홈네트워크에 적합한 접근제어 방식에 대한 고찰

황진범*†, 한종욱*†

Study of the Access control model for Home Network

*Electronics and Telecommunications Research Institute

†University of Science & Technology

E-mail : hjb64253@etri.re.kr

요약

본 논문에서는 홈네트워크에서 댁내의 디바이스가 제공하는 서비스에 대해 불법적인 사용을 제한하고 각 사용자 별로 허가된 권한 내에서만 서비스를 이용할 수 있게 하는 접근제어 방식을 제안한다. 기존의 중앙집중 접근제어 방식과, 분산 접근제어 방식은 홈네트워크에 적용했을 때 중앙기기의 부하집중, 비밀정보의 침해 가능성, 사용자의 불편함 등의 문제를 가지고 있다. 본 논문에서는 기존의 접근제어 방식의 문제점을 분석하고 이를 해결하기 위하여 홈네트워크에 적합한 접근제어 방식을 제안한다.

1. 서론

홈네트워크는 가정의 각 가전 및 사무기기 등이 지능화되고 네트워킹 능력을 갖게 되어 서로 통신하게 되면서 사용자로 하여금 어느 곳에서도 집안의 디바이스들을 제어하거나 서비스를 사용할 수 있게 해주는 기반환경을 말한다. 홈네트워크는 다양한 환경으로 구성되어 다양한 서비스를 제공할 수 있으며 서비스를 제공하는 각 디바이스는 여러 사용자에 의해 사용될 수 있다. 서비스 중에는 원격 진료, 가스 조절, 출입문 통제 등 거주자의 안전과 비밀에 밀접하게 관련된 것들이 있기 때문에 각각의 사용자마다 허용되는 서비스를 차별화하여 각각의 사용자의 권한에 맞는 서비스를 제공하고 불법적인 서비스 사용의 제한이 가능한 홈네트워크에 적합한 접근제어 기술이 필요하다.

기존의 홈네트워크에서의 접근제어기술은 크게 두 가지 방식으로 연구되어 왔다. 중앙 디바이스가 대행자로서 모든 디바이스에 대한 접근제어를 대행하는 중앙집중 접근제어 방식[1]과 각 단말 디바이스 별로 접근제어를 수행하는 분산 접근제어 방식[2]이다. 위의 두 가지 접근제어 방식은 홈네트워크에 그대로 적용하기에는 몇 가지 문제점이 있다. 중앙집중 접근제어 방식은 통제가 편리하고 통일될 수 있다는 장점이 있는 반면에 중앙 디바이스에 병목현상이 야기될 수 있으며, 중앙 디바이스를 관리하는 사람은 댁내 모든 디바이스 및 서비스에 대한 접근 권한을 갖게 되어 관리자에 의해 각 개인의 권리가 침해될 가능성이 있다. 또한 중앙 디바이스가 모든 디바이스 및 서비스에 대한 권한을 갖기 때문에 중앙 디바이스만 해킹되면 댁내 모든 디바이스에 대한 불법적인 접근이 가능해진다. 단말 디바이스 별 분산 접근제어 방식은 하나의 단말이 해킹되어도 다른 단말에 바로 심각한 영향을 끼치지 못한다는 것, 그리고 각 단말 별로 인증 및 접근제어가 수행되기 때문에 부하가 분산되어 병목현상을 막을 수 있고 확장이 용이해 진다는 것. 또한 각 소유자가 자신의 디바이스를 관리함으로써 모든 디바이스에 대한 접근권한을 갖는 Super User의 존재가 불필요하므로 개인의 권리를 더욱 보호할 수 있다는 등의 장점이 있지만, 반면에 가구 구성원 모두가 관리자가 되어 보안설정을 담당해야 하며 보안에 대한 구체적인 지식을 가지고 있어야 한다는 것과 각각의 디바이스 별로 보안 정책을 설정해야 하므로 디바이스가 많아 질수록 정책을 변경할 때에 수많은 작업이 필요하게 된다는 단점이 있다.

본 논문에서는 홈네트워크에서 제공하는 서비스를 보안의 중요도에 따라 분류하고 가장 보안이 중요한 서비스에 대해서는 각 단말 디바이스가 접근제어를 수행하고 그 외의 서비스에 대해서는 중앙디바이스가 접근제어를 수행하게 함으로써 통일되고 편리한 접근제어 정책을 사용하면서 사용자의 비밀 정보를 최대한 보호하고 중앙기기에서의 병목현상을 제거하는 방안을 제안한다.

