OSGi 프레임워크 기반의 침입차단서비스[1]

강철범[0] 장희진 송병욱 김상욱
경북대학교 컴퓨터과학과
{cbkang[0], janghj, bwsong, swkim}@woorisol.knu.ac.kr

Firewall Service based on OSGi Framework Environment

Chulbum Kang[0], Heejin Jang, Byungwook Song, Sangwook Kim
Dept. of Computer Science, Kyungpook National University

요 약

홈 네트워크가 갈수록 많이 사용되고, 또 그에 따른 보안에 대한 수요도 늘어나고 있다. 본 논문에서는 침입차단시스템을 OSGi 프레임워크 기반의 서비스형태로 구현한다. 침입차단시스템은 JES에서 여러 가지 모니터링 및 제어 서비스의 형태로 나타나고 외부의 유무선 클라이언트는 이러한 서비스를 통해 홈 네트워크 내부에 있는 침입차단시스템을 제어한다. 이 침입차단시스템은 보안상태기반의 트래픽으로 그 위험여부를 판단하며 JES를 사용하면 환경에 상관없이 자유롭게 서비스를 이용할 수 있다. 본 논문에서는 PDA와 같은 무선 클라이언트에서 침입차단시스템에 대한 제어서비스를 구현한다.

1.서론

개방형 서비스 게이트웨이(OSGi)[1]는 원거리 네트워크를 근거리 네트워크나 홈 네트워크와 연결해 준다. OSGi 프레임워크의 핵심적인 임무는 다양한 서비스를 제공하는 것인데 현재 OSGi 프레임워크는 HttpService, LogService, AdminService 등의 홈 네트워크를 위한 기본적인 서비스를 제공한다. 홈 네트워크 내부를 안전하게 보호하기 위해 보안서비스가 요구되며 특히 홈 네트워크 외부에서도 내부의 보안관련시스템을 제어할 수 있도록 OSGi 프레임워크 상에 보안관련서비스를 정의할 필요가 있다.

본 논문은 OSGi 프레임워크 기반의 침입차단서비스를 제안하고 구현하였다. 이러한 서비스는 침입차단시스템[2,3,4]의 기능을 홈 게이트웨이를 통해 서비스의 형태로 제공한다. 이로써 외부에 있는 관리자는 자신이 설정한 정책에 의하여 위험여부를 판정할 수 있고 또한 내부의 상황을 실시간으로 외부에 있는 관리자에게 알림으로서 관리자가 그에 상응한 조치을 취할 수 잇게 한다

본 논문의 제2절에서는 OSGi 프레임워크 기반의 침입차단서비스에 관련되는 OSGi, JES(Java Embedded Server)[5,6]에 대해 간략히 소개하고 제3절에서는 침입차단시스템의 작동원리와 JES를 통한 침입차단서비스 제공을 보여주고 외부 클라이언트와 침입차단시스템간의 통신 구조를 보인다. 제4절에서는 PDA와 같은 무선클라이언트에서의 침입차단시스템제어를 구현 예로 보이고 제5절에서 결론 및 향후 연구 방향을 제시한다.

1. 본 연구는 정보통신연구진흥원이 지원하는 이동 네트워크 정보보호기술개발연구의 일부분임.

2. 관련연구

2.1 OSGi(Open Service Gateway Initiative)

OSGi는 홈 네트워크의 여러 가지 정보가전과 응용 프로그램간의 API를 정의하는 것을 목적으로 구성된 단체이다. OSGi의 규격은 자바의 플랫폼 독립성과 실행코드의 네트워크 이동성을 이용하여 소용량 메모리 디바이스를 위한 동적인 서비스의 제공을 목표로 제정한 표준이다. OSGi를 구성하는 중요한 엔터티는 서비스, 번들, 프레임워크 이다. 여기서 서비스가 가장 핵심이다. 서비스는 특정 기능을 수행하는 자바 인터페이스와 실제 구현 객체이고 번들은 서비스를 제공하기 위한 기능적 배포 단위이고 프레임워크는 번들의 라이프 사이클을 관리하는 번들 실행환경이다.

