通信情報保護學會論文誌
第 6 卷 第 4 號, 1996. 12

Man-Machine에 의한 효율적인 침입 탐지 시스템 설계

신 장 균*, 나 민 영*, 박 병 호**, 최 병 갑*

Design of Efficient Intrusion Detection System using Man-Machine

Jangkoon Shin, Minyoung Ra, Byungho Park, Byungkab Choi

요 약

네트워크의 발달로 시공간을 초월하여 자료 및 자원의 공유, 분산처리, 컴퓨터 통신이 가능하게되는 순기능도 있으나, 반면에 전세계 어디에서든지 컴퓨터를 통하여 컴퓨터 시스템의 무단 이용과 시스템의 파괴, 저장된 자료의 유출 등의 수단으로도 이용되고 있다. 최근의 동향은 국내뿐만아니라 외국에서도 한국으로의 해킹사례가 늘고 있어 그 심각성이 날로 증대되고 있다. 따라서 국방 전산자원을 보호해 줄 수 있는 시스템의 개발 및 적용이 시급하다.

본 논문에서는 예상되는 각종 침입에 대해 전산망 보안 요구사항을 도출하고 감사데이타를 활용하는 통계적 침입 탐지 및 규칙기반 침입 탐지 기법 분석을 통해 침입 탐지 시스템을 설계하고자 한다.

Abstract

Networking revolution provides users with data and resources sharing, distributed processing, and computer communication in cyberspace. However, users may use computers as a way of unauthorized access, system destruction, and leakage of the stored data. In recent trend, incresing of hacking instances which are from domestic as well as abroad reaches to the level of seriousness. It, therefore, is required to develop a secure system for the National Depense computing resources and deploy in practice in the working field as soon as possible.

In this paper, we focuss on finding the security requirements of a network and designing Intrusion Detection System using statical intrusion detection and rule-based intrusion detection analysis through accumulating audit data.

---

* 육군사관학교 전산학과
** 東北大 大學院 情報科學研究科/電氣通信研究所
본 논문은 1996년도 육군사관학교 화랑대 연구소 연구비 지원에 의해 수행된 연구임.

1. 배 경

최근 일련의 해킹사례[1]들은 네트워크의 발달로 우리들에게 가져다준 이익보다도 더 해로운 결과들이 나타날 수도 있다는 것을 보여준다. 특히, 국내 해커뿐만 아니라 외국의 해커들이 국내 중요 전산망에 침입하여 자료의 유출과 훼손등 그 공격 양상은 다양화되고 침입 횟수는 날로 증가 추세에 있다.

특히, 국가 기간 전산망에는 항시 적의 침입이 예상되고 있어 고도의 경계의 태세를 유지해야 한다. 급속한 컴퓨터 네트워크의 발달은 시간과 공간을 초월하는 새로운 시대로 급변화시켜가고 있어, 목전에 다가온 21세기는 더많이 전산망을 활용할것이며 국방분야에서도 각종 네트워크를 통한 국방 정보의 생산관리 및 활용은 군 전투력을 좌우하는 중요한 요소로 부각되고 있다. 국방망 해킹 발생시 피해의 심각성은 심대하며 그 위협은 날로 증대되고 있는 실정이다. 특히 고도의 보안 안전장치가 요구되는 군의 컴퓨터 시스템에서 고려되어야 할 적극적인 보안 대책으로서 비인가자에 의한 침입의 탐지는 시급히 개발, 적용되어야 한다. 국방 분야에서는 각종 컴퓨터 네트워크가 각 제대별로 구축되어 활용중에 있고 이 네트워크를 통한 무기체계와 국방정보의 획득, 가공, 관리 및 활용등 광범위한 분야로 확대되고 있어 항시 적의 침입이 예상되고 있으므로 이를 탐지하고 침입으로부터 국방 전산자원을 보호해 줄 수 있는 시스템의 개발 및 적용이 시급하다.

본 논문에서는 예상되는 각종 침입에 대한 침입 유형 및 침입 기술을 고찰하고 감사기록을 활용하는 통계적 침입 탐지 및 규칙기반 침입 탐지 기법을 분석한 후 전산망의 보안 요구사항을 도출하여, 이를 바탕으로 효율적인 Man-machine 침입 탐지 시스템 설계를 제안한다.

2. 침입 유형 및 침입 기술

2.1 침입 유형

침입탐지에 대한 초기 연구는 컴퓨터 시스템 추적 데이터를 분석하는 방법에 대한 것으로 다양한 기준으로 추출되어 모아진 데이터를 사용하여 일괄처리 형식으로 설계되었다. 현재는 통계적 방법과 인공지능의 전문가 기법을 이용한 추론 방법을 이용한 실시간 귀납적 시스템에 대한 연구가 진행되고 있다. 위협탐지를 위한 검색 추적 분석에 사용될 수 있는 침입의 유형은 다음과 같다.

- 외부 침입자 : 컴퓨터 사용이 허락되지 않은자가 비밀키를 여러번 시도하거나 비밀통로 (covert channel)를 통해서 시스템에 침입하는 경우.
- 내부 침입자 : 비록 컴퓨터 사용은 허용되었지만 데이터, 프로그램 등의 특정 자원에 접근할 수 없는 자가 허락없이 침입하는 경우로서 다른 사용자의 비밀키를 사용하는 가면을 쓴 형태의 사용자와 엑세스 제어 메카니즘을 우회해서 자원에 접근하는자.

컴퓨터 시스템에 직접적인 침입뿐만 아니라 데이터 송수신시 네트워크상에 침입하여 여러가지 형태의 위협이 존재하는데 이를 살펴보면 다음과 같이 분류되어질 수 있다.

