論 文
5-4-2

침입 방지를 위한 능동형 통합 보안 관리 시스템
Active Enterprise Security Management System for Intrusion Prevension

박재성(Jae-Sung Park)[1] 박재표(Jae-Pyo park)[2] 김원(Won Kim)[3] 전문석(Moon-Seog Jun)[4]

요약

최근 시스템과 네트워크를 위협하는 해킹, 바이러스 등의 공격이 증가하고 있다. 기존의 시스템 보안이나, 네트워크 관리 시스템(NMS)만 가지고는 다양하고 강력한 위협들에 대해서 안전하지 못하다. 따라서 Firewall, IDS, VPN, LAS(Log Analysis System) 등의 보안 시스템을 구축하여 시스템과 네트워크를 위협으로부터 방어해 왔다. 하지만 보안 시스템간의 상호 연계성이 부족하여 효과적인 대응체계를 마련하지 못하고 중복 보안으로 인한 비효율성이 지적되었다. 이에 대한 대책으로 통합 보안 관리가 필요하게 되었고 위협에 대해 적극적으로 대처할 수 있는 능동형 보안이 필요하게 되었다. 최근에는 통합 보안 관리(Enterprise Security Management), 침입자 추적(Intrusion Tracking), 침입자 유인(Intrusion Induction) 등으로 좀 더 효과적이고 적극적인 보안 네트워크를 구성할 수 있다. 하지만 이 시스템들 또한 업체별 보안 시스템간의 상호 연동이 어려운 실정이고 대응 조치 또한 체계적이지 못하며 위협을 사전에 방지하지 못하고 사후 대처에 급급한 실정이다. 따라서 본 논문에서는 원격에서 안전하게 네트워크를 관리할 수 있는 능동형 통합 관리 모듈을 제안한다.

Abstract

Attacks such as hacking, a virus intimidating a system and a network are increasing recently. However, the existing system security or network management system(NMS) cannot be safe on various threats. Therefore, Firewall, IDS, VPN, LAS(Log Analysis System) establishes security system and has defended a system and a network against a threat. But mutual linkage between security systems was short and cannot prepare an effective correspondence system, and inefficiency was indicated with duplication of security. Therefore, an active security and an Enterprise Security Management came to need. An effective security network was established recently by Enterprise Security Management, Intrusion Tracking, Intrustion Induction. But an internetworking is hard for an enterprise security systems , and a correspondence method cannot be systematic, and it is responded later. Therefore, we proposes the active enterprise security management module that can manage a network safely in this paper.

1) 정회원 : 숭실대학교
2) 정회원 : 숭실대학교
3) 정회원 : 전주기전여자대학
4) 정회원 : 숭실대학교

논문접수 : 2004. 4. 20.
심사완료 : 2004. 4. 27.

1. 서 론

인터넷과 컴퓨터기술의 발전으로 인하여 시스템과 네트워크를 위협하는 해킹, 바이러스 등의 공격이 증가하고 있다. 기존의 시스템 보안이나 네트워크 관리 시스템(NMS)만 가지고는 다양하고 강력한 위협들에 대해서 안전하지 못하다. 따라서 Firewall, IDS, VPN, LAS(Log Analysis System) 등의 보안 시스템을 구축하여 시스템과 네트워크를 위협으로부터 방어해 왔다. 하지만 보안 시스템간의 상호 연계성이 부족하여 효과적인 대응체계를 마련하지 못하고 중복 보안으로 인한 비효율성이 지적되었다. 이에 대한 대책으로 통합 보안 관리가 요구 되었고 위협에 대해 적극적으로 대처할 수 있는 능동형 보안이 필요하게 되었다. 최근 통합 보안 관리(Enterprise Security Management), 침입자 추적(Intrusion Tracking), 침입자 유도(Intrusion Induction) 등으로 좀 더 효과적이고 적극적인 보안 네트워크를 구성할 수 있었다. 하지만 이 시스템들 또한 업체별 보안 시스템간의 상호 연동이 어려운 실정이고 대응 조치 또한 체계적이지 못하며 위협을 사전에 방지하지 못하고 사후 대처에 급급한 실정이다. 따라서 네트워크 위협에 대해서 능동적이고 체계적인 대응 체계를 갖춘 침입 방지를 위한 능동형 통합 보안 관리 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 제 2절에서는 시스템 보안, 네트워크 보안, 통합 보안 관리, 능동형 보안 구조의 장단점을 살펴보고, 제 3절에서는 기존의 보안 구조를 개선한 능동형 통합 보안 관리 모듈을 제안한다. 제 4절에서는 실제 침입을 시도할 때에 능동적으로 침입 방지가 되는지 성능 평가를 한다. 또한 안전한 로그 전달이 되는지 확인한다. 제 5절에서는 결론 및 향후 연구 방향을 제시한다.

