# 전사적 통합보안관리 표준의 확장

○
유진택, 한석재, 조명휘, 소우영
한남대학교 컴퓨터공학과

# Development of Enterprise Security Management Standard

○
Jin-Taeg Yoo, Suk-Jae Han, Myeong-Hwi Jo, Woo-Young Soh
Dept. of Computer Engineering, HanNam University

**요약**

최근 보안 관련 사고의 급증으로 침입차단 시스템, 침입탐지 시스템 및 가상 사설망 등의 기능이 통합된 보안 관리 시스템(ESM)에 대한 요구가 급증하고 있다. 효율적인 ESM 개발을 위해서는 개발자와 관련 단체들에 의한 표준화 작업이 필수적이며, 최근 ISTF는 침입차단 시스템(Firewall), 침입탐지 시스템(IDS) 및 가상 사설망(VPN)의 로그 형식 표준을 발표하였다. 그러나, ISTF의 표준은 통합보안관리시스템에서 필요한 이벤트 및 제어 등의 모든 사항들을 포함하고있지 않아 이에 대한 추가 및 확장이 요구된다. 본 연구에서는 ISTF의 Firewall, IDS 및 VPN의 로그 형식을 분석하고 이 표준의 확장 개발을 위하여 추가되어야 할 항목에 대하여 논하고자 한다.

## 1. 서론

초기 보안시장에서의 보안의 개념은 침입차단시스템(Firewall)수준을 넘지 못했으나 최근에는 침입차단, VPN(가상사설망), 침입탐지, 시스템 보안, 인증, 데이터 백업에 이르기까지 전문화되었다. 보안의 핵심이 보안 제품 적용 후 적절한 보안정책에 따른 유지관리라고 볼 때 이와 같은 전문적이고 세분화된 제품의 통합관리의 필요성은 당연할 것이다[1].

미국의 보안업계에 가장 널리 사용되고 있는 보안 표준 프로토콜로는 OPSEC과 IDS를 위한 IAP(Intrusion Alert Protocol) 등이 있으나 아직까지는 완전히 국제표준으로 자리잡지 못한 상태이다[4][7]. 많은 국내 개발 업체들도 ESM의 중앙관리모듈을 출시하면서 OPSEC을 지원하고 있으며 자체 표준을 제안하기 위한 움직임도 활발하다. 이와 같이 이기종 보안 솔루션의 상호 연동을 위한 보안 프로토콜 표준화 문제가 ESM 상용화의 최대 현안으로 급부상하고 있으며, 이러한 문제를 해결하기 위하여 침입차단 시스템, 침입탐지 시스템, 가상 사설망 사이의 로그 자료 교환을 위한 표준이 ISTF(국내 인터넷 보안기술 포럼)에 의해 개발되었다. 따라서, 본 연구에서는 ISTF의 로그형식 표준을 분석하고 본 표준에 확장 추가되어야할 사항에 대하여 논한다.

본 논문의 2장에서는 ISTF의 침입차단 시스템, 침입탐지 시스템, 가상 사설망의 로그형식 표준을 분석하고, 3장에서는 성공적인 통합보안관리시스템을 위하여 본 표준에 확장 추가되어야할 사항에 대하여 논한 다음, 4장에서 결론을 맺는다.

## 2. ISTF 로그 형식 표준 분석

이 장에서는 통합 보안 관리 시스템의 핵심 기술인 표준화에 대하여 ISTF의 로그형식 표준을 분석한다. ESM 개발자들은 자신의 보안 시스템 연동을 위해 표준화를 시도해 왔으나, 그 세부사항은 대개의 경우 공개되지 않는다[2][3][4]. 예를 들면, OPSEC이나 ACTIVE SECURITY의 경우 외부에 SDK나 API를 제공하여 다른 보안 제품과 연동이 가능하도록 하고 있으며 ISTF의 이벤트 표준은 공개되었지만, 국내 보안 업체들의 컨소시엄인 SAINT의 경우 보안 업체들 간의 협의를 통하여 표준화 작업을 시도하여 SAINT API를 만들었으나 세부 표준사항은 공개되지 않고 있다. ESM을 위한 표준은 로그 형식인 이벤트 메시지 및 제어 메시지 등의 표준화가 필요하나 최근 발표된 ISTF 표준은 침입차단시스템, 침입탐지시스템, 가상 사설망의 로그 형식만 표준화하였다[5][6]. 이 표준에서 데이터 모델은 UML의 클래스 다이어그램을 기반으로 하여 정의한다. 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. 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 논문에서는 어떤 것을 선택해야하는지는 결정하지 않는다.

## 2.1 침입차단 시스템 로그 형식 표준

침입탐지시스템 같은 다양한 보안 제품들이 침입차단시스템에서 생성되는 로그를 사용할 수 있도록 침입차단시스템의 로그 형식에 대한 표준을 정의한다. 이러한 로그로 다른 침입 탐지 시스템을 포함한 보안제품간의 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[5].

침입차단시스템의 이벤트 클래스를 살펴보면 가장 상위에 FWSLF-Message(Firewall System Log 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 Sensor, CreateTime, Source, Target, Classification, AdditionalData클래스의 집합관계로 구성된다.

