2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

통합보안관리시스템을 위한 웹 기반 인터페이스의 설계

최현희*, 권윤주*, 정태명*
*성균관대학교 전기전자 및 컴퓨터공학부 실시간시스템 연구실
e-mail : {hhchoi, yjkwon}@rtlab.skku.ac.kr, tmchung@ece.skku.ac.kr

A Design of Web-based Interface for Integrated Security Management System

Hyun H. Choi*, Yoon J. Kwon*, Tai M. Chung*
*Real-Time Systems Laboratory,
School of Electrical and Computer Engineering, Sungkyunkwan University

요 약

이기종 보안제품을 통합관리하기위한 통합보안관리시스템은 보안관리를 위한 불필요한 중복을 피하고 제품들을 효율적으로 상호운용하기위해 제안된 보안관리 구조이다. 본 논문은 다양한 보안제품으로 구성된 보호대상 네트워크의 보호 상황을 모니터링하고, 보안제품들이 상호 유동적으로 결합하여 작동할 수 있는 통합보안관리시스템을 위한 웹 기반 인터페이스 구조를 소개한다. 보안제품들에 대한 통합보안관리를 인터넷상에서 이미 친숙한 웹 기반 관리 기술을 이용함으로써 보안관리자들에게 편의성과 일관성을 제공하였으며, 보안정책에 대한 지식이 부족한 일반 사용자도 쉽게 보안관리를 수행할 수 있도록 설계되었다. 또한, 자바 애플릿을 이용하여 구현된 보안관리 인터페이스는 통합보안관리를 위해 요구되는 정보들을 동적으로 원격지의 보안관리자에게 제공함으로써 보안관리의 공간적 제약을 제거하였다.

1. 서론

오늘날처럼 확장된 네트워크 상에서 다수의 시스템이 설치되어있을 경우, 네트워크의 전반적인 접근정책을 파악하고 설정하는 것은 상당히 어려운 작업이다. 각 시스템마다 별도의 관리자를 배치한 경우에도 각 관리자간의 원활한 정책 의견교환과 의사소통이 필요하나 이러한 과정을 거쳐 정책이 적용되기까지의 시간 낭비뿐만 아니라, 잘못된 의사소통으로 인해 네트워크 접근차단정책에 치명적인 결함을 가질 수도 있다. 따라서, 이러한 문제점을 극복하기위해 통합보안관리시스템이 등장하게 되었다.

통합보안관리시스템을 통해 관리자는 이기종으로 구성된 다수의 보안 제품군들을 통합 관리할 수 있기 때문에 관리의 편의성을 제공받으며, 보안위협에 빠르고 정확하게 대처할 수 있다는 장점을 갖는다. 관리자는 초기 통합보안관리시스템을 통해 보안정책을 설정하고, 부차적인 감시활동이나 보안시스템들이 스스로 해결할 수 없는 복잡한 문제들에 대해서만 조율활동을 취하면 된다. 또한, 관리자는 통합보안관리시스템을 통해서 각 보안정책들 간의 상관관계를 한 눈에 파악하여 보안정책의 오류나 보안정책간 충돌 현상, 보안정책으로 인한 서비스 장애 등의 문제점들을 쉽게 발견하고 수정할 수 있는 가능성을 부여 받는다.

통합보안관리시스템이 중앙에서 각 보안시스템들의 정책과 보안관리에 필요한 정보들을 중앙 집중적으로 관리해줌으로써, 보안관리자는 통합된 인터페이스를 통해 제공되는 네트워크 전반에 걸친 보안 상황을 한 눈에 파악할 수 있다. 또한, 각 보안시스템들의 정책에 따른 문제점이 발생하였을 경우나, 사용자 요구로 정책의 수정이 필요한 경우에 관리자는 보안시스템들의 정책을 전체적으로 점검하여 문제가 발생할 수 있는 정책의 유무와 정책 수정에 따른 결과를 예측할 수 있다.

