홈 네트워크 환경에서 OTP 알고리즘을 이용한 개선된 사용자 인증 기법

김재용*, 정용훈*, 전문석*
숭실대학교 컴퓨터학과*
e-mail:{raient, s0178}@ssu.ac.kr, mjun@computing.ssu.ac.kr

A Study on Home Network Device Access Control by using token-based on OTP

Jae-Yong Kim*, Yong-Hoon Jung*, Moon-Seog Jun*
Dept. of Computer Engineering, Soongsil University*

요 약

홈 네트워크 서비스 산업은 미래의 국가발전과 새로운 변혁의 원동력으로서 향후 발전 가능성이 매우 크다고 할 수 있으나, 홈 네트워크 서비스의 보급이 확산되고 다양한 형태의 홈 네트워크 서비스가 등장하면서, 사이버공격의 대상 범위 또한 확대되어 사회적, 경제적으로 우리 사회에 큰 불안 요소로 작용할 가능성이 있고, 홈 네트워크 서비스의 침해사고 발생을 방지하고 사용자의 정보가 노출되지 않는 사용자 인증이 필요하다.

본 논문에서는 OTP를 기반으로 한 인증서를 이용하여 홈 네트워크의 보안요소 중 사용자 인증과 접근제어에 관하여 연구 하였으며, 인증 서버와 클라이언트 간에 동기화된 OTP 난수 값으로 인증서 정보를 암호화 하여, 외부 공격으로부터 보다 안전한 사용자 인증 기법을 제안한다.

1. 서론

현대사회는 IT 산업의 급격한 발전과 함께 실공간과 사이버공간의 자연스러운 연결로 인해 업무환경뿐만 아니라 가정에서의 홈 네트워크 서비스가 등장하고 발전 해 왔다. 이러한 흐름에 따라 여러 IT 기술 들 중 계속적인 이슈가 되고 있는 홈 네트워크 서비스 산업은 미래의 국가발전과 새로운 변혁의 원동력으로서 향후 발전 가능성이 매우 크다고 할 수 있으나, 홈 네트워크 서비스의 보급이 확산되고 다양한 형태의 홈 네트워크 서비스가 등장하면서, 사이버공격의 대상 범위 또한 확대되어 사회적, 경제적으로 우리 사회에 큰 불안 요소로 작용할 가능성이 있고, 홈 네트워크 서비스의 침해사고 발생을 방지하고 사용자의 정보가 노출되지 않는 사용자 인증이 필요하다.

본 논문에서는 외부 클라이언트가 PDA와 같은 Mobile 단말기로 홈 네트워크를 컨트롤 하기위하여 홈 네트워크의 보안요소 중 사용자 인증과 접근제어에 관하여 연구 하였으며, 한국정보통신기술협회의 단체 표준인 홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘(TTAS.KO-12.0030) 표준에서 고려하지 않은 댁외 에서 홈 네트워크 사업자의 인증 서버를 거치지 않고 홈 서버로 바로 접속하는 경우의 사용자 인증방법으로 OTP 기반의 인증서를 이용한 홈 네트워크 사용자 인증방식을 제안한다.

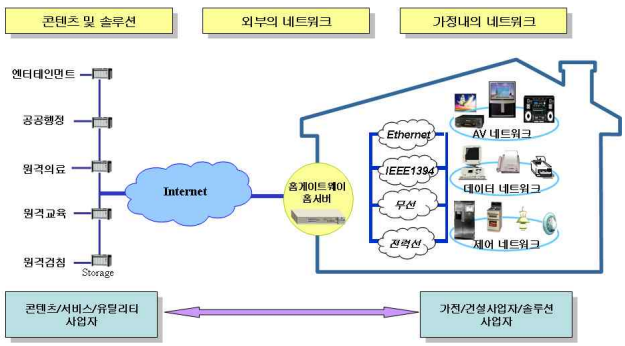
사용자 인증의 인증서는 X.509 v3의 인증서를 기반으로 사용하고 X.509 v3의 확장영역에 사용자의 그룹을 나누어 디바이스를 제어하고 접근이 제한된 디바이스는 ACL(Access Control List)을 추가하여 접근제어를 하는 방법으로 접근이 제한된 사용자와 이를 관리하는 관리자로 나누어 각 디바이스에 대한 접근제안과 외부 공격으로 부터의 안전하게 보호 할 수 있다.