Heartbeat 클래스는 분석기에서 Heartbeat 메시지를 사용하여 다른 보안 시스템에 상태를 알려주며, 지정된 시간에 메시지를 전송한다. Heartbeat 클래스는 Sensor, CreateTime, 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, Service, Process클래스의 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 source, target, 분석기에서 수행되는 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 계승되며, SNMP 트래픽, 웹 트래픽, FTP 트래픽에 관련된 추가적인 정보를 제공한다.

## 2.2 침입탐지 시스템 로그 형식 표준

침입탐지 시스템의 로그 형식에 대한 표준은 침입탐지 시스템의 탐지 결과를 이용하고자 하는 보안 시스템 통합관리시스템, 침입 분석 시스템 등의 보안 시스템이 침입탐지 시스템에서 생성되는 로그를 통하여 연동이 가능하도록 침입탐지 시스템의 로그 형식에 대한 표준을 정의하였다[6].

IDSLF-Message(Intrusion Detection System Log

Format-Message) 클래스는 가장 상위에 위치한 클래스로 Alerts 클래스와 Heartbeats 클래스의 집합관계로 표현된다. Alert 클래스는 일반적으로 침입탐지 시스템의 분석기가 검출한 경고를 관리 시스템으로 전송할 때 전송되는 정보를 나타내며 Analyzer, CreateTime, DetectTime, AnalyzerTime, Source, Target, Classification, Assessment, AdditionalData 클래스의 집합관계로 표현된다. 또 하위의 ToolAlert, OverflowAlert, CorrelationAlert 클래스로 계승된다. Heartbeat 클래스는 침입차단 시스템의 HeartBeat 클래스와 같다.

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 생성되며 Node, Process 클래스의 집합관계로 표시된다. Classfication 클래스는 경고의 이름 또는 관리기가 무엇인지 결정할 수 있는 다른 정보를 제공하며 name, url 클래스의 집합관계로 구성된다. Source 클래스는 alert를 만드는 이벤트의 원천에 관한 클래스이고 이벤트는 한 개 이상의 소스를 가지며 Node, User, Process, Service 클래스의 집합관계로 구성된다. Target 클래스는 alert를 만드는 이벤트의 목표에 관한 클래스이고 하나의 이벤트는 한 개 이상의 목표를 가지며 Node, User, Process, Service, FileList 클래스의 집합관계로 구성된다. Assessment 클래스는 분석기의 이벤트의 영향, 대응으로 취해진 동작, 확신 정도를 제공하며 Impact, Action, Confidence 클래스 집합관계로 구성된다.

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 분석기가 생성한 alert와 heartbeat의 생성 시각을 의미한다. DetectTime 클래스는 분석기에 의해 검출된 alert와 heartbeat의 시각을 의미한다. AnalyzerTime 클래스는 분석기의 현재 시각을 나타내는데 사용한다. 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 클래스와 Process 클래스와 Service 클래스도 침입 차단 로그와 같은 형식으로 되어 있다.

## 2.3 가상 사설망 로그 형식 표준

가상 사설망 로그 형식에 대한 표준은 가상사설망 시스템의 탐지 결과를 이용하고자 하는 보안 시스템 통합 관리시스템, 침입 분석 시스템 등의 보안 시스템이 가상사설망 시스템에서 생성되는 로그를 통하여 연동이 가능하도록 가상사설망 시스템의 로그 형식에 대한 표준을 정의하였다[8].

VPNSLF-Message(Virtual Private Network System Log Format - Message) 클래스는 가장 상위에 위치한 클래스로 Connect, Heartbeat, KeyExchange, SAD 클래스의 집합관계로 구성된다. Connect 클래스는 접속시도와 접속에 의해 발생되는 모든 로그를 표현하고 Device, CreatTime, Source, Target, Action, Classification, AdditionalData 클래스의 집합관계로 구성된다. Heartbeat 클래스는 Heartbeat 메시지를 사용하여 관리기에게 현재의 상태를 알려주며 Device, CreatTime, AdditionalData 클래스의 집합관계로 구성된다. KeyExchange 클래스는 VPN 장치간의 연결을 맺기 위해서 정보를 교환하고 기술하기 위한 클래스이며 Device, CreatTime, Source, Target, AddtionalData 클래스의 집합관계로 구성된다. SAD 클래스는 패킷에 대한 처리 규칙이 저장되는 클래스이며 Device, CreatTime, SADParameters 클래스의 집합관계로 구성된다. SADParameters 클래스는 SAD항목의 내용(AH 인증 알고리즘, ESP 암호화 알고리즘, 터널모드 또는 전송모드 등)을 기술한 클래스이다. VPNSLF-Message 하위 클래스 중 핵심 클래스를 살펴보면 Device, Source, Target, Classification, AdditionalData 클래스를 Connect 클래스와 Heartbeat 클래스의 핵심 클래스로 생각할 수 있다. Device 클래스는 Connect나 Heartbeat 메시지 뿐만 아니라 KeyExchange, SAD 메시지를 생성하는 장치에 관한 클래스이며 Node, Process 클래스의 집합관계로 구성된다. Classification 클래스는 Connect의 이름 또는 그것이 무엇인지 알려주는 정보를 제공하며 name, url클래스의 집합관계로

