신하거나 예외적으로 수행되는 행위를

검사하여 비정상적 인 요소가 발생되면 비정상 레코드를 생성한다.

AUDIT-RECORD RULE

조건 : new Audit.Record
Audit.Record matches Profile
Profile.Variable-Type = t

본체 : AuditProcess(Audit.Record, Profile);

END

- 주기적 행위 갱신 규칙 : 주기적 행위 갱신 규칙은 Clock 주기가 수행된 후에 발생되며 프 로 파일을 갱신하거나 예외적으로 수행되는 행위를 검사한다.

PERIODIC-VARIABLE-UPDATE RULE

조건 : Clock mod p = 0
Profile.Period = p
Profile.Variable-Type = t

본체 : PeriodProcess(Clock, Profile);

END

- 비정상 레코드 규칙 : 비정상 레코드 규칙은 새로운 비정상 레코드를 점검하여 해당 규칙에 서 주어진 패턴과 일치될 때 적용되며 보안 담당자에게 비정상 행위 발생 사실을 알리는 메 시지를 출력한다.

ANOMALY-RECORD RULE

조건 : new Anomaly-Record
Anomaly-Record.Profile matches profile-pattern
Anomaly-Record.Event matches event-pattern

본체 : PrintAlert('Suspect intrusion of type ...', Anomaly-Record);

END

- 주기적 비정상 분석 규칙 : 주기적 비정상 분석 규칙은 interval이 마지막일 경우에 마지막 interval이 수행된 후 일정 주기 내에 생성된 비정상 행동 레코드들의 분석에 적용되며 보안 담당자에게 비정상 행위에 대한 긴급보고 메시지를 출력한다.

PERIODIC-ANOMALY-ANALYSIS RULE

조건 : Clock mod p = 0

본체 : Start = Cloak - p;
A = SELECT FROM
Anomaly-Records
WHERE Anomaly-Record.
Time-stamp 〉 Start; generates summary report of A;

END

3.2.2 규칙 기반 이상 상태 감지 기법

이 기법은 과거의 감사 기록을 분석하여 사용자 패턴을 기술하는 규칙을 자동 생성하여 이용한다는 점 외에는 통계적 이상 상태 감지 기법과 유사하다. 규칙 생성은 과거의 감사 자료 뿐 아니라 시스템의 보안 정책, 과거의 침입 방식 및 시스템 관리 사항들이 이용된다. 자동 생성되는 규칙들은 과거의 감사 자료를 분석하여 생성되기 때문에 전문가가 예측하지 못할 사항들을 포함할 수 있다.

규칙들은 사용자, 프로그램, 권한, 타임 슬롯, 터미널 등의 과거 행동 패턴을 나타낸다. 생성된 규칙은 if (condition) then (action)의 형식을 취하며, 정확성을 높이기 위해 지속적으로 수정 관리된다. 생성된 규칙은 특징 값이 과다하거나, 과거의 자료 값의 과소, 다른 규칙과 중첩 등의 경우에는 가지치기(rule pruning)를 통하여 정리된다. 이렇게 생성된 규칙들은 현재 관찰되고 있는 행동의 패턴이 과거의 패턴을 따르는지 결정하기 위해 비교된다.

이 기법은 통계적 이상 상태 감지 기법과 같이 목적 시스템의 취약점에 대한 사전 지식을 요구하지 않으며, 과거의 행동을 관찰하고 미래가 과거와 같을 것이라고 추측하는데 기초를 두고 있다. 따라서 이식성이 높은 반면

효율성을 높이기 위해서는 대량의 규칙 베이스가 필요하다.

3.2.3 규칙 기반 침입 감지 기법

이 기법은 기본적으로 전문가 시스템에 기초한다. 전문가 시스템은 규칙 집합과 이들 규칙 집합을 이용하여 입력 자료에 대한 결론을 유도하는 작동 모듈로 구성된다. 여기서 규칙들은 과거의 감사 기록을 분석하여 자동 생성되지 않고 전문가에 의해서 생성된다. 대개의 경우 목적 시스템의 보안 담당자 및 시스템 관리자와의 인터뷰를 통하여 알려진 침입 시나리오 및 주요 침입 방법에 대한 정보를 수집하여 규칙을 작성한다. 따라서 이 기법은 규칙 작성 기술에 따라 성능이 결정된다. 규칙 작성에 사용되는 휴리스틱의 예는 다음과 같다[1].