2.2 JES(Java-Embedded Server)

JES 는 OSGi 표준에 근거하여 만들어졌으며 이를 구성하는 컴포넌트는 작은 용량의 프레임워크와 서비스이다. 프레임워크는 어플리케이션과 플라그 앤 플레이 서비스로 구성되고 어플리케이션의 로딩, 설치, 활성화, 실행, 제거 와 서비스 호출 등을 관리할 수 있는 런타임 환경을 제공한다. JES 서비스는 프레임워크에 의해 사용 및 관리된다. JES는 Log, Http, Admin 및 코아 서비스

외에도 사용자가 자신의 서비스를 그림 1과 같이 추가하여 구현할 수 있다.

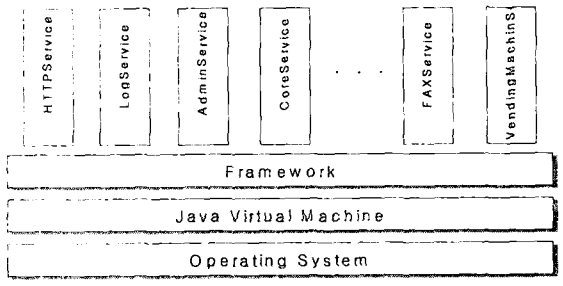

그림 1 JES 구조

3.OSGi 프레임워크 기반의 침입차단

3.1 서비스 전체구조

홈 네트워크에서 서비스 게이트웨이와 침입차단시스템을 외부에서의 보안 관리 어플리케이션이 제어하는 전체적인 구조는 그림 2와 같다.

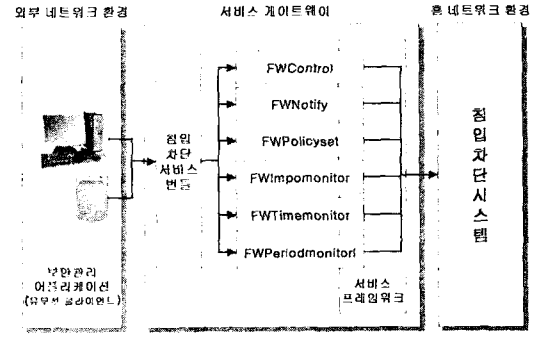

그림 2. 보안서비스

3.2 침입차단모듈

침입차단모듈은 네트워크 트래픽의 상태를 감시하고 분석하고, 보안 정책에 따라 트래픽을 제어하기 위한 방화벽 시스템 모듈이다. 이 모듈은 트래픽정보 수집기와 보안 정책 관리기 두 개 부분으로 구성된다.

트래픽 상태 정보 수집기는 패킷을 수집하고, 패킷의 정보를 분석하여 현재 트래픽 상태를 파악하기 위한 것으로, 상태 유닛 테이블, 통계 분석 모듈, 히스토리 정보 생성기, 상태 전이 신호 생성기로 구성되어 있다.

상태 유닛 테이블은 전체 네트워크, 프로토콜, 내부 호스트, 커넥션으로 구분되는 상태 유닛의 정보를 트래픽 정보에 따라 갱신하고 관리하기 위한 것이다. 상태 유닛은 트래픽을 가질 수 있는 객체이다. 이것은 누적되는 패킷 정보가 통계 분석 모듈에 의하여 가공된 정보를 포함하게 된다.

히스트리 정보 생성기는 트래픽 상태에 따른 보안 정책의 적용 기록을 보관하는 것으로, 향후 보안 정책 수립의 참고 자료가 된다.

트래픽 상태 정보 수집기에서 생성된 정보는 상태 전이 신호에 의하여 보안 정책 관리기로 전달된다. 상태 전이 신호는 일정한 시간 간격 또는 정의되어 있는 트래픽 이벤트가 발생 하였을 경우, 네트워크 트래픽의 상태를 보안 정책 관리기로 전달하기 위한 것이다.

