通信情報保護學會論文誌
第 10 券 第 2 號, 2000. 6

침입 차단 시스템을 위한 FTP 프록시 보안 모델의 구현

이 문 구*, 김 재 각*, 전 문 석**

Implementation of FTP Proxy Security Models for firewall Systems

Moon-Ku Lee*, Chae-Kak Kim*, Moon-Seog Jun*

요 약

인터넷의 급속한 발전으로 학교나 기업체 등의 네트워크가 인터넷을 통해 공유되면서 누구에게나 접속이 허용되어 많은 보안상의 문제가 발생하게 되었다. 이러한 문제점을 해결하기 위해서 기존의 호스트 기반 보안 정책에서 네트워크 기반의 보안 시스템으로 침입차단 시스템을 설치하지만, 침입차단 시스템은 보안을 위하여 최소 권한만을 인정하므로 사용자에게 투명한 서비스를 제공해 주지 못한다.

따라서 본 논문에서는 침입차단 시스템에 프록시를 두어서 서비스의 투명성을 제공하고, 강력한 보안 기능을 갖는 FTP 프록시 보안 모델(FTP-PSM : FTP Proxy Security Model)을 설계 및 구현을 하고, 원격 보안 탐색 도구인 SAINT를 이용하여 FTP-PSM의 안전에 대한 취약성 여부를 분석하고, 보안기능과 성능과의 관계를 응답시간 측정을 통해 측정함으로써 평가하였다. FTP-PSM은 강한 인증 기능을 위하여 일회용 패스워드 기능을 제공하고, 정당한 사용자에게 서비스 제공 여부를 결정하기 위해 강제적 접근제어와 임의적 접근제어 기능 그리고 FTP 명령어 사용 권한을 사용자 그룹별로 인증하는 기능을 제공하여 FTP 보안의 문제점을 해결한다.

ABSTRACT

The rapid growth of Internet requires proper methods to protect the privacy and integrity of the traffic. In order to solve these problems, the firewall systems can be installed between the internal network and external network. The firewall systems has the least privilege, so it does not provide transparency to the user. This problem of transparency can be solved by using the proxy. In this thesis, I have designed the FTP-PSM (FTP Proxy Security Model) which provides transparency for the firewall systems and has a strong security function. In this thesis, I have designed the FTP-PSM which provides transparency for the firewall systems, and we used SAINT(Security Administrator's Integrated Network Tool) to check if there is a vulnerability in the proposed FTP proxy and executed an efficiency evaluation for its secured. Our proposed FTP-PSM fundamentally blocks out hacking by providing a one-time password function for enhanced authentication. It also solves security problems by providing mandatory access control(MAC) and discretionary access control(DAC) functions in order to decide whether or not it will provide service to the user. Furthermore, it solves FTP security problems by providing functions of authenticating FTP commands permission by the user group.

keyword : *FTP-PSM, SAINT, One-time password, MAC, DAC*

* 김포대학 인터넷정보과
** 숭실대학교 정보과학대학

Ⅰ. 서 론

최근 인터넷에 대한 관심의 증대와 인터넷에 연결된 호스트의 숫자가 폭발적으로 증가함에 따라 사용자는 인터넷에 접속하여 다양한 형태의 정보 및 여러 종류의 통신 서비스 등을 쉽게 제공받고 있다. 반면에 인터넷망을 통해 불법 사용자 및 해커의 침입 등으로 정보의 손실, 파괴, 변조 등에 의한 피해가 늘고 있다.[2] 인터넷으로부터 이러한 피해를 막기 위하여 침입차단 시스템을 내부 망과 외부 망 사이에 설치하여 네트워크상의 한 지점에서 일괄적인 보안 정책을 적용시켜 관리함으로써 내부 망의 정보 자산에 대하여 보안 수준을 한 점에서 일괄적으로 높일 수 있다.[3] 그러나 침입차단 시스템은 게이트웨이(gateway)역할을 하므로 네트워크 인터페이스간의 투명한 서비스에 대하여 한계가 있다.[1]

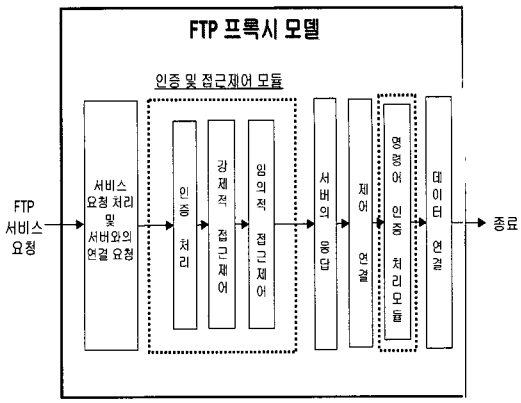
본 논문에서는 침입차단 시스템을 위하여 네트워크 인터페이스간의 투명한 서비스는 물론 보안기능이 강화된 FTP 프록시 보안 모델을 제안하였다. 논문의 구성은 다음과 같다. 2장에서는 제안한 FTP 프록시 보안 모델의 설계와 전반적인 흐름도를 기술하였고, 3장에서는 사용자 인증 기능의 구현내용을 기술한다. 그리고 4장에서는 임의적 및 강제적 접근제어 기능을 구현하고, 5장에서는 명령어 사용권한 인증 기능을 구현한다. 그리고 6장에서는 FTP 프록시 보안 모델을 구현한 시스템에 대하여 원격보안 탐색 도구인 SAINT(Security Administrator's Integrated Network Tool)를 이용하여 보안 기능에 대한 분석을 하였으며, 7장에서는 제안한 FTP 프록시 보안 모델에 대한 결론과 차후 연구방향 등을 기술한다.

Ⅱ. FTP-PSM(FTP-Proxy Security Model)의 설계

본 장에서는 보안 기능이 강화된 FTP 프록시 보안 모델 FTP-PSM (FTP Proxy Security Model)에서 제안하고자하는 보안기능을 설계하고 그 처리과정의 흐름도를 기술하였다.

