개방형 네트워크 보안 시스템 아키텍처에 관한 연구

김창수* · 김택천** · 정회경**

*청운대학교 인터넷학과 · **배재대학교 컴퓨터공학과

A Study on Open Based Network Security System Architecture

Chang-su Kim* · Tak-chen Kim** · Hoe-kyung Jung**

*Dept. of Internet, Chungwoon University · **Dept. of Computer Engineering, Paichai University

E-mail : *ddoja69@chungwoon.ac.kr · **{tckim· hkjung}@pcu.ac.kr

요 약

기존의 시스템들이 보안적인 요소를 포함하려 한다면 많은 비용 문제와 함께 복잡한 설치 과정을 거쳐야 했으며 폐쇄적인 구조로 많이 구성되어 사용자 측면에서는 많은 불편을 감수해야만 보안이 확립되는 단점을 갖는 구조를 취하고 있었다.

본 논문에서는 이런 단점들을 공개 보안 도구 사용과 보안 서버를 프락시 서버, 인증 서버 등을 모두 포함하는 베이스천 호스트(bastion host) 형태의 방화벽 시스템으로 구성함으로써 집중적인 구성이 가능하여 비용 및 관리 면에서도 편리함과 독립적인 보안을 동시에 제공된다. 또한, 각각의 보안 대상 호스트에도 별도의 보안 소프트웨어를 설치하여 다양한 보안 레벨을 적용할 수 있도록 구성하였다. 더욱이 암호화 정책에 따라 암호화 알고리즘을 적용하여 보안의 수준을 한 차원 높였으며 자주 사용하는 서비스에 대해서는 프락시 서버를 제공하여 사용자들에게는 투명성을 제공했다.

본 논문에서는 시스템 보안과 네트워크 보안의 유기적인 연동을 통해 개방적이면서도 유연하고 독립적인 보안을 확립할 수 있는 형태의 보안 시스템을 제안한다.

ABSTRACT

If existing system need to expand security part, the security was established after paying much cost, processing of complicated installation and being patient with inconvenience at user's view because of closed structure.

In this thesis, those defects could be overcome by using open security tools and constructing security server, which is firewall of 'bastion' form including proxy server, certification server and so on. Also each security object host comes to decide acceptance or denial where each packet comes from, then determines security level each hosts. Precisely it is possible choosing the packets from bastion host or following at the other policies. Although an intruder enter into inside directly, it is constructed safely because encryption algorithm is applied at communication with security object host.

This thesis suggests more flexible, independent and open security system, which improves existing security through systematic linkage between system security and network security.

키워드

network security, proxy server, bastion host, encryption algorithm

Ⅰ. 서 론

정보화 시대가 되어감에 따라 많은 곳에서 정보 시스템을 구축, 운영하고 있고 대부분의 작업들이 정보 시스템을 통해 이루어지고 있으며, 데이터의 이동 또한 컴퓨터와 네트워크를 통해 이루어진다. 하지만 정보 시스템 구축의 보안관리 및 네트워크 시스템 보안 운영을 소홀히 하여 네트워크 보안에 많은 허점이 노출되고 있다.

기존의 네트워크 시스템은 보안을 강화하려 많은 비용과 복잡한 설치 과정을 거쳐야 했으며 대부분 폐쇄적인 구조로 구성되어 사용자 측면에서 본다면 상당한 불편을 감수해야만 보안이 확립되는 구조를 갖는다[1,2,3].

이에 비용 및 관리측면에서 효율성 및 편리함과 독립적인 보안을 동시에 제공할 수 있는 개방

형 네트워크 보안 시스템의 필요성이 대두되었다. 개방형 네트워크 보안 시스템은 네트워크 보안과 시스템 보안의 유기적이고 효과적인 결합이 이루어지게 되어 보다 향상된 보안 시스템으로의 발전 가능성에 대해서 제시한다.

이에 본 논문에서는 네트워크 보안과 시스템 보안의 유기적이고 효과적인 결합이 이루어지게 하여 보다 향상된 보안 시스템 구성이 가능한 개방형 네트워크 보안 시스템 아키텍처를 설계하였다.

