홈 네트워크용 보안 어플라이언스를 위한 트래픽 처리 시스템 구조 설계*

이순구O, 김형식
충남대학교 컴퓨터과학과
{cyrusO, hskim }@cs.cnu.ac.kr

Design of a Traffic Processing System Architecture for Home Network Security Appliance

Soon-Koo LeeO, Hyong-Shik Kim
Dept. of Computer Science, Chungnam National University

요 약

홈 네트워크 기술은 최근에 급격히 발달하고 있으나, 안전성 분야에 대해서는 아직 연구가 미흡한 실정이다. 본 논문에서는 홈 네트워크를 위한 보안 어플라이언스를 제안한다. 필터링과 리맵핑 기술을 이용 하여 악의적인 접근을 차단하고, 홈 네트워크 내부의 정보를 보호함으로써 홈 네트워크의 안전성을 향상시키며, 사용자의 편의성을 고려한 통합된 환경설정 기능을 제공하는 보안 어플라이언스를 설계하고자 한다.

1. 서론

참여정부는 2003년 8월 국가발전을 위한 핵심 산업으로 10대 IT 신성장동력을 선언하였다. 정보통신부가 주관처로 확정된 홈 네트워크 산업은 정보통신 네트워크를 중심으로 가정에서 사용하는 통신, 방송, 가전 등 다양한 IT기기들을 네트워킹하여 가정에서 풍요로운 디지털 라이프를 할 수 있도록 하는 새로운 유망사업 분야이다. 우리나라는 이미 세계 최고의 초고속 인터넷 망을 보유하고 있을 뿐만 아니라 홈 네트워크 산업에 필요한 인프라를 충분히 보유하고 있기 때문에 어느 나라보다도 관련 산업의 조기 활성화에 세계시장 선점에 유리한 위치에 있다.

홈 네트워크 구축으로 가정 내 모든 정보가전들이 외부망과 연동됨에 따라 해킹, 바이러스 유포 등 사이버 공격에 홈 네트워크가 노출되어있는 만큼 악성 트래픽이나 악의적인 공격이 홈 네트워크 내부로 유입되지 않도록 하는 것이 매우 중요하다.

본 논문은 부하의 정도(overhead)가 높지 않은 응용수준의 게이트웨이를 설계하고, 이를 바탕으로 보안 어플라이언스의 프로토타입을 설계한다. 응용 수준의 게이트웨이가 신뢰하지 않는 접근 및 비정상 트래픽을 통제함으로써 해킹이나 악의적인 공격에 대응 할 수 있는 방법과 IP주소 은닉기술을 이용한 홈 네트워크 안전성 향상 기법을 제시한다.

* 이 논문은 " 대학 IT 연구센터 육성지원사업" 에 의하여 수행된 과제의 결과임.

2. 전체적인 시스템 구조

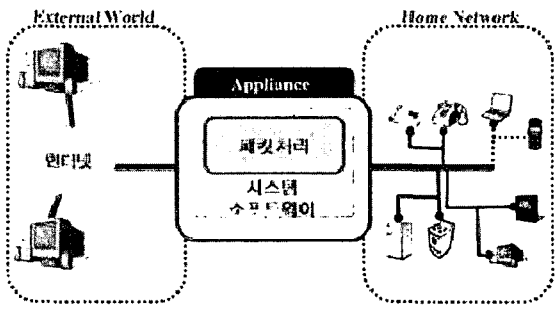

그림 1: 시스템 구조

홈 네트워크를 위한 보안 어플라이언스의 전체적인 구조는 그림 1과 같다. 외부망과 홈네트워크가 통신하는데 보안 어플라이언스가 홈 게이트웨이의 역할을 하며 트래픽 제어를 한다.

보안 어플라이언스는 응용수준의 게이트웨이와 안전성 향상을 위한 모듈들로 구성된다. 그림 2와 같이 게이트웨

이는 Libpcap 라이브러리와 Libnet 라이브러리로 구현되어 기본적인 게이트웨이 역할을 하고, 안전성 향상을 위한 필터링 모듈과 리맵핑 모듈은 게이트웨이 위에 적재되어 코어 엔진(Core Engine) 역할을 한다.

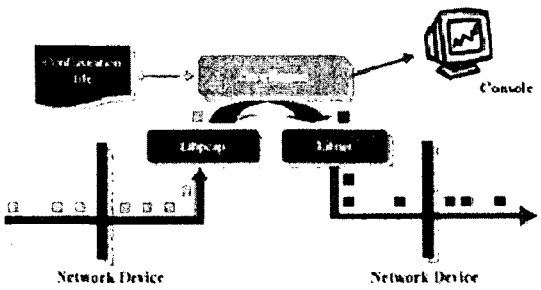

그림 2: 패킷 처리구조

3. 기능 모듈 설계

안전성 향상을 위한 코어엔진에는 크게 필터링 모듈과 리맵핑 모듈이 탑재되어있다. 필터링 모듈은 비정상 트래픽 및 악의적인 접근에 대한 제어를 하고, 리맵핑 모듈은 홈 네트워크 내부 정보의 은닉 및 보호하는 역할을 한다. 코어엔진은 설정파일을 기반으로 동작하는데, 설정파일은 사용자의 편의성을 위해 웹 인터페이스를 통해 제어기능을 제공한다.

