백도어형 사설망의 작업효율 개선에 관한 연구

정회원 이 현 창*, 이 종 언**

A Study on the Improving Operation Efficiency of the Back-door type Private Network

Hyun-Chang Lee*, Jong-Eon Lee** ***Regular Members***

요 약

본 논문에서는 동일 공간범위 내에서의 정보교환 시 방화벽 시스템 없이도 시스템 보안과 전송속도에 우수한 효과가 있는 백도어형 사설망의 단점을 분석하고 이를 개선하기 위한 방법을 제시하였다. 제시된 방법의 효과를 입증하기 위해 윈도우 기반 컴퓨터들과 유닉스 기반 컴퓨터들을 한 공간 내에 설치한 후 파일교환을 시행한 결과, 본래의 백도어형 사설망이 가진 보안적 특징과 파일 전송속도의 극대화 장점은 그대로 유지되면서도 파일교환에 필요한 서버가 생략되는 효과가 있음을 확인하였다. 특히, 두 번의 조작에 의해 이루어졌던 파일교환이 한 번의 조작으로 가능해져 사용상 편리성이 증가되고 작업 시간도 크게 단축되는 등 작업효율이 향상됨을 확인하였다.

Key Words : backdoor, LAN, 전산망, 보안, 사설망

ABSTRACT

In this paper, we analyzed the weakness of the Back-door type private network which was effective method of system security and transmission speed in the same area without firewall system, and presented the solution to improve it. To prove the effect of this solution, Windows based systems and UNIX based systems are set up in same area, data transmission was tried. According to the result, this solution can maintain the advantage of the Back-door type private network and can have the advantage of removing file server and increasing operation efficiency by reducing the number of operation.

Ⅰ. 서 론

1.1 전산망의 보안 문제

최근에는 컴퓨터의 저가격화, 고성능화와 인터넷 등의 보급에 의한 네트워크 화에 따라 대부분의 컴퓨터들이 거대한 네트워크를 형성해 정보교환과 공유가 원활해지고 있다. 이에 힘입어 회사나 그룹 단위로의 네트워크는 필수적이 되었으며 한 개인이 동일 공간 내에 2대 이상의 컴퓨터를 역할 분담해 활용하고, 이들 컴퓨터는 전산망을 통해 정보를 교환하도록 구성하는 경우도 많아졌다. 이와 같은 추세에 따라 데이터 전송 시 약점을 이용해 중요 정보를 노리는 해커(hacker)와 크래커(cracker) 또한 증가하고 있으며, 이 때문에 컴퓨터 시스템의 보안 문제가 크게 대두되 방화벽 시스템과 같은 장비를 이용해 보안을 강화하고 있다.[1, 2] 그러나, 방화벽 시스템이 구축된 전산망이라도 그 내부의 구성원간은 사실상 방화벽이 없는 상태이므로 방화벽 내에 있는 컴퓨터 사이에서는 상호간 보안이 어려우며, 학내망(學內網)이나 사내망(社內網) 내부에서는 구성

* 국립 공주대학교 공과대학 정보통신공학부 부교수 (hclee@kongju.ac.kr)
** 국립 공주대학교 공과대학 전기전자공학부 교수 (jelee@kongju.ac.kr)
논문번호 : KICS2005-07-307, 접수일자 : 2005년 7월 27일, 최종논문접수일자 : 2006년 3월 2일

원간의 컴퓨터 보안이 사각지대에 놓인다. 예를 들어, 학내망의 방화벽 내에는 교수 컴퓨터와 학생 컴퓨터가 공존하며, 이 때 교수실 내의 컴퓨터들은 학생 컴퓨터의 공격 대상이 될 수 있고, 이러한 내부 공격에는 취약함을 나타낸다.[3],[4] 이에 따라 동일공간 내의 컴퓨터 사이에서 계정과 비밀번호가 암호화되어 있지 않은 텔넷(telnet)이나 FTP를 사용할 경우 패킷 도청에 의해 이러한 정보가 쉽게 유출되며, 이의 대안으로 SSL(Secured Socket Layer)[5]이 제시되고 이를 이용한 텔넷과 FTP가 사용되기도 하지만, 서버의 경우 이러한 데몬(daemon)이 설치되어 있다는 것만으로도 포트 스캔(port scan)을 거쳐 해당 포트에 오버플로(over-flow) 공격이 가능한 허점이 있다. 이러한 점을 고려해 유닉스(UNIX) 기반 시스템에서는 다른 컴퓨터로부터의 접속은 거부하고 서버 관리자 컴퓨터 등 특정 주소에만 반응하도록 IP 필터링(패킷 필터링) 기법[6]이 고안되고 xinetd나 ipchain 프로그램 등이 제작, 사용되는데, 이는 학내망이나 사내망에서 가변 IP 주소를 사용하는 경우 서버 관리자의 주소가 항시 변화하므로 적용할 수 없는 단점이 있고, 서버 관리자가 고정 IP 주소를 사용한다 하더라도 공격자가 자신의 주소를 서버 관리자의 주소로 둔갑해 접근하는 경우 허점이 노출된다.

