通信情報保護學會誌
第3卷 第3號, 1993.9

침입 감지 모델 설정과 시스템의 분석

신종태*, 이대기*

이 논문에서는 고도의 정보보호를 필요로 하는 문서나 시스템에 대한 불법 행위를 막을 수 있는 침입 감지 시스템을 설계함에 있어 필요한 시스템 모델의 구성요소를 분석하였다. 또한 외국에서 개발되었거나 개발 중인 침입 감지 시스템들을 소개하였다. 전산망이나 컴퓨터 시스템에 있어 신분확인과 외부의 침입을 막기 위한 1차적인 방어 수단이 되지만 이러한 것들이 타협이나 공모에 의해 파괴되었을 때 이러한 침입 감지 시스템은 큰 역할을 수행하게 된다. 앞으로 다양한 형태의 내부적/외부적 침입 행위와 컴퓨터 시스템을 악용하려는 모든 행위를 즉각적으로 감지하는 기능을 수행하는 실시간 침입 감지 시스템에 대한 연구가 절실히 요구될 것이다.

1. 도 입

컴퓨터 기술과 통신 기술의 발달은 고도의 정보 통신망을 이룩하는데 지대한 공헌을 하였다. 고도의 정보 통신망의 실현은 인류에게 신속하고 정확하게 처리할 수 있도록 유용한 정보를 제공하였다.

그러나 이러한 장점의 이면에는 컴퓨터 통신망을 통한 정보의 위조 및 도청 등의 불법 행위로 인한 많은 문제점들이 대두되었다. 특히 고도의 정보보호를 필요로 하는 문서나 시스템에 대한 불법 행위는 엄청난 피해를 동반하고 있으며 이러한 사례는 급증하고 있다. 전산망이나 컴퓨터 시스템에 있어 신분확인과 액세스 제어 기술은 외부의 침입을 막기 위한 1차적인 방어 수단이 되지만 이러한 것들이 타협이나 공모에 의해 파괴 되었을 때의 피해는 매우 증폭되어진다. 그러므로 이러한 침입을 감지하는 시스템의 개발을 요구하게 되었으며 기존의 auditing 기법에 전문가 기법, 통계적 기법, 인공 지능적 기법 등 여러 첨단 기술을 적용한 시스템을 개발하게 되었다.

따라서 이러한 침입을 분석하고 감지하여 문제점을 사전에 방지하는 침입 감지 시스템을 설계하는 기술은 각종 주요 컴퓨터 시스템에 응용될 것이며 정보 시스템의 안전도 향상에 크게 기여할 것이다.

본 논문에서 사용되는 용어 가운데 외부 침입자라 함은 컴퓨터 시스템의 사용을 허락받지 않은 침입자를 말하며 내부 침입자라 함은 컴퓨터 시스템의 사용을 허락 받았지만 특별히 데이타, 프로그램, 자원 등의 사용이 허락되지 않은 침입자를 나타낸다.

* 한국전자통신연구소

2. Intrusion Detection 모델

2.1. 모델 설정의 기본 개념

Intrusion Detection 모델 설정의 기본적 개념은 일상적이고 표준적인 동작을 잘 감시하여 정해진 규칙(rule)에 잘 부합되는지를 확인하도록 하는 것이라 할 수 있다. 이는 다음의 그림으로 설명될 수 있으며 방지기법으로는 audit trail, 암호화 등을 비롯하여 각종 보안 서비스를 들 수 있으며 위협 요소는 우연적인 실수와 악의적인 공격 그리고 하드웨어 결함 등에 이르기까지 전반적으로 고려되어야 한다.

2.2. 모델의 주요 구성 요소

일반적인 Intrusion Detection 전문가 시스템에 있어 주요한 구성요소로는 subject, object, 감사 레코드, profile, 비정상 행동 레코드, 규칙 등 6가지로 나누어 나타낼 수 있다.

Subject는 사용자를 말하며 object는 화일, 명령어, 장치 등의 자원을 나타낸다. 감사 레코드에는 대상 시스템에서 생성한 object에 대한 subject의 행동이 수록되어 있으며, object에 대한 subject의 행동을 결정하는 구조인 profile은 template에서 자동으로 생성되어진다. 비정상 행동 레코드는 이러한 행동이 검출될 때 생성되며, 규칙은 사전에 설정된다.

