WAP 기반의 무선 단말기를 이용한 효과적인 IDS 관리/제어 시스템 구현

김행욱[0] 정숙희 강홍식
인제대학교 전산학과
hukim[0]@nice.inje.ac.kr, deliz@hanmir.com, hskang@nice.inje.ac.kr

Design of Management and Control WAP Based Intrusion Dection System Using Mobile Terminal

Haeng-Uk Kim[0], Suk-Hee Jung, Heung-Seek Kanag
Dept. of Computer science, Inje University

요 약

현재 웹기반의 네트워크 침입 탐지 시스템은 관리자가 네트워크가 연결된 상태에서 관리자가 컴퓨터앞에서 감시하고 그에 적절한 대응을 해야 하지만 관리자가 자리를 비웠을 경우에는 그러한 침입에 신속하게 대응하기가 어렵다. 하지만 무선 인터넷의 발달로 인하여 관리자가 무선 단말기 상에서 네트워크 침입탐지를 감지하고 그에 적절한 대응을 할 수 있게끔 하기 위해서 본논문을 작성하게 되었다. 본 논문에서는 WAP Push FrameWork 기술을 바탕으로 해서 모바일 기반에서 시스템 관리자가 장애탐지, 네트워크 모니터링, IP관리 등을 직접 무선 단말기 상에서 관리함으로써 IDS관리를 좀더 효율적으로 관리할수 있을것이다.

1. 서 론

인터넷이 생활 속으로 파고든지 어느덧 10년 남짓, 어느 새 우리 주변의 모든 것을 바꾸어 놓고 있다. 그 중의 하나가 무선 인터넷이라고 할수 있다. 유선 통신에 비해서 언제, 어디서나, 누구에게나 통신을 할 수 있는 휴대와 이동의 용이성으로 인해, 최근 무선통신은 어떠한 기술보다도 빠르게 성장하고 있다. 최근 네트웍의 관리 및 서버 관리는 전문 네트워크 관리자의 역할 및 서버관리자의 역할이 매우 중요시 되고 있다. 인터넷의 특성상 시스템의 장애를 미리 예측하기가 힘들기 때문에 그러한 장애가 발생하였을 때 신속한 발견과 대응이 무엇보다도 중요하다. 이에 관리자의 좀더 효율적인 시스템 관리와 보안을 위해서 관리자가 시스템앞에서 항상 컴퓨터를 마주보고 관리를 하기에는 시간의 한계가 있다. 또한 관리자가 외부에 있을 때 시스템에 보안상 문제가 발생한다든지 시스템을 관리해야할 상황이 있다면 관리자가 가지고 있는 무선 단말기를 이용한다면 보다 능동적이고 효율적으로 시스템을 관리할수 있을 것이다. 이러한 시스템 구현을 위해서 본 논문은 작성되었다. 한편 국내 이동통신사들은 낮은 대역폭이라든지, 불안정한 연결성, 높은 전송 비트 에러율, 제한된 베터리 등의 문제점을 아직까지 가지고 있다. 그러한 문제점들과 유선과 무선의 효과적인 데이터 전송을 위해서 WAP 포럼이 결성되고 그포럼에서 WAP 프로토콜이 개발되었다. 세계적으로 무선인터넷의 규격은 WAP과 마이크로소프트사의 ME(Micro Explore) 일본 NTT-docomo 사의 I-Mode 등이 있지만 대부분의 사용자들이 WAP을 채택해서 사용하고 있다. 본 논문도 현재까지 무선인터넷이 표준이라고 할수 있는 WAP프로토콜을 적용해서 서버 및 네트워크 관리자가 네트워크 관리 및 시스템의 보호를 할수 있는 관리 기법을 제시하고자 하였다. 본 논문은 총 5장으로 구성되어 있으며 1장은 모바일 환경에서의 현재 이루어지고있는 상황과 서버 및 네트워크 관리의 어려움, 2장은 현재 무선인터넷상에서 가장 핵심적인 기술인 WAP기술, 3장에서는 실제 WAP기술을 이용하여 IDS 관리 시스템을 설계, 4장에서는 시스템의 구현 결과와 구현 결과에 대한 검토, 5장에서는 향후 연구과제에 다하여 서술하였다