보안 정책 관리기는 트래픽의 상태에 따라 보안 정책을 결정하고 수행하기 위한 것으로, 보안 상태 그래프 생성기와 보안 상태 그래프, 필터링 규칙 생성기로 구성되어 있다. 보안 상태 그래프는 네트워크 트래픽 상태의 변화에 따라 상태 전이가 이루어지면서, 전이된 새로운 노드의 보안 정책을 수행하여 변화되는 트래픽에 대응하기 위한 것이다. 이것은 보안 생태 그래프 생성기에 의하여 구성된다.

필터링 규칙 생성기는 새로운 보안 정책을 트래픽 제어기에 적용될 수 있는 필터링 규칙으로 변화하는 것이다.

보안 상태 그래프에서의 상태 전이는 그림 3와 같은 과정으로 진행된다.

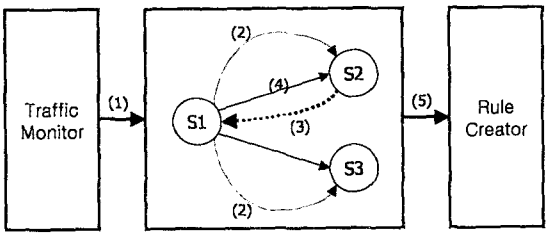

그림 3. 상태 전이 과정

상태 전이 신호 생성기(Traffic Monitor)에서 상태 그래프로 상태 전이 신호가 전달되면, 현재 트래픽 상태를 나타내는 S1은 자신의 조건이 상태 전이 신호를 수용할 수 있는지 검사한다. 자신이 수용 가능하면 상태 전이는 일어나지 않고, 현재의 보안 정책이 고수된다. 그러나, 자신이 수용할 수 없는 경우에는 자신과 연결되어 있는 모든 상태 노드에게 상태 전이 신호를 전달하여 수용 가능한 노드가 있는지 검사한다. 수용 가능한 노드가 없다면 앞의 경우와 마찬가지로 상태 전이는 일어나지 않고, 현재의 정책이 고수된다. 그러나, 수용 가능한 노드가 있다면, 상태 전이가 발생하여 현재 상태가 수용 가능한 노드로 변경되고, 기존의 보안 정책은 취소되고, 새로운 노드의 보안 정책이 적용된다.

3.3 OSGi 기반의 침입차단 서비스 기법

정의된 침입차단서비스는 다음과 같다. 우선 침입차단서버를 구동시키고 정지시키는 침입차단서버 제어서비스(*FWControl*), 외부 클라이언트에서 내부 침입차단서버에 설정된 정책을 필요에 따라 변경하기 위한 침입차단 정책설정서비스(*FWPolicyset*)가 있다. 또한 외부 클라이언

트에서 내부 침입차단상황을 모니터링하기 위한 서비스가 제공된다. 주기별로 모니터링 상황을 외부 클라이언트에 전송하기 위한 침입차단상황 주기별 모니터링 서비스(*FWPeriodmonitor*), 설정된 정책에 의해 중요한 내용순으로 모니터링 결과를 전송하는 중요도별 모니터링 서비스(*FWImpmonitor*), 현재까지의 모니터링 상황을 시간대별로 제공하는 시간별 모니터링 서비스(*FWTimemonitor*) 등이 있다. 이외에 내부 네트워크에 위급한 상황이 발생했을 경우 침입차단서버에서 외부의 클라이언트로 경보와 함께 상황의 내용을 전송하는 침입차단경보 서비스(*FWNotify*) 가 있다. 이러한 서비스는 생명주기에 따라서 동적으로 서비스 게이트웨이에 배치되어 다른 번들의 서비스와 상호작용 한다.