2.3. Subject와 Object

Subject는 모든 동작의 초기 주체로서 터미날 사용자, 프로세스, 시스템 등을 들 수 있다. 그러므로 모든 동작은 subject에 의해서만 시작되며 subject는 그룹으로 설정함이 가능하다.

Object는 동작을 받는 대상이며, 화일, 프로그램, 메세지, 레코드 등을 들 수 있고 그룹으로 설정함이 가능하다.

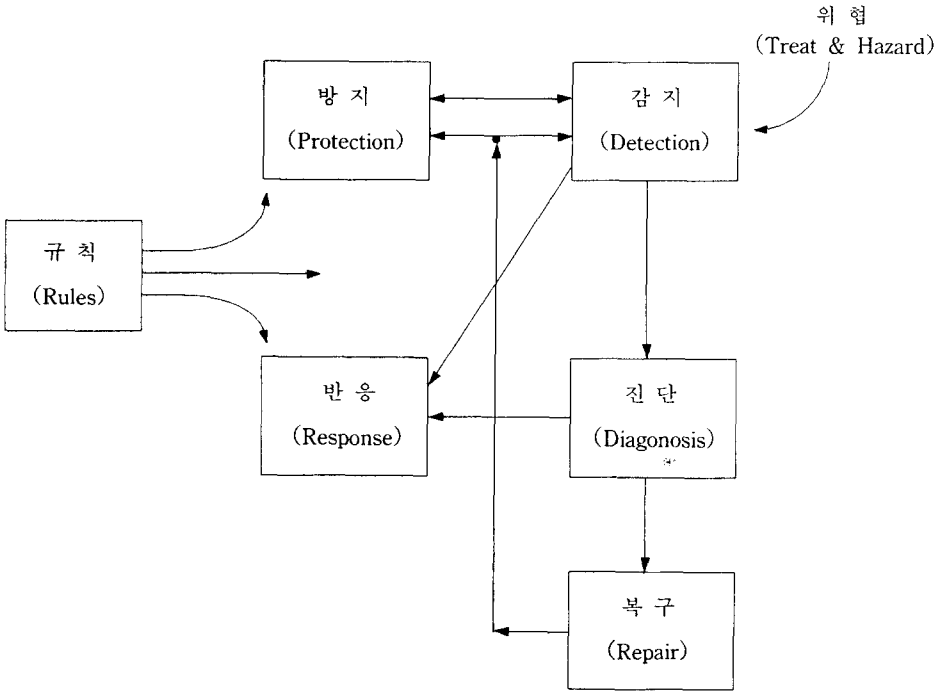
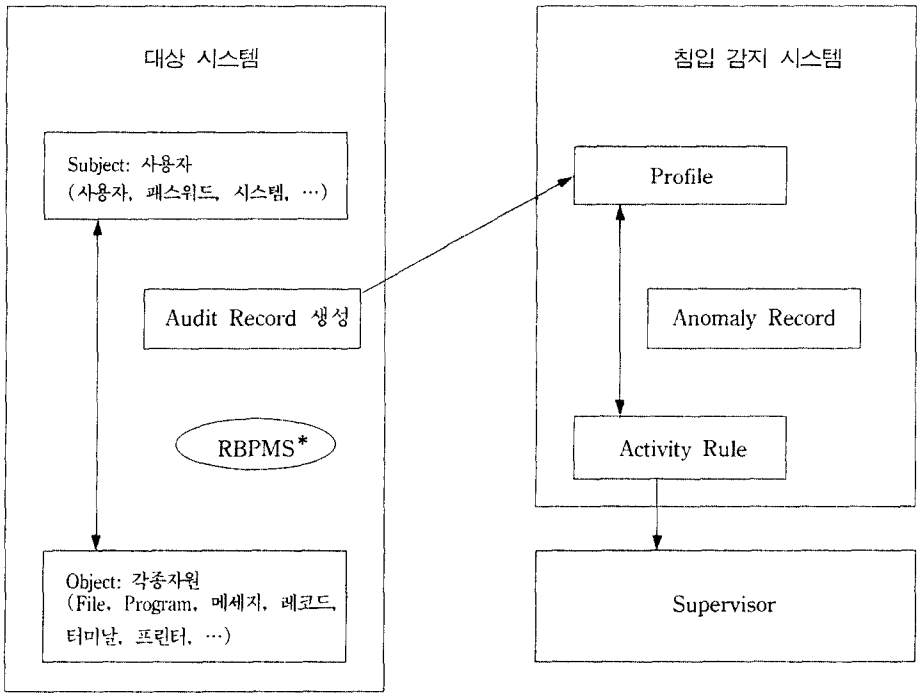


