情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

ISO/IEC의 IDS 기술 표준 동향

김 윤 정*, 이 기 한**

요 약

본 고에서는 ISO/IEC의 IDS (Intrusion Detection System) 표준화 동향에 대한 내용을 기술한다. ISO/IEC에서는 IDS를 국제표준 형식이 아닌, 기술문서 형식으로 구성하고 있으며, 이들 문서들은 IDS 기본 구조에 대한 것(IT intrusion detection framework)과 기업 등에서 IDS를 선정하고 배치, 운영하는데 도움을 주는 것(Guidelines for the selection, deployment and operation of IDS)의 크게 2 가지로 구성된다.

Ⅰ. 서 론

ISO/IEC에서는 침입탐지 시스템에 대한 기술 표준으로 표 1과 같은 2 가지 부류의 문서를 제공하고 있다[1,2]. 이들은 IDS 기본 구조에 대한 것(IT intrusion detection framework)과 기업 등에서 IDS를 선정하고 배치, 운영하는데 도움을 주는 것(Guidelines for the selection, deployment and operation of IDS)으로, 문서구성은 국제표준(International Standard) 형식이 아닌, 기술문서(Technical Report) 형식을 취하고 있다.

〔표 1〕 ISO/IEC IDS 관련 문서

분류	문서 제목	문서형식
IDS 구조	IT Intrusion Detection Framework	기술문서 (TR)
IDS 선정, 배치, 운영 지침	Guidelines for the selection, deployment and operation of intrusion detection systems	기술문서 (TR)

첫 번째 문서인 IDS 구조 문서가 제공되는 목적은 다음과 같다[1].

- 침입 탐지 관련 용어와 개념
- 침입 탐지 과정에서의 기능들
- 침입 탐지의 일반적인 모델
- 침입 탐지를 위한 기본적인 입력 소스들
- 침입 탐지 분석의 다양한 방법들
- 침입이 발생했을 때의 대응 행동들
- 일반적 구현, 적재 및 침입탐지 관련 논의들

다음으로 두 번째 문서인 IDS 선정, 배치, 운영 지침 문서가 제공되는 목적은 다음과 같다[2].

- IDS의 능력
- IDS를 이용할 때의 장점과 단점
- IDS 배치시의 구성적인 요구사항과 제약사항들
- 자사 IT 환경에 가장 적합한 IDS를 식별하는 법
- 자사 IT 구조와 정책, 자원과 연계한 침입탐지 전략과 구현을 개발하는 법
- IDS의 결과물을 관리하는 법(필요한 절차와 방법들)
- 침입 탐지 기능을 자사의 보안 상황과 연결하는 법
- 범죄 증거 보존 등과 같은 법적 논의에 대해 설명하는 법

본 고에서는 우선, IDS 구조에 대한 문서 내용을 살펴보고, 다음으로 IDS 선정, 배치, 운영 지침에 대한 내용을 살펴본다.

Ⅱ. IDS 기본 구조

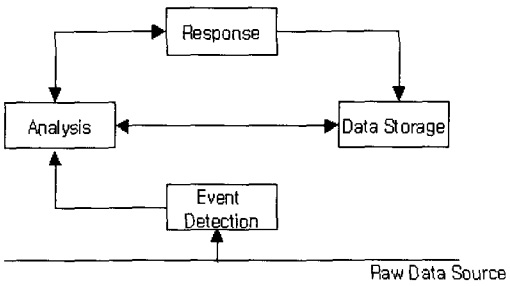
IDS 기본 구조 관련하여 침입탐지의 일반적인 모

* 서울여자대학교 정보통신공학부 ({yjkim, knight}@swu.ac.kr)

델, 침입탐지의 특성, 침입탐지 구성론, 침입탐지 분석방법, 구현, 배치시의 고려사항에 대하여 살펴본다.

