통합 보안 관리 시스템 표준화에 대한 연구*

소 우 영**
**한남대학교 컴퓨터 공학과

요 약

정보기술의 발달로 보안사고가 증가되면서 침입차단 시스템, 침입탐지 시스템 및 가상 사설망 등의 기능이 통합된 보안 관리 시스템(ESM)의 개발에 대한 요구가 증가되고 있다. 그러나, 불행하게도 개발자들은 관련 표준의 미비로 어려움을 겪어왔다. 최근 ISTF가 침입차단 시스템 및 침입탐지 시스템의 로그 형식 표준을 발표하였으나 실제적으로 효율적인 ESM을 위해서는 이벤트 및 제어 메시지 등의 추가적인 표준 개발이 요구된다. 본 연구는 ISTF 표준을 분석하고 침입차단 시스템 및 침입탐지 시스템의 이벤트 및 제어 표준을 제안하고자 하며, 본 연구 결과는 ESM의 개발과 지속적인 관련 표준 개발에 도움이 될 것이다.

A Study on ESM(Enterprise Security Management) System Standard*

Woo-Young Soh**

ABSTRACT

As the development of information technology and thus the growth of security incidents, there has been increasing demand on developing a system for centralized security management, also known as Enterprise Security Management(ESM), uniting functions of various security systems such as firewall, intrusion detection system, virtual private network and so on. Unfortunately, however, developers have been suffering with a lack of related standard. Although ISTF recently announced firewall system and intrusion detection system log format, it still needs for truly efficient ESM further development of the related standard including event and control messaging. This paper analyses ISTF standard and further suggests an additional event and control messaging standard for firewall and intrusion detection systems. It is expected that this effort would be helpful for the development of ESM and further related standard.

1. 서 론

최근 급속한 정보통신기술의 발달에 따라 네트워크를 통한 정보의 공유와 개방화가 가속화되면서 정보시스템은 다양한 보안 위협에 노출되어 있으며 각종 보안 사고가 사회적 문제로 대두되고 있다[1]. 이에 따라 시스템을 안전하게 보호하기 위하여 조직의 잠재적인 보안위협을 관리하고 시스템에 대한 공격에 대비하기 위하여 침입차단시스템, 침입탐지시스템, 가상 사설망 및 취약점 스캐너 등의 다양한 보안도구 들이 운영되고 있으며, 이러한 보안도구들은 그 기능 면에서 볼 때 보안관련 정보의 교환 등 상호 밀접한 연관성을 내포하고 있으나, 기존의 도구들은 그러한 상호 연동성을 수행하지 못하고 있어 통합적인 보안 체계로서의 효율인 역할을 수행하지 못하고 있는 실정이다[13]. 이러한 문제의 중요한 원인 중의 하나는 단위 보안 도구가 대개 개별적으로 개발되어 제품의 개발사가 다를 경우는 물론 동일 개발사의 제품일 경우에도 상호 연동이 제대로 이루어지지 못하는 데서 비롯된다.

최근 이러한 문제 해결 방안의 하나로 단위 보안관리 도구들을 상호 연동하여 보안침해에 대응할 수 있도록 통합화하는 노력이 진행되고 있으며, 이에 따라 침입차단 시스템, 침입탐지 시스템, 가상 사설망 등의 이기종 보안 도구들을 중앙에서 통합 관리하여 도구간의 상호연동을 통해 전체 정보시스템에 대한 정책수립이 가능한 전사적 보안관리 시스템(ESM : Enterprise Security Management)이 각 벤더들에 의해 개발되고 있다[15][16]. 그러나, 기존의 이러한 시스템들은 표준화 등의 기술적인 한계와 실제 적용 상의 문제로 인하여 자사의 단위 보안 도구간의 통합관리 및 타사의 단위 보안 도구간의 통합관리 수준에서 제한적으로 개발되고 있으며, 시스템 기반의 관리만 이루어지고 있어 진정한 통합보안관리는 어려운 실정이다[21]. 이러한 한계를 극복하기 위해서 자사 및 타사의 단위 보안 도구간의 로그, 메시지 및 제어 등의 연동을 위한 표준화 노력이 국내외에서 다각도로 진행되고 있으나 아직 부족한 실정이다[17].

따라서, 본 연구에서는 단위 보안 도구간 상호운영상의 문제점을 중심으로 ESM의 국내.외 표준화 동향을 분석하고 현재의 표준을 확장 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 ESM의 개요, 구성 및 표준화 동향에 대해서 기술한 다음, 3장에서는 ISTF의 ESM 표준에 대하여 논하고, 4장에서는 ISTF의 표준에 추가되어야할 표준을 제안하며, 5장에서 결론을 맺는다.

2. 통합 보안 관리 시스템

2.1 통합 보안 관리 시스템의 개요

통합 보안 관리 시스템이란 침입 차단 시스템, 침입 탐지 시스템, 가상 사설망 등 이 기종 보안 도구를 중앙에서 통합 관리하는 시스템으로 도구간 상호연동을 통해 전체 정보 시스템에 대한 보안정책 수립이 가능한 시스템이다[13][15].

통합 보안 관리 시스템은 네트워크 보안정보의 중앙 관리 및 네트워크 보안상태에 대한 유용한 피드백을 제공 목적으로 다양한 대규모 보안자료의 수집, 분석 및 전달을 자동화함으로써 보안도구들의 상호 연동을 통하여 보안 시스템을 체계적으로 관리하기 위하여 개발되었다[16].

그러나 ESM에 대한 정확한 개념 정립이 아직 안된 실정이며, 수립된 보안정책에 따라 시스템이 신속하고 효과적인 조치를 위해 각종 경보 기능을 제공하는 등 일련의 워크플로우를 일

관되게 지원하는 것으로 이해되고있다. 일반적으로 ESM은 Enterprise Security Management, 즉 전사적 통합보안관리를 의미하며 다음의 두 가지 영역에 초점을 두고 있다.

하나는 User Administration 및 Management 영역의 ESM으로 보안 또는 정책관리에 따른 사용자 및 접근관리에 중점을 두며, 인증이나 단일 접속 기능을 포함하는 경우가 많다. 이러한 유형은 초기 ESM 개념으로 보안보다는 시스템 관리 수준으로 볼 수 있다.