- 다른 사용자의 개인 디렉토리에 있는 파일을 읽지 말아야 한다.
- 다른 사용자들의 파일에 쓰지 말아야 한다.
- 로그인 한 사용자들은 몇 시간 후에 그들이 전에 사용한 똑같은 파일을 종종 접근한다.
- 대개 디스크 디바이스 대신 상위 수준의 OS 유틸리티에 의존한다.
- 동일 시스템에 한번 이상 로그인 하지 않는다.
- 시스템 프로그램을 복사하지 않는다.

이 기법은 주로 통계적 이상 상태 감지 기법과 상호 보완적인 방법으로 사용된다. 통계적 기법이 과거의 감사 자료에 의존하는데 비해 이 기법은 전문가에 의해 이미 알려진 침입 방법을 이용하여 침입을 감지하기 때문에 목적 시스템의 특수한 환경들을 충분히 고려할 수 있는 장점이 있다.

이 기법의 단점은 다음과 같다.

- 침입 감지의 유연성이 적다. 지식 베이스 내의 규칙들과 감사 자료를 비교하기 때문에 규칙에 명시되지 않은 약간 변형된 침입 시나리오는 감지하지 못한다. 이 문제는 시나리오를 감사 자료와 독립적으로 고급 표현 방법을 이용함으로써 어느 정도 해결할 수 있다. Garvey와 Lunt가 제안한 모델 기반 침입 감지 기법은 이와 같이 감사 자료와 독립적으로 시나리오를 작성한다[11].
- 진행 중인 침입의 발견이 어렵다. 이미 알려진 침입 시나리오를 기반으로 생성된 규칙을 이용하기 때문에 모든 침입 및 손상이 이루어진 후에 그 사실을 알게 된다.
- 규칙 베이스의 생성 및 갱신인 어렵다. 일반적으로 규칙은 보안 전문가를 통하여 규칙 베이스 프로그래머에 의해 생성되므로 목적 시스템의 상황 변화 등으로 인한 규칙 갱신이 매우 어렵다.

규칙 기반 침입 감지 기법은 다양한 시스템에 적용되었으며 IDES[7][9] 및 USTAT[6]등은 대표적인 적용 사례이다. IDES에서는 목표 감사 기록을 규칙 베이스의 규칙들에 대응시켜 일치될 경우 사용자의 의심 정도를 증가시키고 충분한 규칙들이 일치되어 의심 율이 임계치를 초과할 경우 비정상으로 보고한다. IDES역시 위에서 열거한 단점을 공유한다. 즉, 규칙 적용에의 융통성 결여로 규칙상의 침입 시나리오에서 약간 변형된 형태로 주어진 감사 기록은 감지하지 못한다. 이러한 문제점은 시나리오가 하위 수준으로 기술된 데에 기인한다. USTAT 모델은 이와 같은 문제를 극복하기 위하여 상위 수준의 시나리오 모델을 개발했다.

USTAT는 구체적인 특정 행동보다는 오히려 일반적인 행동에 근거하여 규칙을 생성하기 때문에 규칙의 수가 적어진다. 또한 행동의 시작에서 끝까지의 상태 천이도를 이용하여 새로 학습된 침입 행동을 수용하기 위하여 규칙들이 쉽게 수정된다.

3.3 모델 기반 침입 감지 기법

Garvey와 Lunt에 의해 제안된 모델 기반 침입 감지 기법[11]은 적용 도메인에 관한 지식을 적절히 사용함으로써 가정에 대한 가능한 모든 증거들의 효과 측정을 목표로 하는 증거 추론(evidential reasoning)에 이론적인 기초를 두고 있다. 이 기법에서는 불법 침입자가 공격시 체계적 패스워드 공격 등의 전형적인 절차를 이용한다고 가정한다. 이미 알려진 공격 방법에 대하여 공격 모델을 개발하고, 이러한 공격 모델에 근거하여 관측 행위를 연관 시켜 불법 침입 여부를 추론한다. 즉 가정된 공격 시나리오에 속하는 행위를 찾아서 침입을 감지해 낸다. 공격 시나리오는 침입자와 대상 시스템에 따라 다를 수 있으며 주어진 공격 시나리오에서 침입자의 다음 행동을 예측하게 된다.

