홈 네트워크 서비스를 위한 RBAC 기반의 접근제어 시스템의 설계

김도우*·김건우*·이준호*·한종욱*
*한국전자통신연구원

Design of Access Control System based RBAC for Home Network Services

Do-Woo Kim*·Geon Woo Kim*·Jun-Ho Lee*·Jong-Wook Han*
*Electronics and Telecommunications Research Institute
E-mail : dwkim@etri.re.kr

요 약

홈 네트워크 환경은 기업과 공공기관의 네트워크 환경과 달리 다양한 유무선 네트워크 기술의 사용, 미들웨어와 프로토콜의 혼재, 댁내 정보가전기기의 제한적인 시스템 자원, 댁내 사용자의 보안 인식 부족 등으로 인하여 홈 네트워크에 연결된 홈 디바이스나 홈서비스는 공격에 의한 보안취약성을 가진다. 따라서 홈 네트워크 환경에서 신뢰할 수 있는 서비스를 제공하기 위해 보안은 상당히 중요한 요소이다. 본 논문에서는 안전한 홈 네트워크 서비스를 제공하기 위한 RBAC 기반의 접근제어 시스템을 설계하고자 한다.

ABSTRACT

Compared to corporation and government networks, home devices and services connected in a home networks has security threats because of the use of various wired and wireless network, middleware and protocol in digital home environment, a restricted system resource of home information appliances and the users who do not care about security. So security is critical element to provide secure services in a home network environments. In this paper we design the access control system based on RBAC to offer secure home network services.

키워드
Home Network, RBAC, Access Control

Ⅰ. 서 론

현재 홈 네트워크 기술은 홈네트워킹 기술과 미들웨어 기술 등 다양한 기술들이 활발히 연구 및 제안되고 있으며, 표준화 작업도 진행되고 있다.

홈 네트워크 환경은 기업과 공공기관의 네트워크 환경과 달리 다양한 유무선 네트워크 기술의 사용, 미들웨어와 프로토콜의 혼재, 댁내 정보가전기기의 제한적인 시스템 자원, 댁내 사용자의 보안 인식 부족 등으로 인하여 홈 네트워크에 연결된 홈 디바이스나 홈서비스는 공격에 의한 보안취약성을 가진다. 그래서 홈 네트워크 기술이 보급되기 위해서는 최우선적으로 해결해야 할 기

술 중의 하나가 정보보호기술이다. 홈 네트워크 정보보호기술은 악의적인 목적을 가진 공격자가 네트워크를 통하여 댁내에 침입하여 디바이스나 개인 프라이버시를 침해하는 것을 방지할 수 있다. 홈 네트워크 정보보호기술의 하나로 사용자가 홈 네트워크에 접속할 때에 사용자를 인증하는 사용자 인증 기술이 있다. 이는 홈 네트워크 서비스를 이용하고자 하는 사용자는 반드시 ID/PW 방식 또는 인증서 방식 등의 인증 과정을 수행한 후에, 그 결과에 의해 댁내에 존재하는 다양한 서비스를 이용할 수 있다[1-3],

현재 악의를 가진 공격자를 차단하기 위한 사용자인증 서비스는 다양한 분야에서 많이 이루어지고 있지만, 홈 네트워크에서 제공하는 서비스가 다양하고 복잡해짐에 따라 단순한 사용자 인증만으로는 완전한 보안 서비스를 제공할 수 없다. 홈 네트워크에는 많은 장치와 서비스, 그리고 다수의 사용자가 존재하기 때문에 모든 서비스에 대한 접근제어 관리가 필요하다. 따라서 본 논문에서는 안전한 신뢰성 있는 홈 네트워크 서비스를 제공하기 위한 RBAC 기반의 접근제어 시스템을 설계하고자 한다.