- 도청 : 파일의 네트워크 상에서 송수신시 가만히 엿듣고 만 있는 행위
- 변조 : 네트워크상에서 임의의 변조된 정보를 송신하는 행위
- 누출 : 네트워크 상의 정보를 도청하여 외부로 유출하는 행위

- 파괴 : 네트워크 선을 절단하여 송수신이 불가능하게 하는 행위

위의 분류중 본 논문의 연구 대상은 시스템에 직접 침입 유형을 대상으로 하는 탐지기법의 연구로 한정 하겠다.

2.1.1 패스워드 이용

1) 패스워드 구조

컴퓨터 자원을 활용하기 위해서는 합법적인 사용자나 혹은 불법적인 사용자(일명 해커)이든 시스템에 로그인 절차를 거쳐야 한다. 컴퓨터에 패스워드를 제시하는 것은, 정당한 사용자임을 증명하기 위함이다. 패스워드는 컴퓨터가 유저(user)의「정체」(identity)를 「인증」(authenticate)하기 위함[2]으로 정당한 사용자라고 인증되어야만 시스템 안으로 들어갈 수 있다. 즉, 침입자에 대한 방어의 최전선은 패스워드 시스템이다.

UNIX 시스템에서의 패스워드는 /etc/passwd 파일에 시스템내의 유저를 기록하고 있다. 이 파일에는 각 유저의 유저명, 이름, 식별정보 및 기본 어카운트 정보를 포함하고 있다.

UNIX 시스템에서의 패스워드는 8문자 길이까지의 패스워드를 선택할 수 있는데, 이것은 56비트의 값(7비트 ASCII사용)으로 변환되어 키로써 암호화 루틴에 입력된다. crypt(3)로 알려진 암호화 루틴은 National Institute of Standards and Technology(NIST)의 데이터 암호화 규격(DES)에 기초를 두고 있다.

2) 패스워드 추측 전략

그러나 실제적으로 사용자들이 사용하는 패스워드는 쉽게 기억할 수 있는 사용자 본인과 깊은 관계의 문자열을 사용하며, 더욱이 어떤 사용자는 그의 패스워드를 선택할 때 터무니없이 짧은 것을 고른다. 퍼듀(Purdue) 대학의 한 조사 결과 약 7,000명의 사용자 계정중 거의 3%가 3문자 내지 더 적은 문자로 되어 있었다[3]. 해커는 3문자 내지 그 이하의 문자 길이를 가진 모든 가능한 패스워드를 공격 한다면 가능한 문자와 숫자 조합으로 구성된 패스워드를 알기란 그리 오랜 시간이 걸리지 않는다. 한 가지 간단한 구제책은 시스템이 6문자 이하의 패스워드는 거절하도록 하거나 혹은 모든 패스워드의 길이가 정확히 8문자가 되게 요구하는 것이다.

일반적으로 보안에 관심이 없는 사용자들은 자신의 이름, 그들이 사는 거리의 이름, 평범한 사전어, 주민등록번호, 군번, 생년월일 등을 조합하여 선택한다. 이것은 즉시 O(n)에 의한 컴퓨터 수행시 패스워드를 해독할 수 있게 한다.

효과적인 패스워드 추측시 사용될 수 있는 단어는 다음과 같다.

- 단순히 숫자를 나열하라. 예) 1111
- 성, 본인 및 가족의 이름을 이용하라. 자녀가 많은 경우 장남과 장녀 혹은 막내의 이름을 이용하라.
- 전화번호, 주민등록번호의 끝자리, 군번, 주소, 생년월일, 자동차 번호를 이용하라.
- 취미, 아호, 별명, 고향 또는 저명한 지형지물, 졸업한 학교명을 이용하라.
- 유행어를 이용하라.
- 위 단어를 상호 순열에 의하여 수행하라.

2.1.2 침입 방법 (유닉스 시스템)

1) 패스워드 이용 침입

유닉스 시스템에서 해킹 방식이란 /etc/passwd를 이용해서, 패스워드를 알아내는

방식을 말한다. 현재 UNIX 의 패스워드 체계는 패스워드를 정하면 그 정한 패스워드가 저장되는 것이 아니고, 정한 문자열을 Cript에 의해 암호화 시켜서 /etc/passwd에 저장한 후, 나중에 로그인 할 때 유저가 암호를 입력하면 그것을 다시 암호화해서 문자열 비교를 행하는 방식으로 이루어진다. Cript 는 역함수가 존재하지 않는 방식이다. 일단 암호화 된 것은 그것으로부터 역으로 원래 입력한 문자열(raw password)을 유추해 내기란 거의 불가능하다.

현재 패스워드를 해독하는 방법은 수많은 단어 문자열들을 무작위로 넣어서 대응시키는 방법을 사용한다. 결국 해킹은 사전 파일을 가지고 사전 내에서 한 단어씩을 불러내 그것을 암호화하고 암호화된 문자열과 /etc/passwd 내의 문자열과 비교해서 찾아내는 방법을 사용한다. 해킹이 체크하는 순서는 ID 문자열을 변형시켜 문자열을 만들어 일단 대입한다. 그런 다음 ID 뒤에 숫자를 붙여 비교해 나간다. 하지만 다양한 숫자와 문자열 그리고 특수문자를 무작위로 결합하여 만든다면 조합의 가짓수가 기하급수적으로 증가되므로 찾아내기란 아주 어렵게 된다. 문제는 대부분의 사용자가 평소 친근한 단어를 이용하기 때문에 개인정보를 알면 패스워드를 유추하기란 그리 어렵지 않게 된다.