또 다른 하나는 취약점분석이나 위험평가 등의 Risk Assessment 영역으로 네트워크나 시스템의 취약점 및 위험요소를 분석하고 모니터링하는 관리도구의 형태를 취하며 제품에 따라 분석 또는 정책관리, 모니터링 및 경보 등의 기능을 제공하며 최근의 ESM이 이에 속한다[20].

최근의 ESM은 네트워크나 시스템 리소스들의 각종 위험요소들을 분석하고 모니터링하는 관리 도구로서 침입차단시스템, 침입탐지시스템, 안티바이러스 제품 등 기존의 Multi Vendor 보안 솔루션들을 통합 관리함으로서 관리의 효율성을 높이고 능동적인 보안대책설정을 도와주는 보안관리 도구로 이해된다.

초기의 ESM은 각 시스템들을 원격 관리할 수 있는 정도의 개념이었으며 원격관리 이외에 단순한 정도의 로그 분석 기능을 수행하는 시스템으로 발전해 왔다. 실질적으로 ESM이라 불릴 수 있는 형태는 복잡하고 전문화된 통합보안 관리시스템으로 전체가 하나의 유기적이고 통합된 기능을 수행하는 시스템이다. 궁극적으로 ESM 완벽한 유기적 연동 및 통합은 현재로서는 어려운 실정이다[20].

ESM의 목적은 각 보안시스템들을 효과적으로 관리하는데 있으며, 이러한 효율성은 보안관리에 필요한 가치 있는 정보의 획득에 있다. 또한 이러한 정보의 획득을 위해서는 우선 이들 정보의 원천이 될 수 있는 로그의 수집 및 보안시스템 등 각 시스템에 대한 상태확인이 필요하며 이러한 사항은 개별 시스템의 특성에 따라 다른 방법이 사용될 수 있다.

수집된 로그 정보는 관리자에게 전달되고 분석되어 개별 보안시스템에 따른 정책설정을 통하여 적절한 대응조치가 취해진다. 이러한 프로세스는 우선 개별 로그 정보를 통합해서 한 곳에서 정보를 수집할 수 있어야 관리가 용이하며 단순한 정보 수집의 차원을 넘어서 정보 가공을 통한 가치 있는 정보를 생성 할 수 있어야한다.

이러한 가공된 정보 및 각 시스템의 상태 분석을 통해 관리자는 보안 관리에 대한 의사결정을 할 수 있으며 관리자는 각 보안시스템에 맞는 대응 정책을 설정할 수 있게 된다.

ESM은 발생 가능한 각종 위험 요소들, 즉, 시스템, 네트워크 침입, 오작동 등 노출된 위험을 지속적으로 제거하고 예방할 수 있는 효과가 있다. ESM을 운영함으로써, Multi Vendor 보안제품의 통합보안관리, 일관된 보안규칙의 적용(네트워크, 시스템, 애플리케이션 및 데스크탑 등), 단일 콘솔을 이용한 보안관련 이벤트 감시 및 경보 제공, 상이한 형태의 위협 및 공격의 신속한 대응, 정보 자산별 업무 위험도에 따른 실시간 분석 및 의사 결정 지원, 지속적인 취약점 분석에 따른 보안 규칙 운영 등의 체계적인 보안관리를 수행 할 수 있다[13][15].

2.2 통합 보안 관리 시스템의 구성

ESM의 일반적인 구조는 논리적인 3계층 또는 4계층으로 나눌 수 있으며 3계층 구조는 Agent, Manager 및 Console part로 나눌 수 있으며 4계층 구조는 Agent, Sub(Local)Manager, Master(Global)-Manager 및 Console part로 나눌 수 있다[9][14].

1계층은 주로 보안장비로 운영되며 정의된 규칙에 의해 이벤트와 보안정책을 적용하고 수집된 자료를 Manager 서버에게 전달 통제한다.

2계층은 1계층으로부터 전달된 이벤트를 저

장하고 정해진 규칙에 의해 이벤트를 분석 저장하며 3계층에 그 내용을 인공 지능적으로 통보하고 각종 정책에 대한 저장, 분석 및 보고 기능 등을 수행한다.

3계층은 2계층으로부터 분석 전달된 각종 자료에 대한 시각적 정보전달기능과 상황판 기능을 수행하며, Manager서버에게 각종 규칙을 설정하는 지휘 통제 업무를 수행한다.

2.3 통합 보안 관리 시스템의 기능

통합보안관리 시스템의 관리 대상은 Router, Switch, System 등의 Network장비와 침입 차단 시스템, 침입 탐지 시스템, Access Control, VPN, Content Security, Scanner 등의 보안 시스템이 있다[16].

통합 보안 관리 시스템의 핵심 요소 기술로는 Risk Classification Methodology, Abnormal Detection/Re-action, Integrated Policy Management, Normalization/Rule base Event Collection 등이 있으며 각 역할은 다음과 같다.

Risk Classification Methodology 기술은 각 단위 보안제품별 보안 패턴에 대한 분석을 통하여 위험/취약점 분류방법론을 ESM 자체에서 보유하며, 대상 시스템의 위험도에 따른 대응 및 설정 기준을 정립하고 그 내역을 Rule로서 통합 보안 관리 시스템에 포함시킨다.

Abnormal Detection/Re-action 기술은 통계적 기법, 규칙기반 기법, 인공지능기법 및 Data Mining 기법 등 사용된 기법을 기준으로 탐지하고 단순 수동 또는 능동적인 대응구조를 가지고 있는지를 파악한다.

Integrated Policy Management 기술은 수집된 정보의 분석을 통하여 알아낸 보안 취약점 및 대응조치를 중앙에서 단위 보안제품에 적용할 수 있어야 하며, 동일 벤더의 제품이거나, 정책 수정이 가능한 인터페이스 API를 제공하는 경우에는 자동으로 그렇지 않은 경우에는 각 단위 보안제품의 정책 편집기를 system call을 통하여하여 적용하지만, 통합 보안 관리 시스템에서 보안정책을 설정하면 이와 연관된 모든 단위 보안 제품의 해당 정책에 반영되고 그 결과가 통합 보안 관리 시스템을 통하여 백업, 유지, 운영되는 것이 이상적이다.

