情報保護學會論文誌
第13券 第3號, 2003. 6

PKI를 기반으로 한 실시간 무선 원격제어 시스템의 구현

이 문 구

Implementation of Real-time Wireless Remote Control System Based on Public Key Infrastructure

Moon-ku Lee

요 약

기존 웹 기반인 시스템 관리 소프트웨어 솔루션들은 시간적, 공간적 제약을 갖는다. 그리고 오류 메시지에 대한 불확실한 통보와 실시간 지원요구 및 긴급조치가 어렵다는 문제점들을 갖는다. 이러한 문제들을 해결하기 위해서 모바일 통신기기를 이용하여 원격시스템을 관리 및 모니터링하고 즉각적으로 원격지의 시스템을 제어할 수 있는 무선 원격제어 시스템(W-RCS)을 설계 및 구현하였다. 구현된 무선 원격제어 시스템은 이러한 문제의 해결뿐만 아니라 보안의 문제도 갖고 있다. 그러므로 본 논문에서는, 무선 원격제어 시스템을 위한 보안 문제에 초점을 맞추어 진행하였으며, 공개키 인증 기반구조를 기본으로 하는 W-RCS의 보안기능은 사용자에 대한 모바일장비 사용자 인증과 대상 시스템 접근제어 기능을 갖는다. W-RCS는 실시간 사용자 인증 기능을 실행하도록 하여 자원관리자와 모바일 단말기 사용자의 유연성을 높이고, 중단 없는 서비스의 제공뿐만 아니라 안전한 모바일 오피스 환경을 제공한다.

ABSTRACT

Existing web-based system management software solutions show some limitations in time and space. Moreover, they possess such as shortcomings unreliable error message announcements and difficulties with real-time assistance supports and emergency measures. In order to solve these deficiencies, Wireless Remote Control System(W-RCS) was designed and implemented. W-RCS is able to manage and monitor remote systems by using mobile communication devices for instantaneous control. The implementation of W-RCS leads to these security problems as well as solutions to aforementioned issues with existing web-based system management software solutions. Therefore, this paper has focused on the security matters related to W-RCS. The security functions based on public key infrastructure include mobile device user authentication and target system access control. The W-RCS allows real-time user authentication, increases the flexibility of resource administrators and mobile device users, and provides not only uninterrupted services, but also safe mobile office environments.

Keyword : public key infrastructure, real-time user authentication, target system access control

Ⅰ. 서 론

기존의 웹 기반인 유선 시스템 관리 소프트웨어 솔루션들은 시간적, 공간적 제약과 오류사항에 대한 통보가 불확실하거나 신속한 지원요구 및 실시간 긴급조치가 어렵다는 문제점들을 갖는다. 따라서 본 논

* 본 연구는 2003학년도 김포대학의 연구비 지원에 의하여 연구되었습니다.
* 김포대학 컴퓨터계열 조교수(yeon0330@kimpo.ac.kr)

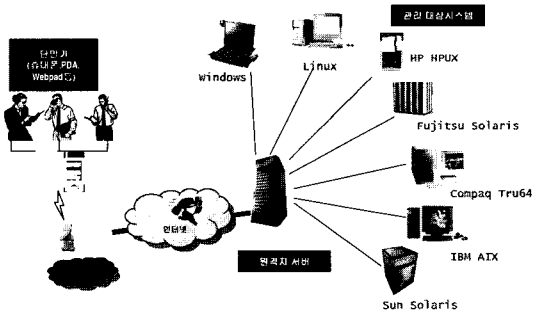
문에서는 모바일 통신기기(휴대폰, PDA, Smart Phone, Webpad 등)를 이용하여 원격시스템을 관리 및 모니터링하고 즉각적으로 원격의 시스템을 제어할 수 있는 무선 원격제어 시스템을 제안한다. 그러나 날로 급증하는 정보화의 역기능 현상으로 나타나는 각종 정보의 해킹 및 크래킹 등으로부터 안전한 정보의 전송에 관한 중요성이 더욱 강조되고 있다. 따라서 본 논문에서는 기존의 유선 시스템 관리 솔루션들의 문제점을 해결할 수 있을 뿐만 아니라 보안기능이 강화된 무선 원격제어 시스템(W-RCS : Wireless-Remote Control System)을 설계 및 구현하였다. W-RCS의 보안 기능은 모바일 장비 사용자의 인증과정, 인증된 사용자라도 대상서버를 제어하려면 대상서버의 제어권한을 부여받기 위한 시스템 접근권한 및 명령어 사용권한을 위한 제어기능을 갖는다. 이렇게 시스템에 접근제어 권한을 부여받은 사용자라도, 공인된 인증기관으로부터 인증된 사용자임을 확인하기 위한 PKI 기반의 인증과정을 실행하도록 한다. 이상의 인증 및 보안 기능은 기존의 무선 원격제어 시스템과는 차별화된 기능으로, 사용자에게 신뢰성과 안정성을 제공해 줄 뿐만 아니라, 중단 없는 서비스의 제공과 함께 안전한 모바일 원격제어 시스템 환경이 가능하도록 할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 무선 원격제어 시스템의 구조를 설명하고 3장에서는 원격제어 서버의 구조와 모듈별 주요 기능들을 기술한다. 그리고 4장에서는 PKI를 기반으로 한 실시간 무선원격제어 시스템(W-RCS)의 보안기능에 대하여 기술하였다. 그리고 5장에서는 구현된 시스템의 성능평가를 하였고, 마지막으로 6장에서는 결론과 차후 연구방향 등을 기술한다.