2) 프로그램들의 버그이용 침입

일반적으로 보안에 관심있는 시스템 관리자라면 자신의 패스워드를 쉽게 해독 가능한 패스워드를 사용하지 않을 것이다. 해커가 비록 일반 사용자의 패스워드를 해독해냈다 하더라도 시스템내의 많은 분야의 자원을 사용할 수는 없다. 하지만 시스템의 뒷문(back door)으로 알려진 버그를 이용한다면 슈퍼유저가 아니더라도 그 권한을 행사, 시스템을 해킹할 수 있게 된다. 그러므로 보안과 관련된 버그의 경우 해커의 공격 목표가 된다. 이전부터 유명한 sendmail debug에 관한 버그(해커가 root shell을 획득하게 하는 버그)나 tftp(Trivial File Transfer Protocol), at 버그, 인터넷 웜 사건에서 이용되었던 fingerd의 버그등이 한 예이다.

그러나 이들은 대부분 80년대 후반이나 90년대 초반에 너무나 유명해져버린 버그들로 지금은 모두 해결이 된 버그들이다. 그러나 운영자의 실수로 위의 버그들이 패치(patch)된 프로그램을 설치하지 않고 오래 전의 프로그램을 그냥 가져다 설치하는 경우 이런 버그로부터 해킹 당할 수 있기 때문에 주의를 요한다.

위의 예처럼 프로그램의 버그나 셋업 실수 등으로 보안상의 허점이 발생되었을 경우 이를 security hole이라 총칭한다.

3. 침입 탐지 기법

침입 탐지는 침입자의 행동이 합법적인 사용자의 행동과 다르다는 가정에 기초를 두고 있다. 물론 침입자에 의한 공격과 합법적인 사용자에 의한 자원의 평범한 이용 사이에 확실하고 정확한 구분이 어렵다. 침입 탐지 시스템의 설계자가 직면하고 있는 임무의 본질을 보면 전형적인 침입자의 행동이 합법적인 사용자의 행동과 구분되더라도 이들 행동에는 겹치는 부분이 있다. 그래서 침입자 행동의 부정확한 해석은 더 많은 정당한 사용자를 불법적인 침입자로 오인할 수 있다. 그래서, 실질적으로 침입을 탐지하는데 타협과 기술적인 요소가 필요하다. 앤더슨(Anderson)의 조사[4]에서는 적당한 확신을 가지고 위장된 사용자와 합법적인 사용자간의 차이를 구분할 수 있다고 가정했다. 합법적인 사용자 행동의 형태는 컴퓨터를 사용한 기록(audit record)을 관찰함으로써 만들어질 수 있고 그런 형태들로부터 중요한 이탈 행위가 발견될 수 있다. 앤더슨은 직권 남용자(불법적인 형태로 수행하는 합법

적인 사용자)를 발견하기는, 변칙적 행동과 정상적인 행동의 차이가 미미하다는 점에서 더욱 어렵다고 제시한다. 그런 위반은 단지 변칙적인 행동 조사를 통해서는 발견될 수 없다고 결론을 내렸다. 그러나 직권 남용자 행동은 그럼에도 불구하고 변칙 행동을 제한하는 어떤 조건 종류의 지능적인 정의에 의해 발견될 수도 있다. 마지막으로 비밀 사용자(clandestine user)의 탐지는 순전히 자동화된 기술의 범위 이상으로 느껴졌다.

침입 탐지를 위한 기본적인 툴은 감사기록이다. 사용자에 의해 진행 중인 몇몇 기록은 침입 탐지 시스템에 입력 자료로써 유지돼야만 한다.

감사 기록의 한 좋은 예는 Dorothy Denning에 의해 개발된 것이다[5]. 각 감사 기록의 필드는 다음과 같다.

Audit Record = { Subject, Action, Object, Exceptional-Condition, Resource-Usage, Time-Stamp }

- 주체(Subject): 행동의 창시자. 주체는 전형적으로 터미널 사용자이지만 사용자나 사용자 그룹을 대신해서 행동을 하는 과정도 될 수 있다. 모든 활동은 주체에 의해 발생되는 명령들을 통해 발생된다. 주체는 다른 접근 클래스로 그룹화될 수 있고 이런 클래스는 겹칠 수 있다.
- 행동(Action): 객체와 함께 주체에 의해 실행되는 작용. 예를 들면 로그인, 읽기, 입출력 수행, 실행등을 포함한다.
- 객체(Object): 행동의 수용체. 예를 들면, 파일, 프로그램, 메시지, 레코드, 터미널, 프린터, 사용자 혹은 프로그램 생성 구조들을 포함한다. 주체는 전자우편과 같은 어떤 행동의 수용자일 때 객체로 간주된다. 객체는 형태에 의해 그룹지울 수 있다. 객체 알갱이는 객체 형태와 환경에 의해 다양할 수 있다. 예를 들면, 데이터베이스 행동은 전반적으로 혹은 레코드 수준에서 감사 될 수 있다.
- 예외 조건(Exceptional-Condition): 만일 예외 조건이 있다면 복귀될 때 제시되는 것들을 나타낸다.
- 자원 이용(Resource-Usage): 각 요소는 몇몇 자원의 이용된 양을 표시하는 양적인 요소들의 목록(즉 인쇄된 혹은 디스플레이된 라인 수, 읽고 쓰여진 레코드의 수, 프로세서 타임, 사용된 I/O단위들, 경과된 세션 시간)
- 타임 스탬프(Time-Stamp): 행동이 발생 되었을 때 확인하는 유일한 시간과 날짜 소인

3.1 통계적인 이상 탐지(Statistical Anomaly Detection) 기법

침입 탐지에 대한 방법 중 하나인 통계적 이상탐지 기법은 일정 기간 동안 합법적인 사용자들의 행동에 관련된 데이터의 수집을 포함한다[6]. 그런 후 높은 수준의 확신을 가지고 합법적인 사용자 행동인지를 결정하기 위해 통계적인 테스트가 관찰된 행동에 적용된다.