전문가 시스템에 기초한 규칙 기반 침입 감지 기법에 비교할 때 모델 기반 침입 감지 기법은 적용절차가 쉽다. 보안 담당자에 의해 개발되고 공격 시나리오로 기술되는 공격 모델은 감사 자료 형태로 기술되는 전문가 시스템의 규칙보다 수정이 용이하다. 공격 시나리오를 뒷받침 하는 증거들은 감사 자료로부터 침입 감지 시스템에 의해서 인식되기 때문에 규칙의 유지 보수가 전문가 시스템보다 용이하다. 공격 모델은 사건 발생 순서대로 공격 시나리오가 자연스럽게 정의되기 때문에 침입 감지 능력이 높다. 모델 기반 기법의 규칙에는 불확실성이 포함되기 때문에 불확실성하에서의 추론을 지원할 수 있다. 물론 전문가 시스템에서도 휴리스틱에 기초한 근사치 정보가 취급될 수 있으나 결과에 대한 해석이 어렵다.

이 기법의 장점은 다음과 같다.

- 사건 발생 순서에 따라 시나리오가 작성되고 현재의 사건 관련 데이터에 초점을 두고 감사 자료를 선택적으로 적용하기 때문에 취급할 감사자료의 양을 축소할 수 있다.
- 공격 시나리오에서 침입자의 다음 행동을 예측할 수 있기 때문에 예방적 조치가 가능하다.

한편, 이 기법은 공격 시나리오에 기초를 두고 있기 때문에 기지의 공격 모델에만 적용이 가능하다는 단점을 가진다. 따라서 이 기법은 다른 기법과 마찬가지로 통계적 이상 상태 감지 기법 등과 같은 다른 기법과의 병용이 바람직하다.

3.4 신경회로망 기법

신경회로망은 상호 연결된 뉴런으로 구성된다. 각 뉴런은 연결 상의 가중치를 통하여 다른 뉴런으로부터 입력을 받아 자체의 출력 값을 생성한다. 연결 가중치는 연결된 뉴런 사이의 활동 레벨간의 상호관계의 정도를 나타낸다. 따라서 가중치가 변함에 따라 각 뉴런의 그리고 전체 신경회로망의 입력 처리 결과가 달라진다.

이와 같은 신경회로망은 주어진 입력 자료 집단의 학습 패턴을 이용하여 지속적으로 가중치를 조절하는 알고리즘을 이용하여 학습할 수 있으며 전형적인 패턴 분류기(classification)로써 이용된다.

학습 과정을 살펴보면 정상적인 시스템 사용 시의 감사 자료와 비정상적인 또는 침입 상황하에서의 감사 자료를 신경회로망의 입력으로 주어 반복적으로 처리하는 과정에서 가중치를 조절해 나감으로써 정상 사용자와 비정상 사용자의 감사 자료 패턴을 분류하게 한다.

통계적 이상 상태 감지 기법은 과거의 감사 기록을 분석하여 평균적인 통계적 측정치를 결정하고 현재의 감사 자료와 그 측정치와의 차이로써 침입을 감지한다. 신경회로망은 이와

같은 통계적 기법의 기능을 수행할 수 있는 기법으로서 통계 분포에서의 가정 등을 필요로 하지 않고 과거의 감사 자료를 이용한 지속적인 학습 과정을 통하여 감사 주체의 통계적 행동 특성을 수립하고 그 특성에 근거한 패턴 분류 방식으로 침입 감지 기능을 수행한다.

신경회로망 기법과 통계적 이상 상태 감지 기법과의 특성을 비교해 보면 다음과 같다.

- 통계적 기법은 감사 주체의 행위가 복잡하기 때문에 관측된 입력 패턴과 과거의 주체 행위 패턴과의 매칭이 어렵다. 따라서 통계치를 잘못 분석하면 침입 감지가 잘못 이루어지며, 매칭에 실패하면 침입 감지를 실패하게 된다.
- 통계적 기법은 주체 행위에 대하여 가우시안 분포 등의 가정하에 감사 기록 분석이 이루어 지는데 이 가정은 항상 성립한다고 볼 수 없다. 따라서 통계분석 자체에 오류가 발생할 수 있다. 신경회로망 기법은 패턴 분류를 위한 학습 과정에서 이러한 가정이 필요치 않으며 단지 대상 사용자의 패턴을 대표할 수 있는 시나리오 즉, 감사 자료 중 어떤 상황(입력)이 정상 사용자(출력)이고 어떤 상황이 비정상 사용자인지에 관한 정보만을 필요로 한다.
- 침입 감지를 위한 통계적 측정치 평가는 직관적이고 경험적으로 이루어지기 때문에 모든 주체에 맞는 측정치 평가가 어렵다. 신경회로망에서는 학습을 통하여 개별 주체에 대한 상황을 종합적으로 고려하여 측정치를 평가할 수 있다.
- 과거 감사 기록 분석에 필요한 통계 처리 알고리즘의 개발 비용이 고가이며, 목적 시스템의 상황 변화나 새로운 시스템에 적용시에는 새로운 알고리즘 개발이 필요하다. 그러나 신경회로망 기법은 학습을 위한 입력 자료만 주어지면 새로운 환경에서의 통계분석이 가능하므로 비용이 저렴하고 신속한 프로토타입 개발에 유리하다.