Normalization/Rule base Event Collection 기술은 정규화 된 이벤트를 수집함으로써 표준화된 이벤트를 수집하여야 연동이 용이하다.

2.4 통합 보안 관리 시스템의 표준화 동향

보안시스템들을 통합관리하기 위해서는 우선 관련 표준이 제정되고 그 표준에 따라 시스템이 개발되어야 한다. 벤더들이 SDK (Software Development Kit)를 제공하는 경우의 대표적인 예는 Check Point 사의 OPSEC이라는 SDK와 IAP(Intrusion Alert Protocol), Network Associates의 Active Security 등이 있으며, 이벤트 표준화의 경우 국내 보안업체들의 컨소시엄인 SAINT와 국내 인터넷 보안기술 포럼(ISTF)에서 만든 이벤트로그 표준화 등이 있다.

보안 이벤트 연동의 대표적인 인터페이스로는 침입차단시스템과 침입탐지시스템간의 상호연동에 의한 제품들이 있다. 그러나 자사 제품군들에 대한 인터페이스는 어느 정도 성공적이나 멀티벤더 제품군들에 대한 인터페이스와 연동은 표준화 미비 및 상호 기술적인 제약 사항으로 어려운 실정이며 표준화가 시급하다.

OPSEC(Open Platform of Security)의 목적은 SVN(Secure Virtual Network) 환경 내의 보안제품 간의 상호연동성과 통합을 지원하여 SVN을 더욱 안전한 환경으로 만들기 위한 것이다. 또한, OPSEC SDK를 이용하여 구현된 응용프로그램들은 OPSEC을 통한 통신을 보호하기 위해 SSL을 사용하며 각종 보안 제품간의 인터페이스를 지원한다[7].

Network Associates사의 Active Security는 중앙의 보안 관리 시스템이 보안 정책을 관리하고 감시 및 탐지를 수행하는 보안 시스템들로부터 이벤트를 보고 받아 설정된 정책에 따라 대응책을 결정하여 제어 메시지를 보내거나 정책을 수정하여 자동적으로 네트워크 보안 관리를 수행하는 시스템이다[8].

3. 통합 보안 관리 시스템 표준

이 장에서는 통합보안관리 시스템의 핵심 기술인 표준화에 대하여 기존의 표준을 분석한다.

전술한 바와 같이 많은 벤더들이 자신의 보안 시스템의 통합을 시도하며 벤더 자신의 보안 제품의 연동을 위해 표준화를 시도하고 있으나, 그 세부사항은 대개의 경우 공개되지 않는다. 예를 들면, 전 장에서 기술된 OPSEC이나 ACTIVE SECURITY의 경우 외부에 SDK이나 API를 제공하여 다른 보안 제품과 연동이 가능하도록 하고 있으며 국내 인터넷 보안 기술 포럼(ISTF)의 이벤트 표준은 공개되었지만, 국내 보안 업체들의 컨소시엄인 SAINT의 경우 보안 업체들간의 협의를 통하여 표준화 작업을 시도하여 SAINT API를 만들었으나 세부 표준사항은 공개되지 않고 있다.

3.1 ISTF 표준화 개요

ISTF는 침입차단 시스템과 침입 탐지 시스템의 로그 형식만 표준화하였다[18][19]. 그러나, 통합 보안 관리에서는 로그 형식인 이벤트 메시지뿐만 아니라 제어 메시지도 표준화되어야 보안시스템간의 통합보안관리가 가능하다. 이 표준에서 데이터 모델은 UML의 클래스 다이어그램을 기반으로 하여 정의한다. [그림 1]은 ISTF의 침입탐지시스템 클래스 개요를 예시하고 있다. 이 클래스 다이어그램은 클래스와 클래스간의 관계를 표현한다. 클래스의 정의는 위쪽에 클래스의 이름이 기술되고, 아래쪽에는 클래스에 해당하는 속성들이 나열된다. 본 문서에서 나타나는 클래스의 표현은 속성을 생략하고 클래스 이름만으로 표현하기도 한다. 이 경우 각 클래스는 속성과 함께 정의되므로, 클래스의 정의 부분을 참조하여야한다. 또한 클래스 이름 자체가 속성인 경우도 있다.

클래스간의 관계에는 계승 관계(inheritance)와 집합 관계(aggregation)가 있다. 계승 관계는 '이다(is-a)' 또는 '종류(kind-of)' 관계로 정의되며, 어떤(상위) 클래스를 계승받으면 계승받은 (하위) 클래스는 상위 클래스의 모든 속성과 연산을 계승받게 된다. 또한, 하위 클래스는 하위 클래스에 대해서만 적용될 수 있는 추가적인 속성과 연산을 정의할 수 있다. △표시로 계승 관계를 표현할 수 있다.

집합 관계는 '부분(part-of)' 관계로 정의되며, 여러 클래스가 모여서 하나의 클래스를 구성하는 것을 의미한다. 즉 집합 클래스를 구성하기 위해서 집합 클래스의 속성들과 집합 관계에 있는 클래스들의 모든 속성들을 합하여 전체 속성으로 구성된다.

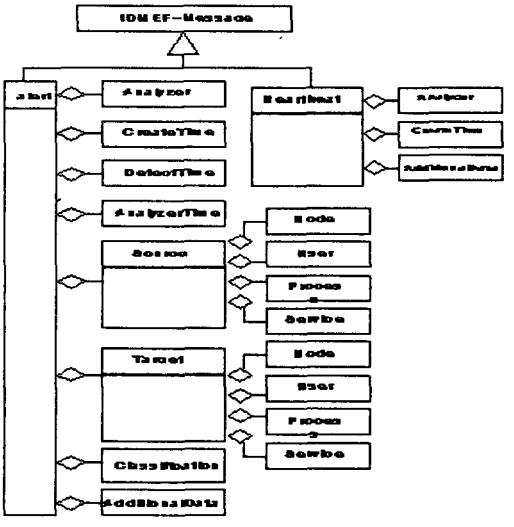


그림 1 침입 탐지 시스템 클래스 개요

◇ 표시로 집합 관계가 표현되며, 집합 관계 표현 시에 몇 개의 객체가 참여할 수 있는지를 결합성(occurrence indicator)을 통하여 표현할 수 있다. 결합성은 집합 관계에 있어서 부분이 되는 클래스 쪽에 쓰이며, 다음과 같은 의미를 가진다.

