2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

침입탐지시스템 패러다임의 변천 과정 및 발전방향

엄정호*, 정태명
성균관대학교 전기전자 및 컴퓨터공학부
e-mail:jheom@rtlab.skku.ac.kr

Transition and development of Intrusion Detection System's paradigm

Jung H. Eom*, Tai M. Chung
School of Electronical & Computer Engineering,
SungKyunKwan University

요약

본 논문에서는 현재 침입차단시스템과 더불어 관심이 고조되고 있는 침입탐지시스템 패러다임의 변천과정과 발전방향에 대해 설명하였다. 침입탐지시스템의 역사와 개념을 간략히 설명하였으며, 네트워크 기술의 발달로 침입탐지시스템의 탐지대상과 방법의 변천과정을 설명하였다. 또한, 현재 연구/개발되고 있는 침입탐지시스템들의 양상이 독창적이고 지능적으로 고도화되는 침입형태에 따라 하이브리드형과 구조 통합형으로 변화하고 있다는 것을 제시하고 있다. 그리고 현재 개발되고 있는 침입탐지시스템들의 한계점과 문제점을 지적하였다. 마지막으로 한계점을 극복하고 문제점을 해결할 수 있도록 향후 연구/개발되는 침입탐지시스템이 갖추어야 할 기능을 제시하였다.

1. 서론

네트워크가 발전함에 따라 정보 통신 기술은 가히 혁명적인 발전을 거듭해 왔으며, 특히 인터넷의 발전은 데이터 전송 속도의 고속화, 대용량의 데이터 전송 등을 가져와 업무 효율을 향상시키고 정보화 사회로의 변화를 가져왔으며, 국가 경쟁력을 강화시켜 주는 긍정적인 효과를 거두고 있다. 그러나, 인터넷의 확장으로 인한 시스템의 불법 침입, 중요 정보의 유출 및 변경·훼손, 불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등 역기능도 인터넷 기술의 발전과 더불어 날로 증대되어 피해 규모가 심각한 수준에 이르고 있다. 특히, 악의적인 사용자들에 의한 독창적이고 지능적인 형태의 불법침입 기술이 개발, 사용하고 있는 지금, 이에 대한 대응책은 그 어느 때보다 절실히 요구되고 있다.

이에 정보보호의 중요성이 부각되고 있는 가운데 보안 대책이 시급히 마련되고 있는 실정이다. 특히, 이러한 기술 중의 하나인 침입탐지 기술은 침입 차단 기술과 함께 안전한 정보화 환경 구축을 위해 주목받는 기술 중의 하나가 되고 있다. 현재는 초기의 침입탐지시스템의 단점을 보안하고 다양해지고 있는 침입에 대해 능동적인 대처할 수 있고, 대규모 네트워크 상에서도 효율적으로 탐지할 수 있는 침입탐지시스템에 대한 연구가 지속되고 있다.

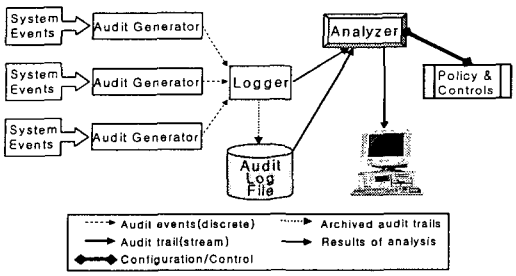
본 논문에서는 대표적인 보안 시스템의 한 분야이며 차세대 네트워크 보안에 해결책으로 각광받는 침입탐지시스템에 대해서 다룰 것이다. 2장에서는 침입탐지시스템의 역사 및 기본 개념을 간략히 설명하고, 3장에서는 현재 개발되었거나 연구중인 침입탐지시스템의 양상에 대해 살펴보고, 4장에서는 침입탐지시스템의 현재 동향 및 한계와 발전방향을 제시하고, 5장에서는 결론을 맺는다.

