홈 네트워크 접근 제어 모델에 관한 연구

김건우*, 김도우, 이준호, 황진범, 한종욱

*한국전자통신연구원

A study on Access Control Model for Home Network

Geon-woo Kim* · Do-woo Kim, Jun-ho Lee, Jin-beon Hwang, Jong-wook Han

*Electronics and Telecommunications Research Institute

E-mail : kimgw@etri.re.kr

요 약

다양한 이동 기술, 센서, 원격 제어 및 인프라가 발달하고 생활의 질에 대한 기대치가 높아짐에 따라 홈 네트워크에 관한 다양한 기술과 서비스에 관한 연구과 개발이 진행되고 있다. 현재까지는 사용자에게 높은 수준의 홈 네트워크 서비스 개발에 중점을 둔 반면에, 이의 안전성을 보장하는 홈 네트워크 보안에 관해서는 많은 연구가 이루어지지 않고 있는 실정이다. 따라서 본 논문에서는 다양한 사용자가 각자의 특성과 취향에 맞는 홈 네트워크 서비스를 제공받을 수 있고, 외부의 불법 접근이나 침입으로부터 홈 네트워크 시스템을 안전하게 보호하기 위한 홈 네트워크 접근 모델을 제안하고자 한다.

ABSTRACT

As various mobile technologies, sensor technologies, remote control and infrastructure are developing and expectations on quality of life are increasing, a lot of researches and developments on home network technologies and services are actively on going. Until now, we focused on how to provide users with high-level home network services, while not many researches on home network security for guaranteeing safety are progressing, So, in this paper, we propose an access control model for home network that provides various users with home network services up one's characteristics and features, and protects home network systems from illegal accesses or intrusions.

키워드

홈 네트워크 보안, 인증, 접근 제어, 보안 정책

Ⅰ. 서 론

홈 네트워크는 이동통신, 초고속 인터넷 등 유·무선 통신 네트워크를 기반으로 가정 내의 A/V, 데이터통신 및 정보가전 기기들이 네트워크로 상호 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스를 제공받을 수 있는 가정 환경을 구축하여 국민들에게 편리하고, 안전하고, 즐겁고, 윤택한 삶을 제공할 수 있는 새로운 IT 기술 이용 환경이라 할 수 있다[1].

홈 네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버 공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, 서비스 거부 공격, 통신망 도·감청 등에 보안 취약성을 내포하고 있다[2]. 또한 정상적인 홈 네트워크 사용자일지라도 사용자의 권한과 특성을 고려해서 서로 다른 서비스를 제공해야 할 필요성이 있다.

따라서 본 논문에서는 홈 네트워크에서의 취약성을 제거하고 안전성을 확보하며, 사용자 레벨의 보다 다양한 서비스를 제공하기 위한 접근 제어 모델을 제시하고, 수반되어야 하는 기반 보안 기

술을 제안한다.

II. 본 론

안전하고 다양한 레벨의 홈 네트워크 서비스를 제공하기 위해서는 사용자 인증, 접근 제어 및 이를 관리하기 위한 보안 정책 관리 기능 등이 필요하다. 강력하고 효율적인 사용자별 접근 제어는 사용자 인증 정보를 기반으로 동작하며, 홈 네트워크 관리자는 각 가정의 특성을 고려한 접근 제어 정책을 설정한다.

본 논문에서 제안하는 홈 네트워크 보안 모델은 홈 게이트웨이를 기반으로 동작한다.

그림 1은 홈 네트워크 보안을 위한 컴포넌트를 도식화한 그림이다.

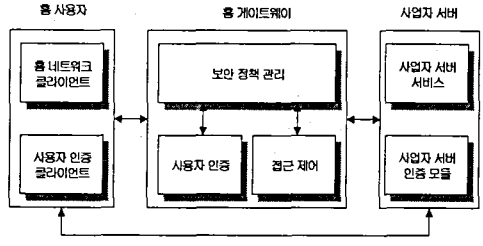

그림 1. 홈 네트워크 보안 컴포넌트

홈 네트워크 시스템은 크게 홈 네트워크 클라이언트, 홈 게이트웨이 및 사용자 서버로 구성되며, 제어 대상인 홈 디바이스와 홈 네트워크 서비스가 추가될 수 있다.