n=정확하게 "n" 개(생략되면 n=1)=exactly n
0..*=영(zero) 이상=zero or more
1..*=하나(one) 이상=one or more
0..1=영 또는 하나=zero or one
n..m= "n" 개에서 "m" 개 사이("n" 개와 "m" 개 포함)=between n and m

데이터 모델에서 사용되는 자료형은 구현을 위한 요구 사항이 아니라, 어떤 종류의 데이터인지를 표시하는 것이다. 실제 구현 자료형은 표현에 관한 문서에서 따로 정의해 주어야 한다. 예를 들어, INTEGER인 경우, binary 32 bit 정수, binary 64 bit 정수, XML(Extensible Markup Language)의 문자열로 표현될 수 있으며 본 문서에서는 어떤 것을 선택해야하는지는 결정하지 않는다.

◇ INTEGER: 정수형의 자료형 제공
◇ CHARACTER: UTF-8으로 부호화된 자료형
◇ STRING: CHARACTER로 구성된 특정한 길이의 자료형
◇ BYTE: 8bit의 parity가 없는 이진 정보
◇ ENUM: 가능한 값의 나열형 변수로 각각 값(rank)과 키워드를 가진다.
◇ DATETIME: 날짜와 시간 정보를 제공. 시간 표현의 정밀성은 본 표준에서는 정의하지 않고, 표현 방식을 ISO8601:2000에 따라서 9가지 중 한가지 형태의 STRING으로 한다[10].
◇ NTPSTAMP: NTP timestamp를 의미하며, RFC 1305 및 2030에 자세하게 기술되어 있다[11][12]. 64비트의 부호 없는 고정 소숫점 숫자로 상위 32비트는 정수부를, 하위 32비트는 실수부를 표현.
◇ PORTLIST: 포트 번호의 나열로, INTEGER들을 ' , ' 로 연결해준다. 또한 ' - ' 로 범위를 지정할 수도 있다. 예를 들어, 5-25, 53, 69-119, 123-514로 표현.
◇ Unique Identifier: 유일한 identifier는 STRING으로 표시되며 2 종류의 Unique한 id가 있다. 첫 번째는 Analyzer class의 analyzerid 속성으로, 만약 지정되면 침입탐지 시스템 환경을 포함한 보안 시스템 환경에서 모든 보안 시스템에 대하여 유일하게 정의되어야 한다. 단 모든 보안 시스템 환경에서 유일한 것은 아니고, 속해 있는 보안시스템에 대하여 유일하게 정의되어야 한다. default 값은"0" 으로 분석기가 유일한 id를생성할 수 없을 때 부여한다. 두 번째는Alert, Heartbeat, Source, Target, Node, User, Process, Service, Address, UserId 클래스의 경우 각 분석기에 의해 보내지는 메시지에 대하여 유일하게 id를 할당해 준다. default 값은 "0" 으로, 분석기가 유일한 id를 생성할 수 없을 때 부여한다. 이 두 종류의 id를 결합하면 보안 시스템 환경에서 유일한 메시지의 id를 얻을 수 있다.

3.2 ISTF 침입차단시스템 로그형식 표준

ISTF는 침입탐지시스템 같은 다양한 보안 제품들이 침입차단시스템에서 생성되는 로그를 사용할 수 있도록 침입차단시스템의 로그 형식에 대한 표준을 정의했다. 이러한 로그로 다른 침입 탐지 시스템을 포함한 보안 제품간의 연동이 가능하고 보안제품의 성능을 향상시킬 수 있을 것이다. 침입차단시스템의 로그형식은 UML의 클래스 다이어그램을 사용하여 데이터 모델을

정의하여, 확장성과 융통성이 보장되도록 하였다. 또한, 침입 탐지 시스템의 로그와 호환성을 고려하여 침입차단 시스템으로부터 수집된 자료를 기반으로 작성되었다[18].

침입차단시스템의 이벤트 클래스를 살펴보면 가장 상위에 FWMEF-Message(Fire Wall Message Exchange Format - Message)클래스가 있으며 하위에 Connect 클래스와 Heartbeat 클래스가 있다. 침입차단 시스템에서 접속 시도와 접속에 의해 발생되는 로그의 형태는 Connect 클래스에 표현된다. Connect 클래스는 침입차단 시스템에서 접속 시도와 접속에 의해 발생되는 로그의 형태를 표현하며, 접속 시도는 내부로의 접속 시도뿐만 아니라 외부로의 접속 시도를 포함한 접속에 관한 모든 정보를 나타낸다. Connect 클래스는 Sencor, Create Time, Source, Target, Classification, AdditionalData 클래스의 집합관계로 구성된다.

Heartbeat 클래스는 센서에서 Heartbeat 메시지를 사용하여 다른 보안 시스템에 상태를 알려주며, 지정된 시간에 메시지를 전송한다. Heartbeat 메시지를 받았다면 분석기는 동작하고 있고, Heartbeat 메시지를 받지 못했다면 시스템은 동작하지 않고 있다는 것을 알려준다. 경우에 따라서는 시스템의 운영 정보가 기록되기도 한다. Heartbeat 클래스는 Sencor, Create Time, AdditionalData 클래스의 집합관계로 표시된다.

Sensor 클래스는 Connect나 Heartbeat 메시지를 생성하는 검출기에 관한 클래스로 각각의 메시지는 단지 하나의 검출기에서 생성되어야 하며 Node, Process 클래스의 집합관계로 구성된다. Classification 클래스는 connect의 이름 또는 그것이 무엇인지 알려주는 정보를 제공하며 name, url 클래스의 집합관계로 표시된다. Source 클래스는 접속을 시도하여 connect를 만드는 원천에 관한 클래스로 Node, User, Service클래스의 집합관계로 표시된다. Target 클래스는 connect를 시도하는 목표에 관한 클래스로 Source 클래스와 같은 구성이다.

