제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

안전한 네트워킹을 위한 통합 보안 엔진의 보안 관리 프레임워크 구현

조수형*, 김정녀*
*한국전자통신연구원 보안운영체제연구팀
e-mail : {shjo,jnkim}@etri.re.kr

The Implementation of Integrated Security Engine's Management System for Secure Networking

Su-Hyung Jo*, Jeong-Nyeo Kim*
* Secure Operating System Research Team, ETRI

요 약

인터넷이 가지고 있는 보안 취약성 때문에 바이러스, 해킹, 시스템 침입, 시스템 관리자 권한 획득, 침입사실 은닉, 서비스거부공격 등과 같은 다양한 형태의 네트워크 공격에 노출되어 있다. 이러한 네트워크 공격으로 인해 인터넷에 대한 침해가 증가하고 있어 공공기관과 사회기반시설 및 금융 기관은 피해 규모와 영향이 크다. 따라서, 인터넷 침해를 최소화하기 위해 동적으로 침입을 감지하고 제어할 수 있는 보안 기술이 필요하다. 본 논문에서는 네트워크의 패킷을 필터링하고 침입을 탐지하며 불법 침입을 통보하는 커널 수준의 통합 보안 엔진을 설계하고 구현하여 안전한 네트워킹 환경을 제공하며, 보안 환경의 변화에 민첩하게 유기적으로 대처할 수 있는 통합된 관리 방법을 제시한다.

1. 서론

인터넷의 급속한 발전과 보급으로 네트워크 환경은 점점 거대해지고 있으며, 인터넷의 간편하고 편리한 네트워크 접속과 제공하고 있는 다양한 서비스로 인하여 그 형태가 복잡해지고 있다. 그러나, 바이러스, 해킹, 시스템 침입, 시스템 관리자 권한 획득, 침입사실 은닉, 서비스거부공격 등과 같은 다양한 형태의 네트워크 공격으로 인해 인터넷은 항상 해킹의 위험에 노출되어 인터넷에 대한 침해가 증가하고 있고, 공공기관과 사회기반시설 및 금융 기관은 피해 규모와 영향이 점점 증가하고 있다.

인터넷의 핵심 요소인 라우터는 네트워크의 데이터 패킷흐름을 제어하고 적합한 목적지에 도달하는 최적의 길을 결정한다. 라우터의 오류 또는 라우터에 대한 공격에 의한 피해는 전체 네트워크에 대한 피해가 될 수 있다. 즉, 라우터는 내부와 외부 네트워크 사이나 서로 다른 네트워크 사이에서 트래픽을 관리하는 장치이다. 따라서, 라우터에 대한 보안 기술이 인터넷의 침해를 막기 위해 반드시 필요하다. 그러므로, 라우터에 대한 접근제어를 제공하고 불법 네트워크 침입을 막는 네트워크 보안 기술이 필요하다.

또한, 기존 네트워크의 보안 방식은 단일 기능의 개별적 보안 시스템 위주로 구현되어 보안 시스템간의 상호 연동이 어려우며 정보 보호 인프라의 구축이 복잡하고 어렵다. 정보 통신기술의 진화에 따라 새롭게 등장하는 보안 취약점에 따라 발생 가능한 여러 유형의 사이버 테러에 능동적으로 강력하게 대응할 수 있는 통합 보안 네트워킹이 요구되고 있다.

본 논문에서는 네트워크 공격에 대응하는 보안 기능을 갖는 라우터나 게이트웨이 등의 네트워크 노드를 위해 커널 영역에서 패킷 필터링, 침입 분석 및 감사 추적[1, 2], 인증 및 접근제어를 제공하는 통합 보안 엔진을 설계하였다. 그리고, 통합 보안 엔진을 보안 정책[3, 4]에 의해 관리하고, 웹 브라우저를 사용하여 플랫폼에 관계없이 보안 관리를 제공하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 웹 브라우저를 사용하여 보안 관리를 제공하기 위한 기술에

대하여 설명한다. 3 장에서는 보안 관리 프레임워크의 구조를 설계하고, 4 장에서는 설계한 구조에 따른 구현 예를 제시한다. 그리고, 5 장에서 결론을 맺는다.

