한국산학기술학회논문지
Vol. 11, No. 3, pp. 920-925, 2010

홈 네트워크 시스템에서 x.509 v3 인증서를 이용한 사용자 인증 및 접근제어 시스템의 구현

이광형[1*], 이영구[2]
[1]서일대학교 인터넷정보과, [2]숭실대학교 컴퓨터학과

Implementation of user authentication and access control system using x.509 v3 certificate in Home network system

Kwang-Hyoung Lee[1*] and Young-Gu Lee[2]
[1]**Dept. Internet Information Seoil University**
[2]**Dept. of Computer Science, SoongSil University**

요 약 본 논문은 유무선 네트워크와 댁내 가전기기로 구성된 홈 네트워크 시스템은 각종 외부 위협요소로부터의 사이버 공격 대상이 될 수 있을 뿐만 아니라 해킹, 악성코드, 웜 바이러스, DoS공격, 통신망 도청 등의 보안취약성을 가지고 있다. 이로 인해 사생활 침해, 개인정보의 노출, 개인정보의 도용 등 많은 문제가 발생한다. 따라서 홈 네트워크상에서 해당 사용자의 자산 및 개인정보를 보호할 수 있는 보안 프로토콜의 필요성은 점차 증대되어가고 있다. 따라서 본 논문에서는 공개키 인증서를 이용하여 사용자를 인증하고 인증된 정보를 기반으로 해당 기기에 대한 권한을 차등 부여함으로서 허가 받지 않은 사용자로부터의 댁내 자산 및 개인 정보를 보호할 수 있는 사용자 인증과 접근제어 기술을 이용한 홈 네트워크 보안 프로토콜을 설계하고 제안한다.

Abstract A home network system is made up of home devices and wire and wireless network can not only be the subject of cyber attack from a variety factors of threatening, but also have security weakness in cases of hacking, vicious code, worm virus, DoS attack, tapping of communication network, and more. As a result, a variety of problems such as abuse of private life, and exposure and stealing of personal information arose. Therefore, the necessity for a security protocol to protect user asset and personal information within a home network is gradually increasing. Thus, this dissertation designs and suggests a home network security protocol using user authentication and approach-control technology to prevent the threat by unauthorized users towards personal information and user asset in advance by providing the gradual authority to corresponding devices based on authorized information, after authorizing the users with a Public Key Certificate.

Key Words : Home-Network, Authentication, Access Control

1. 서론

최근 정보통신 기술의 발전으로 인간은 다양하고 편리한 서비스에 대한 관심이 높아지고 있다. 최근 컴퓨터 및 정보통신 기술의 발달과 함께 급속히 발전하는 인터넷 기술은 데이터 서비스는 물론 인터넷 폰, 전자신문, 주문형 비디오, IPTV 등 다양한 멀티미디어 서비스를 가능하게 하였으며, 이러한 인터넷의 발전은 홈 네트워크의 발전에 큰 영향력을 주었다.

홈 네트워크를 구성하는 HDTV, 디지털캠코더, Home theater, 인터넷 냉장고 등의 디지털 가전기기들의 보급이 활성화 되면서 가정은 단순한 가정에서 하나의 네트워크를 구성하는 가정으로 바뀌게 되었다. 홈 네트워크를 구성하는 기술에는 다양한 응용기술들이 있으며 여러 신호

이 논문은 2008년 서일대학 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이광형(dreamace@seoil.ac.kr)
접수일 10년 01월 07일 수정일 10년 03월 02일 게재확정일 10년 03월 18일

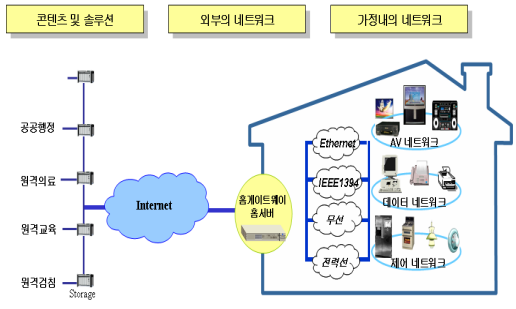
들을 전송할 수 있는 무선 기술이 핵심으로 응용되고 있다. 과거 '홈오토메이션 시스템'에서 본격적인 '홈네트워킹 시스템'으로 전환이 시작되었다[1].