3.1 필터링 모듈

필터링 모듈은 허용되지 않는 접근을 차단하는 모듈이다. 필터링 모듈은 IP주소기반의 접근제어와 포트번호기반의 응용서비스별 접근제어가 가능하고, 설정파일에 기반한 정적제어와 DOS공격처럼 의심이 가는 접근에 대해 시스템이 동적으로 차단하는 동적제어로 구분된다.

예를들어 그림 3과 같이 Trust Zone으로부터 들어오는 패킷은 홈 네트워크 내부에 전달되고 Distrust Zone의 접근은 차단하고, 로깅(logging)과 감사(auditing)를 통하여 보안성을 향상시킨다.

정적제어의 경우 설정파일을 기반으로 접근제어가 이루어진다. 설정파일의 경우 손쉬운 환경을 제공하기 위해 웹 기반의 인터페이스를 제공하는데 3.3절 환경설정 모듈에서 자세히 알아보기로 한다.

동적제어의 경우에는 IDS등의 침입을 감지할 수 있는 프로그램의 도움을 받는다. DoS등과 같은 비정상 트래픽의 발생을 침입탐지 프로그램이 알려주면, 필터링 모듈이 접근제어를 수행한다.

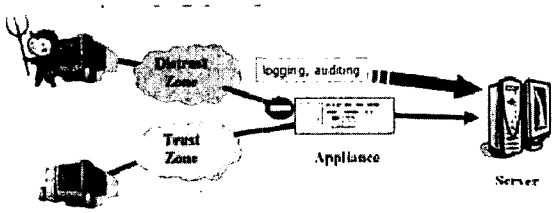

그림 3: IP주소기반 필터링

필터링 모듈은 Libpcap으로 캡쳐한 패킷을 설정파일과 비교하여 IP주소나 포트가 일치하는 패킷을 Libnet으로 보내지 않는 방식으로 동작한다. Libpcap을 통하여 캡쳐된 패킷이 Libnet 라이브러리를 통하여 다른 네트워크 인터페이스로 나가기전에 필터링 모듈이 개입하여 선별적으로 내보내도록 한다.

3.2 리맵핑 모듈

홈 네트워크 내부의 IP주소 은닉 및 보호를 위하여 IP 리맵핑 기술을 활용한다. 리맵핑은 다른 호스트에 연결될 때 실제 IP주소 대신 가상 의 IP주소를 할당하여 연결함으로써 실제 IP주소를 숨겨 안전성을 향상시키는데 목적이 있다. 이에 홈 네트워크 외부에서는 실제 IP주소를 알 수 없게 되어 악의적인 접근을 원천적으로 차단 하는데 도움을 준다.

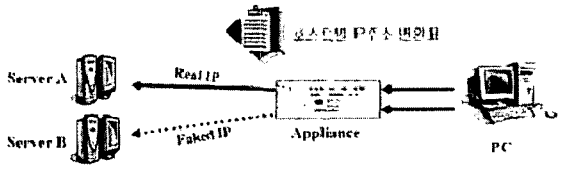

그림 4: 호스트기반 리맵핑

리맵핑 모듈에는 가상 IP주소가 사용된다. 가상 IP주소는 실제로 서브넷에 존재하는 IP주소 이며, 실제 IP주소를 은닉하기 위하여 실제 IP주소 대신 이용된다. 외부에서 가상 IP주소를 가지고 홈 네트워크 내부에 접근은 가상 IP주소를 가진 호스트가 없으므로 무의미하다. 리맵핑 자체도 어플라이언스 내부에 유지

되고 있는 정보를 기반으로 리맵핑이 이루어지므로 가상 IP로 실제 호스트에 접근은 불가능하다.

리맵핑 모듈은 호스트 기반의 리맵핑과 세션기반의 리맵핑으로 구성된다.

호스트 기반의 리맵핑은 그림 4처럼 연결된 호스트 별로 가상 IP를 다르게 주는 방식이다. 홈 네트워크 내부에서 외부의 호스트로 연결될 때 실제 IP주소는 보안 어플라이언스에 의해서 가상의 IP주소로 변환된다. 가상 IP주소의 수가 유한하기 때문에 서로 다른 호스트에도 동일한 가상 IP주소로 연결될 수 있다. 가상 IP주소가 유한한 이유는 가상 IP주소도 실제로 서브넷에서 사용할 수 있는 IP주소이어야 하기 때문이다. 호스트별로 가상 IP주소의 분배 방식은 long타입의 IP주소를 가상 IP주소로 나눈 나머지 값을 색인으로 하여 결정한다. 리맵핑을 통하여 다른 호스트와 연결이 되면 보안 어플라이언스 내부에 실제 IP주소와 가상 IP주소의 사상관계를 가지고 있고, 패킷이 되돌아 올 때 가상 IP주소를 실제 IP주소로 변환하는데 사용한다.