1.2 방화벽 및 기타 보안 시스템

앞서 논한 바와 같은 동일공간 내의 정보교환 시 발생하는 문제점들을 해소하기 위해 그림 1과 같은 기본 구조를 가진 방화벽 시스템을 이용할 수 있으며, 이는 그 용도와 상태에 따라 여러 가지 변화된 형태가 제시되고 있다.[7]

그러나, 이와 같은 개인 방화벽 내에서 서버 등을 운영하는 경우 방화벽 시스템 또한 항시 가동상태에 있어야 하므로 또 하나의 서버를 운영해야 하는 경제적 부담과 운영의 부담이 발생하고, 일반 사용자의 경우 방화벽 시스템을 최상으로 운영할 능력 확보가 어렵다. 즉, 학내망의 모든 교수들, 또는

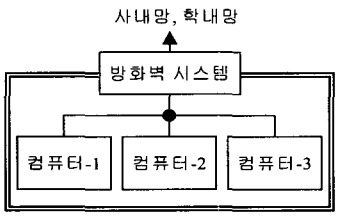

그림 1. 개인 방화벽 구축에 의한 보안

사내망의 모든 부서에서 각각 방화벽 시스템을 구축해 운영한다는 것은 경제적인 면에서나 운영 부담 측면에서 현실적으로 어렵다 할 수 있다.

개인 정보 전송의 보안을 위해 외부에 공개하는 시스템들은 그림 2에 나타낸 바와 같이 별도의 망을 형성하고, 보안이 필요한 시스템들은 나름대로 별도의 망을 구성한 후 이들 사이에 교량역할을 하는 중계 시스템을 구축해 공개용 전산망과 보안용 전산망을 분리하는 DMZ 방법이나 Screened Network 방법이 제시되고 그 활용 방안이 연구되고 있다.[8]

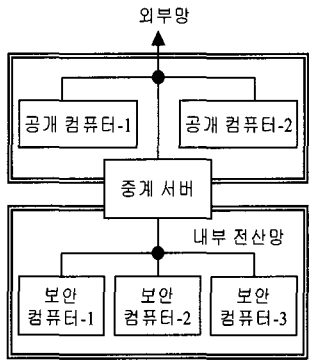

그림 2. 전산망 분리에 의한 보안

이들 방법은 보안에 있어 매우 효과적이고 내부 전산망 사이에는 기존의 보안에 취약한 프로그램이나 프로토콜을 그대로 사용할 수 있다. 그러나 중계 서버가 허점에 노출되면 내부 전산망 모두가 위험에 노출되므로 고도의 전문 운영자가 필요하고 별도의 중계 서버를 설치해 운영하는 등 비교적 대규모 전산망에서 사용할 수 있으며, 개인이 활용하기에는 경제적으로나 운영적인 면에서 많은 어려움이 따른다.

1.3 백도어형 사설망의 제시

앞서 논한 바와 같은 소규모 시스템에서의 운영 부담에 대한 문제점을 해소하기 위해 Lee[9]등은 별도의 방화벽 설치 없이도 동일 공간 범위 내에서 우수한 보안효과와 통신속도의 극대화를 이룰 수 있는 백도형 사설망을 제시하였는데, 이는 다음 장에서 논하는 여러 가지 장점이 있지만 파일 전송 시 비밀 파일서버를 통해 모든 전송이 이루어지므로 비록 단순한 형태의 파일서버라 할지라도 파일을 전송할 때마다 이 서버를 켜고 부트시키는 과정이 필요하다. 또한, 파일을 전송할 때는 데이터 송

신 컴퓨터에서 파일서버로 전송한 후 다시 데이터 수신 컴퓨터에서 파일서버로부터 파일을 가져와야 하는 2중의 작업이 필요하며, 특히 두 컴퓨터가 약간이라도 거리가 떨어져 배치된 경우 매번 작업자가 두 컴퓨터 사이를 오가며 작업해야 하는 단점이 존재한다.

