홈네트워크에서 인증서버를 이용한 사용자 인증 메커니즘

이윤경, 주홍일, 박지혜, 한종욱

한국전자통신연구원

User Authentication Mechanism Using Authentication Server in Home Network

Yun-kyung Lee, Hong-il Ju, Jee-Hye Park, Jong-wook Han

Electronics and Telecommunications Research Institute

E-mail : neohappy@etri.re.kr

요 약

안전한 홈네트워크를 위해서 사용자 인증은 가장 기본적인 요소이다. 사용자 인증을 통해서 권한을 가진 사람만이 홈네트워크를 이용할 수 있도록 하는 것이 필요하다. 사용자가 원하는 다양한 인증수단(ID/PW, 인증서, 생체정보 등)들 중 하나를 이용하여 사용자 인증이 가능하도록 함으로써 사용자 편의성을 얻을 수 있다. 또한 홈게이트웨이에 인증서버의 기능을 추가하여 사용자는 홈게이트웨이에만 인증을 받으면 홈게이트웨이, 즉 인증서버의 대리인증기능을 통해서 홈네트워크 서비스를 이용할 수 있다. 본 논문에서는 이러한 인증서버를 이용한 사용자 인증메커니즘에 관하여 기술한다.

ABSTRACT

User authentication is an essential component for secure home network service. It enables authorized persons to use the home network. Using of various authentication methods provides user convenience. To add to this, using of home gateway included of authentication server function enables that once users are authenticated in the home gateway, the users use all authorized home network service. It is possible by authentication agent of home gateway. This paper describes user authentication mechanism using authentication server.

키워드

사용자 인증 메커니즘, 홈네트워크, 인증서버, 홈네트워크 보안

Ⅰ. 서 론

정보통신 기술의 발달로 홈 내에서 각종 인터넷 컨텐츠를 이용할 수 있는 시대가 되었다. 다양한 인터넷 컨텐츠가 계속 개발되고 있으며, 이들 컨텐츠를 이용하기 위해서는 사용자 인증과정이 반드시 필요하다. 그러나 컨텐츠마다 사용자 인증을 위해서 요구하는 인증 수단이 다르고, 동일한 인증수단(예: ID/PW)을 요구하더라도, 각 컨텐츠마다 등록된 사용자 인증정보가 다르기 때문에, 사용하는 컨텐츠가 많아질수록 사용자가 기억해야 하는 자신의 인증정보는 그만큼 증가하게 된다. 그리고 Single-sign-on을 이용한다 하더라도계약을 맺은 컨텐츠 서버들 사이에서만 single-sign-on을 이용할 수 있기 때문에 결국 여러 개의 인증 정보를 기억하거나, 휴대하여야 한다. 이에 대한 해결책의 하나로 본 논문에서는 인증서버를 이용한 사용자 인증메커니즘을 제안하게 되었다.

홈네트워크는 완전히 새로운 네트워크 망이 아니라 기존의 네트워크 시스템을 축소해서 홈으로 가져온 것이라고 할 수 있다. 즉, 집안의 다양한 정보가전 기기들이 네트워크를 형성하여 서로 통신하고, 이들 네트워크가 외부 인터넷망과 연결되어 외부 사업자들이 제공하는 서비스를 댁내에서도 이용할 수 있는 것을 말한다. 그리고 우리는 홈네트워크를 통해서 좀더 편리하고, 안전한 생활을 영위할 수 있다. 예를 들어 댁외에서 댁내의

가스밸브를 잠근다거나, 전등을 켜고, 끌 수 있으며, 외출했다가 귀가할 때 보일러또는 에어컨을 댁외에서 미리 켜서 집안 온도를 조절해 둘 수도 있다. 또한 TV를 이용하여 인터넷 뱅킹을 할수도 있고, 양방향 디지털 TV로 TV를 보면서 쇼핑을 함께 할 수도 있으며, 병원에 가지않고, 댁내에서 간단한 진단 및 처방을받을 수도 있다. 이러한 환경을 구축하는 것이 홈네트워크의 목표이고, 홈네트워크를 이용하는 사람들의 안전과 프라이버시 보호를 위하여 홈네트워크 보안이 필요하다. 또한 이들 홈네트워크 서비스를 이용하기 위해서는 사용자 인증과정이 반드시 필요하게 되므로 사용자 인증메커니즘은 홈네트워크 보안의 가장 기본이 된다고 할 수 있겠다.