2. 웹 기반의 관리에 필요한 기술

웹 브라우저를 사용자 인터페이스(GUI)로 사용하여 웹 기반의 관리 시스템을 구현하는 JSP 기술에 대하여 설명한다. 그리고, 영어와 한글을 모두 지원하는 GUI 를 만들기 위해 자바의 Internationalization 기법에 대하여 알아본다.

2.1 JSP (Java Server Page)

JSP (Java Server Page)는 서블릿으로 웹 페이지의 내용이나 형태를 제어하는 기술이다. 서블릿이란 동적 컨텐츠를 생성하는 웹 컴포넌트로 서블릿 컨테이너에 의해 관리되는 프로그램이다. 자바 프로그래밍에서 서블릿은 javax.servlet.Servlet 인터페이스를 이행하는 자바클래스이다. 그리고, 대부분이 HTTP 프로토콜 서비스를 지원하는 javax.servlet.http.HttpServlet 을 확장한 http 서블릿이다. 이진코드로 컴파일된 서블릿은 웹 서버에 동적으로 탑재되어 서블릿 컨테이너에 의해 실행된다. 서블릿은 서블릿 컨테이너에 의해 이행되는 요청과 응답의 패러다임을 통해 웹 브라우저와 상호작용한다. 서블릿 컨테이너는 서블릿이라는 웹 컴포넌트를 담는 그릇으로 서블릿의 탑재, 인스턴스화 및 초기화 등 서블릿의 생명주기를 관리한다. 서블릿 컨테이너는 요청/응답 프로토콜로 최소한 HTTP/1.0 을 지원해야 하며, HTTP/1.1 지원을 강력하게 권고하고 있다. 경우에 따라서는 HTTPS(HTTP over SSL)을 기반으로 하는 요청/응답 프로토콜을 지원할 수도 있다.

JSP 는 웹 개발자와 디자이너가 웹 페이지를 빠르게 개발할 수 있고, 쉽게 유지 보수 할 수 있도록 도와준다. 그리고, 플랫폼에 관계없이 손쉽게 웹 기반의 응용을 개발 할 수 있도록 해준다. 서블릿은 웹 개발자에게 웹 서버 기능을 확장할 수 있는 단순하고 일정한 메커니즘을 제공하므로 현재 많은 개발자들이 서블릿을 이용하여 웹 응용을 개발하고 있다.

2.2 Java Internationalization

Internationalization(국제화)은 응용 프로그램을 수정하지 않고 다수의 언어와 지역적 특성에 적용될 수 있도록 하는 응용 프로그램의 디자인 과정이다. 이와 반대로 응용프로그램에 지역적으로 독특한 요소들을 추가하고 문구를 변환함으로써 특정 지역이나 언어에 적합하도록 하는 Localization(지역화)가 있다. 다시 말하면, 국제화는 컨텐츠를 모든 나라의 사람들이 볼 수 있도록 지원하는 것이고, 지역화는 반대로 특정 나라나 특정 언어를 사용하는 사람들에게 제한되어 볼 수 있게 하는 것이다.

국제화 프로그래밍을 함으로써, 지역화된 데이터를 포함하여 같은 프로그램이 언어나 지역적 특성에 적합한 형태로 수행될 수 있다. 그리고, 상태 메시지, GUI 컴포넌트의 라벨 등과 같은 문자 요소가 프로그램에 직접 삽입되지 않고 소스 코드와 분리되어 저장되며 동적으로 로드된다. 또한 새로운 언어를 제공하기 위하여 프로그램을 다시 컴파일 하지 않아도 되고 날짜와 통화 단위와 같은 문화에 종속적인 데이터는 사용자가 거주하는 지역과 사용하는 언어에 적합한 형태로 표현된다. 프로그래밍 순서는 다음과 같다.

1) property 파일이나 ResourceBundleList 를 상속받아 English 버전과 Korean 버전의 클래스를 생성한다.

2) locale 을 정의한다.

3) resourceBundle 을 생성한다.

4) resourceBundle 로부터 텍스트를 가져온다.

5) 상태 메시지, GUI 컴포넌트의 라벨 등과 같은 문자 요소를 설정한다.