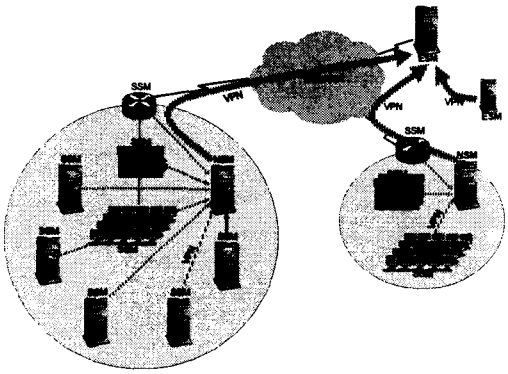
2. 관련연구

정보 통신과 컴퓨터기술의 발전과 함께 불법 침입으로 인한 정보 시스템에 대한 위협 또한 급속히 증가하고 있다. 패스워드 추측, 버퍼오버플로우, 백도어, 바이러스, Dos공격 등의 시스템 공격 기술도 점점 다양화되고 지능화 되어가고 있다. 따라서 안전한 시스템 운영을 위하여 물리적 보안, 계정 관리, 파일 관리, 응용 프로그램 관리, 로그 관리와 같은 여러 가지 보안 장치가 필요하게 되었다. 그러나 시스템 보안은 전체적인 네트워크 보안이 어렵고 관리자의 시스템 관리 능력에 따라 시스템 보안이 좌우되는 단점이 있다. 또한 수동적 대응 체계를 가지고 있어 안전한 시스템 관리가 힘들다. 시스템 보안만 가지고는 Sniffing, Spoofing, Hijacking, RPC 공격, Virus 등의 네트워크 공격에 대하여 안전하지 못하여 네트워크 전체를 관리할 수 있는 NMS, Firewall, IDS, VPN, LAS 등의 보안 시스템 등이 필요하게 되었다. 이러한 보안 시스템은 각각의 네트워크 보안 요소간의 연계성이 부족하고 지엽적인 보안으로 인한 보안성이 결여될 수 있을 뿐만 아니라 중복 보안으로 인한 효율성이 저하 될 수 있다. 이러한 단점들 때문에 통합 보안 관리가 필요하게 되었으나 통합 보안 관리 모델 또한 업체별 보안 시스템간의 상호 연동을 위한 호환이 어렵고 적극적인 대응 체계를 갖추지 못하고 있다[1]. 따라서 점차 다양하고 강력해지는 공격들에 대하여 효과적으로 대응하기 위하여 침입 방지, 침입자 추적, 침입자 증거 수집, 침입 유도, 침입 감내 등의 능동형 보안이 필요하게 되었다. 현재 다양한 능동형 보안 방법들이 등장했지만 이 또한 보안 모듈간의 상호 연계성이 부족하고 지엽적 보안으로 보안성이 결여되고 중복 보안으로 네트워크와 시스템 효율성이 저하되는 문제점을 가지고 있다[2][3].

따라서 본 논문에서는 네트워크 위협에 대해서 능동적이고 체계적인 대응 체계를 가진 침입 방지를 위한 능동형 통합 보안 관리 시스템을 제안한다.

