네트워크 패킷을 기반으로한 실시간 침입 탐지 시스템

*이경하, **은유진, **김기현, **임채호 *정태명
*성균관대학교, **한국정보보호센터

Real-Time Intrusion Detection System based on Network Packets

*K. H. Lee, **Y. J. Eun, **K. H. Kim, **C. H. Lim, **T. M. Chung
*SungKyunKwan University, **Korea Information Security Agency
khlee@yeonam.skku.ac.kr, silver@kisa.or.kr, danny@kisa.or.kr,
chlim@certcc.or.kr, tmchung@simsan.skku.ac.kr

요 약 문

인터넷의 역기능 현상으로부터 시스템을 보호하고 소유한 정보를 지키려는 노력은 다양한 보안 시스템의 개발로 이어졌다. 보안 시스템은 시스템을 기반으로 한 것과 네트워크를 기반으로 한 것으로 나눌 수 있는데, 본 논문에서는 네트워크 기반의 보안 시스템을 설계하였고, 설계된 시스템으로부터 가능한 침입탐지 기술들을 언급하고 있다.

1. 서론

소수의 단체나 특정 국가에 의해 시작되었던 정보화는 지금 우리가 살고 있는 현대 문명의 발전에 큰 비중을 차지하고 있다. 수많은 국가들의 정보화를 위한 노력은 많은 사람들에게 다양한 종류의 서비스를 제공하고 있으며, 보다 손쉬운 정보 교환을 가능하게 하였다. 한편, 인터넷을 이용한 정보 교환은 사용자들에게 많은 편리를 가져왔으나, 정상적인 서비스 방해, 시스템내의 중요한 데이터 파괴, 불법접속과 같은 인터넷의 역기능 현상으로 인한 피해도 발생하게 되었다. 이러한 역기능 현상으로 인한 피해가 확산됨에 따라, 보다 안전한 인터넷 사용을 위한 여러 가지 보안 기술들에 대한 연구와 개발이 진행되게 되었다.[1][3][5][16]

침입탐지 시스템(Intrusion Detection Systems)이란 '컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 규정하는 시스템으로, 가능하면 실시간으로 처리하는 시스템'을 말한다.[4][12] 이러한 침입 탐지 시스템은 역기능 현상으로부터 안전한 정보 관리와 시스템 보호를 목적하며, 침입행위들을 감시하고 침입자의 불법 접속을 탐지보고 한다. 또한, 로그 파일이나 응용 프로그램들의 취약점들, 기타 침입흔적에 대한 점검을 통하여 시스템의 보안성을 유지하게 한다. 일반적으로, 침입 탐지 시스템은 시스템을 기반으로 하는 것과 네트워크를 기반으로 하는 것으로 크게 둘로 나눌 수 있다.

- 시스템을 기반으로 하는 침입 탐지 시스템은 파일 점검 및 각 어플리케이션들의 버전 확인 등을 통한 취약점 점검들을 실행함으로 시스템의 불법 사용에 대한 점검과 예방을 목적으로 하고 있다. 하지만, 침입에 대한 실시간적인 침입탐지를 제공하는 것이 어렵다는 것과 불법 침입자들이 로그 파일들을 조작할 경우 침입 판정에 대한 정확성을 줄 수 없다는 단점이 있다. COPS[9][15], SATAN[15], TIGER[15]와 같은 '시스템 취약성 점검 도구들'은 시스템을 기반으로 하는 침입 탐지 시스템의 기능을 수행하는 보안 시스템이다.

- 네트워크를 기반으로 하는 침입 탐지 시스템은 네트워크 상에 있는 패킷을 이용한 침입을 탐지하는 시스템으로 침입탐지에 따른 빠른 응답시간을 제공한다. 즉, 실시간적인 침입 탐지 및 처리를 할 수 있으며 침입에 대한 적극적인 대응과 실패한 접속에 대한 정보 수집이 가능하다는 장점이 있다.