3. 보안 관리 프레임워크의 설계

통합 보안 엔진은 커널 영역에서 패킷 필터링, 침입 분석 및 감사 추적, 인증 및 접근제어를 제공하여 네트워크를 안전하게 구성하고 관리하는 보안 기술이다. 라우터나 게이트웨이와 같은 네트워크 노드에 통합 보안 엔진을 탑재하여 안전한 네트워킹을 제공할 수 있다.

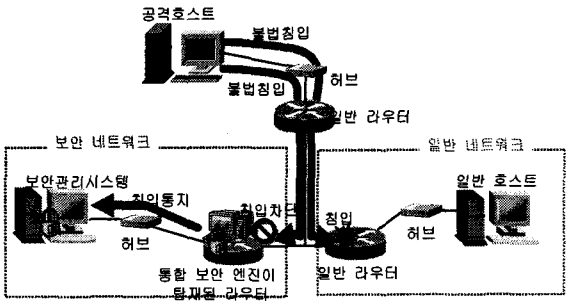

그림 1. 보안 관리 프레임워크의 구성도

그림 1 은 공격 시스템으로부터 침입을 차단하고 제어하는 보안 관리 프레임워크의 구성도이다. 통합 보안 엔진이 탑재된 라우터와 관리 시스템으로 보안 네트워크를 구성한다. 공격시스템은 외부 네트워크에서 허브와 일반 라우터을 거쳐 보안 네트워크와 일반 네트워크에 공격을 시도한다. 통합 보안 엔진이 탑재된 라우터는 필터링 정책과 침입 탐지 정책을 이용하여 네트워크 공격을 탐지하여 차단하고 이를 보안관리 시스템에 통지한다. 통합 보안 엔진으로 구성된 보안 네트워크는 침입을 차단하여 네트워킹을 원할히 수행할 수 있다. 그러나, 일반 네트워크는 침입이 발생하면 공격을 당해서 일반 라우터는 일반 시스템으로 라우팅을 수행하지 못한다.

통합 보안 엔진은 다음과 같은 기능을 제공한다. 필터링 정책에 의해 허가된 패킷은 수신하고, 허가되지 않은 패킷을 거부하는 기능, 침입 탐지 정책에 의해 네트워크의 침입을 분석하고 침입에 대응하는 기

능, 허가 받지 않은 사용자가 시스템을 사용하는 것을 막고 모든 주체는 객체에 접근 할 수 있는 권한을 가진 경우에만 접근이 가능하도록 제어하는 기능, 보안에 필요한 필터링 정책, 침입 탐지 정책, 접근제어 정책을 결정하는 기능, 결정된 정책을 적용하는 기능, 통합 보안 엔진을 관리하는 기능을 제공한다.

통합 보안 엔진은 패킷 필터링과 침입 분석을 어플리케이션 영역이 아닌 커널 영역에서 제공하여 침입 탐지를 최적화하고 불법 네트워크 침입에 실시간으로 대응하는데 이용된다. 통합 보안 엔진을 보안 정책에 의해 관리하여 안전한 네트워킹 환경을 제공하고, 웹 브라우저를 사용하여 관리의 편리성과 효율성을 제공한다.

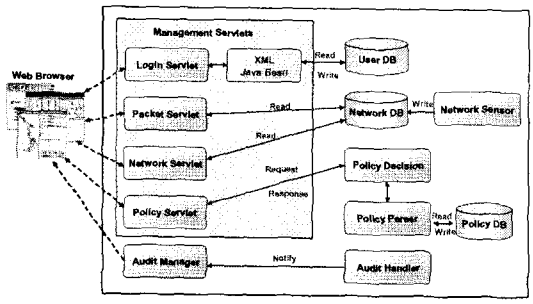

그림 2. 보안 관리 시스템의 구조

그림 2 는 보안 관리 시스템의 구조이다. 보안 관리 시스템은 management servlet, network sensor, policy decider, policy parser, audit manager, audit handler 와 데이터베이스로 구성된다. 웹 브라우저를 실행하여 보안관리 GUI 에 접속하고, 웹을 통해 관리 명령을 내린다. 사용자 ID 와 비밀번호를 입력하면, Login 서블릿은 XML Java Bean 을 통해 사용자 데이터베이스에 접근하여 응답한다.