통계적인 이상 탐지 기술들은 두가지 넓은 범주 즉, 임계치 탐지와 프로필-기반 이상탐지로 구분된다.

3.1.1 임계치 탐지

임계치(threshold) 탐지는 일정 시간 간격 동안 특별한 사건형태의 발생건수를 세는데 관계한다. 만약 수치가 발생 예상했던 정당한 수치를 능가 한다면 침입이 추측된다. 임계치 분석 그 자체로는 어느 정도 정교한 공격에 대해서 조잡하고 효과없는 탐지기이다. 임계치

와 시간 간격 둘 다 정해져야만 한다. 사용자의 가변성 때문에, 그런 임계치는 다수의 잘못된 긍정들이나 또는 잘못된 부정들을 만들어 낼 것 같다. 그러나 단순한 임계치 탐지기는 더욱 정교한 기술과의 결합에 유용할 수 있다.

3.1.2 프로필 기반 이상 탐지

프로필 기반 이상 탐지는 개인 사용자 혹은 사용자 관련 그룹들의 과거 행동을 특징지우고 그런 후 심각한 이탈 행위를 발견하는데 초점을 둔다. 프로필-기반 시스템은 파라미터들의 집합으로 구성될 수 있기 때문에 단지 단일 파라미터에서의 이탈 행위만을 갖고 경계 신호를 하는데 충분하지 않을 수도 있다.

이런 접근의 기본은 감사 기록의 분석이다.

첫째, 설계자는 사용자 행위를 측정하는데 사용될 정량적 계량 단위를 결정해야한다. 일정 시간 동안 감사 기록의 분석이 평균 사용자의 행동 윤곽을 결정하는데 이용될 수 있다. 그래서 감사 기록은 전형적인 행동을 정의하는 일을 한다.

둘째, 현 감사 기록은 침입을 탐지하는데 이용된 입력이다. 즉, 침입 탐지 모델은 평균적인 행동으로부터 이탈을 결정하기 위해 입력되는 감사 기록들을 분석한다.

프로필 기반 이상 탐지에 사용되는 계량단위들의 예는 다음과 같다.

- 카운터 : 관리행동에 의해 동작에서 리셋 할 때까지 증가하는 양의 정수. 예를 들면, 한 시간 동안 단일 사용자에 의해 로그인된 횟수, 단일 사용자 세션 동안 주어진 명령이 수행된 횟수 그리고 1분 동안 패스워드 실패의 횟수를 포함한다.
- 게이지(gauge) : 감소 또는 증가하는 양의 정수. 전형적으로 게이지는 몇몇 실체의 현재 값을 측정하기 위해 이용된다. 예를 들면, 사용자 응용에 할당된 논리적 연결의 수와 사용자의 처리를 위해 대기했다 나가는 메시지 수를 포함한다.
- 간격 타이머 : 두 관련된 사건 사이의 시간 길이. 예로, 한 계정에 연속적 로그인들 사이의 시간 길이이다.
- 자원 이용 : 특정 주기동안 소비된 자원의 양. 예로, 한 사용자 세션동안 인쇄된 페이지 수와 프로그램 수행에 소비된 총시간을 포함한다.

3.2 규칙 기반 탐지(Rule-Based Detection) 기법

규칙 기반 기술은 시스템에서 사건들을 관찰하고 활동이 주어진 패턴인지 혹은 의심스러운 패턴인지를 유도하는 규칙을 적용함으로써 침입을 발견한다.

규칙 기반 이상 탐지는 그것의 접근 발견과 장점의 견지에서 통계적 이상 탐지와 비슷하다. 규칙 기반 시도에서, 과거 감사 기록들은 이용 패턴을 확인하고 이런 패턴들을 기술하는 규칙들을 자동으로 만들어 내기 위해 분석된다. 규칙들은 사용자, 프로그램, 특권, 타임슬롯, 터미널 등의 과거 행동 패턴을 제시할 수 있다. 현재 행동이 관찰되고 각 트랜잭션은 과거에 관찰된 어떤 행동 패턴에 따른가를 결정하는 일련의 규칙들과 비교된다. 규칙 기반 탐지 기술들은 두가지 넓은 범주 즉, 이상 탐지와 침투 확인으로 구분된다

통계적 이상 탐지와 마찬가지로 규칙기반 이상탐지는 시스템내의 보안 약점들에 관한 어떤 지식을 요구 하지 않는다. 오히려 그 구조는 과거 행동을 관찰하고 미래가 과거와 같을 것이라고 추측하는 것에 기초를 둔다. 이러한 방법이 더 효율적이기 위해 더욱 큰 규칙 데이터 베이스가 필요하다.

규칙기반 침투확인은 침입 탐지를 위해 매우 다른 접근 방법을 취하고 있다. 이런 시스템은 알려진 침투, 또는 알려진 약점을 이용하는 침투를 확인하기 위해 규칙들을 이용하는 것이다. 행동이 설정된 이용 패턴의 제한 범위 안에 있을 때 조차도 의심스러운 행동을 확인하는 규칙이 또한 정의 될 수 있다. 전형적으로 이러한 시스템에 이용된 규칙들은 기계와 운영체계에 한정된다. 또한 이런 규칙들은 감사기록들의 자동화된 분석 방법이 아니라 "전문가"에 의해 생성된다. 일상 절차는 목표시스템의 안전을 위협하는 한짝의 알려진 침투 시나리오와 주요 사건을 수집하기 위해 시스템 관리자와 보안 분석가들과 인터뷰하는 것이다. 그래서 이 방법들의 효력은 규칙을 세우는데 관련된 기술에 의존된다.