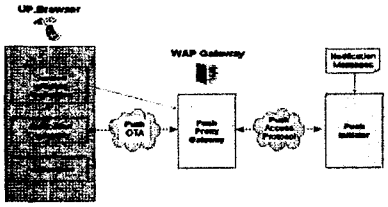
2. WAP

현재의 이동통신망에서 인터넷 서비스를 제공할 수 있도록 하기 위하여 Unwired Planet社(現 Phone.com社)에서는 HDTP(Handheld Device Transport Protocol)와 HDML(Handheld Device Markup Language)을 개발하고, Nokia社에서는 TTML(Tagged Text Mark-up Language)를 개발하였다. 또한 Ericsson社에서는 ITTP(Intelligent Terminal Transfer Protocol)를 개발

이에 1997년 6월에 Ericsson, Motorola, Nokia, Unwired Planet 4개사가 공통 규격을 제정하기로 하고 WAP(Wireless Application Protocol) 포럼을 결성하였고, 2002년 현재 전세계 500여가가 넘는 업체가 참여하고 있다. WAP의 목적은 디지털 셀룰러 전화(PCS 등)와 무선 터미널에서 인터넷 서비스를 이용할 수 있도록 하고, 다른 종류의 무선 통신망 기술에서 운용될 수 있는 무선 프로토콜 규격을 개발하고, 다른 종류의 무선 통신망 기술과 장비들에도 쓰일 수 있는 컨텐츠와 응용기술을 개발하는 것이다.[1][2]

2.1 WAP PUSH 서비스

Push 서비스는 WAP 1.2부터 포함되기 시작한 서비스로 WAP 클라이언트, 즉 무선 단말기로부터 서비스 요청 없이 일련의 데이터를 무선 단말기로 전송(Pushing Data)하는 기술이다.[4]



<그림1 WAP PUSH 서비스>

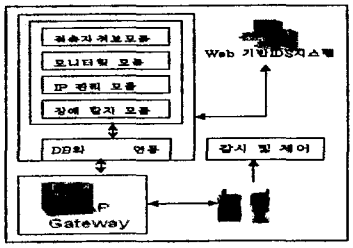
무선 인터넷 서비스는 기본적으로 클라이언트의 요청에 대한 응답을 보내주는 풀(Pull) 방식과 클라이언트의 요청이 없어도 서버가 클라이언트에 정보를 전달해 주는 푸시(Push) 방식으로 분류할 수 있다. 사용자의 입장에서 보면, 풀 방식은 사용자가 브라우저에서 직접 URL을 입력하거나, 하이퍼 링크를 선택하는 등의 행위를 통해 정보를 찾아다니는 방식이며, 푸시 방식은 사용자가 원하는 정보에 대한 기본적인 기술을 해 놓으면 서버가 관련된 정보를 사용자에게 배달해 주는 방식이라고 볼 수 있다.

위 그림의 WAP 전송 방식을 설명하면, 먼저 WAP 서비스를 제공하는 Web Server는 WAP Gateway 서버에 통지 메시지를 전달한다. 다음은 WAP Gateway 서버는 Phone(Client)에게 통지 메시지를 전달한다. 만약, 이 메시지가 캐시를 비우라는 명령이라면 캐시를 비운다. 이 메시지가 경보 메시지라면 착신음을 울리고, 새로운 메시지가 도착했음을 알린다. 그 다음 단계는 착신음을 들은 사용자가 확인 버튼을 누르면 착신음에 포함된 URL에 접속한다. 그러면 WAP Gateway 서버는 WAP 서비스가 전송한 URL에서 데이터를 요청하고 WAP 서비스는 컨텐트 정보를 WAP Gateway 서버에 전달한다. 마지막으로 WAP Gateway 서버가 Phone에 해당 컨텐트를 전달한다.[3]

3. 시스템 설계

3.1 시스템 특성

WAP을 이용하여 해당 IDS 및 ASP가 설치되어있는 시스템에 접속한후 페이지를 연결하며, ASP 모듈은 IDS시스템이 설치되어있는 시스템과 연결을 설정하여 명령어를 넘겨주며 결과값을 넘겨 받은후에 모듈에서 제공하는 기능들의 값을 휴대폰으로 넘겨준다. 또한 WAP PUSH를 이용해서 장애탐지가 발견되었을시 장애탐지에대한 ALERT메시지를 핸드폰으로 발송하여준다. 또한 ASP 서버는 소켓으로 연결되어 있어 선택된 명령어를 전달해주고 결과값을 넘겨 받아온후 모바일 단말기이 화면에 맞게 그 값들을 보여주는 특성을 가지고 있다.[6]



<그림2 IDS 관리 및 제어 시스템 설계>

본 시스템은 그림과 같이 크게 4가지 모듈로 구성되어있다.