본 논문에서는 홈네트워크를 위한 사용자 인증 메커니즘을 제안하고자 한다. 본 논문에서 제안한 사용자 인증메커니즘은 홈네트워크 뿐만 아니라 일반 네트워크 시스템에서도 충분히 적용 가능하리라 본다.

II. 홈네트워크 모델링

본 논문에서 고려하는 홈네트워크 모델은 대부분의 사람들이 아파트 생활을 하거나 여러 개의 단독주택이 모여 사는 한국의 주택 구조에 가장 적합하다. 즉, 홈내부에서 연결된 통신망을 외부와 연결하기 위한 네트워크 망을 제공할 뿐만 아니라, 각종 홈네트워크 서비스를 제공하는 홈네트워크 사업자 서버가 있고, 사업자 서버는 각가정의 홈게이트웨이와 연결되어 있다. 홈게이트웨이는 댁내망과 댁외망을 연결하는 기능을 수행한다. 또한 홈게이트웨이는 홈서버의 기능을 함께 하고 있어서, 사용자 인증 및 접근제어 기능을 수행할 수 있을 뿐만 아니라, 홈게이트웨이의 고유 기능인 다양한 통신수단에 대한 브릿지 기능도 수행한다. 댁내의 모든 디바이스는 홈게이트웨이를 중심으로 연결되어 있어서, 사용자가 월패드, 웹패드, PDA, TV, 노트북 등의 클라이언트 기기를 이용하여 댁내 디바이스를 제어하기 위한 명령을 내리면, 이 명령을 홈게이트웨이에서 받아서, 해당 디바이스를 제어하는 구조이다.

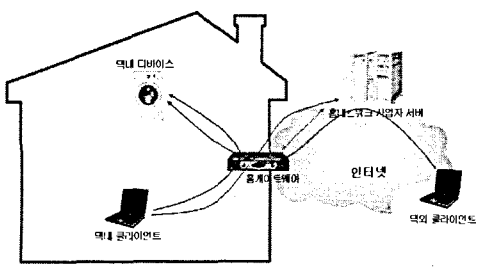

그림 1. 홈네트워크 모델링

그림 1에서 볼 수 있듯이 홈게이트웨이를 중심으로 모든 디바이스가 연결되고, 서비스가 이루어진다. 그리고 앞서 기술하였듯이 홈게이트웨이가 홈서버의 기능을 함께 수행하며, 홈서버는 인증서버의 기능을 포함하고 있다. 즉, 홈게이트웨이에서 홈네트워크 서비스에 대한 인증 및 접근제어 기능이 수행된다.

홈네트워크 서비스는 크게 세 가지로 구분할 수 있다: 댁내의 사용자가 댁내의 디바이스를 제어하고자 하는 경우, 댁내의 사용자가 홈네트워크 사업자 서버가 제공하는 서비스를 이용하는 경우, 댁외의 사용자가 댁내 디바이스를 제어하고자 하는 경우. 댁내의 사용자가 댁내의 디바이스를 제어하고자 하는 경우의 홈네트워크 서비스는 댁내의 사용자가 홈네트워크 서비스용 클라이언트 프로그램이 탑재된 클라이언트 기기(예 : 웹패드, 월패드, PDA, 노트북, PC 등)를 이용하여 댁내 기기의 제어 명령을 내리면, 이 명령을 받은 홈게이트웨이가 사용자를 인증하고, 해당 사용자가 기기에 대한 접근 권한이 있는 경우 댁내디바이스에 제어명령을 내려서 사용자가 원하는 제어 서비스가 이루어지는 서비스를 말한다. 그리고 댁내의 사용자가 홈네트워크 사업자 서버가 제공하는 서비스를 이용하는경우의 홈네트워크 서비스는 댁내의 사용자가 홈네트워크 서비스용 클라이언트 프로그램이 탑재된 클라이언트 기기를 이용하여 홈네트워크 사업자 서버가 제공하는 서비스 이용을 요청할 경우 홈게이트웨이에서 사용자 인증과 접근제어 기능을 수행한 후, 해당 서비스에 대한 접근 권한이 있을 때에만 사업자 서버와 연결되는 구조로 서비스가 이루어진다. 마지막으로, 댁외의 사용자가 댁내 디바이스를 제어하고자 하는 경우의 홈네트워크 서비스는 홈네트워크 서비스용 클라이언트 프로그램이 탑재된 기기를 이용하여 댁외에서 댁내의 특정 디바이스를 제어하고자 할 경우, 홈네트워크 사업자서버에 네트워크 접근 인증을 받은 후, 인증이 성공하면 홈게이트웨이에 연결되고, 사용자가 원하는 서비스(댁내 기기 제어명령)가 해당 홈게이트웨이로 전달되며, 사업자 서버가 넘겨준 사용자 인증 정보와 사용자가 요청한 서비스를 보고, 해당 사용자의 접근권한을 체크하여 접근권한이 있는 경우에 한해서 홈게이트웨이는 해당 댁내 디바이스로 제어 명령을 내리는 서비스이다. 이러한 홈네트워크 모델하에서 사용자를 인증하기 위한 인증 메커니즘을 다음 장에서 제안하고자 한다.