1. 침입탐지의 일반적인 모델 (Generic Model of Intrusion Detection Process)

ISO/IEC에서 정의하는 침입 탐지의 기본 모델은 그림 1과 같이, 원시 데이터(raw data source), 사건 탐지(event detection), 분석(analysis), 대응(response), 데이터 저장소(data storage)의 5 가지 요소로 구성된다.

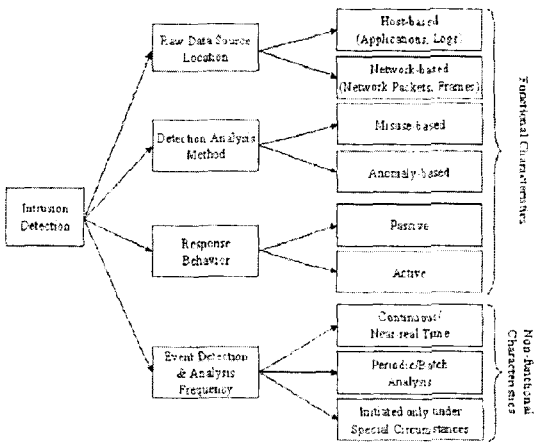


〔그림 1〕 ISO/IEC 침입탐지 기본 모델

'원시 데이타'는 여러 곳의 시스템 자원으로부터 얻어진 감사 자료들과, 시스템 자원의 사용내용(CPU 사용도, 메모리 사용도, 시스템 자원의 고갈도 등), 네트워크 관련 정보 등을 말하며, '사건탐지'는 실제 사건을 탐지하는 방안으로 여기서의 사건이란 특정 데이터, 환경, 행동 등의 발생 상황을 말한다. 이 사건들은 간단한 사건들과 복잡한 사건의 두 부분으로 나눌 수 있다. 사건들을 분석하여 실제 침입이 발생할 확률을 결정하는 것이 '분석' 기능이다. 분석 시 이용하는 정보들은 '사건탐지' 결과와 이전의 분석으로부터 얻어진 결과들, 각 사용자들의 행동양식에 대한 정보, 각 개체 및 시스템의 수행 양식 정보, 기타 위험하다고 알려진 사이트 및 개인에 대한 정보 등이다. '대응'은 침입이 발생했다고 판단된 경우 이를 관리자에게 알려주는 방안에 대한 것으로, 결과는 보통 콘솔에 GUI로 나타나며, 기타 이메일, 페이저, 메신저 서비스 등이 이용될 수 있다. '데이타 저장소'에는 탐지된 사건 결과, 분석에 필요한 모든 데이터들, 알려진 침입에 대한 프로파일들, 세부적인 원시 데이터들(추후 추적 등을 위하여 사용될 수 있다)이 저장된다. 데이터 저장소는 저장된 데이터를 보호할 수 있는 정책 하에 관리되어야 한다.

2. 침입탐지의 특성들 (Characteristics of Intrusion Detection)

침입 탐지 시스템이 가져야 할 일반적인 특성들은 크게 기능적인 것과 비 기능적인 것의 두 가지로 나눌 수 있다. 기능적인 특성들은 다시, 원시 데이타의 근원지가 어디인지, 탐지 분석 방법이 무엇인지, 대응 행동이 어떠한 지의 세 부류로 나누어진다. 원시 데이타의 근원지가 어디인지는 호스트 기반 방식(사용자 감사 자료와 시스템 로그 등)과 네트워크 기반 방식(네트워크 패킷과 네트워크 프레임 등)으로 나뉘어진다. 탐지 분석 방법의 일반적인 분류방법은 오용 기반(misuse-based)과 이상 기반(anomaly-based)으로 나눌 수 있다. 오용기반 침입 탐지 방법은 미리 잘못된 행동들을 지정하고 이 행동들이 발생하는지를 검사하는 것으로, 시그너처 분석 방법(signature analysis) 등이 이에 속한다. 이상기반 침입 탐지 방법은 정상적인 경우의 시스템 및 사용자들의 궤적을 기록해 놓고, 이를 벗어나는 행동들을 침입으로 간주하고 탐지하는 것으로, 통계적인 방법(statistical approach) 등이 이에 속한다. 침입이 탐지되었을 때의 대응행동은 수동적인 것과 능동적인 것으로 나눌 수 있다. 수동적인 대응방법은 시스템 자체의 수정은 수행하지 않는 반면에, 능동적인 대응방법은 수정이 필요한 경우, 시스템 자체의 수정도 수행한다. 비기능적인 특성이란, 사건 탐지/분석을 수행하는 주기에 관