2. 관련연구

2.1. 홈 네트워크

홈 네트워크에 대하여 미국의 소비자가전협회(CEA : Consumer Electronics Association)의 HNIT(Home Networking and IT)분과에서는 “가전기기 및 전자 시스템들이 원격 접근 및 원격제어가

가능하도록 서로 연결하는 것” 이라고 정의하고 있다. 즉, 홈 네트워크를 통하여 각 제품들은 서로 연결되어 상호간에 서비스를 공유할 수 있어야 하며, 사용자는 원격에서 분산되어 있는 기기들을 제어하거나 각각의 기기들이 제공하는 서비스를 이용할 수 있어야 한다. 이러한 홈 네트워크 서비스가 적용된 환경을 디지털 홈이라고 한다. 2003년에 정보통신부가 한국의 차세대 성장 동력 산업의 하나로 지목하면서 디지털 홈이라는 용어가 처음 사용되었다. 디지털 홈이란 홈 네트워킹 기술과 이 기술이 구현된 정보가전을 하나의 개념으로 통합한 개념으로, 유비쿼터스 환경이 일반 가정에 적용된 것을 의미한다.



[그림 1] 홈 네트워크 구성도

홈 네트워크는 [그림 1]과 같이 가정 내의 기기들이 통신이 가능하도록 하나의 네트워크로 묶고 이를 외부 인터넷 망과 연결하여 가정 내/외부 어디서나 사용자의 위치에 관계없이 가전 기기들을 제어할 수 있도록 하는 것이며 또한 외부 콘텐츠 원격의료, 원격교육 등 가정 내에서 외부에 있는 서비스를 사용하는 것이 홈 네트워크이다.

2.2. OTP (One Time Password)

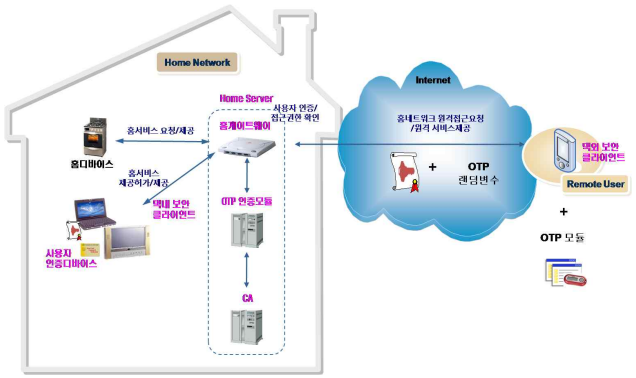
OTP는 1회에 한해 사용할 수 있는 비밀번호를 생성하는 시스템으로 매번 다른 비밀번호를 이용하여 사용자를 인증하는 방식이다. 이중 요소 사용자 인증의 대표적인 방법인 OTP는 기본적으로 암호학적인 아이디어를 바탕으로 고안된 것으로 보안성이 높고 사용하기에 편리한 방식이다. 매번 다른 패스워드를 사용하기 때문에 고정된 패스워드를 사용하는 방식과 달리 패스워드 재사용 공격이 불가능하고, 암호학적 알고리즘을 사용하기 때문에 기존에 사용된 패스워드로부터 다음에 사용될 패스워드를 예측하는 것이 불가능하며, 따라서 안전하다. OTP 토큰 또는 사용자 PC에 저장된 OTP용 프로그램에 사용자 비밀번호와 일회용 비밀번호 생성용 입력값을 입력하면, 암호 알고리즘을 사용해서 일회용 패스워드를 생성하게 된다. 여기서 들어가는 입력값을 매번 다른 값으로 입력해야 일회용 패스워드가 생성되며, 이 입력값을 어떤 값으로 입력하는가에 따라 다양한 OTP 방식으로 분류된다.