AdditionalData 클래스는 패킷의 헤더처럼 복잡하여 데이터 모델에 의해서 표현될 수 없는 정보를 표현하기 위하여 사용한다. Time 클래스는 타임을 표현하기 위한 클래스로 Connect와 Heartbeat 클래스의 구성 클래스이다.

CreateTime 클래스는 분석기에 의해 생성되는 Connect와 Heartbeat의 시각을 의미한다. 지원 클래스 핵심 클래스의 주요 부분을 구성하며, 그들 간에 공유된다. Node 클래스는 host나 라우터, 스위치 같은 다른 종류의 네트워크 장치를 구분하는데 사용되며 Location, Name, Address 클래스의 집합관계로 표시된다. Address 클래스는 네트워크, 하드웨어, 응용 프로그램 주소를 표현하는데 사용되며 address, netmask 클래스의 집합관계로 표시된다.

User 클래스는 사용자를 표현하며 UserId 집합 클래스를 위한 container 클래스로 사용되며 UserId 클래스의 집합관계로 표시된다. UserId 클래스는 사용자에 관한 자세한 정보를 제공하며 name, number 클래스의 집합관계로 표시된다.

Process 클래스는 검출기 프로세스를 기술하는데 사용되며 name, pid, path, arg, envg 클래스의 집합관계로 표시된다.

Service 클래스는 source와 target에 관련된 네트워크 서비스를 기술하는데 사용되며 name, port, portlist, protocol 클래스의 집합관계로 이루어지며, 하위의 SNMPService, WebService, FTPService 클래스로 계승된다. WebService 클래스는 웹 트래픽에 관련된 추가적인 정보를 제공하며 url, cgi, method, arg 클래스의 집합관계로 구성된다. SNMPService 클래스는 SNMP 트래픽에 관련된 추가적인 정보를 제공하며 oid, community, command 클래스의 집합관계로 구성된다. FTPService 클래스는 FTP 트래픽에 관련된 추가적인 정보를 제공하며 url, method 클래스의 집합관계로 구성된다.

3.3 ISTF 침입탐지시스템 로그형식 표준

본 표준의 로그 형식은 침입 경고를 어떻게 분류 검출할 것인가를 정의하는 대신 메시지의 형식과 구성에 관한 내용이 정의된다.

IDMEF-Message 클래스는 가장 상위에 위치한 클래스로 하위에 시스템에서 검출하는 메시지를 의미하는 Alerts 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스가 있다. Alert 클래스는 일반적으로 침입탐지 시스템의 분석기가 검출한 경고를 관리 시스템으로 전송할 때 전송되는 정보를 나타내며 Analyzer, CreateTime, DetectTime, AnalyzerTime, Source, Target, AdditionalData, Classification 클래스의 집합관계로 표현된다. 또 하위의 ToolAlert, OverflowAlert, CorrelationAlert 클래스로 계승된다.

Heartbeat 클래스의 분석기는 Heartbeat 메시지를 이용하여 시스템상태를 관리기에게 지정된 시간에 전송한다. Heartbeat 메시지를 수신했다면 분석기는 동작중임을, 그렇지 않으면 시스템은 동작하지 않고 있다는 것을 의미한다. 경우에 따라서는 시스템의 운영 정보가 기록되기도 한다. 모든 관리기는 Heartbeat 메시지 수신기능을 지원해야하지만 수신 후 메시지 이용은 선택적이다. Heartbeat 클래스는 Analyzer, CreateTime, AnalyzerTime, AdditionalData 클래스의 집합관계로 표시된다.

ToolAlert 클래스는 공격 도구나 트로이 목마 등 악의적인 프로그램 침입이 시도될 경우 관련 정보를 제공하며 name, command, alertident 클래스 집합관계로 표시된다. CorrelationAlert 클래스는 여러 개의 경고 정보간의 상관 관계를 표현하며 name, alertident 클래스의 집합관계로 표시된다. OverflowAlert 클래스는 buffer overflow 공격에 관련된 추가적인 정보를 전송하며, program, size, buffer 클래스로 구성된다.

Analyzer 클래스는 Alert나 Heartbeat 메시지를 생성하는 분석기에 관한 클래스로 각각의 메시지는 단지 하나의 분석기에서 생성되어야 한다. 로그 포맷에서는 계층적인 침입탐지를 금지하는 것은 아니지만 계층적인 침입탐지 시스템에 대해 분석기의 id 전달은 지원하지 않으며, Node, Process 클래스의 집합관계로 표시된다. Classification 클래스 alert의 이름 또는 그에 대한 정보를 제공하며 name, url 클래스의 집합관계로 표시된다.

Source 클래스는 alert를 만드는 이벤트 소스에 관한 클래스로 하나의 이벤트는 한 개 이상의 소스를 가질 수 있으며, 분산 서비스 거부 공격을 예로 들 수 있다. Source 클래스는 Node, User, Process, Service 클래스의 집합관계로 표시된다.

Target 클래스는 alert를 만드는 이벤트의 목표에 관한 클래스로 하나의 이벤트는 한 개 이상의 목표를 가질 수 있으며, 포트 sweep이 그 예이다. Target 클래스는 Node, User, Process, Service 클래스의 집합관계로 표시된다. AdditionalData 클래스는 패킷의 헤더처럼 복잡하여 데이터 모델에 의해서 표현될 수 없는 정보를 표현하기 위하여 사용한다. Time 클래스는 타임을 표현하기 위한 클래스로 Alert와 Heartbeat 클래스의 구성 클래스이다.

CreateTime 클래스는 분석기에 의해 생성되는 alert와 heartbeat의 시각을 의미한다. DetectTime 클래스는 분석기에 의해 검출된 alert와 heartbeat의 시각을 의미한다. AnalyzerTime 클래스는 분석기의 현재 시각을 나타내는데 사용하며 전송 과정에서 시각이 삽입되기 때문에 가능한 한 늦게 채워 져야한다. 지원 클래스는 핵심 클래스의 주요 부분을 구성하며 그들 사이에 공유된다. Node 클래스는 host나 라우터, 스위치 같은 다른 종류의 네트워크 장치를 구분하는데 사용되며 Location, Name, Address 클래스의 집합관계로 표시된다. Address 클래스는 네트워크, 하드웨어, 응용 프

로그램 주소를 표현하는데 사용되며 address, netmask 클래스의 집합관계로 표시된다.