2. 침입탐지시스템의 역사 및 개념

2.1 침입탐지시스템의 역사

2.1.1 침입탐지 시스템 개발 이전

침입탐지 이전에는 감사(audit) 시스템이 사용되었는데, 감사는 시스템 이벤트의 시차별 기록을 생성, 기록, 검사하는 것을 의미한다. 이 당시 감사 시스템의 주목적은 시스템 운영에 대한 사용자 책임을 할당 및 유지, 이벤트 재작성, 피해평가, 시스템 문제점 감시, 피해복구, 시스템의 부적절한 사용을 탐지하는 것이었다. 감사 시스템의 구조는 [그림 1]과 같이 감사기록 생성기, 기록기, 분석기, 그리고 보고 체계로 되어 있으며, 수동 및 컴퓨터 프로세싱이 가능하였다[1].



[그림 1] Audit System 구성

2.1.2 침입탐지시스템의 태동

1970년대 컴퓨터의 속도, 크기, 수가 증가함에 따라 컴퓨터 보안에 대한 요구가 확연히 증가하였으며, 70년대 후반에는 정부기관과 EDP(Electronic Data Processing) 상업기관이 모여서 보안, 감사, 통제에 대한 정의를 보고서로 생산하였다. 그 무렵 DOD(The U.S. Department of Defense)에서도 군관련 컴퓨터 시스템 사용이 증가하면서 보안 메커니즘로써 컴퓨터 감사에 대한 관심이 증가하였다.

1980년, Anderson은 Reference Monitor 개념을 발표했는데 여기서 처음으로 침입탐지 개념을 사용하였으며, 컴퓨터 감사 메커니즘을 컴퓨터 문제 발생시, 컴퓨터 보안 담당자에 의해 사용될 수 있도록 정보로 변경하자는 제안을 하였다. 또한, 불필요하고 관련성 없는 보안감사 기록을 제거하는 감사축약이라는 용어를 제시하였다.

1980년 중반 Dorothy Denning과 Peter Neumann은 IDES(Intrusion Detection Expert System)이라는 실시간 침입탐지시스템을 개발하면서 본격적인 연구가 시작되었다. 그 이후, 미 국방성, DARPA, SRI/CSL, COAST에 의해 주도적으로 침입탐지시스템에 대한 연구가 활발히 진행되었다[1].

2.2 침입탐지시스템 개념

2.2.1 침입탐지시스템의 정의

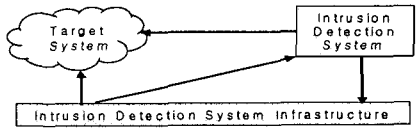
1980년에 Anderson은 침입탐지에 대한 개념을 처음으로 사용하였다. 그는 침입을 정보 접근, 정보 조작, 시스템 무력화 등에 대한 고의적이면서도 불법적인 시도로 정의하였으며, 여기서 침입은 비밀성, 무결성, 가용성을 훼손하려는 시도를 의미한다. 침입탐지 시스템은 이러한 침입을 목적으로 특정 시스템에 불법적으로 접속하여 시스템을 사용, 오용, 남용하는 것을 감지하고 문제점을 처리하는 시스템이라 정의하고 있다. 즉, 침입탐지 시스템이란 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말한다[2]. 침입탐지시스템의 기본 개념은 감시, 보고, 대응 요소로 다음과 같다[3].

① 감시(Monitor) : 목표 시스템 활동에 대한 정보 를 감시하고 조사한다.

② 보고(Report) : 목표 시스템 활동에 대해 수집 한 정보를 IDS 하부구조에 보고한다.

여기서 하부구조란, 시스템 보안/보호 기능을 가 지고 있는 시스템이라 할 수 있다.

③ 대응(Response) : 보안 취약점을 줄이거나 보안 사고에 대해 대처하는 것이다.