II. 제안하는 무선 원격제어 시스템의 구조

1. 시스템의 전체 구성 요소

웹 기반의 유선 시스템관리 소프트웨어 솔루션들은 시스템에 문제가 발생할 때 실시간으로 문제 발생의 원인을 파악 및 해결하는데 있어서 시간적, 공간적 제약을 갖는다. 그리고 이메일이나 콘솔의 경보(alarm) 기능 등은 담당자가 자리를 비우거나 미 확인시에는 장애 통보가 불확실하다는 것이다. 또한, 지원요구 발생시 유선통화 요청 및 방문지원까지 적지 않은 시간지연 및 원격지원이 불가능하다. 이러한 문제들을 해결하고자 모바일 단말기(휴대폰, PDA, Smart Phone, Webpad)로 이동 중에도 원격의 시스템을 실시간으로 모니터링 할 뿐만 아니라 문제가 발생되면 즉각 모바일 단말기로 장애통보를 해주며 원격의 시스템에 바로 접근해서 문제를 해결 할 수 있는 무선 원격제어 시스템(W-RCS)을 제안한다. [그림 1]은 시스템의 전체 구성도를 도식화 한 것으로 W-RCS는 크게 원격지 제어서버와 관리대상 시스템 그리고 모바일 장비로 구성된다.



〔그림 1〕 시스템의 전체 구성도

III. 원격지 제어서버의 구조와 주요기능

1. 제어서버의 구조와 기능

원격지 제어서버는 크게 웹 서버(Web server), 코어 엔진(Core Engine) 그리고 응용 프로토콜 인터페이스(Application Protocol Interface) 모듈로 구성된다. [그림 2]는 모바일 장비로 실시간에 대상 시스템을 원격제어 하기 위한 구조의 동작과정을 모듈로 도식화 한 것이다.

1) 모바일 웹 서버(Web server)는 모바일 단말기 상에서 원격지 시스템의 모니터링 결과와 실행명령에 대한 출력결과를 모바일 단말기의 기종에 적절한 형태로 출력해 주는 기능을 제공하기 위하여 표현 모듈(Presentation Module)을 탑재한다.

2) 코어 엔진(Core Engine)은 다음의 모듈들로 구성된다.

- 통보 관리(Notification Manager) 모듈은 원격지 시스템의 오류상태 발생시 관리자 또는 지정된 사용자에게 이메일 또는 단문메시지 형태로 통보하는 기능을 제공한다.

- 세션 관리자(Session Manager) 모듈은 모바일 단말기를 통하여 접속한 사용자의 세션 관리 기능을 제공한다[7],[8].

- 이벤트 관리자(Event Manager)모듈은 원격지 시스템에서 발생한 각종 이벤트를 분석하여 데이터베이스에 기록과 동시에 통보여부를 판단하여 통보 관리자(Notification Manager)에게 전달하는 기능을 제공한다.

- 기록 관리자(History Manager)모듈은 모바일 단말기를 통하여 원격지 시스템에 제어기능 수행 시이에 대한 각종 기록(Log File) 정보를 관리하는 기능을 제공한다.

- 에이전트 관리자(Agent Manager) 모듈은 제어서버를 통하여 관리대상이 되는 원격지 시스템 에이전트들의 상태 등을 체크하는 기능을 제공한다.

- 마크업 언어 변환기(Markup Language Converter) 모듈은 접속한 모바일 단말기의 종류를 자동 판별하여 해당단말기에서 수용 가능한 마크업 언어(mHTML, WML, HDML 등)으로 자동 변환하여 주는 기능을 제공한다.

- 환경구성 관리자(Configuration Manager) 모듈은 사용자 등록, 원격지 시스템 정보 등록, 모니터링 항목의 임계값 설정 등 각종 구성 정보를 등록 관리하는 기능을 제공한다.