IDES(Intrusion Detection Expert System)[5,7,8]에서 사용된 침투확인 구조는 다음과 같은 전략을 나타낸다. 감사기록은 그것들이 생성될 때 검토되고 그리고 그것들은 규칙기반에 대응된다. 만약 어울리는 한쌍이 발견되면 사용자의 의심율이 증가된다. 만약 충분한 규칙들이 대응되고, 비율이 제한 범위를 넘게 되면 비정상의 보고를 하게 된다. IDES방법은 감사기록의 검토에 기반을 둔다. 이것의 약점은 융통성 부족이다. 주어진 침투 시나리오에 대하여 약간 다르거나, 또는 복잡 미묘한 방식들로 각각 다양하게 생성될 수 있는 수 많은 감사 기록들이 있을 수도 있다. 명확한 규칙들에서 모든 이러한 편차들을 정확하게 정의하기란 어려울 수도 있다. 또 다른 방법은 특정 감사 기록에 독립적인 상위 수준의 모델을 개발하는 것이다. 이러한 예는 USTAT[9]로 알려진 상태 전이 모델이다. USTAT는 UNIX감사 메커니즘에 의해 기록된 구체적인 특정 행동들보다 일반적인 행동들에 관계된다. USTAT는 239개의 사건을 근거로하여 감사기록을 제공하는 SonOS 시스템에서 구현되었다. 단지 그러한 행동들과 포함된 파라메터를 사용하여 의심스러운 활동의 특성을 밝히는데 상태 천이 다이어그램이 개발된다. 수많은 감사할 수 있는 다른 사건들을 더 적은 수의 행동들로 표현 했기 때문에 규칙 생성 프로세스는 더 단순하다. 또한 상태 천이 다이어그램이 새로 학습된 침입 행동들을 수용하기 위하여 쉽게 수정된다.

4. 제안된 효율적인 침입 탐지 시스템 설계

4.1 전산망 보안 요구 사항

4.1.1 보안 위협의 형태

일반적인 정보 보호의 개념에는 정보가 외부로 노출되는 것을 방지하는 비밀성(confidentiality), 허가되지 않은 자에 의한 정보의 변조를 막는 무결성(integrity), 정보가 분실되지 않고 항상 존재하며 획득 가능한 상태를 의미하는 가용성(availability)의 구성요소가 있는데 이러한 비밀성, 무결성, 가용성은 여러가지 형태의 보안 위협을 받는데 위협의 형태는 크게 누출(disclosure), 수정(modification), 파괴(destruction), 불법 사용(illegal use)으로 분류할 수 있다.

Threats = { Disclosure, Modification, Destruction, Illegal use }

- Disclosure : 허가없이 외부로 유출하는 행위
- Modification : 불법적으로 임의의 내용을 변질하는 행위
- Destruction : 자원이나 시스템을 이용 불가 하도록하는 행위 즉 가용성 위협

행위

- Illegal use : 허가되지 않은자가 자원을 이용하는 행위

4.1.2 네트워크 운영 방법

제아무리 잘 만들어진 프로그램일지라도 100% 완벽하게 침입을 탐지할 수는 없다. 완벽한 탐지를 위해 지속적인 모니터링으로 이상 탐지시 정보 보안 담당관에의한 사용자 인증을 즉각 실시해야만 한다. 특히 국방분야의 Ⅰ급비밀은 그 유출시 관계국과 전쟁이나 국익에 심대한 손해를 미치게되므로, 철벽같은 보안을 유지해야만한다. 우선 가장 손쉬운 방법은 물리적으로 차단된(Off line) 형태로 운영해야하며, 다른 비밀 등급은 다음과 같이 보안위협에 대처된다면, 네트워크 상에서 운영이 가능 할 것이다. 표 1은 각 비밀등급에 따른 특성과 운영 방법을 나타내며 그림 4.1은 표1을 도식화하였다.

표 1. 비밀등급과 운영환경

비 밀 등급	특 성	운 영 환 경
Ⅰ급 (Top Secret)	국가의 존망에 관계된 정보 (전쟁유발, 외교단절)	물리적으로 차단된 시스템
Ⅱ급 (Secret)	국가의 전략적 정보 (군사상 막대한 영향 초래)	보안기능이 있는 컴퓨터 네트워크
Ⅲ급 (Confidential	전술적 정보 (군사상 해로운 결과 초래)	
대외비 (Restricted)	비밀은 아니지만 보호가치 있는 정보	
평문(Unclassified)	일반 정보	컴퓨터 네트워크

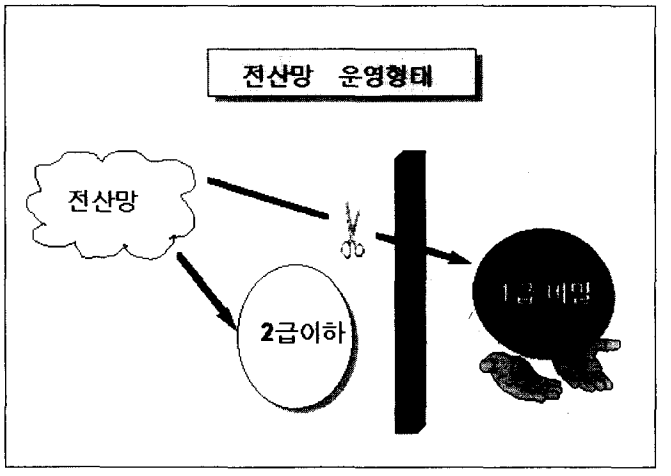


그림 4.1. 전산망 운영 형태

시스템 접근 방지나 데이터 보호는 사용자나 관리자의 보호하고자하는 의지가 가장 중요하다.