이러한 솔루션을 통하여 유무선 인터넷을 통한 각종 가전제품과 가스밸브, 조명 등을 원격제어하고 원격검침, 주차관리, 출입통제, 원격보안, 부재중 방문객관리 등 다양한 기능을 갖춘 홈 네트워크 서비스가 자리 잡게 될 것이며 나아가 편리한 생활문화와 신규 고용창출에 기여할 것으로 예상된다[10].

따라서 본 논문에서는 불법적인 사용자의 침입을 사전에 차단하기 위하여 공개키 인증서를 통해 사용자를 인증한다. 또한 사용자 인증서에 해당 사용자의 기기 작동 권한을 차등적으로 명시함으로서 각 디바이스에 대한 접근 제어 및 외부 공격으로 댁내 디바이스를 보호할 수 있는 사용자 인증과 접근제어 기술을 이용한 홈 네트워크 보안 프로토콜을 설계하고 제안한다.

2. 관련연구

홈 네트워크 시스템의 구성도는 그림 1과 같으며 이러한 홈 네트워크 시스템은 크게 외부네트워크, 홈 게이트웨이, 내부 네트워크, 홈 미들웨어, 각종 디지털 정보 가전기기 그리고 다양한 응용서비스로 구성된다[9].



[그림 1] 홈 네트워크 시스템 구성도

홈 네트워크 환경에서의 각종 디바이스들은 인터넷과 직접적으로 연결되어 있어 언제라도 외부 위협요소로부터 공격에 대상이 될 수 있으며, 디바이스의 다양성과 홈 디바이스의 자원 공유 등으로 인해 고려해야 할 보안요구 사항은 더욱더 복잡해지고 있다[3,4].

2.1 사용자 인증

홈 네트워크에서는 각 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증과정이 필요하다. 이를 위해 생체인식, 패스워드, 인증서, 스마트카드, RFID 등의 다양한 사용자 인증기술의 활용이 가능하며 사용자 인증기술은 외부에서 홈 네트워크에 대한 원격 접근과 댁내에서 인터넷 뱅킹과 같은 서비스 사업자가 제공하는 서비스를 이용하고자 할 때 해당 사용자가 정당한 사용자임을 증명하는 하기 위한 수단으로 사용된다[7].

2.2 홈 네트워크 미들웨어 보안

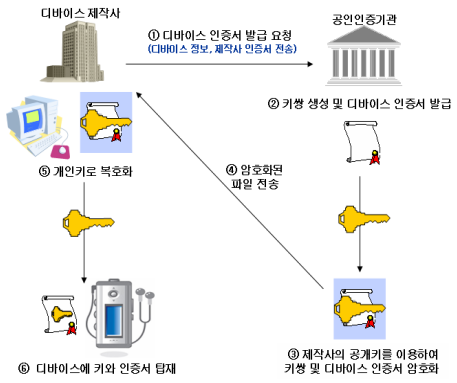
홈 게이트웨이와 서로 상이한 플랫폼을 가진 각각의 디바이스를 제어하기 위해서는 이들을 하나로 제어하고 관리할 수 있는 미들웨어가 필요하다. 이러한 미들웨어 자체에서도 기본적인 보안 기능이 제공되고 있으며, 현재 미들웨어에서의 보안 요소를 표준으로 제정하여 사용하기 위한 연구가 계속적으로 진행되고 있다. [표 1]은 홈 네트워크에 사용되는 미들웨어에 따른 보안 기술들을 보여주고 있다[5,6].

