인증기반 홈제어 시스템 구현

장혜영° 조성제 최종무
단국대학교 정보컴퓨터학부
{chenil° sjcho choijm}@dankook.ac.kr

An Implementation of Home Control System with Authentication Mechanism

Hye-Young Chang° Seong-Je Cho Jongmoo Choi
Division of Information and Computer Science, Dankook University

요 약

언제, 어디서나 사용자가 원할 때 시스템을 사용할 수 있는 유비쿼터스 분야에 대한 관심이 고조되는 가운데 전등, TV, 오디오, 전자 열쇠 등을 제어하는 홈 제어 시스템이 개발되어 상용화 되고 있는 것이 요즘의 추세이다. 이렇게 유비쿼터스가 급격히 진보됨에 따라 같이 대두되는 부분이 바로 보안이다. 언제, 어디서나 사용자가 원할 때 시스템을 사용해야 하지만 반드시 자격을 가지고 있는 사용자만이 이용할 수 있어야 한다. 본 논문에서는 인텔 XScale 프로세서 기반의 하드웨어 시스템에서 임베디드 리눅스 운영체제를 이용하여 홈 제어 시스템을 구현하였다. 또한 인증 모듈을 적용함으로써 보안을 강화시켰다.

1. 서 론

현재 시중에는 홈 네트웍으로 연결이 가능한 디지털 제품들, 즉 디지털 TV나 인터넷 냉장고, 인터넷 보일러, 통신기기 등이 출시되고 있다. 또한 언제, 어디서나 가전기기들을 제어할 수 있는 홈 제어 시스템이 내장된 아파트도 만들어지고 있다[1].

이렇게 모든 것이 연결되고 공유됨으로써 우리의 생활을 윤택하게 할 수 있지만 또 다른 면에서는 심각한 정보보호, 프라이버시 등의 보안문제가 발생할 수 있다. 보안의 중요성은 리처드 헌터의 말을 인용하면 다음과 같다. "미래는 부자를 제외하고는 프라이버시를 즐길 수 있는 사람이 거의 없던 과거와 비슷해 질 것이다. 이제 모든 컴퓨터와 사물이 하나로 연결되는 유비쿼터스 네트워크의 시대가 온다. 세계는 누구나 편하게 정보에 접근할 수 있는 멋진 세상이 될 것이다. 하지만 한편으로는 고도의 네트워크화 된 세상에서는 누군가의 실수가 곧바로 범죄에 이용되고, 시스템의 작은 버그는 엄청난 혼란을 야기한다. 크래킹에 의한 정보유출, 바이러스 유포, 저작권 침해 등 가상 세계에서 벌어지는 각종 부작용이 우리 삶을 위협하게 될 것이다." 라고 주장하는 바와 같이 유비컴퓨팅 환경에서의 사회적 역기능을 경고하고 있다[2]. 즉 모든 것이 정보를 공유하고 활용하는 열린 환경은 더욱더 보안에 대한 중요성을 부각시킨다.

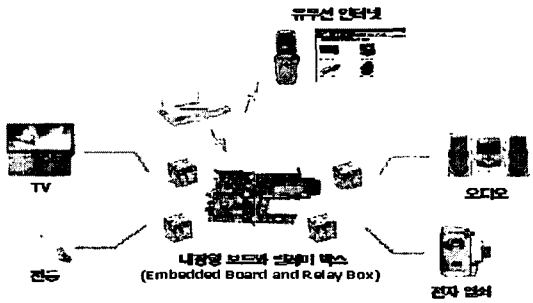
본 논문은 유비쿼터스 시대의 선봉이라 할 수 있는 홈 제어 시스템을 구현하고 인증모듈을 추가하여 보안을 강화시켰다. 인텔사의 XScale 프로세서를 가지는 보드를 사용하였고, 이 보드에 내장형 리눅스 운영체제 RedHat Linux 9.0 버전을 탑재한 후에 내장형 웹 서버로 GoAhead를 설치하였다.