본 논문의 구성은 다음과 같다. 제2장에서는 네트워크 보안 침입 유형을 기술하고, 제3장에서는 네트워크 시스템 보안 기반 기술을 설명한다. 제4장에서는 네트워크 보안 시스템 아키텍처를 기반으로 실제 개방형 네트워크 시스템을 설명하고 5장에서 결론과 함께 향후 연구방향을 대해 기술한다.

II. 관련연구

2.1 부당한 액세스 유형

2.1.1 시스템의 방해

어느 시스템의 중심적 역할을 가지고 움직이는 호스트 등에 대해서 대량의 패킷이나 메시지를 보내어 그 호스트의 CPU 사용률을 비정상적으로 높여 운용을 방해하는 것이다[1,2,3,4,]. 또 다른 방법으로서는 부정한 경로 정보를 고의로 흘려 통신 불능, 또는 패킷루프와 같은 상태가 되는 경우도 있다. 이들 방법은 시스템에 영향을 주며 시스템 전체를 파괴시킬 수도 있다. 이를 그림 1에 보인다.

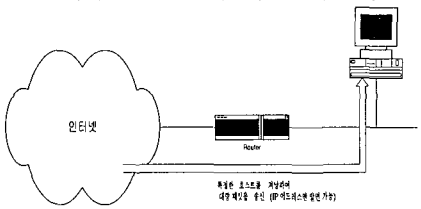

그림 1. 시스템 방해

2.1.2 네트워크상의 데이터 복제

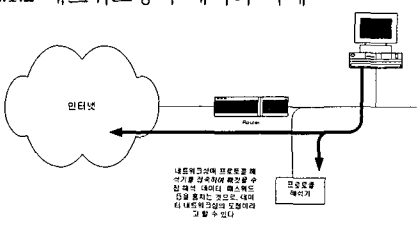

그림 2. 네트워크상의 데이터 복제

네트워크상의 데이터 복제는 그림 2와 같이 네트워크상에 흐르고 있는 데이터를 직접 훔치는 방법이다. LAN이나 WAN에서 실제로 사용되고 있는 네트워크에는 프로토콜 해석기 등을 장치함으로써 패킷을 수집할 수가 있으며 그 패킷에서 필요한 정보를 분석하는 것도 가능하다.

2.2 NIS(Network Information Service) 공격

NIS에 의한 공격에는 NIS 서버 스푸핑(spoofing)에 의한 공격, NIS 클라이언트 스푸핑에 의한 공격, 데몬 프로그램 버그를 이용하는 방법으로 이루어진다[4,5,6,7,8].

NIS 서버 스푸핑은 NIS 클라이언트의 RPC 요청에 대해 서버보다 먼저 가짜 정보를 보내주어 클라이언트를 공격하는 방법이다. 그림 3에 NIS 서버 스푸핑에 대해 보인다.

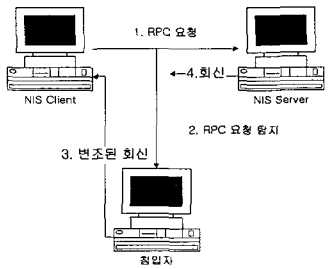

그림 3. NIS 서버 스푸핑 공격

III. 시스템 보안

3.1 베이스천 호스트

베이스천 호스트는 보호하고자 하는 네트워크의 외부에 공개되어 있는 호스트를 지칭하는 말이다. 베이스천 호스트의 역할은 시스템 관리자가 망 보안의 가장 강력한 장소로 인식하며, 내부 망으로 침입할 수 있는 영역으로 베이스천 호스트를 통하게 함으로써 위험 지역의 범위를 안정시키는 역할을 해 준다[7,8]. 일반적으로 베이스천 호스트는 높은 보안 상태를 유지하고 있다 가정하고, 감사(Audit) 기능 또는 추적(Trail) 기능을 갖고 있으며, 보안 유지를 위한 응용 소프트웨어들이 존재한다. 대부분 2개의 패킷 필터링 라우터 사이의 유닉스 시스템을 베이스천 호스트라고 한다. 외부 라우터는 인터넷과 베이스천 호스트 사이의 트래픽만 허락된다. 내부 라우터는 내부 네트워크(안전한 네트워크)과 베이스천 호스트의 트래픽만이 허락된다.