1. 현재 시스템에 접속하여있는 접속자들의 정보를 수집하여 핸드폰에 제공해주는 모듈
2. IDS의 기능들을 모니터링 하는 모듈
3. 시스템에 접속하여 있는 사용자들의 IP 관리를 하는 모듈(IP 추가나 장애탐지 모듈에 의해서 발견된 침입의 징후가 보이는 IP들을 차단하는 모듈을 말한다)
4. 시스템에 접속하여 비정상적인 행동, 악의적인 공격에 대하여 탐지 및 그 정보들을 핸드폰으로 알려주는 모듈.

3.2 접속자 정보 모듈 구성

사용자의 시스템 사양 CPU정보, 접속자 정보를 수집하여 핸드폰에 제공하여 관리자가 각 시스템의 사양 및 접속자 정보를 파악할수 있도록 하는 기능을 제공한다.

<표1 시스템 및 접속자 정보 관리>

구 분	기 능
접속자 정보	접속자의 IP, 접속시간정보 제공
시스템 정보	시스템 사양, 메모리 정보

3.3 장애탐지 모듈 구성

본 시스템의 가장 중요한 모듈 구성이라고 말할수 있는 장애탐지 모듈은 시스템에 각종 장애 발생시 예를 들어 외부의 불법 침입이나, 해킹의 시도가 IDS에 발견되었을 때 관리자에게 PUSH 서비스를 이용하여 신속하게 정보를 제공하는 모듈이다. 장애 탐지 모듈에서는 각종 해킹 공격에 대한 정보를 서버 관리자에게 보고 하는 역할을 한다. 장애탐지 부분을 세분화 해보면 특히 비정상정익 침입이 시도되었을 때 이 시도를 유선상의 IDS에서 발견하여 그 발견된 침입에대한 각정 정보 등을 무선상의 단말기로 통보해주는 기능을 담당하고 있는 이때 무선상의 단말기에는 비정상적인 행위의 내용, 공격의 특성, 위험

정도, 침입시도를 하고있는 IP주소 등의 정보를 보여준다. 그러면 관리자는 단말기의 정보를 확인하고 만약 이런 공격이 위험하다는 판단을 하게되면 무선단말기를 이용해서 직접 제어할수 있을것이다.[7]

<표2 장애탐지 및 관리>

구 분	기 능
장애탐지	장애탐지 및 해킹 탐지 기능
장애탐지 정보	시스템의 장애탐지에 대한 정보 제공

3.4 IP 관리 모듈 구성

현재 접속하고 있는 사용자들의 IP 관리 및 계정 관리 기능을 하는 모듈로서 사용자들이 악의 적인 행위를 했을 때 혹은 장애탐지 발견시 그에 해당하는 IP 의 접근 차단 및 계정 삭제의 기능을 담당하는 모듈이다.

<표3 IP / 계정 관리>

구 분	기 능
IP 관리	IP 관리 기능
계정 관리	사용자의 계정 관리기능

3.5 네트워크 모니터링 모듈 구성

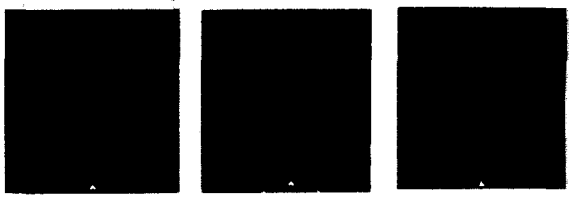
네트워크 모니터링 기능은 라우팅 테이블을 모니터링 하여 현재 테이블에 있는 항목들의 목적지 주소, 게이트웨이 주소, 플래그, 인터페이스 이름을 관리자에게 제공하는 역할을 수행한다.