II. 관련연구

2.1 홈 네트워크 환경의 보안 요구사항

홈 네트워크 환경에서의 보안 요구사항은 홈의 정의에 따라 달라질 수 있다. 그리고 댁내에 어떠한 홈 네트워크 기술들이 포함될 것인가에 따라 달라진다. 댁내의 네트워크가 외부 액세스망과 연결되어 있지 않다고 가정하면, 안전한 홈 네트워크 환경을 제공하는 것은 쉽다. 그러나 댁내의 네트워크가 인터넷과 같은 외부의 액세스망과 연결되어 있다면, 안전한 네트워크 서비스를 제공하기 위해 고려해야 할 요소들은 많아진다. 또한 댁내에 한 명만이 거주하고 있다면, 안전한 홈 네트워크 구축이 쉬울 수 있다. 하지만, 댁내에 여러 명의 구성원이 거주하면 한 명이 거주하는 형태와 비교해 볼 때 훨씬 복잡한 보안 정책들이 필요하다[2].

홈 네트워크 환경에서의 보안 요구사항은 기업과 공공기관의 네트워크 환경과 마찬가지로 다음과 같은 기능을 보장해야 한다[2].

- 인증(Authentication) : 누구에게 디바이스와 홈서비스를 사용하도록 허락할 것인가?
- 기밀성(Confidentiality) : 디바이스로 전달된 메시지를 누구에게 읽도록 허락할 것인가?
- 무결성(Integrity) : 사용자와 디바이스나 홈서비스 사이에 전송되는 정보는 권한을 가진 사용자만이 정보를 수정할 수 있어야 한다.
- 가용성(Availability) : 사용자가 필요할 때 디바이스나 홈서비스를 사용할 수 있도록 보장해야 한다.
- 인가(Authorization) : 각 디바이스에서 제공하는 서비스나 정보에 대해 가족 구성원 각각에 대해 어느 정도의 접근권한을 주어야 하는가?

2.2 기존의 접근제어 방식

기존의 접근 제어 방식은 크게 자율적 접근제어, 강제적 접근제어, 그리고 역할기반 접근 제어 등이 있다.

자율적 접근제어(Discretionary Access Control, DAC)는 주체나 또는 그들이 소속되어 있는 그룹들의 신분(ID)에 근거하여 객체에 대한 접근을 제한하는 방법이다. 즉, 접근 통제는 객체의 소유자에 의하여 임의적으로 이루어진다. 그러므로 어떠한 접근허가를 가지고 있는 한 주체는 임의의 다른 주체에게 자신의 허가를 넘겨줄 수 있다[1,4].

강제적 접근 제어(Mandatory Access Control, MAC)는 객체에 포함된 정보의 비밀성과 이러한 비밀 정보에 대하여 주체가 갖는 정형화된 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다. MAC 정책은 DAC 정책에 비해 객체의 소유자에 의하여 변경할 수 없는 주체와 객체간의 접근제어 관계를 정의하며 주체가 객체를 판독하고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제약사항이 복사된 객체에 전파된다. MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체대객체 단위로 접근 제한을 설정할 수 없다[1,4].

시스템이 대규모화되고 다양해지면서 조직들은 그 조직 특성에 적합한 복잡한 보안 정책을 필요로 하게 되었고, 보안 정책의 일관성 유지 및 보안 정책의 변경을 실제 시스템에 적용하기 위한 비용이 높아졌다. 앞에서 언급한 기존의 자율적 접근제어와 강제적 접근제어의 메커니즘인 접근제어 목록, 능력기반 접근제어, 레이블 기반 접근제어 기법들은 규칙 수준에서 접근 제어 서비스를 제공하기 때문에 위와 같은 요구를 만족시키기 어렵다. 기존의 접근 제어 기법에서는 각 사용

자에게 권한을 할당하는 반면, 역할-기반 접근 제어 기법에서는 필요한 역할(Role)과 그 역할이 수행할 수 있는 연산을 보안 정책에 맞게 정의한 후, 실제 사용자들에게 각자 역할을 할당하는 기법이다[4,5].