현재 네트워크 보안관리를 위해 설치되어 있는 각 보안제품들이 서로 다른 관리 툴을 사용함으로써 보안제품간의 상호 연동 및 관리상에 어려움이 있다. 그리고 지역적으로 넓게 분포된 분산시스템의 경우 보안 운영조직을 가져야 하는 데서 발생하는 인건비 부담과 현지에 직접 가서 처리해야 한다는 부담감이 있다. 이러한 문제를 통합적으로 단일 웹 인터페이스를 통하여 관리함으로써 시간적 절약과 각종 비용 절감 효과를 갖을 수 있다.

본 논문에서는 방화벽(Firewall)과 침입탐지시스템(*IDS: Intrusion Detection System*), 그리고 가상사설망(VPN: Virtual Private Network)과 같은 보안제품군에 대한 통합 모니터링 및 관리를 함으로써 일관된 보안정책의 설정이 가능하도록 현재 본 연구진이 개발중인 웹 기반의 통합보안관리시스템을 소개하며, 그 중에서 클라이언트 개발에 관한 내용을 다루고자 한다. 본 논문의 구성은 2 장에서는 연구동향에 대해 기술하며, 3 장에서는 통합보안관리를 구성하는 클라이언트에 대한 구현 설명을 마지막으로 4 장에서는 결론 및 향후 통합보안관리를 위한 인터페이스에서 추가 진행되어져야 할 연구 방향에 대해서 언급하고자 한다.

2. 연구 동향

2.1 통합보안관리시스템

현재 통합보안관리시스템에 대한 연구 동향을 살펴보면 Checkpoint 사의 OPSEC(Open Platform Security) [1,2]과 Network Associates 사의 Active security 시스템 [3,4]의 개발이 활발히 이루어지고 있다.

OPSEC 은 각 보안시스템들간의 개입 없이 자동적인 보안관리를 목적으로 한다. 전체적으로는 각 보안시스템의 동등한 위치에서 상호협력 한다는 면에서 분산보안시스템의 특징을 갖고 있다. 그러나 OPSEC 의 경우 통합보안기능을 적용하기 위해 도입 가능한 보안제품군이 Checkpoint 사 제품과 OPSEC Framework Partners 에 소속된 회사의 제품으로 한정된다는 단점을 갖고 있다.

Active security 시스템의 구조를 살펴보면, 개념적으로 보안과 관련되는 이벤트를 탐지하는 시스템인 센서(sensor), 보안에 대한 어떤 동작을 수행하는 시스템인 행위자(actor), 그리고 이들의 행위를 중재하고 조율하는 중개인(arbiter)으로 구성되어 있다. OPSEC 과 달리 중개인이라는 존재(event orchestra)를 두어 정책과 각 보안관련 사건의 수집 및 사건들에 대한 행위를 중앙에서 제어하는 기능을 갖는 중앙 집중적 보안시스템이다. 그러나 현재 이를 지원하는 제품군은 다양하지 않으며, Network Associates 사의 보안제품들간에서만 상호연동을 지원하는 단점을 갖고 있다. 이러한 단점을 보안한 것으로 1998 년부터 이기종 환경에서 방화벽에 대한 통합보안관리시스템이 연구되었다[11, 12].

다양한 보안제품이 나오고 있는 요즘 모든 보안제품들에 대한 단일 관리의 필요성과 관리의 편이성, 접근성 향상을 위하여 통합보안관리시스템을 위한 웹 기반의 인터페이스에 대한 연구가 활발히 진행되고 있다.

2.2 웹 기반 관리

1990 년대 초반에 등장한 World Wide Web 기술은 인터넷의 대중화에 크게 기여하였으며, 멀티미디어 관련 응용프로그램의 개발과 사용을 촉진시켰다. 이러한 웹 기술은 어떤 플랫폼에서도 사용할 수 있을 뿐만 아니라, 통신망 상에 분산되어 있는 다양한 형태의 데이터들을 간단하면서도 강력한 방식으로 쉽게 제공받을 수 있도록 함으로써 가장 각광받는 기술 중의 하나로 주목 받고 있다.