본 논문의 2장은 기존의 접근제어 방식의 단점을 분석하였고 3장은 제안된 접근제어기법

에 대해 설명하였다. 마지막으로 4장에서 결론과 앞으로의 연구 방향에 대해서 설명하였다.

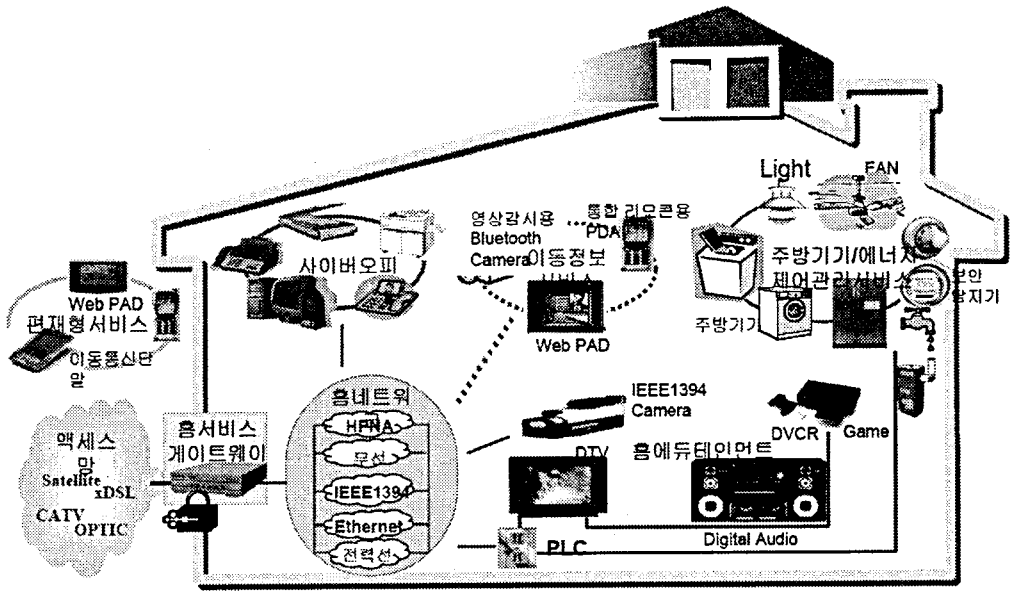


그림 1. 홈네트워크 모델

2. 기존 홈네트워크 접근제어 방식

홈네트워크는 외부 인터넷과 Hybrid Fiber/Coax (HFC), Digital Subscriber Line (DSL), Integerated Services Digital Network (ISDN) 등의 다양한 망을 통해 연결되며 홈네트워크의 내부 망 또한 Ethernet, HomePNA, IEEE802.11, Zigbee, PLC 등 다양한 유무선 기술이 적용된 망으로 구성이 된다. 홈게이트웨이는 홈의 내외부의 다양한 망이 서로 연결되어 통신할 수 있도록 하는 인터페이스 역할을 해주는 중앙 디바이스로 일반적으로 홈네트워크는 그림 1과 같이 구성된다[3,4,5,6]. 홈네트워크를 구성하는 기기들은 그림1과 같이 홈네트워크 서비스를 사용하기 위한 PDA나 PC, 노트북, 웹패드 그리고 휴대 전화 등의 클라이언트와, 홈네트워크 내,외부를 연결해 주는 홈게이트웨이, 그리고 냉장고, 오디오, 전등 등 사용자에게 서비스를 제공해주는 디바이스로 나눌 수 있다.

홈네트워크는 향후에 유비쿼터스 컴퓨팅 환경의 시발점으로서 수십 개의 장비들을 갖게 될 것이다. 어느 장비들은 모든 홈 구성원이 공용으로 사용하게 될 것이며, 몇몇 장비들은 각 개인의 소유가 될 것이다. 그리고 홈은 그 구성원간의 관계에 따라 다음과 같은 4가지 환경으로 나뉘어 질 수 있다[7].

