WAP기반의 침입 기법 차별을 이용한 원격 침입 경보 시스템

강태호°, 김원진, 방훈, 원대희, 이재영
한림대학교 컴퓨터공학과
[Lamius, wjkim, hooni, dhwon, jylee]@isul.ce.hallym.ac.kr

A WAP Based Remote Intrusion Alert System using Distinction of Intrusion Techniques

T.H.Kang°, W.J.Kim, H.Bang, D.H.Won J.Y.Lee
Dept. of Computer Engineering, Hallym Univ.

요 약

기존의 침입 탐지 시스템들은 모두 관리자가 지속적으로 직접 컴퓨터 앞에 앉아 모든 감사 결과들을 보고 처리해야 되는 불편한 점을 가지고 있다. 본 논문에서는 이러한 불편한 점에서 약간이나마 탈피하고자 관리자가 부재시에도 위급한 침입 행위를 발견시에 관리자의 PDA나 휴대폰으로 경고 메시지를 보냄으로서 관리자가 즉각적으로 대처할 수 있도록 도움을 주고자 함을 목적으로 제안한다. 그러나 모든 침입에 대한 감사기록을 관리자에게 경고 메시지로 송신하는 것은 오히려 cost가 비싸지는 점이 발생하므로 본 논문에서는 각 해킹 기법들을 자별화 하여 즉각적인 대처가 필요한 침입 사항만을 선별하여 호출하는 시스템을 제안하고 구현한다.

1. 서 론

시스템의 관리자는 보안에 대한 직관적인 개념만을 가지고 보안 관리가 가능해야 한다. 관리자에게 보기에 편하고 사용하기에 용이한 인터페이스를 제공함으로써 보안 시스템 관리가 불편한 작업이 아님을 보여야 한다[1].

침입 탐지 시스템은 최종적으로 관리자가 판단 및 대응을 하게 된다는 것은 자명한 사실이다. 하지만 관리자가 항상 컴퓨터 앞에 앉아 있어야 한다는 점은 관리자에게 많은 부담을 주고 있는 것이 현실이다. 본 논문에서는 이러한 점에서 약간이나마 관리자에게 부담을 덜어주기 위해 관리자 부재시에도 위급한 침입 행위를 발견하게 되면 관리자의 PDA나 휴대폰으로 경고 메시지를 보냄으로서 관리자에게 도움을 주고자 함이 목적이다.

본 논문은 2장에서 침입 탐지 기법에 대해 알아보고, 3장에서는 무선 인터넷에서의 PUSH 기술에 대해 설명한다. 4장에서는 이를 이용한 원격 침입 경보 시스템에 대해 설명하고, 5장에서 구현 및 검토를 한 후 6장에서 결론 및 향후 연구 과제에 대해 서술한다.

2. 침입 탐지 기법

침입 탐지 기법은 컴퓨터 시스템이 해킹 공격에 대비하고 대응할 수 있도록, 시스템과 네트웍 자원으로부터 비정상적인 사용, 오용, 남용 등에 대한 정보를 실시간으로 수집, 분석하여 침입 및 침입시도의 징후를 찾아내고 보고하는 방법이며, 본 논문에서는 Smurf Attack, Land Attack, Network Scan, SYN flooding, Buffer Overflow 등의 침입을 탐지하였다.

2.1 Smurf Attack

공격하고자 하는 호스트의 IP주소를 송신 주소로 하여 ICMP echo request를 로컬 네트워크 전체에게 브로드캐스트 주소로 보내게 되면, 대상 호스트는 되돌아오는 echo reply 패킷 때문에 마비 상태에 빠지게 된다. Smurf 공격은 ICMP echo request 패킷 중에서 broadcast address를 가진 패킷을 필터링하거나, 임계치 이상의 echo reply 패킷이 도착하는 것을 카운트 하는 방법으로도 탐지 할 수 있다[2,4]. 후자의 방법으로는 5초안에 5번 이상의 echo reply를 탐지하게 된다[5].

2.2 Land Attack

Land attack은 소스 시스템의 IP주소를 공격하고자 하는 시스템의 IP 주소와 포트로 바꾸어 전송하면 공격받은 호스트는 루프 상태에 빠져 IP 스택에 심각한 장애를 유발하게 된다. Land attack을 탐지 하기 위해서는 라우터에서 내부 주소를 가진 외부 패킷을 필터링하거나 송신 주소와 목적지 주소가 같은 경우를 비교하면 된다[4].

