홈게이트웨이 기반 홈네트워크 접근제어 메커니즘

김건우*, 김도우, 이준호, 황진범, 한종욱

*한국전자통신연구원

Home Gateway-based Home Network Access Control Mechanism

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 통신 기술, 센서, 원격 제어 및 네트워크 인프라가 발달하고 생활의 질에 대한 기대치가 높아짐에 따라 홈네트워크에 관한 다양한 기술과 서비스에 관한 연구와 개발이 활발히 진행되고 있다. 홈네트워크 기술은 아직까지는 초기 투자 단계로서 사용자에게 필요한 서비스를 개발하고 편리성을 증대시키는 방향으로 개발되고 있지만, 더욱 서비스가 활성화되면 편리성을 보장할 수 있는 안전성에 관한 연구가 병행되어야 할 것이다. 따라서 본 논문에서는 내/외부의 불법 접근 및 허가되지 않은 접근으로부터 홈네트워크 시스템을 안전하게 방어하고 보호하기 위한 접근 제어 메커니즘을 제안한다.

ABSTRACT

As various mobile technologies, sensor technologies, remote control and network 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, home network is just beginning, and we are developing home network services necessary to users, incrementing easiness, however we need to research on the safety of home network system guaranteeing the easiness as the services are going actively. So, in this paper, we propose the access control mechanism for protecting the home network system against indoor/outdoor illegal accesses and unauthorized accesses.

키워드

홈네트워크 보안, 접근 제어, 보안 정책

Ⅰ. 서 론

홈네트워크는 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].

홈네트워크는 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 홈네트워크 사용자일지라도 사용자의 권한과 특성을 고려해서 서로 다른 서비스를 제공해야 할 필요성이 있다.

따라서 본 논문에서는 각 댁내마다 설치되어 있는 홈 게이트웨이를 기반으로 모든 홈네트워크

서비스를 제어하기 위한 실시간 접근 제어 메커니즘을 제안한다.

II. 본 론

홈네트워크 서비스의 다양성과 편리성의 보장하기 위해서는 안전성을 강화하는 것이 중요하다. 홈네트워크 서비스는 원격으로 디바이스를 제어하거나 서비스를 제공하기 때문에, 다양한 사용자 인증 기술을 필요로 하며, 더불어 접근 제어와 같은 강력한 홈네트워크 보호 메커니즘을 구현할 필요가 있다.

접근 제어 방식으로는 임의적 접근 제어 방식(DAC: Discretionary Access Control), 강제적 접근 제어 방식(MAC: Mandatory Access Control) 및 역할기반 접근 제어 방식(RBAC: Role-based Access Control) 등이 있다. 비교적 규모가 크거나 다양한 접근 제어를 효율적으로 수행하기 위해서는 일반적으로 RBAC 방식이 널리 사용되고 있으며, 본 논문에서도 RBAC 방식을 사용한다.

그림 1은 홈 게이트웨이를 기반으로 동작하는 홈네트워크 시스템 접근 제어 메커니즘의 구성을 보여주고 있다.

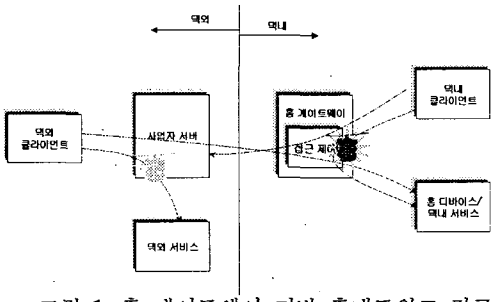

그림 1. 홈 게이트웨이 기반 홈네트워크 접근 제어 구조

홈네트워크 시스템은 크게 홈 게이트웨이, 사업자 서버, 홈 클라이언트(댁내/댁외), 및 홈 디바이스/서비스로 구성된다.

모든 접근 제어는 닥 댁내마다 설치되어 있는 홈 게이트웨이에서 수행된다. 본 논문에서 제시하는 접근 제어 정책은 각 댁내 사용자를 기반으로 동작하며, 각 호별 또는 단지별로 접근 제어를 수행하기 위해서는 사업자 서버에서 동작할 수도 있다. 하지만 본 논문에서는 홈 게이트웨이에서 수행되는 접근 제어만을 고려한다.

2.1 RBAC

기존의 임의적 접근 제어 방식(DAC)이나 강제적 접근 제어 방식(MAC)에서 subject와 resource 간의 직접적인 관계를 규정한데 반해, RBAC 방식은 subject와 resource 사이에 Role이라는 새로운 컴포넌트를 두어, 이 Role을 통해서 다 컴포넌트간의 관계를 간접적으로 규정한다. 따라서 네트워크 규모가 커지고 접근 제어가 복잡해짐에 따라 적은 overhead가 발생하고 효율적으로 관리할 수 있는 장점을 가지고 있어 널리 사용되고 있는 방식이다.