홈 네트워크 클라이언트는 댁내는 물론 댁외에서도 사용이 가능하며, 휴대가 간편하고 사용이 용이해야 한다. 댁내에서 사용 가능한 홈 네트워크 클라이언트로는 DTV, PC, Wall-Pad, Mobile Phone 등이 있으나 일반적으로 IP 기반 TV를 중심으로 개발되고 있다. 이러한 홈 네트워크 클라이언트는 홈 네트워크 서비스를 위한 인터페이스 기능과 사용자 인증 기능을 제공해야 한다.

홈 게이트웨이는 홈 네트워크 보안의 핵심 모듈로서, 사용자 인증, 접근 제어 및 보안 정책 관리 기능을 제공하며, 각 호별로 설치된다.

사업자 서버는 각 홈 네트워크 서비스 제공자별로 동작하며 기존 인증 방식을 고수한다.

2.1 인증

인증 방식은 크게 디바이스 인증과 사용자 인증으로 구분될 수 있다. 디바이스 인증 방식은 홈 클라이언트를 포함하는 홈 디바이스와 홈 게이트웨이 사이에서 발생하는 인증 방식으로 사용과 관리가 용이해서 현재 많이 사용되고 있는 방식이다. 하지만 추후 다양해지는 홈 네트워크 서비스를 제공하기에는 한계를 가지며, 효율적인 접근 제어를 보장하지 못한다. 또한 홈 디바이스 분실이 발생하면 예상치 못한 문제가 발생할 수도 있다. 따라서 본 논문에서는 이러한 단점을 보완하기 위해서 사용자 인증 방식을 채택하고 있다. 사용자 인증 방식은 디바이스 인증 방식에 비해서 사용자 개입이 필요하다는 단점이 있지만, 차별화된 다양한 서비스를 제공받고자 하는 욕구를 충족시킬 수 있다. 다만 안전성과 용이성을 어떻게 확보할 수 있는가 하는 것이 관건이다.

홈 네트워크 특성을 고려하면, 다양한 연령과 특성을 가진 사용자가 존재할 수 있다. 디지털 방식에 익숙하지 않는다거나, 사용자 인증과 홈 네트워크 서비스를 사용하는데 많은 어려움을 겪을 수도 있다. 따라서 모든 홈 네트워크 사용자를 고려해서 각자의 취향에 맞는 인증 방식을 사용할 수 있도록 다양한 사용자 인증 방식을 채택하고 있다. 이는 ID/Password 방식, 인증서 방식, 생체 방식, 및 RFID 등을 이용한 방식이 있다.

그림 2는 이러한 다양한 인증 방식을 제공하는 통합 인증 메커니즘을 나타낸다.

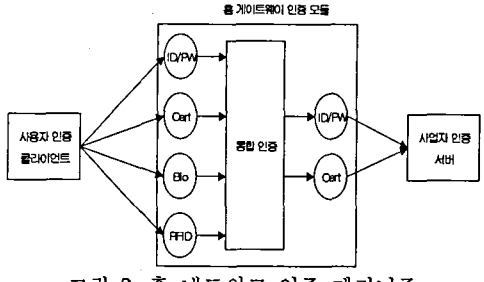

그림 2. 홈 네트워크 인증 메커니즘

기존의 홈 네트워크 사업자 서버는 ID/Password 인증 방식이나 인증서를 사용한 인증 방식만을 고수해서 사용하는 경향이 있다. 즉, 사용자가 채택하는 생체 인증 방식, RFID를 통한 인증 방식은 사업자 서버와 연동할 수 없기 때문에, 자동 매핑을 담당하는 통한 인증 모듈이 필요하다. 이를 통해 홈 게이트웨이는 사업자 서버와 홈 네트워크 사용자에 상호 인증 방식에 대한 투명성을 보장하며, 사용자 개입을 최소화한 인증 메커니즘을 제공할 수 있다.

2.2 접근 제어

보다 다양하고 차별화된 서비스를 제공하기 위해서는 각 사용자별 인증이 선행되어야 하며, 이를 기반으로 실시간 접근 제어가 가능해야 한다. 이를 통해서 내·외부의 불법 접근을 차단하고, 비록 정당한 사용자일지라도 불필요한 접근을 제어하기 때문에, 시스템의 안전성과 효율성을 극대화할 수 있다.

그림 3은 접근 제어 모델을 나타낸다.

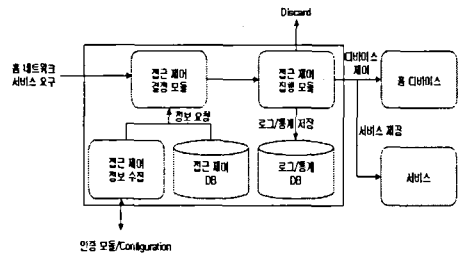

그림 3. 홈 네트워크 접근 제어 모델

홈 네트워크 접근 제어 모델은 접근 제어 결정 모듈, 접근 제어 집행 모듈, 접근 제어 정보 수집 모듈, 접근 제어 DB, 및 로그/통계 DB로 구성된다.