2.1 FTP-PSM의 보안기능 설계

FTP 프록시 보안 모델 FTP-PSM (FTP Proxy Security Model)은 침입차단 시스템의 기능을 보다 효율적으로 하고 인터넷 보안 및 FTP의 보안 문제

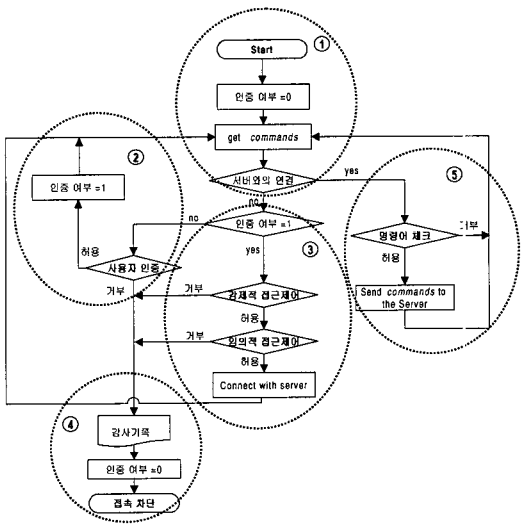


〔그림 1〕 제안한 FTP-PSM의 설계

를 해결하기 위하여 다음과 같은 기능들을 설계하여 제공한다 그림 1.

- 일회용 패스워드를 이용한 사용자 인증 기능
- 강제적 접근 제어 기능
- 임의적 접근 제어 기능
- 사용자 그룹별 명령어 사용권한 인증기능 FTP-PSM에서 보안 기능의 흐름도는 그림 2와 같으며 그 실행 과정은 다음과 같다.

① FTP 서비스 요청이 발생하면 처음에는 인증이 안되어 있으므로 인증 여부를 0으로 설정하고, 명령어를 입력받은 후 서버와 연결이 되었는지 확인한다.



〔그림 2〕 FTP-PSM의 설계를 위한 보안 기능 흐름도

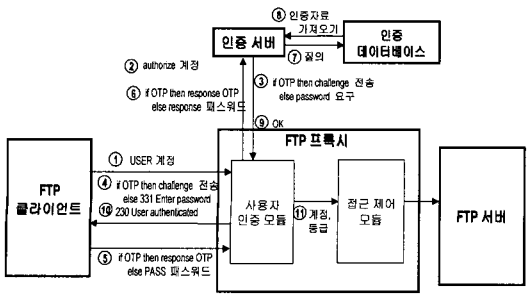
② 서버와 연결이 안되었으면 인증 여부가 1이 아니므로 사용자 인증 과정을 처리한 다음 인증 여부를 1로 설정하고 다시 명령어를 입력받는다.
③ 인증 여부가 1이면 즉, 인증을 거쳤으면 강제적 접근제어를 실행하고, 임의적 접근제어가 허용되면 서버와 연결이 된다.
④ 사용자 인증에서 거부되거나, 강제적 또는 임의적 접근제어가 실패했을 경우 감사기록을 남기고 인증 여부를 0으로 설정한 뒤 접속을 차단한다.
⑤ 접근 제어가 허용된 다음 서버와 연결이 되어있으므로 명령어를 체크하여 명령어 사용권한이 있는지를 확인하고, 명령어 사용권한이 확인되면 서버에게 바로 명령어를 실행하도록 보낸다. 만약, 명령어 사용에 대한 권한이 없으면 사용자에게 권한이 없음을 알리고 다음 명령어를 입력받는다.

Ⅲ. 사용자 인증 기능 구현

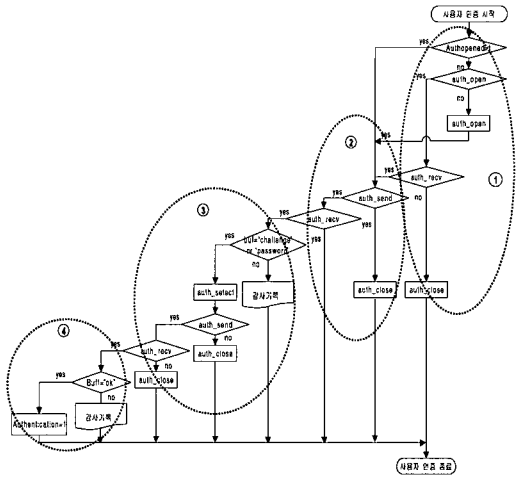
FTP-PSM의 인증 기능으로는 일반적인 UNIX 시스템에서 사용되는 평문으로 전송하는 패스워드방법뿐만 아니라 일회용 패스워드(One-time password) 두 가지 모두를 지원한다.

FTP-PSM에서 인증 서버를 통하여 사용자 ID 및 패스워드로 일반적인 패스워드 기능과 일회용 패스워드기능을 처리하기 위한 인증과정의 전체적인 처리과정은 그림 3과 같으며, 그 절차는 다음과 같다.

① FTP 클라이언트가 "user 계정"을 FTP 프록시에 전송한다.
② FTP 프록시의 사용자 인증 모듈에서는 인증 서버에게 계정을 인증하도록 요구한다.



〔그림 3〕 FTP-PSM의 인증처리 과정



〔그림 4〕 사용자 인증 기능 처리과정

③ 사용자의 계정이 등록되어 있어서 인증이 확인되면 클라이언트에게 일반적인 패스워드를 실행할 것인지 또는 일회용 패스워드를 실행할 것인지를 요구한다.
④ 사용자 인증 모듈에서는 FTP 클라이언트가 일회용 패스워드인 경우 챌린지값을 전송하고, 그렇지 않으면 응답 코드 "331번과 패스워드"를 입력하라는 메시지를 보낸다.
⑤ FTP 클라이언트는 일회용 패스워드를 사용하는 경우 자신의 패스워드로 계산된 결과 값 즉, 일회용 패스워드를 보내지만 그렇지 않은 경우는 pass 명령과 일반 패스워드를 입력한다.
⑥ 사용자 인증 모듈에서는 인증 서버에게 일회용 패스워드인 경우는 일회용 패스워드 응답을 전송하고 그렇지 않으면 패스워드를 인증 DB에 전송한다.
⑦ 인증 서버에서 일회용 패스워드 또는 패스워드에 관한 질의를 인증 데이터베이스에게 한다.
⑧ 인증 데이터 베이스로부터 패스워드를 확인한 자료를 인증 서버로 가져온다.
⑨ 인증 서버에서는 일회용 패스워드 또는 일반 패스워드에 대한 인증을 승인한다.
⑩ 사용자 인증 모듈에서는 응답 코드 230과 사용자가 프록시에게 인증되었음을 알린다.

이러한 사용자 인증기능 처리과정에서 사용자 ID 및 패스워드 확인은 인증 서버가 담당하게되며 사용자 인증과정을 통과하지 못할 경우 FTP-PSM은 클라이언트와의 연결을 종료하게 된다.