3. 제안하는 시스템

3.1. 전체 시스템

본 논문에서 제안하는 홈 네트워크 시스템의 사용자 인증은 OTP를 기반으로한 공개키 암호알고리즘의 인증서를 통해 사용자를 인증하며 개인의 인증서를 홈 서버로부터 받아서 개인의 디바이스로 홈 시스템을 컨트롤 하는 방법이다. 또한 기존의 홈 네트워크 환경에서 반드시 경유하여야 하는 사업자 인증서버를 거치지 않고 사용자가 외부에서 클라이언트 디바이스와 홈 서버가 직접적으로 인증할수 있는 시스템을 제안하고 있다.

시스템의 전체구조는 [그림 2]와 같이 PDA 등과 같은 외부 클라이언트 즉, 외부에서 사용자가 인터넷 망을 통하여 홈 네트워크에 사업자 인증서버에 대한 경유업이 직접적으로 접근 및 사용자 인증을 수행한다.



[그림 2] 제안하는 시스템 구조

홈 서버에 접근할 때 OTP 기반의 인증서를 이용하여 사용자를 인증하는 방법과 홈 디바이스에 대한 접근제어를 하는 방법에 대하여 제안하였다.

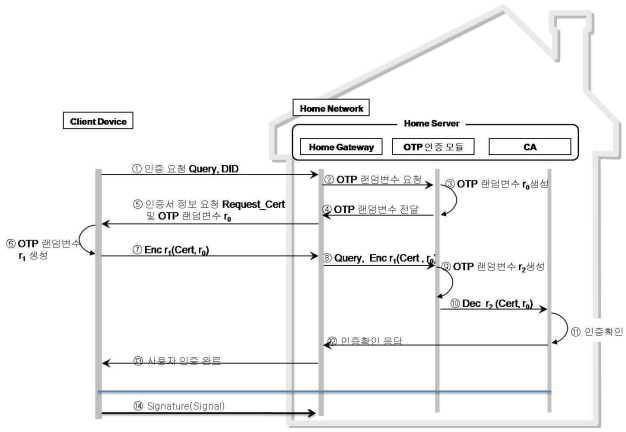
사용자 인증은 외부 사용자의 클라이언트 디바이스가 탑재한 OTP 모듈에서 생성한 OTP 랜덤변수와 인증서를 이용하여 기존 방법보다 안전하게 사용자를 인증하는 방법을 제안한다. 홈서버에는 외부 사

용자의 클라이언트 디바이스와 홈 네트워크 내에 홈 디바이스 간 통신을 위한 홈 게이트웨이와 사용자 인증을 위한 OTP 인증모듈, CA로 구성된다.

홈 디바이스 접근제어는 외부에서 클라이언트가 홈 디바이스를 제어할 때 각 사용자마다 접근제어목록이 다르게 구성되어 있으며, 사용자가 이미 사용하고 있는 디바이스에 대해서 다른 사용자가 사용 할 수 없는 다중 접근제어를 각 사용자가 생성하는 OTP 랜덤변수를 이용하여 제공한다. 관리자는 사용자의 등급에 따라 접근이 가능한 디바이스와 접근이 불가능한 디바이스로 나누어 관리를 할 수 있고,, 클라이언트는 관리자로 부터 접근제어 목록을 추가/삭제를 요청 할 수 있고 요청이 이루어지면 클라이언트는 인증서를 홈 서버로부터 재발급 받는다.

3.2. 사용자 인증과정

사용자 인증과정은 [그림 3]과 같이 클라이언트가 발급받은 인증서와 서로 동기화 한 OTP 모듈로 생성한 OTP 랜덤변수를 가지고 사용자가 외부에서 SSL(Secure Sockets Layer)을 통하여 홈 네트워크에 접속을 요청한다.