III. 홈 네트워크 접근제어 시스템

3.1 홈서비스를 위한 접근제어 시스템

댁내는 다양한 디바이스들과 정보가전기기로 구성되고 다양한 역할을 가지는 사용자들이 존재하기 때문에, 이들 사용자들과 다양한 디바이스에 대하여 다양한 접근권한을 할당하고 제어할 수 있는 접근제어기능이 제공되어야 한다. 안전하고 신뢰성 있는 홈 네트워크 서비스를 제공하기 위해서 접근권한 검증을 수행하는 접근제어시스템은 홈 네트워크 구성요소들에 내장되어야 한다. 접근제어시스템은 홈게이트웨이 혹은 홈서버에 탑재되어 각 사용자에게 할당된 접근권한을 검증하고, 그 결과에 따라서 홈 디바이스를 제어하거나 홈서비스를 제공하는 기능을 제공한다.

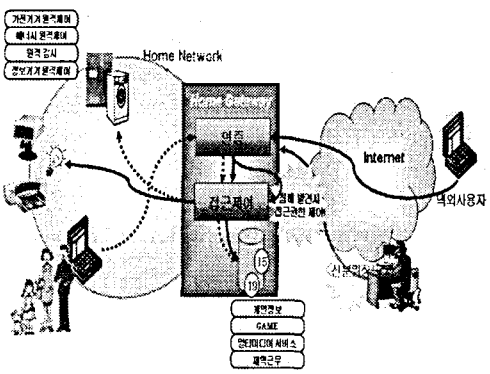

그림 1. 홈 네트워크 환경에서의 접근제어 개념도

3.2 접근제어 시스템의 설계

홈 네트워크 접근제어 시스템은 접근제어 검증모듈, 접근제어 집행모듈, 보안정책 관리모듈로 구성된다. 접근제어 검증모듈은 권한검증 유닛, 검증정보 수집 유닛으로 구성되고, 접근권한 집행모듈은 접근제어 처리유닛, 로그관리 유닛, 알림처리 유닛, 디바이스 제어 유닛으로 구성되어진다.

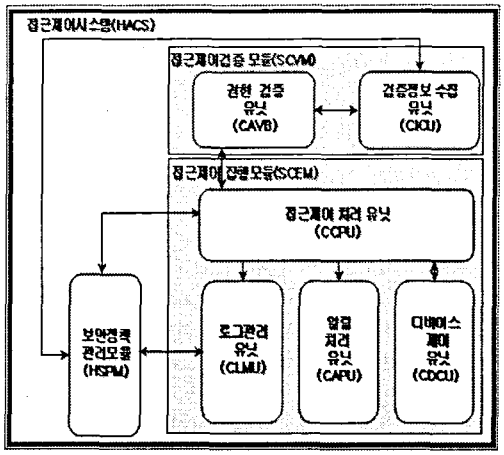

그림 2. 접근제어 시스템의 구성도

① 권한검증 유닛

권한검증 유닛은 접근제어 처리 유닛으로부터 검증 요청을 받으면 보안 정책 관리 블록의 접근제어 정책정보를 기반으로 접근여부를 결정한다. 접근을 결정하는데 필요한 시간, 상황 등과 같은 정보들은 검증 정보 수집 유닛을 통해서 제공받고, 그 결과를 접근 제어 처리 유닛에 통보한다.

② 검증정보 수집 유닛

검증 정보 수집 유닛은 권한 검증에 필요한 다양한 환경 정보를 수집해서 제공한다. 즉, 시간 정보, 주변 홈 디바이스 상태 정보, 사용자 정보, 센싱 정보 등을 포함하며, 실시간으로 권한 검증 유닛과 연동한다.

③ 접근제어 처리 유닛

접근 제어 처리 유닛은 보안 정책 관리 모듈로부터 사용자 정보를 전달받으면, 이를 기반으로 권한 검증 유닛에 권한 검증을 요청한다. 권한 검증 유닛으로부터의 응답을 기반으로 디바이스 제어 유닛, 알림 처리 유닛 및 로그 관리 유닛과 연동해서 해당 작업을 수행한다.

