내규모 조직에 적합한 계층적 구조의 통합보안관리시스템에 관한 연구

박준홍, 남길현

국방대학교 전산정보학과

A Study on the Hierarchical Integrated Security Management System for the Large Scale Organization

Joon-Hong Park, Kil-Hyun Nam

Dept. of Computer & Information Science, National Defense University

요 약

본 논문은 다양한 침입행위를 탐지하고 보안시스템의 효율적 관리를 보장하는 국방전산망과 같은 대규모 네트워크 환경에 적합한 계층적 구조의 통합보안관리시스템 모델에 대한 연구이다. 전산망 위협요소 및 공격유형에 따른 취약점을 분석하여 필요한 전산망 보호기술을 판단하고 침입차단/탐지시스템, 안티바이러스 시스템, 취약점분석 시스템 등의 보안시스템과 상호연동 모델을 분석하여, 도출된 요구사항을 기반으로 대규모 조직에 적합한 계층구조의 통합보안관리시스템의 구축 방안을 제시하였다.

I. 서론

인터넷의 확산으로 인해 정보화 환경이 가속화되면서 정보보호 기술개발도 다변화하고 있다. 내부 네트워크 환경에서 점차 외부 네트워크 환경으로 변화함에 따라 정보보호 제품 및 서비스도 개방화된 환경 속에서 보안을 담당할 수 있도록 발전하고 있다. 이러한 보안 패러다임의 변화로 많은 조직들이 자사가 보유한 유형, 무형의 정보보호를 위하여 앞다투어 보안 시스템을 구축하고 있는 추세에 있다. 그러나 제조사별로 보안 시스템의 인터페이스와 관리 방법이 상이하고 이를 통합할 수 있는 표준화된 상호연동 방안이 존재하지 않아 상대적인 관리비용이 증가하며, 이로 인해 종합적인 모니터링 및 통제능력을 상당 부분 상실하고 있는 실정이다.

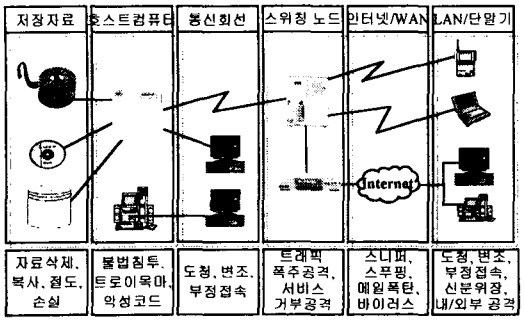
이러한 문제점을 고려하여 단일 기능을 수행하는 전용 제품에서 복합적인 보안 서비스를 수행할 수 있는 통합형태 제품의 등장과 지속적인 모니터링 및 신속한 대응, 통합 관리 등의 기능을 제공하는 효율적이고 능동적인 보안 관리 제품인 통합보안관리시스템의 도입 움직임이 활발히 일어나고 있다. 조직의 전사적 정보보호 업무 수행을 중앙집중형으로 관리할 수 있도록 하는 통합보안관리시스템은, 분산되어 있는 보안 시스템들의 효율적인 관리와 신속한 공격대응을 조직의 보안정책과 일관되게 지원한다는 점에서 최근 급격히 부각되고 있다. 하지만 이와 같은 통합보안관리시스템도 단일 중앙관리운영은 정보수집 및 분석과 대규모 하부구조를 지닌 네트워크에서는 부하집중이 문제시 될 수 있다.

따라서 본 논문에서는 기본적인 침입행위에 대한 탐지 및 대응은 개별적으로 수행하고 하부 통합보안관리시스템의 탐지 결과를 상위의 시스템이 통합 분석하는 중앙 집중적인 관리에서 지역적 분산 개념으로의 시스템 운영으로 네트워크의 트래픽과 서버의 부하를 감소시킬 수 있는 계층구조의 통합보안관리시스템 구축 방안을 제시하고자 한다.