Network sensor 는 호스트 정보, 라우팅 정보, 패킷 정보와 같은 네트워크 정보를 수집하여 Network DB 에 저장한다. Network DB 에 의 내용을 가지고 Packet 서블릿과 Network 서블릿은 네트워크의 구성 현황을 지도로 보여주며 패킷의 통계를 처리한다. 인터페이스 카드 종류, IP 주소, 하드웨어 주소, MTU 크기, 상태 및 옵션의 네트워크 인터페이스 정보와 OS 정보, 부팅 경과 시간, 현재 시간, 시스템 이름, 디스크 크기의 시스템 정보를 보여주고, 라우팅 테이블의 추가, 삭제 및 수정을 할 수 있다. 프로토콜과 인터페이스 별로 패킷 통계정보로 보여주고, 라우터와 시스템들의 네트워크 상황을 지도로 구성하여 보여준다.

Policy decider 는 네트워크 침입 탐지를 위한 정책을 결정하고, Policy parser 는 데이터베이스의 정책 내용을 변환한다. Audit manager 와 Audit handler 는 불법 접근, bad packet, 침입의 경보를 처리한다. 라우터가 DoS 공격이나 바이러스 공격을 받으면 공격내용을 보안관리 GUI 에 실시간으로 표한다. Policy DB 는 접근제어 규칙, 필터링 규칙, 침입 탐지 규칙의 정책에 대한 데이터베이스이다.

4. 보안 관리 프레임워크의 구현

Linux Kernel 2.4.18 (Red Hat 7.3)에서 정책 기반의 보안 관리 시스템을 개발하고 있다. JSP 서버 프로그램으로 톰캣 4.0.4 과 자바 컴파일러로 JDK 1.3.1[5]을 사용한다. 톰캣 4.0[6]은 웹 서버 기능과 JSP 1.2/Java Servlet 2.3 Container 의 JSP [7]서버 기능을 모두 지원하는 프로그램이다. 서블릿 컨테이너는 웹 서버나 애플리케이션 서버와 결합되어 요청과 응답 패러다임에 따라 네트워크 서비스를 제공한다. 톰캣 4.0 은 각 사용자 별 Session 관리를 지원한다.

사용자가 웹에서 바로 응용 프로그램을 시작하고 Stand Alone 응용으로 동작시킬 수 있는 Java Web Start[8]를 사용한다. Java Web Start 는 애플릿과 웹 기반의 응용이 가지는 장점들을 모두 가지며 Stand Alone Application 의 장점을 동시에 제공하는 자바 실행 프레임워크이다. 초기에 한번 전체 구성요소를 다운로드하고 서버에서 Java Web Start Application 을 구성하는 구성요소가 변경되면, 자동으로 다운로드하여 클라이언트에 설치한다. Java Web Start 를 설치 후 MIME 유형을 설정하는데, 파일 확장자는 "jnlp"이고 MIME 유형은 "application/x-java-jnlp-file"이다.

관리 시스템에 로그인하면 HTTP 프로토콜로 네트워크 서블릿을 통하여 구성정보를 검색하고 GUI 에 네트워크 구성을 Map 으로 보여준다.

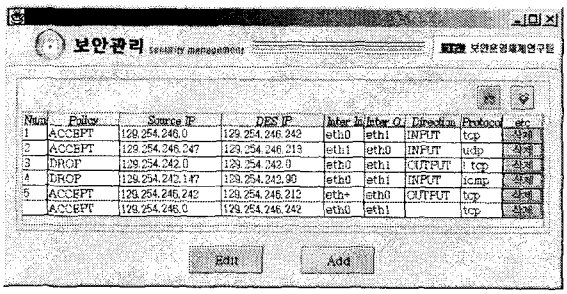

그림 3. 패킷 필터링 정책 화면

그림 3 은 패킷 필터링 정책에 대한 화면이다. 필터링 정책은 발신지 주소, 목적지 주소, 입력 인터페이스, 출력 인터페이스, 발신지 포트번호, 목적지 포트번호, 프로토콜 종류, 프로토콜의 세부 옵션에 따라 허가와 거부의 행동을 취한다. 필터링 정책에 의해 허가된 패킷은 수신하여 침입 분석 및 감사 추적 모듈로 전달하고, 허가되지 않은 패킷을 거부한다. 침입 분석 및 감사 추적 모듈이 패킷을 검사하기 전에 필터링 정책에 의해 패킷을 1 차적으로 분류하여 네트워크 공격에 대한 처리 효율을 높일 수 있다.