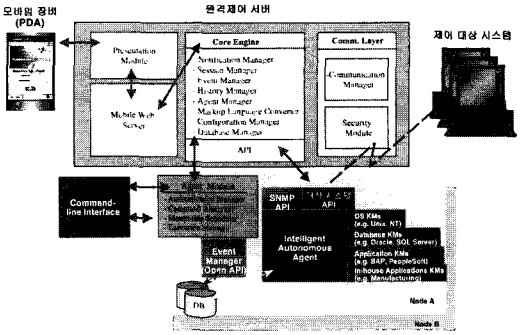
- 데이터베이스 관리자(Database Manager) 모듈은 제어서버에서 사용하는 원격 데이터베이스 관리 시스템에 접속하여, 각종 SQL 질의(Query)를 담당하는 기능을 제공한다.

- 통신 관리자(Communication Manager) 모듈은 원격지 제어서버와 대상 시스템간의 통신 기능을 담당하며, 원격지 서버로부터 전송된 에이전트와 대상 시스템간의 통신에서 SSL(Secure Socket Layer)방식으로 통신이 이루어진다[7][8].

- 보안 모듈(Security Module)은 단말기와 제어서버 그리고 원격지 서버 에이전트와 대상 시스템간의 통신에서 인증 및 접근제어 등 보안 기능을 제공 및 관리한다[1].

3) 응용 프로토콜 인터페이스(Application Protocol Interface) 모듈은 다른 유선상의 시스템 관리 소프트웨어 솔루션들과의 연동을 위한 인터페이스 기능을 제공한다. API 모듈은 원격지 제어 대상 서버와의 연동을 위하여 주로 대상 에이전트에서 현재 모니터링하고 있는 항목들에 대한 다양한 상태를 추출하는데 사용되는 모듈이다. API 모듈은 원격지 제어서버 에이전트가 아닌 대상 시스템의 에이전트와 직접 통신을 하도록 구성되어 있다.

원격지 제어서버와 대상 시스템간의 통신은 에이전트에 의해서 자원의 모니터링, 관리 그리고 제어명령이 전달된다[6]. 이러한 에이전트엔진은 인증관리자 모듈(Authentication Manager), 명령 분석자(Command Analyzer) 모듈, 모니터링 스케쥴러(Monitoring Scheduler) 모듈, 그리고 실행 관리자 모듈(Execution Manager)로 구성된다.



〔그림 2〕 제어대상 시스템을 위한 원격 제어 서버의 구조

인증 관리자 모듈은 모바일 단말기를 통하여 원격지 서버에 접근하여 제어 및 관리기능을 수행하기 위해서 해당 시스템의 인증절차를 받도록 하는 기능을 제공하며, 인증이 성공하면 로그인한 사용자의 권한에 따라서 시스템 제어기능의 권한이 주어진다[13].

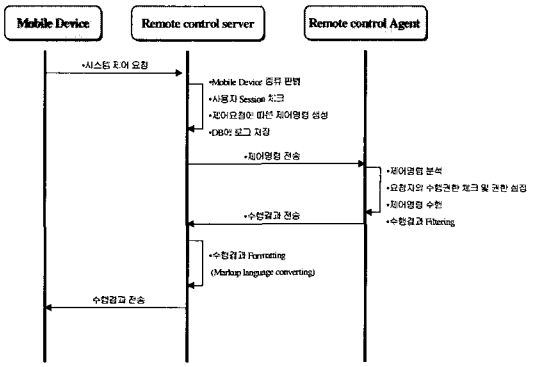
명령 분석자 모듈은 사용자가 수행을 요청한 명령(Command)을 분석하여 해당시스템에 적절한 형태의 명령으로 변환하는 기능을 제공한다. 모니터링 스케쥴러 모듈은 모니터링 하고자하는 항목을 설정한 구성환경에 의해 주기적으로 모니터링 하며, 모니터링 된 데이터를 수집한다. 또한 설정된 임계값을 초과했을 때 제어 서버쪽으로 이벤트정보를 생성하여 전송하는 기능을 제공한다[4],[5]. 실행 관리자 모듈은 명령 분석자에게서 분석된 명령어를 수행하며, 이의 결과를 출력 또는 포메팅 하는 기능을 제공한다.

통합 인터페이스(Integrated Interface) 모듈은 역시 다른 유선상의 시스템 관리자들과의 연동과 사용자 요청에 대한 인터페이스 모듈을 제공한다[10].