본 논문의 구성은 다음과 같다. 2장에서는 전체 시스템 설계 사양에 대하여 살펴보고, 3장에서는 시스템 구현 방식에 대해 설명하고, 4장에서는 결론 및 향후과제를 제시한다.

2. 시스템 설계

2.1 전체 시스템 설계 구성도

전체 시스템의 구성은 (그림 1)과 같다. Home Control Board와 가전기기들과 원격 호스트 컴퓨터들은 릴레이 박스를 통하여 상호 통신이 가능한 상태이고, 보드에서 작동하고 있는 웹 서버를 통하여 외부로부터도 원격지의 웹 클라이언트를 통하여 실시간 명령을 받아 가전기기를 제어한다.

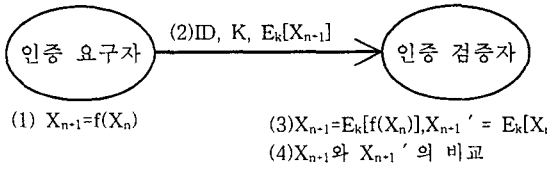


(그림 1) 전체 시스템 구성

2.2 인증 시스템 설계 구성도

네트워크 환경에서 사용자 인증을 위해 사용되는 일반

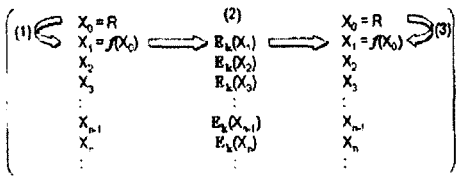
패스워드는 암호화되지 않은 상태로 전달되기 때문에 중간에 노출될 위험이 있다. 그러므로 네트워크 상에서 기존 방식의 패스워드 노출 취약점을 보완하기 위해 일회용 패스워드 방식이 제안되었다. 일회용 패스워드 방식은 기존 방식과는 달리 네트워크 상에서 검증자(클라이언트)로 전달되는 인증 요구자(서버)의 인증용 패스워드가 매번 다른 값을 갖도록 해줌으로써 패스워드가 노출 된다 하더라도 이 패스워드는 한 번 밖에 사용하지 않는 패스워드이기 때문에 다른 공격자가 이를 사용하여 인증을 받을 수 없다.



(그림 2) 인증 흐름 설계도

본 논문에서는 처음 시스템 설정 시에 난수인 초기값 X_0를 생성하여 이 값을 각각 인증 요구자와 검증자에 저장해 둔다. 이 상태에서 인증 요구자가 검증자로부터 인증을 받기 위해 (그림 2)의 (1)과같이 $X_{n-1}=f(X_n)$를 계산한다. 그리고, (2)에서 자신의 사용자 번호인 ID와 키 K, $E_k[X_{n-1}]$를 인증 정보로 인증 검증자에게 전달한다. (3)에서 인증 검증자도 (1)에서와 마찬가지로 $X_{n-1}=f(X_n)$를 계산하고 이를 암호화하여 $E_k[X_{n-1}]$를 구한다. (4)에서 인증 검증자는 (2)에서 보내온 x값과 (3)에서 구한 x′ 값을 비교하여 같으면 인증 요구자를 인증하게 된다. 인증이 성공적으로 이뤄지게 되면 인증 검증자는 X_{n-1}값을 저장해 둔다.

일회용 패스워드 생성 과정을 좀더 자세히 살펴보면 (그림 3)과 같다.



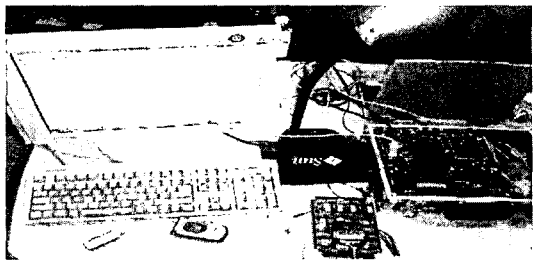
(그림 3) 일회용 패스워드 생성 과정

(1)에서 인증 요구자는 $X_0=R$ 값에 대해 일방향 함수f를 수행하여 $X_1=f(X_0)$을 생성하고 (2)에서 인증 요구자는 X_1 값을 E로 암호화 하여 $E_k[X_1]$값을 인증 검증자로 전달한다. (3)에서 인증 검증자는 자신이 저장하고 있는 $X_0=R$로부터 $X_1=f(X_0)$을 구하여 이를 E로 암호화 하여 $E_k[X_1]$ 값을 구한 뒤에 (2)에서 전달 받은 값과 비교하게 되고, 값이 같으면 인증 요구자를 인증하게 된다. 새로 계산된 $X_1=f(X_0)$값은 인증 요구자와 검증자가 각각 저장하여 다음 인증 과정에서 사용된다.[3]

