제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

차세대 인터넷 서버의 보안 시스템 설계

김강호*, 안창원*, 정성인*
*한국전자통신연구원
e-mail : khk@etri.re.kr

Design of a Security System on the Next Generation Internet Server

Kangho Kim*, Chang-won Ahn*, Sungin Jung*
*Electronics and Telecommunications Research Institute

요 약

최근 인터넷 환경이 널리 퍼지면서 인터넷 서버들의 보안위협은 갈수록 증가하고 있다. 이러한 인터넷 서버의 보안 사고를 예방하기 위하여 기관들은 정보보호 솔루션인 방화벽, 침입탐지 시스템, 바이러스 백신, 보안운영체제 등을 도입하였으나 개별적인 보안 솔루션을 적용함으로써 관리 효율성이 떨어지고 보안 사고 위험은 증가하고 있다. 그래서 현재는 개별 보안 솔루션을 통합관리하는 ESM 을 도입하고 있다. 차세대인터넷 서버도 인터넷에 연결되어 있어서 해킹으로부터 자유로울 수 없기 때문에 차세대 인터넷 서버에 적합한 ESM 이 필요하다. 우리는 공개 소프트웨어 보안 도구를 조합하여 응용 프로세스 레벨에서 가볍고 기본 보안 기능을 충실히 갖춘 ESM 을 설계하였다. 본 논문에서는 그 ESM 의 설계 내용을 중심으로 자세히 소개하고, 현재까지 구현된 결과도 간략히 소개한다.

1. 서론

최근 인터넷 환경이 널리 퍼지면서 인터넷 웜, 바이러스, 해킹 등과 같은 보안 위협요소들은 갈수록 증가하는 추세이며 그로 인해 인터넷에 연결된 컴퓨터의 보안 위협은 늘어나고 있다. 서버에 저장된 기업의 중요 자료나 고객의 신상명세가 해킹에 의해 유출되거나 파괴된다면 기업으로서는 큰 손실이다. 또한 인터넷 서비스를 제공하는 기업의 인터넷 서버가 해킹으로 파괴된다면 복구하기 위해 투입되는 비용과 서비스가 중단된 동안의 비용을 부담해야 한다[2].

이러한 인터넷 서버의 보안 사고를 예방하기 위하여 기업은 정보보호 솔루션인 방화벽(firewall), 침입탐지시스템(IDS), 바이러스 백신, 보안운영체제(secure OS) 등을 도입한다. 그러나 필요한 보안 영역마다 개별적인 보안 솔루션을 적용함으로써 전체적인 관리가 이루어지지 않아 관리 효율성은 갈수록 떨어지고 보안 사고 위험은 증가하고 있다. 그래서 현재는 그 동안 개별적으로 도입해온 각종 보안 시스템을 통합 관리하는 ESM(Enterprise Security Management) 솔루션을 요구하고 있다[3]. ESM 은 방화벽, IDS(HIDS, NIDS), VPN 을 하나의 툴에서 관리한다. 따라서 기업이 개별적으로 도입해온 각종 보안 솔루션을 통합관리도구가 설치된 서버에서 하나의 콘솔로 관리할 수 있다.

지난 2000 년부터 등장한 ESM 은 관리인력을 최소화하기 위한 로그 통합에서 출발했지만 이 후 보안 제품의 연동이라는 관점에서 중요하기 다루어지기 시작했다. 2001 년부터는 ESM 과 연동하는 각 보안 제품에 대한 이해를 기반으로 침입 탐지 기능을 높이는 작업이 진행되었다. 많은 로그 이벤트를 관리자에게 그대로 보여주는 것이 아니라 일정 기준에 따라 선별해서 실시간 대응체제를 갖추자는 것이다[3].

차세대 인터넷 서버(NGIS)[4]는 일반 기업의 웹 서버처럼 인터넷에 연결되어 있어서 인터넷을 통하여 웹 서비스와 같은 일반적인 인터넷 서비스를 제공할 뿐만 아니라 고품질 영화 스트리밍 서비스를 제공하는 서버이다. NGIS 도 인터넷에 연결되어 있기 때문에 다른 인터넷 서버처럼 보안사고로부터 자유로울 수 없다. 해킹과 같은 공격으로부터 NGIS 를 보호하기 위해서 NGIS 에 적합한 ESM 을 개발하였고, 그 ESM 을 SafeGaurd 라 한다. 본 논문에서는 SafeGuard 를 소개한다.