④ 로그관리 유닛

로그관리 유닛은 홈 게이트웨이나 홈 서버에서 발생하는 모든 상황을 로그로 기록하며, 이를 보안 정책 관리 모듈에 제공해서 관리자가 로그와 통계 정보를 모니터링할 수 있도록 한다.

⑤ 알림 처리 유닛

알림처리 유닛은 보안 정책 관리 모듈의 접근 제어 정책을 검증한 결과 예외 상황이나 응급 상황, 또는 통보할 필요가 있는 상황이 발생하면, 정책에 정의된 사용자와 해당 기관에 통보하는 역할을 수행한다.

⑥ 디바이스 제어 유닛

디바이스 제어 유닛은 접근 제어가 성공적으로 수행되어 접근이 허용되면 홈 디바이스에 해당하는 미들웨어와 연동해서 해당 제어 명령을 수행한다. 미들웨어와의 연동을 통하여 디바이스 제어를 위한 권한 검증 결과 정보를 전달한다. 결과 및 미들웨어 타입을 매개변수로 가지며 디바이스의 동작 결과를 반환한다. 이러한 미들웨어에는 LnCP, UPnP 등이 있으며 추후 다양한 미들웨어와 연동할 수 있는 확장성을 고려해서 설계되어야 한다.

⑦ 보안정책 관리모듈

보안정책 관리모듈은 접근권한 검증을 수행하기 위한 정책 정보의 생성 및 관리 기능을 수행한다.

Ⅳ. 결론

홈 네트워크 환경의 발전과 더불어 홈 네트워크에서 제공하는 서비스가 다양하고 복잡해짐에 따라 단순한 사용자 인증만으로는 완전한 보안 서비스를 제공할 수 없다. 따라서 본 논문에서는 다양한 홈 디바이스와 홈서비스가 존재하는 홈 네트워크 환경에서 안전하고 신뢰성 있는 서비스를 제공하기 위한 접근제어 시스템을 설계하였다.

현재 설계된 시스템을 구현 중에 있으며, 향후 다양한 접근제어 기법들을 홈 네트워크 환경에 적용하여 효율적이고 안전한 홈 네트워크 서비스를 제공할 수 있는 연구를 계속해서 진행할 것이다.

참고문헌

[1] 김도우, 한종욱, 주홍일, 이윤경, "홈네트워크 서비스를 위한 접근제어 시스템의 설계", 한국멀티미디어학회, Vol.7 No.2, 2004

[2] Carl M. Ellison, *Home Network Security*, Intel Technology Journal, 2002.

[3] Guoyou He, *Requirements for Security in Home Environments*, Residential and Virtual Home Environments Seminar on Internetworking, Spring 2002.

[4] David F. Ferraiolo, R.S. Sandhu, Serban Gavrila, D.Richard Kuhn and Ramaswamy Chandramouli, *Proposed NIST Standard for Role-Based Access Contro*", ACM Transactions on Information and Systems Security (TISSEC), Volume 4, Number 3, August 2001.

[5] S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, *Role based access control model*", IEEE Computer, 29 February 1996.

[6] David F. Ferraiolo, D Richard Kuhn, *Role-Based Access Control*, Artech House Inc, 2003

[7] Matthew J. Brodeur, *Security Concerns In Home Automation Technologies*, 2001.

[8] David Ferraiolo and Richard Kuhn. *Role-based access control*", In 15th NIST-NCSC National Computer Security Conference, pages 554-563, Baltimore, MD, October 13-16 1992.

[9] Kim Thomas, *Building a Secure Home Network*, SANS Institute, 2001

[10] Stallings William, *Network Security Essentials: Applications and Standards*, Prentice Hall, 2000.

[11] Gerard O'Driscoll, *Essential Guide to Home Networking Technologies*, Prentice Hall, 2000.

[12]http://www.iec.org/online/tutorials/home_net/