II. 전산망 위협요소 및 보호기술

1. 위협요소 및 공격유형

정보시스템에 대한 위협과 공격유형은 정보통신망 기술의 발전과 더불어 다양한 형태로 변화하고 있으며 점차 컴퓨터 범죄화, 지능화 및 정보전의 양상으로까지 급변하고 있는 실정이다. [그림 1]은 대표적인 전산망 위협요소 및 공격유형이다.



[그림 1] 전산망 위협요소 및 공격유형

2. 전산망 보호기술

전산망 보안 메커니즘은 비밀보장, 접근통제, 데이터의 무결성, 신분확인 및 부인방지 등의 보안 서비스를 제공하기 위하여 네트워크상의 정보를 기술적으로 보호하는 것으로서 요구되는 보안 수준을 지원하기 위하여 다른 보안 메커니즘과 함께 결합되어 사용될 수 있다.

1) 암호기술

암호기술은 사용하는 키의 종류에 따라 암호화 키와 복호화 키가 같은 대칭키 암호 알고리즘과, 암호화 키와 복호화 키가 다른 공개키 암호 알고리즘으로 구분된다. DES, IDEA 등과 같은 대칭키 암호 알고리즘은 암·복호화 속도가 빠르고 키의 길이가 짧다는 장점이 있으나 키의 분배가 어렵고 사용자 증가에 따른 관리해야 할 키의 개수가 상대적으로 많다는 단점이 있다.

이에 반해 공개키 암호기술은 RSA, Elliptic Curve 암호 등이 있으며 키의 분배가 용이하고 사용자의 증가에 따른 관리해야할 키의 개수가 상대적으로 적으며, 여러 분야에서 응용이 가능하다는 장점을 지니고 있으나, 암·복호화 속도가 느리고 키의 길이가 길다는 단점이 있어 데이터의 암호화보다는 키의 교환이나 전자서명에 주로 이용된다[1].

2) 전자서명

전자서명은 데이터에 대한 서명과 서명된 데이터에 대한 검증의 절차로서 정의된다. 서명은 비밀 정보인 공개키 암호 알고리즘의 비밀키를 사용함으로써 데이터의 암호화 및 검사값을 생성하는 과정이며, 검증은 서명자의 공개 정보를 사용하여 정보를 보낸 사람이 누구인지를 알아내는 과정이다. 전자서명의 구현은 대칭키, 공개키 암호시스템과 해쉬 알고리즘을 응용하여 이루어지며, 전자서명이 유용하고 안전하려면 위조 불가, 서명자 인증, 부인 불가, 변경 불가, 재사용 불가, 진위판단 등의 조건을 만족시켜야 한다.

3) 공개키 기반구조

공개키 기반구조(PKI : Public Key Infrastructure)는 공개키 암호기술이나 전자서명기술을 이용하여 전자결재나 전자메일 등 전자거래의 안전성, 신뢰성을 보장하기 위하여 당사자의 신분확인 기능, 전자업무 내용의 정보보호 및 무결성 기능, 전자행위에 대한 부인봉쇄 기능 등을 신뢰할 만한 제3자(인증기관)가 확인 및 증명할 수 있도록 갖추어진 하드웨어, 소프트웨어 등을 포함하는 체계를 말한다[1].

PKI는 전자상거래 뿐만 아니라 전자우편, FTP, Telnet 등과 같이 네트워크 상에서 통신되는 모든 데이터의 암호화를 위하여 필요한 기반체계로서, 특히 인터넷과 같은 개방 환경에서는 암호키 관리 체계 없이는 데이터의 안전한 유통을 보장할 수 없다. PKI에 의해서 구현되는 계층적 인증 구조나 상호 인증 방식에 의하여 조직간의 안전한 데이터 통신을 위한 신뢰 관계를 형성할 수 있게 된다.

4) 접근통제

접근통제(Access Control)는 보안시스템의 중요한 기능적 요구사항 중의 하나로 외부 사용자가 내부 네트워크로 또는 내부 사용자가 인터넷 등과 같은 외부 네트워크로 통신하기 위해 시스템에 접근할 때 허용된 시스템에서 접근요청을 하는지, 통신 대상이 되는 목적지 시스템에 대한 접근 권한이 있는지, 중요자료가 허가없이 반출되는지를 검사하여 허용여부를 결정한다. 따라서 네트워크의 특정 자원에 대해서 접근 자격이 있는지를 검사한 후 접근여부를 결정함으로써 불법 침입자에 의한 불법적인 자원 접근 및 파괴를 방지할 수 있다. 접근통제는 크게 임의적 접근통제와 강제적 접근통제, 역할기반 접근통제로 나누어진다.