[그림 2] 침입탐지시스템 개념도

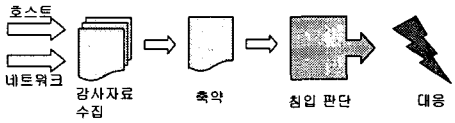
2.2.2 침입탐지시스템의 구성 요소

이러한 개념을 가지고 설계된 침입탐지시스템의 구성요소는 감사 자료의 수집 및 축약, 침입 판단, 그리고 대응이며, 각 단계별 기능은 다음과 같이 수행한다[4].

① 감사자료 수집 및 축약 : 침입판단의 근거가 되 는 감사자료(Audit Data)를 수집하고 불필요한 자료를 축약하는 단계이다.

② 침입판단 : IDS의 핵심과정으로 수집, 축약된 감사자료를 갖고 있는 침입유형과 비교함으로써 침입여부를 판단한다.

③ 대응 : 침입에 따른 대응을 수행하는 단계이다.



[그림 3] 침입탐지시스템의 구성요소

2.2.3 침입탐지시스템의 필요성

침입탐지시스템의 역할은 다음과 같다[5].

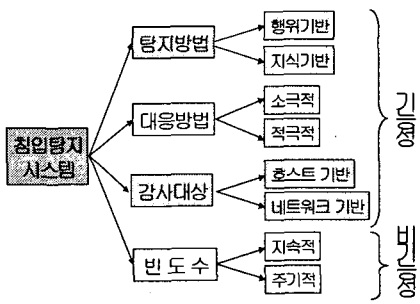
① 다른 보안장치로부터 보호되지 못하는 보안 위 배와 침입을 탐지한다.

② 조직 내부에 현존하고 있는 다양한 위협을 도 출한다.

③ 침입에 대한 정보를 제공함으로써 그 대응책을 수립할 수 있다.

3. 기존 침입탐지시스템의 양상

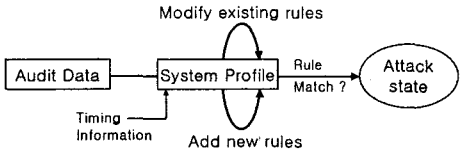
일반적인 침입탐지시스템 분류는 IBM 연구소에서 [그림 4]와 같이 네 가지 특성에 따라 분류하였으나, 지금까지 개발된 침입탐지시스템은 대체로 비정상 행위 탐지기법과 오용 탐지기법으로 한 탐지방법과 호스트와 네트워크를 기반으로 한 감사대상에 의한 탐지기법을 중점으로 발전해 왔다. 그래서 본 논문에서도 현재의 침입탐지시스템의 양상을 탐지방법과 감사대상에 따른 분류에 초점을 맞추어 설명할 것이다.[6]



[그림 4] 일반적인 침입탐지시스템 분류

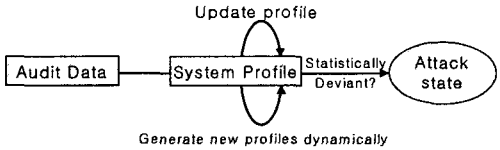
3.1.1 탐지방법에 따른 침입탐지시스템

오용 탐지 기법은 초기에 많이 사용됐던 기법으로, 침입 행위에 대해서 기존에 알려진 침입 행위와 비교하여 탐지하는 방법이다. 그러나, 초기에 알려진 침입 행위에 대한 자료 부족으로 효과적인 탐지가 불가능했다.



[그림 5] 오용 탐지기법

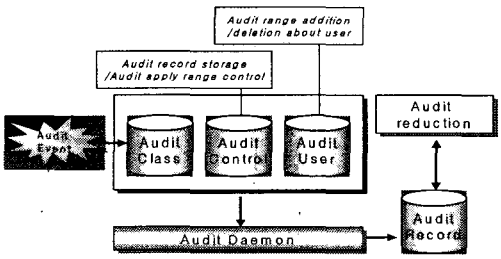
비정상 행위 기법은 실제로 탐지된 행위를 가지고 기존의 정상적인 행동 패턴과 어긋날 경우 침입으로 간주하는 방법이다[7].