IV. 개방형 네트워크 보안

4.1 라우터 설정 보안

4.1.1 어드레스 제어

인터넷 접속은 일반적으로 라우터를 사용하며 조직 내부에서 인터넷에 접속을 하는 경우 라우팅이 수행된다. 라우터는 송신원 IP 어드레스와 수신처 IP 어드레스를 보고 라우팅여부를 판단하여 송신원 IP 어드레스만 한정 하거나 송신원 IP

어드레스와 수신처의 IP 어드레스 쌍(pair)으로 한정하여 허가된 어드레스만 인터넷으로의 통신을 허가하는 방법이 있다. 그림 4에 조직 내외의 통신과 패킷 내의 IP 어드레스 제어를 보인다.

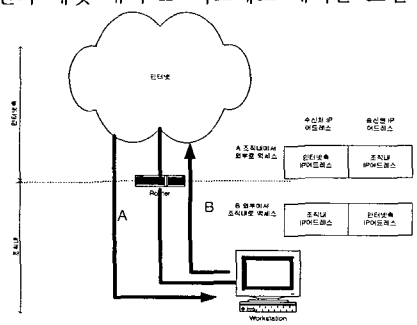

그림 4. IP 어드레스 제어

라우터 상에 호스트 A의 IP 어드레스와 호스트 B의 IP 어드레스만 패킷 통신만을 허용한다고 정의하면 호스트 A와 호스트 B만이 통신할 수가 있고 그 이외의 호스트들은 통신을 직접적으로는 할 수 없게 된다.

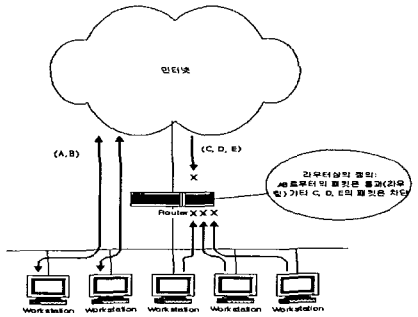

그림 5. 라우터에 IP 어드레스 정의

그림 5는 라우터에 IP 어드레스 정의를 보인다. IP 헤더의 참조 및 분석이라는 라우터의 기능을 이용해서 통신의 보안을 설정한다. IP 어드레스를 체크할 때 보안 여부를 판단하여 보안 설정에 위배되는 패킷은 라우터를 통과시키지 않고 파기한다. 이와 같은 설정을 한 경우는 라우터가 패킷을 처리할 때 일반적인 라우팅 처리에 이 보안용 처리가 더해진다.

일반적인 라우터의 라우팅 처리의 경우 통신 패킷을 수신하며, 우선 IP 헤더를 보고 헤더 필드 중 수신처 IP 어드레스에서 수신처의 IP 네트워크를 판단한다. 수신처의 IP 네트워크까지 패킷을 라우팅 시키면서 라우팅 테이블을 검색하여 다음 라우터에 패킷을 전송한다.

4.2 개방형 네트워크 보안 시나리오

네트워크 보안 툴 및 유틸리티들을 이용하여 보다 유연하면서 향상된 기능을 제공 할 수 있는 보안 시스템과 다양한 형태의 네트워크 보안 시나리오 중 중소규모의 회사 및 연구소에 알맞은 보안 시나리오이다. 중소규모라고 해도 대규모 네트워크에서도 자신만의 보안 서브 네트워크를 구축할 수 있도록 유연성을 확보하여 구성하였다. 그림 6은 개방형 네트워크 보안 시나리오를 위한 구성도이다.