2. W-RCS의 동작 과정

모바일 장비와 원격지 제어 서버 그리고 에이전트

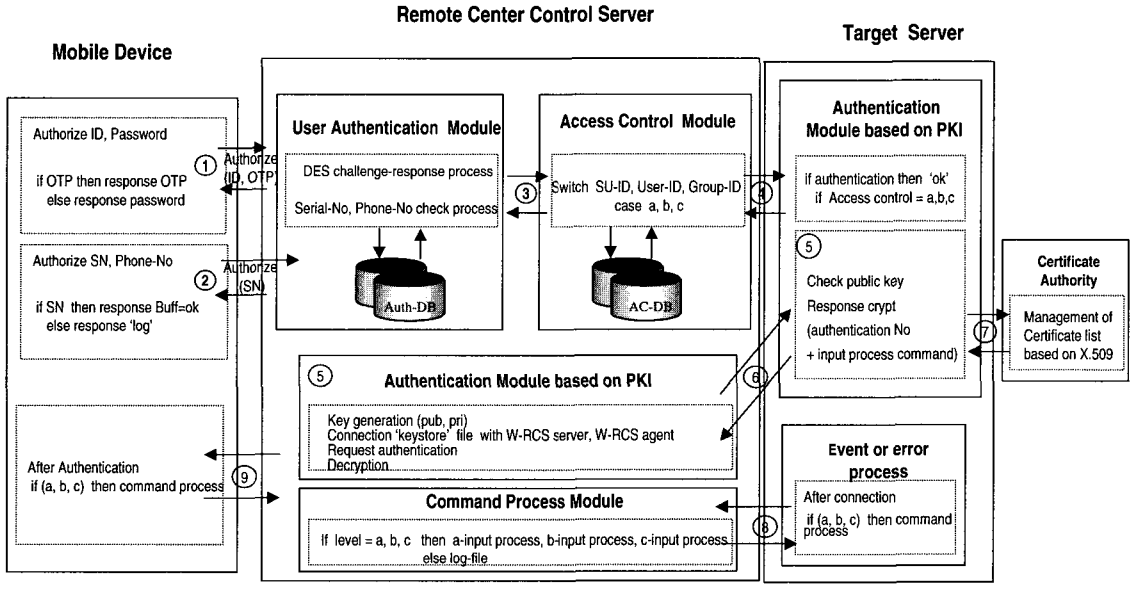
가 상호 동작하는 과정은 [그림 3]과 같다. 원격지 제어서버의 웹 서버는 JSP 엔진기능이 제공되며, 모바일 장비의 종류를 판별하고, 모바일 장비로부터 시스템 제어요청(request)을 받아서 원격지 제어서버의 엔진으로 처리를 넘기고, 그 결과를 응답(response)하는 부분을 담당한다[5],[6]. 이때, 모바일 장비의 종류를 판별하고, 사용자의 세션을 체크한 후 제어 요청에 따른 제어 명령을 생성하면서 데이터베이스 연결 모듈을 통하여 각종 데이터베이스 정보를 질의 및 업데이트 모듈로 처리한다. 또한 제어요청에 따른 처리내용은 데이터베이스에 로그 파일로 저장되고, 제어 명령은 에이전트로 전송된다.



〔그림 3〕 W-RCS의 동작

원격지 제어서버의 에이전트 엔진은 제어명령을 분석하고 요청자의 수행권한 체크 및 권한 설정을 하기위하여 정보를 파싱(parsing)하여 정보 추출, 객체에 저장하는 페이지 퍼메팅(Page formatting), 원격지 에이전트의 상태 체크, 이벤트 발생시 전자메일과 유선관리시스템 전송, 사용자 세션 관리, 기타 데이터의 분석 및 가공을 위한 대부분의 로직 그리고 응용 프로토콜 인터페이스 모듈 등으로 처리과정이 이루어진다.

원격지 에이전트모듈에서 각 에이전트들은 원격지 서버의 노드(host)들에 설치되며, 이는 원격지 콘솔과의 통신, 모니터링 데이터의 추출 그리고 제어명령을 분석한다. 그리고 요청자의 수행권한 체크 및 권한 설정, 제어명령 수행 그리고 수행결과를 필터링(filtering)하여 원격지 서버에 전송하도록 명령어 라인 인터페이스(Command Line Interface)를 제공한다. 원격지 제어 서버에서는 에이전트로부터 전송되어온 수행 결과를 마크업(markup language) 언어(HTML, XML 등)로 변환하는 사용자 인터페이스 과정을 갖은 후 수행결과를 모바일 장비에 전송한다. 모바일 장비에서는 사용자 인증을 위한 기본 보안기능 만 설정될 뿐 어떠한 모듈도 설치되지 않으며, 기본적으로 설치되어 있는 브라우저만 있으면 사용가능하다. 응용 프로토콜 인터페이스에서 제공하는 기능



〔그림 4〕 W-RCS의 보안기능 처리과정

은 대상 시스템의 유선 콘솔에서 제공하는 대부분의 모니터링 기능과 원격 제어기능을 제공할 수 있다.