3. 능동형 통합 보안 관리

AESM(Active Enterprise Security Module)은 통합 보안 관리와 능동형 보안의 장점을 살리고, 단점을 제거하여 능동형 통합 보안 관리를 하기 위한 보안 모듈로써 SSM(System Security Module), NSM(Network Security Module), ESM(Enterprise Security Module)의 세 모듈로 구성 되어있다. 각 모듈은 로그 관리, 시스템 상태 관리, 시스템 관리, 프로그램 관리, 보안 관리의 5가지 기능을 가지고 있으며 모든 기능은 원격지에서도 접근가능하다.



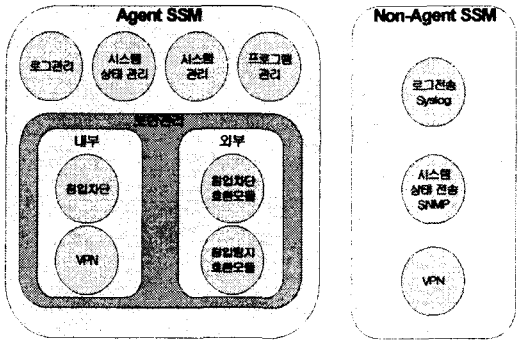
[그림 1] AESM 전체 구조

[fig. 1] AESM total structure

그림 1은 능동형 통합 보안 관리 모듈의 전체 구조를 나타내고 있다.

3.1 SSM (System Security Module)

방화벽, 웹 서버, 파일 서버, 라우터, 기타 네트워크에 연결되어 메시지를 주고받을 수 있는 장치들이 SSM으로 동작할 수 있다. 또한 하나의 네트워크에 여러 개의 SSM이 존재 할 수 있다. SSM은 Agent SSM과 Non-Agent SSM으로 구성되어 있다. Agent SSM은 Agent 설치가 가능한 시스템이나 네트워크 장비에 설치된 모듈로써 다음의 기능을 수행한다. 첫째, SSM 자체의 로그를 파일이나 DB에 저장 및 관리하며 NSM로 로그 정보를 안전하게 전달한다. 둘째, SNMP 프로토콜을 사용하여 시스템의 상태 및 동작중인 프로그램들을 변경하고 관리한다. 셋째, 외부로부터의 접근을 통제하기 위한 침입 차단과 NSM과의 안전한 통신을 위한 VPN 그리고 기존의 침입 차단, 탐지 시스템과의 호환기능이 있다[4]. Non-Agent SSM은 Agent 설치가 불가능한 시스템이나 네트워크 장비로써 표준 syslog 프로토콜이 지원되는 시스템이나 네트워크 장비에서 NSM로 로그를 전송하고 표준 SNMP 프로토콜이 지원되는 시스템이나 네트워크 장비에서 시스템 상태정보를 NSM로 전송 한다. 또한 표준 VPN 프로토콜이 지원되는 시스템이나 네트워크 장비는 NSM과 VPN을 연결한다.



[그림 2] SSM 구조

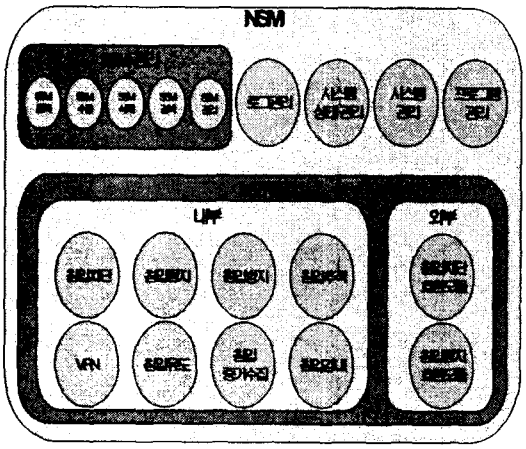
[fig. 2] SSM structure

그림 2는 SSM의 구조를 나타내고 있으며 Agent SSM은 안전하게 원격 관리가 가능한 모듈이며 Non-Agent SSM은 관리자의 수동 설정으로 가능한 표준화된 모듈이다[5].