신경회로망 기법은 위와 같은 장점에도 불구하고 그 자체로써 다른 침입 감지 기법을 대체하기는 어렵다. 신경회로망 기법은 근본적으로 주어진 학습 자료에 따라 패턴을 분류하기 때문에 처리 결과에 대한 해설(explanation)방법이 없다. 단순히 학습 시 주어진 과거의 감사 자료의 패턴에 근거하여 정상 또는 비정상 사용자를 분류해 내며 왜 그러한 결과가 도출되었는지에 대한 해설 방법이 없다. 이 문제는 신경회로망의 근본적인 문제로서 전문가 시스템을 보조적 수단으로 사용할 수도 있다. Debar등은 신경회로망 기법을 이용한 자료 필터링 시스템을 제안했다[11]. 이 시스템은 사용자 행동에 현저한 사용 습관이 존재하며 감사 자료 사이에는 상호 연관 관계가 존재한다는 가정 하에, 순환 회로망(recurrent network)을 이용하여 감사 자료 사이의 정규 규칙을 찾아 여기에 맞지 않는 감사 자료를 필터링하는 방법을 이용했다. Doumas등은 신경회로망 기법을 이용한 바이러스 인식과 분류 모델을 제안하였다[12]. 이 모델은 BACKPROP 및 SOFM 네트워크에서 바이러스의 유형에 대한 입력 자료를 이용하여 학습을 시킨 뒤 바이러스의 인식 및 분류에 적용했다.

신경회로망 기법의 또 다른 예는 침입 감지 시스템의 한 요소로 사용되는 시스템이다[4]. 이 시스템은 신경회로망 요소와 전문가 시스템 요소로 구성되며 신경회로망은 통계적 자료 분석 기능을 담당하고 전문가 시스템은 신경회로망의 결과를 분석하고 침입 감지를 위한 형태로 변형시킨다.

3.5 지문 비교 침입 감지 기법

기존의 침입 감지 기법과는 다른 침입 감지 기법으로 지문(thumbprints)비교 침입 감지 기

법이 제안되었다[13]. 이 기법은 특히 복잡한 컴퓨터 네트워크 상에서의 침입 감지를 위한 기법으로 기존의 기법과는 달리 과거의 감사 기록에 의존하지 않는다. 네트워크 상에서 한 사용자는 한 컴퓨터에 로그인 하여 다시 다른 컴퓨터들을 계속 로그인 할 수 있으며 이와 같은 네트워크 연결을 연결 체인(또는 확장된 연결) 이라고 한다. 침입 감지 서비스가 행해지는 네트워크의 일부 즉 도메인 내에서 연결 체인이 시작되어 그 도메인 밖으로 나갔다가 다시 들어올 경우 두개의 부분 연결 체인이 하나임을 인식하기는 어렵다. 만약, 공격자가 자신의 신분 위장을 위하여 이러한 방법을 이용할 경우 침입 감지는 더욱 어려워진다.

이 기법의 기본 개념은 연결 체인 상의 다른 두 노드에서의 연결 활동 내용 즉 지문은 동일하기 때문에 연결 체인의 시작을 찾을 수 있다는 것이다. 즉, 어떤 사용자가 사용한 ls명령은 연결 체인상의 모든 노드를 통과하며 동일하다는 것이다. 실제로 이 기법에서 지문은 사용자의 모든 명령을 이용하지 않고 자료의 체크 섬과 같이 일정 시간 간격을 두고 채취되기 때문에 비교될 지문의 자료는 크지 않다. 이 기법은 분산 침입 감지 시스템인 UC Davis의 DIDS시스템[13] 등에 적용되었다.

이 기법을 이용할 수 있는 분야 및 장점은 다음과 같다.