그림 2는 RBAC 구성을 보여준다.

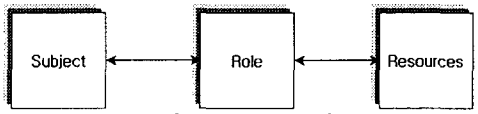

그림 2. RBAC 구성

홈네트워크 시스템은 다양한 사용자와 이들이 사용할 수 있는 다양한 홈 디바이스/서비스들이 존재하며, 이들 간의 접근 권한 연관 관계는 RBAC 메커니즘을 통해서 정의된다.

즉, 접근 하고자 하는 주체(Subject)는 각 홈네트워크 사용자, 대상(Resource)은 홈네트워크 사업자가 제공하는 홈 디바이스나 서비스 등이 될 수 있다.

따라서 RBAC 모델이 적용된 홈네트워크 접근 제어 구성의 예를 보면 그림 3과 같다.

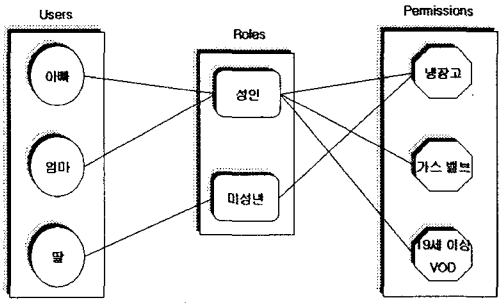

그림 3. RBAC 구성 예

그림 3에서 보는 바와 같이, 엄마와 아빠는 성인이라는 Role에 포함되어 있기 때문에는 모든 Permission을 가질 수 있는데 반해, 딸은 미성년 Role에 포함되어 있어 가스밸브와 19세 이상 VOD 서비스를 제공받을 수 없다.

접근 권하는 각 댁별로 별도로 관리하며, 권한을 가지는 사용자(예, 아빠)에 의해서 임의로 수정될 수 있기 때문에, MAC 메커니즘을 통해서 효율적으로 관리할 수 있다.

2.2 홈 게이트웨이 접근 제어

홈 게이트웨이를 경유하는 홈네트워크 서비스에 대한 접근 제어 메커니즘에 대해서 설명한다. 예를 들어 댁내=>댁내 서비스, 댁내=>댁외 서비스, 댁외=>댁내 서비스 등이 해당되며 미리 정해진 접근 제어 정책에 의해서 제어된다.

홈 게이트웨이에서 발생하는 모든 접근 제어는

사용자 인증 정보를 기반으로 하기 때문에, 사용자 인증 과정이 선행되어야 한다.

그림 4는 홈 게이트웨이에서 수행되는 보안 모듈의 구성을 보여주고 있다.

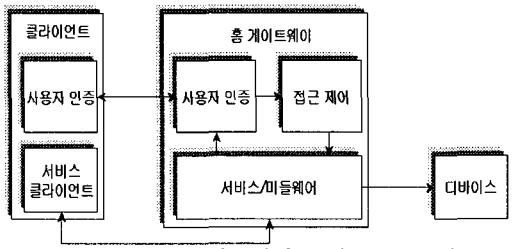

그림 4. 홈 게이트웨이 보안 모듈 구성

사용자가 댁내/외 클라이언트를 통해서 디바이스를 제어하거나 서비스를 제공받기 위해서 홈 게이트웨이에 접속하면, 홈 게이트웨이는 우선 사용자를 검증하기 위한 사용자 인증 모듈을 수행한다. 사용자 인증 과정이 성공적으로 수행되면, 사용자 인증 정보과 접근 하고자 하는 대상(디바이스, 서비스)을 기반으로 접근 제어 메커니즘을 수행해서 그 결과를 서비스 모듈에 제공한다. 따라서 서비스 제공 모듈은 접근 제어 결과를 바탕으로 서비스 제공 여부를 판단한다.

그림 5는 홈 게이트웨이에서 수행되는 접근 제어의 구성을 보여 준다.