3.2 NSM (Network Security Module)

NSM은 SSM을 관리하기 위한 모듈로써 하나의 네트워크에 한 개의 NSM이 존재한다. NSM은 첫째, Agent가 설치된 SSM의 로그 관리, 시스템 상태 관리, 시스템 관리, 프로그램 관리, 보안 관리를 한다. 둘째, NSM 자체

의 로그나 SSM으로부터 전달되어진 로그를 분류하고 DB에 저장한다. 또한 ESM로 로그 정보를 안전하게 전달할 수 있다. 셋째, SNMP 프로토콜을 사용하여 시스템의 상태를 관리한다[7]. 넷째, 시스템내의 계정 및 파일 관리를 하며 동작중인 프로그램들을 변경하고 관리한다. 다섯째, 외부로부터의 접근을 통제하기 위한 침입 차단기능이 있고, NSM과의 안전한 통신을 위한 VPN 기능이 있다. 또한 기존의 침입 차단, 탐지 시스템과의 호환성을 위한 침입 차단, 탐지 호환 기능이 있으며, 능동형 보안을 위한 기능이 있다.



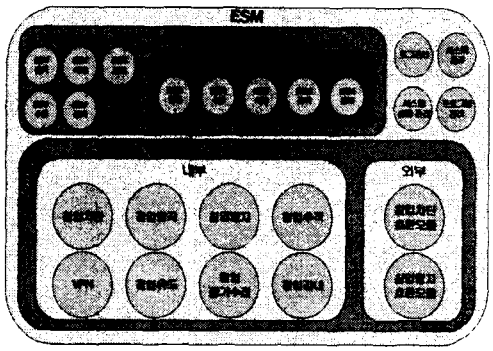
[그림 3] NSM 구조

[fig. 3] NSM structure

그림 3은 NSM의 구조를 나타내고 있다. SSM 관리부분에서는 동일 네트워크내의 SSM을 감지하여, 등록하고, 수정, 삭제, 검색 및 관리한다. 그 외 모듈 등은 원격에서 VPN을 통하여 안전하게 관리한다[6].

3.3 ESM(Enterprise Security Module)

ESM은 NSM이나 하위 ESM을 관리하기 위한 모듈이며 외부 네트워크에 존재할 수 있다. ESM은 첫째, NSM의 SSM 관리, 로그 관리, 시스템 상태 관리, 시스템 관리, 프로그램 관리, 보안 관리를 한다. 둘째, ESM 자체의 로그나 NSM으로부터 전달되어진 로그를 분류하고 DB에 저장한다. 또한 상위 ESM로 로그 정보를 안전하게 전달한다. 그 외는 NSM과 동일한 기능을 수행한다.