따라서 본 논문에서는 백도어형 사설망의 장점은 그대로 유지하면서 단점을 개선해 더욱 효과적인 사용을 위한 방법을 제시하고자 한다.

Ⅱ. 백도어형 사설망의 문제점 및 개선방안

2.1 백도어형 사설망의 문제점

2.1.1 백도어형 사설망의 원리 및 특징

백도어형 사설망은 그림 3과 같이 각 컴퓨터에 2개의 네트워크 인터페이스 장치를 설치해 한 장치(eth0)는 기존의 주 전산망과 접속하고, 나머지 장치(eth1)는 내부적으로 사설망을 구성하고 있다.[9]

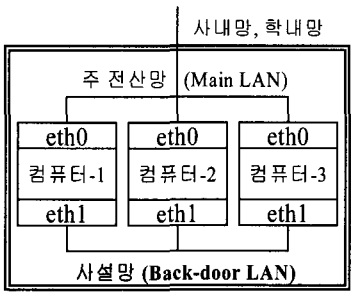

그림 3. 백도어형 사설망의 구성

각 컴퓨터들은 라우팅(routing) 정보를 설정해 데이터가 입출력 될 장치(eth0나 eth1)를 결정하는데,[10] 사설망에는 주 전산망에서 사용하지 않는 IP 주소, 즉 RFC-1918[11]에서 규정한 사설 IP 주소 그룹을 사용하고, 넷-마스크(net-mask)에 의해 이 IP 주소 그룹일 경우 eth1을 통해 입출력하고, 그 이외의 주소들은 모두 기본 장치(default gateway)인 eth0을 향하도록 설정하면 일반 데이터는 기본 장치를 경유해 주 전산망으로 접속되고, 개인 데이터는 사설망을 통해 해당 컴퓨터에 전달된다. 이에 따라 백도어형 사설망은 다음과 같은 특징을 가진다.[9]

첫째, 기존의 주 전산망 구조에 영향을 주지 않으면서 쉽게 설치하고 운영할 수 있다.

둘째, 개인 데이터는 주 전산망을 거치지 않고 별도의 망을 거치므로 정보가 외부로 유출되지 않는다.

셋째, 주 전산망에 부하를 주지 않으면서 설치된 사설망의 최대 속도로 정보 교환을 할 수 있다.

넷째, 계정 및 비밀번호 유추 공격, 패킷 도청이나 데몬 오버플로 공격을 받지 않으므로 기존의 텔넷과 FTP를 보안기능 없이 그대로 사용할 수 있다.

다섯째, 윈도우 기반 시스템에서는 외부로 공유 디렉토리 정보가 유출되지 않음에도 불구하고 사설망에는 공유 디렉토리가 나타나며 정상적으로 공유가 가능하다.

여섯째, 스테이션 당 네트워크 인터페이스 장치 한 개의 추가 이외에 별도의 하드웨어나 소프트웨어를 설치할 필요가 없어 경제적이면서 전문지식 없이 설치할 수 있다.

일곱째, 사설 IP 주소를 사용하므로 가변 IP 주소를 사용하는 경우에 관계없이 적용시킬 수 있다.

2.1.2 백도어형 사설망의 문제점

백도어형 사설망을 이용한 데이터 전송에서, 윈도우 기반 컴퓨터대 윈도우 기반 컴퓨터일 경우에는 공유 프로토콜(NetBEUI, TCP/IP)의 바인딩을 조절함으로써 주 전산망으로는 네트워크 클라이언트로만 작용하고 사설망으로는 네트워크 서버와 클라이언트 모두를 가동시켜 공유가 가능하다. 그러나, 윈도우 기반 컴퓨터대 유닉스 기반 컴퓨터 사이의 데이터 전송에서는 보안상 유닉스 기반 컴퓨터에 데몬을 설치하지 않기 때문에 그림 4와 같이 별도의 비밀 파일서버를 설치하고 이를 경유해 데이터를 전송한다.