3.4 외부 클라이언트와 침입차단시스템간의 통신

침입차단시스템을 관리하기 위한 인터페이스 JES를 이용하여 통신하게 된다. 관리자 인터페이스는 침입차단시스템에 직접 접근하지 않고 JES에게 필요한 정보를 요구하고, JES는 그러한 요구에 따랄 침입차단시스템에 해당하는 정보를 받아서 넘겨준다. 외부 클라이언트에 있는 보안 어플리케이션은 항상 대기하고 있다가 침입차단 경보서비스에서 오는 U에 패킷으로 받아드리고 TCP로 연결하여 상응한 정책을 정한다. 만약 클라이언트 어플리케이션이 실행 안되고 있는 경우에는 서비스 게이트웨이에서 또 그에 상응하는 침입차단 상황 주기별 모니터링 서비스가 실행 되여 클라이언트한테 메시지를 보낸다. 이렇게 JES를 이용함으로서 외부에 대한 보안과 인증이 가능하며 또한 다양한 형태의 인터페이스 플랫폼을 지원할 수 있다.

4. PDA에서 침입차단서비스 구현

PDA와 같은 무선 클라이언트에서 침입차단서비스의 제어를 위한 어플리케이션 MFWS(Mobile Firewall System)을 구현하였다.

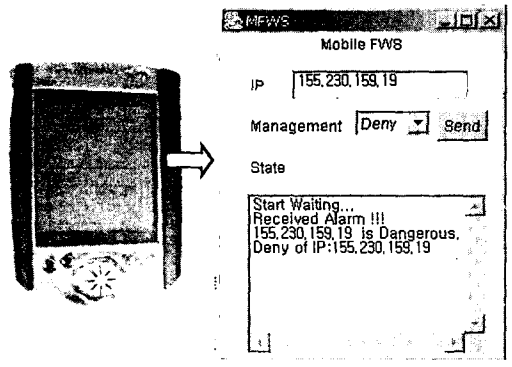

그림 4. MFWS

무선 랜(LAN)이 설치된 환경에서 클라이언트가 PDA로 홈 네트워크에 설치된 침입차단시스템이 외부로부터 침입이라고 판정되는 컴퓨터의 IP Address를 PDA에 보내준다. MFWS는 대기하고 있다가 이러한 위험 메시지를 받으면 관리자가 그에 상응하는 특정 IP 에 대하여 차단한다. 그림 4는 침입차단서비스 제어를 위한 MFWS의 작동 화면이다.

5. 결론 및 향후 연구방향

OSGi 기반의 프레임워크를 구현한 JES에서 침입차단을 하나의 서비스의 형태로 구현하였고 PC나 PDA 와 같은 유무선 클라이언트에서 침입차단서비스에 대한 제어를 구현하였다.

현재 구현한 침입차단시스템은 트래픽 상태 기반이고 유선환경인 PC 에서는 그 트래픽에 대한 감시가 뚜렷하게 반영되지만 PDA 와 같은 제한된 환경에서 통제와 제어는 아직 빈약하다.

본 OSGi 프레임워크 기반의 침입차단서비스는 추후 네트워크 트래픽에 대한 더 많은 정보와 분석이 필요하고 및 그에 따른 보다 구체적이고 정확한 통제가 필요한다.

그리고 향후 침입차단시스템 뿐만 아니라 침입탐지시스템도 OSGi 프레임워크 기반의 서비스 형태로 구현이 필요하며 침입차단시스템과 침입탐지시스템의 연동, 및 통합제어가 필요하며 특히 관리자가 외부에서 PDA와 같은 제한된 시스템 환경에서의 구체적이고 효율적인 제어가 필요할 것이다.

참고문헌

[1] OSGi, "OSGi Service Gateway Specification - Release 2.0", http://www.osgi.org

[2] R. Sailer, M Kabatnik, "History based distributed filtering - a tagging approach to network-level access control," Computer Security Applications, 2000, pp.373-382

[3]. M. Lyu and L. Lau, "Firewall security: policies, testing and performance evaluation," Computer Software and Applications Conference, 2000, pp.116-121

[4]. R. Knobbe, A. Purtell and S. Schwab, "Advanced security proxies: an architecture and implementation for high-performance network firewalls," Military Communications Proceedings, 1999 pp.734-738

[5] Sun Microsystems, Inc, "Java Embedded Server 2.0 ", http://www.sun.com/software/embeddedserver

[6] Sun Microsystems, Inc, "Java Embedded Server 2.0 ", http://www.sun.com/software/embeddedserver/whitepapers/index.html