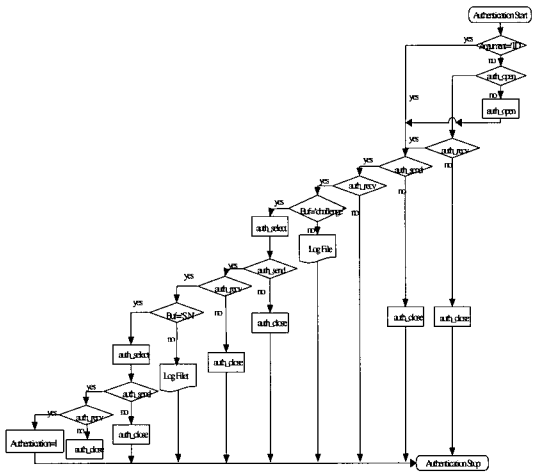
Ⅳ. W-RCS의 보안 기능

1. W-RCS에서 제공되는 보안 기능

W-RCS의 보안 기능은 모바일 장비 사용자가 원격 제어서버에 접근하고자 할 때, ① 사용자의 ID를 입력하면 서버에서 일회용 패스워드 생성을 위한 챌린지 값을 전송하게 되고 일차적인 인증과정이 끝나면, ② 이차적인 인증과정으로 사용자가 소유하고 있는 모바일 장비의 일련번호(Serial Number)를 확인하는 과정으로 모바일 장비 사용자의 인증처리과정이 진행된다. 이렇게 원격제어서버에서 인증된 모바일 사용자라고 하더라도 제어하고자 하는 대상서버에 접근하여 명령어를 실행하고 시스템을 제어하려면 접근제어기능에 의하여 해당 사용자의 권한이 부여되어야 한다. ③ 접근제어에 의한 권한부여는 Supwr-user, Group-user, User 의 ID에 따라 접근권한을 받기 위하여 데이터베이스로부터 자료를 확인한다. ④ 접근제어의 등급에 따라 권하이 부여된다. ⑤, ⑥ 이렇게 권한 부여를 할당 받은 사용자 혹은 그룹은 W-RCS 서버와 에이전트의 요청에 따라 원격에서 시스템의 명령어 사용권한을 갖기 위하여 등록된 사용자들은 암호화된 키 값을 키 스토어에서 생성한다. ⑦ 이렇게 생성된 암호화 키 값은 X.509 기반의 공개키 기반 구조(PKI)의 공인된 인증과정을 실행하는데 사용된다. ⑧ 사용자가 원격 시스템에 접속한 이후에러 혹은 이벤트에 대하여 시스템을 제어할 때도 역시 권한 등급(a, b, c)에 의해서만 시스템을 제어할 수 있다. ⑨ 이렇게 연결이 설정된 이후에 지속되는 시스템 제어과정도 역시 주어진 권한 등급내에서만 처리가 가능하다.

2. 사용자 인증 기능

모바일 장비 사용자가 원격제어서버에 접근하려면 원격제어서버로부터 사용자 인증처리과정을 갖게 된다[그림 5]. 인증을 위한 매개변수(argument)로 사용자의 ID를 입력하게 된다.



〔그림 5〕 사용자 인증 기능 처리과정

```
static int authenticated = 0;
static int user_auth (int ac, char *av[], char *cbuf
{
   char       buf1[512], buf2[512], buf3[512], *p;
 /* 사용자 인증과정이 실행되었는지를 확인  */
if (authuser[0] == '0' || ! authopened)
 /* 사용자 ID를 인증 서버에 전송  */
if (auth_send(buf1) {
            auth_close();
            authopened = 0 ;
            return(writemsg(0, usage3));
            returen(writemsg(0, usage)));
}
 /* 인증 서버로부터 메시지 수신  */
if (auth_recv(buf2, sizeof(buf2)))  {
            auth_close();
            authopened = 0 ;
            return(writemsg(0, usage));
}
/* one-time password를 실행하기 위하여 challenge 값을
생성하여 비교 */
if (!strncmp(buf, "challenge"  ,10)  ||  !  strncmp(buf,
"chalnecho",10)) ;
if (buf2 != '0') char  ebuf[512];
sprintf(ebuf,"인증되었다는메시지 전송 :%s ", $&buf[2]);
/* 모바일 장비의 serial number 비교로 2차 인증과정 */
if (strcmp(buf3, "serial-num" ,10) || !strcmp(buf3, "serial_
num", 10)) ;
   else return (writemsg(0, usage));
```

〔그림 6〕 인증기능의 pseudo code

- 만약 인증이 이미 실행되었다면 "Authentication = 1"로 설정이 되어서 인증과정을 종료하고 다음단계의 보안과정이 진행된다.