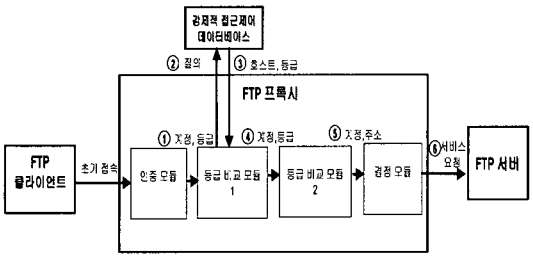
Ⅳ. 접근제어 기능 구현

4.1 강제적 접근제어기능

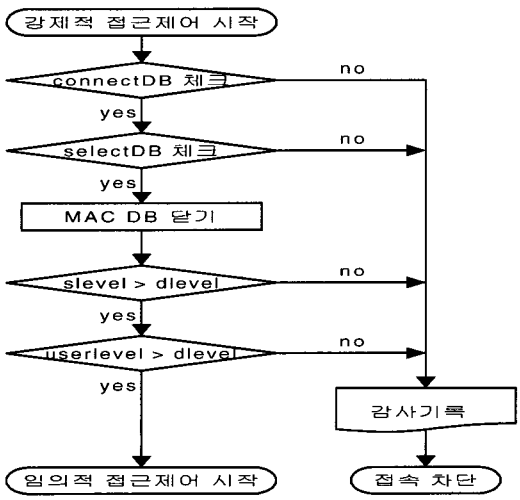
강제적 접근제어(MAC : Mandatory Access Control)는 주체 및 객체의 보안 등급에 근거하여 주체의 객체에 대한 접근을 제어하는 방법으로 주체 및 객체의 중요도에 따라 보안 등급을 설정하고, 주체가 객체에 접근 하고자 할 때, 주체 및 객체의 보안 등급에 따라 접근제어를 하고 있기 때문에 강제적 접근제어가 임의적 접근제어에 비해 세밀한 접근제어를 가능하게 해줌으로써 보안에 대한 높은 신뢰성을 제공한다.[13]

강제적 접근제어 처리를 위한 각 모듈의 내부적인 처리단계를 흐름은 그림 6과 같으며 그 과정은 다음과 같다.

- 강제적 접근제어 관련 DB에 연결한다.
- DB로부터 데이터를 읽어온다.
- DB를 닫는다.



〔그림 5〕 강제적 접근 제어 처리과정 설계



〔그림 6〕 강제적 접근제어 기능의 흐름도

- 근원지 호스트 등급과 목적지 호스트 등급을 비교한 후 근원지 호스트의 등급이 목적지 호스트의 등급보다 작을 경우 감사기록을 남기고 접속을 차단한다.
- 사용자 그룹 등급과 목적지 호스트 등급을 비교한 후 사용자 그룹 등급이 목적지 호스트 등급보다 작을 경우 감사 기록을 남기고 접속을 차단한다.
- 모두 통과하였을 경우 임의적 접근제어를 적용한다.

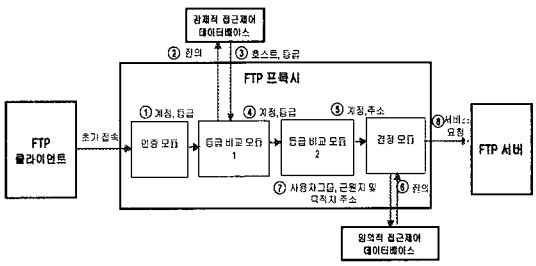
4.2 임의적 접근제어 기능

임의적 접근제어(DAC : Discretionary Access Control)는 주체의 신분에 근거한 보안 기능으로서, 주체에 대한 접근권한을 확인하여 객체에 대한 접근제어를 수행한다. 임의적 접근제어를 침입차단 시스템에 적용하기 위해서는 임의적 접근제어의 대상이 되는 주체 및 객체의 정의와 접근제어 규칙이 기술되어야 한다. 제안하는 FTP-PSM에서 주체는 FTP 서비스를 요청한 호스트가 속해 있는 네트워크 그룹이 되며, 객체는 침입차단 시스템을 통하여 접근을 요구받는 호스트가 속해 있는 네트워크 그룹이 된다. 임의적 접근제어 규칙의 경우 사용자 그룹별로 각각 규칙 적용이 이루어지며, 하나의 사용자 그룹이 복수개의 규칙을 가질 경우 우선 순위가 높은 규칙이 적용된다. 올바른 접근제어를 수행하기 위해서는 보안정책에 위배되지 않는 접근제어 규칙을 설계하는 것도 중요하지만, 먼저 주체 및 객체에 대한 신분확인이 올바르게 수행되어야 한다.[11]

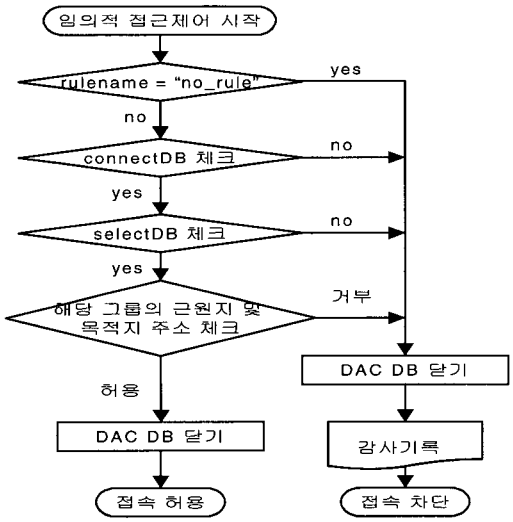
본 논문에서 제안한 FTP-PSM의 임의적 접근제어는 그림 7과 같으며 그 처리과정은 다음과 같다.

① 부터 ⑤까지 사용자의 인증과 강제적 접근제어 과정이 처리된다.

⑥ 사용자의 IP 주소에 근거하여 "결정 모듈"에서 임의적 접근제어 데이터베이스에게 사용자의 신분을 확인하기 위한 질의를 한다.



〔그림 7〕 임의적 접근제어 처리과정



〔그림 8〕 임의적 접근제어 흐름도

⑦ 임의적 데이터 베이스로부터 사용자 그룹, 근원지 및 목적지 주소를 가져온다.

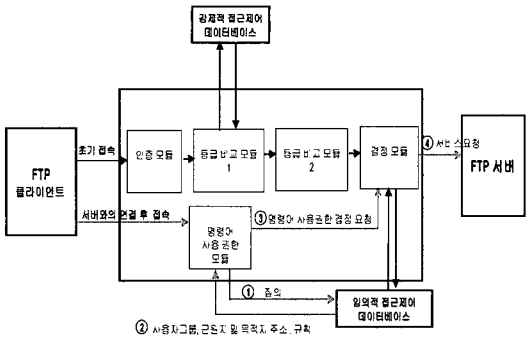
⑧ 사용자의 IP 주소에 근거하여 "결정 모듈"에서 사용자의 그룹, 근원지 주소, 목적지 주소가 등록이 된 사용자인지 확인하여 접근이 허용되면 FTP 서버에게 서비스 요청을 한다.