웹 기반 기술은 SNMP (Simple Network Management Protocol), CMIP (Common Management Information Protocol), 그리고 DMI (Desktop Management Interface) 등의 기존의 표준 관리 기술 뿐만 아니라 개별적으로 사용되는 관리 기술들도 쉽게 포함할 수 있는 장점이 있다[5, 6, 7].

웹 기반의 관리 기술에 대한 관심은 WBEM(Web-based Enterprise Management)이라는 연합의 결성과 그 행적에서 나타난다. WBEM 은 1996 년 7 월에 Microsoft, Intel, Cisco, Compaq, BMC Software 등의 대규모 기업들과 75 개의 다른 소프트웨어 및 하드웨어 개발자들에 의해 결성된 것으로 웹 기술을 이용하여 관리 될 수 있는 상품을 개발하겠다는 결의를 발표했으며, 이러한 상품들을 관리하기 위한 관리 기술 연구 결과 발표를 통해 WBEM 을 제의했다[8].

현재 웹 기반관리 인터페이스 구현을 위해 가장 활발히 사용되고 있는 자바는 인터넷 상에서 네트워크 응용 프로그램을 개발하고 수행시키는데 있어 새로운 접근 방법을 제시하는 혁신적인 프로그램 언어로 인식되고 있다. 자바로 개발된 응용프로그램은 다양한 플랫폼에 이식되어 수행될 수 있으며 웹 브라우저를 통해 쉽게 배포 될 수 있다는 장점을 가진다[9,10, 13].

3. 통합보안관리를 위한 사용자 인터페이스

보안관리자와 통합보안관리 서버를 연결하는 인터페이스 역할을 수행하는 클라이언트는 자바 기술을 이용하여 웹 브라우저를 통한 관리를 가능하게 한다. 그리고 보안관리자로부터 전달된 요구를 통합보안관리 서버로 전달하고 그 결과를 사용자에게 통보하는 기능과 통합보안관리시스템의 각 하위 구성 요소들로부터 전달된 사건정보를 사용자에게 전달하는 기능을 제공한다.

3.1 통합보안관리 인터페이스의 목표 및 특성

통합보안관리 인터페이스의 설계 목표는 단일 관리 인터페이스를 통하여 이기종의 보안제품들을 통합관리하기 위한 보안정책을 설정하고, 보호대상 네트워크 상에서 발생하는 다양한 보안 사건들을 보안관리자가 통합 분석할 수 있는 보안관리 인터페이스를 제공하는 것이다. 또한, 보안정책에 대한 전문적인 지식이 부족한 사용자도 쉽게 보안관리를 수행할 수 있도록 관리자의 추상적인 정책 및 다양한 설정요구를 관리 서버로 전달, 처리하는 것 역시 관리 인터페이스의 설계 목표이다.

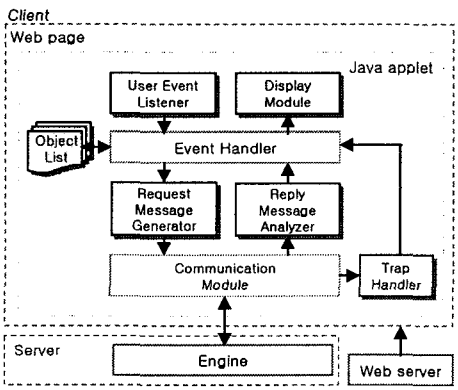
웹 기반 인터페이스는 사용자 인터페이스 상에서 엔진으로부터 받은 보안시스템에 대한 정보를 이용하여 Topology 구조를 동적으로 구성함으로써 보안관리

자가 좀더 편리하게 보안시스템들의 상태를 감지할 수 있도록 지원한다. 또한, 이기종의 보안제품들에 대하여 단일 인터페이스를 통한 통합관리를 가능케 함으로써, 보안관리자는 보호대상 네트워크에 대한 보안관리의 편의성을 제공받을 수 있다. 이러한 보안시스템들에 대한 통합관리는 기존의 보안시스템들의 재구현이나 수정이 필요 없이 그에 해당하는 에이전트를 추가함으로써 다양한 보안시스템들을 수용할 수 있는 확장성을 가진다. 마지막으로, 웹을 기반으로 구현된 관리 인터페이스는 보안관리자가 원격지에서도 웹에 접근할 수 있는 장소라면 어느 곳에서든 공간적인 제약 없이 보안관리 기능을 수행할 수 있다.

