Web 기반의 내부 정보유출 차단기법 및 프로토콜 설계

백 승 엽° 장 성 만 이 극
{psy9511°, smjang, leegeuk}@ai.hannam.ac.kr

Information Outflow Interception Method and It's implementation Based in Web

Seung-Yub Baek° Sung-Man Jang Geuk Lee
Dept. of Computer Engineering, Hannam University

요 약

본 논문에서는 내부로의 정보유출 보호를 위해 패킷의 이동경로를 분석함으로써 내부적으로 노출되어 있는 패킷에 송수신량을 측정하여 패킷 도청을 차단하는 기법을 제안한다. 서버와 클라이언트로 구현하여 웹을 통하여 실시간으로 패킷의 도청을 탐지 및 차단할 수 있도록 설계 및 구현하였다.

1. 서 론

정보보안이 대두되는 시점에서 현제 내부 사용자에 의한 패킷 도청 및 절취에 대한 대비책이 미흡하다. 따라서 내부 정보망 보안의 취약점을 이용해 정보를 절취하는 악의적 행위를 방지하고 탐지, 예방하여야 한다. 정보를 유출시키기 위해서 가장 많이 사용하는 패킷 절취기법에는 스니핑이 있으며, 이 기법은 허브의 주소테이블을 오버플로우시켜 패킷의 목적지주소를 변경시키는 Switch Jamming기법, 공격자를 라우터로 인식시키게 하는 ARP Redirect기법, 다른 세그먼트에 존재하는 호스트간의 트래픽을 절취하는 ARP Spoofing기법, 위조된 ICMP패킷을 전송해 공격자에게 패킷을 전송하게 하는 ICMP Redirect기법 마지막으로 스위치의 span/monitor port를 이용한 기법이 있다. 대부분의 기업이 보안피해를 경험했다는 실태에 비추어 보면, 보안위험을 완화하기 위하여 안전한 보안 시스템을 구축하고 지속적으로 보안 관리를 강화하는 것은 생존을 위한 초석이다. 기관이나 기업에서 사내의 보안을 강화하기 위해 많은 강구책을 내고 있는 시점에서 아직 내부 정보망에서의 내부 사용자에 의한 보안의 취약점이 드러나고 있는 상황이다. 내부 사용자는 방화벽을 우회하거나 혹은 그 테두리 안에서 도청 및 공격을 쉽게 시도할 수 있고 탐지하는데도 많은 어려움이 있다. 따라서 이런 신뢰를 무기로 악의적인 행위를 하는 사용자를 실시간으로 웹을 통해 탐지해내고 차단함이 개발의 목적이다.

본 논문의 구성은 다음과 같다. 2장에서는 패킷을 유출시키고 패킷의 흐름을 저해하는 기법을 분석하고, 3장에서는 서버와 연동하여 웹에서 실시간으로 패킷유출을 탐지 및 차단하는 프로토콜 및 차단 기법을 설계한다. 4장에서는 프로토콜 및 탐지서버를 구현하며 마지막 5장에서는 결론을 맺는다.

본 연구는 과학기술부 지역협력연구사업(R12-2003-004-02002-0) 지원으로 수행되었음

2. 관련연구

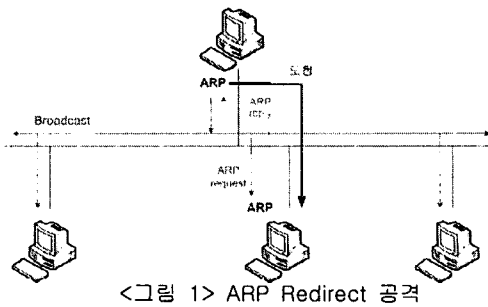
인터넷과 네트워크를 통한 정보의 이동이 증가하면서 정보에 대한 도청이나 절취가 행해지고 있고 이런 일련의 행위를 정보유출이라 한다. 네트워크상에서는 정보를 유출하기 위해 패킷을 도청하거나 절취하는 방법을 사용한다. 패킷을 이용해 정보를 유출하는 기법은 다음과 같다.

2.1 Switch Jamming

많은 종류의 스위치들은 주소 테이블이 가득 차게 되면 모든 네트워크 세그먼트로 트래픽을 브로드캐스팅하게 된다. 따라서 공격자는 위조된 MAC주소를 지속적으로 네트워크에 흘림으로서 스위칭 허브의 주소 테이블을 오버플로우시켜 다른 네트워크 세그먼트의 데이터를 도청할 수 있게 된다.