<표4 네트웍 모니터링 관리>

구 분	기 능
네트웍 모니터링	네트웍의 인터페이스정보 관리

4. 시스템 구현 결과 및 검토

구현결과를 캡처를 한 화면은 다음 그림과 같다. 다음 그림들은 Phone.com사의 시뮬레이터 브라우저를 통해서 제공되는 것이다. 먼저 <그림 3>의 첫 번째 그림을 보면 각 항목마다 제공되는 서비스가 보일것이다.[2] 1번 항목은 현재 유선상의 서버에 접속해 있는 접속자들의 정보를 보여주는 항목이며, 2번 항목은 서버의 네트웍을 모니터링해주는 항목이다. 3번 IP관리 항목은 서버 관리자가 유선상에서 뿐만 아니라 무선상에서도 각각의 IP에대한 관리를 할수 있는 항목이다. 예를 들어 접속해 있는 IP가 악의적인 행동을 하는 아이피로 판단되었을시 IP를 차단할수 있다. 마지막으로 장애를 탐지하는 항목이 있는데 서버에 어떤 악의적인 패턴이나, 패킷이 들어왔을 경우 어떤 공격이 가해지고 있는지 얼마나 위험한지를 알수 있는 항목이다. 만약 그런 공격의 징후가 발견되었을시에 WAP의 PUSH서비스를 이용해서 Mobile이나 PDA로 메시지를 보내주는 기능을 하게 되는데 무선 단말기에는 해킹 시도가되는 공격의 종류, 해킹 공격이 서버에게 미치는 위험도, 침입이 시도되고있는 IP주소등의 정보를 표시하고 있어서 관리자가 그에대한 정보를 확인한후 PUSH 서비스를 이용해서 직접 유선상의 IDS를 제어 할수 있을 것이다. 그외의 그림은 각각의 메뉴에 대한 결과를 나타내주는 화면이다. 시뮬레이터에 표현된 텍스트들은 모바일 액정의 한계가 있으므로 정말 필요한 정보들만 출력해야 하는 어려움이 있었다.



<그림3 시스템 결과 캡춰 화면>

5. 결론 및 향후 전망

현재 유선인터넷의 네트웍 관리자나 보안관리자들은 항상 컴퓨터 앞에 있어서 컴퓨터의 모니터 화면을 늘 주시해야하는 어려움이 있다. 또한 그러한 관리자들은 외부에서는 서버나 네트웍 관리를 하기에는 공간적이나 시간적인 제약이 많이 따르게 되는 것이 아직까지의 현실이며, 외부에 나가있을 때 유선상의 서버에 어떠한 침입을 받았을 때 그러한 상황에 즉각 대처하기가 어려운게 사실이다. 그리하여 본 논문에서는 이런 네트웍 관리자나 보안관리자들에게 좀더 유연한 환경에서 서버 및 네트웍을 관리하고 보호할수 있고, 그리한 위급상황에 좀더 유연하게 대처하기 위해서 WAP 기반의 유무선을 연동하여 네트웍을 관리, 보호할수 있는 무선 시스템을 설계/구현 하였다. 관리자는 무선 단말기나 PDA를 통해서 자신이 관리하는 서버의 각종 정보를 파악할수 있을 것이며, 또한 외부에 있을시 유선 상의 서버에 행해지는 침입시도등을 무선단말기를 통해서 제공받을수 있으며 그러한 정보를 통하여 직접 서버를 관리/통제 할수 있을것이다. 또한 외부의 침입으로 의심되는 IP주소를 체크하고 그러한 IP주소를 차단할수 있을것이다. 하지만 아직까지 휴대폰의 낮은 전송속도와 무선인터페이스의 특징인 작은 화면으로 인해 관리자에게 정말 필요한 정보들만 보여줘야하는 어려움이 있었다. 앞으로 무선인터넷은 IMT-2000이 정식으로 상용화 되면 데이터의 전송량이나 전송 속도 뿐만 아니라 멀티미디어정보까지 제공되어지게된다. 그렇게 되면 좀더 많은 정보를 관리자에게 효과적으로 보내줄수 있을것이며 각종 멀티미디어 자료뿐만 아니라 전송속도 저하로 인한 어려움 또한 많이 줄어들 것으로 보인다. 또한 무선인터넷을 이용한 IDS및 네트웍관리에 대한 좀더 깊은 연구가 필요할것이다.

6. 참고문헌

[1] <http://www.wapforum.org>
[2] <http://www.phone.com>
[3] 홍준호 외 2인공저 about WAP 2001.
[4] 배준현 WAP 푸시 프레임웍의 이해
[5] <http://www.zionwap.net>
[6] LG-EDS 시스템 아엔텍팀 무선인터넷 어플리케이션 프로그래밍
[7]http://cesec.ajou.ac.kr/~kagi/intro_ids/intro_ids.html