User 클래스는 사용자를 표현하며 UserId 집합 클래스를 위한 container 클래스로 사용되며 UserId 클래스의 집합관계로 표시된다. UserId 클래스는 사용자에 관한 자세한 정보를 제공하며 name, number 클래스의 집합관계로 표시된다.

Process 클래스는 검출기 프로세스를 기술에 사용되며, name, pid, path, arg, envg 클래스의 집합관계로 표시된다.

Service 클래스는 source와 target에 관련된 네트워크 서비스를 기술에 사용되며, name, port, portlist, protocol 클래스의 집합관계로 이루어지며, 하위의 SNMPService, WebService 클래스로 계승된다. WebService 클래스는 웹 트래픽에 관련된 추가적인 정보를 제공하며 url, cgi, method, arg 클래스의 집합관계로 구성된다. SNMPService는 SNMP 트래픽에 관련된 추가적인 정보를 제공하며 oid, community, command 클래스의 집합관계로 구성된다.

4. 통합보안관리 시스템 표준화

본 장에서는 보안 시스템간의 유연한 연동을 위한 침입차단시스템과 침입탐지시스템의 이벤트 메시지와 제어 메시지의 표준에 대하여 제안한다. 여기서 제안하는 표준화 메시지는 현재 ISTF 표준화를 보완하여 침입탐지시스템이나 침입차단시스템에서 발생하는 이벤트 메시지와 각 시스템의 상태 정보에 대한 이벤트를 제공한다.

이 표준화 메시지는 침입탐지시스템이나 침입차단시스템의 침입 관련 이벤트를 제공함으로서 실제 침입차단시스템이나 침입탐지시스템의 이벤트에 상세하게 접근할 수 있다. 따라서 통합 관리 시스템이 갖춰야할 이벤트의 통합 처리를 보다 세밀하게 하여 침입 관련 오용을 더욱 줄일 수 있을 것이다. 특히 침입탐지시스템의 이벤트는 오용이 많이 발생함으로 관리의 어려움이 있으나, 여기서 제안하는 상세한 침입 관련 이벤트와 여러 이벤트를 취합함으로서 오용을 줄일 수 있을 것이다.

또한 현재 ISTF의 문서에서 제시되지 않는 상태 정보 이벤트를 제안함으로서 침입차단시스템이나 침입탐지시스템 자체의 과부하나 오류를 막을 수 있다. 이러한 상태 정보 관련 메시지가 없는 기존의 시스템을 사용하는 경우 관리자가 직접 각각의 시스템의 상태를 확인하여 시스템의 오류나 과부하를 점검하였으나 제안한 상태 정보 이벤트를 활용함으로써 통합관리 및 시스템 자체의 과부하와 오류 방지가 가능하다.

4.1 침입차단시스템 메시지 표준화

ISTF의 침입차단시스템 이벤트 형식의 전체 클래스는 크게 Connect 메시지와 HeartBeat 메시지로 나뉜다. Connect 메시지는 접속 정보에 대한 로그 자료를 보내 준다. 그러나, 침입차단 정책에 위반되는 메시지를 의미하는 침입차단시스템의 Alert 메시지에 대한 형식은 없다. 따라서, 본 절에서는 ISTF에서 제시되지 않은 침입 관련 메시지로서 통합 관리 시스템이 각 시스템에서 발생하는 침입관련 이벤트를 취합할 수 있는 Alert 메시지를 제안한다. 여기서 제안하는 Alert 메시지는 침입관련 이벤트에 대한 상세한 내역을 포함함으로서 이벤트를 취합하는데 적합하도록 하였고, 실제 침입에 대한 RAW 데이터를 제공함으로서 관리자가 침입 이벤트에 대한 검증을 할 수 있도록 고려하였다. 통합관리 시스템에서는 침입 관련 이벤트에 침입의 강도를 표시함으로서 이벤트 취합을 보다 쉽게 하였다.

제안된 침입차단시스템의 Alert 메시지 클래스는 [그림 2]와 같이 ISFT에서 제시한 Sensor 클래스와 Source와 Target 클래스를 사용하였으며

보조 클래스 중 Alert 보조 클래스를 사용한다. Alert 메시지 클래스는 침입차단시스템의 정책 중 위반되는 패킷의 세션 정보를 담고 있다.

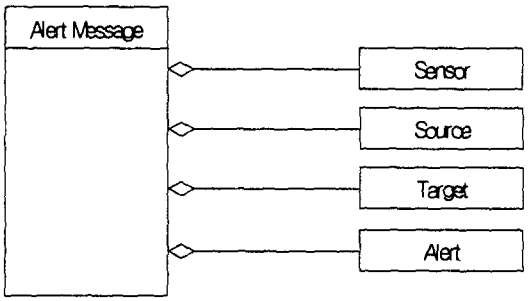


그림 2 Alert 메시지 클래스

Alert 보조 클래스는 [그림 3]과 같이 Sensor나 Source, Target 클래스에서 가지고 있지 않은 정보를 가지고 있다. Alert 보조 클래스는 ENUM 형의 AttackType과 ENUM 형의 AttackLevel을 포함하며 보조 클래스 Dump를 포함한다. AttackType은 위반 정책의 종류를 나타낸다. 또한 AttackLevel은 정책 위반의 강약을 나타낸다.

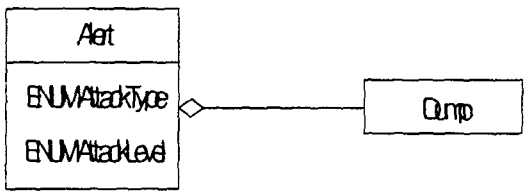


그림 3 Alert 보조 클래스

보조 클래스인 Dump 클래스는 [그림 4]와 같이 INT size, CHAR data 속성으로 구성된다. Dump 클래스는 실제 패킷을 담고 있으며 Size는 패킷의 크기이며 Data는 Char의 배열로 저장된다. Dump 클래스는 정책 위반의 강도가 높을 시 관리자로 하여금 분석 또는 분석 의뢰를 할 수 있도록 한다.