비밀 파일서버는 고성능의 것이 필요한 것은 아니므로 비록 비용이나 운영 부담 측면에서 크게 문제가 되지는 않지만, 파일을 전송하기 위해서, 예를 들어 윈도우 컴퓨터측에서 유닉스 컴퓨터 측으로 데이터 전송을 할 경우 그림 4와 같이 윈도우 컴퓨터에서 파일서버로 데이터를 전송하고 유닉스 컴퓨

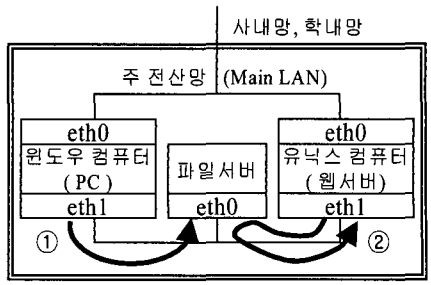

그림 4. 윈도우 기반 컴퓨터 대 유닉스 기반 컴퓨터의 파일교환

터에서 클라이언트 자격으로 파일서버로부터 파일을 가져가는 두 번의 조작이 필요하다. 특히 이러한 조작은 동일 공간 내라 하더라도 두 컴퓨터의 거리가 떨어져 있는 경우나 시스템 개발 및 시험과 같이 자주 파일을 전송해야 하는 경우에는 그 불편함이 가중되고 작업 효율이 현저히 떨어지는 문제점이 있다.

이 시스템을 이용할 경우, 작업 초기에 파일서버를 부트시키는 시간이 1회 필요하고, 그 이후에는 송신측 컴퓨터의 작업시간과 수신측 컴퓨터의 작업시간, 그리고 양측을 오가는 2번의 이동시간이 각 반복작업마다 필요하므로 전체 소요시간은 다음과 같이 나타낼 수 있다.

$$t_{tot,fs} = t_{boot} + (t_{trns} + 2 \cdot t_{mv} + t_{recv}) \times n \quad (1)$$

여기서,

t_{boot} : 파일서버의 부트 시간

t_{trns} : 송신측 컴퓨터 조작시간

t_{mv} : 작업자 이동시간

t_{recv} : 수신측 컴퓨터 조작시간

n : 반복 횟수

이다.

따라서, 파일 전송이 반복되는 횟수가 많은 작업, 예를 들어 웹 컨텐츠 개발이나 웹 기반 프로그램 개발작업 등에서는 반복 횟수가 늘어남에 따라 전체 작업시간이 크게 늘어난다.

2.2 문제점의 개선 방안

이상에서 살펴본 백도어형 사설망의 운영상 불편함과 별도의 비밀 파일서버 설치 문제를 해결하기 위해 다음과 같은 2가지 방법을 고려할 수 있다.

2.2.1 콘솔(console) 제어형

파일서버가 설치된 이유를 살펴보면 웹서버 등으로 사용되는 유닉스 컴퓨터의 해킹 확률을 저감하기 위해 데몬의 설치를 자제하고 클라이언트로서 파일전송을 하기 위함이다. 따라서 그림 5와 같이 작업용 PC에 FTP 서비스 프로그램을 설치한다면 파일서버를 생략한 상태에서도 유닉스 컴퓨터는 클라이언트 자격으로 파일을 전송할 수 있는데, FTP 서비스 프로그램은 다음과 같은 사항들을 고려해야 한다.

첫째, 평상시의 안전을 위해 on/off가 자유로워야 할 것. 이는 데몬 형식으로 설치되지 않고 독립 프로그램 형식으로 구성된 것이라면 필요할 때만 잠시 가동시켜 사용하고 평상시는 가동시키지 않아 해킹의 위험에 노출될 확률은 크게 낮아진다.

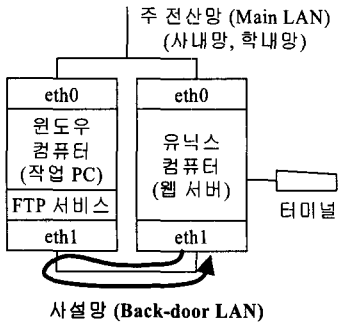

그림 5. 윈도우 PC에 FTP 서비스의 설치

둘째, 서비스 대상 네트워크 장치를 선택할 수 있을 것. 즉, 외부망에 대해서는 서비스되지 않고 사설망에 대해서만 서비스해 외부망에서 이러한 서비스의 존재 유무를 파악하지 못하도록 한다.