3. 구현

3.1 전체 하드웨어

본 연구는 레드햇 9.0 커널 2.4.19버전이 설치되어 있는 PXA255-Pro 보드에 릴레이 박스와 연결하여 홈 제어 시스템의 대상인 스탠드, 오디오, TV, 컴퓨터의 전원을 제어하게 만들었다. 이때 접속하는 클라이언트 시스템은 Linux 레드햇 9.0 2.4.22커널이다.



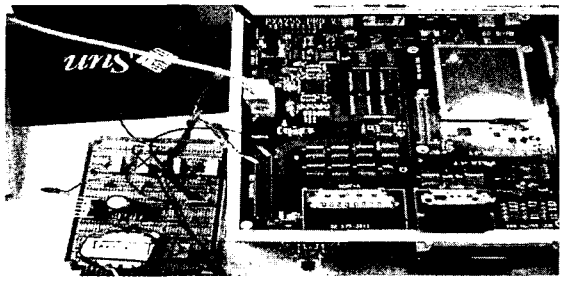
(그림 4) 하드웨어 전체 구현환경

3.2 릴레이 박스

일반적으로 전기회로를 개폐(開閉)하는 조작을 다른 전기회로의 전기적(電氣的)인 세력의 변화에 의하여 행하는 장치이다. GPIO 드라이버를 구현하여 등록시키고 PXA255 보드에서 GPIO 3번을 통해 제어 하고 있다. 릴레이의 내부에는 전기의 흐름을 단속할 수 있는 물리적인 스위치가 구현되어있고 전자석의 힘에 의해 그 역할을 하게 된다. 따라서 GPIO 3번 핀을 통해 전원이 가해지면 릴레이의 전자석이 붙게 되어 스탠드에 전원을 공급한다. 릴레이 박스는 GPIO 핀을 통해 보드와 연결되면 Xscale PXA255기반 보드는 84개의 GPIO를 지원한다. 본 연구에서는 GPIO3 번을 사용하고 제어하는데 필요한 레지스터 GPDR0, GPSR0, GPCR0 들을 설정해주었다. GPSR0의 GPIO 3번 비트에 1을 셋해주면 전류가 흐르고, GPCR0의 GPIO 03비트에 1을 셋해주면 전류가 끊긴다.

릴레이 제어를 위해 GPIO 드라이버를 구현 하는데 모듈로 작성하여 적재한다. 커널과 통신하는 부분은 seun_gpio_open, seun_gpio_release, seun_gpio_ioct로 구성되었다. 이 함수들 중에 응용 프로그램이 GPIO 핀을 선택하거나 설정할 때 사용하는 함수는 seun_gpio_ioctl 이다. 릴레이 박스를 (그림 5)와 같이 구현되었다.

레지스터 이름	기 능
GPDR	GPIO 핀의 방향을 설정
GPSR	GPIO pin output set register
GPCR	GPIO pin output clear register