2.3 Network Scan Attack

Network Scan 공격은 직접적인 공격의 방법이라고 할 수는 없지만, 대상 호스트의 취약점을 검색할 수 있기 때문에 침입의 전 단계로 사용되고 있다. Network Scan 공격을 탐지하기

위해서는 감사자료 수집 모듈에서 수집한 패킷 중에서 TCP 패킷을 필터링하고 그중 연결요청 패킷인 SYN 패킷을 필터링하여 TCP로 연결 요청을 하는 패킷만을 수집한다. 주어진 일정한 시간안에 하나의 IP소스로부터 임계치 이상의 연결 요청이 발생하면 침입으로 판정한다[5].

2.4 SYN flooding Attack

SYN공격은 대상 시스템에 연속적인 SYN패킷을 보내서 넘치게 만들어 버리는 공격이다. 각각의 패킷이 목적 시스템에 SYN-ACK 응답을 발생시키는데, 시스템이 SYN-ACK에 따르는 ACK(acknowledgement)를 기다리는 동안, backlog 큐로 알려진 큐에 모든 SYN-ACK 응답들을 넣게된다. SYN-ACK은 오직 ACK가 왔을 때나 내부의 비교적 길게 맞추어진 타이머의 시간이 넘었을때만 이 3단계 교환 TCP 통신 규약을 끝내게 된다. 이 큐가 꽉찼을때 들어오는 모든 SYN요구를 무시하고 시스템이 인증한 사용자들의 요구에 응답할 수 없게 되는 것이다. SYN flooding을 탐지하는 방법은 TCP의 연결 요청 패킷을 검사하여 일정한 시간 안에 하나의 소스로부터 다수의 연결요청이 발생하게 되는 것을 탐지 한다. SYN flooding과 네트워크 스캔 공격은 하나의 IP주소로부터 연결 요청을 시도하는 횟수를 카운트하는 것은 동일하나, 네트워크 스캔 공격이 여러 포트를 대상으로 하는 반면에 SYN flooding 공격은 하나의 포트를 대상으로 하기 때문에 하나의 소스로부터 하나의 포트로 임계치 이상의 연결요청을 카운트하게 된다[5].

2.5 Buffer Overflow

메모리의 구조는 프로그램이 메모리 상에서 수행 될 때 프로그램이 들어가는 자리인 Text 부분과 이미 설정되어 있는 data, static 변수등의 데이터가 들어 있는 Data 부분, 임시로 기억되어 질 내용을 담는 stack 영역으로 분류된다. 이때, main()와 서브 함수인 sub()이 있다고 할 때, sub()에 있는 local 변수를 오버 플로우시켜 return address에 있는 원래의 복귀 주소를 변경하여 루트 권한의 쉘코드를 실행시킨다. 만약 실행 시에 루트 권한을 갖는 Set User ID비트가 설정된 프로그램에 오버 플로우 취약점이 있다면, 쉘 코드를 실행시키지 않고도 루트권한을 획득할 수 있다[5].

이러한 버퍼 오버플로우 공격을 탐지하는 방법은 실제 프로그램은 다른 이름으로 바꾸고, 새로운 wrapper 프로그램을 만들어서 argument의 size가 정해준 size를 초과하지 않을 경우에만 실제 프로그램을 호출하여 주는 프로그램을 만들어 주면 된다[6].

3. WAP PUSH Framework

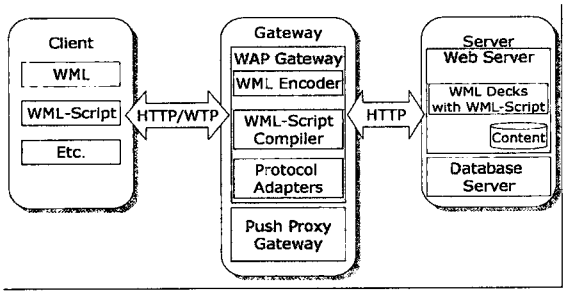

그림 1 WAP 시스템의 구성과 각 구간별 전송 방식

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 수있다[7].

그림 1의 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 Cateway 서버가 Phone에 해당 컨텐트를 전달한다[8].