침입 탐지를 위해 개발되어진 시스템을 보면[4], 외부에서 시스템 내부로 침입과 내부적 위협을 감시하는 SRI International의 IDES(Intrusion Detection Expert System)[19], 알려진 침입 패턴만을 탐지하는 실시간 침입탐지 시스템으로서 Porras가 Penetration State Transition Analysis라는 모델에서 만든 STAT(State Transition Analysis Tool)[13], 미 NCSA(National Computer Security Center)에서 Multics를 사용하는 네트워크 환경을 위해 개발된 MIDAS(Multics Intrusion Detection and Alerting System)[13], Smaha에 의해 제시되어 미 공군을 위해 개발된 Haystack과 같은 침입탐지 시스템들이 있다[4][12]. 또한 상용화되어 있는 제품으로써, ISS(Internet Software Solution)에서 제공하고 있는 'Real-Secure'는, 네트워크 패킷들에 대한 분석을 통하여 기본적인 침입을 탐지 할 수 있도록 개발되었다.

본 논문에서는 IP 패킷헤더의 정보와 패턴매칭을 이용하여 침입이라고 판정할 수 있는 유형들을 분류하고 각 유형에 대한 탐지 방법과 이러한 유형의 침입들을 효과적이면서도 실시간적으로 탐지할 수 있는 네트워크기반의 침입탐지 시스템 모델을 제시하였다. 본 논문의 내용은 2장에서 침입 탐지 시스템의 전체 모델을 제시하며, 3장에서는 전체 시스템에서의 각 부분 모듈에 대한 설명을, 4장에서는 헤더의 정보를 이용한 침입 탐지 항목들과 각 항목들에 대한 구체적인 설명들을, 그리고 마지막으로 5장에서 앞으로 연구해야 할 과제와 결론순으로 구성하였다.

2. System Design

본 시스템은 네트워크 패킷을 기반으로 하는 침입탐지 시스템 모델로서, 패킷 정보를 이용하여 침입 여부를 탐지하고 침입에 대한 적절한 조치를 실시간적으로 취할 수 있도록 설계되었다. 특히, 침입을 탐지하는 부분에 있어서는 침입 항목과 검색 시간을 고려하여 그 기능을 모듈화 하였다. - 만일 모듈화된 기능들을 좀더 확장한다면, 로컬 네트워크내의 여러 호스트에서 분산실행도 가능 할 것이다.[10]

전체시스템의 구성은 침입과 관련된 자료 수집을 위해 네트워크 인터페이스 장치로부터 IP 패킷들을 감시하는 패킷 스캐너(Packet Scanner)와, 주어진 침입 항목으로부터 침입여부를 판단하는 분석기들

(Analyzers) 그리고, 사용자와 분석기(Analyzer) 그리고 실행 관리자(Action manager) 사이에서 침입 관련 사항을 처리하는 중간조정기(Coordinator), 사용자로부터 침입에 대한 대응방법을 처리하는 실행 관리자(Action manager)로 이루어져 있다.

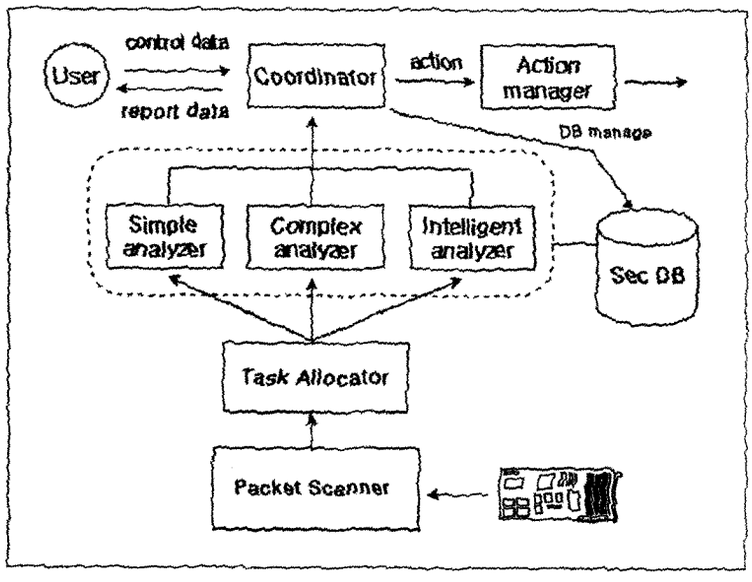

그림 1. 전체 침입 탐지 시스템 모델

3. 침입탐지 시스템의 상세 모듈들

본 장에서는 위에서 제안한 네트워크를 기반으로 한 침입 탐지 시스템의 각 모듈들이 어떠한 기능을 가지고 동작하는지, 각 모듈들에 대한 자세한 사항들을 살펴보기로 한다.