III. 보안시스템 현황 및 분석

보안시스템은 여러 형태의 보안서비스 구현을 통해 각종 위협으로부터 내부의 중요자산을 보호하는 것이다. 현재 적용 가능한 대표적인 보안시스템으로는 침입차단시스템(Firewall), 침입탐지시스템(IDS), 안티바이러스 시스템, 취약점분석 시스템 등이 있다.

1. 침입차단시스템

침입차단시스템의 기본 목표는 위험지대를 줄이기 위해 적극적인 보안대책을 제공하는 것이지만

네트워크 사용자에게 투명성을 보장하지 않아 약간의 제약을 주게된다. 주요기능은 네트워크에 대한 접근통제나 외부 네트워크로부터의 보호이며 일반적으로 라우터나 응용게이트웨이에 구현된다.

침입차단시스템을 이용한 네트워크 보안은 호스트의 전체적인 보안을 강화시켜줌과 동시에 보안정책을 효율적으로 시행할 수 있게 하는 등의 장점이 존재하는 반면, 우회 공격, 내부 사용자의 공격, 바이러스 방어 곤란 등의 단점이 있다[2].

2. 침입탐지시스템

침입탐지시스템은 사용자 및 외부 침입자가 컴퓨터시스템 또는 네트워크의 자원을 정당한 권한없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오용하여 권한이외의 자원을 사용하기 위한 시도를 사전에 탐지하여 그 피해를 예방하는 시스템이다.

침입탐지시스템은 내부사용자의 오·남용 탐지 및 방어가 가능하다는 장점이 있으나, 새로운 침입기법에 대한 즉각적인 대응이 곤란하고 운영 및 관리의 어려움이 존재한다.

또한 침입탐지시스템에서의 기술적 관건은 컴퓨터 시스템의 침입여부를 판단하기 위한 근거를 어디에서, 얼마나 정확하게, 그리고 신속하게 찾을 수 있느냐에 달려있다. 그리고 침입판정시 오판율을 줄이는 문제도 기술적으로 지속적인 성능향상을 통해 해결해야 할 큰 과제이다.

3. 안티바이러스 시스템

최근에는 인터넷을 통한 바이러스의 유통이 급격히 증가함에 따라서 네트워크상에서 바이러스에 감염된 파일이 첨부문서의 형태로 들어오는 과정을 근원적으로 차단하는 안티바이러스 시스템이 부각되고 있다. 안티바이러스 시스템은 시스템 감시와 인터넷 감시기능을 통해 모든 바이러스 유입경로를 24시간 백그라운드 동작으로 실시간 감시하고 파일의 복사, 이동이나 인터넷으로부터의 다운로드 등 다양한 상황에서 바이러스 유입을 차단시키는 종합적인 시스템이다[3]. 또한, 외부 네트워크에서 내부 네트워크로 통하는 경계선에 바이러스 백신 엔진을 탑재한 전용서버를 두어 이를 통하여 받는 모든 데이터들에 대해 바이러스 감염여부를 검색, 치료 및 복구하는 바이러스 월(Virus Wall)이 등장하였다.

4. 취약점분석 시스템

취약점분석 시스템은 크게 시스템 기반의 취약점분석과 네트워크 기반의 취약점분석으로 구분되며, 그 기능에 따라 시스템에 대한 접근을 기록·통제하는 보안도구, 패스워드 파일의 보안관련도구, 시스템 내부 보안 점검도구, 원격 시스템의 보안 점검도구 등이 있다. 보안관리자는 취약점분석 시스템을 통하여 O/S의 패치 여부, 계정 보안의 취약점, 최신 발견된 버그 등을 분석, 대응할 수 있게 된다. 대표적인 취약점분석 시스템은 ISS, SATAN, SAINT, COPS 등이 있으며 이러한 보안 도구들이 모든 보안 취약점을 점검해 주지 못하기 때문에 여러 도구들을 복합적으로 사용하는 것이 바람직하다.