[그림 4] ESM 구조

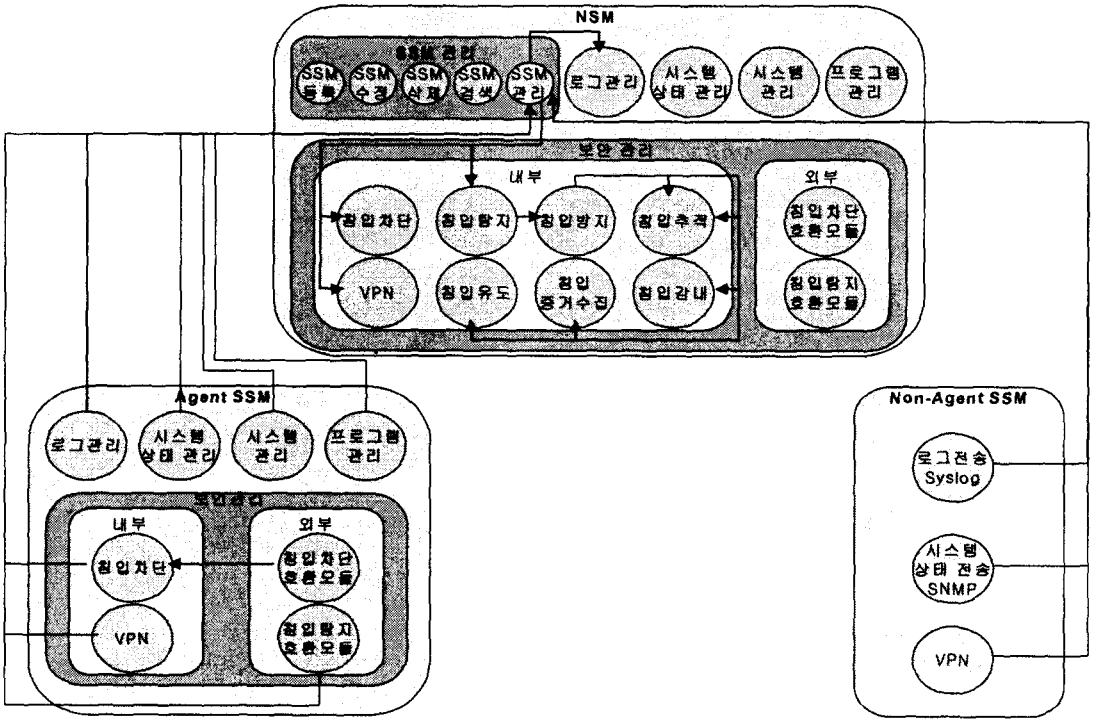
[fig. 4] ESM structure

그림 4는 ESM의 구조를 나타내고 있다. NSM 관리부분에서는 동일 네트워크내의 NSM을 자동 감지하거나, 관리자가 임의로 등록, 수정, 삭제, 검색 및 관리한다. 그 외 모듈들은 원격에서 VPN을 통하여 안전하게 관리한다.

3.4 AESM 동작

3.4.1 SSM과 NSM과의 동작

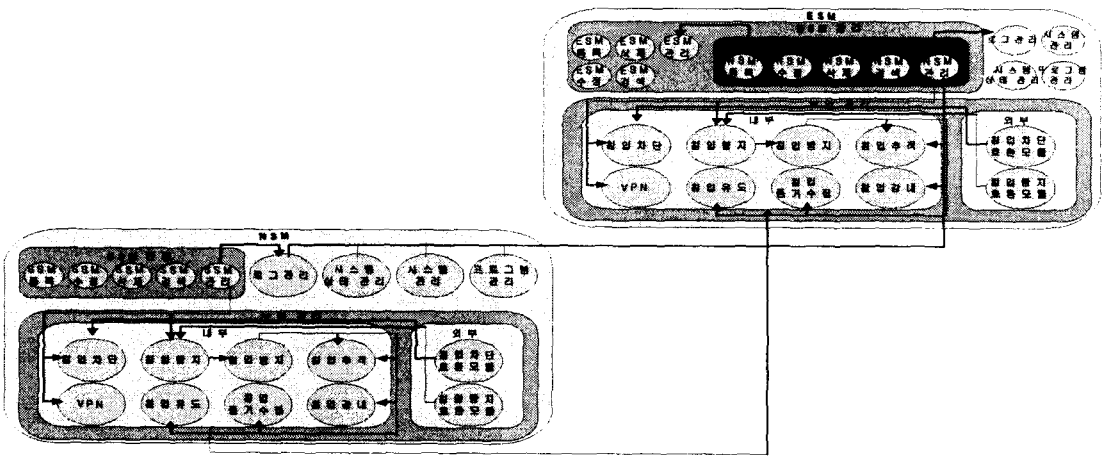
그림 5는 SSM과 NSM과의 동작을 나타내고 있다. Agent SSM에서는 NSM으로 정보를 전달하고, NSM은 Agent SSM과 VPN 인증을 거쳐 안전한 원격 관리를 수행한다. Non-Agent SSM은 표준화된 로그 전송, 시스템 상태 전송, VPN 등을 통하여 정보를 전송한다. NSM은 SSM으로 받은 정보를 가지고 로그 관리 모듈에서 로그 필터링을 하여 DB로 저장한다. 또한 SSM은 침입 탐지, 침입 차단, VPN 모듈에 정보를 전달한다.