- 도메인 내에서 시작되어 밖으로 나갔다가 다시 들어오는 연결 체인의 감지가 가능하다. 따라서 내부의 공격자 발견이 유리하다.
- 어떤 노드가 연결 체인 상의 통과 노드로 사용됐는지 발견할 수 있다.
- 정확한 공격 지점 조사에 이용 가능하다.
- 인터넷 상에서의 침입 감지가 가능하다.
- 부분적인 인터넷 상에서도 사용 가능하다.
- 지문 자체가 작기 때문에 제반 오버 헤드가 적다.

이 기법의 단점은 다음과 같다.

- 트로이 목마 등과 같은 침입에는 사용할 수 없다.
- 연결 체인 상의 각 노드의 일부가 통신 정보를 암호화하든지 또는 각 노드의 암호 기법이 다를 경우 사용할 수 없다.
- 연결 체인 상의 모든 노드가 이 기법 사용에 참여해야 한다.
- 지문이 전체 통신 내용의 일부만 포함하고 있기 때문에 연결 상의 상세한 내용 추적이 불 가능하다.

3.6 기존 침입 감지 기법의 비교

지금까지 살펴본 각 기법들의 특성 및 장단점을 요약하면 표 1과 같다.

표 1. 감사 추적 및 침입 감지 기법의 비교

기 법	특 징	장 점	단 점
임계치 감지	감사 기록의 통계적 분석으로 사건의 임계치 결정	• 시스템의 취약성과 무관 • 알려진 침입 기법에 적용용이 • 오버헤드가 적음	• 제한적 성능 • 알려진 사건들에만 적용 가능
프로파일 기반	감사 기록 분석으로 사용자 프로파일 생성	• 목적 시스템의 취약성과 무관 • 알려진 침입 기법에 적용용이	• 사용자 증가시 프로파일생성관리가 문제 • 사용자 개별 사용 습관 등의 고려가 어렵다. • 통계 알고리즘의 높은 개발비용

규칙 기반 이상 상태 감지	감사 기록 분석으로 사용자 패턴에 대한 규칙의 자동 생성	• 사용자 규칙의 자동 생성 • 시스템 환경 고려 가능	• 대량의 규칙 베이스 생성 관리 필요 • 규칙과 일치되지 않는 침입 감지가 어렵다.
규칙 기반 침입 감지	전문가의 지식에 근거한 규칙 생성. 전문가 시스템에 기초	• 시스템의 취약성등 특수 사항 고려가능	• 규칙 베이스 생성 및 갱신이 어렵다. • 규칙에서 벗어난 침입감지가 어렵다. 진행중인 침입 감지가 어렵다.
모델 기반 침입 감지	가정된 공격 시나리오에 속하는 행위를 찾아 침입 감지	• 감사자료의 선택적 적용으로 취급 감사자료의 양을 축소 • 공격 시나리오에서 다음 행동예측으로 예방조치 가능	• 기지의 공격 모델에만 적용 가능
신경회로망 기법	감사기록으로부터 통계적인 사용자 패턴의 자동학습	• 학습 기능 이용. 통계분석 알고리즘 불필요 • 개별 사용자에 대한 종합 상황 고려가능 • 통계분석이 쉽고 이식성이 높다.	• 처리 결과에 대한 해설이 어렵다.
지문 비교 침입 감지	네트워크 상의 연결노드들의 활동내용(지문)을 일정 시간마다 채취하여 비교	• 네트워크 상의 정확한 공격 지점 조사 가능 • 도메인 내외에 걸친 공격자 발견용이 • 지문의 양이 적어 오버헤드가 적다.	• 트로이목마등 시스템 내부 침입감지불가 • 노드의 활동내용 암호화시 사용불가 • 상세한 추적 내용 분석이 불가능 • 모든 노드가 동일 기법 사용해야 가능

4. 주요 침입 감지 시스템

침입을 분석하고 감지하여 문제점을 사전에 방지하는 기술은 발전을 거듭하여 시스템화되고 있다. 이러한 예로서 IDES(Intrusion Detection Expert System), MIDAS(Multics Intrusion Detection and Alerting System), NAURS(Network Auditing Usage Reporting System), Discovery, NADIR(Network Anomaly Detection and Intrusion Reporter) 등을 들 수 있다.