3.2 웹 기반 인터페이스 설계

보안시스템에 대한 통합 관리를 위해 다중의 사용자가 통합보안관리시스템에 동시에 접속할 경우 심각한 병목현상을 초래할 수 있다. 이를 해결하기 위해 클라이언트와 엔진간의 통신 속도를 강화하고, 각 보안정책 간의 충돌 현상을 방지할 수 있도록 보안관리 인터페이스를 설계하여야 한다. 또한, 관리 인터페이스는 보안관리자의 관리기능 수행요구 처리 및 보안 사건의 관리자 통보 기능을 효율적으로 수행 할 수 있도록 설계되어 보안관리자가 보안 사건들에 대한 통합 분석을 통하여 적절한 보안정책을 설정할 수 있도록 지원할 수 있어야 한다. 마지막으로, 웹 기반관리 인터페이스는 다양한 그래픽 콤포넌트들을 통하여 관리자에게 사용 편이성을 제공하여야 한다.

(그림 1)은 웹 통합보안관리를 위한 인터페이스 구조를 도시한 것이다.



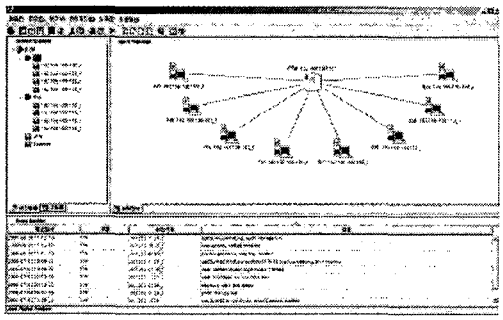
(그림 1) 사용자 인터페이스 구성도

웹 클라이언트는 HTTP 서비스를 이용하여 엔진과 연결을 설정하고, 웹 브라우저를 이용하여 통합보안관리 인터페이스 콤포넌트들로 구성된 자바 애플릿을 실행한다. 애플릿이 로드된 클라이언트는 사용자를 위한 인터페이스를 관리자에게 제공하고, 관리자 이벤트를 기다린다.

Communication Module 은 엔진과 통신 채널을 형성하여 통합보안 서비스 관리에 필요한 메시지를 송·수신 모듈로서 엔진으로부터 수신한 메시지는 파싱을 통하여, 일반 사용자 요구 처리에 의한 응답이면 Reply Message Analyzer 로 보내지게 되며, 트랩 메시지의 형태이면 Trap Handler 로 그 값을 전달한다.

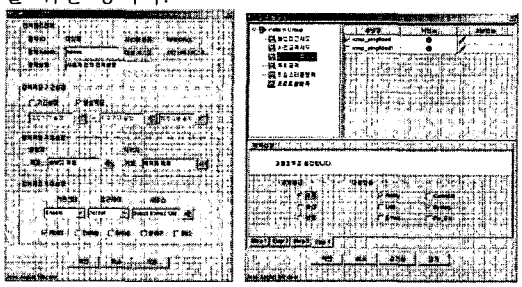
Event Handler 는 보안이벤트의 분석 및 대응행동 수행의 역할을 담당한다. 사용자로부터 입력된 이벤트를 분석하여 엔진 또는 객체 리스트에게 이벤트를 요구한다. 이벤트 처리는 추출 또는 응답된 정보를 사용자 인터페이스 상에 표현될 수 있도록 Display Module 에게 정보를 전달한다. 만약에 IDS 로부터 침입사고 상황이 발생하였을 경우 Monitoring Viewer 를 통해 관리자에게 보고하며, 침입자에 대한 방화벽 차단정책 적용결과를 다시 Event Handler 를 통하여 통보한다.