[그림 6] 비정상 행위 탐지기법

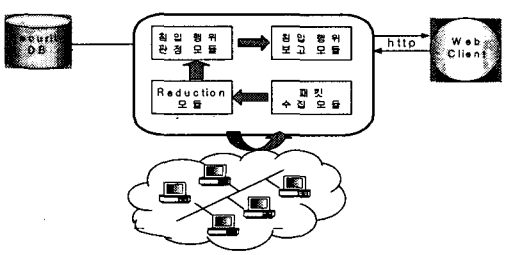
3.1.2 감사 방법에 의한 침입탐지시스템

단일 시스템이나 환경에서 사용된 호스트를 기반으로 한 탐지 방법은 시스템에서 감사자료를 수집하여 침입을 탐지하는 것으로써 네트워크 발전 이전에 각광받던 방법이다.



[그림 7] 호스트 기반 탐지기법

네트워크 기술의 발전과 더불어 네트워크를 통한 공격이 다양해지므로써 네트워크 패킷을 검사하여 침입을 탐지하는 네트워크 기반 탐지기법은 실시간 탐지 기술이 더해지면서 꾸준히 발전하고 있는 추세이다[8].



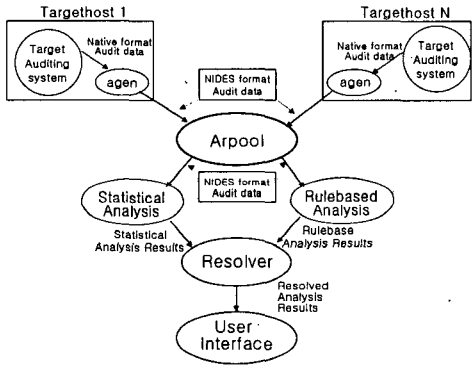
[그림 8] 네트워크 기반 탐지기법

4. 침입탐지시스템의 현재 동향과 발전 방향

4.1 침입탐지시스템의 현재 동향

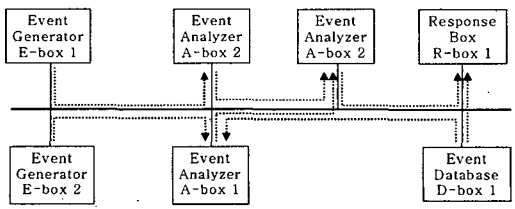
초기 침입탐지시스템은 탐지기법 특성을 기준으로 하여 모델을 만들었으며, 탐지 대상도 극히 제한적이었다. 그리고 기존의 침입탐지시스템의 모델은 단일 시스템 환경에 적합하게 설계되어 대규모 네트워크의 확장에 어려움을 가지고 있었으며, 각각의 모델들이 독자적인 통신 메커니즘 형태로 되어 있어, 상호연동 및 기존 시스템에서 재사용이 불가능했다. 현재는 이러한 단점을 극복하기 위해서 한가지 이상의 기능을 혼합하여 사용할 수 있는 하이브리드형과 한 개 이상의 시스템을 상호 연결 및 다른 시스템에서 재사용이 가능한 구조 통합 공용형이 연구/개발되고 있다.

하이브리드 형으로 대표적인 예는 1980년대에 SRI에서 개발한 NIDES(Next- generation Intrusion Detection System)로 IDES의 확장형이며, 통계 알고리즘을 이용한 비정상적/오용 행위탐지 기법을 모두 이용한 침입탐지시스템이다[9].



[그림 9] NIDES 구성요소

그리고 구조 통합 공용형으로 대표적인 예는 현재 DARPA의 지원아래 연구중인 CIDF(Common Intrusion Detection Framework)로 상호 협력할 수 있는 침입탐지에 대한 프레임워크를 제시하였으며, 기존의 침입탐지 시스템들이 지닌 구성요소들을 재사용하고, 서로 다른 종류의 구성요소들이 통신할 수 있는 인터페이스에 대한 정의를 제시하였다. 전체적으로 통합된 침입탐지 모델을 세우기 위해서 침입탐지 기법의 확장 및 서로 다른 방식으로 얻어지는 정보들에 대한 통합이 필요하고, 통신 프로토콜에 대한 정의가 요구된다. 또한, 기존의 시스템들을 기반으로 하여 확장되어야 하며, 시스템에 적합한 공통 언어를 사용해야 한다[6].