그리고 FTP-PSM에서 임의적 접근제어 처리의 설계를 위한 세부적인 흐름도는 그림 8과 같으며, 각 처리과정은 다음과 같다.

- 적용규칙이 no_rule이면 감사 기록을 남긴 후 접속을 차단한다.
- DB를 열고 해당 적용 규칙 rule 테이블과 연결한다.(일반적으로 ftp_rule이 적용)
- DB에서 데이터를 읽는다.
- 해당 그룹의 근원지 주소 및 목적지 주소에 대한 인증을 확인한다.
- 거부되면 DAC(Discretionary Access Control : 임의적 접근제어) DB에 감사기록을 남긴 후 접속을 차단한다.
- 허용되면 DAC DB를 닫고 접속을 허용한다.

V. 명령어 사용권한 인증 기능 구현

FTP-PSM은 보안 기능으로 사용자에 대한 인증 기능과 강제적 및 임의적 접근제어 기능을 제공한다. 그리고 서버와 연결된 후에 FTP-PSM에서는 사용자



〔그림 9〕 명령어 사용권한 인증 처리과정

그룹별로 FTP 명령어에 대한 사용권한을 제어한다. 따라서 초기 침입차단 시스템에 접속하고자 할 때 관리자에게 일부 FTP 명령어(예, CWD, REST, STOR, NLIST)에 대한 사용권한이 있는 사용자에 대해서만 실행이 가능하도록 하는 제어 기능이다. 이러한 사용자 그룹별 명령어 사용권한 제어 기능은 외부망의 사용자가 FTP 프록시를 통하여 내부 시스템의 익명의 FTP 프록시 서버에 접속하여 파일을 전송하려 할 경우 파일의 검색 및 읽고 쓰기를 금지하는 기능이며, FTP가 파일을 전송하기 위한 프로토콜인데 실제로 이러한 명령어사용에 대한 권한이 없다면 FTP를 사용할 수 없게되므로 FTP 보안의 문제점을 해결할 수 있게된다.

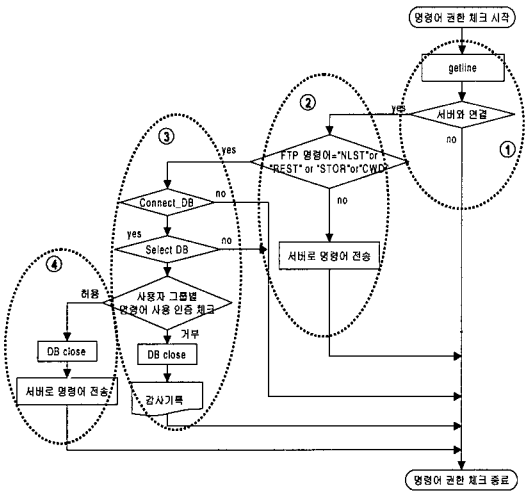
서버와의 연결 후 사용자 그룹별로 FTP 명령어 사용에 대한 권한이 있는지를 인증하는 처리과정을 그림 9에서 나타내었으며, 다음에서 그 세부적 처리과정을 기술하였다.

① 서버와의 연결이 있은 후 사용자 그룹별로 FTP 명령어 사용 권한을 인증하는 과정을 시작한다.

② FTP 클라이언트가 FTP 명령어인 CWD, REST, STOR, NLIST 등을 사용하려면 FTP 클라이언트는 이들 명령어에 대한 사용 권한이 있는지를 인증받기 위해서 임의적 데이터 베이스로부터 자료를 가져온다.

③ 이때 임의적 접근제어 데이터 베이스로부터 사용자 그룹별로 사용자 그룹, 근원지, 목적지 주소, ftp 규칙 등을 갖고 FTP 명령어 CWD, REST, STOR, NLIST의 사용 권한에 대한 인증을 "결정 모듈"에서 처리한다.

④ 처리가 완료되면 FTP 서버에게 이미 등록이 되어있는 사용자의 패스워드를 입력함으로써 서버와의 연결이 이루어진다.



〔그림 10〕 명령어 사용권한 제어 처리과정 흐름도

그리고 명령어 사용에 대한 권한을 제어하고자하는 기능을 제공하는 처리과정의 흐름도는 그림 10와 같으며 그 처리과정은 다음과 같다.

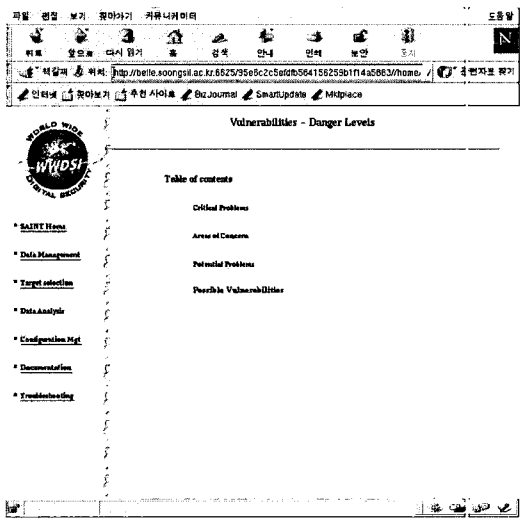
- 명령어를 받아들이고, 서버와 연결이 되어있는 상태인지 확인한다.
- 서버와 연결이 되어있는 상태이면 입력된 명령어가 "NLST", "REST", "STOR" 또는 "CWD"인지 확인한다. 만약, 4가지 명령어 중에 속하지 않는 명령어라면 서버로 명령어를 전송한다.
- 4가지 명령어 중 하나이면 해당 DB와 연결하고, DB로부터 명령어 사용권한을 갖은 사용자인지를 인증하기 위한 사용자의 ID와 주소를 가져온다.
- 해당 사용자 그룹별 명령어 사용 권한이 있는지를 확인하고, 명령어 사용 권한이 있으면 DB를 닫고 서버로 명령어를 전송한다.