〔그림 2〕 침입탐지의 일반적 특성

계된 것으로, 준 실시간으로 수행하기, 주기적/배치로 수행하기, 특정 조건에서만 수행하기의 세 가지 부류로 나눌 수 있다. 그림 2에 이들 침입 탐지의 일반적 특성이 나타나 있다.

3. 침입탐지 구성론 (Architecture Considerations)

작은 회사나 단체의 경우에는 하나의 IDS로 운영을 해도 충분하나, 복잡하고 큰 환경에서는 하나의 IDS로는 필요한 모든 요구를 충족하지 못할 수 있다. 이 경우, 다수의 IDS가 모여서 전체 침입 탐지 기능을 수행해야 할 필요가 있으며, 이 때 각 IDS는 전체 시스템의 일부 요소 기능을 수행한다. 다수 IDS가 상호 동작하는 방법은 계층적(hierarchical) 방법과 중앙 집중적(centralized) 방법으로 나눌 수 있다. 계층적 방법에서는 각 IDS 요소들이 원시 데이타에서 사건을 탐지하고 분석하는 작업을 수행하고 그 결과를 상위에서 모아 최종 침입 탐지 여부를 결정한다. 중앙 집중적 방법에서는 각 IDS 요소들은 원시 데이터를 모으는 작업만을 수행하고 중앙관리 노드에서 이 원시 데이타들을 모아서 사건탐지/분석 등의 작업을 수행하게 된다. 중앙 집중적 방법은 간단하다는 장점은 있기는 하나, 어느 정도 작은 시스템에서 적합하지 큰 시스템에서는 적합하지 않다. 중앙 집중적 방법이 좀 더 큰 시스템에서도 유용하도록 하기 위하여 원시 데이타가 모아지는 대로 양을 줄이는 방법을 사용할 수도 있다.

4. 침입탐지 분석 방법 (Intrusion Detection Analysis Methods)

시그너처 분석 방법(signature analysis), 통계적인 방법(statistical approach), 전문가 시스템(expert systems), 상태 변환 분석 기법(state transition analysis), 신경망 네트워크(neural networks), 사용자 이상 행동 탐지 (user anomalous behavior identification) 및 이들을 결합한 방법 등 다양한 기법들이 침입 탐지 분석에 사용된다.

5. 구현, 배치시 및 기타 고려사항들(Implementation and Deployment Issues/Intrusion Detection Issues)

IDS 구현시 효율성(efficiency)과 기능성(functionality) 등을 고려하여야 하고, 침입 탐지 방법이 회사의 보안 정책에 부합하도록 구성되어야 한다. 또한 네트워크 관리 시스템과의 상호 동작성, 다른 IDS와의 연관성 등도 고려되어야 한다.

Ⅲ. IDS 선정, 배치, 운영 지침

IDS 선정, 배치, 운영 지침과 관련하여 IDS에서 탐지하는 공격들, IDS가 제공하는 기능들과 제공하지 못하는 제한점들, IDS 선정시 고려사항, IDS 배치 및 운영 지침에 대하여 살펴본다.