홈 네트워크 사용자로부터 서비스 요구가 오면, 접근 제어 결정 모듈은 접근 제어 결과를 접근 제어 집행 모듈에 통보한다. 접근 제어를 결정하기 위해서 우선 인증 모듈과 연동해서 사용자 정보를 취득하고, 다양한 환경 정보를 수집한 후, 서비스 타입과 더불어 접근 제어 DB를 검색하는 키로서 사용한다. 결과를 기반으로 접근 제어 집행 모듈은 해당 홈 디바이스를 제어하거나 서비스를 제공하며, 접근이 허용되지 않으면 그 결과를 통보하고 로그로 기록한 수 요청을 폐기한다.

2.2.1 접근 제어 DB

접근 제어를 위한 데이터베이스는 xPSL(eXtensible Policy Specification Language) 언어 체계를 따른다. xPSL은 XML을 기반으로 하며, 홈 네트워크를 위한 최적화된 언어이다.

실제로 접근 제어 DB는 보안 정책 관리 시스템에서 설정되어 저장되며, 이들 간에는 TLS와 같은 안전한 통신 방식을 통해서 연동한다.

그림 4는 접근 제어 DB와 이를 위한 연동 구조를 보여준다.

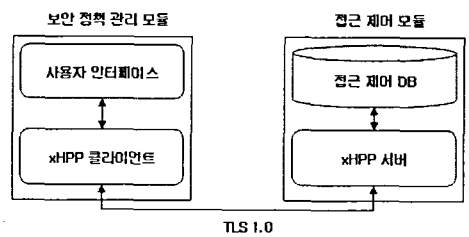

그림 4. 접근 제어 DB 관리

xHPP 프로토콜은 보안 정책 관리 모듈과 접근 제어 모듈간 연동을 위해서 제안된 프로토콜로서 다음과 같은 기능을 포함해야 한다.

- 보안 정책 요청 및 응답
- 보안 정책 설정 요청 및 응답
- 홈 디바이스 상태 요청 및 응답
- 로그/통계 정보 수집 요청 및 응답
- 인증서 요청 및 응답

각 홈 게이트웨이에 설치되는 접근 제어 DB는 이를 사용하는 사용자의 수와 정책의 복잡도에 따라, 용량이 결정된다. 따라서 다양한 홈 구성원을 고려하면, 확장성과 효율성을 지원하기 위해서 NIST에서 제안한 RBAC(Role-basec Access Control) 방식을 사용한다. RBAC 은 ACL(Access Control List)과 달리 Role이라는 컴포넌트를 사용해서 사용자와 홈 디바이스/서비스의 관계를 정의하는 방식으로서, 복잡하거나 대규모의 접근 제어 모델에서 사용되는 방식이다.

2.2.2 접근 제어 결정

접근 제어 결정 모듈은 홈 네트워크 사용자로부터 서비스를 요청받으면, 기반 정보를 바탕으로 접근 허가 여부를 결정하는 모듈이다.

이를 나타낸 그림은 그림 5와 같다.

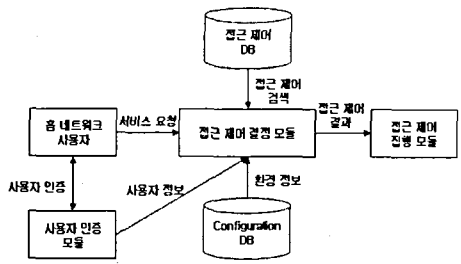

그림 5. 접근 제어 결정 모듈

접근 제어 결정 모듈은 서비스를 요청받으면, 우선 사용자 인증 과정을 거친 후 사용자 정보를 수신한다. 또한 이미 설정되어 있는 환경 정보와 접근 제어 정책을 검색해서 접근 여부를 결정한 후, 그 결과는 접근 제어 집행 모듈에 전송한다.

2.2.3 접근 제어 집행

접근 제어 집행 모듈은 접근 제어 결정 모듈로부터 접근 제어 결과를 수신해서, 집행하는 모듈이다.

접근 제어 집행 모듈은 그림 6과 같다.