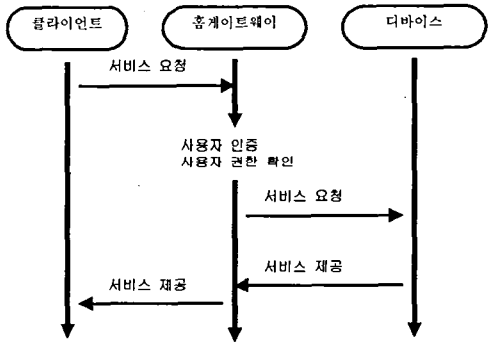
- Single-Person Homes
- Couple With Small Children
- Families With Teenagers
- Adult Guests and Roommates

혼자서 생활하는 집의 경우가 가장 단순한 보안시스템이 요구되는 경우이며 십대 자녀 및 방문자가 있는 경우와 룸메이트와 생활하는 집이 가장 많은 보안을 요구하며 보안이 까다로운 환경으로 분석되고 있다. 홈네트워크에서의 접근제어는 위의 4가지 환경에 모두 적용될 수 있도록 설계되어야 한다. 기존의 홈네트워크에서의 접근제어는 크게 두가지 방식으로 연구되어 왔는데, 하나는 중앙 디바이스가 대행자로서 홈네트워크 내부의 각 디바이스에 대한 접근제어를 수행하는 중앙집중 접근제어 방식[1]이고, 다른 하나는 UPnP 미들웨어[2]와 같은 단말 별 분산 접근제어 방식이다. 그림 2는 두 방식의 일반적인 접근제어 모델을 나타낸다.

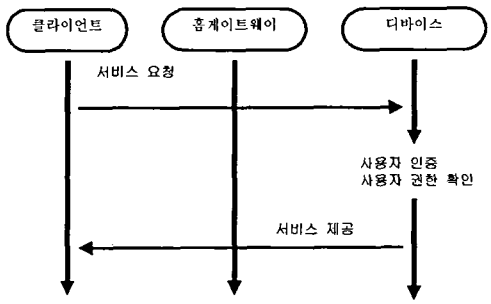
중앙집중 접근제어 방식에서는 사용자가 서비스를 요청할 때에 홈게이트웨이에서 사용자를 인증하고 접근권한을 확인한 후 적합한 요청에 대해서만 디바이스에게 서비스를 요청한다. 디바이스는 홈게이트웨이에게 서비스를 제공한다. 이때, 디바이스와 홈게이트웨이에는 상호 신뢰관계가 구축되어 있음을 가정한다. 이후, 홈게이트웨이는 디바이스에서 제공하는 서비스를 클라이언트에게 전달한다. 분산 접근제어 방식에서는 홈게이트웨이는 클라이언트와 디바이스 간의 물리적인 연결만 제공할 뿐 인증 및 접근제어에 대

한 기능은 제공하지 않고, 각 디바이스에서 사용자에 대한 인증 및 접근제어를 수행한다.

중앙집중 접근제어 방식은 중앙 디바이스에서 RBAC[8]과 같은 접근제어 기법을 적용하여 편리하고 통일된 접근제어 정책을 적용할 수 있기 때문에 관리가 편리하고 안정적이라는 장점



(a) 중앙집중 접근제어



(b) 분산 접근제어

그림 2. 기존 홈네트워크 접근제어 모델

이 있는 반면 앞에서 언급한 홈네트워크의 4가지 환경중 Single-Person Homes 에 적합한 방식으로 다음과 같은 단점을 가지고 있다.

- **병목현상** : 홈게이트웨이에서 모든 인증 및 접근제어 절차가 수행되기 때문에 홈 내부 디바이스가 수십 개에 이르게 되면 홈게이트웨이에 부하가 집중되어 병목현상이 발생한다.

- **Super User** : 홈게이트웨이를 관리하는 관리자는 댁내의 모든 서비스에 임의로 접근이 가능하다. 때문에 관리자에 의해 홈 내부 구성원의 비밀을 침해될 여지가 있다. 관리자에 대해 100% 신뢰할 수 없는 환경-Roommates와 거주하는 경우-이나 그렇지 않더라고 개인의 비밀이 보장되어야 하는 서비스의 경우 문제가 발생할 수 있다.

- **Security Hole** : Super User의 경우와 마찬가지로 불법침입자가 홈게이트웨이를 해킹하면 댁내의 모든 서비스에 대한 권한을 소유하게 되므로 홈게이트웨이 하나의 해킹만으로 댁내구성원의 모든 비밀이 침해될 수 있다.

반면에 분산 접근제어 방식은 접근제어 수행에 대한 부하가 각 디바이스에 분산되며 홈게이트웨이가 댁내 모든기기에 대한 접근권한을 가지고 있을 필요가 없는 장점을 갖는 반면에 다음과 같은 문제점이 있다.