본 논문은 2 장에서 NGIS 를 간단히 소개하고, 3 장은 SafeGuard 를 설계시 요구사항들을 설명한다. 4 장은 요구사항을 반영한 SafeGuard 설계를 설명하고, 5 장은 설계에 따른 현재 구현 결과물을 화면 단위로 설명한다. 마지막으로 6 장에서 결론과 함께 앞으로 추가 또는 개선할 점들을 정리한다.

2. 차세대 인터넷 서버

차세대 인터넷 서버(Next Generation Internet Server, NGIS)는 고성능 인터넷 환경, 고품질 무선통신 환경, 높은 인터넷 사용률을 보유한 한국에서 인터넷 기반 가상 공동체(cyber community) 서비스를 제공하기 위한 시스템이다. 고품질 정보통신 서비스를 제공하기 위해서 고대역폭 네트워크가 필요하고 그 대역폭이 전역적, 지역적으로 고르게 분산되어 있어야 한다. 몇 개의 서버가 서비스를 제공하면 백본(backbone) 네트워크의 사용량이 늘어나서 백본 네트워크 증설 비용도 증가할 뿐만 아니라 서비스 요구도 집중되어 서버에 과부하가 걸릴 수 있다.

NGIS 는 이러한 문제점을 해결하기 위하여 설계되었다. NGIS 는 네트워크 대역폭을 효율적으로 사용하기 위해서 정보통신 서비스를 전역과 지역 서비스로 구분한다. 넓은 지역에 서비스를 제공하는 서버는 전역서버(global server)이고 IDC, 전자정부, 디지털 도서관, 새로운 산업을 위한 응용서비스를 제공한다. 좁은 지역에 서비스를 제공하는 지역서버는 회사, 대학교, 아파트 단지와 같이 지역 네트워크에 바탕을 둔 지역 공동체를 위한 서비스를 제공한다. 지역서버는 일종의 서비스 캐쉬와 같은 역할을 담당하는데 최종사용자가 의식하지 못하지만 전역서버와 협동하여 서비스를 제공한다.

지역서버의 내부는 고품질 스트리밍 서비스를 제공하기 위한 NS 카드 최대 4 개, 일반 인터넷 서비스를 위한 일반 기가비트이더넷(*GbE*) 카드 2 개가 설치되어 있다. NS 카드는 각각 하나의 GbE 카드를 포함하고 있지만 스트리밍 데이터를 전송 용도로만 사용한다. 나머지 2 개의 일반 *GbE* 카드가 일반 인터넷 서비스 또는 스트리밍 서비스의 연결, VCR 동작 요청, 단절 등의 메시지를 받는다. 그러므로 NS 카드의 GbE 은 네트워크 보안이 필요 없고 일반 GbE 의 트래픽은 감시해야 한다.

NGIS 의 지역서버는 기업의 전산실 또는 IDC 등과 같이 전문 시스템관리자가 지역적으로 가까운 곳에서 서버를 관리하지 못하는 곳, 즉 아파트 단지의 MDF 실과 같은 곳에 설치되어 운영되기 때문에 좀 더 완벽한 보안 기능을 요구하고, 손쉬운 원격 관리는 반드시 필요하다.

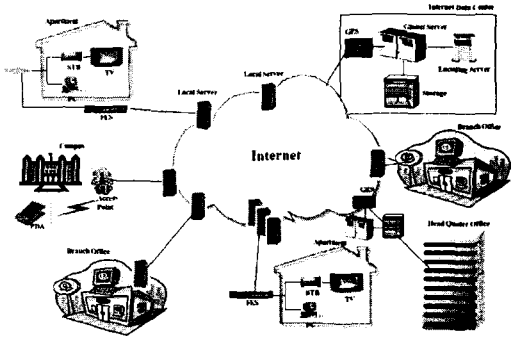


그림 1: NGIS 서비스 개념도

3. NGIS 보안 시스템 요구사항

이 장에서는 NGIS 환경에서 필요한 보안 시스템 요구사항을 설명한다.

TCSEC 기준 C2 레벨 이상

NGIS 는 리눅스 커널을 기반으로 개발되기 때문에 기본설정인 상태에서는 보안등급은 TCSEC 기준으로 볼 때, C1 레벨(level) 이상 C2 레벨 미만의 상태이다. 여기에 적절한 보안 도구를 적용하여, NGIS 의 보안 수준을 C2 레벨 이상 B1 레벨 미만으로 유지할 수 있도록 NGIS 의 보안 아키텍처를 재구성한다.

서버보안

컴퓨터 보안은 크게 컴퓨터 네트워크 보안과 네트워크 말단에 연결된 서버의 보안으로 나눌 수 있다. NGIS 의 보안 시스템은 서버의 보안만을 구현하는 것을 목표로 한다. 네트워크 보안은 다른 도구들을 도입하여 구현할 것이다.