III. 인증 메커니즘

본 논문에서 제안하는 사용자 인증 메커니즘에서는 사용자를 인증하는데 있어서 사용자의 불편을 최대한 덜어주기 위하여 홈게이트웨이를 인증서버로 활용한다. 즉, 홈게이트웨이가 사용자 인증의 주체가 되기도 하고, 사용자 인증을 대리하는 기능도 한다.

댁내의 사용자가 댁내의 디바이스를 제어하고

자 할 경우 홈게이트웨이는 단순히 사용자 인증의 주체로써의 기능만을 수행한다. 즉, 사용자가 홈게이트웨이에 미리 등록해 둔 사용자인증정보들 중 사용자가 원하는 한 가지를 이용하여 홈게이트웨이에 인증을 받는다.

댁내의 사용자가 댁외의 홈네트워크 사업자 서버가 제공하는 서비스를 이용하고자 할 경우 홈게이트웨이는 사용자 인증 주체로써의 기능과 사용자 인증을 대리하는 기능을 모두 수행하게 된다. 즉, 사용자가 사업자 서버에 등록할 때 이용한사용자 인증정보를 홈게이트웨이에 함께 등록해둠으로써 사용자는 홈게이트웨이에 등록해둔 자신의 인증정보들 중 하나를 이용하여 홈게이트웨이에 인증을 받고, 홈게이트웨이는 사용자를 인증한 후 적절한인증정보를 이용하여 홈네트워크 사업자 서버와 사용자 인증과정을 수행하는 인증의 대리하는 기능을 수행한다. 그림 2는 댁내의 사용자가 댁외의 홈네트워크 사업자 서버가 제공하는 서비스를 이용하고자 할 경우의 인증 플로우를 보여준다.

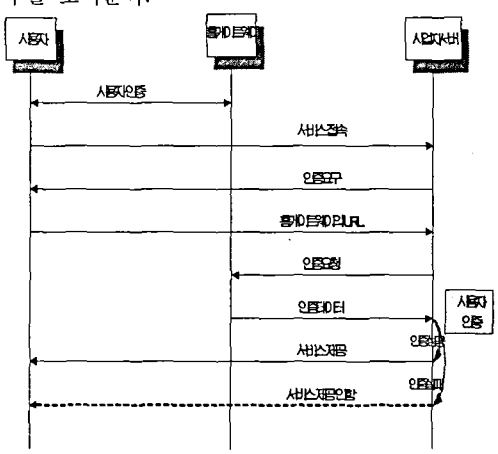

그림 2. 댁내의 사용자가 댁외의 서비스를 이용하고자 할 경우의 인증과정

댁내의 사용자는 홈게이트웨이에 먼저 사용자 인증을 받은 후, 홈네트워크 사업자 서버가 제공하는 서비스에 접속한다. 이때, 홈네트워크 사업자 서버가 사용자 인증을 요구하면 사용자는 홈게이트웨이의 URL 주소를 사업자 서버에 가르쳐주고, 사업자 서버는 그 URL(홈게이트웨이)에 접속하여 사용자 인증정보를 요구한다. 홈게이트웨이는 조금전에 자신에게 인증을 받은 사용자의 인증 정보를 사업자 서버에 제공하고, 사업자 서버는 그 정보를 이용하여 사용자를 인증하게 된다. 이때, 댁내의 사용자가 홈게이트웨이에 인증을 받을 때 자신의 인증정보를 제공해줄 것을 요청하는 사업자 서버의 정보도 함께 주어야 엉뚱한 곳에 사용자 정보를 제공하는 것을 막을 수 있다.