1. IDS에서 탐지하는 공격들

IDS가 보고하는 공격은 서비스 거부 (denial of service), 정보 수집 (information gathering), 정보 공개 (information disclosure), 시스템 침입 (system penetration)의 4 가지 부류로 나눌 수 있다. 이 중, 정보 수집은 침입자의 스캐닝 (scanning)을 탐지하는 것으로, 이것은 모든 공격의 가장 공통적인 것으로 볼 수 있으며 또한 좀더 심각한 공격이 나타나기 전의 선행공격이기도 하다.

2. IDS의 기능과 제한점

IDS가 제공하는 기능들은 다음과 같다.

- 시스템 사건과 사용자 행동의 감시와 분석
- 시스템 설정의 보안 상태에 대한 시험
- 알려진 공격에 대응하는 시스템 사건의 패턴 인식
- 일반적인 행동과는 통계적으로 다른 행동 패턴 인식
- 침입이 탐지 되었을 때 적합한 수단으로 적합한 관리자에게 알리기
- 분석 엔진에 탑재된 보안 정책 측정
- 보안 전문가가 아니어도, IDS를 이용함으로써 중요한 보안 탐지 기능을 수행할 수 있음

위와 같은 기능을 제공하는 반면에 IDS는 다음의 기능은 제공하지 못한다.

- 방화벽이나 바이러스 탐지 등과 같은 보호기반구조의 취약성 보완
- 네트워크 로드나 시스템 로드가 심한 경우의 침입 탐지
- 서비스 거부 공격에 대한 효율적인 탐지
- 새로운 공격이나 존재하는 공격이 변형된 공격 탐지
- 고도의 숙련된 공격자에 의해 수행되는 공격에 효율

적으로 대처하기
- 사람의 간섭 없이 공격들에 대한 세세한 분석 수행

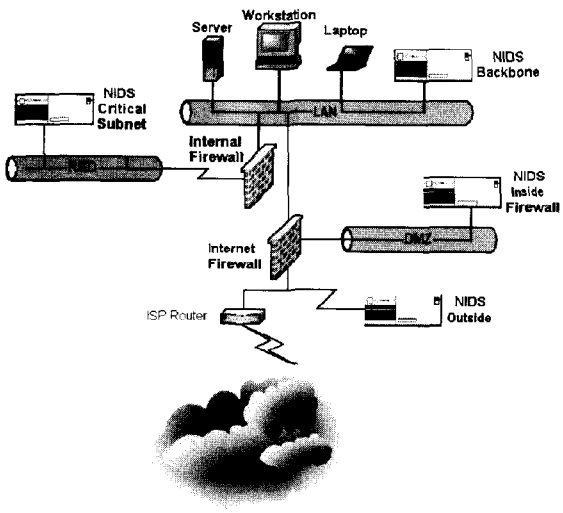
3. IDS 선정시 고려사항

여러 종류의 IDS가 현재 사용가능한데, 이들은 무료로 지급되는 공개용에서부터 최신의 하드웨어를 필요로 하는 고가의 상업용 시스템까지 다양하다. IDS 개발 업체에서 제공하는 제품 설명서에는 네트워크 로드가 심한 경우에도 IDS가 얼마나 침입을 잘 탐지하는지 그리고 이런 경우 IDS를 배치하고 운영 관리하는 것이 얼마나 어려운지에 대한 설명은 거의 나타나 있지 않다. 제품 설명서에는 단지 IDS가 탐지할 수 있는 공격들에 대한 설명만 나타난다. 그러나, IDS를 설치할 업체의 네트워크 상황을 고려하지 않고 IDS의 false positive나 false negative률을 계산한다는 것은 쉬운 일이 아니다. 결과적으로 IDS 개발 업체에서 제공하는 제품 설명서만으로는 부족하며, '자사 환경에 IDS를 설치시 고려해야 할 가정에는 무엇이 있겠는가' 등의 정보들을 IDS 개발 업체에 추가로 요구하는 것이 필요할 수 있다.