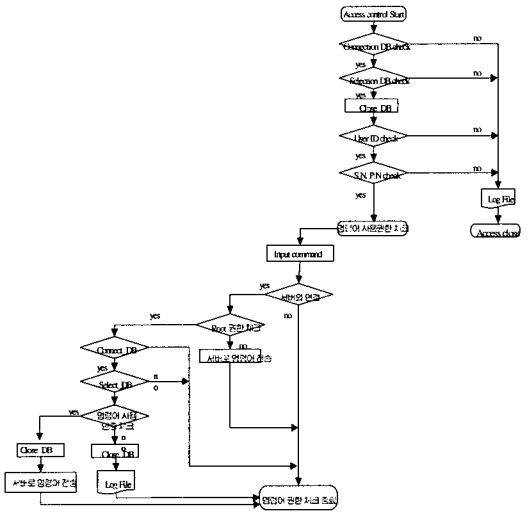
- 인증과정이 실행되지 않은 사용자는 일회용패스워드(one time password)방식으로 패스워드를 전송하여 패스워드 스니핑(sniffing)과 같은 도청으로부터 보

호된다. 원격지 서버에서는 임의의 난수로 생성된 챌린지 값을 모바일 사용자에게 전송하게 되고, 모바일 사용자는 자신의 패스워드를 키 값으로 하여 챌린지 값으로 DES 알고리즘을 실행한다.

이렇게 해서 생성된 결과값(response)과 모바일장비의 일련번호를 서버에 전송하면 서버에서는 입력된 사용자의 ID를 이용하여 데이터베이스를 검색하게 되고, 이미 등록되어있는 사용자의 정보(즉, 초기에 등록된 사용자의 패스워드)로 역시 DES 알고리즘을 동작한다. 이렇게 얻어진 결과와 사용자로 부터 보내온 결과값을 비교하여 같으면 본인임이 인증된다.

- 이러한 일차적인 인증과정이 진행되고 나서, 사용자가 소유하고 있는 모바일 장비의 일련번호가 서버에 등록된 일련번호와 일치하는지를 검증받게 된다. 이러한 과정이 실행됨으로 해서 도난으로 인한 사용자의 오류를 사전에 막을 수 있다.

3. 시스템 접근 및 명령어 사용권한 제어기능



〔그림 7〕 접근권한 및 명령어 사용권한 제어 기능

- 모바일 장비 사용자가 원격지 제어서버로부터 인증되었다면, 다음 단계는 명령어를 입력하여 대상 시스템을 제어하는 것이다.

- 제어서버로부터 인증된 사용자라도 대상 시스템에 접근하여 제어하려면 명령어 입력을 위한 권한을 부여 받아야 한다. 이는 사용자의 등급에 따라 명령어 입력 권한에 제한을 두어 인가되지 않은 사용자가 원격에서 대상 서버를 제어할 수 없도록 하고, 사용자의 등급에 따라 시스템을 제어 하도록 하여 사용자의 오용 또는 남용에 의하여 시스템이 제어되지 않도록 하기 위함이다.

- 때문에 인증된 사용자의 권한 부여를 위하여 접근제어 데이터베이스를 체크한다. 이때 원격지 서버 데이터베이스에 설정되어 있는 보안 등급을 확인하고자 사용자의 ID에 따라 사용자를 SuperUser-ID, User-ID, Group-ID와 모바일 장비의 일련번호 혹은 폰 넘버를 체크한다. 또한, 정상적으로 접근제어가 허용된 사용자라도 루트(root)권한이 있는지를 확인한 후 명령어 사용 권한을 부여받게 된다.

- 만약 보안등급이 설정되지 않은 사용자가 권한 부여를 할당받고자 접속하였다면, 접근을 허용하지 않고 로그파일만 남기고 접근권한 제어과정이 종료된다.

```
# define AC-LEVEL  "AC-TABLE"
char    ac(table, darabase, temp, check-ac)
            char *table, *database, *temp ;
            int check_ac ;
/* 접근제어 수행여부에 대한 체크  */
if (ac_check == 'y' && ac_slevel !='n')
    ac_glevel = ac(AC-TABLE, DATABASE, namp2, 1) ;
/* Super-User ID와 Grpup ID의 등급 체크  */
if (ac_sulevel - ac_glevel) > 0 ) {
            dt.userid = authuser ;
            dt.subject = raddr ;
            -----          }
            exit(1) ;
/* Grpup ID와 User ID 의 등급 체크  */
if (ac_glevel - ac_ulevel) > 0 ) {
            dt.userid = authuser ;
            dt.subject = raddr ;
            -----          }
            exit(1) ;
/* 접근제어 DB에 포함되어 있지 않은 ID의 체크  */
else if (ac_check == 'y' && ac_slevel == 'n') {
            exit(1) ;
}
```

〔그림 8〕 사용권 및 접근제어 pseudo code

4. PKI 기반의 인증기능

W-RCS의 보안기능을 처리하기위한 마지막 단계로서 PKI 기반의 인증기능 과정을 처리하게 된다.

- 모바일 장비(예, PDA) 사용자가 원격지 제어서버로부터 인증처리과정과 접근 및 명령어 사용권한을 부여 받았다고 하여도, 대상 서버에 접근하기 위해서는 공인된 인증기관으로부터 인증된 사용자만이 대상 시스템에 접근이 가능하다.

- 여기서 공인된 인증은 공개키 기반구조(Public

Key Infrastructure)로써 X.509를 따르고 있다.