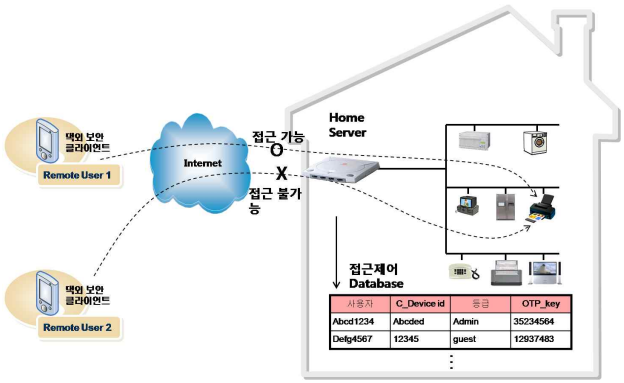


[그림 3] 사용자 인증과정

사용자 인증요청이 전송되면 홈 서버는 사용자의 인증서 정보와 OTP 생성한 랜덤변수를 사용자에게 요청하고, 사용자는 홈 서버와 동기화 한 OTP 모듈에서 생성한 OTP 랜덤 변수 r값을 생성하여 r값을 대칭키 알고리즘의 개인키로 인증서 정보와, 홈서버로부터 전송받은 OTP 랜덤변수를 함께 암호화하여 전송을 한다. 홈 서버의 OTP 인증 모듈 역시 생성한 OTP 랜덤 변수 r값으로 암호화 된 인증서 정보를 복호화 하고, 복호화된 인증서의 정보와 초기 홈 서버에서 생성한 OTP 랜덤변수를 CA에서 검증하여 인증서의 정보가 확인되면 홈 게이트웨이를 통해 사용자에게 인증확인 응답을 전송 함 으로 사용자에 대한 인증을 완료한다. 이후 클라이언트 디바이스는 홈 네트워크 상의 홈 디바이스를 제어 할 수 있다.

3.3. 홈 디바이스 접근제어

사용자 인증과정이 이루어지면 [그림 4]과 같이 홈 게이트웨이를 통하여 각 디바이스를 접근이 이루어진다. 외부 클라이언트가 홈 디바이스에 접근 할 때 사용자에 따라 홈 디바이스에 접근권한이 부여되고, 홈 서버는 외부 클라이언트의 인증서를 통해 접근 가능 여부를 판단해 홈 디바이스의 접근을 통제한다.



[그림 4] 디바이스 접근제어

① $Enc_{h(r\|Key)}(DIDNum, Control\ Command), DID$

- OTP 모듈에서 생성한 랜덤변수 r값과 자신의 키를 연접한 후 해쉬한다.

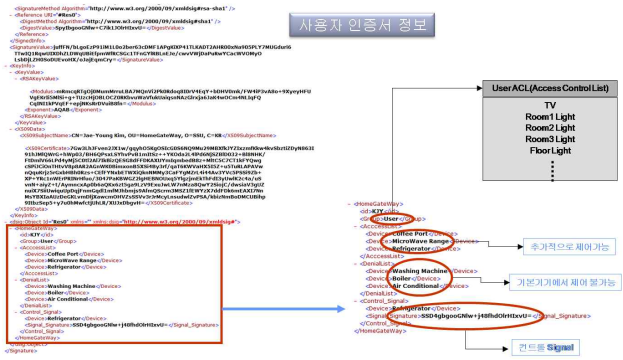
- 해쉬값과 X.509 기반의 애트리뷰트인 DIDnum와 Control Command 메시지를 암호화한 값과 클라이언드 자신의 DID를 홈서버에 전송한다.

② 홈 서버는 클라이언트의 DID 값을 이용하여 복호화 하여 DIDnum와 Control Command를 확인한 후 통보한다.

3.4. 사용자 인증서

사용자 인증과정에서 사용되는 인증서에는 기본적으로 사용자 권한에 맞는 기기들을 [그림 5]와 같이 접근제어목록 ACL을 그룹으로 묶어 구성한다.