[그림 5] SSM과 NSM간의 동작

[fig. 5] Operation between SSM and NSM

3.4.2 NSM과 ESM과의 동작

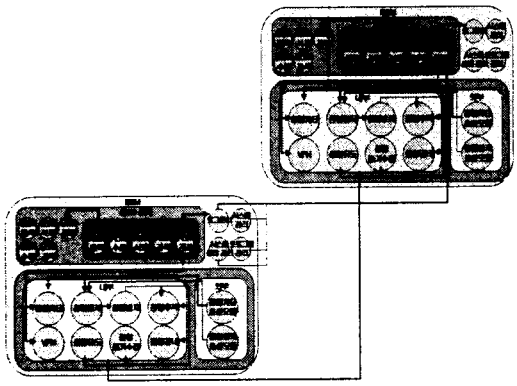


[그림 6] NSM과 ESM간의 동작

[fig. 6] Operation between NSM and ESM

그림 6은 NSM과 ESM과의 동작을 나타내고 있다. NSM은 ESM으로 정보를 전달하고, ESM은 NSM과 VPN 인증을 거쳐 안전한 원격 관리를 한다. ESM은 NSM으로부터 받은 정보를 가지고 로그 관리 모듈에서 로그 필터링을 하여 DB로 저장한다. 또한 ESM은 NSM의 보안 관리 모듈을 원격에서 관리한다.

3.4.3 ESM과 ESM과의 동작

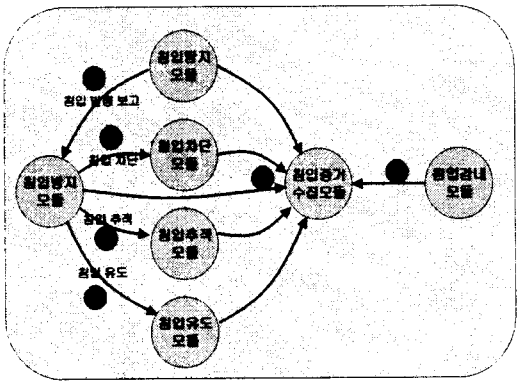


[그림 7] 상위 ESM과 하위 ESM간의 동작
[fig. 7] Operation between upper layer ESM and lower layer ESM

그림 7은 상위 ESM과 하위 ESM과의 동작을 나타내고 있다. 하위 ESM은 상위 ESM으로 정보를 전달하고 상위 ESM은 하위 ESM과 VPN 인증을 거쳐 안전한 원격 관리를 수행한다. 상위 ESM은 하위 ESM으로부터 받은 정보를 가지고 로그 관리 모듈에서 로그 필터링을 하여 DB로 저장하다. 또한 상위 ESM은 하위 ESM의 보안 관리 모듈을 원격에서 관리한다.

3.4.4 보안 관리 모듈 동작

그림 8은 보안 관리 모듈의 동작을 나타내고 있다. 침입 탐지 모듈에서 공격을 탐지하면 침입 방지 모듈로 이벤트를 발생 시키고 설정된 규칙에 따라, 침입 유도, 침입 차단, 침입 추적의 이벤트를 발생 시킨다. 그리고 모든 보안 관리 모듈은 침입 증거 수집 모듈에 정보를 전달한다. 또한 예상치 못한 침입이 발생한 경우 시스템 자원을 보호하고 복구하기 위하여 관리자가 침입 감내 모듈을 이용하여 시스템을 복구 할 수 있다.