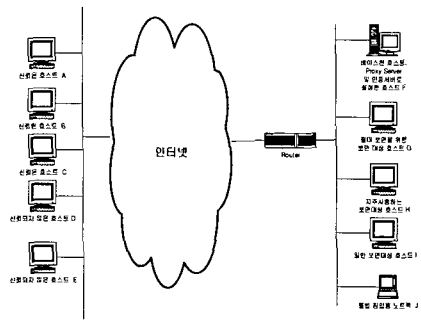

그림 6. 개방형 네트워크 보안 시나리오를 위한 구성도.

4.2.1 호스트 F 구성

베이스천 호스트의 구성은 베이스천 호스트 구성 규칙에 따라 최대한 철저히 안정된 서비스만 제공되며 사용자 계정은 관리자 외에는 모두 제거했다. 또한 관리자의 경우에도 외부에서의 접속에 의한 관리는 허용하지 않았다. 그리고 TIS 방화벽 툴킷(TIS Firewall Toolkit)을 이용하여 인증 서버와 프락시 서버를 구성했으며 도메인 네임 서비스를 제공하고 있다. 그리고 만약 암호화 기법 적용단계에 따라 암호 쉘과 S/KEY, logdaemon등을 사용할 수도 있다.

4.2.2 보안대상 호스트 G, H, I 구성

보안을 위한 보안 대상 호스트에는 일단 TCP Wrapper를 설치한 후 각각의 특성에 따른 접근 규칙을 따로 두었는데 그 접근 규칙은 절대 보안을 요하는 호스트 G의 경우 내부네트워크에 대해서도 오직 호스트 F로부터의 정상적인 접속만을 허용하고 외부 네트워크에 대해서는 접근조차 허용되지 않게 구성한다. 자주 사용하는 호스트 H의 경우는 외부 네트워크에 대해서만 접속을 허용하지 않으며 내부 네트워크에 다른 호스트들로부터의 접속을 모두 허용한다. 일반 보안 대상 호스트 I의 경우는 호스트 F로부터의 접속과 정상적 외부접속을 허용한다. 그리고 내부 네트워크에서도 접속 대상 호스트를 규정하여 그 호스트만이 접근가능 하게 구성한다.

4.2.3 그 밖의 구성

각각의 보안 대상 호스트에는 보안 쉘을 도입한다. 그러나 만약 보안을 요하는 호스트가 적고 일반 사용자가 많다면 보안 쉘 도입에 대해 신중

히 검토해야 한다. 프락싱 동작 시 S/KEY로 암호화 기법을 적용하였고 각각의 호스트 접근 규칙을 portmap, netacl, TCP wrapper등으로 네트워크 접근 규칙을 설정 해준다.

4.3 개방형 네트워크 보안 시스템 동작 방식

1) 신뢰된 호스트로부터 보안 대상 호스트로의 접속

신뢰된 호스트로부터 보안대상 호스트에 접속은 라우터에서 라우팅 테이블의 규칙에 따라 접속 가능한 호스트인지를 판단하고 각 서비스에 따라 베이스천 호스트를 경유하여 또 한 번의 접속 규정을 따르게 된다. 그런 후 각각의 해당 서비스의 프락시 서버를 사용하여 보안대상 호스트로의 접속이 이루어진 후 인증이 필요한 서비스에 한해서 인증 과정을 거친 호스트에 한해서 접속이 허용 된다.

2) 신뢰되지 않은 호스트로부터 보안 대상 호스트로의 접속

신뢰되지 않은 호스트로부터 보안 대상 호스트로 접속을 시도하면 라우터에서 라우팅 테이블 규칙에 따라 접속 허용 여부를 판단한다. 이때 대부분의 신뢰 되지 않은 컴퓨터는 제외된다.

일부 해킹기술로 라우터를 통과 하여 베이스천 호스트로 접속이 이루어지면 베이스천 호스트에서 해당 호스트의 접속 규정을 다시 한 번 적용하게 된다.

3) 보안대상 호스트에서 다른 보안 대상 호스트로의 접속

보안 대상 호스트에서 다른 보안 대상 호스트로의 접속 시에도 베이스천 호스트와 프락시 서버 및 인증 서버를 통과하게 된다. 이는 각 보안 대상 호스트의 보안 수준을 다 다르게 줄 수 있기 때문이다. 그렇게 함으로써 상당한 보안을 요하는 호스트와 자주 사용하면서 일반적인 보안 수준을 따르는 호스트들의 유연성을 확보하기 위한 것이다. 결과적으로 내부 보안까지도 보안 수준을 달리 적용할 수 있다.