네트워크에 침입이 발생하면 이를 Audit Manager 에게 알려준다. Audit Manager 는 침입 탐지 메시지를 받

아 GUI 에 디스플레이 하기 위하여 데이터 변환하여 디스플레이 한다. 전달하는 이벤트들은 Java Object Serialization 을 이용한 자바 객체에 설정하여 객체를 직접 전달한다.

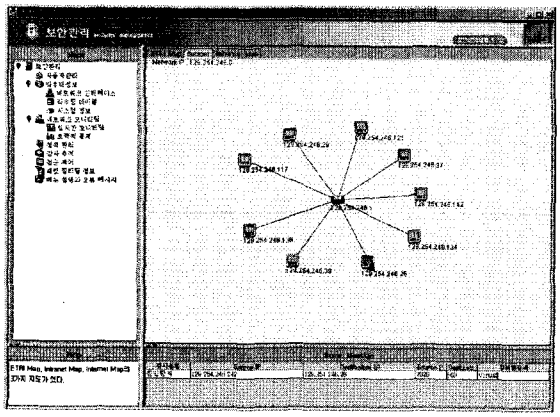

그림 4. 네트워크 침입 탐지 화면

그림 4 는 네트워크 침입을 탐지하여 침입 내용을 보여주는 화면이다. 침입으로 탐지된 패킷의 발신지 주소, 목적지 주소, 발신지 포트, 목적지 포트, 침입 종류의 정보를 보여주고, 해당 호스트의 아이콘을 변화시킨다. 실시간 Audit 메시지를 Audit Manager 를 통하여 GUI 에게 전달한다. Audit 메시지를 수신할 GUI 는 반드시 이벤트 수신에 앞서 Audit Manager 에 등록되어야 한다. Audit Manager 는 수집되는 이벤트의 손실을 막기 위해 Event Queue 를 사용하며 수집과 전송을 별도의 Thread 를 사용하여 처리한다. Audit Manager 는 웹 서버인 Tomcat 과는 별도의 프로세스로 운영된다. 관리 시스템의 GUI 는 자바로 구현하여 자바를 지원하는 모든 시스템에서는 운영체제와 무관하게 운용될 수 있다.

5. 결론

통합 보안 엔진은 네트워크를 구성하는 게이트웨이, 라우터, 스위치 등과 같은 네트워크 노드에 보안 기능을 부가하여 안전한 네트워킹을 제공할 수 있는 보안 기술이다. 통합 보안 엔진은 패킷 필터링과 침입 분석을 어플리케이션 영역이 아닌 커널 영역에서 제공하여 침입 탐지를 최적화하고 시스템의 성능 오버헤드를 최소화하며 불법 네트워크 침입에 실시간으로 대응하는데 이용된다. 이러한 통합 보안 엔진을 보안 정책에 의해 관리 및 제어하여 안전한 네트워킹 환경을 제공하고, 웹 브라우저를 사용하여 관리의 편리성과 효율성을 제공한다.

참고문헌

[1] Stephen Northcutt and Judy Novak, Network Intrusion Detection. An Analyst's Handbook, 2nd ed. New Riders, 2001.
[2] IETF Intrusion Detection Working Group http://www.ietf.org/html.charters/idwg-charter.html
[3] IETF Policy Working Group http://www.ietf.org/html.charters/policy-charter.html
[4] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, The Common Open Policy Service Protocol: RFC 2748, January 2000. http://www.ietf.org/rfc/rfc2748.txt
[5] Java, http://java.sun.com/
[6] Tomcat, http://jakarta.apache.org/
[7] JSP, http://java.sun.com/products/jsp/
[8] Java Web Start http://java.sun.com/products/javawebstart/
[9] 조수형, 김정녀, "침입 탐지를 위한 정책 기반의 보안 관리", 제 29 회 한국정보과학회 추계학술대회, October 2002.