- **통일성, 안전성 부재** : 각각의 구성원이 자신이 소유한 디바이스에 대해 접근제어 정책을 수립하므로 통일성이 부족하고, 비전문적인 사람이 관리하게 되므로 안전성이 부족해진다.

- **사용자의 불편** : 모든 사용자가 보안에 대한 지식이 필요하게 되고 사용자가 추가되거나 정책이 변경되는 경우 각각의 디바이스마다 일일이 접근제어정책을 재설정해줘야 하므로 사용자에게 큰 불편을 준다. 예를 들면, 사용자가 추가된 경우 홈게이트웨이를 통한 RBAC같은 경우는 각 Role에 사용자를 할당해주기만 하면 기존의 정책을 변경 없이 적용 가능한 반면 단말 디바이스 별로 접근제어를 수행하는 경우는 모든 디바이스에 새로운 사용자에 대한 정책을 추가해야 한다.

3. 제안된 접근제어 방식

3.1 서비스 분류

본 논문에서는 홈네트워크 내에서 각 디바이스가 제공하는 서비스의 종류를 보안 정도에 따라 다음의 3등급으로 분류하였다.

- **Critical Secret**

- **Normal Secret**

- **No Secret**

Critical Secret 서비스는 홈네트워크 관리자도 접근이 허가되지 않는 서비스로 디바이스 소유자 및 소유자가 허가한 극히 일부의 사용자만 접근이 가능한 서비스이다. 이는 가장 보안이 강력한 서비스로 디바이스가 직접 접근제어를 수행한다. 디바이스의 소유자는 서비스에 대한 보안의 중요성 여부, 홈네트워크 관리자에 대한 신뢰성 여부에 따라서 Critical Secret 서비스의 범위를 정해야 한다. Normal Secret 서비스는 홈

네트워크 관리자에게 접근이 허가되며 홈게이트웨이가 디바이스에게 접근제어 권한을 위임 받아 사용자에게 권한을 발급하는 서비스이다. 이 서비스는 홈게이트웨이가 해킹되었을 경우에 소유자 및 사용자에게 경미한 피해만 입힐 수 있는 서비스이다. No Secret 서비스는 누구에게나 접근이 허용되며, 다른 사용자에게 아무런 피해도 끼치지 못하는 서비스이다. No Secret 서비스는 아무런 인증 및 접근제어 과정 없이 누구나 사용할 수 있다.

Critical Secret 서비스는 개인의 비밀과 밀접한 관련이 있는 서비스이기 때문에 주로 소유자 혼자 사용하는 경우가 대부분이므로 한번 설정하면 변경하는 경우가 드물 것이고, Normal Secret 서비스의 경우는 그 외의 대부분의 사용자에게 접근제어 정책이 적용되므로 빈번한 정책변화가 일어날 것이다. 때문에 Critical Secret 서비스의 경우는 디바이스의 소유자가 직접 접근권한을 관리하고 Normal Secret 서비스의 경우는 홈게이트웨이에서 권한을 위임 받아 관리하도록 한다. 이러한 방식은 접근제어 정책을 설정함에 있어서 사용자의 불편을 최소화하면서 홈게이트웨이에서 RBAC과 같은 중앙집중 접근제어 방식을 사용하여 보다 편리하고 안전한 관리를 할 수 있게 한다. 또한 홈게이트웨이가 해킹된다 해도 침입자는 다른 서비스에는 접근할 수 있겠지만 Critical Secret 서비스에는 쉽게 접근할 수 없어 사용자의 최소한의 비밀을 보장할 수 있다. 마찬가지로 댁내에서 누가 홈게이트웨이를 관리하게 되든 내부 구성원의 Critical Secret 서비스는 노출되지 않을 수 있다. 마지막으로 접근제어 권한의 위임과 서비스 사용에 대한 권한을 부여할 때에 권한 인증서를 사용함으로써 홈게이트웨이는 최초의 권한발급과, 재발급 시에만 관여하며 그 이후의 서비스 사용에 대해서는 사용자와 디바이스간에 직접적으로 인증 및 권한 확인 절차가 진행되어 부하가 각 디바이스로 분산되어 병목현상을 방지할 수 있도록 한다.