Ⅳ. SAINT를 이용한 보안기능 분석

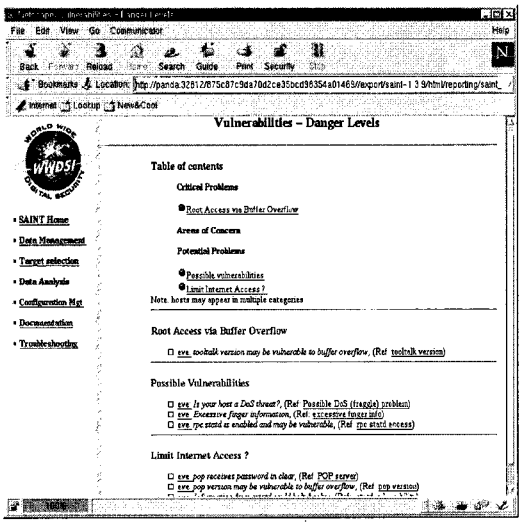
SAINT(Security Administrator's Integrated Network Tool)는 보안 관리자가 사용하는 네트워크 도구로써 원격 호스트나 네트워크에 대한 정보를 수집하고, 정보를 분석하여 결과를 보고서로 출력하는 원격 보안 탐색 도구이다. 원격 호스트나 네트워크에 대한 정보는 finger, NFS, NIS 등과 같은 네트워크 서비스를 이용하여 수집하고, 그 정보는 잠재적인 보안 취약점이나 다양한 네트워크 서비스들에 대한 내용을 나타내는데, 이러한 취약점들과 내용은 네트워크 서비스들이 잘못 설정되거나 구성된 경우 등을 나타낸다. SAINT는 이 정보들을 토대로 규칙 기반 시스템을 이용하여 잠재적인 보안 문제들을 분석한다. 침입차단 시스템을 위한 FTP 프록시의 취약성을 점검하기 위한 SAINT의 실행 환경은 다음과 같다:

1) 취약성 분석 도구
   - SAINT version 1.1.3
2) SAINT가 설치된 시스템
   - Panda (203.253.25.54)
3) 취약성을 점검할 호스트
   - 침입 차단 시스템에 제안한 FTP 프록시가 설치된 호스트 (Security)
     IP address : 203.253.25.52
     Host type : Sun OS 5
   - 침입 차단 시스템에 제안한 FTP 프록시가 설치되어있지 않은 일반 호스트 (eve)
     IP address : 203.253.25.1
     Host type : Sun OS 5

보안 기능이 강화된 FTP 프록시가 설치된 호스트를 SAINT를 이용하여 보안에 대한 취약한 부분을 탐색한 화면은 그림 11과 같으며, 취약점을 위험 레벨에 따라 나타내는데, 위험 레벨은 다음과 같이 세 개의 레벨로 나뉘어진다:



〔그림 11〕 TFTP-PSM 기반의 호스트에 대한 취약성 탐색 결과



〔그림 12〕 FTP-PSM이 없는 호스트의 취약점을 위험 레벨로 표현

- 치명적인 문제들(Critical Problems)
- 주의를 요하는 분야(Areas of Concern)
- 잠재적인 문제들(Potential Problems)

그리고 제안한 FTP프록시가 없는 일반 호스트를 SAINT를 이용하여 보안의 취약한 부분을 탐색한 결과는 그림 12와 같으며, 취약점들은 다음과 같이 나타난다:

1) 치명적인 문제점(Critical Problems)은 가장 취약성이 높아서 외부의 해커로부터 침입되기 쉬운 부분을 나타낸다. SAINT로 취약성을 분석하기 위하여 Solaris 2.5.1 이 설치된 일반적인 호스트에 별도의 보안 프로그램을 설치하지 않은 상태에 대하여 검사하여 본 결과 "root access via Buffer overflow"라는 취약성을 보였다. 이는 루트로의 접근에 대한 버퍼의 오버플로우 라는 약점을 이용해서 루트의 권한을 빼앗는 취약성을 나타낸다.
2) 주의를 요하는 분야(Areas of Concern)는 위험도는 비교적 덜하지만 염두에 두어야 할 부분을 나타내는데 이 부분에 대해 관련된 취약성이 나타나지 않았다.
3) 잠재적인 문제들(Potential Problems)과 관련된 취약성은 셋 중에서 가장 취약성의 정도는 약하지만, 침입될 가능성이 언제나 있는 잠재적인 부분들로써 SAINT로 취약성을 분석하기 위하여 Solaris 2.5.1이 설치된 일반적인 호스트에 별도의 보안 프로그램을 설치하지 않은 상태에 대하여 검사하여 본 결과 "excessive finger information" 이라는 취약성을 보였다. 이는 finger server로부터 나오는 finger 정보들이 너무 많을 경우 생기는 결과로서, 이러한 finger 정보들로부터 해커는 사용자들의 패스워드를 추측할 수 있게된다.

다음에 SAINT 화면에 보여지는 잠재적이 문제들로는 "rpc-statd access-rpc-statd"로 침입을 받을 수 있다는 취약성으로 rpc 서비스는 잘못하면 해커가 유용한 로컬 계정을 알지 못하더라도 원거리에서 침입하여 루트 권한을 얻을 수 있는 취약한 분야이다.

원격 로그인 서비스인 "rlogin"은 원격 사용자들로 하여금 패스워드가 없이도 login server에 로그온 하도록 한다. 이 취약성은 제 3의 사용자가 얼마든지 원하는 시스템에 억세스를 가능하게 됨으로서 취약성이 발생할 수 있다. 또한 서비스 부인 공격과 인터넷 억세스의 한계로 pop 서버의 오버플로우와 패스워드로 인한 취약점등을 나타낼 수 있다.