- 원격 제어서버의 보안 모듈은 keystore에 사용자의 키 쌍(key pair)으로서 공개키(public key)와 비밀키(private key)를 생성하여 보유하고 있다.

- 인증된 모바일 사용자가 대상 서버에 접속하고자 연결요청을 한다.

- 대상 시스템에서는 접속을 요청한 사용자의 개인정보를 데이터베이스로부터 체크한다. 그리고 공인된 인증기관으로부터 사용자의 인증번호와 인증 유효기간 등에 관련한 정보를 얻는다.

- 대상서버에서는 사용자의 공개키로 인증번호와 시스템의 접근허용에 대한 명령을 암호화 하여 전송한다.

- 원격지 제어 서버는 사용자의 비밀키로 복호화를 실행하여 대상 서버로의 접속허용여부를 얻게 된다.

- 사용자는 원격에서 모바일 장비를 이용하여 부여된 권한 내에서 원격의 대상 시스템을 제어하기 위한 명령어 입력을 할 수 있다.

```
void main(int ac, char *av[])
{
openlog(LOG_PID, LOG_GID) ;
 if (!strcmp(st, authrule, USE)) authflg = 1;
 if (gethostname(hosrbuf, sizeof(hostbuf))) strcpy(hostbuf,
"unknown");
 hostbuf[sizeof(hostbuf-1] = '\0';

 /* 입력된 명령어 신호 체크 루틴 */

 /* 호스트명과 포트번호를 이용하여 system server에
접근할 RCserver 객체를 만든다.*/

public RCserver(hostname, inputport) throws unknownHost
Exception
{
if(SSL_PKG) {// SSL connection//
// keystore 파일의 full path 설정 string keyfile = " " ;

// X.509를 기반으로하는 공인 인증기관으로부터 인증체크

//SSL context를 생성하고 SSL socket 객체를 얻음.

  SSLcontext  context =SSLcontext.getInstance("TLS");
  TrustManager[] trusterManagers
  =tmf.getTrustManagers();
  context.init(null, trustManagers();
  context.ini(null, trustManagerw, null) ;
  //SSL connection
 rcSocket=
 ssf.createSocket(InetAdderss.getByName(hostName), port);

  // 서버와 입출력 스트림 생성
 out = new PrinterWriter(rcSocket.getOutputStream(), true);
```

〔그림 9〕 PKI 인증과정 pseudo code

V. 성능 평가

본 논문에서 구현된 시스템의 보안 기능에 대한 성능을 평가해 보았다. [표 1]은 보안처리 과정이 시행되지 않은 경우, 각 시스템 별로 접속 시간에 따른 응답시간을 측정한 것이다. 이때 테스트 환경으로 PDA는 Compaq iPAQ 3850을 사용하였으며, 무선모뎀으로는 CDMA - 1X(144kbps), 제어서버로는 Solaris 2.7이다. 이에 대해 대상서버로는 역시 Solaris 2.7이고, 수행된 명령은 파일리스트 보기 "ls -al"을 실행하였다.

〔표 1〕 접속시간/Response time 측정결과

측정항목 / 횟수	PDA→제어서버	제어서버→대상서버	수행시간 (ls -al)	대상서버→제어서버	제어서버→PDA
1	1.240	0.811	1.5	0.189	0.989
2	2.988	0.538	0.82	0.182	0.889
3	1.132	0.595	0.824	0.219	1.192
4	0.975	0.320	0.822	0.202	1.219
5	1.023	0.321	0.907	0.286	0.782
6	1.230	0.322	0.743	0.191	0.913
7	1.219	0.305	0.790	0.190	0.837
8	0.899	0.325	0.793	0.170	1.328
9	0.938	0.305	0.806	0.201	0.895
10	1.151	0.343	0.838	0.195	0.923
평균	1.0765	0.3668	0.8643	0.2025	0.9967

[표 1]의 결과에서 PDA에서 제어서버로 접속 및 응답하는데 평균 1.0765초 이고, 제어서버에서 대상서버로는 평균 0.3668초 있다. 즉, PDA에서 제어서버로 접속하는 시간은 제어서버에서 대상 서버로 접속하는데 소요되는 지연시간에 비하여 평균 3배정도의 시간이 소요 되었다. 또한, 대상 서버에서 제어서버로 연결되는 데는 평균 0.2025초 그리고 제어서버에서 PDA로 연결되는 데는 0.9967초가 소요되어 접속설정을 위한 지연시간에 비해 응답시간은 평균 0.2141초가 적게 소요됨을 알 수 있었다.