이런 정보들을 기반으로 IDS 선정시 다음 사항들을 고려할 수 있을 것이다.
- 시스템 환경 (네트워크 구조도와 지도 등, 각 호스트의 운영체제 시스템, 라우터, 브리지, 스위치 등의 네트워크 장비들)
- 현재 시스템에 설치된 보안 기법들 (방화벽의 수, 형식, 위치, 인증 서버들, 데이터와 링크 암호 기법, 바이러스 방지 패키지 등)
- IDS 보안 정책 (어떠한 정보 자산이 보호되어야 하는가, 어떤 형식의 IDS가 필요한가, IDS는 어디에 배치될 것인가, 어떤 종류의 침입을 탐지할 것인가.
- 가격 (IDS 구입에 필요한 예산은 얼마인가, IDS를 업체의 보안 정책에 따라 설정하고 사용할 사람이나 자원을 보유하고 있는지 등)
- HIDS (Host-based IDS)를 선택할 것인가 아니면 NIDS (Network-based IDS)를 선택할 것인가.
- 성능 (IDS가 처리해야 하는 대역폭은 얼마인가, 그 대역폭 하에서 잘못된 보고는 어느 정도까지 허용가능한가, 고속의 IDS를 구입하는 것이 좋을지 아니면 느리지만 적정 가격의 제품을 구입하는 것이 좋은지 등)
- 제품 개선 주기
- 기존 네트워크 관련 제품(방화벽, 취약점 점검 시스템, 파일 무결성 검사 프로그램, 네트워크 관리 프로그램, 바이러스 방지 프로그램 등)과의 호환성

4. IDS 배치

IDS는 보통 해당 기업의 상황에 맞게, HIDS (Host-based IDS)나 NIDS (Network-based IDS)를 선택하여 설치하게 된다. 이 때 HIDS나 NIDS의 각 장단점을 고려하여 선정, 배치하도록 하



〔그림 3〕 NIDS 배치 위치

며, 기업에 따라서는 기업망 전체를 보호하기 위하여 HIDS, NIDS 두 제품을 결합시켜 배치하는 곳도 필요할 수 있다.

제공되는 모든 기능을 가진 HIDS는 보통 중요한 서버에 대하여만 설치가 이루어진다. HIDS는 각 서버에 대하여 고유한 설정을 수행한 후 동작하므로, 자사의 모든 서버에 HIDS를 설치하는 것은 비용면으로도 고가이고 시간 낭비인 면도 있을 수 있다. 우선 중요 서버에만 HIDS를 설치함으로써 경험이 부족한 관리자가 중요한 위험 결과에만 집중할 수 있는 장점을 마련해 주기도 한다.

NIDS의 배치는 배치 위치를 그림 3과 같이 외부 방화벽 안에 두느냐/ 외부 방화벽 밖에 두느냐/ 주 네트워크 백본에 두느냐/ 특별 서브넷에 두느냐 등을 고려할 수 있는데 각각은 장단점을 고려하여 결정할 수 있다. 예를 들어, NIDS를 외부 방화벽 안쪽에 두는 경우 방화벽에 의하여 차단되는 공격은 탐지하지 못하는 단점이 있는 반면, NIDS를 외부 방화벽 밖에 두는 경우 침입결과 내용이 너무 많아서 IDS 결과를 분석하는 것이 대단히 어려운 작업이 되는 단점이 있는 등이다.

5. IDS 운영

IDS 선정, 배치 후 IDS 운영 전에 기업은 다음 사항 등을 결정할 필요가 있다.

- IDS 결과를 분석하고 대응하기 위한 권한과 책임의 할당
- IDS가 침입을 보고했을 때 취해져야 할 동작들
- IDS가 침입 결과를 보고했을 때 응답을 자동으로 또는 반자동으로 처리하기 위한 조건 정의

IDS 운영시 중요 로그 파일들이 암호화하지 않고 전송되는 등의 문제를 가질 수 있으며, 침입자들은 이러한 IDS의 취약점을 이용하려 할 수 있다.