군에서 가장 중요시 하는 비밀의 누설확률은 누설자의 비밀인지도에 비례하며 다수인 경우는 인지자의 SP의 곱과 같다[11].

즉, SP (비밀 보호 확률) = 1- SN (비밀의 인지도)

$$P\ (\text{동시에 보호할 수 있는 확률}) = \prod_{i}^{n} SP_i (\text{단 } 1 \le i \le n)$$

비밀인지자 전원의 보호 노력이 요구되므로 비밀인지자를 가장 작게하는 것이 바람직하다.

4.2 침입 탐지 시스템 설계

이 절에서는 국방 전산 자원중 특히 데이터 파일에 대한 침입 탐지를 수행하는 전산망 침입 탐지 시스템을 설계한다.

4.2.1 설계 철학

침입자에 의한 공격과 합법적인 사용자에 의한 자원의 평범한 이용 사이에 확실하고 정확한 구분이 있다고 예상할 수는 없으나 침입 탐지는 침입자의 행동이 합법적인 사용자의 행동과 다르다는 가정에 기초를 두고 있다. 침입 탐지는 침입방어 시스템이 실패했을때 시스템의 제2방어노선으로 최근에 많은 연구의 초점이 되어 왔다. 이러한 관심은 다음의 이유로 증가되고 있다.

- 침입이 충분히 빠르게 탐지되면 시스템 손상전에 침입자를 축출시킬 수 있다. 그렇지 못한다 하더라도 최소한 피해를 줄일 수 있다.
- 효과적인 침입 탐지 시스템은 침입을 막는 억제책으로서 작동할 수 있다.
- 침입 탐지는 침입 기법에 관한 모든 정보를 모을 수 있도록 해주는데 이는 침입 탐지 기능을 강화시키는데 사용될 수 있다.

본 논문에서는 지금까지 설명된 사항들을 근거로 국방 환경의 특성과 현 기술 수준을 고려하여 실현가능성에 중점을 두고 국방 침입 탐지 시스템을 제안한다. 본 연구에서 제안하고자 하는 시스템은 규칙 기반 탐지 시스템으로 발견 명시 감사 형태의 레코드를 이용한다. 제안되는 시스템은 다음과 같은 배경하에서 연구되었다.

- Rule-based 기법 : 확정된 rule만을 근거로 한다. 즉 rule이 다이내믹하게 추가되거나 삭제되지않고 처음 정의된대로 유지 운용된다.
- 알려진 공격에 대해서만 탐지 수행 : 감사 데이터가 rule 에 의해 검사되므로 rule로 표현된 공격에 대해서만 탐지 가능하다.
- 수동(manual) 탐지기능 첨가 : 대부분의 침입탐지 시스템들이 침입 탐지 과정을 완전 자동화 하고 있는데 비해 본 연구에서는 수동 탐지 기능을 첨가하여 국방 환경에서 손쉽게 적용 가능토록 하였다.
- II급 및 III급 관리 : 본 연구에서 침입 탐지 대상으로하는 데이터 파일은 II, III 급 데이터 파일 이다.
- OS 액세스 메카니즘에 의한 침입 탐지를 검증 : 본 연구에서의 침입 탐지는 독립된 워크스테이션을 그 플랫폼으로

하여 rule base와 fact base를 운용함으로써, OS에 의한 침입 탐지를 우회 통과한 침입이나 misuse를 탐지하고 OS에 의한 제작업을 검증한다.

4.2.2 제안하는 Man-Machine 시스템 구조

제안된 전산망 침입 탐지 시스템은 앞에서 설명된 설계철학을 고려하여 2중적인 감시체계를 구비한 시스템으로 다음 그림 4.2.와 같이 구성된다.

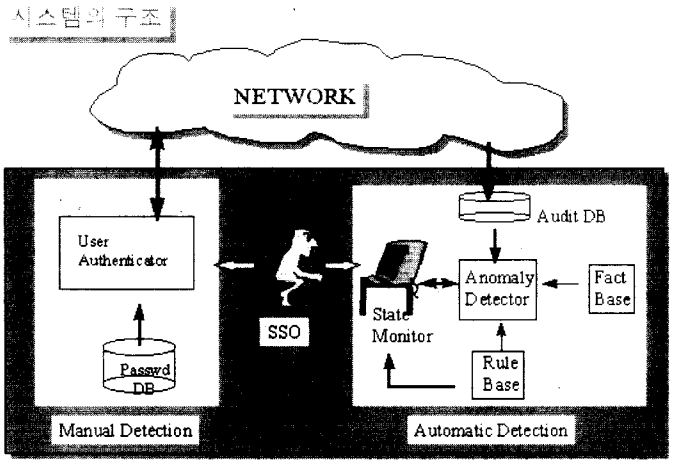


그림 4.2. 전산망 침입 탐지 시스템 구조

제안된 시스템의 주요 구성요소를 설명하면 다음과 같다.

1) Fact base : 데이터 파일과 사용자에 관한 각종 정보를 저장한다. 즉 데이터 파일에 관하여는 파일명, 파일 그룹 및 계층, 비밀등급, 운용가능시간 등에 관한 정보가 유지되고, 사용자에 관해서는 사용자 id, 그룹 id, 비밀권한 등에 관한 정보가 유지된다.
2) Rule base : 각 파일별로 비밀등급별 운용에 관한 정보가 저장된다. 이 정보들은 if_then 의 형태로 저장된다.