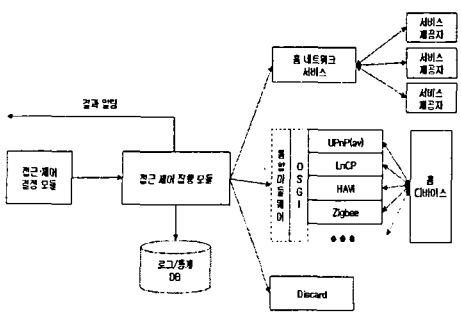

그림 6. 접근 제어 집행 모듈

접근 제어 집행은 요청하는 서비스의 타입과 접근 제어의 결과에 따라서 3가지 형태로 구분될 수 있다. 먼저 홈 디바이스를 제어하고자 하는 경우, 현재 개발 중인 통합 미들웨어나 OSGi와 연동해서 각 홈 디바이스를 제어하며, 서비스인 경우, 홈 네트워크 서비스 제공자가 제공하는 컨텐츠를 이용할 수도 있다. 또한 접근 제어 결과에 따라서 요청을 폐기 처분하고, 그 결과는 로그/통계 DB에 저장한다.

로그 DB는 syslogd과 같은 기존의 로그 데몬을 사용하거나 별도의 로그 파일을 구성할 수도 있다.

2.3 보안 정책 관리

각 호별로 설치되어 있는 홈 게이트웨이의 보안 정책을 설정하고 관리하기 위한 모듈로서, 별도의 디바이스에 설치할 수도 있다. 다만 이에 대한 접근은 엄격히 통제되어야 하며, 홈 게이트웨이의 모든 접근 제어와 상황 인지 기반 정책은 보안 정책 관리 모듈을 통해서만 관리되어야 한다. 그림 7은 보안 정책 관리 모듈의 구성을 나타낸다.

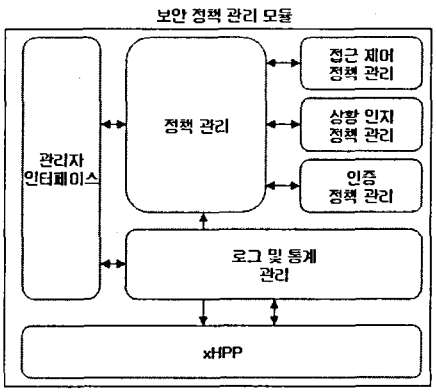

그림 7. 보안 정책 관리 모듈

보안 정책의 기능은 크게 관리자 인터페이스, 정책 관리 기능, 로그 및 통계 관리 기능, 홈 게이트웨이와의 연동을 위한 xHPP 프로토콜로 구성된다. 관리하는 보안 정책은 다시 접근 제어 정책, 상황 인지 정책 및 인증 정책으로 구분되어 홈 게이트웨이에 적용된다.

III. 결 론

홈 네트워크 서비스는 사용자에게 편리한 홈 디바이스를 통해서 개인의 특성에 맞는 다양한 서비스를 용이한 방식으로 제공하는데 그 목적이 있다고 할 수 있다. 하지만 이러한 홈 네트워크의 편리성은 안전성을 보장하지 못하면, 자칫 예상치 못한 결과를 초래할 수도 있다.

따라서 본 논문에서는 각 호별 홈 게이트웨이를 기반으로 동작하는 접근 제어 모델을 제안한다. 이를 댁·내외 불법 접근으로부터 홈 네트워크 시스템을 안전하게 보호하기도 하지만, 불필요한 서비스로의 접근을 사전에 차단하는 기능도 제공한다. 즉, 다양한 홈 네트워크 사용자의 특성을 고려할 때, 모든 사용자가 동일한 권한을 부여받을 필요는 없을 것으로 보여 지며, 각 사용자의 특성과 역할에 맞는 권한을 부여받는 것이 바람직하다.

즉, 각 사용자의 특성과 기호에 맞는 사용자 인증 과정을 거친 후, 이 정보와 서비스를 기반으로하는 실시간 접근 제어 서비스를 제공하고자 한다. 각 접근 제어 정책은 보안 정책 관리 모듈에 의해서 설정되고 분배되며, 확장성과 효율성을 고려해서 RBAC을 기반으로 한다.

참고문헌

[1] 김정원, 정보통신부, "홈 네트워크 산업 활성화 정책 방향", 정보과학회지, 2004, 09, 제 22권 제 9호 통권 제 184호

[2] 한종욱, 김도우, 주홍일, 한국전자통신연구원, "홈 네트워크 보안 프레이워크 구축을 위한 고려사항", 정보과학회지 2004, 09, 제 22권 제 9호 통권 제 184호