통합보안관리를 위한 사용자 인터페이스의 메인 화면은 (그림 2)와 같다. 메인 화면에 나타난 트리 뷰(Tree View)를 이용하여 관리대상 네트워크의 시스템별 및 그룹별 에이전트 구성을 나타낸 것으로서 보안제품 및 보안관리 에이전트에 정책을 설정할 수 있다. 또한, Topology 를 통하여 통합보안관리 서버와 에이전트에 대한 상태정보를 확인할 수 있으며, 마지막으로 관리 인터페이스 하단에 구성된 실시간 보안 사건 감시화면을 통하여 다수의 보안 에이전트로부터 수신되는 보안 이벤트를 감시, 분석할 수 있다.



(그림 2) 통합보안관리의 메인 화면

(그림 3)은 보안관리자가 보안제품에 대한 정책 설정을 위한 창이다.



(그림 3) 정책 설정 창 (방화벽:왼쪽, IDS:오른쪽)

정책 설정 시 동일한 보안관리 대상 객체에 대해 서로 상반되는 두개의 정책이 존재할 수 없도록 정책 목록에 대한 관리가 이루어져야 한다. 보안관리자가 설정 요구한 정책 내용에 대한 분석 및 기존 정책과의 비교 작업을 통해 보안관리자는 정책 설정시 서로 다른 유형을 가진 정책들 간에 일관성을 유지할 수 있다.

3.3 통합보안관리 사용자 인터페이스의 기능

보안관리자의 분석 및 보안정책 설정과 같은 보안관리 기능 수행을 위해 부가적으로 제공되는 서비스로는 사용자관리, 정책관리, 성능관리, 구성관리, 로그관리, 통계관리, 보안감시 등이 있으며 각각에 대한 내용은 (표 1)과 같다.

(표 1) 사용자에게 제공되는 서비스

서비스 종류	내 용
사용자관리	사용자 추가/삭제/등록정보관리 사용자 등급별 관리
정책관리	통합정책의 조회/설정/변경 정책 무결성 검사 보안제품 형태별 정책 관리 대응정책 관리
성능관리	통합보안관리시스템과 각 보안 제품들에 대한 CPU/Memory/Disk 정보제공 각 성능 항목 임계치 설정/변경 각 성능 항목 임계치 초과 시 통지 방식 조회/설정/변경
구성관리	보안제품의 요약 정보 열람 보안제품의 설명 정보 수집
로그관리	보안제품별 및 제품 형태별 로그 정보 열람 보안제품의 사건 등급별 기록여부 선택 기능
통계관리	보안제품별 통계정보 작성 및 저장 기능 보안제품의 통계정보 갱신 스케쥴링 기능 전체 사건에 대한 통계정보 작성 및 저장 기능 전체 사건에 대한 통계정보 갱신 스케쥴링 기능
보안감시	탐지된 침입 알림 보안제품 성능 이상 알림 보안제품의 현재 상태 표시 지역 관리 동작 알림 새로운 제품의 운영 개시 알림 통합보안관리 사용자 로그인 알림

로그는 시스템의 어느 시점에서의 상태 또는 이벤트의 기록으로, 보호대상 네트워크에 대한 보안상황분석을 위한 자료로 사용된다. 로그관리는 통합보안관리 자체로그와 각 보안 시스템에 대한 로그 검색 기능을 가진다.

통계관리는 보안정책이 적용된 관리대상 보안제품들로부터 수집된 통계적 데이터를 기반으로 보안관리자가 설정한 기간에 따른 시스템별, 특정 시간별로 이벤트 발생현황을 다양한 그래픽 콤포넌트들을 통하여 보여진다.