4.1 IDES (Intrusion Detection Expert System)

IDES는 대상 시스템의 여러 행동을 관찰하여 독립적인 사용자, 그룹, 원거리 호스트, 등의 행위가 정당한 지를 조사하는 미국의 SRI에서 개발한 침입 감지 시스템으로 특정한 대상 시스템이나 응용 환경등에 독립적인 Dorothy Denning이 제안한 IDES 모델을 근간으로 설계되었다. 이는 IDES를 분석함에 있어 매우 핵심적인 사항이 되며 일반적인 침입 감지 시스템에 대한 framework를 제공한다. IDES는 시스템을 파괴하기 위한 외부자 침입과 부여된

권한을 넘어 특권을 오용하려는 내부자 침입을 모두 포함하여 안전 문제를 위배하는 모든 형태의 침입을 감지하는 독립적인 메커니즘을 제공하는 것을 목적으로 한다. 즉, 시스템 사용자의 행위가 지금까지 시스템을 사용한 여러 형태들로부터 추론하여 기대된 행위로부터 이탈한 정도가 크거나 전문가 시스템 규칙에 근거하여 미리 설정한 규칙에 위배되는 경우 이를 비정상적인 행위로 결정하고 이를 시스템에 알려 해당 조치를 수행하게 된다.

IDES는 이와 같이 profile된 통계적 주체 지식 베이스를 유지한다. 이러한 프로 파일에는 침입 감지 measure들의 집합 각각에 대하여 주체의 기대되는 행위들이 수록되어 있다. 시스템에는 침입을 감지하기에 충분한 양의 데이터가 저장되어야 하겠지만 시스템 기억용량의 한계로 인하여 과거 행위 데이터를 저장하는 것 보다는 프로 파일들이 도수표, 평균, 분산 등을 유지하여 통계학을 이용하여 행위의 적법성 여부를 결정하게 된다.

결과적으로 침입이라는 것은 사용자의 비정규적인 행위에서 발견되며 대상 시스템에서 공급되는 감사 레코드들에서 추론되어진다.

4.2 MIDAS (Multics Intrusion Detection and Alerting System)

MIDAS는 미국 정부 Multics 시스템을 모니터 하기 위하여 NCSC(National Computer Security Center)가 개발한 침입 감지 시스템으로 NCSC의 네트워크 메인 프레임에 대한 침입과 오용을 실시간으로 감지하여 알려준다.

이 시스템도 SRI의 Dorothy Denning과 Peter Neumann의 침입 감지 연구에 매우 많은 영향을 받았으며 IDES가 사용자의 과거 행위들을 바탕으로 잘못된 행위를 감지하는 방향과는 달리 MIDAS는 침입을 정의한 priori 규칙을 근간으로 운용되는 침입 감지 시스템으로 개발되었다.

MIDAS는 stand-alone형 LISP 머신으로 구현되었으며 초당 150개의 추론을 할 수 있는 능력을 지닌 전문가 시스템 셸(shell)을 사용하고 있다. MIDAS의 행위 규칙은 LISP에서 만들어지며, 사용자의 통계적 프로 파일은 LISP 구조로 되어 있다. Denning의 침입 감지 모델을 근간으로 하여 compiling, debugging 등의 각종 메커니즘들을 제공하는 전문가 시스템 셸인 P-BEST (Production-Based Expert System Toolset)라는 도구들을 사용하여 개발되었으며 사용자 명령어 레벨에서 모니터 한다.

4.3 NAURS (Network Auditing Usage Reporting System)

NAURS는 MILNET과 ARPANET에 대한 TAC 접근 제어 시스템과 연동 되어 사용되고 있으며 TAC(Terminal Access Controller)들과 NAC(Network Access Controller)들로 부터 발생된 네트워크 행위를 감시한다.

NAURS는 TAC/NAC login, TAC/NAC login 실패, logouts, open and close connections, 온라인 상태의 TACs 등에 관한 데이터를 수집하고 이를 데이터베이스 형태로 유지 관리한다.

NAURS는 지난 행위에 대한 background 분석과 현재 사용자에 대한 실시간 분석을 모두 수행한다. 그리하여 이상하다고 판단되는 이벤트들은 즉시 보고하며 일정 기간별 주기적 감사 분석 결과를 보고해 준다. NAURS의 프로토타입에서는 호스트 컴퓨터와는 분리된 시스템으로 구동되며 네트워크 사용자가 화일의 이동이나 remote login 등의 접근을 할 수 없도록 설계되어 있다. 이 프로토타입에서 장치의 축소화, 기능의 분배, 침입의 실시간 감지 능력, 감사 데이터베이스의 축소화 등을 부가하여 실용 생산품으로 개발하게 될 것이다.