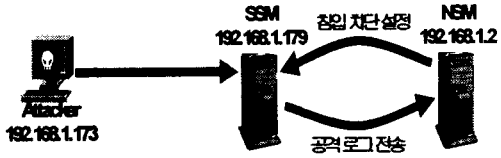


[그림 8] 보안 관리 모듈의 동작
[fig. 8] Operation of Security Management Modular

4. 성능 분석 및 평가

4.1 침입 방지 모듈 작동 여부

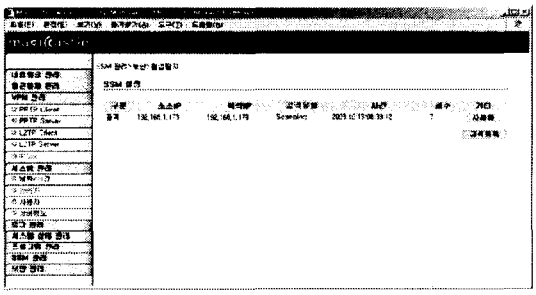
침입 방지 모듈의 작동 여부를 테스트하기 위하여 임의 SSM 모듈을 공격하여 자동으로 침입 차단이 되는지 테스트한다.



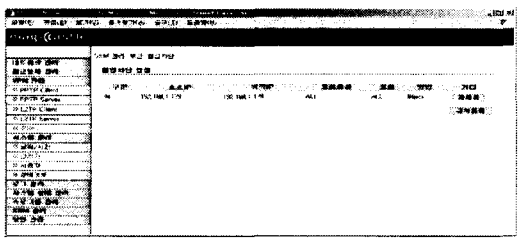
[그림 9] 침입 방지 모듈의 테스트 시나리오
[fig. 9] Test Scenario of Intrusion Prevention Module

테스트 시나리오는 그림 9에서처럼 공격자가 SSM에 스캐닝 공격을 시도하면 SSM은 공격 로그를 NSM에 전달하고 NSM은 자체 침입

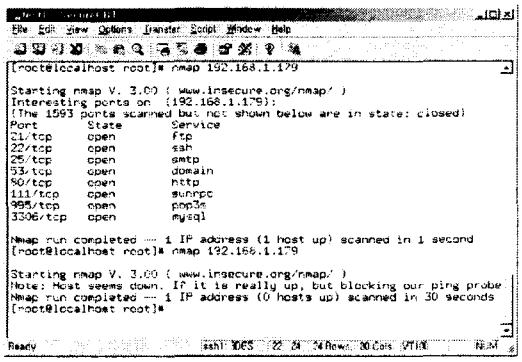
탐지 모듈에 의해서 공격을 판단하여 자동으로 SSM에 침입 차단 설정을 한다. 공격자(192.168.1.173)는 SSM (192.168.1.179)에 nmap을 사용하여 스캐닝 공격을 시도하면 SSM은 공격 로그를 NSM에 전달하고 NSM은 자체 침입 탐지 모듈에 의해서 그림 10과 같이 침입을 탐지하고 그림 11과 같이 자동으로 SSM에 침입 차단 설정을 한다. 제대로 침입 차단 설정이 되었는지 nmap을 사용하여 다시 스캐닝 공격을 했지만 응답이 없음을 확인할 수 있다. 재공격 시 그림 12와 같이 시스템이 차단됨을 확인할 수 있다.



[그림 10] 침입 탐지 화면
[fig. 10] An Intrusion Detection Screen



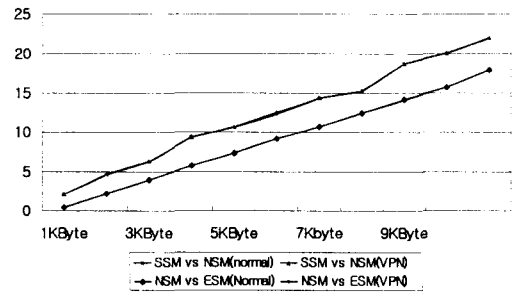
[그림 11] 자동으로 침입 차단된 화면
[fig. 11] The screen that it was blocked off an intrusion automatically



[그림 12] 재공격 시 시스템 차단 화면
[fig. 12] A system interception screen about a reattack

4.2 모듈 간 VPN 성능 테스트

SSM, NSM, ESM 각 모듈 간 VPN 설정을 했을 때와 안 했을 때를 비교하여 AESM 모듈을 사용 할때에 얼마큼의 성능을 낼 수 있는지 테스트 한다. SSM, NSM, ESM 모듈에 VPN 설정을 하기 전과 후에 각각 패킷 크기를 늘려가며 전송 속도를 측정하였다. 각 모듈 간 패킷 크기를 1 KByte에서 10 KByte까지 1 KByte 단위로 하여 10번씩 측정하였다.