저장되는 rule은 다음과 같은 내용에 관한 것들이다.

- 사용자들은 다른 사용자의 개인 디렉토리에 있는 파일들을 읽지 말아야 한다.
- 사용자들은 다른 사용자들의 파일에 쓰지 말아야 한다.
- 로그인한 사용자들은 몇 시간 후에 그들이 전에 사용한 똑같은 파일들을 종종 접근한다.
- 사용자들은 직접 디스크 디바이스를 보통 열지 않고 상위 수준의 운영체제 유틸리티에 의존한다.
- 사용자들은 동일한 시스템에 한 번 이상 로그인을 하지 말아야 한다.
- 사용자들은 시스템 프로그램의 복사물을 만들지 않는다.

이러한 규칙들은 anomaly detector가 감사 데이터를 분석하여 침입을 발견하는데 사용된다.

3) Anomaly detector : fact base로부터 각 데이터 파일에 관한 정보와 rule base로부터 비밀등급별 운용에 관한 규칙과 감사 database 로부터 감사 레코드를 입력으로 받아 사용자의 액세싱이 침입이 아닌가를 검사한다. 이때 II급 비밀은 매 접근마다 모니터링하고 III급 비밀은 배치(batch) 형식으로 검사한다. 침입이 발견되면 state monitor로 디스플레이해 주고 벨을 울려 표시해준다.

4) 감사 database : 감사 데이터를 저장해 놓는 데이터베이스로서 이 데이터는 네트워크를 통하여 메인 시스템으로부터 전달받는다. 감사 데이터는 다음과 같은 항목을 갖는 레코드로 구성된다.

Audit Record = { Subject ID, Object ID, Operation, Access_time, Exception_Condition }

여기서 각 항목의 의미는 다음과 같다.

- Subject ID : 유니크한 사용자 id이다.
- Object ID : 사용자가 액세스하는 대상 즉 여기서는 파일의 유니크한 id이다.
- Operation: 사용자가 파일에 취한 행동으로 read, write, delete, copy, execute, modify등 여러 종류가 있다.
- Access_time : 사용자가 파일을 액세스하기 시작한 시간
- Exception_condition : 시스템에 의해 거부된 행위를 기술하는 것으로 이는 거부를 일으킨 명확한 이유뿐만 아니라 사용자의 의도도 추론하는데 쓰인다.

5) State monitor : SSO(Site Security Officer)와의 인터페이스로서 SSO는 이를 이용하여 anomaly detector가 발견한 침입에 대해 적절한 조치를 취한다. 이때 SSO는 rule base의 rule을 이용하여 분석 검증하거나 혹은 user authenticator를 이용하여 사용자를 직접 확인할 수 있다.

6) User authenticator : anomaly detector로부터 보고된 침입에 대해 사용자와 직접 교신을 통하여 침입 여부를 검증하는 모듈로서 SSO는 수상한 사용자에게 패스워드를 물어보고 이를 패스워드 DB의 패스워드와 비교하여 침입자를 식별해낸다.

4.2.3 구현문제

실시간 침입 탐지 시스템에서 사용 가능한 정보의 특성과 침입 탐지 관리 문맥 기반 성질은 규칙을 기반으로 하는 접근 방법에 적당하다. 문제 결정을 수행하기 위한 절차적 지식은 규칙에 근거한 시스템으로 구현될 수 있다. 규칙에 근거한 지식 베이스 시스템을 이용하여 병렬 탐지 과정에 대한 문제를 결정하기 위하여 추론 엔진을 사용한다. 일반적인 추론 시스템은 각 사용자 명령에서 일어나는 데이터를 사용하여 비정상적인 행위를 탐지하는 근원적인 증상을 제공하고 있다.

탐지 과정은 문제를 결정하기 위하여 추론 기관(Inference Engine)을 이용하고 있다. 일반적인 추론 시스템은 각 자원에서 발생된 데이터를 사용하여 잘못된 자원의 근원인 증상을 결정하는 것이다. 그러나, 네트워크 시스템에서 발생할 수 있는 침입 탐지의 요인은 감시를 하는 시스템에 의한 경고 보고 데이터의 처리 기능과 관련된 관리 기능의 협조를 통한 지식 베이스 그리고 이를 결정하는 규칙 베이스 시스템인 탐지기반 시스템의 탐지 프로세

스와 경고 발생 프로세스의 결정만으로 가능하다. 경고 발생 과정은 규칙 베이스에 근거하고 경고 발생 제안 구조를 사용하고 있다.

이러한 시스템을 구현할 때에는 다음과 같은 사항을 고려하여 구현하여야 한다.

- 실시간 문제 : 제안된 시스템은 배치뿐만 아니라 리얼타임으로 지원할 수 있어야 한다. 감사 데이터는 감사 DB에 저장 되는대로 즉시 읽혀 처리되어야 한다.
- 전문가 시스템 문제 : Rule base 에 포함되어야 할 rule의 선정과 이를 표현하는 방법이 명확하게 제공되어야 한다.
- 목표환경 : 제안된 시스템이 구현될 환경 즉 OS 및 하드웨어 환경이 고려되어야 한다. 또한 네트워크 환경도 매우 중요한 요소이다.
- 소스 코드 언어 : 시스템을 구현할 언어도 고려되어야 한다. 고급언어에 내장시켜 개발한다면 이러한 점도 간과되어서는 않된다. 특히 다른 사용자 도구와의 인터페이스 문제도 고려되어야 한다.
- 병렬환경 : 부하를 분산시키기 위해 CPU를 둘 이상 운용해야 할 필요가 있는가를 고려한다. 예를 들어 CPU가 둘인 경우라면 하나의 CPU는 감사 데이터를 모으는데 사용되고 다른 하나의 CPU는 감사 데이터를 처리하는데 사용될 수 있다.