〔표 2〕 인증 Time 측정결과

측정항목 / 횟수	제어서버인증	대상서버인증
1	0.176	0.968
2	0.168	0.962
3	0.168	0.920
4	0.165	0.953
5	0.173	0.963
6	0.167	1.045
7	0.165	1.328
8	0.163	1.091
9	0.165	0.950
10	0.174	0.936
평균	0.168	1.0116

[표 2]는 제어서버와 대상 서버로의 인증과정을 실행한 경우에 소요되는 시간을 측정한 것이다. PDA

가 제어서버로부터 인증을 받기위해서 지연되는 시간은 평균 0.168초였으며, 대상 서버로부터의 인증에 소요되는 시간은 1.0116초가 소요되었다. 이는 인증기관으로부터의 인증절차 등으로 인한 지연시간인 것임을 알 수 있다. 한번 인증과정이 이루어진 이후, 다음 지속적인 명령어 입력과 시스템 제어를 실행할 수 있다.

Ⅳ. 결 론

본 연구는 모바일 단말기로 이동 중에도 원격지의 시스템을 실시간으로 모니터링 할 뿐만 아니라 문제가 발생되면 즉각 모바일 단말기로 장애통보를 해주거나, 원격지의 시스템에 바로 접근해서 문제를 해결할 수 있는 원격제어 기능을 제공할 수 있는 실시간 무선 원격제어 시스템(W-RCS)을 설계 및 구현하였다. 그러나 유선과 무선이 공용하는 시스템에서 보안은 아무리 강조하여도 부족하다고 고려된다. 때문에 본 연구에서는 모바일 장비 사용자가 원격지 서버에 접속하기 위하여 강력한 인증과정을 수행해야만 한다. 그리고 원격지 서버로부터 인증된 사용자라도 대상 서버에 접속하여 명령어를 원격에서 입력하려면 명령어 사용에 대한 권한을 부여 받아야 한다. 이렇게 명령어 사용권한을 부여 받은 사용자라도 실제 대상 시스템을 제어하기 위해서는 대상 시스템으로부터 다시 한번 인증과정을 수행해야만 한다. 여기서 대상 시스템은 PKI 기반의 인증과정을 실행하여 사용자의 공개키로 인증번호 및 명령을 암호화 하여 전송한다. 사용자는 자신의 비밀키로 복호화 과정을 실행함으로써 완벽한 보안과정이 실행된다. 그러나 일반적으로 보안 기능이 강화되면 상대적으로 시스템은 보안 기능 처리과정 등 지연시간으로 인하여 성능이 저하되는 경우가 많다. 그렇기 때문에 인증과정을 시행한 경우와 그렇지 않은 경우에 대하여 명령어 처리를 위해 소요되는 지연시간을 측정하였다. 그러나 대상 시스템에 연결 설정을 위해서 소요되는 인증을 위한 지연시간 평균 1.0016초이며, 이는 W-RCS를 위한 강력한 보안 기능에 비하여 시스템을 원격에서 제어하는데 현재로서는 저해 요소가 되지 않았다. 다만, 향후 보다 더 신속한 서비스를 요구하는 사용자들의 요구를 만족하고자 한다면 위의 실험에서 보여준 응답 시간을 조금 더 줄일 수 있도록 연구하고자 한다.

참 고 문 헌

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

[2] Carles Arehart, Nirmal Chidambaram, etc. "Professional WAP" Wrox. 2000.

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

[4] Dr. Mikael Sjodin 2002 *"Remote Monitoring and Control Using Mobile Phone"*.

[5] Ericsson Enterprise AB 2002 EN/LZT 102 3511 RC *"The path to the Mobile Enterprise"*.

[6] http://www.cis.upenn.edu/~bcpierce/courses/629/papers/Concordia-White paper, *"Mobile Agent Computing"*.

[7] James F. Kurose and Keith W. Ross, *"Computer Networking"*, Addison Wesley 2nd-Edition, 2002.

[8] Kaveh Pahlavan and Prashant Krishnamnurthy, *"Principles of Wireless Networks"*, Prentice-Hall. 2002.

[9] Richard E. Smith *"Internet Cryptography"* Addison Wesley, 5th-Edition, 2002.

[10] Sumit Deshpande Office of the CTO Reserved October 7, 2002, *"The Future of wireless Enterprise Management"*.

[11] Sybase Whitepaper, 2002. *"iAnywhere Mobile Manager"*.

[12] Timbukutu Pro, 2002. *"A secure approach to deployment of remote control technology"*.

[13] 이문구, "침입 차단 시스템을 위한 FTP 프록시 보안 모델의 구현", 한국통신정보보호학회 논문지 제10권 제2호, 2000. 6.

〈著者紹介〉

이 문 구 (Moon-ku Lee) 정회원

1984년 : 숭실대학교 전자계산학 (학사)
1993년 : 이화여자대학교 대학원 전산교육학 (석사)
2000년 : 숭실대학교 대학원 컴퓨터시스템 (공학 박사)
2000년 3월~현재 : 김포대학 컴퓨터계열 조교수
<관심분야> 네트워크 프로그래밍, 인터넷 보안, 암호화 알고리즘, 전자상거래 보안, 침입탐지 및 차단시스템