5. 보안시스템 상호연동 모델

1) Hybrid Integration 모델

Hybrid Integration 모델은 개별 보안시스템을 하나의 서버 또는 하드웨어에 탑재한 통합보안시스템 모델로서 침입차단시스템 내부에 일부의 침입탐지시스템 기능을 탑재하는 것이 일반적이다. 그러나 이러한 시스템은 전문 침입탐지시스템에 비해 침입탐지패턴 등의 수준은 떨어진다[4].

이 모델의 대표적인 사례로는 Cisco IOS 침입차단시스템이 있는데 이것은 기존 침입차단시스템에 가상사설망(VPN)과 최소한의 침입탐지시스템의 기능을 탑재한 것이고, NetScreen-10/100은 침입차단시스템에 가상사설망과 일부공격탐지 기능을 갖추고 있다.

2) Interoperational 모델

Interoperational 모델은 미리 정해진 프로토콜을 통하여 개별 보안시스템간의 상호 작용 및 통합이 이루어지는 모델이다[4]. 보안시스템간의 연결구조는 각 보안제품이 독립적으로 운영되면서 상호연동을 통하여 보안기능을 수행하는 구조이다. 이 구조에서는 각기 다른 보안제품이 직접 연결되어 있으며 특별한 이벤트 발생시 상호 정의된 규칙에 따라 동작할 수 있다. 예를 들어 침입탐지시스템에서 침입이 탐지되었을 경우 해당하는 출발지 주소에 대한 접속 거부 등의 규칙을 침입차단시스템에서 설정하도록 하는 것이다. 이 구조는 두 객체(Object)간에 관리자가 개입되지 않고 동작하는 구조로 별도의 관리자 인증 없이 객체 인증만을 통해서 동작하게 된다.

3) Broker 모델

Broker 모델은 개별 보안시스템 간의 상호 연동 및 통합이 브로커를 통해서 이루어지는 모델이며 개별 시스템은 자신에 탑재되는 에이전트와 연

능에만 집중할 수 있다[4]. 이 모델은 다수의 보안 제품이 하나의 서버에 연결되어 있으며, 하나의 서버가 모든 통제를 하도록 구성되어져 있다. 이와 같이 구성함으로써 각각의 보안시스템은 통합관리로 인해 발생되는 오버헤드를 서버로 분산 할 수 있게 된다. 또한 통합보안관리를 위해 서버는 데이터수집, 저장 및 분석작업을 항상 수행하게 되며 매니저는 필요한 경우 서버로 접속하여 그 상황과 결과를 모니터링 할 수 있게 된다[5].

Ⅳ. 대규모 네트워크 환경의 통합보안관리시스템

1. 요구사항 분석

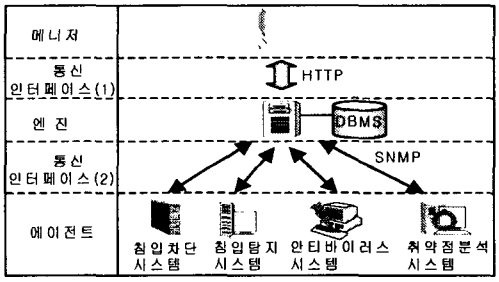
효율적인 통합보안관리시스템 운영을 위한 요구사항은 다음과 같이 일반적 요구사항과 기술적 요구사항으로 구분할 수 있다.