3.1 패킷 스캐너(Packet Scanner)

'그림 2'에서 보여주고 있는 패킷 스캐너는 로컬 네트워크 상에 있는 여러종류의 패킷들 중에서 해당 시스템에 접속하는 패킷을 수집하여 전달하는 모듈이다. 수집되는 패킷들은 1차 필터링(filtering)과정에서 TCP, UDP, ICMP 패킷들과 같이 자주 시스템 침입에 사용되는 패킷들을 추출하여 작업 할당기(Task Allocator)로 전송되고, 전송 후 분석기에서 요구하는 침입 판정 자료로서 사용된다.

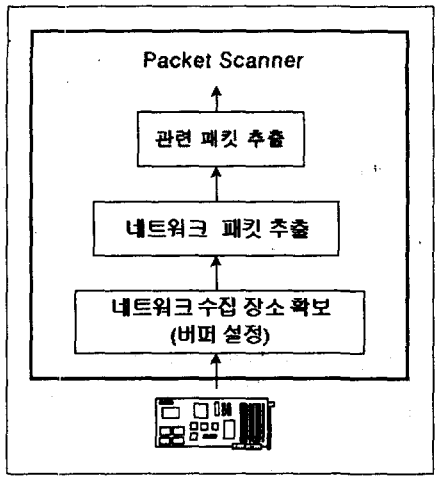

그림 2. Packet Scanner

3.2 작업 할당기(Task Allocator)와 침입관련 정보 수집

작업 할당기는 패킷 스캐너로부터 1차 필터링된 패킷들을 침입탐지 관련 항목 점검에 따른 복잡성과 검색에 소요되는 시간을 기준으로 분류되어진, 단순 분석기(Simple Analyzer), 고난도 분석기(Complex Analyzer), 그리고, 지능형 분석기(Intelligent Analyzer) 중에 선택되어진 한 분석기로 전송되며, 선택되어진 분석기에서 침입 여부를 조사 받게 된다. 여기에서 사용되고 있는 각각의 분석기들이 하는 일들은 다음과 같다.

- 단순 분석기(Simple Analyzer) : 패킷내의 단순 정보만을 이용하여 SecDB에 저장되어 있는 침입 판단의 근거가 되는 자료와의 비교를 통하여 외부로부터의 침입 여부를 탐지한다. 고난도 분석기(Complex Analyzer)와 지능형 분석기(Intelligent Analyzer)와 비교할 때, 가장 빠른 응답시간을 제공할 수 있다. 단순 분석기에의해 점검되는 내용들은 Simple Protocol Probing, Source Probing, Well-Known Port Probing, 특정 Port를 이용한 Service Probing 등과 같은 점검 항목들이 있다.

- 고난도 분석기(Complex Analyzer) : 패킷 헤더로부터 침입과 관련된 여러 정보를 종합하거나, 혹은 특정 패킷에 관한 축적된 정보를 분석하여 시스템내의 침입을 탐지한다. 그리고, 일정 시간 동안 특정 항목을 감시하여 얻은 정보를 근거로 하여 침입여부를 판정한다. UDP Packet Field Probing, 특정 Port를 이용한 Service Counting Probing, 정보 유출 가능한 서비스에 대한 탐지, 간단한 Pattern Matching등은 고난도 분석기에 의해 실행되는 기술들이다.