[그림 13] 모듈간 VPN 성능 테스트 결과
[fig. 13] The VPN performance test results between modules

그림 13과 같이 SSM, NSM 간 속도와 NSM, ESM 간 속도는 약 1.6ms의 성능 감소를 나타

내고 1KByte 당 0.35ms의 성능 감소가 나타나는 것을 알 수 있다. 보안 로그의 크기는 10KByte 미만이므로 안전하고 효과적인 실시간 로그 전달을 할 수 있다.

5. 결론 및 발전방향

본 논문에서는 통합 보안 관리와 능동형 보안을 개선한 안전한 능동형 통합 보안 관리 모듈 AESM을 제안하였다. 기존의 통합 보안 관리의 단점인 능동형 보안 요소를 적용함으로써 침입에 대해 능동적으로 대처할 수 있도록 했다. 침입 추적, 침입 유도, 침입 증거 수집, 침입 감내 모듈과 침입 탐지, 침입 차단 모듈을 결합함으로써 중복 보안의 비효율성을 제거하고 지엽적 보안 결점을 제거하였다. 세 단계의 Agent 구조로 이루어져서 권한의 한계가 명확하고 VPN 인증을 통한 원격 관리가 가능하기 때문에 안전한 원격 보안 관리를 할 수 있다. 하지만 침입 방지 모듈의 오판 율이 있고 관리자의 규칙 설정과 능력에 의존적인 것이 많다. 좀 더 지능화된 침입 방지 모듈을 추가 한다면 훨씬 더 강력한 보안 모듈이 될 것이다.

참고문헌

[1] 이만영, 차세대 네트워크 보안 기술, 생능출판사

[2] 방효찬 외 3인, "액티브 네트워크를 이용한 능동 보안 관리 프레임워크", Proc. of COMSW2002, pp200-303, July 2002.

[3] 손승원, "Active Security 기술 발전 전망", 정보처리학회 Sigcom Review Vol.1, pp.95-107, March 1999.

[4] D. New, M Rose, RFC 3195 "Reliable Delivery for syslog", November 2001.

[5] U. Blumenthal, B. Wijnen, RFC 3414 "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", December 2002.

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

박 재 성

2002년 숭실대학교 컴퓨터학부(학사)
2004년 숭실대학교 대학원 컴퓨터학과(석사)
2004년~현재 숭실대학교 대학원 컴퓨터학과 박사과정
관심분야 : VPN, ESM, Mobile Embeded System

박 재 표

1996년 숭실대학교 컴퓨터학부(학사)
1998년 숭실대학교 대학원 컴퓨터학과(석사)
2001년 숭실대학교 대학원 컴퓨터학과 박사과정 수료
1998년~현재 국립 한경대학교 컴퓨터공학과 강사
관심분야 : 전자상거래 보안, 컴퓨터 통신, 영상처리, 멀티미디어 보안

김 원
1988년 숭실대학교 전자계산학과(학사)
1993년 숭실대학교 대학원 컴퓨터학과(석사)
1997년 숭실대학교 대학원 컴퓨터학과(박사)
1995~현재 전주기전여자대학 실용예술학부 조교수
관심분야 : 멀티미디어 통신, 멀티미디어 저작권 보호, 컴퓨터 알고리즘

전 문 석

1980년 숭실대학교 컴퓨터공학과(학사)
1986년 University of Maryland 전산과 (석사)
1989년 University of Maryland 전산과(박사)
1989년 Morgan State University 전산수학과 조교수
1989년~1991년 New Mexico State University 부설 Physical Science Lab. 책임연구원
1991년~현재 : 숭실대학교 정보과학대학 정교수
관심분야 : 네트워크보안, 컴퓨터알고리즘, 병렬처리, VLSI 설계, 암호학