- ㅇ 일반적 요구사항
- · 보안시스템의 통합관제 및 다양한 보안 이벤트 로그 수용
- · 침해로그 발생에 따른 대응방책 제공
- · 네트워크 관리기능
- · 레포트, 알람기능, 사용자 인터페이스
- ㅇ 기술적 요구사항
- · 데이터 마이닝과 침해행위 추출
- · 데이터 암호화, 사용자 인증
- · 로그 관리 및 데이터의 일관성

2. 통합보안관리시스템 구성요소

본 논문에서 제안하는 통합보안관리시스템의 구조는 3장에서 언급된 보안시스템 상호연동 모델인 브로커(Broker) 모델을 기반으로 구성된다. 이는 다수의 보안시스템을 효율적으로 관리할 수 있고, 정책 기반의 관리가 가능하며 각 시스템에서 발생하는 이벤트들의 집합과 필터링이 가능하다. 구성요소는 메니저, 엔진, 그리고 에이전트 등 3개 부분으로 구성되어 있다.

통합보안관리시스템의 에이전트들은 대규모 네트워크 상에 분산 설치되어 있는 이기종의 침입차단/탐지시스템 및 안티바이러스 시스템, 취약점분석 시스템들에 설치되어 보안관리 정보들의 수집과 보안정책 제어의 기능을 수행하며, 보안관리 엔진은 관리대상 네트워크 내의 모든 보안시스템들을 통합 관리하기 위한 정보 수집과 제어를 위하여 각 에이전트들과 상호 연동한다. 수집된 정보는 통합보안관리시스템 메니저에게 제공되어 보안정책 설정 근거 자료로 사용되며, 보안 관리자는 이 정보를 바탕으로 새로운 보안정책을 설정하여 보안제어를 통합보안관리시스템 엔진을 통하여 해당 에이전트에게 전달한다[6]. [그림 2]는 통합보안관리시스템의 전체 구성도를 나타낸다.

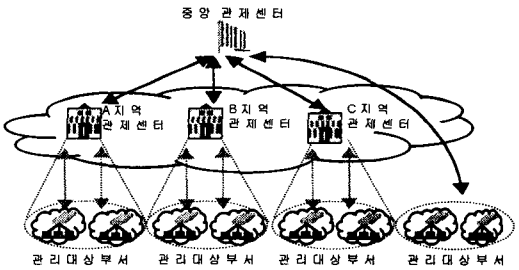


[그림 2] 통합보안관리시스템 구성도

3. 계층적 구조의 통합보안관리시스템

1) 계층적 구성방안

통합보안관리시스템을 구축하기 위해서는 지원범위와 관리 도메인을 확정한 후, 관리기능을 전하는 것이 바람직하며, 이때 고려되어야 할 것은 에이전트 추가에 따른 시스템 확장성의 보장이다. 대규모 네트워크의 통합보안관리시스템의 전체구성은 지역과 운영조직을 고려하여 중앙 관제센터, 부 관제센터, 관리대상으로 3단계로 구성한다. 하나의 통합관리시스템에서 관리 가능한 관리대상의 수는 환경에 따라 매우 다르다. 그것은 대상 보안시스템의 이벤트 발생횟수 및 양에 따라 크게 영향을 미치기 때문이다. 국방전산망에서의 계층 구조는 [그림 3]과 같이 중앙 관제센터, 지역 관제센터, 관리대상부서로 계층을 구분하고, 관리대상부서의 대상 시스템 수와 지역을 고려하여 지역 관제센터를 추가 설치 운영한다.



[그림 3] 계층적 구성

2) 기능 및 구성요소

중앙 관제센터와 지역 관제센터는 지역의 관리대상부대의 수와 트래픽 양에 따라 서버에 대한 구성이 달라질 수 있지만 기본적인 구성은 동일하

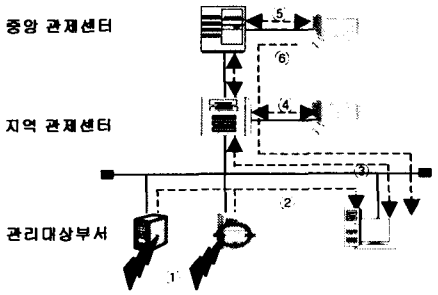
다. 각 계층별 주요 기능 및 구성요소는 [표 1]과 같다.