구성된다. Source 클래스는 접속을 시도하여 connect를 만드는 원천에 관한 클래스이며 Node, User클래스의 집합관계로 구성된다. Target클래스는 Connect를 시도하는 목표에 관한 클래스이며 하위 클래스는 Source 클래스와 같다. AdditionalData클래스는 데이터 모델에 의해서 표현될 수 없는 정보를 표현하기 위해서 사용하고 CreatTime 클래스는 분석기에 의해 생성되는 Connect와 Heartbeat의 시각을 의미한다. Node 클래스는 host나 라우터, 스위치 같은 다른 종류의 네트워크 장치를 구분하는 사용되며 location, name, address클래스의 집합관계로 구성된다.

Address클래스는 네트워크, 하드웨어, 응용 프로그램의 주소를 표현하는 사용되며 address, netmask클래스의 집합관계로 구성된다. User클래스와 Userid클래스는 침입차단시스템의 User, Userid클래스와 같다.

## 3. ESM 표준의 확장 요구 사항

본 절에서는 보안 시스템간의 유연한 연동을 위하여 요구되는 ISTF 표준의 확장 요구사항에 대하여 기술한다.

ESM에서 침입탐지시스템이나 침입차단시스템의 침입 관련 이벤트를 제공함으로서 실제 침입차단시스템이나 침입탐지시스템의 이벤트에 상세하게 접근할 수 있는 방법이 요구된다. 또한 상태 정보 관련 메시지는 시스템의 상태 정보 이벤트를 활용함으로써 통합관리 및 시스템 자체의 과부하와 오류 방지가 가능할 것이다. 예를 들면, ISTF 표준에서의 침입차단시스템의 이벤트 형식의 전체 클래스는 크게 Connect 메시지와 HeartBeat 메시지로 나눈다[5]. Connect 메시지는 접속 정보에 대한 로그 자료를 보내 준다. 그러나, 침입차단정책에 위반되는 메시지를 의미하는 침입차단시스템의 Alert 메시지에 대한 형식은 없으며 이에 대한 표준의 확장이 요구된다. 시스템의 운영 장애나 에러 메시지관련 정보를 각 단위 보안시스템 사이에 교환할 경우 여러 보안 장비의 관리가 용이하고 관리자가 시스템의 취약성을 쉽게 파악할 수 있을 것이다. ISTF에서 제시한 침입탐지시스템 이벤트 메시지는 침입관련 이벤트의 내용을 상세하게 다루지 않고 있다. 따라서, 실제 침입에 대한 RAW 데이터를 제공함으로서 관리자가 침입 이벤트에 대한 검증을 할 수 있도록 이벤트를 취합하는데 유용한 침입관련 이벤트에 대한 상세한 내역을 포함할 수 있어야 할 것이다.

가상 사설망에서 SAD 클래스는 패킷에 대한 처리 규칙을 저장하는데 패킷을 폐기, 통과, 적용하는 부분이 기술되어 있지 않다. 패킷들에 대한 보안정책을 적용할 수 있는 클래스를 확장해야 할 것이다.

## 4. 결론

ESM제품들의 대부분은 자사의 보안 제품군이나 협력회사 제품만을 지원하게 되어 있으며, 설치 운용되고 있는 다양한 보안 제품들의 상호 운용을 위해서는 각 보안 시스템들의 로그 표준화와 이들을 전달하고 관리하기 위한 보안 프로토콜의 제정이 시급하다.

본 논문에서는 통합 보안 관리 시스템을 위한 ISTF의 로그 형식 표준을 분석하였으며, 다양한 보안 장비의 통합 및 연동에 필요한 메시지 형식의 이벤트 등이 표준에서 확장되어야할 사항에 대하여 논하였다.

단순한 통합적인 정보 수집이 아닌 보안 시스템들간의 연계된 동작이 이루어 질 수 있고, 더 나아가 보안 제품군들만이 아닌 네트워크 관리 시스템들과의 협조와 데이터 교환 등 전체 관리 시스템들을 폭 넓게 통합관리 할 수 있는 프레임워크의 개발이 필요하며 통합 보안 관리에서의 모든 작업이 효율적으로 이루어지기 위해서는 보안 제품 제어 메시지에 대한 표준화 등의 작업이 진행되어 지속적으로 확장 보완되어야 할 것이다.

## 참고 문헌

[1] "ESM 동향 및 추세" 정보보호뉴스, 2000, 11

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

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

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

[5] ISTF, "Firewall System Log Format", ISTF-004, 2001, 5

[6] ISTF, "Intrusion Detection System Log Format", ISTF-005, 2001, 5

[7] J. Betser, A. Walther, M. Erlinger, T. Buchheim, B. Feinstein, G. Matthews, R. Pollock, K. Levitt "Creating the IETF-IDWG Intrusion Alert Protocol (IAP)"

[8] ISTF, "Virtual Private Network System Log Format", 2003, 3