4. WAP기반의 침입 기법 차별을 이용한 원격 침입 경보 시스템의 설계 및 구현

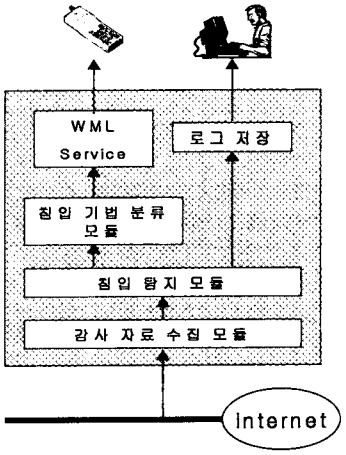

그림 2 제안된 RIAS 모델의 기본 구조

본 장에서는 네트워크 기반의 침입 탐지를 수행하여 탐지된 침입 기법들의 차별화를 통해 위험 단계가 높은 침입을 관리자에게 경보하는 시스템(RIAS : A Remote Intrusion Alert System)을 설계한다. 앞으로 편의상 원격 침입 경보 시스템은 RIAS로 표기하도록 하겠다.

RIAS는 감사 자료 수집 모듈, 침입 탐지 모듈, 침입 기법 분류 모듈등으로 나눌수 있다. RIAS시스템의 구성은 그림 2와 같다.

4.1 감사 자료 수집 모듈

감사 자료 수집 모듈은 libpcap 라이브러리를 이용하여 구현하였다. 자료 수집 방법은 이더넷 프레임부터 TCP 세그먼트까지 상세한 정보를 얻을 수 있는 필터링 방법을 이용하였다[9].

4.2 침입 탐지 모듈

침입 탐지 모듈은 수집된 네트워크 패킷을 이용하여 2장에서

설명한 침입 기법인 Smurf Attack, Land Attack, Network Scan, SYN flooding, Buffer Overflow 등을 탐지하게 된다.

4.3 침입 기법 분류 모듈

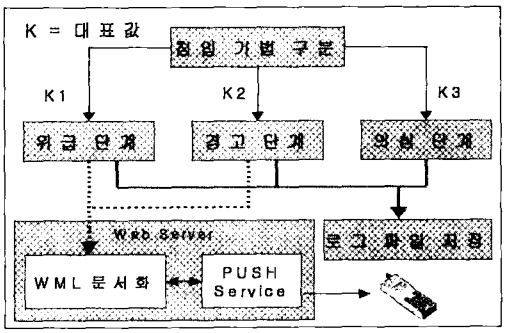

그림 3 침입 기법 구분 동작 구조

침입 기법 분류 모듈에서는 침입 기법을 차별화 하게된다. 침입 기법을 위급 단계, 경고 단계, 의심 단계의 3가지로 분류하였다. 첫 번째인 위급 단계는 침입 사실만으로도 시스템에 물리적인 영향을 끼치는 즉, 시스템 다운이나 서비스 정지 등 시스템 파괴적인 기법들을 지정한다. 본 논문에서는 Smurf Attack과 Land Attack, SYN flooding Attack등을 위급 단계로 구분하였다. 이 3가지 침입 기법들은 2장에서 설명한바와 같이 시스템 장애나 네트워크 마비등을 일으키는 심각한 침입 기법이므로 위급 단계로 지정하였다. 본 논문에서는 이 위급 단계의 침입 기법들이 휴대폰이나 PDA로 알려지게 되는 등급이 된다. 두 번째인 경고 단계는 지금 즉시 시스템에 영향을 끼치지는 않겠지만 앞으로 위급 단계 수준으로 확대 가능성이 있는 공격들을 지정하였다. 본 논문에서는 Buffer Overflow Attack을 경고 단계로 구분하였다. 이 침입 기법은 시스템의 관리자 권한을 획득하기 위한 공격 방법으로 시스템에 장애등을 일으키지는 않지만 권한 획득시에는 위협적인 공격이 되기 때문에 경고 단계의 침입 기법으로 분류하였다. 본 논문에서 이 등급은 PUSH로 호출되는 등급은 아니지만 WML 서비스를 제공하여 관리자가 휴대폰이나 PDA로 PULL 서비스를 원할 시 공격자와 공격기법을 Display해 줄 수 있도록 하였다. 세 번째인 의심 단계는 경고 단계로의 확대 가능성이 있는 공격을 지정하였고, Network Scan 공격이 여기에 속한다. 이 등급은 단순히 로그로만 저장이 된다. 단순히 의심 단계의 침입 기법만 로그에 저장되는 것이 아니라 본 논문에서 제안한 3단계의 침입 기법들은 모두 로그 저장이 기본이 된다.
그림 3은 이러한 침입 기법 구분후 WAP 서비스까지 제공되는 절차를 나타낸것이다.
본 논문에서 침입 기법 모듈을 개별적으로 둔 이유는 향후 새로운 침입 기법들의 추가나 패치등으로 인해 탐지가 불필요해진 침입 기법들을 유연하게 갱신하기 위해서 구분하였다.