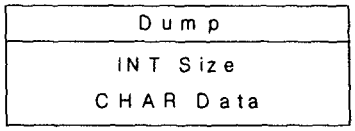


그림 4 Dump 클래스

Operation 클래스는 [그림 5]와 같이 운영 장애나 에러 메시지를 가지고 있으며 Operation 클래스에는 OpType, AlertLevel, ErrCode 등이 있다. 정수형으로 선언된 OpType은 운영 메시지의 종류를 나타내며 ENUM 형으로 선언된 AlertLevel은 경고의 강도를 나타낸다. 또한 ErrCode는 각 침입차단시스템의 운영 에러에 관한 번호를 나타낸다. 운영 에러는 하드디스크의 공간이 부족하거나 과부하로 인하여 CPU의 사용량이 계속해서 높은 수치를 나타내거나 메모리의 사용량이 계속해서 높은 수치를 나타내는 등의 메시지를 뜻한다. 침입차단시스템의 운영 에러 번호는 각 벤더마다 다르게 하여 설정할 수 있으며 통합 관리 시스템에서는 각 벤더의 코드 번호로 각 운영 메시지를 식별할 수 있도록 한다. 이러한 운영 클래스는 각 시스템의 장애를 관리자가 직접 관리하였으나, 제안한 메시지 클래스에서 이러한 상태 정보 메시지를 제시함으로서 통합 관리 시스템의 장점인 여러 보안 장비의 쉬운 관리와 관리자가 시스템의 취약성을 쉽게 파악할 수 있도록 하였다. 상태 정보 메시지는 보조 기억장치로 사용되는 하드디스크의 상태나 CPU의 상태, 주 기억 장치인 메모리의 상태를 실시간으로 파악함으로서 각 시스템의 에러나 오류를 미리 예방할 수 있을 것이다.

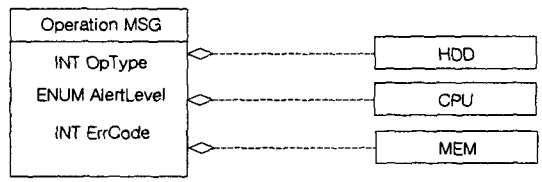


그림 5 Operation MSG 클래스

Operation MSG 클래스의 보조 클래스로는 HDD, CPU, MEM 클래스 등이 있으며 HDD 클래스는 하드디스크의 사용량을 알림으로서 경고를 하며 CPU 클래스는 CPU 사용량을 MEM 클래스는 메모리의 사용량 등을 알려준다.

Opearation MSG 클래스의 HDD 클래스는 [그림 6]과 같이 정수형으로 선언된 TotSize, UseSize, UsePer 속성으로 구성되며 TotSize는 총 하드디스크의 용량을 나타내며 크기는 Kbyte 단위로 표현한다. UseSize는 사용된 용량으로 Kbyte 단위로 표현한다. UsePer는 사용한 하드디스크의 용량을 백분율로 나타낸 것이다.

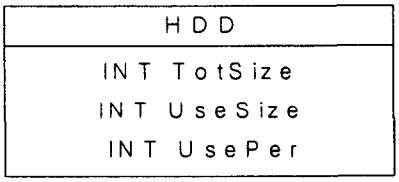


그림 6 HDD 클래스

Opearation MSG 클래스의 CPU 클래스는 [그림 7]과 같이 정수형으로 선언된 UsePer 속성으로 구성된다. 이속성은 사용한 CPU 양을 백분율로 나타낸 것이다.

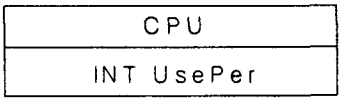


그림 7.CPU 클래스

Opearation MSG 클래스의 MEM 클래스는 [그림 8]과 같이 정수형으로 선언된 UsePer, TotSize, UseSize 속성으로 구성되며 TotSize는 총 메모리의 용량을 나타내며 크기는 Kbyte 단위로 표현한다. UseSize는 사용된 용량으로 Kbyte 단위로 표현한다. UsePer는 사용한 메모리의 용량을 백분율로 나타낸 것이다.

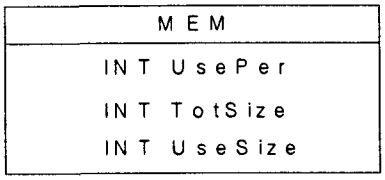


그림 8 MEM 클래스

4.2 침입탐지시스템 메시지 표준화

ISTF 문서에서 침입탐지시스템의 이벤트 형식의 전체 클래스는 크게 Alert 메시지와 HeartBeat 메시지로 나뉜다. 통합 관리 시스템은 각각의 시스템에서 발생하는 침입관련 이벤트를 취합하는 것이 핵심이나 현재 ISTF에서 제시한 메시지는 침입관련 이벤트의 내용이 부족하다. 본 절에서 제안하는 Alert 메시지는 침입관련 이벤트에 대한 상세한 내역을 포함함으로서 이벤트를 취합하는데 적합하도록 하였고, 실제 침입에 대한 RAW 데이터를 제공함으로서 관리자가 침입 이벤트에 대해 검증 할 수 있도록 하였다. 또한 통합관리 시스템에서 침입 관련 이벤트에 침입의 강도를 표시함으로서 이벤트 취합을 용이하게 하였다.

그러나 위에서 제시한 침입 차단 시스템의 Dump 클래스와 같은 패킷의 내용에 대한 클래스가 없으므로 Alert 클래스에 Dump 클래스를 추가한다.

보조 클래스인 Dump 클래스는 실제 패킷을 담고 있으며 [그림 4]와 같이 Size는 패킷의 크기이며 Data는 Char의 배열로 저장된다. Dump 클래스는 정책 위반의 강도가 높을 시 관리자로 하여금 분석 또는 분석을 의뢰 할 수 있게 한다.

다음은 운영 메시지에 관련된 메시지로 운영중 장애가 일어나거나 운영 에러가 발생했을 때의 경고 메시지이다.