각 그룹을 토대로 제어가 가능하도록 하고, 해당 그룹에서 제어가 불가능한 기기를 다루기 위해서 AccessList 엘리먼트를 추가시켰고 기본그룹에서 제어를 막아두기 위해 DenialList 엘리먼트를 추가하여 각 디바이스에 접근에 대한 제어를 한다.



[그림 5] 사용자 인증서

4. 결론

홈 네트워크 기술의 발전과 더불어 함께 증가하는 보안적 위험을 미연에 방지하고 줄이기 위하여 지속적인 관심과 활발한 연구가 계속적으로 이루어져야 하는데, 홈 네트워크 분야 역시 이러한 문제에 적극적이고, 지속적으로 대응해야 한다. 홈 네트워크 서비스의 침해사고 발생의 방지와 사용자의 정보를 노출 시키지 않기 위해서 안전한 사용자 인증 기법이 필요하다.

본 논문은 홈 네트워크 사업자의 인증서버를 거치지 않고 외부의 사용자가 홈 네트워크의 홈 서버와 직접적으로 안전한 사용자 인증을 수행 할 수 있는 보다 안전한 인증 방식을 제안한다.

자신의 클라이언트 디바이스의 인증서를 오프라인에서 홈 서버로부터 직접발급 받으며, 클라이언트 디바이스와 홈 서버간에 동기화 한 OTP 모듈로 생성하는 랜덤변수로 인증서의 정보를 암호화 하여 안전하게 보호한다. 또한 발급받은 인증서와 OTP 랜덤변수의 값을 이용하여 사용자 인증과 디바이스 접근제어를 한다. 제안한 프로토콜에서는 데이터는 항상 암호화 되어 전송되므로 불법적인 장치가 클라이언트의 개인키와 난수 r값을 모르면 데이터의 정보가 노출될 위험은 없다. 또한 기존의 홈 서버에서 생성하는 난수 r값을 서로 동기화 하여 서버에서 클라이언트로 먼저 전송해야되는 사전 동작을 생략함으로서 통신상의 오버헤드를 감소시키는 효과를 동반하고 있다.

사용자 인증과정에 있어서 홈 서버와 클라이언트의 OTP에서 생성한 1회성 난수 r값을 이용해 암호화하여 스니핑 등의 공격에 보다 안전한 인증을 제공하고,개인키와 인증서를 유추하는 것은 어렵고, 홈 디바이스를 제어할 때 메시지는 해쉬한 값을 다시 암호화 하여 전송하기 때문에, 중간에서 메시지를 가로채더라도 메시지의 내용을 유추하는 것은 불가능하다.

향후 연구과제로는 다양한 홈 디바이스를 제어하는 방법과 연산 수행능력이 떨어지는 휴대용 기기를 이용한 무선에서의 홈 디바이스 접근 및 제어하는 방법에 관한 연구가 필요하며, 기존의 유선망에서 사용하는 안전한 보안 프로토콜과 제안한 방법을 적용하여 보다 안전한 보안 프로토콜에 관한 연구가 필요하다.

참고문헌

[1] 박동준, “홈 네트워크 보안에 관한 연구”, 건국대학교, 2005.

[2] 한종욱, 김도우, 주홍일, 이윤경, 남택용, 장종수, “안전한 홈 네트워크 구축을 위한 보안요구사항”, 정보처리학회지, VOL. 11, pp.38-45, 2004.

[3] 하원규, 김동환, 최남희, “유비쿼터스 IT 혁명과 제3공간 - 물리공간과 전자공간의 융합”, 전자신문사, 2003.

[4] 이영구, “SOAP 기반의 홈 네트워크 구축을 위한 보안 프로토콜 설계및 구현”, 숭실대학교, 2006

[5] H.Schulzrinne, X. Wu, and S. Sidiroglou, "Ubiquitous Computing in Home Networks", IEEE comm. Mag. Oct. 2003.

[6] Zhuge, J.; Yao, R., "SC05-7 Security Mechanisms for Wireless Home Network", GLOBECOM-NEW YORK, VOL 3, 2003.