[표 1] 계층별 기능 및 구성요소

계층 구분	기 능	구성요소
중앙 관제센터	· 종합 상황 모니터링 · 지역 관제센터 보고에 따른 상황 분석 및 대응 · 보안정책 설정 · 유관기관과의 협조	· 센터서버 · 웹서버 · 센터콘솔 · 상황판
지역 관제센터	· 관리대상부서 이벤트 통합 · 보안 전문가에 의한 원격 보안 조치 · 상황 감시 및 보고 · 중앙 관제센터 보안설정에 따른 정책실행	· 센터서버 · 웹서버 · 센터콘솔 · 상황판
관리대상 부서	· 보안 시스템 운영 · 관리 · 지역 관제센터로 이벤트보고 · 시스템 관리자에 의한 기본 조치	· 사이트 서버 · 보안시스템

3) 동작 시나리오

[그림 4]는 국방전산망에서의 계층 구조간 통합 보안관리시스템 동작 수행과정을 설명한다.



[그림 4] 동작 시나리오

① 보안 시스템으로부터 침입행위 발생, 취약점 및 바이러스 감지

② 관리대상부서 서버로 이벤트 전송

③ 이벤트 통합 및 지역 관제센터로 이벤트 전송

㉮ 경고메시지 발생, 지역 관제센터로 이벤트 전송

㉯ 이벤트 유형 및 위험도에 따른 자동조치 및 사이트 시스템 관리자에 의한 기본조치

㉰ 지역 관제센터로 조치사항 전송

④ 지역 관제센터 이벤트 통합 및 조치

㉮ 상황판 경고 발생 (→ 중앙 관제센터로 이벤트 전송)

㉯ 각 지역 CERT팀에 침해 사실통보

㉰ 보안 전문가에 의한 원격 조치

㉱ 처리보고서 작성(→ 관리대상부서 및 중앙 관제센터로 전송)

⑤ 이벤트 발생 상황 및 처리에 대한 모니터링

㉮ 상황판 경고 발생

㉯ 중앙 CERT 팀에 침해사실 통보

㉰ 필요시 유관기관과 협조

㉱ 침해내용 분석 및 조치사항 판단 등 종합 분석 실시 (최초 공격지 및 공격루트 추적)

㉲ 위험도 판단에 따른 보안정책 설정 판단

⑥ 중앙 관제센터에 보안 정책 하달

(→ 관리대상부서에 대한 보안정책 설정)

V. 결론

본 논문에서는 대규모 네트워크 환경에서 다양한 침입행위를 탐지하기 위한 보안 시스템의 상호 연동 모델을 분석하여 대규모 조직에 적합한 계층적 구조의 통합보안시스템 구축에 관한 방안을 제시하였다. 제시된 통합보안시스템은 중앙 집중적인 관리에서 지역적 분산 개념으로의 시스템 운영으로 네트워크의 트랙픽과 서버의 부하를 감소시킬 수 있고, 하부의 관리대상 증가에 따른 확장성과 기능성을 보장할 수 있으며, 다단계 침해행위 추출을 통해 탐지결과에 대한 신뢰성부여 및 오판율을 최소화할 수 있다. 또한 사고 대응 및 복구를 위한 통합된 환경 제공과 보안전문가 부족 등에 따른 인력의 효율적 운용이 가능하다. 향후 본 논문에서 제시된 계층적 구조의 통합보안시스템에 대한 전산망 환경에서의 성능 검증 및 보완 작업으로 좀더 발전된 보안 시스템의 연동방안 연구가 이루어진다면 보다 효율적인 전산망 보안 체계를 확립할 수 있을 것이다.

참고문헌

[1] 한국정보보호진흥원, 정보보호 표준교재, 한국정보보호진흥원, 1999.

[2] 이만영 외, 전자상거래 보안 기술, 생능출판사, 1999.

[3] 안철수, "신종 바이러스 대응체계 구축", SIS2000, 2000.

[4] 안혜연, "통합보안관리시스템", 제7회 정보통신망 정보보호 워크숍, 2001.

[5] 어울림정보기술, ASEN(Adaptive Security for Enterprise Network), 어울림정보기술, 2000.

[6] 이동영 외4명, "SNMP를 이용한 웹기반의 통합보안관리시스템", 한국정보처리학회 추계학술대회 논문집, 1998