이상과 같은 조건을 갖춘 FTP 서비스 프로그램을 작업용 PC에 이용한다면 FTP 서비스에 대한 공격의 확률은 다음과 같이 저감될 수 있다.

$$P_{on} \times P_{FTP} \times P_{bug} \quad (2)$$

여기서,

P_{on} : 작업용 PC가 가동되어 있을 확률

P_{FTP} : 작업용 컴퓨터 사용 중 FTP 프로그램이 가동되어 있을 확률

P_{bug} : 프로그램 버그에 의해 사설망 대상의 FTP 서비스를 외부망에서 접속할 수 있는 확률

이다. 예를 들어 주 5일 하루 8시간 근무의 경우, 점심시간을 포함해 하루 9시간 컴퓨터가 켜져 있고 근무 중 서버와의 파일전송을 매일 30분씩 빠짐없이 한다고 가정하면,

$$P_{on} = (9\text{시간})/(24\text{시간} \times 7\text{일}) = 0.054$$

$$P_{FTP} = (0.5\text{시간})/(9\text{시간}) = 0.056$$

따라서, 항시 가동중인 서버에 FTP 데몬을 설치했을 때 보다 작업용 PC에 설치한 경우 상대적으로 해킹 확률이 다음과 같이 크게 낮아질 수 있다.

$$P_{on} \times P_{FTP} = 0.003$$

여기에 프로그램 버그에 의한 해킹 확률을 고려하면 확률은 지극히 낮아짐을 알 수 있다.

이러한 콘솔 제어형을 이용할 경우의 파일전송

작업시간은 파일서버가 생략되어 파일서버 부트시간과 송신측 컴퓨터의 조작시간이 없어지므로 식 (1)은 다음과 같이 나타낼 수 있다.

$$t_{tot,con} = (2 \cdot t_{mv} + t_{recv}) \times n \qquad (3)$$

2.2.2 원격 제어형

앞서 제시한 콘솔 제어형은 별도의 하드웨어 추가 없이 단지 소프트웨어의 설치만으로 파일서버가 생략되고 한번의 조작으로 파일을 전송할 수 있는 장점이 있지만, 작업용 PC와 서버용 컴퓨터 사이의 거리가 떨어져 있을 경우 서버의 콘솔 조작을 위해 이들 사이를 오가며 작업을 해야 하는 단점이 있다.

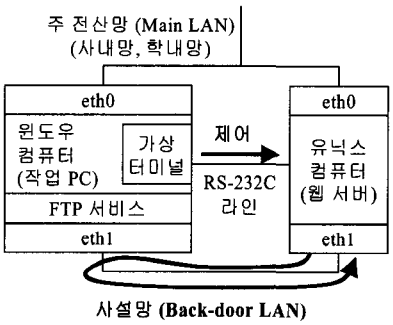

그림 6. 원격 제어형 데이터 전송 흐름도

따라서 그림 6과 같이 유닉스 컴퓨터의 직렬 통신단자와 작업용 PC를 RS-232C 케이블을 이용해 접속하고 작업용 PC에서 터미널 에뮬레이터 프로그램을 이용해 서버를 조작하면 두 컴퓨터 사이를 오가지 않으면서도 앞서 제시한 콘솔 제어형과 동일한 효과를 얻을 수 있다.

이와 같은 직렬통신에 의한 가상 터미널은 유닉스 컴퓨터의 부속 콘솔로 동작하므로 별도의 데몬 없이 유닉스 고유의 기능으로 가능하며, 직렬통신 라인은 점 대 점(point-to-point) 접속이므로 주 전산망이나 사설망과 무관해 시스템 보안에 영향을 주지 않는다. 이때 작업에 소요되는 시간은 오직 수신측 컴퓨터로 데이터를 전송하는 시간만이 존재하므로 식 (3)은 다음과 같이 나타낼 수 있다.

$$t_{tot,rem} = t_{recv} \times n \qquad (4)$$

Ⅲ. 실험 및 고찰

3.1 실험용 전산망의 구성

개선된 백도어형 사설망의 효과를 확인하기 위해

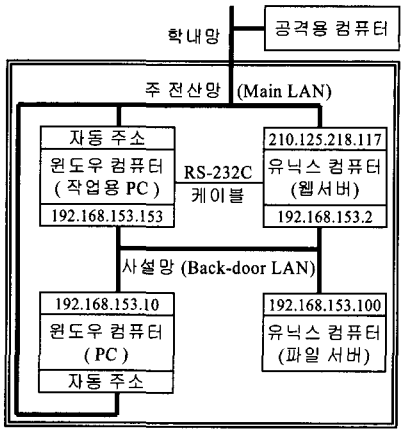

그림 7. 실험용 전산망의 구성

그림 7과 같은 실험용 전산망을 구성하였다.