로그분석 또는 통보된 이벤트로부터 침입 및 공격 그리고 잠재적인 보안문제 발견 시 감시활동을 하는 보안시스템과 정책적용 및 대응 시스템들이 보안관리 서버의 자율적인 대응 방식에 따라 관리자의 개입 없이 신속한 대응을 할 수 있으며, 또한 보안관리자가 세부적인 정책설정 과정이나 인위적인 보안사건 처리가 요구되는 경우 정책 설정을 할 수가 있다.

호스트 혹은 네트워크 상에서 발생하는 각종 사건들을 수집, 분석하여 침입자에 의한 침입 활동을 발견하고 이를 관리자에게 통보하는 동작을 수행하는 침입탐지시스템의 기능을 바탕으로 사용자는 침입에 대한 정보를 얻고, 그것에 대한 정책 설정을 방화벽으로부터 네트워크와 네트워크 사이에 위치하여 네트워크간의 통신 연결을 선별적으로 허가 혹은 불허하는 역할을 통해서 특정 네트워크 혹은 호스트에 대한 접근 제어를 수행할 수 있는 방화벽시스템을 가지고 보안성을 향상시킨다.

4. 결론 및 향후 계획

본 논문에서 소개한 다양한 보안제품들에 대한 통합보안관리 인터페이스는 보안관리의 유연성을 제공하기 위한 웹 인터페이스의 적용과 보안정책에 대한 전문적인 지식이 부족한 일반 사용자도 쉽게 보안 관리를 수행할 수 있는 개념적인 보안 서비스 제공을 중점으로 구현되었다. 그 결과 이기종 보안제품들에 대하여 단일 인터페이스를 통한 통합보안관리를 가능케 함으로써 보안관리자에게 편리성을 제공하였으며, 단일 인터페이스를 통하여 각 보안정책들 간의 상관관계를 쉽게 모니터링함으로써 보안정책오류나 정책간 충돌현상 등을 쉽게 발견하고 수정할 수 있었다. 또한, 웹 기반의 인터페이스 사용자의 공간적 제약을 제거함으로써 시간적 절약과 비용을 절감하였다.

현재 본 연구진은 방화벽과 침입탐지시스템 이외의 보안 제품군에 대한 통합을 진행 중이며, 보다 다양한 보안 제품군에 대한 분석을 통하여 현재의 통합보안관리구조로 더욱 확장해 나갈 계획이다.

참고문헌

[1] Check Point Software Technology, Inc., Open Platform for Security (OPSEC) Technical Note, 2000.

[2] Check Point Software Technology, Inc., Check Point VPN-1/Firewall-1 OPSEC API Specification Version 4.1, Nov 4 1999.

[3] Network Associates, Inc., Automating Security management white Reducing Total Cost of Ownership, 1999.

[4] Network Associates, Inc., Active Security Getting Started Guide Version5.0, 1999.

[5] J.Case, M.Fedor, et el, "The Simple Network Management Protocol (SNMP)," RFC 1157, May. 1990.

[6] ITU-T, Information Protocol (CMIP)-Part1: Specification", Recommendation X.711, 1991.

[7] DMTF, "DMI White Paper", July. 1996.

[8] WBEM Consortium, "Web-Based Enterprise Management Proposal. HyperMedia Management Schema Overview", Revision 0.04. July. 1996.

[9] G. Jones, E. Zeisler and L. Chen, "Web-based Messaging Management Using Java Servlets," Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management, May. 1999.

[10] J. P. Martin-Flatin, "Push vs. Pull in Web-Based Network Management," Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management, May. 1999.

[11] 방기홍, 김홍선, 정태명, "이기종 환경의 침입차단 시스템을 위한 웹 기반 보안 서비스 관리시스템의 클라이언트 개발," KIPS 추계학술대회, 1999.

[12] 이동영, 김동수, 방기홍, 김홍선, 정태명, "SNMP 를 이용한 웹 기반의 통합보안관리 시스템," KNOM Review, Vol.2, No.1, Apr. 1999.

[13] 홍원기, 공지영, "웹 기반의 관리 기술," KNOM Review, Vol.1, No.1, Feb. 1998.