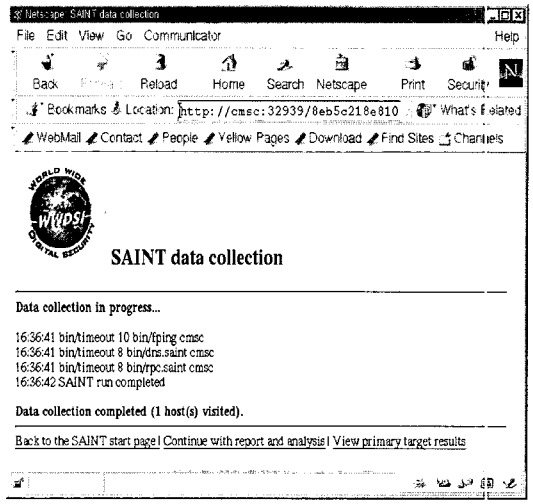
일반적인 호스트는 버퍼 오버플로우를 이용한 루트 접속이나 서비스 거부의 위협, finger 서비스를 남발한 공격, rpc. statd의 취약점, pop 서버의 취약점 등을 가지고 있지만, 본 논문에서 제안한 FTP-PSM 기반의 호스트는 강력한 인증 기능으로 가장 일반적이면서도 치명적인 패스워드 스니핑과 같은 위험요소에 절대적으로 안정적인 보안 기능을 갖는다. 그리고 강제적 접근제어 기능에서 주체와 객체의 등급에 따라 접근의 허용여부가 결정되므로 시스템을 무력화시키거나 서비스를 거부하는 등과 같은 플러딩(flooding) 공격으로 버퍼의 오버플로우가 발생하여도 루트접속이 전혀 이루어질 수 없으므로 완벽한 보안과 함께 서비스의 안정성을 갖게된다. 또한 FTP가 갖고 있는 보안의 문제점들은 FTP 명령어 사용권한에 대한 인증 기능으로 시스템 관리자가 인증하는 사용자만이 FTP 명령어를 사용할 수 있도록 함으로써 FTP의 홈 디렉토리를 수정하는 등의 해킹에 완벽하게 대응 할 수 있다. 그밖에도, 메일과 관련된 POP 서버의 패스워드 문제 또는 POP 서버의 오버플로우와 같이 잠재적으로 갖을 수 있는 취약한 문제점도 제안한 FTP-PSM을 기반으로 하는 FTP 프록시의 호스트에서는 보안성이 뛰어남을 보여 주었다. SAINT를 이용한 이상의 취약점 점검 결과는 표 1에 정리하였다.

이와 같이 더욱 강화된 보안 기능을 갖도록 설계된

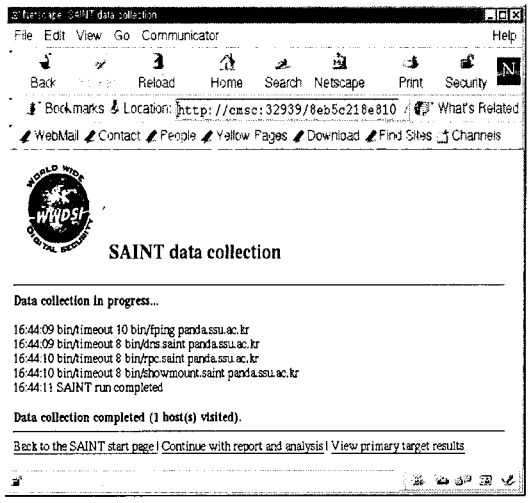
〔표 1〕 SAINT를 이용한 취약점 점검 결과

취약 항목 \ 호스트		일반적인 호스트	제안한 FTP-PSM 기반의 호스트
치명적인 문제점	- ping 공격 - password or IP sniffing - syn flooding	버퍼 오버 플로우를 이용한 루트접속 공격을 받을 수 있다.	버퍼 오버플로우 공격은 받을 수 있어도. 다양한 접근제어로 루트 접속으로 인한 공격은 불가능하다.
잠재적인 문제점	- 원격 접속 (rsh, rlogin) - ftp 관련 보안 위협 (writable ftp home dir, ftpd, FTP 취약점) - finger 초과 공격 - pop 서버의 패스워드문제 - pop 서버의 오버플로우	FTP의 문제와 서비스 거부의 위협 및 pop 서버와 관련된 잠재적인 취약점들을 갖고 있다.	FTP 명령어 사용을 위한 사용자 그룹별 인증 기능과 접근제어로 FTP 관련 보안 문제는 해결이 되며, 일회용 패스워드와 다양한 접근제어 기능으로 finger 초과 공격 및 pop 서버관련 취약점이 없었다.

FTP 프록시 보안모델은 그 설계상의 안정성이 검증되었으며, 실제 테스트 프로그램에서 각 보안 기능별로 안정성이 있음이 평가되었다. 그리고 SAINT 탐색도구의 결과 보안문제에서 취약한 부분이 나타나지 않았다. 그렇다면 이러한 보안 기능과 실제 성능과는 어떠한 연관 관계를 갖을 수 있을지 SAINT를 이용하여 성능을 평가하였다. 본 논문에서 제안한 FTP 프록시가 설치된 호스트와 그렇지 않은 호스트 각 각의 경우에 인증 및 접근제어 그리고 명령어 사용권한 인증 등과 같은 강력한 보안 기능을 실행하기 위하여 보안 기능이 강화되는 단계를 light, normal, heavy라는 3단계로 나누어서 시간을 측정하도록 탐색하였다. 보안 기능을 실행하기 위하여 자료를 수집한 시점에서, 보안 기능이 완료되는 시점까지 자료를 수집한 시간까지의 응답 시간(response time)을 측정하였다. 먼저 처음의 보안 단계로 인증 기능만을



〔그림 14〕 FTP-PSM 기반 호스트의 응답시간 결과(light)



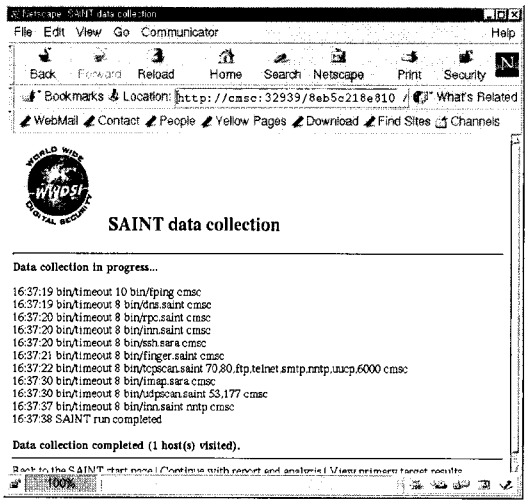
〔그림 13〕 FTP-PSM 기반이 아닌 호스트의 응답시간 결과(light)

〔그림 15〕 FTP-PSM 기반이 아닌 호스트의 응답시간 결과(normal)

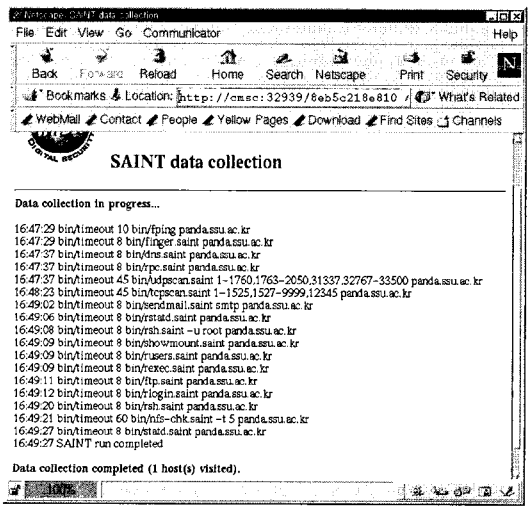
실행하기까지의 단계인 light 단계의 자료 수집과 그 결과에 대한 응답이 있기까지의 시간을 측정한 결과는 그림 13 및 그림 14와 같다.