그림 1. 침입 감지 시스템 개념도



* RBPMS: Rule-based Pattern Matching System

그림 2. 침입 감지 시스템의 주요 구성 요소

2.4. 감사 레코드

수행된 행위에 대한 감사 기능으로 생성된 감사 레코드에는 대상 시스템에서 생성한 object에 대한 subject의 행동이 수록되어 있다. 감사 레코드는 subject, action, object, 예외조건, 자원 사용, 시간 스탬프 등 6개 tuple들로 구성되어 있다. 여기서 action은 subject에 의해 수행되는 operation을 나타내며, 자원 사용도는 사용된 CPU시간이나 I/O unit 등의 정량적인 값을 의미하며 시간 스탬프는 action이 발생한 시간을 나타낸다. 모든 activity는 object action으로 분해되어 단일 object인 감사 레코드로 수용된다.

기존의 감사 기법에서의 문제점으로는 수행되는 모든 형위에 대한 감사를 수행하지 않고 명령어 등의 특정한 것만을 검사함과 또한 subject 필드가 포함되지 않고 설명 정보도 매우 부족함을 들 수 있다.

2.5. Profile

Subject와 object의 집합체로 object에 대한 subject의 행동을 결정하는 구조인 profile은 10개의 구성요소를 가지며 이들은 변수 이름, 행위 패턴, 예외 패턴, 자원 사용 패턴, 측정을 위한 시간 간격을 나타내는 주기, metric과 통계적 모델의 특별한 타입을 정의하는 추상적인 데이타 타입을 나타내는 변수 타입(예 : 평균과 표준편차 모델을 갖는 이벤트 가운터), 통계적 테스트에 사용된 제한값이나 상한값이나 표준편차 등을 나타내는 threshold, subject 패턴, object 패턴, 이전의 값들의 분포 상태를 나타내기 위해 통계적 모델에서 사용되며 카운트나 합 등을 의미하는 측정 value 등을 들 수 있다.

2.6. 비정상 행위 레코드

침입 감지 시스템이 구동되면 행위 규칙에 의해서 activity profile을 갱신하고 변칙적이거나 비정상적인 행동이 검출될 때 비정상 행위 레코드를 생성한다.

본 레코드는 event, 시간 스탬프, profile 등으로 구성되어 있다. 비정상을 일으킨 event에는 audit 레코드에서 발생되는 비정상 행위에는 'audit'로, 현 interval 동안에 사용된 데이타에서 발생되는 비정상 행위에는 'period'로 나타낸다. 이에 따라 시간 스탬프에는 audit 레코드에 대한 시간 스탬프나 interval 정지 시간이 기록되고 profile에는 비정상적으로 검출된 activity profile의 이름이 수록된다.

2.7. 행위 규칙

침입 감지는 사전에 설정된 행위규칙에 따라 감사 레코드와 profile의 패턴을 비교함으로 수행된다.

행위규칙은 audit 레코드 규칙, 주기적 행위 갱신 규칙, 비정상 레코드 규칙, 주기적 비정상 분석 규칙으로 구분되며 각 규칙들은 조건 부분과 본체 부분으로 구성되어 있다.

Audit 레코드 규칙은 새로운 audit 레코드와 activity profile의 패턴이 일치될 때 발생되며 profile을 갱신하거나 예외적으로 수행되는 행위를 검사하여 비정상적인 요소가 발생되면 비정상 레코드를 생성한다. 주기적 행위 갱신 규칙은 클럭 주기가 수행된 후에 발생되며 profile을 갱신하거나 예외적으로 수행되는 행위를 검사한다.