[그림 10] CIDF 구성요소

이처럼, 기존의 단일 시스템 및 단일 환경에서의 침입탐지 시스템들이 지닌 한계를 극복하고, 서로 다른

침입 탐지기법들과 침입 정보를 상호 공용할 수 있는 공통적인 표기 및 언어를 사용할 수 있는 침입탐지 모델의 연구가 여러 연구기관에서 활발히 진행되고 있는 가운데, 오용과 비정상 통합 탐지 및 계층화를 목적으로 한 EMERALD, 분산 에이전트 기반으로 탐지하는 AAFID 등이 그 목적으로 개발되고 있는 시스템들이라 할 수 있다[6].

4.2 침입탐지시스템의 발전 방향

4.2.1 현재 침입탐지시스템의 한계 및 문제점

현재, 침입탐지시스템이 네트워크가 증대되고 복잡해짐에 따라

- 모든 패킷검사가 불가능하고,
- 감사자료의 효율적인 분석/축약이 불가능하고,
- 대규모 환경에서는 침입탐지에 한계가 있으며,
- 침입을 목적으로 한 모빌코드엔 취약하다.

그리고 침입기술이 고도화되고 정교하게 됨에 따라 - 새로운 공격 탐지에 수동적이며,

- 침입자의 정확한 위치나 경로, 의도를 파악할 수 없고,
- 일단 침입이 발생하면 피해를 입기 전에 초 기 탐지가 불가능하다.

침입탐지시스템의 자체 및 상호간에도

- 피해에 따른 신속한 피해분석 및 회복 능력 이 부족하고,
- 피해복구를 위한 완벽한 가이드가 없으며,
- 시스템 자체에 대한 내구성도 떨어지고,
- 각 시스템간의 운영을 위한 표준안도 마련 되어 있지 않은 실정이다[10].

4.2.2 향후 침입탐지시스템의 발전 방향

현재 침입탐지시스템의 한계 및 문제점을 고려해 볼 때 앞으로의 침입탐지시스템은 대규모 네트워크 환경에 적용되고 다양한 침입에 대한 탐지가 가능해야 한다. 그리고 대량의 침입 패턴 모델을 보유하여 초기에 침입을 탐지할 수 있어야 하며, 내구성 및 신속한 피해분석 능력을 보유해야 한다. 또한, 각 서로 다른 침입탐지 기법을 상호 협력하여 공용할 수 있도록 설계해야 하며, 침입에 대한 실시간 탐지 및 역추적 기능, 그리고 탐지에 이은 신속하고 자동화된 대응 능력을 고려해야 한다. 다음은 이러한 능력을 수행할 수 있도록 향후 침입탐지시스템이 갖추어야 할 기능들이다.