2.2 ARP Redirect 공격

위조된 arp reply를 보내는 방법을 사용하는데 공격자 호스트가 공격자의 MAC주소가 라우터의 MAC주소라는 위조된 arp reply를 브로드캐스트로 네트워크에 주기적으로 보내어, 스위칭 네트워크상의 다른 모든 호스트들이 공격자 호스트를 라우터로 믿게 한다. 결국 외부 네트워크와의 모든 트래픽은 공격자 호스트를 통하여 지나가게 되고 공격자는 이를 통하여 필요한 정보를 도청할 수 있게 된다.



<그림 1> ARP Redirect 공격

2.3 ARP Spoofing 공격

공격자는 자신의 MAC주소를 도청하고자 하는 두 호스트의 MAC주소로 위장하는 arp reply(또는 request)패킷을 네트워크에 브로드캐스트한다. 이러한 arp reply를 받은 두 호스트는 자신의 arp cache를 업데이트 하게 되고, 두 호스트 간에 연결이 일어날 때 공격자 호스트의 MAC주소를 사용하게 된다. 결국 두 호스트간의 모든 트래픽은 공격자가 위치한 세그먼트로 들어오게 된다.

2.4 ICMP Redirect 공격

Internet Control Message Protocol은 네트워크 에러 메시지를 전송하거나 네트워크 흐름을 통제하기 위한 프로토콜로 ICMP Redirect를 이용하여 패킷을 절취한다. ICMP Redirect 메시지는 하나의 네트워크에 여러 개의 라우터가 있을 경우, 호스트가 패킷을 올바른 라우터에게 보내도록 알려주는 역할을 하는데 이를 악용하여 다른 세그먼트에 있는 호스트에게 위조된 ICMP Redirect 메시지를 보내 공격자의 호스트로 패킷을 송신하도록 하여 패킷을 절취한다.

2.5 스위치의 span/monitor port를 이용한 공격

스위치에 있는 monitor 포트를 이용하여 도청하는 방법이다. monitor 포트란 스위치를 통과하는 모든 트래픽을 복 수 있는 포트로 네트워크 관리를 위해 만들어 놓은 것이지만 공격자가 트래픽들을 도청하는 장소를 제공할 수 있다.

3. 프로토콜 및 차단기법 설계

3.1 프로토콜

Group Level Status Data

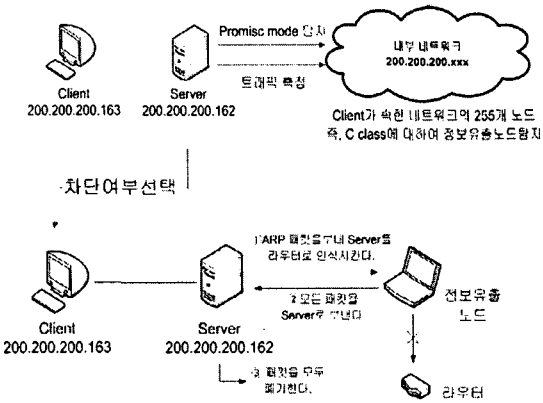
<그림 2> 정보유출 탐지 및 차단 프로토콜

<표 1> 프로토콜의 field 설명

Field	설명
Group	Server와 웹상에 Client의 정보를 담은 field
Level	현재 실행중인 탐지 및 차단의 단계에 대한 정보를 담은 field
Status	실행중인 프로그램의 단계에 대한 상태 및 진행상황 등의 정보를 담은 field
Data	실시간으로 주고받는 공격 노드에 대한 탐지 자료 및 차단 진행 정보 등의 정보를 담은 field

3.2 탐지 및 차단기법 설계

패킷의 도청을 막고 도청하는 공격자 노드를 차단시키기 위하여 크게 3가지 단계를 적용하여 탐지 및 차단을 하도록 설계하였다. 공격자 노드를 탐지하기위해 ARP Redirect기법을 사용하고 네트워크의 트래픽을 측정한다. 탐지된 노드에 대하여 차단 여부를 선택하고 선택된 노드의 패킷을 수거하여 모두 폐기한다. 다음 그림은 패킷을 도청하는 노드를 탐지하고 차단하는 순서이다.