4.4 Discovery

컴퓨터 서비스가 상업적으로 제공되어질 때 외부 사용자에 의해서 야기되는 침입 위협을 나타내기 위해 미국의 TRW에 의해서 개발된 침입 감지 전문가 시스템이 Discovery이다. 그러므로 Discovery는 가입자에 의해 빈번하게 사용되는 패턴을 기억하게 하여 해당 패턴이 정규 패턴을 찾아 차이점을 감지하는 전문가 시스템이라 할 수 있다. 이를 위해 Discovery는 서비스 형태와 접근 방법에 의해 사용자 profile을 개발하고 사용자의 여러 행위가 발생할 때마다 사용자의 profile을 갱신한다.

상업적 사용 환경 하에서는 가입자는 서비스를 제공하는 컴퓨터 시스템과 정보 자산의 안전성이나 무결성을 유지함에 큰 관심이 없고 서비스 제공 회사의 안전성 유지 프로그램에 잘 따르려 하지 않음으로 보다 빈번한 여러 종류의 위협이 나타나게 된다. 이러한 예로는 가입자가 자기의 패스 워드를 남에게 넘겨주거나, 자신의 단말기를 남에게 빌려주어 사용자가 곧바로' 침입자가 되는 것 등을 들 수 있다. 그리하여 Discovery는 합법적인 사용자 id, 액세스 코드 등을 갖고 있는 불법 사용자를 감지하려 하며 궁극적으로 감지와 방어 모두를 목적으로 하게 된다.

4.5 NADIR (Network Anomaly Detection and Intrusion Reporter)

NADIR는 하나의 운영체제에 대한 침입 감지와는 반대로 전산망의 침입 감지 문제를 해결하기 위하여 NL(National Laboratory, Los Almos)에서 시험적으로 개발한 침입 감지 시스템이다. NL의 주 전산망인 ICN(Integrated Computing Network)을 위해 개발한 NADIR은 네트워크의 안전성에 대한 책임을 가지는 자에 의해 수행되었던 감사 레코드의 분석 체제를 개선하고 발전시켜, 하나의 행위에 대한 반응으로서의 결과 제시가 30초이내에 수행되도록 실시간 전문가 시스템으로 개발하고자 하였다. 이리하여 예외적인 행위가 NADIR에 의해 감지되었을 때 이를 운용 요원에 알리고 악의적인 행위를 발견하기 위해 관련 tool이 실행되게 한다.

이 시스템은 외부의 '해커' 뿐만 아니라 특권을 지닌 내부 자의 오용도 감지할 수 있도록 설계되었다. NADIR은 대상 시스템의 동을 모니터 하여 감사 레코드를 수집하는 데이터 수집 부문을 비롯하여 프로 파일을 생성하는 데이터 처리 부문, 전문가 규칙을 적용하여 결과를 생성하는 침입 감지 부문, 상태를 나타내고 이면 분석(background Analysis)을 수행하는 사용자 인터페이스 부문, 특별한 침입에 대한 보고문을 주기적으로 생성하는 보고문 생성 부문, 수정 복구 등의 6개 부문으로 기능적으로 나눌 수 있다.

5. 결 론

지금까지 감사 추적 및 침입 감지 시스템의 문제점과 요구 사항을 분석하고 기존의 기법들과 시스템들의 특성 및 장단점을 분석해 보았다. 기존의 어느 기법도 침입감지 시스템의 모든 요구 사항을 만족하지 못하며, 지금까지 개발된 다양한 침입 감지 모델들은 복수의 기법을 적절히 병용하고 있으나 앞장에서 살펴보았듯이 만족할 수준은 못되고 있다. 따라서 완전한 침입 감지 시스템 설계를 위해서는 모든 요구 사항을 만족할 수 있는 새로운 기법이 필요하다. 그러나, 침입 감지 문제는 그 자체가 복잡 난해하며 또한 창과 방패의 문제와 같아서 그러한 기법은 앞으로도 존재하기가 어렵다. 현 시점에서 기대할 수 있는 것은 우수한 기법 개발과 현존하는 기법의 적절한 병용 방안이다. 예를 들면 IDES모델은 프로파일

기반 및 규칙 기반 침입 감지 기법 등을 병용하여 상당 수준의 성능을 나타내고 있다.