- 지능형 분석기(Intelligent Analyzer) : 지능형 분석기는 침입을 탐지함에 있어, 단순 분석기나 고난도 분석기보다 많은 정보가 필요하다. 또한, 정확한 침입 탐지를 위해서는 패킷 전송자로부터 침입 탐지와 관련한 사전 정보 제공과 패킷 전송경로와 관련한 약간의 추가적인 정보뿐만 아니라, Expert System과 같은 지능적 처리가 요구된다. 다른 분석기보다 침입 여부에 대한 분석이 복잡하며, 수집된 정보를 근거로 한 사용자의 침입 탐지 정책이 있어야 한다. Source Routing, Complex pattern matching과 같은 기술은 여러 정보를 종합하여 분석함으로써 침입을 판정하게 된다.

3.3 중간조절기(Coordinator)

중간조절기는 사용자와 분석기들과 관련하여, 각 모듈들 사이에서 전송 및 수신되는 메시지들을 처리하는 모듈이다. 중간조절기는 메시지를 교환하는 대상에 따라 동작하는 기능도 조금씩 차이가 있는데, '표 1'에서 중간 조절기의 역할들을 살펴보면 다음과 같다.

침입분석기와 중간조절기	• 각 분석기들로부터 침입판정에 따른 자료를 전송 받는다.
사용자와 중간조절기	• 각 분석기로부터 전송받은 침입관련 자료를 임의의 보고형식을 사용하여 사용자에게 보고한다. • 사용자로부터 침입에 대한 적절한 조치 방안을 입력받거나, Secure DB에 침입과 관련된 특정 데이터를 삽입 혹은 삭제 등의 관리하기 위한 데이터를 입력받는다.
실행 관리자와 중간조절기	• 사용자로부터 입력받은 제어 데이터를 실행 관리자에게 전송한다.
SecDB와 중간 조절기	• 사용자로부터 전송받은 제어 데이터(Control Data)를 이용하여 데이터 베이스를 관리한다

표 1. 중간조절기 동작

3.4 실행 관리자(Action Manager)

실행 관리자는 사용자의 요구와 침입에 따른 대응행동을 처리하는 모듈이다. 여기에서 침입 대응 행동에 대한 결정은 사용자에 의해 결정되어 진다. '표 3'의 내용은 실행 관리자 내부에서 실행되는 각 기능들이다.

- 침입에 대한 대응 : 실행관리자는 침입 판정후, 침입에 대한 대응행동을 취한다. 대응행동의 방법으로는 침입자로 확인되거나, 침입에 대한 시도를 하는 사용자에게 경고 메시지를 전송하는 소극적인 방법과 현재 시스템 내부의 사용자가 침입관련 행동을 할 때, 관련 사용자를 로그 아웃 시키거나 침입이라 판정되는 패킷을 제거하는 적극적인 방법이 있다.

- 다른 보안 모듈과의 상호 협조 : 침입탐지 시스템은 독립적인 모듈로서 보안을 유지하기보다는 다른 보안 모듈과의 협조를 통하여 보안성을 더욱 높일 수 있다. - 역추적 시스템과의 협조를 통한 침입자에 대한 추적, 다른 시스템에게 필요한 정보제공 등.

3.5 Secure Database(SecDB)

SecDB(보안 데이터 베이스)는 단순 분석기, 고난도 분석기, 지능형 분석기가 침입을 탐지할 때, 침입 판정의 근거 자료들을 제공한다. Private DataBase인 SecDB의 데이터들은 내부적으로 침입 패턴 유형, Configuration data, Source Address, Destination Address, Port, Routing information과 같이 여러개의 데이터 베이스로 세분화되어 관리된다. 또한, 침입자들에 대한 추가 정보나 새로운 침입탐지 항목의 삽입 또는 침입 자료로서 의미가 없어진 자료의 삭제등, 침입 관련 데이터의 관리, 유지보수가 사용자에 의해 가능하도록 설계되었다.