비정상 레코드 규칙은 새로운 비정상 레코드가 규칙에서 주어진 패턴과 일치될 때 발생되며 보안 담당자에게 발생 사실을 알리는 메세지 출력을 수행한다.

주기적 비정상 분석 규칙은 interval이 마지막일 경우에 interval이 수행된 후에 발생되며 주기에 대한 비정상 레코드들을 분석하여 보안 담당자에게 비정상 행위에 대한 긴급보고 메세지를 출력한다.

3. Profile의 통계적 모델

Object와 subject에 관련된 특정한 행위를 수록한 activity profile에는 signature, 정규 activity의 description 등이 포함되어 있다. 이렇게 관찰된 것은 통계적 metric 형태나 통계적 모델 형태로 변환된다.

Metric 모델에는 한 주기 동안 발생한 감사 레코드의 수를 나타내는 event counter, 관련된 event들 사이의 시간길이를 나타내는 간격시간, 한 주기 동안 행위들에 의해 소비된 자원의 양을 나타내는 자원 measure 등이 수록된다.

통계적 모델은 새로운 측정값을 이전의 측정값과 비교하여 정상 여부를 결정한다. 이용 가능한 모델로는 operational 모델, 평균과 표준편차 모델, Multivariate 모델, Markov Process 모델, Time Series 모델 등이 있다.

Operational 모델은 제한값을 미리 계산하여 정해놓고 새로운 측정값을 제한값과 비교하는 모델이며 패스워드 실패의 수에 대한 event counter와 같은 Matric 모델 형태처럼 경험적으로 침입을 예측하게 된다.

평균과 표준편차 모델은 비정규적인 행위를 평균과 표준편차에 의한 신뢰구간으로 결정하는 모델이며 event counter, intenval time, resource measure 등에 적용이 가능하다. 이 모델은 operational 모델의 제한값을 정하기 위한 정규 activity에 관한 사전 지식이 없어도 가능하며 신뢰구간이 측정된 데이타들에 의존함으로 사용자별로 다르게 정의될 수 있게 된다. 하지만 오래된 측정값과 최근의 측정값이 같은 영향을 줄 수 있으므로 이를 보완하여 최근 측정값에 더 많은 가중치를 주도록 설계할 수 있다.

Multivariate 모델은 두개 이상의 metric들이 상호 관계를 갖는 것으로 표준편차 모델을 이용하며 경험적인 데이타가 여러 측정값들의 조합에서 더 좋은 식별력으로 얻어지는 결과를 이용하여 결정하는 형태의 모델이다.

Markov Process 모델은 event counter에만 적용되는 모델이며 상태 변수가 event 형태가 되며 상태 사이의 전이 빈도를 상태 전이 행렬로 구성된다. 이 모델은 명령어 순서가 중요한 명령어들 사이의 전

이를 조사함에 유용하게 사용된다.

Time Series 모델은 관찰된 측정값 각각의 순서와 도착 시간 간격을 이용하여 결정하는 모델이다.

4. 주요 침입 감지 시스템

4.1. IDES

IDES(Intrusion Detection Expert System)는 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 환경 등에 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 메카니즘을 제공하는 것을 목적으로 한다. 즉, 시스템 사용자의 행위가 지금까지 시스템을 사용한 여러 형태들에서 추론하여 기대된 행위로부터 이탈한 정도가 크거나 전문가 시스템 규칙에 근거하여 미리 설정한 규칙에 위배되는 경우 이를 비정상적인 행위로 결정하고 이를 시스템에 알리어 해당 조치를 수행하게 된다.

그리하여 IDES는 profile된 통계적 subject 지식베이스를 유지한다. 이러한 profile에는 침입 감지 measure들의 집합 각각에 대하여 기대되는 subject의 행위들이 수록되어 있다. 시스템에는 내부와 외부의 침입을 감지 하기에 충분한 양의 데이타가 저장되어야 하겠지만 시스템 기억용량의 한계로 인하여 과거 행위 데이타를 저장하는 것보다는 profile들이 도수표, 평균, 분산 등을 유지하고 통계학을 이용하여 행위의 적법성 여부를 결정하게 된다. 결과적으로 침입이라는 것은 사용자의 비정규적인 행위에서 발견되며 대상 시스템에서 공급되는 audit 레코드들에서 추론되어 진다.