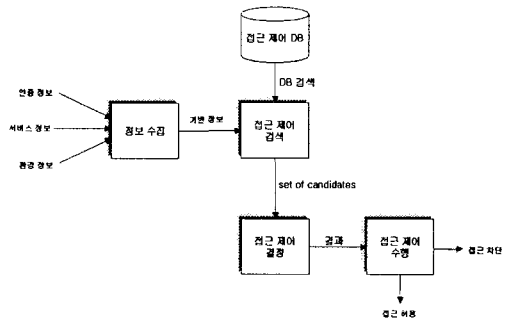

그림 5. 접근 제어 구성

접근 제어 정보 수집 모듈은 사용자 인증 정보, 접근 하고자 하는 대상 정보 및 접근 제어 판단에 영향을 미칠 수 있는 로그 정보 등을 분석해서 기반 정보를 구성한 후 접근 제어 검색 모듈에 제공한다. 접근 제어 검색 모듈은 이를 기반으로 접근 제어 DB를 검색해서 해당하는 모든 정책을 접근 제어 결정 모듈에 제공한다. 여러 접근 제어 정책 중 하나만을 선택하는 것은 접근 제어 결정 모듈의 기능이며, 미리 설정된 상위 보안 정책을 기반으로 한다. 접근 제어 수행 모듈은 접근 제어 결과를 반영해서 접근을 차단하거나 허용한다.

접근 제어 DB는 다양한 상용 데이터베이스를 사용하거나 상용 홈 게이트웨이의 사양을 고려해서 파일 시스템을 사용할 수 있다. 본 논문에서는 파일 시스템 방식을 사용하며, 저장 문법은 xHDL(eXtensible Home security Description Language) 언어를 사용한다.

2.3 사업자 서버 접근 제어

홈 게이트웨이를 거쳐지 않는 서비스(댁외=>댁외)에 대한 실시간 접근 제어를 수행하는 모듈로서, 다음과 같은 기본 요구사항을 만족할 수 있어야 한다.

- 홈 게이트웨이 기반 접근 제어
- 기존 사업자 서버 흐름을 그대로 유지
- 사업자 서버의 역할 최소화

위와 같은 요구사항을 만족하는 사업자 서버 접근 제어 모듈은 그림 7과 같다.

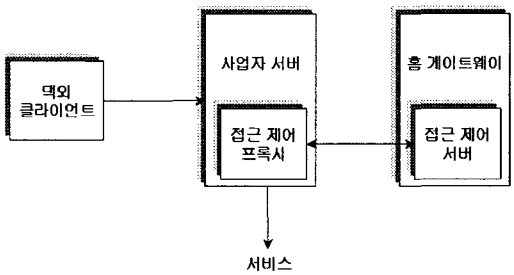

그림 7. 사업자 서버 접근 제어

사업자 모듈은 접근 제어 정책과 서버 기능을 포함하지는 않지만, 홈 게이트웨이를 거치지 않는 서비스 접근에 대해서는 접근 제어 프록시를 통해서 접근 여부를 결정하는 기능을 지원한다.

2.4 xHDL

접근 제어를 포함하는 보안 정책을 기술하기 위한 언어로서 XML 문법을 사용하며, 홈네트워크 접근 제어 정책을 표현하는데 효율적인 문법 구성을 지원한다.

xHDL을 구성하는 element을 보면 다음과 같다.

- user element
- object element
- object-group element
- role element
- rule element

이들 각각의 element들은 해당하는 홈네트워크 컴포넌트들을 정의하며, role element는 접근 제어 정책을 기술하고, rule element는 보안 정책을 기술한다.

그림 6은 xHDL을 구성하는 element간의 연관관계를 규정한다.

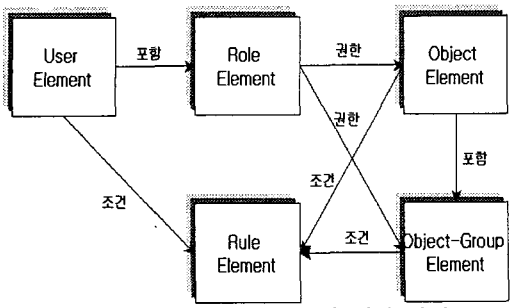

그림 6. xHDL element 간 연관 관계

Role element는 접근 제어를 위한 핵심 element로서 user element를 포함하고 object element와 object-group element에 대한 권한을 가짐으로써 user와 object간의 접근 권한 관계를 간접적으로 규정한다. rule element는 user element, object element, object-group element를 조건으로 검사한 후, 정의된 보안 정책을 수행한다.

III. 결 론

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

홈네트워크 사업은 현재 시범 사업을 끝내고 본격적인 서비스 제공을 본격화하고 있는 시작 단계로서, 서비스의 안전성을 지원할 수 있는 방안에 관한 연구와 대안이 아직 미흡한 실정이다.

따라서 본 논문에서는 각 호별 홈 게이트웨이를 기반으로 동작하는 접근 제어 메커니즘을 제안한다. 즉, 홈 게이트웨이가 각 서비스 접근 권한을 제한함으로써 내/외부로부터의 불법 접근을 차단하고 불필요한 서비스 사용을 제한함으로써 안전성을 확보할 수 있다.

또한, 홈 게이트웨이를 거치지 않는 서비스는 사업자 서버의 접근 제어 프록시 기능을 통해서 실시간으로 접근 권한을 제어할 수 있다.

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