댁외의 사용자가 댁내의 디바이스를 제어하고자 할 경우 홈게이트웨이는 댁내의 사용자가 댁외의 홈네트워크 사업자 서버가 제공하는 서비스를 이용하고자 할 경우와 마찬가지로 사용자 인증 주체로써의 기능과 사용자 인증을 대리하는 기능을 모두 수행한다. 댁외의 사용자가 원하는 홈게이트웨이에 접근하여 댁내의 디바이스를 제어하고자 할 때, 먼저 홈네트워크 사업자서버에 네트워크 접근 인증을 받아야 하는데, 이 과정에서 사용자가 직접 홈네트워크 사업자서버에 인증을 받을 수도 있고, 홈게이트웨이의 URL 정보를 홈네트워크 사업자서버에 알려줌으로써 홈게이트웨이에 자신의 인증을 대리해줄 것을 요청하여 네트워크 접근인증을 받을 수도 있다. 사용자가 홈게이트웨이에게 자신의 인증을 대리해줄 것을 요청할 때, 사용자는 홈게이트웨이에 먼저 인증을 받아야 한다.

댁외의 사용자가 댁내의 디바이스를 제어하고자 할 경우에는 먼저 사업자 서버에 접속하여 네트워크 접근 인증을 받아야 한다. 사용자가 홈네트워크 사업자 서버에 접속하여 자신의 집의 홈게이트웨이에 접근하고자 하면 먼저 사업자 서버가 인증을 요구하고, 이때 사용자는 자신의 인증정보가 등록된 홈게이트웨이의 URL 주소를 알려준다. 그러면 사업자 서버는 임시로 홈게이트웨이와 사용자 사이에 네트워크를 연결해 주고, 홈게이트웨이와 사용자 사이에 사용자 인증이 가능하도록해준다. 댁외의 사용자가 홈게이트웨이에 접속하여 사용자 인증을 받은 후, 자신의 인증정보를 전해줄 사업자 서버를 알려주면 홈게이트웨이는 홈네트워크 사업자 서버의 인증요청 메시지에 응답하여 해당 사용자의 인증정보를 전해준다. 사업자 서버는 사용자 인증정보를 이용하여 해당 사용자를 인증하고, 인증이 성공하면 홈게이트웨이와 사용자 사이의 네트워크 연결을 유지하고, 인증이 실패하면 네트워크 연결을 끊음으로써 사용자가 홈게이트웨이에 접근하여 댁내 디바이스를 제어할 수없도록 한다.

IV. 일반 네트워크에 대한 응용

3장에서 기술한 홈네트워크에서의 사용자 인증 메커니즘을 홈네트워크가 아닌 일반 네트워크에서 적용할 수 있다. 홈게이트웨이를 믿을만한 인증서버라고 가정하면, 사용자는 자신의 인증정보들을 인증서버에 저장해 두고, 사용자가 컨텐츠를 이용하고자 할 때 특정 컨텐츠에 대한 인증정보를 사용자 대신 인증서버가 제공하도록 하여, 사용자가 그 컨텐츠를 이용할 수있도록 한다. 이를 위해서 사용자는 특정 컨텐츠 서버에 등록할 때 사용한 자신의 인증정보를 인증서버에 등록하고, 인증서버의 데이터베이스에는 특정 컨텐츠 서버에 등록할 때 사용한 인증정보를 등록해두고, 인증서버의 데이터베이스에는 특정 컨텐츠 서버에