4.2. MIDAS

MIDAS(Multics Intrusion Detection and Alerting System)는 미국 정부 Multics 시스템을 모니터하기 위하여 NCSC(National Computer Security Center)가 개발한 침입 감지 시스템으로 NCSC의 네트워크 main frame에 대한 침입과 오용을 실시간으로 감지하여 알려준다. 이 시스템도 SRI의 D. Denning과 P. 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 profile은 LISP 구조로 되어 있다. Denning의 침입 감지 모델을 근간으로 하여 compiling, debugging 등의 각종 메카니즘들을 제공하는 전문가 시스템 셸인 P-BEST(Production-Based Expert System Toolset)라는 도구들을 사용하여 개발되었으며 사용자 명령어 레벨에서 모니터 한다.

4.3. NAURS

NAURS(Network Auditing Usage Reporting System)는 MILNET과 ARPANET에 대한 터미날 접근 제어 시스템과 연동되어 사용되고 있으며 TAC(Terminal Access Controller)들과 NAC(Network Access Controller)들로부터 발생된 네트워크 행위를 감시한다. NAURS는 TAC/NAC login, 행위와 실패, logouts, open and close connections, 온라인 상태의 TACs 등에 관한 데이타를 수집하고 이를 데이타베이스 형태로 유지관리한다.

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 프로토타입은 호스트(SRI-NIC)와는 분리된 시스템으로 구동되었으며 네트워크 사용자가 file 이동이나 원거리 login 등의 접근을 할 수 없도록 설계되어 있다. 이 프로토타입에서 장치의 축소화, 기능의 분배, 침입의 실시간 감지 능력, 감사 데이타베이스의 축소화 등을 부가하여 실용 생산품으로 개발하였다.

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 감지할 수 있다. 이를 위해 Discovery는 서비스 형태와 접근 방법에 의해 사용자 profile을 개발하고 사용자의 여러 행위가 발생할 때 마다 사용자의 profile을 갱신한다.

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

4.5. NADIR

NADIR(Network Anomaly Detection and Intrusion Reporter)는 하나의 운영체제에 대한 침입 감지와는 반대로 전산망의 침입 감지 문제를 해결하기 위하여 미국의 NL(National Laboratory, Los Almos)에서 시험적으로 개발한 침입 감지 시스템이다. NL의 주 전산망인 ICN(Integrated Computing Network)의 안전을 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. 운용하는 중 예외적인 행위가 NADIR에 의해 감지되었을 때에는 해당사항을 운용요원에 알리고 악의적인 행위의 발견을 위해 관련 tool이 실행되게 한다. 이 시스템은 외부의 '해커' 뿐만 아니라 특권을 지닌 내부자의 오용도 감지할 수 있도록 설계되었다.

NADIR은 대상 시스템의 행동을 모니터하여 감사 레코드를 수집하는 데이타 수집 부문을 비롯하여 프로화일을 생성하는 데이타 처리 부문, 전문가 규칙을 적용하여 결과를 생성하는 침입 감지 부문, 상태를 나타내고 이면분석(background analysis)을 수행하는 사용자 인터페이스 부문, 특별한 침입에

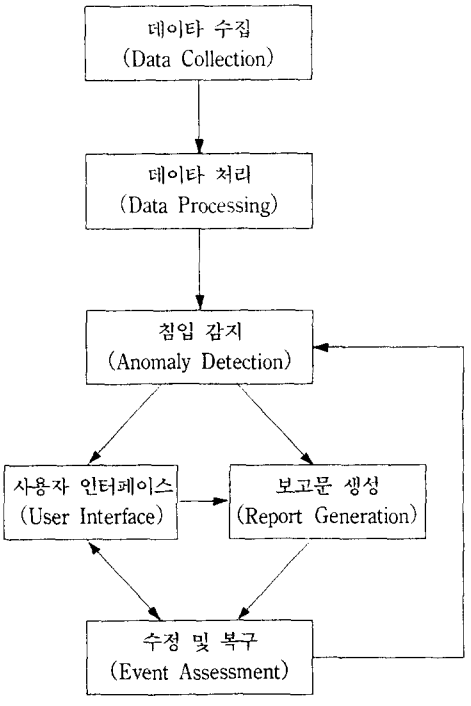


그림 3. NADIR의 기본 동작 개념도

대한 보고문을 주기적으로 생성하는 보고문 생성 부문, 수정 복구 등 6개 부문으로 기능적으로 나눌 수 있다. (그림 3)은 이러한 부문별 상호 동작 및 연관 관계들을 나타내고 있다.