4. 네트워크 패킷정보를 이용한 침입 탐지 기술

인터넷에서 사용되는 정보들은 수많은 패킷들도 구성되어 송/수신되는데, 불법 접속자들 역시 인터넷에 접속 후, 일반 사용자들이 사용하는 동일한 경로와 패킷들, 때로는 비정상적인 패킷들 - 패킷 필드를 조작한 패킷들 -을 이용하여, 시스템 내부로 침입한다. 만약 인터넷에서 사용되는 수많은 패킷들 중, 불법 접속자들이 침입을 목적으로 사용되는 패킷이 어떤 패킷인지, 어떤 유형의 패킷이 침입 시도에 사용되는지를 알 수 있다면 관련 패킷들을 조사함으로써 시스템의 보안성을 높일 수 있을 것이다. 본 장에서는 3장에서 언급한 각 분석기들의 침입 항목들에 대한 구체적인 내용들과 특히, 패킷의 IP 헤더 정보를 이용[17][18], 침입이라고 판단 할 수 있는 침입 탐지 기술들에 대하여 살펴보고자 한다.

4.1 Protocol Probing

정보를 교환함에 있어 두 지점사이(전송자와 수신자)에서 패킷 전송/수신에 따른 프로토콜의 사용은 필수라고 할 수 있다. 네트워크에서 사용되는 프로토콜들은 현재 RFC 1700에 등록되어 있는 프로토콜들 이외에도 특정목적을 위해 사용되거나, 새로이 만들어 사용하고 있는 프로토콜들이 있다. 침입자는 현재 사용중인 프로토콜을 이용한 침입이나 새로운 프로토콜을 이용하여 시스템 내부로 침입할 가능성이 있는데, Protocol Probing은 이러한 침입에 대한 탐지를 목적으로 한다.

- Unknown Protocol Probing : RFC에 등록되어 있지 않은 프로토콜이나 각 시스템의 '/etc/services'에 등록되어 있지 않은 프로토콜 이외에 시스템의 이상을 일으킬 수 있는 알려지지 않은 프로토콜을 탐지한다.[18]

- Specific Protocol Probing : 특정 프로토콜을 사용하여 시스템에 이상을 유발하는 경우를 탐지 한다. 예를 들어 UDP 경우, UDP 패킷의 각 field에 삽입되어 있는 값들이 기준값을 만족시키는지를 조사한다. UDP Bomb과 같은 침입 수법을 사전에 탐지 할 수 있다.

4.2 IP Address Probing

인터넷에서의 주소는 정확한 정보를 송/수신함에 필수적이다. 정보 전송에 사용되는 패킷 헤더에는 전송지 주소(Source Address)와 목적지 주소(Destination Address)가 입력되어 이러한 패킷들을 요구한 주소지로 전송하게 된다. 패킷 내의 주소들은 침입 탐지의 자료로서 활용될 수 있는데, 그 방법들은 다음과 같다.[2][6][7][8][11]

- Non-acceptable Host's Address : SecDB에 의해 관리되고 있는 침입자가 주로 활동하는 네트워크 혹은, 호스트의 주소를 이용하여 침입을 탐지한다.

  - Source Address : 침입자들이 주로 활동하는 호스트 혹은 네트워크의 전송지 주소를 갖고 있는 패킷들과 침입 시도에 대한 가능성이 많은 호스트들의 주소를 탐지한다.
  - Destination Address : 침입을 목적으로 사용되고 있는 웹 호스트처럼, 감시가 필요한 호스트나 네트워크로 접속을 시도하는 패킷을 점검한다. 내부의 사용자가 침입을 목적으로 하는 정보 수집을 위하여 해킹 호스트에 접근하는 것을 탐지하여, 추후 침입시도를 대비하여, 특별 감사나 관리를 함으로 시스템의 보안을 유지한다.

- Unspecified Address : 침입자가 침입을 목적으로 인증되지 않은 호스트를 이용하거나 패킷의 주소 부분을 조작하여 침입을 시도하는 것을 탐지한다.