응용 프로세스로 구현

완벽한 서버의 보안을 구현하기 위해서는 서버의 네트워크 계층, 플랫폼/운영체제 계층, 응용/데이터 계층에 전체에 각 계층별로 그림 2에 나열한 차원(dimension)에 여러 가지 보안 기능을 구축해야 한다. 그 기능들을 운영체제의 커널에 구현하는 방법과 응용 프로세스로 구현하는 방법이 있는데 우리는 후자를 채택한다.

응용 프로세스로 구현함으로써 여러 가지 장점이 있다: (1) 운영체제 커널의 변화에 둔감하고; (2)기능확장이 쉽고 (3)커널 컴파일이 필요 없고 (4) 서버 운영 중 기능을 설치 또는 삭제가 용이하다. 응용 프로세스로 구현함으로써 발생하는 보안상의 부족한 점은 보안 운영체제(Secure OS)를 도입함으로써 해결하는 것이 바람직하다.

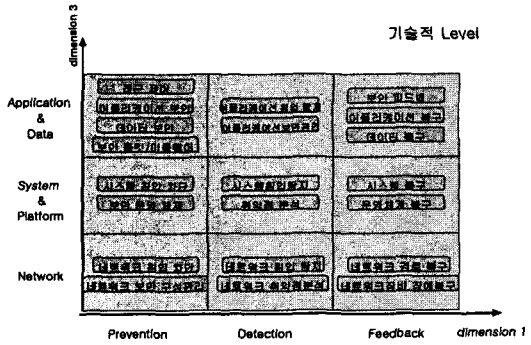


그림 2: 정보보안 아키텍처의 기술적 레벨

ESM 지원 및 시스템관리 시스템과 연동

컴퓨터 보안에 완벽한 것이란 없지만 최대한 보안이 철저한 서버를 만들기 위해서는 개별적으로 개발되어 있는 컴퓨터 보안 도구들을 적절히 설치하여 각 기능의 장점을 살리고 단점을 서로 보완해야 한다.

개별적인 컴퓨터 보안 기능을 구현한 도구들은 로그 분석기, 서비스 접근제어기, 방화벽, HIDS(Host-based Intrusion Detection System), NIDS(Network-based Intrusion Detection System), 파일 무결성 검사기 등의 형태로 공개소프트웨어 또는 상용 소프트웨어로 개발되어 있다. 개별 도구 간의 연동을 구현하여 좀 더 완전하고 능동적인 보안을 실현할 수 있도록 이들을 통합한 ESM 기능을 제공한다. NGIS 는 지역/광역 서버를 원격관리하기 위하여 시스템 관리 시스템(System Management System, SMS)를 개발하고 있다. NGIS 의 보안관리는 이 SMS 에 통합되어 시스템 관리의 일환으로 통합 보안 관리 기능을 제공한다.

공개소프트웨어 활용

ESM 을 개발하기 위해서 필요한 개별 보안 도구들은 표 1에 정리된 것처럼 안정된 기능들이 다양하게 구현되어 있다. 다양한 개별 도구 중에서 비용절감과 원천코드 확보 측면을 고려하여 SafeGaurd 를 구현할 때는 공개 소프트웨어를 최대한 활용하기로 한다.

NGIS 도 인터넷에 연결되어 외부에 노출되어 있기 때문에 외부의 공격에 취약점을 가질 수 있다. 이 취약성을 최소화하기 위하여 제공하는 서비스를 제한하고, 접근제어와 방화벽(firewall)을 사용하여 서비스 받을 수 있는 클라이언트의 수를 최소화하였다. 접근제어와 방화벽으로 서버를 일정수준으로 보호할 수 있으나 그 기능만으로 충분하지 않다. 그래서 서버의 보안 기능에 침입탐지시스템(Intrusion Detection System, IDS), 파일 무결성 검사 및 파일 복구 기능을 추가하였다.

표 1: 보안 도구

구분	공개소프트웨어	상용소프트웨어
IDS	Snort[6] Prelude Grsecurity Snare[5] LIDS	수호신 IDS SecureWorks IDS NeoWatcher (NIDS) NeoGuard(HIDS)
SecureOS	-	RedOwl
Firewall	ipchains, iptables	수호신 firewall SecureWorks Firewall NeoGate 인터가드 화랑
파일무결성 검사	Tripwire	Tripwire
ESM	-	수호신 ESM SecureWorks ESM 인젠 ESM spider-1

개별 보안 도구를 유형별로 간단히 설명하면 다음과 같다.