세션 기반의 리맵핑은 전체적으로 호스트 기반의 리맵핑과 같은 구조를 갖는다. 차이점은 호스트 기반의 리맵핑의 경우 호스트 별로 가상 IP주소가 항상 동일하게 정해져 있지만 세션 기반의 리맵핑은 가상 IP주소가 세션에 따라 수시로 바뀐다는 점이다. 세션은 시작 IP주소와 시작 포트번호의 조합으로 나타낼 수 있다. 세션기반의 리맵핑의 경우에는 서로 다른 호스트에서 동일한 시작 포트번호를 가지고 동일한 호스트에 접속할 수 있으므로 호스트 기반의 리맵핑 보다 더 많은 정보를 유지해야 한다. 시작 IP주소, 시작포트번호, 도착 IP주소, 도착 포트번호 그리고 가상 IP주소의 사상관계 정보를 유지해서 되돌아오는 패킷을 실제 IP주소로 바꿔 호스트에 보내준다.

3.3. 환경설정 모듈

환경설정 모듈은 일반 사용자들에게 편리한 인터페이스를 제공하기 위하여 웹 인터페이스를 이용한다. 사용자는 웹 인터페이스를 통하여 설정파일을 설정할 수 있다. 일반적으로 게이트웨이에는 보이지 않기 때문에 접근이 불가능하지만, 설정파일의 관리 목적으로 웹 서비스만 제한적으로 허용한다.

설정파일은 하나의 파일로 되어있으며, 정책사항, IP 필터링, 포트 필터링, 리맵핑의 4가지 섹션이 존재한다. 정책사항은 긍정정책(positive policy)와 부정정책(negative policy) 두 가지를 지원하는데, 사용자의 선택에 따라 긍정정책은 0로 부정정책은 1로 설정파일에 기록된다. 상황에 따라서 긍정정책 혹은 부정정책을 선택적으로 사용할 수 있도록 유연성을 제공한다. IP 필터링의 설정 파일 내용은 유연성을 제공하기 위 하여 IP주소와 서브넷을 함께 사용한다. 예를 들면 192.168.1.0/24와 같은 형태인데, 이것은 192.168.1.0에서 192.168.1.254까지의 IP주소를 모두 포함한다. 포트 필터링은 나열된 포트 번호가 설정파일에 기록된다. 포트 필터링의 경우에도 IP필터링과 함께 정책사항의 영향을 받으므로 선택한 정책사항에 맞춰 나열한다. 리맵핑은 나열된 가상 IP주소가 설정파일에 기록된다. 가상 IP주소는 서브넷에서 존재하는 IP주소를 사용해야만 패킷이 되돌아 올 때 다시 주소변환을 할 수 있어 정상적인 동작이 가능하다.

웹 인터페이스를 통하여 설정파일을 설정하는데 있어, 스니핑과 같은 악의적인 접근을 막기 위하여 http대신 https 서버를 사용한다. 내부로부터의 접근은 안전하다고 판단하여 인증과정을 거치지 않으며, 외부에서의 접근은 웹 서버의 인증모듈을 이용한 사용자 인증을 거친다.

4. 결론

홈 네트워크가 현실로 다가옴에 따라 보안 요구는 점차 증가하고 있다. 이를 위해 홈 네트워크 내부의 안전성을 향상 시킬 수 있는 방안이 필요하고, 홈 네트워크 자체의 안전성도 보장할 수 있는 기술이 필요하다.

본 연구에서는 홈 네트워크의 안전성 향상을 위한 보안 어플라이언스를 제안하였다. 필터링 및 리맵핑을 통한 패킷 처리를 이용하여 홈네트워크 안전성 향상방안에 대해 제시하였고, 안전한 코딩기법을 통하여 보안 어플라이언스 자체의 안전성 향상 기법을 제시하였다.

이와 같이 안전한 홈 네트워크를 위한 보안 어플라이언스를 설계함으로써 아직 미비한 홈 네트워크 보안 기술을 확보하였으며, 이 기술을 이용하여 홈 네트워크 보안 분야의 요소기술로 활용할 수 있다.

참고문헌

[1] T.S. Eugene Ng, " A Waypoint Service Approach to Connect Heterogeneous Internet Address Space", USENIX Annual Technical Conference 2001

[2] Carl M. Ellison, " Home Network Security", Intel Technology Journal