이번에는 접근제어 기능이 처리되는 normal 단계 과정의 자료 수집과 그 결과에 대한 응답이 있기까지 시간 측정결과는 그림 15 및 그림 16와 같다.

마지막으로 보다 강화된 보안 기능의 단계인 heavy 과정은 FTP 명령어 사용권한 인증 과정이 실행되는 경우의 자료 수집과 그 결과에 대한 응답이 있기까지 시간 측정을 탐색한 화면은 그림 17 및 그림 18과 같다.



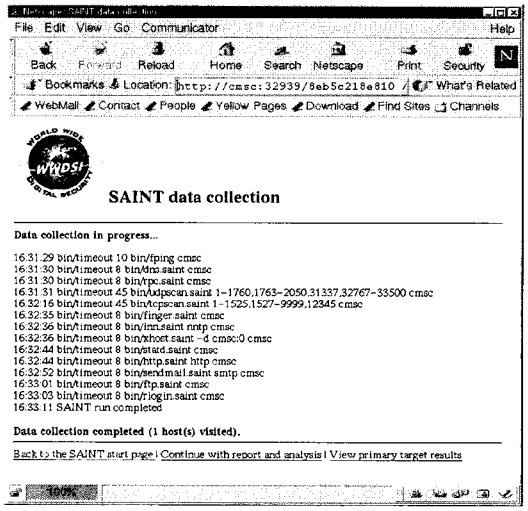
〔그림 16〕 FTP-PSM 기반 호스트의 응답시간 결과(normal)



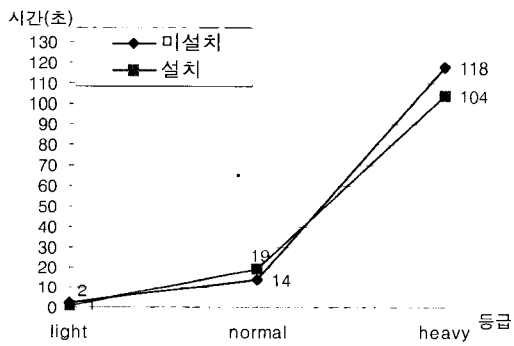
〔그림 17〕 FTP-PSM 기반이 아닌 호스트의 응답시간 결과(heavy)

SAINT를 이용하여 보안 기능의 실행 정도에 따라 사용자 인증기능 실행 단계는 light, 접근제어 실행 단계는 normal 그리고 사용자 명령어 사용 인증을 제어하는 heavy의 3단계로 나누어서 각 호스트의 보안 기능 실행 시작 시점에서 결과를 보여주는 시점까지의 자료를 수집하면서 소요되는 응답시간을 측정하였다.

제어가 실행되는 단계인 normal 경우는 FTP 프록시가 설치된 경우는 14초이고, FTP 프록시가 설치되지 않은 경우의 응답 시간은 19초의 결과를 보여주었다. 이러한 결과는 인증 기능과 임의적 접근응답 시간 결과는 그림 19과 같이 FTP 프록시가 설치된 호스트의 경우와 그렇지 않은 호스트의 자료 수집 결과 응답시간은 FTP 프록시가 설치된 경우는 처음 인증기능이 실행되는 light 단계의 경우 오히려 시간이



〔그림 18〕 FTP-PSM 기반 호스트의 응답시간 결과(heavy)



〔그림 19〕 응답시간 결과

1초이고, FTP 프록시가 설치되지 않은 호스트의 경우 자료를 수집하여 결과를 보여주기까지의 응답 시간이 2초가 소요되었다. 반면에 접근제어 기능뿐만 아니라 강제적 접근제어 기능까지 실행이 되었으므로 자료 수집시간이 5초가 더 소요되었다. 그러나 명령어 사용 인증 기능과 같은 보다 강화된 보안 기능이 실행되는 경우는 자료를 수집하여 결과를 보여주기까지의 응답 시간이 FTP 프록시가 설치된 경우는 104초이고, FTP 프록시가 설치되지 않은 경우의 응답시간은 오히려 118초가 소요되었다. 일반적으로 보안 기능이 강화되면 반면에 그 성능 면에서는 미약한 경우가 많지만, 본 논문에서 제안하는 FTP 프록시 보안모델은 보안성이 뛰어나면서 성능 면에서도 미약한 부분이 극히 적음을 알 수 있다.

Ⅶ. 결 론

이와 같이 더욱 강화된 보안 기능을 갖도록 설계된 FTP 프록시 보안모델은 그 설계상의 안정성이 검증되었으며, 실제 테스트 프로그램에서 각 보안 기능별로 안정성이 있음이 평가되었다. 그리고 SAINT 탐색 도구의 결과 보안문제에서 취약한 부분이 나타나지 않았다. 그렇다면 이러한 보안 기능과 실제 성능과는 어떠한 연관 관계를 갖을 수 있을지 SAINT를 이용하여 성능을 평가하였다. 본 논문에서 제안한 FTP 프록시가 설치된 호스트와 그렇지 않은 호스트 각 각의 경우에 인증 및 접근제어 그리고 명령어 사용권한 인증 등과 같은 강력한 보안 기능을 실행하기 위하여 보안 기능이 강화되는 단계를 light, normal, heavy라는 3단계로 나누어서 시간을 측정하도록 탐색하였다. 보안 기능을 실행하기 위하여 자료를 수집한 시점에서, 보안 기능이 완료되는 시점까지 자료를 수집한 시간까지의 응답 시간(response time)을 측정하였다. 먼저 처음의 보안 단계로 인증 기능만을 실행하기까지의 단계인 light 단계의 자료 수집과 그 결과에 대한 응답이 있기까지의 시간을 측정한 결과는 그림 13 및 그림 14와 같다. 인터넷 사용이 급성장하고 많은 학교나 기업체 등의 네트워크가 인터넷을 통해 공유되면서 누구에게나 접속이 허용되어 많은 보안상의 문제가 발생하게 되었다. 이러한 문제들을 해결하기 위해 보안 기능이 강화된 FTP 프록시가 필요하다. 프록시는 정당한 사용자만이 정당한 서비스를 받을 수 있게 하기 위하여 인증 기능을 제공한다. 인터넷을 통해 간단한 인증 기능이 수행될 때 사용자의 ID와 패스워드는 인터넷상에서 암호화되지 않은 체로 전송되기 때문에 인터넷상의 패킷을 가로채는 프로그램을 이용할 경우에는 사용자의 ID와 패스워드가 공개될 수 있다. 이러한 문제를 해결하기 위해 사용하는 일회용 패스워드는 매번 인증할 때마다 사용하는 패스워드가 다르기 때문에 패스워드가 공개되어도 시스템을 보호할 수 있다.