복수의 기법 병용에는 고려해야 할 문제점이 있다. 각 기법들은 주어진 감사 자료를 입력으로 하여 자체의 결과를 생성해 내며, 경우에 따라서는 각 기법의 결과가 다를 수도 있고 기법 사이에 상충 작용이 발생할 수도 있다. 따라서 이러한 문제를 중재하기 위한 통합 기법이 요구된다. 이러한 통합 기법은 각 기법의 가능한 오류를 탐지하여 최종 결과에 반영할 수 있어야 한다. 예를 들면, 통계적 이상 상태 감지 기법은 출장 중인 적법한 사용자가 원격지에서 로그인 할 경우 가능한 침입자로 판단할 수 있다. 사용자의 권한 변화, 새로운 사용자 추가, 사용 중지, 부서 변경, 이사, 휴가 등 사용자에 대한 새로운 사항 및 시스템 내의 화일, 디렉토리, 디바이스, 권한 등에 대한 정보를 고려할 방법이 통합 기법에서 요구된다. 이러한 방법으로 개발되는 침입 감지 시스템은 각종 주요 컴퓨터 시스템에 응용될 것이며 정보 시스템의 안전도 향상에 크게 기여할 것이다.

참 고 문 헌

[1] W. Stallings, "Network and Internetwork Security", Prentice Hall, 1995.

[2] Dorothy E. Denning, "An Intrusion Detection Model", IEEE Trans. S. E., 1987. 2.

[3] Teresa F. Lunt, R. Jagannathan, "A Prototype Real-Time Intrusion Detection Expert System", 1988 IEEE S&P, 1988. 7.

[4] H. Debar, et al, "A Neural Network Component for an Intrusion Dectection System", IEEE Computer Society Symposium Research in Security and Privacy, 1992, pp240-250.

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

[6] K. Ilgun, "USTAT: A Real-time Intrusion Detection System for UNIX", IEEE Computer Society Symposium Research in Security and Privacy, 1993, pp16-28.

[7] Teresa F. Lunt, Ann Tamaru, etc, "IDES : A Progress Report", 6th IEEE CSAC, 1990.12.

[8] ISO 10116-7 : security audit framework, 1993. 3.

[9] ISO 10164-7 : IT - Security Management - Part 7 : Security Alarm Reporting Function, 1992.

[10] ISO 10164-6 : IT - Security Management - Part 6 : Log Control Function, 1992.

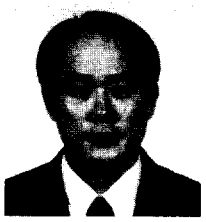
[11] Bobby G. Miller, Paul E. Proctor, "A Requirements-Oriented Analysis of Computer Misuse Detection Systems", I. D. Workshop, 1991. 5.

[12] A. Doumas, et al, "Design of a Neural Network for Recognition and Classification of Computer Viruses", Elsevier Science, 1995, pp435-448.

[13] S. Staniford-Chen, "Distributed Tracing of Intruders", Univ. of California, Davis, M.S. Thesis, 1995.

[14] T. D. Garvey, T. F. Lunt, "Model-Based Intrusion Detection", 14th NCSC, 1991.10.

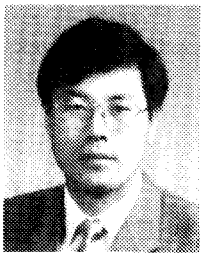
□ 著者紹介



소 우 영

1979년 2월 중앙대학교 전자계산학과 학사
1981년 2월 서울대학교 대학원 계산통계학과 전자계산학 석사
1991년 1월 매릴랜드대학교 대학원 전자계산학과 박사
1981년 3월 ~ 1985년 3월 공군사관학교 수학과 전자계산학 전임강사
1991년 9월 ~ 현재 한남대학교 전자계산공학과 부교수

※ 관심분야 : 인공지능, 신경회로망, 통신망 정보보호



강 창 구

1979년 2월 한국항공대학 항공전자공학과 공학사
1986년 2월 충남대학교 대학원 전자공학과 공학석사
1993년 8월 충남대학교 대학원 전자공학과 공학박사
1979년 ~ 1982년 한국공군 기술장교
1987년 ~ 현재 ETRI 책임 연구원

※ 관심분야 : 부호 이론, 통신 프로토콜, 통신 및 컴퓨터 보안, 정보보호 서비스 및 메카니즘

김 대 호

1977년 한양대학교 전자공학과 학사
1984년 한양대학교 산업대학원 전자공학과 석사
1993년 Univ. of Maryland at College Park
Dept. of Computer Science Visiting Scholar
1977년 ~ 현재 한국전자통신연구소 책임연구원

※ 관심분야 : 전송분야, 통신 및 컴퓨터 보안