Operation MSG 클래스는 [그림 5]와 같이 운영 장애나 에러 메시지를 포함하며 OpType, AlertLevel, ErrCode 등이 있다. 정수형으로 선

언된 OpType은 운영 메시지의 종류를 나타내며 ENUM 형으로 선언된 AlertLevel은 경고의 강도를 나타낸다. 또한 ErrCode는 각 침입 차단 시스템의 운영 에러에 관한 번호를 나타낸다. 운영 에러는 하드디스크의 공간이 부족하거나 과부하로 인하여 CPU의 사용량이 계속해서 높은 수치를 나타내거나 메모리의 사용량이 계속해서 높은 수치를 나타내는 등의 메시지를 뜻한다. 침입 차단 시스템의 운영 에러 번호는 각 벤더마다 다르게 하여 설정 할 수 있으며 통합 관리 시스템에서는 각 벤더의 코드 번호로 각 운영 메시지를 식별할 수 있도록 한다. 이러한 운영 클래스는 각 시스템의 장애를 관리자가 직접 관리하였으나, 제안한 메시지 클래스에서 이러한 상태 정보 메시지를 제시함으로서 통합 관리 시스템의 장점인 여러 보안 장비의 쉬운 관리와 관리자가 시스템의 취약성을 쉽게 파악할 수 있도록 하였다. 상태 정보 메시지는 보조 기억장치, CPU 및 주 기억 장치의 상태를 실시간으로 파악함으로서 각 시스템의 에러나 오류를 미리 예방할 수 있다.

Opearation MSG 클래스의 HDD 클래스는 [그림 6]과 같이 정수형으로 선언된 TotSize, UseSize, UsePer 속성으로 구성되며 TotSize는 총 하드디스크의 용량을 나타내며 크기는 Kbyte 단위로 표현한다. UseSize는 사용된 용량으로 Kbyte 단위로 표현한다. UsePer는 사용한 하드디스크의 용량을 백분율로 나타낸다.

Opearation MSG 클래스의 CPU 클래스는 [그림 7]과 같이 정수형으로 선언된 UsePer 속성으로 구성된다. 이 속성은 사용한 CPU 양을 백분율로 나타낸다.

Opearation MSG 클래스의 MEM 클래스는 [그림 8]과 같이 정수형으로 선언된 UsePer, TotSize, UseSize 속성으로 구성되며 TotSize는 총 메모리의 용량을 나타내며 크기는 Kbyte 단위로 표현한다. UseSize는 사용된 용량으로 Kbyte 단위로 표현한다. UsePer는 사용한 메모리의 용량을 백분율로 나타낸다.

위에서 사용된 하드디스크나 메모리는 일반적으로 사용된 용어이며 주기억장치나 보조 기억 장치로도 표현될 수 있다.

제5장 결론 및 향후 과제

최근 네트워크 기술의 발전으로 보안시스템의 중요성이 높아지고 있다. 이에 따라 단독 침입차단/탐지 시스템구조, 이 기종 보안시스템 구조, 특정회사의 통합시스템 구조 등 다양한 형태의 보안 시스템이 운영되고있으며, 점차 지능화되고 급변하는 네트워크 공격, 협동을 통한 네트워크 공격의 분산화/대규모화, 분산침입탐지/차단 기술의 요구 등 환경의 변화에 적응하기 위한 노력을 기울이고있다. 그러나, 단독 보안시스템 구조의 한계, 유연한 보안시스템 구축의 한계, 유기적인 상호연동을 통한 침입탐지 및 대응능력의 한계, 통합된 보안정책 적용 관리의 어려움 등이 이 분야의 문제로 지적되고 있다. 이러한 문제를 해결하기 위한 노력의 하나는 통합보안관리 시스템의 핵심 기술의 하나인 이 기종간의 보안 시스템 연동을 위한 표준을 갖추는 것이다. 본 논문에서는 통합 보안관리 시스템에서의 메시지 형식의 표준을 제시하였으며 제시된 이벤트 표준화를 통하여 다양한 보안 장비를 통합 및 연동에 적용될 수 있을 것으로 기대된다. 앞으로 보안 제품 제어 메시지에 대한 표준화 등의 작업이 추가로 이루어져야 통합 보안 관리에서의 모든 작업이 효율적으로 이루어지고 보안 제품간의 연동이 용이할 것이다.

참고문헌

[1] 월간 정보 보호, 21c 정보 보호 지침서 "기업 정보보호 실천 가이드"

[2] http://www.nessus.org/

[3] http://www.igroolec.co.kr/

[4] http://www.inzen.co.kr/

[5] http://www.oullim.co.kr/

[6] http://www.macrotek.co.kr/

[7] http://www.checkpoint.com/opsec/

[8] http://http://www.nai.com/

[9] http://www.axent.com/

[10] "International Standard: Data elements and interchange formats - Information interchange - Representation of dates and times," ISO 8601, Second Edition, 15 December 2000.

[11] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation, and Analysis," RFC 1305, March 1992.

[12] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC2030, October 1996

[13] Illena Armstrong, "Enterprise Security Management - What are the Odds?", SC Security Magazine, June 2001

[14] Michael O'Neill, "Unix System in a Large Enterprise Environment - Axent ESM", SANS Institute Information security Reading Room, 22 June 2001

[15] David Cott, "Enterprise Security Management - It's in Your Hands", SANS Institute Information security Reading Room, 29 May 2001

[16] Deron Pwel, "Enterprise Security Management(ESM): Centralizing Management of Your Security Policy", SANS Institute Information security Reading Room, 20 December 2000

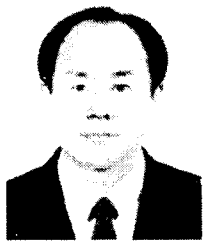
[17] Karenda Barnal, "Proposal for Managing System Security Patches in an Enterprise Network", SANS Institute Information security Reading Room, 30 January 2002

[18] ISTF, "Firewall System Log Format", ISTF-004, May 2001

[19] ISTF, "Intrusion Detection System Log Format", ISTF-005, May 2001

[20] Gardner Dale, "ESM, ASAP!", http://infosecuritymag.com/jun2000/juncoversoty. htm, June 2000

[21] Julia H. Allen, "The CERT Guide to System and Network Security Practices", Addison-Wesely, 2001



소 우 영

1979년 중앙대학교 전산학과(공학사)

1981년 서울대학교 계산통계학과(이학석사)

1991년 메릴랜드대학교 전산학과(이학박사)

1991년 ~ 현재 한남대학교 컴퓨터공학과 교수