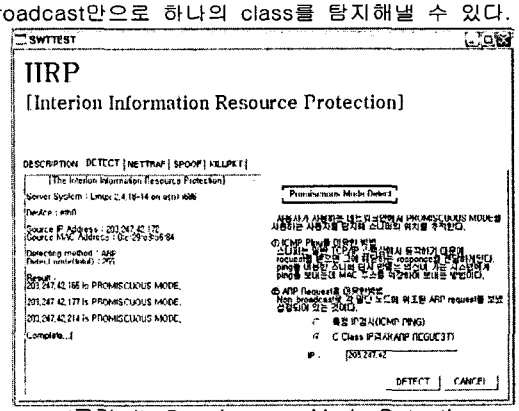


<그림 3> 패킷 도청 노드 탐지 및 차단

4. 탐지 및 차단 기법의 구현

4.1 패킷을 도청하는 노드 탐지

Client를 실행하여 Server와 연결한 후 "Detect" 로 C class의 IP주소를 적어주어 탐지를 실행한다. 두가지 방법을 사용하며 특정 IP 하나만을 탐색하는 방법과 Server가 속한 C class를 검사하는 방법이 있다. 전자인 특정 IP에 대한 탐색은 위조된 MAC주소를 이용하여 promiscuous mode를 사용하는 노드로부터 echo reply를 회신 받아 탐지하게 된다. 후자인 C class에 대한 탐지는 한번의 거짓된 MAC주소가 삽입된 패킷의 broadcast만으로 하나의 class를 탐지해낼 수 있다.



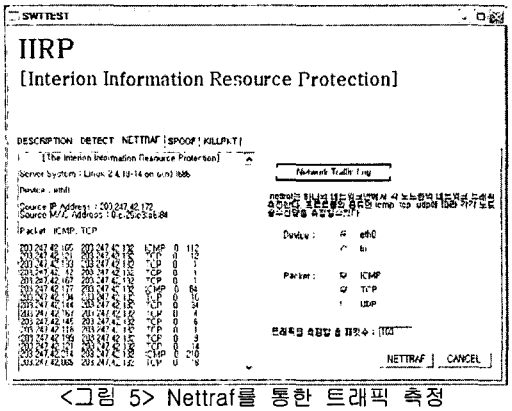
<그림 4> Promiscuous Mode Detecting

<그림 4>는 웹상에서 Client 실행 후 ARP Request 패킷을 사용하여 패킷 도청 노드를 탐지한 결과이다. 총 검색한 노드의 수와 탐지된 Promiscuous mode를 사용하는 노드의 IP Address를 Client에게 전송한다. 따라서 패킷을 도청하는 경로를 파악할 수 있다.

4.2 패킷의 트래픽 측정

Server 프로그램이 속해있는 네트워크 세그먼트의 패킷의 유동량을 특정하고 정보를 수집한다. 또 프로토콜의 정보와 그 종류에 따라 각각 노드들의 송수신량을 측정할 수 있다. "Nettraf"의 실행 시점부터 종료 시점까지 네트워크 세그먼트 내에서 송수신된 패킷들의 유동

량을 측정하고 각 패킷들의 송수신자의 IP정보와 패킷의 크기 등을 수집한다.

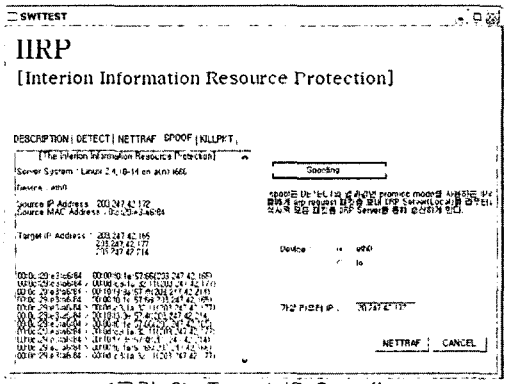


<그림 5> Nettraf를 통한 트래픽 측정

실행 전에 Device와 검색할 패킷의 종류를 선택하고 트래픽 측정을 개시한다. Server가 속한 203.347.42에서의 프로토콜 icmp, tcp, udp에 따라 트래픽량을 측정하고 Client에게 전송한다. 패킷 유출노드의 탐지결과와 트래픽량을 분석함으로써 패킷이 도청되는 경로를 탐지해 낼 수 있고 그 정보를 텍스트 파일로 저장해 선택적으로 도청하는 경로를 차단시킬 수 있도록 구현하였다.