- **IDS**: 이 시스템은 알려진 공격 또는 활동에 대해서 시스템(서버 또는 네트워크)을 감시하고, 공격이 탐지되면 시스템 관리자가 적절한 조치를 취할 수 있도록 관리자에게 알려준다.
- **방화벽**: 침입자가 외부망에서 내부망으로 접근하려는 경로를 차단하는 S/W 또는 H/W 이다.
- **파일 무결성 검사**: 파일 무결성 검사 및 파일 복구외부 기능은 서버의 파일 시스템에 저장된 파일이 의도적인 외부 공격에 의하여 변경되었는지를 검사할 때 사용된다. 의심스런 파일 변경이 발견되면 관리자에게 알린다.
- **접근 제어**: 이 기능은 시스템으로의 네트워크적인 접근과 시스템 자체에서의 정보자원에 대한 접근을 통제한다.

4. 보안 시스템 구조

이 절에서는 그림 3에 표현된 NGIS 보안 시스템의 전체적인 구조를 설명한다. SafeGuard 는 관리대상 시스템(managed system)에 설치되고, SafeGuard 가 정리한 로그를 SMS 서버가 SMS agent 를 통하여 읽어 가는 구조로 되어 있다. 이러한 구조는 에이전트/관리자 구조로 원격관리가 가능하도록 한다.

NGIS 의 보안 관리는 3 장에서 언급한 기본적인 서버보안 기능을 통합하는 것을 목표로 한다. 통합보안관리(Enterprise Security Management, ESM)을 통하여 여러 개별 보안 기능을 하나의 시스템으로 통합할 수 있고, 그로 인하여 쉬운 관리, 개별 기능간의 연동을 제공한다. 관리대상 시스템에 설치되는 SafeGuard 는 그림 1 과 같은 모듈로 구성되어 있다.

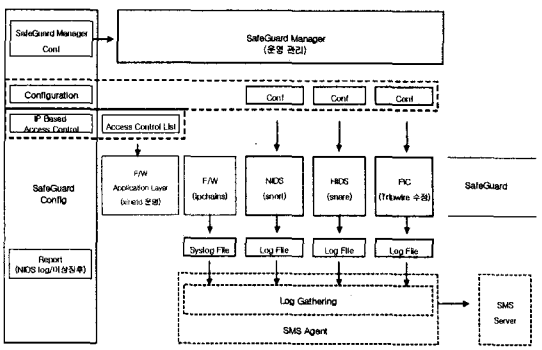
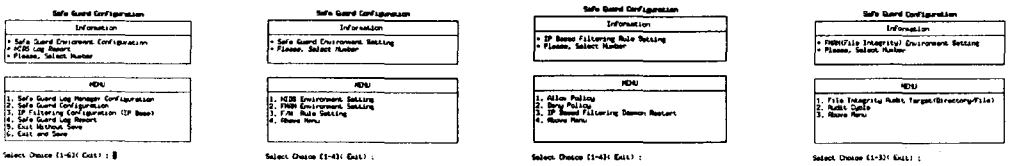


그림 3: SafeGuard 모듈 구성도

SafeGuard 는 SafeGuard Config 와 SafeGuard Manager 로 구성되어 있다. SafeGuard Config 는 각 개별 보안 도구의 설정을 관리하고, SafeGuard Manager 는 개별 도구가 생성한 로그를 침입 심각도(criticality) '상', '중,' '하' 세 단계로 구분하여 별도의 파일에 저장한다. '중' 또는 '하'로 구분된 로그는 SMS 서버가 주기적으로 로그 파일의 내용을 읽어 가도록 한다. '상'으로 구분된 로그가 발생하면 로그 파일에 기록함과 동시에 SNMP 트랩(trap)을 통하여 SMS 서버에 전송하고, SMS 서버는 트랩 메시지를 받는 즉시 관리자에게 통보하여 적절한 보안 조치를 취하도록 한다.

SafeGuard 를 구현할 때 사용한 개별 보안 도구들은 다음과 같다.