5. 결 언

보다 강력한 침입 감지 시스템은 대상 시스템의 약점을 모르는 상황에도 침입의 감지가 가능해야 한다. 이는 이러한 약점을 이용하는 특별한 행동을 관찰하지 않고도 감지가 가능해야 함을 의미한다.

침입 감지 시스템을 연구함에 있어 시스템 설정을 위한 접근 방법에 있어 해결해야 할 것으로는 완전성과 적시성의 고려, 통계적인 모델 설정, profiles, 시스템 설계기법 및 구현 등을 비롯하여 난제들이 매우 많다. 한편으로 안전성을 보다 강화시키는 방법으로 protection을 위한 별도의 계층을 생각할 필요가 있다.

앞에서 제시한 여러 침입 감지 시스템들은 어느 것도 모든 위협을 감지하기에 충분하지는 않다. 성공적인 침입 감지 시스템을 설계하기 위해서는 제시한 여러 접근 방법들이 잘 융합되고 병합되어야 한다고 생각한다. 침입을 나타내는 규칙을 바탕으로 하는 통계적 사용자 profile 접근 방법은 특히 효율적인 결합이 요구되어진다.

그러므로 보다 강력하게 침입을 감지하는 시스템을 구성하기 위해서는 통계적 접근 방법을 사용하는 시스템과 또 다른 접근 방법을 채택한 시스템을 결합하여 사용하거나 병합된 별도의 시스템을 개발함이 합리적일 것이다.

참 고 문 헌

1. [DENN87] Dorothy E. Denning, "*An Intrusion Detection Model*", IEEE Trans. S. E., 1987.2.

2. [JAVI91] H.S. Javitz, A. Valdes, "*The SRI IDES Statistical Anomaly Detector*", 1991 IEEE S&P, 1991.5.

3. [LUNT88] Teresa F. Lunt, R. Jagannathan, "*A Prototype Real-Time Intrusion Detection Expert System*", 1988 IEEE S&P, 1988.7.

4. [LUNT90] Teresa F. Lunt, Ann Tamaru, etc, "*IDES : A Progress Report*", 6th IEEE CSAC, 1990.12.

5. [GARV91] T.D. Garvey, T.F. Lunt, "*Model-Based Intrusion Detection*", 14th NCSC, 1991.10.

6. [VACC89] H.S. Vaccaro, G.E. Liepins, "*Detection of Anomalous Computer Session Activity*", 1989 IEEE S&P, 1989.7.

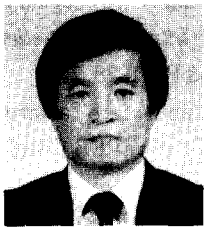
7. [LIEP89] G.E. Liepins, H.S. Vaccaro, "*Anomaly Detection : Purpose and Framework*", 12th NCSC, 1989.10.

8. [MILL91] Boddy G. Miller, Paul E. Proctor, "*A Requirements-Oriented Analysis of Computer Misuse Detection Systems*", I. D. Workshop, 1991.5.

□ 著者紹介

辛 宗 泰

1982년 2월 서울大學校 師範大學 數學科 卒業(理學士)
1987년 8월 崇實大學院 電子計算學科 卒業(工學碩士)
1984년 2월～현재 韓國電子通信研究所 符號技術部 先任研究員



李 大 基

1962년 2월 漢陽大學校 電子工學科 卒業(工學士)
1987년 2월 漢陽大學院 電子工學科 卒業(工學碩士)
1966년 2월～1980년 2월 遞信部 通信技佐
1980년 2월～현재 韓國電子通信研究所 符號技術部 部長