4.3 SPOOF

패킷의 도청하는 경로를 탐지한 정보들을 이용하여 도청노드의 IP주소에게 Server의 컴퓨터가 라우터로 인식시키기 위한 ARP 패킷을 보내 해당 노드의 모든 패킷을 Server를 통하여 송신하게 한다.

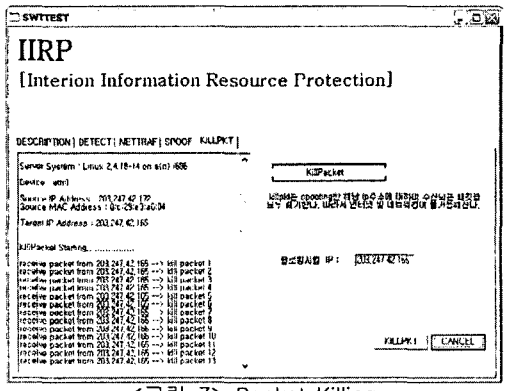


<그림 6> Target IP Spoofing

가상라우터로 사용할 IP주소에 Server의 IP주소를 입력하여 Target IP에 대해 일정한 간격으로 데몬을 종료시킬 때까지 ARP 패킷을 보낸다. 그러면 Server의 IP주소(203.247.42.172)를 Target IP들의 라우터로 인식시켜 모든 패킷을 수신한다.

4.4 KILLPKT

4.3에서 수신하는 Target IP들 중에 차단시킬 IP를 선택하여 해당 IP로부터 수신되는 모든 패킷을 원래의 목적지로 전송해주지 않고 모두 폐기한다.



<그림 7> Packet Killing

<그림 7>은 Target IP에 대하여 수신되는 패킷들을 수신하는 즉시 모두 폐기시킨다. 그러므로 패킷을 유출시키는 노드를 네트워크로부터 고립시켜 정보 의 도청 및 절취를 차단한다.

5. 결론

네트워크가 모여 하나의 커다란 인터넷을 이루지만 그런 작은 네트워크 내의 보안에 취약점이 많은 것이 현실이다. 개인이나 소규모의 네트워크에서부터 보안이 이루어지지 않는다면 더 나아가 회사나 국가의 정보가 유출되고 심각한 문제가 발생할 것이다. 아직 이런 작은 네트워크 세그먼트의 패킷의 유출에 대한 심각성을 인지하지 못하고 방관하는 것이 현실이며 패킷의 유출을 발견하고도 즉각적인 조치가 이루어지기 어려운 상황이다. 네트워크 보안과 패킷의 유출에 대한 지식이 부족한 현실에서 웹을 통하여 손쉽게 다가갈 수 있는 도구가 절실할 때이다. 따라서 정보 유출을 막기 위한 대책의 일환으로 개발된 패킷에 유출을 차단하는 기법은 네트워크 세그먼트 안에서 내부의 적으로부터 네트워크 세그먼트 내에 유동하는 패킷을 보호할 수 있고 패킷 유출 탐지 및 차단이 가능한 기법이다. 이는 소규모 네트워크나 개인 그리고 네트워크들이 일집된 집합체 등이 가장 기본적인 네트워크 세그먼트에서 부터 자신을 보호할 수 있는 도구이다. 또한 네트워크 내에 속한 하나의 노드에만 Server 프로그램을 설치하면 언제 어디서나 웹을 통해 네트워크의 사용자 개개인이 쉽게 사용할 수 있도록 간단한 인터페이스를 제공하여 손쉽게 패킷 유출을 탐지하고 유출 노드를 차단할 수 있다. 향후 연구방향은 현 OS중 사용자가 가장 많은 윈도우즈 기반의 패킷유출 차단시스템을 구축하여 보급화하는 것이다.

참 고 문 헌

[1] W. Richard Stevens, Addison-Wesley, "TCP/IP Illustrated, Volume1, The Protocols:", 2000.

[2] O Reilly, "TCP/IP 네트워크 관리", 한빛미디어, 2001

[3] W. Richard Stevens, "UNIX Networking Programming," 2nd Ed., Vol.1, 1998.