IDS가 침입을 보고했을 때 이에 대한 대처를 어떻게 할지를 정해야 하는데, 자체 대응팀을 구축하던지 외부 업체에 용역을 의뢰할 수도 있다. 외부 업체에의 용역 의뢰는 자사의 비용을 줄이고 자사 직원의 IDS 교육 비용을 줄일 수 있는 등의 장점이 있으나, 용역업체의 정책이 자사의 정책과 맞지 않을 수 있으며 자사의 중요 정보가 용역업체에 노출되는 등의 단점이 있다.

IDS 운영시 위의 사항들을 인지하여 자사의 환경에 적합한 방안을 채택하여 사용함으로써 안전한 IDS 운영에 기여할 수 있다.

Ⅳ. 결론

이상에서 ISO/IEC의 IDS 관련 표준화 동향인 IDS 기본 구조와 IDS 선정, 배치, 운영에 대한 지침의 개괄적 내용을 살펴보았다. ISO/IEC에서는, 기업 관리자 및 관계자가 자사의 IT 환경에 IDS 시스템을 설치할 때 고려해야 할 사항들과 적합한 IDS를 선택 배치 운영하는데 참고할 사항들, 그리고 IT 시스템 관리자와 IT 보안 관리자들이 IDS를 이해하고 이용하는데도 도움이 되는 지침 제공을 목적으로 표준화 작업을 수행하고 있다.

참고문헌

[1] ISO/IEC JTC 1/SC 27 DTR 15947, 문서제목: Security Techniques IT intrusion detection framework, 프로젝트 번호 1.27.25, 작성일 2001-10.

[2] ISO/IEC JTC 1/SC 27 N3775, 문서제목: Text for ISO/IEC 5th WD 18043 - Information technology - security techniques - Guidelines for the selection, deployment and operation of intrusion detection systems (IDS), 프로젝트 번호 1.27.34 (18043), 작성일 2004-01-16.

[3] ISO/IEC JTC1/SC27 TR 13335, Guidelines for the Management of IT and Communication Security.

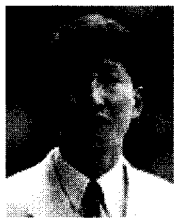
[4] 김윤정, ISO/IEC IDS 기술 표준 동향, 한국정보보호진흥원 정보보호뉴스 vol 50, 2001, 11.

[5] 김정덕, ISO 보안 관리 지침 표준화 동향, 한국정보보호진흥원 정보보호뉴스, 2000, 11.

〈著 者 紹 介〉

김 윤 정 (Yoonjeong Kim)
종신회원

1991년 : 서울대학교 컴퓨터공학과 졸업 (공학사)
1993년 : 서울대학교 대학원 컴퓨터학과 졸업 (공학석사)
2000년 : 서울대학교 대학원 전기컴퓨터공학부 졸업 (공학박사)
2000년~2001년 : (주)엔써커뮤니티 제품개발연구소 차장
2001년~2002년 : (주)데이타게이트인터내셔널 보안기술연구소 차장
2002년~현재 : 서울여자대학교 정보통신공학부 조교수
〈관심분야〉 암호학, 시스템 보안, 암호 응용



이 기 한 (Ki-Han Lee)
비회원

1987년 : 서강대학교 컴퓨터 공학과 졸업 (학사)
1989년 : 서울대학교 대학원 컴퓨터공학과 졸업 (공학석사)
1993년 : 서울대학교 대학원 컴퓨터공학과 졸업 (공학박사)
1995년~1999년 : 서울여자대학교 컴퓨터학과 조교수
1999년~현재 : 서울여자대학교 컴퓨터학과 부교수
1998년~현재 : ISO/TC215 건강카드 대표위원
2002년~현재 : ISO/SC17 스마트카드 전문위원
〈관심분야〉 스마트카드, 보안, 의료 정보, Bio-infomatics