5. 결 론

정보 보호는 보호하고자하는 의지가 충만되고, 제반 환경이 충족되었을때에 100% 완벽 방어된다. 특히, 2차대전의 유물인 이데올로기가 상존하는 한반도에서 적의 침입이 항시 예상되는 현 상태에서 우리의 안보의지는 더욱 굳건히 해야겠다. 국방 분야에서는 각종 컴퓨터 네트워크가 각 제대별로 구축되어 활용 중에 있고 이 네트워크를 통한 무기체계와 국방정보의 획득, 가공, 관리 및 활용 등 광범위한 분야로 확대되고 있어 항시 적의 침입이 예상되고 있어 이를 탐지하고 침입으로 부터 국방전산 자원을 보호해 줄 수 있는 침입 탐지 시스템의 개발 및 적용이 시급한 실정이다.

본 연구에서는 국방 전산 자원을 보호할 수 있는 전산망 침입탐지 시스템을 개발하기 위한 기초 단계로 기존의 침입 탐지 기법을 분석하고, 이를 근거로 전산망의 보안 요구사항을 도출하였으며, Man-Machine 침입 탐지 시스템을 설계하였다. 대부분 시스템 침입의 경우는 합법적으로 작업하는 사용자와는 현저하게 다른 작업을 수행함으로서 시스템상에서 탐지할 수 있으며, 컴퓨터 네트워크를 통해서 대상 시스템으로 부터 감사 레코드를 얻은 것으로 정보 보호에 위배되는 행위들을 실시간내에 탐지하기 위해 시스템과 정보보안담당관에의한 2중 감시체제를 구축하는 기법을 제공하였다. 본 논문의 결과는 허가없이 불법으로 사용하는 침입자와 정상적인 사용 환경에서 비정상적인 행위를 시도하는 부적절한 사용자를 탐지하여 경보하는 국방 전산자원 침입 탐지 시스템의 개발에 필요한 기반을 제공하나 향후 구현시 발생될 수 있는 문제점과 더욱 정확한 탐지 경보를 위한 모델의 세분화를 고려한 후속 연구가 진행되어야 한다.

참 고 문 헌

[1] 이재우외, "국내외 해킹현황 분석", 한국정보보호센타, 1996.

[2] 山口章生 역, Simon Garfinkel, Gene Spaford, "Unix Scurity", (일본) 주식회

사 아스키, 1993.

[3] 이서로외, "파워 해킹 테크닉", 파워북, 1995.

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

[5] Denning, D.E., "An Intrusion Detection Model", IEEE Transactions on Software Engineering, Feb. 1987.

[6] Stallings, W., "Network and Internetwork Security Principles and Practice", Prentice-Hall, 1995.

[7] Lunt, T.F., "Automated Audit Trail Analysis and Intrusion Detection", Proc. of the 11th National Comp. Sec. Conf., pp. 59-66, 1988.

[8] Lunt, T.F., "IDES: An Intelligent System for Detecting Intruders", Process of the Symp Computer Security, Threat and Counter measures, Italy, 1990.

[9] Pogras, P., "STAT: A State Transaction Analysis Tool for Intrusion Detection", Master's Thesis, Univ. of California at Santa Barbara, July 1992.

[10] 신장균, "컴퓨터 네트워크의 보안평가 기준 및 검증방법 연구", 육사 논문집 46집,pp281-305, 1994.

[11] 신장균, 박병호, 유진철, "컴퓨터 네트워크의 보안 품질", 한국통신정보보호학회 종합학술 발표회 논문집, vol.5, no.1, pp41-47, 1995.

[12] 박병호, 최병갑, 나민영, 신장균, "정보보호를 위한 전산망 침투탐지 모델 설계", 한국 CALS/EC학회 종합학술대회발표 논문집, pp251-268, 1996.

□ 著者紹介

신 장 균(終身會員)

1974年 陸軍士官學校 卒業
1979年 서울大 産業工學科 卒業
1983年 美 Wisconsin大(電算學 碩士)
1989年 高麗大 大學院(電算學 博士)
現 陸軍士官學校 電算學科 教授

※ 關心分野 : 運營體制 保安, 分散 시스템

나 민 영(會員)

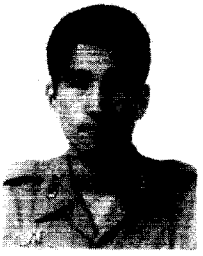
1978年 3月 陸軍士官學校 卒業
1983年 2月 서울大 컴퓨터工學科 卒業(學士)
1986年 2月 서울大 大學院 工學科 卒業(碩士)
1990年 12月 University of Florida 電算學科 卒業(博士)
1986年 ~ 現在 陸軍士官學校 電算學科 副教授

※ 關心分野 : 데이타베이스 시스템, 데이타베이스 保安, 分散데이타베이스

박 병 호(會員)

1983年 2月 檀國大 工科大學卒業(工學士)
1988年 2月 韓國外大 日語科卒業(語學士)
1995年 3月 東北大 大學院 情報科學研究科 卒業(電算學碩士)
1995年 4月 ~ 現在 東北大 大學院 情報科學研究科 博士課程

※ 關心分野 : 情報保護, 形式言語, CAI



최 병 갑

1987年 金烏工大 (電算學 學士)
1995年 美 Murray 洲立大 (電算情報學 碩士)
1995年 ~ 現在 陸軍士官學校 電算學科 專任講師

※關心分野 : 情報保護, 데이타베이스 시스템