침입차단 시스템이 내부망을 보호하기 위하여 내부망과 외부망을 무조건 차단한다면 내부망과 외부망간의 융통성 있는 서비스가 제공되지 않는다. 또한 접근이 허가된 사용자인지를 정확하게 제어하여야만 한다. 이러한 접근제어 기능은 불법 사용자가 도중에 정보를 가로채어 정보의 비밀성을 침해하는 행위, 불법으로 접근하여 데이터를 변경하여 데이터의 무결성 손상, 혹은 허가되지 않은 주체가 시스템에 거짓 정보를 삽입하는 등의 보안 위협으로부터 공격을 받을 수 있다. 그러므로 본 논문에서 제안하는 FTP 프록시 보안 모델에서는 이처럼 내부망과 외부망 사이의 원활한 서비스 제공을 위한 투명성을 제공하면서 접근제어를 위하여 임의적 접근제어와 강제적 접근제어 기능 등을 제공하도록 하였다. 임의적 접근제어 기능은 사용자의 IP 주소에 따라 접속을 허용하거나 거부하는 방법으로 주체 및 객체의 신분에 따라 그 접근제어가 이루어진다. 그러나 임의적 접근제어 기능은 IP 주소에 따라 서비스를 허용하거나 제한하기 때문에 특정 사이트의 사용자 등급에 따라 서비스를 허용하거나 제한할 수 없다. 이러한 한계를 해결하기 위해 사용자의 등급과 접속하고자 하는 객체에 따라 서비스를 허용하거나 제한하는 강제적 접근제어 기능이 필요하다.

이렇게 접근이 허가된 사용자에 대해서도 FTP 명령어 사용에 대한 권한을 관리자로부터 부여받지 않은 사용자를 확인하는 인증 과정을 갖는다. 또한 접근이 이루어진 후에 사용자의 활동 상황을 감시하고, 활동상황 등 여러 가지 내부통제 및 감시를 위한 로그기록 과정이 필요하다.

본 논문에서 제안하는 FTP 프록시 보안 모델(FTP-PSM)을 구현한 시스템을 원격 보안 탐색 도구인 SAINT를 이용하여 성능을 테스트한 결과 보안성이 우수하면서 성능도 우수함을 알 수 있었으므로 차후 다른 서비스를 위한 프록시의 기본 모델이 될 수 있다.

참 고 문 헌

[1] Bill Cheswick and Steve Bellovin, *"Firewalls and Internet Security: Repelling the Wily Hacker"*, Addison Wesley Edition, 1994.

[2] Charlie Kaufman, Radia Perlman, Mikes Speciner, *"Network Security"*, PTR Prentice Hall, 1995.

[3] David Curry, *"Unix System Security-A Guide for Users and System Administrators"* Addision Wesley. 1992.

[4] D. Brent Chapman, Elizabeth D. Zwicky, *"Building Internet Firewalls"*, O'Reilly & Associates, Inc., Printed in the United States of America, 1995.

[5] Douglas Comer and David Stevens, *"Internetworking with TCP/IP Vols I, II and III"*, Prentice-Hall. 1991.

[6] Derek Atkins, etc., *"Internet Security Professional Reference"*, New Riders Publishing, Inc., Printed in the United States of America, pp. 535~614.1996.

[7] Frederick M. Avolio, *"A Network Perimeter with Secure External Access"*, Trusted Information Systems, 1994.

[8] Karanjit Siyank & Chris Hare, *"Internet Firewalls and Network Security"*, New Riders Publishing, 1995.

[9] Marcus J. Ranum, *"Thinking About Firewalls"*, proceedings of the Second World Conference on Systems Management and Security, 1993 Available for FTP from ftp.tis.com:/pub /firewalls/firewall.ps.Z

[10] William Stallings, *"Internet Security Handbook"*, IDG Books Worldwide, Inc., 1996.

[11] Vijay Ahuja, *"Network & Internet Security"*, Academy Press Inc., Printed in the United States of America, 64_71. pp.64-71. 1996.

[12] W. Richard Stevens, *"TCP/IP Illustrated Volume 1 : The protocol"* Addition-wesley, Professional Computing series, October 1995.

[13] 김재성, "침입차단시스템을 위한 강제적 접근제어 기법 설계," 한국정보보호센터, 1998.

[14] 임채호 외, '99 해킹 바이러스 형황 및 대응, 한극 정보 보호센터, 1999.

[15] 전문석, "인터넷 보안", 한국정보문화센터 부설 정보기술 교육원, 1998.

〈著者紹介〉

이 문 구 (Moon-Ku Lee) 정회원
1984년 : 숭실대학교 전자계산학과(학사)
1993년 : 이화여자대학교 교육대학원 전산학과(석사)
2000년 : 숭실대학교 대학원 전산과(공학 박사)
1997년~1999년 명지 전문대학 전산과 겸임교수
2000년3월~현재 김포대학 컴퓨터계열 전임강사
관심분야 : 정보통신, 네트웍 프로그램, 암호 이론, 인터넷 보안, 침입차단 시스템, 전자 상거래

김 재 각 (Chae-Kak Kim)
1981년 : 숭실대학교 전자계산학과(학사)
1985년 : 연세대학교 산업대학원 전산전공(석사)
1998년~ 숭실대학교 대학원 전산과 박사과정
1985년~1994년 LG전자, 삼보컴퓨터 근무
1996년~현재 김포대학 컴퓨터계열 조교수
관심분야 : 암호학, 네트워크 보안, 통신 프로토콜 전자 상거래 보안

전 문 석 (moon-Seog Jun) 정회원
1981년 : 숭실대학교 전자계산학과 (학사)
1986년 : University of Maryland, Computer Science(석사)
1988년 : University of Maryland, Computer Science(박사)
1989년 : Morgan State Univ. 부설 Physical Sccience Lab. 책임 연구원
1991년~현재 숭실대학교 컴퓨터학부 부교수
관심분야 : 병렬처리 시스템, 암호학 알고리즘, 인터넷 보안, 침입 차단 보안 시스템, 정보이론, 전자 상거래 보안