그림에서, 주 전산망은 학내망에 접속되어 자동으로 할당된 주소로 이루어져 있고, 이 전산망에 공격에 사용할 컴퓨터를 접속했으며, 사설망은 사설 IP 주소인 192.168. 체계의 C-클래스 주소를 사용했다. 웹서버는 유닉스와 거의 동일한 환경을 가진 리눅스(Linux)를 사용하고 오로지 http 데몬만을 설치해 주 전산망에 웹 서비스를 행하도록 하였다. 작업용 PC에는 공개 소프트웨어인 DaFTP 프로그램을 이용해 FTP 서비스를 하도록 하였는데, 이 프로그램은 설치된 네트워크 인터페이스 장치 중 하나를 그림 8과 같이 선택하면 이 인터페이스 장치에만 서비스를 제공하고, 특히 이는 데몬 형식이 아니라 프로그램 형태로 되어 있으므로 필요할 때만 프로그램을 가동시켜 사용하기 때문에 앞서 고찰한 FTP 프로그램 조건을 충족한다.

작업용 PC의 가상 터미널은 그림 9와 같이 MS-윈도우에 내장된 하이퍼터미널 프로그램을 사용하였

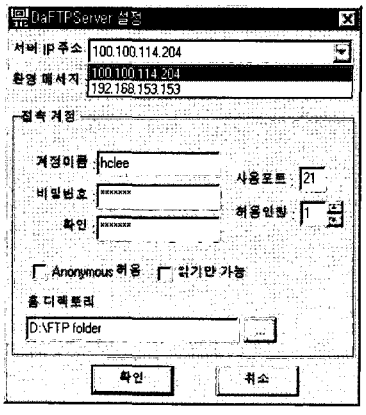

그림 8. FTP 프로그램의 설정

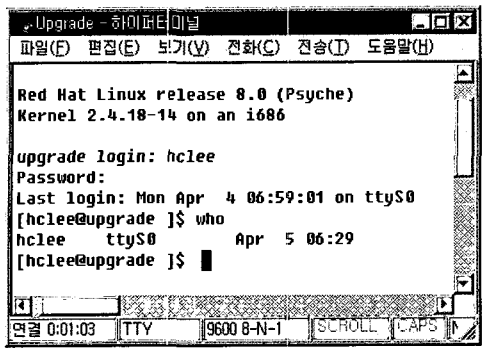

그림 9. 하이퍼터미널 구동 화면

는데, 'ttyS0' 즉, 서버의 부속 터미널로 설정되어 외부 전산망과는 무관함을 알 수 있다.

3.2 보안 효과와 시스템 정상동작의 확인

제시한 전산망의 보안효과를 확인하기 위해 공격용 컴퓨터에서 다음과 같은 종류의 공격을 시도하였다.

- 텔넷, FTP에 대한 계정 및 비밀번호 유추 공격
- 패킷 도청에 의한 통신내용 감지 및 계정, 비밀번호의 추적
- 윈도우 공유 디렉토리의 감지
- 포트 스캔에 의한 포트 감지 및 취약 포트 오버플로 공격
- IP 주소 둔갑에 의한 공격

본 논문에서 제시한 방법은 기존의 백도어형 사설망 특징을 그대로 가지고 있기 때문에 이상의 공격 종류들에 대해서는 동일한 보안효과를 나타내었다.[9]

이와 아울러 작업용 PC에 추가된 FTP 프로그램에 대한 보안을 확인하기 위해 FTP 프로그램이 작동되고 있는 상태에서 공격용 컴퓨터에서 접속을 시도해 본 결과, 작업용 PC는 오직 사설망에 접속된 네트워크 인터페이스 장치에만 반응하기 때문에 공격용 컴퓨터에서는 아무런 반응을 얻을 수 없었다.

주 전산망과 제시한 사설망이 함께 접속된 컴퓨터에서 오동작 가능성을 확인하기 위한 다음과 같은 기능 점검사항에서도 백도어형 사설망과 동일하게 정상적인 동작이 이루어짐을 확인하였다.