대한 사용자 인증정보와 함께 자신의 인증정보를 컨텐츠 서버에 제공할지 여부를 저장해 둔다. 사용자는 컨텐츠 서버에 접속하기에 앞서 인증서버와 먼저 사용자 인증을 수행하고, 인증이 성공하였을 때, 컨텐츠 서버에 접속하여 컨텐츠 이용을 시도한다. 컨텐츠 서버가 사용자 인증정보를 요구할 때 사용자는 자신의 인증정보가 등록된 인증서버의 위치(URL 주소 등)를 컨텐츠 서버에 알려주고, 컨텐츠 서버는 해당 인증서버에 접속하여 사용자 인증을 수행한다. 사용자 인증이 성공적으로 끝나면 컨텐츠 서버는 해당 컨텐츠를 제공하고, 사용자 인증에 실패하면 컨텐츠 서버는 사용자와의 접속을 끊게된다. 사용자와 인증서버, 컨텐츠 서버 사이의 인증과정은 그림 3에 나타나있다.

그림 3과 같은 인증 메커니즘에서 인증서버에 저장된 사용자 정보는 해당 사용자만이 조회, 수정, 입력 가능하여야 할 것이다. 또한 인증서버는 사용자를 인증한 후 사용자가 자신의 인증정보 제공을 동의한 컨텐츠 서버에 대해서 특정 시간 이내에만 컨텐츠 서버에 사용자 인증정보를 제공해야 한다.

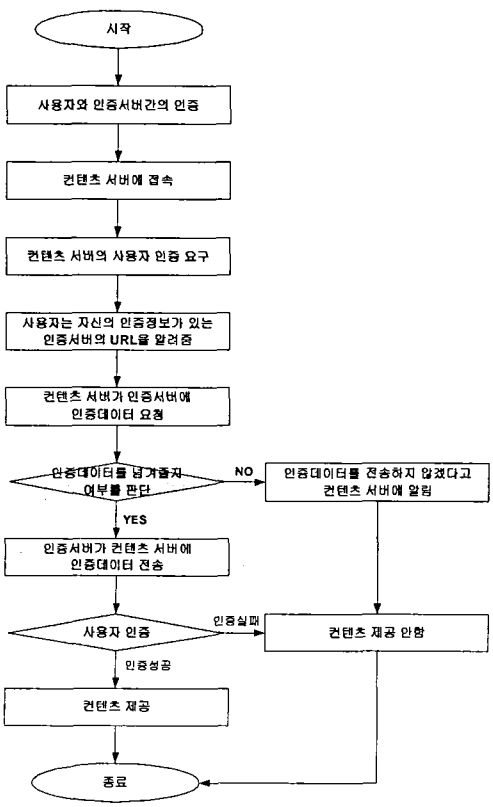

그림 3. 인증서버를 이용한 사용자 인증 과정

V. 결 론

본 논문에서는 홈네트워크에서 사용자 편의성을 고려한 사용자 인증 메커니즘을 제안하였다. 또한 본 논문에서 제안한 인증 메커니즘은 홈네트워크가 아닌 일반 네트워크에서도 충분히 적용가능함을 보였다. 본 논문에서 제안한 인증메커니즘을 적용하면 사용자가 홈네트워크 사업자 서버를 비롯한 다양한 컨텐츠 서버에 등록한 자신의 인증정보를 모두 기억할 필요가 없고, 사용자 단말은 홈네트워크 사업자 서버 혹은 컨텐츠 서버와 사용자 인증과정을 수행하기 위해서 필요한 인증메커니즘을 탑재할 필요가 없기 때문에 경량화된 사용자 단말을 구현할 수 있다. 또한 생체정보 같은 중요한 인증정보를 홈네트워크 사업자 서버와 컨텐츠 서버에 노출하지 않고, 안전한 인증 서버에만 저장함으로써 개인 프라이버시를 보호할 수 있다. 그리고, 사용자는 인증서를 이용한 사용자 인증을 요구하는 홈네트워크 사업자 서버와 컨텐츠 서버에 접속하기 위해서 인증서를 휴대하고 다녀야 하는 불편을 없앨 수 있다는 장점이 있다.

참고문헌

[1] Carl M. Elliso, "Home Network Security", Intel Technology, Spring 2002.

[2] 한종욱, 김도우, 주홍일, 이윤경, 남택용, 장종수, "홈네트워크 보안프레임워크 구축을 위한 고려사항", 한국정보처리학회지, 2004

[3] Guoyou He,"Requirements for Security in Home Environments," Residential and virtual Home Environments Seminar on Internetworking, Spring 2002