(그림 5) 릴레이 박스 구현

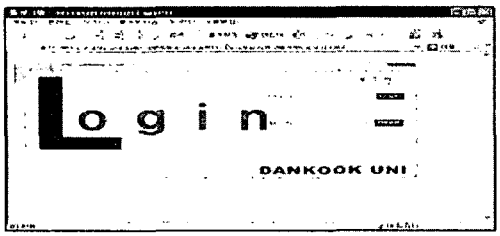
3.3 웹 서버

제안된 시스템이 범용 브라우저를 이용해 접근될 수 있도록 하기위해 본 논문은 내장형 보드에 웹 서버를 구성하였다. 웹 서버를 구성할 때 가장 일반적으로 사용되는 패키지는 아파치이다. 하지만 아파치는 libutil.so와 libpam.so 같은 많은 공유 라이브러리와 아파치 종속적인 모듈들을 사용하기 때문에 자원 제약이 있는 내장형 시스템에서 사용하기에는 성능상에 문제가 있다. 따라서 본 논문은 내장형 시스템을 위한 대표적 웹 서버인 GoAhead와 Boa등을 조사하였고, CGI와 보안 기능을 지원하는 GoAhead를 선택하였다.

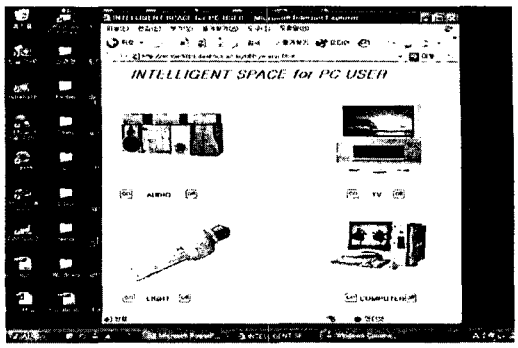
GoAhead사에서 공개한 GoAhead2.1 웹 서버는 HTTP 1.0 프로토콜을 지원한다. 또한 이식성이 뛰어나 디렉토리 등 약간의 환경 변수만 적절히 설정하면 제안된 시스템에 쉽게 이식할 수 있다.

3.4 인증 시스템

http를 이용한 웹 서버에 접속을 하면 (그림 6)과 같은 로그인 초기화면이 나타난다. 사용자는 <아이디>란에 자신의 아이디를 입력하면 그 아이디에 저장되어 있는 X_0=R값을 이용하여 key와 seed를 계산하여 출력하게 된다. 사용자는 key와 seed를 클라이언트에 설치되어 있는 generate에 입력하여 패스워드를 얻은 후 <패스워드> 란에 입력을 하게 된다. 서버에서 계산한 결과 값과 입력한 값이 같게 되면 (그림 7)과 같이 홈 제어 시스템을 이용할 수 있게 된다.



(그림 6) 로그인 화면



(그림 7) 홈 제어 시스템 서비스 화면

4. 결론 및 향후과제

사람이 직접 손으로 집안 기기를 조절하러 다니지 않고 자동으로 제어할 수 있는 홈 제어 시스템의 개념은 1940년 중반에 시작되었다. 그러나 이때의 홈 제어 시스템에 대한 시도는 미약한 기술로 활성화 되지 못하였다가 1990년도부터 인터넷의 발달로 홈 제어 시스템이 다시 활성화되기 시작하였다. 그러나 인터넷이 발달함과 동시에 악용하려는 사람 또한 늘어나게 되었다. 정당한 사용자가 안전하게 편한 홈 제어 시스템을 이용하기 위해서는 인증은 불가피하게 되었다. 그래서 본 논문은 악용하려는 사람이 중간에 아이디나 패스워드를 도용한다 하더라도 다시 쓸 수 없는 일회용 패스워드를 사용하여 더욱더 안전하게 사용자가 웹 기반 홈 제어 시스템을 이용할 수 있게 하였다. 향후 본 논문은 시간이 많이 걸리지 않으면서도 안전한 암호 알고리즘을 도입하여 암호와 인증부분을 더욱 보완할 계획을 가지고 있다.

[참고 문헌]

[1] 강범준, 간은영, 김종몽, 차정민, 최원진, "비트 프로젝트 23호 무선 홈 네트웍 시스템"

[2] 리차드헌터, "유비쿼터스 - 공유와 감시의 두 얼굴"

[3] 박충길, 김영진, 김영길, 백규태, 백기영, 류재철, "S/Key를 개선한 일회용 패스워드 메커니즘 개발", 한국정보보호학회, 9권, 2호, 25-36쪽, 1999

[4] (주)휴인스 기술연구소, "Intel PXA255와 임베디드 리눅스 응용"