- 타 윈도우 시스템에 접속 가능 여부
- PC에서 웹 서비스의 정상 이용 가능 여부
- PC에서 인트라넷 서비스의 정상 이용 가능 여부
- 서버의 정상적인 웹 서비스 제공 여부

3.3 작업효율 증대효과의 측정

제시한 방법의 작업효율 증대효과를 확인하기 위해 임의의 10개 파일을 작업용 PC에서 수정하고 웹서버로 전송하는 작업을 5회 반복하는데 걸리는 시간을 각 전송형태 별로 측정하였다. 이때, 작업용 PC와 웹서버간의 거리는 약 7m이고, 문서 수정에 걸리는 시간은 측정 시간에서 제외시켜 순수하게 파일 전송에 소요되는 시간만을 측정하도록 하였으며, 그 결과를 표 1에 나타내었다.

표 1. 5회 반복 작업 시 측정 결과

(단위 : 초)

측정항목 \ 전송형태	파일 서버형	콘솔 제어형	원격 제어형
파일서버 부트	85		
파일서버 조작	125		
장소 이동	42.5	42.5	
웹서버 조작	135	135	135
장소 이동	42.5	42.5	
계	430	220	135

표 1에 나타난 결과를 살펴보면 앞서 식 (1), (3), (4)에 나타낸 바와 같이 각 전송형태별로 소요시간이 급격히 줄어듦을 알 수 있다.

이와 같은 측정결과를 기존의 파일서버형에 대한 비율로 나타내면 표 2와 같다.

표 2. 5회 반복 작업 시 시간 비율

비교항목 \ 전송형태	파일 서버형	콘솔 제어형	원격 제어형
소요 시간	430초	220초	135초
시간 비율	100%	51.2%	31.4%
효율 비	1	1.96	3.19

따라서 기존의 파일서버형에 비해 콘솔 제어형과 원격제어형에서 작업효율 비가 크게 향상됨을 알 수 있다. 표 1의 결과를 토대로 각 측정항목별 평균 소요시간을 계산하면 표 3과 같다.

표 3. 각 항목별 평균 소요시간

항목	평균 소요시간 [초]
파일서버 조작 (t_{sv})	25
장소 이동 (t_{mv})	8.5
웹서버 조작 (t_{web})	27

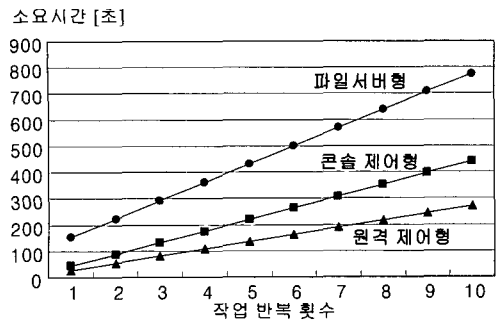

그림 10. 작업 반복횟수 별 소요시간 그래프

이들 값을 식 (1), (3), (4)에 대입하면 작업 반복 횟수 당 각 전송형태별 시간을 계산할 수 있으며, 그 결과를 그림 10에 나타내었다.

그림 10에 나타낸 바와 같이 반복 횟수가 늘어나면 소요 시간의 격차가 점차 커지는 것을 확인할 수 있다.

본 논문에서 제시한 개선된 백도어형 사설망은 기존의 방법과 동일한 보안효과를 나타내면서도 파일서버를 생략할 수 있어 이의 설치 및 운영부담이 없어짐은 물론, 사용 시마다의 부트시간을 생략할 수 있는 효과가 있다. 제시한 콘솔 제어형의 경우 기존의 방법에 비해 5회 반복작업에서 1.96배의 작업시간 단축 효과가 나타났으며, 파일 송신측과 수신측을 오가며 작업할 필요가 없는 원격 제어형의 경우 5회 반복작업에서 3.19배의 효과가 있음을 확인하였다.

Ⅳ. 결 론

본 논문에서는 백도어형 사설망의 문제점을 분석하고 그 개선 방안을 제시하였다. 제시한 개선된 백도어형 사설망을 적용한 경우 다음과 같은 이점이 있음을 실험을 통해 확인하였다.

첫째, 기존의 백도어형 사설망이 가지는 보안상 특징은 그대로 유지되면서 파일 전송에 필요한 비밀 파일서버를 설치할 필요가 없다.