- 확장성 : 단일 네트워크 환경 뿐만 아니라 대 규모 네트워크 환경에서도 사용 가능토록 계층 적 구조를 갖도록 설계되어야 한다. 계층적 구조 라 함은 침입탐지 시스템 단독으로 탐지하기 어 려운 광범위한 침입에 대해 상/하부 침입탐지시 스템으로 구성하여 분산 침입탐지와 통합 분석 을 수행하는 것을 의미한다.
- 적시성 : 침입탐지는 실시간으로 수행되어 피해 이전에 탐지가능해야 한다.
- 역추적 기능성 : 탐지뿐만 아니라 침입경로, 출 발지를 확인하여 침입의도를 파악하고 재침입이 발생하지 못하도록 신속히 대처할 수 있어야 한다.
- 자동화 대응성 : 탐지와 동시에 단순한 공격에 대해서는 시스템 자체에서 자동적으로 대응할 수 있어야 한다.
- 공용성 : 공용 언어 및 메시지를 사용하므로써 침입탐지시스템 응용간 통신이 가능해야 한다.
- 재사용성 : 다른 환경 및 기존에 있는 시스템에 서도 사용 가능해야 한다. 그럼으로써 이질적인 환경에서 사용할 수 있고 재설치 비용을 줄일 수 있다.
- 상호 협력성 : 각각의 침입탐지시스템간 상호 협력할 수 있어야 한다. 서로 다른 vendor들이 제공한 침입탐지시스템일지라도 상호 연동하여 사용 가능해야 한다.
- 내구성 : 침입탐지시스템 자체에도 공격받을 가 능성이 있으므로 견고하며 빠른 회복능력을 지 니도록 설계해야 한다.
- 사용 용이성 : 시스템 관리자들이 손쉽게 사용 할 수 있어야 한다. 아무리 침입탐지시스템이 잘 설계되었어도 관리자가 사용하는데 불편함을 느 낀다면 침입에 대한 대응능력이 저하될 것이다.

5. 결론

본 논문에서는 침입탐지시스템의 변천과정에 따라 침입탐지시스템의 모델의 변화를 살펴보았으며 현재의 침입탐지시스템의 연구/개발 방향과 향후 발전방향을 제시하였다. 침입탐지시스템 개발 이전에는 대부분 감사 시스템을 이용하여 피해평가 분석 위주로 수행되었다. 1980년대에는 단일 환경 및 호스트에 대한 침입탐지 기술이 개발되기 시작했으며, 1980년대 후반에 들어오면서 네트워크 환경이 대규모로 커지고 고속화됨으로써 다양한 침입에 대해 네트워크 중심으로 한 침입탐지시스템의 개발이 본격화되고 하이브리드 형태가 대두되기 시작하였다.

앞으로는 대규모 네트워크 환경에 적용할 수 있으며, 여러 탐지기술을 혼용 및 침입탐지시스템간 상호 협력이 가능하며 다른 보안 시스템과 연동이 가능한 침입탐지시스템이 연구/개발에 주력해야 할 것이다. 또한, 급속도로 발전하는 인터넷 환경에 적용할 수 있는 보다 더 간편하고 손쉽게 이질적인 환경에서도 사용할 수 있고, 여러분야에 응용될 수 있는 자동화 능력을 갖추도록 개발되어야 한다. 마지막으로 탐지뿐 만 아니라 역추적 기능과 자동 대응능력을 보유할 수 있도록 연구를 지속해야 할 것이다.

참고문헌

[1] Rebecca Gurley Bace *"Intrusion Detection"*, Macmillan Technical Publishing PP.7-16. 2000.

[2] Sandeep Kumar, "Classification and Detection of Computer Intrusions", Purdue university 5, Aug., 1995.

[3] Edward G. Amoroso, *"Intrusion Detection"*, AT&A, PP.20-21. 1999.

[4] 이충우, "침입탐지 시스템의 역사와 종류", 정보보호21C, PP.82-85, July. 2001.

[5] 송규철, "침입탐지시스템 구축 및 운영 실무", 제6회 정보보호 심포지움, PP.29-43, 2001.

[6] H.Debar et al. "Towards a taxonomy of intrusion-detection systems", computer Networks 31, PP.805-822. 1999.

[7] Aurobindo Sundaram, "An introduction to Intrusion Detection", ACM, 1996

[8] 김병구, 정태명, "침입탐지 기술의 현황과 전망", 정보과학회지 제18권 제1호, PP.29-39, Jan, 2000.

[9] Teresa F. Lunt, "Detecting Intruders in Computer Systems", Conference on Audition and computer Technology, 1993

[10] Julia Allen et al. *"State of the Practice of Intrusion Detection Technologies vol 1"* Carnegie Mellon University. PP.47-79. Jan 2000