5. 구현 및 검토

본 논문에서 제안된 RIAS를 검토하기 위해 각 단계의 침입 기법들 1가지씩 수행해 보았다. 침입 탐지를 위해 시도한 침입 기법은 mscan을 이용한 Network Scan Attack과 사용자가 "cp /bin/sh, chmod 4755"라는 명령어를 입력하여 Buffer Overflow Attack을 한 경우, 마지막으로 local 네트워크내의 다른 호스트로부터 ICMP echo request 메시지를 임의로 만들어 브로드 캐스트 한 Smurf Attack에 대한 탐지를 수행하여 보았다. 다음 그림 4는 Phone.com Browser를 통해 제공된 WML Service의 출력을 보여주고 있다.
실험 결과는 시뮬레이션을 통해 출력되었듯이 Text 메시지 형식이므로 실제 휴대폰에 보고되는 시간은 WAP Gateway의 다운등의 문제만 발생치 않는다면 많은 시간이 걸리지 않을 것이라 생각된다.

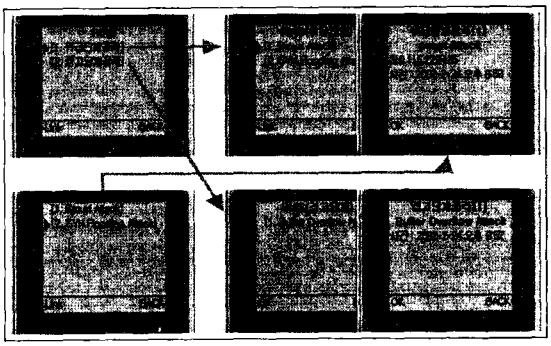

그림 4 WML Service 출력

6. 결론 및 향후 연구 과제

본 논문에서는 침입 기법의 차별화와 무선 휴대폰이나 PDA를 이용할 수 있는 원격 침입 경보 시스템을 제안하였고 이를 설계, 구현해 보았다.
탐지 보고를 관리자가 항상 컴퓨터 앞에서 콘솔등으로 보고받을 수 있지 않는 부재중인 경우를 대비하여 휴대폰이나 PDA로의 원격 경고 시스템을 구성해 보았고, 무선 이동통신의 Cost를 고려하여 침입 기법을 분류해 즉각적인 대처가 필요한 위급 단계의 침입 기법만을 휴대폰이나 PDA로 경고함으로서 Cost의 절감을 기대할 수 있다. 그러나 본 논문의 침입 기법 분류는 관리자가 침입 기법에 대해 정확히 파악하고 있어야 한다는 어려움이 있다. 향후 연구 과제로는 침입 차단 시스템의 추가로 시스템을 확장하여야 할 것이다. 또한 무선 통신 기기의 메모리 확장등과 같은 기계적 발전이 이루어지면 이와 연계하여 경고 메시지뿐만 아니라 휴대폰이나 PDA로 침입의 대응등과 같은 관리 작업도 가능할 수 있도록 연구가 계속 되어져야 할 것이다.

참고 문헌

[1] 임용성, 장덕성, "침입탐지 시스템에 관한 연구", Bull, I.I.S. Vol. 22-1 Jun, 1999.
[2] Sandeep Kumar, "An Application of Pattern Matching in Intrusion Detection" Technical Report CSD-TR-95-009-Coast TR 95-04, March 17, 1995.
[3] Vern Paxson, "Bro: A System for detecting Network Intruders in Real Time", Jan 14, 1998.
[4] Watcher, "NIDS for the masses", Phrack Magazine Vol 8, Issue 53, article 11 of 15.
[5] http://www.certcc.or.kr/
[6] http://www.auscert.org.au/
[7] http://phone.com/
[8] Charles Arehart 외 12인 공저, "Professional WAP", 2000.
[9] Steven McCanne, Van Jacobson, "The BSD Packet Filter: A new Architecture for User-level Packet Capture", December 19, 1992.