4.4 개방형 시스템의 구성 이점

1) 호스트 보안과 네트워크 보안의 유기적인 연동

최신 해킹 기술들로부터 안전한 베이스천 호스트를 구성하고 암호화 어플리케이션을 적용하여 보안 수준을 높일 수 있다.

2) 보안대상의 범위의 확장

개방형 보안 시스템의 경우는 내부 네트워크와 함께 외부에 있는 시스템도 보안 대상에 포함 할 수 있다.

3) 유연하고 다양한 보안수준

폐쇄적인 보안 환경에서도 외부 네트워크와 내부 네트워크간의 연결을 프락시 서버를 사용하여 유연하게 제공하므로 사용자들에게는 투명성을 보장 할 수가 있다. 내부 네트워크에 한 가지 보안 수준이 아닌 다양한 보안 수준을 적용할 수가 있다.

V. 결론

정보통신의 급격한 발전과 더불어 컴퓨터가 보편화되면서 인터넷 사용이 생활화되고 그에 따른 다양한 형태의 네트워크 시설과 기술들이 선보이고 있다. 네트워크의 보급은 생활의 편리성을 제공하였지만 정보에 대한 전송방해, 도청, 불법변조 등의 위험뿐만 아니라, 네트워크 불법접근으로 보관 중인 정보가 유출되는 실정이다.

이에 대처하기 위해 많은 비용과 시간이 투자될 뿐만 아니라 다양한 기술과 고도의 시설 및 장비가 투입되고 있다. 하지만 소규모 단일 네트워크에서는 보안장비를 관리하고 운용하는데 소요되는 비용과 기술 부족에 따른 어려움이 있다.

이에 본 논문에서는 시스템 보안과 네트워크 보안의 유기적인 연동을 통해 개방적이면서도 유연하고 독립적인 보안을 확립할 수 있는 형태의 보안 시스템을 제안하였다.

본 논문에서는 공개 보안 도구 사용과 보안 서버를 프락시 서버, 인증 서버 등을 모두 포함하는 베이스천 호스트 형태의 방화벽 시스템으로 구성함으로써 집중적인 구성이 가능하여 비용 및 관리 면에서도 편리함과 독립적인 보안을 동시에 제공한다. 또한, 각각의 보안 대상 호스트에도 별도의 보안 소프트웨어를 설치하여 다양한 보안 레벨을 적용할 수 있도록 구성하였다. 더욱이 암호화 정책에 따라 암호화 알고리즘을 적용하여 보안의 수준을 한 차원 높였으며 자주 사용하는 서비스에 대해서는 프락시 서버를 제공하여 사용자들에게는 투명성을 제공했다.

향후 연구로서 다양한 네트워크 환경의 동적인 변화에 따라 동적으로 적용할 수 있는 네트워크 보안 관리 모델에 관해 연구하고자 한다.

참고문헌

[1] 최용락 외 3인, 통신망 정보 보호, 도서출판 그린, 2002

[2] 채규혁, 인터넷 방화벽 구축하기, 한빛 미디어, 2001

[3] Simson Garfinkel, Gene Spafford, Practical UNIX & INTERNET Security 3rd edition, O'Reilly & Associates, 2003

[4] Dieter Gollmann, Computer Security, John Wiley & Sons, 2006

[5] Raymond R.Panko, Corporate Computer Network Security, Prentice Hall, 2003

[6] Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Building Internet Firewalls, O'Reilly & Associates, 2000

[7] Norbert Pohlmann, Tim Crothers , Firewall Architecture for the Enterprise, John Wiley & Sons, 2002

[8] Loza, Boris, Unix, Solaris And Linux : A Practical Security Cookbook: Securing Unix *Operating System Without Third-party* Applications, Lightning Source Inc, 2005