  - Unknown Source Address : IP 패킷 필드내의 Source Address의 주소가 인증된 네트워크 주소가 아니라면, 침입자가 역추적을 피하기 위하여 Source address field에 임의의 주소를 조작하여 시스템 내부로 침입할 가능성과, 침입을 목적으로 임의의 주소를 할당한 호스트를 이용하여 침입 할 가능성을 탐지한다.
  - Source and Destination Address : 패킷은 게이트웨이(Gateway)나 라우터(Router)에 통하여 목적지가 있는 로컬 네트워크로 전송되어지는데, 로컬 네트워크에서 외부로 전송되는 패킷의 주소는 반드시 내부에 있는 호스트의 주소가 입력되어지게 된다. 하지만, 내부 사용자가 침입을 목적으로 침입자의 위치나 신분을 은폐하기 위해 Source Address와 Destination Address

의 주소 모두 외부 네트워크 주소로 조작할 수 있는데, 이를 탐지한다.

4.3 Port Probing

- Well-Known Port

  - IANA(Internet Assigned Numbers Authority)에 의해 할당된 특정 서비스들은 0 ~ 1023 port 번호를 사용하도록 예약되어져 있다. 이외의 1024 이상의 번호를 갖는 port들은 시스템에 의하여 할당되어 지는데, 이들 well-known port이외의 port로 접속을 시도하는 패킷은 시스템의 감시를 피해 시스템 내부로 침입하려는 침입자의 시도일 수도 있다. 이를 방지하기 위해 Well-Known Port 이외의 port접속을 탐지한다.

- 특정 Port에 대한 감시

  - 서비스에 대한 감시 : 침입에 취약한 서비스에 대한 침입시도. 네트워크를 이용한 서비스들 중, R-계열의 서비스들이나 시스템내의 중요한 정보들이 쉽게 노출될 위험이 있는 서비스들을 이용한 침입을 탐지한다. - CERT문서나 보안관련 문서에서는 몇몇 서비스들에 대해서는 제공하지 않는 것이 바람직하다고 언급하고 있다.

- 횟수(Counting)에 의한 감시 : 특정 서비스의 사용량을 증가시켜, 시스템 자원을 고갈시킴으로 정상적인 서비스를 방해하는 침입에 대한 것을 탐지한다.

4.4 Pattern Matching

침입자가 어떤 시스템에 대하여 침입시도를 하려 할 때, 사용되는 특정 유형들에 대한 패턴을 탐지한다.[3][8][14]

- FTP : '/etc/ftpusers'에는 시스템의 보안을 목적으로, 몇몇 ID를 이용한 FTP 서비스의 사용을 제한하였다. 침입자는 관리자의 실수나 시스템의 오류로 발생 가능한 사항들에 대하여 사전 점검을 시도하는데, 이러한 시도를 사전에 탐지한다. FTP 서비스에 있어서는 사용이 제한된 ID는 다음과 같다. - root, uucp, bin, daemon, etc

- TELNET : guest, anonymous와 같은 정확한 신분 인증과정 없이 접근하는 사용자에 대한 불법적인 시스템 사용에 대한 사전방지와 root로 접근 시도를 하여 취약점을 조사하려는 시도를 탐지한다.

- MAIL : 특정 ID(사용자)에 대한 탐지. 메일을 통하여 내부에서 외부로, 외부에서 내부로의 침입에 대한 탐지를 한다.

- 기타 : 이외에도 침입의 가능성이 있는 패턴들을 가진 패킷을 구분하여 침입여부를 판정한다.

4.5 Source Routing

IP 헤더의 option field를 검사하여, 라우팅 경로(routing path)에 대한 옵션이 있는 지를 확인하여, 옵션이 셋(set)이 되어 있으면 침입에 대한 점검을 실시한다.

- 침입을 목적으로 라우터에 의해 패킷이 제어되는 것을 피하기 위해, 의도적으로 라우팅 경로를 조작했는지를 점검한다.

- 라우팅 경로에 의심스런 경로 - 해커들이 주로 사용하거나, 특정 gateway에 대한 경로 - 가 있는지를 점검한다. 또한, 사전에 축적되어진 정보를 기반으로, 예상 라우팅 경로 이외의 경로가 패킷 내의 라우팅 경로에 포함되어 있는지를 점검한다.