둘째, 파일서버가 생략됨에 따라 파일서버의 부트시간을 기다리는 절차가 생략되어 작업시간이 더욱 단축될 수 있다.

셋째, 데이터 전송 시 파일 서버에 기인하는 두 번의 조작이 한번으로 가능해짐에 따라 작업시간의 단축과 작업 효율을 증대시킬 수 있고, 이로 인해 작업자의 피로도를 경감시킬 수 있다.

넷째, 콘솔 제어형은 특별한 하드웨어 추가 없이 단순한 소프트웨어의 설치만으로 가능하고, 5회 반복작업 시 파일서버에 의한 방법보다 약 2배 가량 효과적이다.

다섯째, 원격제어형은 간단한 RS-232C 케이블 하나만의 설치로 송신용 컴퓨터에서 모든 작업을 진행할 수 있어 5회 반복작업 시 콘솔 제어형에 비해 1.5배 이상, 파일서버에 의한 방법보다 3배 이상 효과적이다.

본 논문에서 제시한 개선된 백도어형 사설망은 이상에서 살펴본 바와 같은 많은 장점을 지니고 있고, 특히 저렴하면서 전문지식 없이 쉽게 설치, 운영할 수 있기 때문에 일반인에게 광범위하게 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Peterson, L. and B. Dacie, *Computer Networks: A Systems Approach*, Morgan Kaufmann Publishers, Inc., 1996.

[2] Cheswick, W. and S. Bellovin, *Firewalls and Internet Security: Repelling the Wiley Hacker*, Addison-Wesley, Reading, Messachusetts, 1994.

[3] 이철환, 한선관, "교육기관에서의 해킹 기법과 학내망 보안 방안에 관한 연구," *인천교육대학교 과학교육 연구소*, pp.247-278, 2001.

[4] 박정오, "학내전산망의 안전성 확보를 위한 보안진단 에이전트 개발," *컴퓨터교육학회논문지*, Vol.5 No.1, pp.22-34, 2002.

[5] Hickman, Kipp E. B., *The SSL Protocol*, Draft Memo of Netscape Communications, Feb. 1995.

[6] Braden, R. T., "A pseudo-machine for packet monitoring and statistics," *Proceedings of SIGCOMM '88*, Aug. 1988.

[7] Kaufman, C., R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, Prentice-Hall, Englewood Cliffs, New Jersey, 1995.

[8] 이용준, 김봉한, 박천용, 오창석, 이재광, "전산망 보호를 위한 혼합형 방화벽 시스템 구현," *정보처리학회논문지*, Vol.5 No.6, pp. 1593-1602, 1998.

[9] 이현창, 이종언, "백도어형 사설망 구축에 의

한 동일 공간범위의 전산망 보안에 관한 연구," 한국 통신학회 논문지, Vol.29 No.8T, pp.205-212, Aug. 2004.

[10] Narten, T., "Internet Routing," *Proceedings ACM SIGCOMM '89*, Sep. 1989.

[11] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets," *BCP 5, RFC 1918*, Feb. 1996.

이 현 창 (Hyun-Chang Lee) 정회원

1986년 2월 단국대학교 전자공학과 공학사

1989년 8월 단국대학교 전자공학과 공학석사

1996년 2월 단국대학교 전자공학과 공학박사

1996년 3월~2005년 2월 국립 천안공업대학 정보통신과 부교수

2005년 3월~현재 국립 공주대학교 공과대학 정보통신공학부 부교수

<관심분야> 멀티미디어 회로, 마이크로프로세서, 인터넷 응용

이 종 언 (Jong-Eon Lee) 정회원

1979년 2월 명지대학교 전기공학과 공학사

1981년 2월 한양대학교 전기공학과 공학석사

1998년 8월 단국대학교 전자공학과 공학박사

1981년 4월~2005년 2월 국립 천안공업대학 전기과 교수

1999년 3월~2003년 3월 국립 천안공업대학 학장

2001년 10월~2003년 3월 전국 국립 전문대학 협의회 회장

2003년 2월 서울대학교 행정대학원 국가정책과정 수료 (제55기)

2004년 1월~현재 한국 전력기술인 협회 충남지회장

2005년 3월~현재 국립 공주대학교 공과대학 전기전자공학부 교수

<관심분야> 전력·전자 제어, 마이크로프로세서