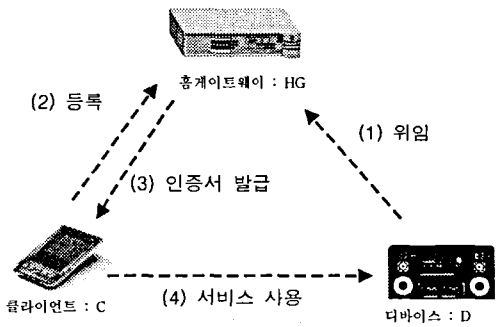
3.3 제안된 접근제어 방식

제안된 접근제어 과정은 크게 위임, 사용자 등록, 인증서 발급, 서비스 이용의 4 부분으로 구성된다. 그림 3은 제안된 접근제어 과정을 나타낸다.

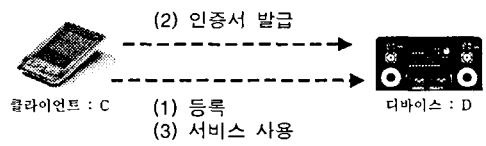
- 위임 : 홈게이트웨이에서 Normal Secret 서비스에 대한 접근권한을 관리하여 사용자에게 적합한 권한을 허가해주는 기능을 하기 위해서는 초기 단계에 디바이스에서 홈게이트웨이로 접근제어 권한을 위임해주는 절차가 필요하다.

- 사용자 등록 : 사용자는 Critical Secret 서비스를 사용하기 위해서는 각 디바이스에 Normal Secret 서비스를 사용하기 위해서는 홈게이트웨이에 인증을 받고 등록하는 과정이 필요하다.

- 인증서 발급 : 사용자는 댁내의 서비스를 사용하기 위해서 Normal Secret 서비스는 홈게이트웨이에게 Critical Secret 서비스는 각 단말 디바이스에게 서비스 사용 권한을 허가해주는 인증서를 먼저 부여 받아야 한다.
- 서비스 이용 : 인증서를 발급받은 사용자는 인증서의 만료기간이 지나기 전까지 해당 인증서를 제출함으로써 서비스를 사용할 수 있으며 인증서가 만료되면 다시 발급 절차를 수행한다.



(a) Normal Secret



(b) Critical Secret

그림 3 제안된 홈 서비스 접근제어 과정

4. Conclusion

본 논문에서는 기존의 홈네트워크에서 연구되어 왔던 중앙집중 접근제어 방식과 분산 접근제어 방식을 홈네트워크에 적용시켰을 경우의 장단점을 분석하고 단점을 해결하기 위한 접근제어 방식을 제안하였다. 먼저 서비스를 디바이스 소유자의 보안 필요성에 따라 3가지로 분류하고 보안이 가장 크게 필요한 서비스는 각 디바이스가 직접 권한 관리를 하며 그 외의 서비스에 대해서는 홈게이트웨이를 통해 중앙집중적으로 관리하는 방식을 제안하여 기존 접근제어

방식의 단점을 보완하였다. 향후 저성능 디바이스에서 공개키 사용을 가능하게 해주는 기술에 대한 연구와 각 서비스별 접근제어 요구사항에 대한 분석과 각 요구사항에 적합한 보안 정책에 대한 연구가 필요할 것이다.

참고 문헌

[1] M. Rahman, *Remote Access And Networked Appliance Control Using Biometrics Features*, IEEE Transactions on Consumer Electronics, Vol. 49, No. 2, MAY 2003

[2] C. Ellison, *UPnP Security Ceremonies Version 1.0*, UPnP Forum, 2003

[3] B. Rose, *Home networks, a standards perspective*, IEEE Communication Magazine, pp. 78-85, 2001.

[4] S. Teger, D.J. Waks, End-*user perspectives on home networking*, IEEE Communication Magazine, pp. 114-119, 2002.

[5] C.R. Holliday, *The residential gateway*, Spectrum, IEEE , Volume: 34 , Issue: 5 , pp. 29 - 31, May 1997.

[6] F.T.H. den Hartog, M.Balm, C.M. de Jong, and J.J.V. Kwaaitaal, *Convergence of Residential Gateway Technology*: Analysis of Evolutionary Paths, Consumer Communications and Networking Conference, pp. 1 - 6, Jan. 2004.

[7] C. Ellison, *Interoperable Home Infrastructure - Home Network Security*, Intel Technology Journal Vol 06. Nov.2002.

[8] R.S. Sandhu, E.J. Coyne, *Role-Based Access Control Models*, Computer, pp. 38 -47, Feb. 1996