5. 결론

네트워크를 기반으로 하는 침입탐지 시스템은 시스템을 기반으로 하는 침입 탐지 시스템과 비교시, 부분적으로 축적된 자료를 사용하는 몇몇 침입 탐지 항목들에 대한 침입 여부를 판정함에 있어 약간의 시간이 필요하지만, 일반적으로, IP 패킷 분석을 통하여 침입에 대한 빠른 탐지를 할 수 있다는 점과 시스템 내부로 침입을 하는 것에 대한 탐지는 물론, 침입을 시도했으나 실패한 경우에 대한 탐지도 가능하다는 장점이 있다.

본 논문에서 제안한 네트워크를 기반으로 하는 침입탐지 시스템은 시스템의 확장성을 고려하여, 침입 항목들을 특성에 맞게 분류하고 각 선택되어진 침입탐지 분석기에서 침입탐지를 수행할 수 있도록 설계하였다. 또한 침입에 대한 대응조치 및 사용자가 침입 탐지관련 자료에 대한 관리가 가능하도록 하였으며, 추가적인 보안 모듈과의 자료협조에 대한 부분 역시 고려하여 설계하였다. 이러한 점들은 추후 전체 보안 시스템과 각 분석 모듈들의 분산 실행에 있어 보다 쉬운 확장성을 제공할 것이다.

시스템 기반의 침입탐지 시스템과의 통합, SecDB에서의 자료 검색을 위한 효율적인 알고리즘 개발, 침입관련 자료(로그 파일)의 증가로 인한 디스크 용량문제, 네트워크를 기반으로 하는 침입탐지에 따른 전체 시스템에 미치는 Overhead, 분석기 기능 향상 - 특히 지능형 분석기(Intelligent Analyzer)에서의 추가적인 침입 탐지 항목 개발 - 등은 향후 좀더 연구되어 할 과제이다.

" 본 연구는 '97년 정보통신 국책과제인 대규모 전산망에서의 침입 탐지를 위한 기본 시스템 개발 과제로서 수행중입니다"

6. 참고 문헌

[1] 정보과학회지, 보안기술 , 통권95호, Apr 1997

[2] 김정훈, Internet Firewall, 정보처리학회지, vol4 No2 March,1997

[3] 한국정보보호센터, 정보시스템 해킹 현황 및 대응, Nov, 1996

[4] 한국정보보호센터, 침입 탐지 모델 분석 및 설계, Sep, 1996

[5] 변경근 외, 전산망 보안점거 도구의 설계 및 구현, 한국정보보호학회 종합학술대회 논문집 Vo.6 No1,

[6] Atkins, Buis, Hare, Nachenberg, Kelley, Nelson, Phillips, Ritchey, Steen, Internet Security, New Riders Publishing, 1996

[7] B.Corbridge, R.Henig, C.Slater, Packet Filtering in an IP Router, LISA V-Sep.30-Oct.3,1991

[8] D.B. Chapman, Network (In)Security Through IP Packet Filtering, Sep,1992

[9] D. Farme and E. Spafford The COPS Security Checker System, USENIX Conference Proceeding, Anaheim, CA, 1990

[10] G. Bruce, R. Dempsey, Security in Distributed Computing, Prentice Hall, 1997

[11] Hare, Siyan, Internet Firewalls and Network Security, New Riders Publishing , 1996

[12] O. Kyas, Internet Security, Thomson,1997

[13] S. Castano, M. G. Fugini, G. Martella, P. Samarati, DATABASE SECURITY, Addisonwesley, 1995

[14] S. M.Bellovin, Packets Found on an Internet, Aug, 23, 1993

[15] S. Garfinkel and G. Spafford, Practical Unix security, OReilly & Associates, Inc.,1991

[16] S. M. Bellovin, Security Problems in the TCP/IP Protocol Suit, April 1989

[17] Safford, Schales, Gess The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment, USENIX, 1993

[18] Stevens, TCP/IP Illustrated Volume 1, Addison Wesley ,1994

[19] T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey, " A REal-Time Intrusion Detection Expert System (IDES) - Final Technical Report", Computer Science Laboratory, SRI International, Menlo Park, California, Feburary 1992.