(a) 초기화면 (b) 환경 설정 (c) IP 기반 접근제어 (d) FMAN 환경설정

그림 4: SafeGuard 설정 화면

- **접근제어**: xinetd 버전 2.3.7-2 를 사용하여 서비스 기반 IP 단위 접근제어를 구현하였다. IP 주소, 도메인명, 도메인, 접근허용시간을 지정할 수 있다[4].
- **방화벽**: ipchains 버전 1.3.10 을 사용하였다. *ipchains* 는 응용 프락시 서버를 이용한 방화벽과 패킷 필터링을 이용한 방화벽 중에서 패킷 필터링 방법을 사용한다. 패킷 필터링을 사용하여 특정 패킷을 허용(accept), 거절(reject), 취소(deny)할 수 있다.
- **HIDS**: snare-0.9-1 을 사용하였다. Snare 는 서버의 각 사용자별 시스템 호출(system call) 사용 기록을 자세히 남겨주고 그 기록을 분석하여 침입을 탐지한다. SafeGuard 는 snare 의 기본 기능에 심각도가 4 인 경우 해당 로그를 발생시킨 프로세스를 강제로 죽이는 기능을 추가로 구현하였다.
- **NIDS**: snort 2.0 사용하였다. Snort 는 이미 알려진 네트워크 공격에 관한 룰(rule)을 정의하고 그 룰에 적용되는 네트워크 트래픽 패턴을 발견하면 네트워크 공격으로 판단하여 공격 내용을 로그 파일에 남긴다. 이 기능은 관리자의 조작 하에서 방화벽과 연동될 수 있다.
- **파일 무결성 검사 및 복원**: 파일 무결성 검사는 tripwire 를 우리의 목적에 맞게 수정한 것(FMAN)을 사용한다. 복원 기능은 SMS 서버의 도움을 받아서 구현한다. FMAN 을 통하여 파일 변조를 탐지해내고 그 이벤트를 SMS 서버에 전송하여 관리자가 파일변조 사실을 알게 된다. 무단 변조된 파일이면 SMS 서버에 저장된 원본 파일로 변조된 파일을 복구한다.

5. 구현 화면

이 절에서는 SafeGuard 의 구현 결과를 화면 단위로 설명한다. 현재는 그림 4처럼 SafeConfig 를 텍스트 기반 인터페이스 형태로, 각 서버에서 개별 보안 도구들을 통합한 사용자 인터페이스 중심으로 구현되어 있다.

SafeGuard Config 를 통한 설정에 따라 SafeGuard Manager 가 침입탐지를 분석하여 SafeGuard 로그 파일에 기록하면 그림 5와 같이 SMS 를 통하여 보안 로그를 살펴 볼 수 있다. 현재는 SafeGuard 의 설정 기능이 SMS 와 통합되어 잇지 않기 때문에 서버의 보안 설정을 변경하려면 그 서버에 직접 로그인한 후 SafeGuard config 를 통해서 가능하다.

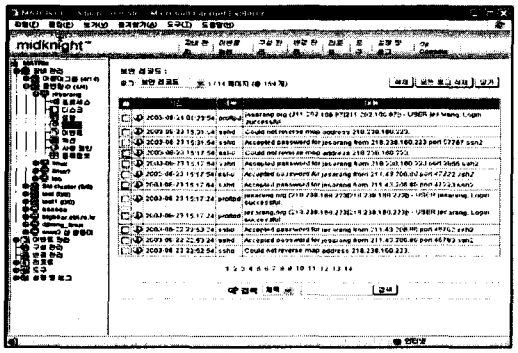


그림 5: SMS 의 보안로그 조회 화면

6. 결론

응용 계층에서 공개소프트웨어만 사용하여 가볍고, 만족할 만한 성능과 기능을 갖춘 ESM 을 구현하였다. 기존의 많은 상용 보안 시스템들이 많은 기능과 강력한 성능을 가지고 있지만 제대로 활용되지 못한 것은 많은 기능을 지원하기 위한 복잡한 사용법이 원인이라고 추측된다. SafeGuard 는 기존 상용 제품의 그러한 문제점을 피해가면서 기본적인 보안기능을 충실히 달성하고, 그 결과 시스템의 보안관리 효율성을 높일 수 있을 것이라고 기대한다. SafeGuard 를 상품화한다면, 다른 상용 제품과 차별성을 부과시켜서 충분히 시장 경쟁력도 있을 것이라고 기대한다.

아직 구현 중이어서 아직 SafeGuard 의 완전한 모습을 소개하지 못했지만 SafeGuard 설정 및 기타 편의 기능을 SMS 와 사용자 인터페이스 수준에서 완전한 통합을 실현하여 다수의 서버를 원격지에서 쉽게 관리할 수 있는 진정한 의미의 ESM 을 구현할 계획이다.

참고문헌

[1] "침입방지시스템 기술현황과 전망," 정보홍, 김정녀, 손승원, 주간기술동향, 통권 1098 호, 2003. 6

[2] "서버보안 이것이 해답이다.", www.secureosforum.org, 2002.

[3] "ESM 을 활용한 기업의 보안 시스템 관리," hackersnews.org, 2002.7.

[4] "Hacking Linux Exposed: Linux security secrets & solutions," Brian Hatch, 2001

[5] Snare homepage, www.intersectalliance.com

[6] Snort homepage, www.snort.org