2.3 디바이스 인증

댁내 디바이스에 불법적인 사용을 방지하기 위해서는 홈 네트워크를 구성하고 있는 디바이스에 대한 인증이 선행되어야 한다. 현재 디바이스 인증은 미들웨어 레벨에서 제공되고 있으며 UPnP의 경우, 디바이스마다 부여된 Security ID를 이용하여 디바이스 등록시점에 인증이 이루어지며 그림 2와 같이 HAVi의 경우는 디바이스마다 고유한 인증서를 발행하여 디바이스를 인증한다[2].

[표 1] 홈 네트워크 미들웨어에 따른 보안 기술

미들웨어	제공하는 보안기능
UPnP	•Ver 1.0에서는 보안기능이 정의되어 있지 않음 •Ver 2.0에서 보안기능이 추가 - 제품 인증 - 기기간 인증 - 접근제어를 위한 디바이스가 자체적인 ACL - 기밀성
Jini	•Ver 1.0에서는 Java Security에 의존 - 사용자 인증 - 기기간 인증 - 메시지 무결성 및 기밀성 - 접근제어 •Ver 2.0에서 추가적으로 상호인증, 인가기능, 코드 무결성 등에 대한 기능 강화
HAVi	- HAVi인증서를 이용한 인증 - 접근제어



[그림 2] HAVi의 디바이스 인증과정

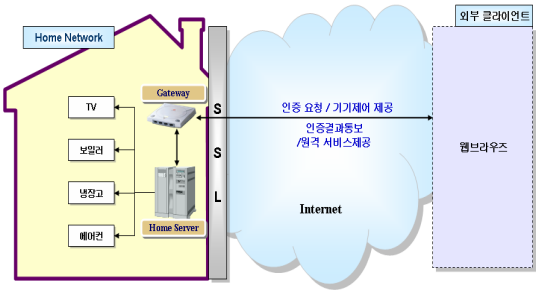
2.4 접근제어

사용자에 따라 제공받을 수 있는 홈서비스의 종류가 다르고 홈 네트워크 구성요소에 대한 제어 범위도 다르므로 각 사용자에게 부여된 권한에 맞는 기능만을 사용할 수 있게 하는 접근 제어 기술이 요구된다. 현재의 홈 네트워크 시스템의 구조를 고려할 때 접근제어를 위한 접근제어 목록은 각 단말기에 내장하고 있는 것이 효율적이다. 하지만 안정성 측면이나 사용자 측면과 같은 여러 요소들에 대해 일관된 보안정책을 적용해야 한다는 점에서 홈 게이트웨이에서 종합적으로 관리하는 것이 좀 더 효율적이다.

3. 제안 시스템 구조

3.1 제안하는 시스템

본 논문에서 제안하는 Home Network 시스템의 사용자 인증은 인증서를 이용하여 대칭키 암호화 방법으로 사용자를 인증하며 개인의 인증서를 홈 서버로부터 받아서 개인의 디바이스로 홈 시스템을 컨트롤 하는 방법이다.



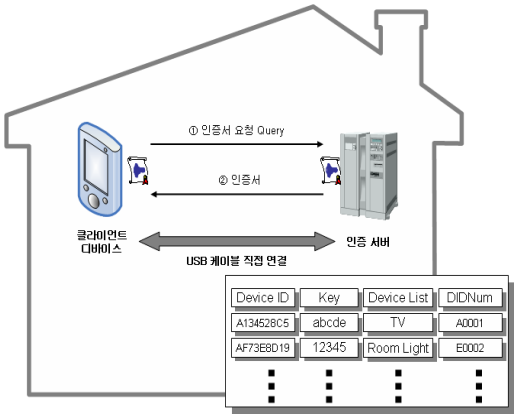
[그림 3] 제안하는 시스템의 전체구조

시스템의 전체구조는 그림 3과 같이 PDA 등과 같은 외부 클라이언트 즉, 외부에서 사용자가 인터넷 망을 통하여 홈 네트워크에 접근할 때 사용자의 인증과 디바이스에 대한 접근제어를 하는 방법에 대하여 제안하였다.

3.2 인증서 발급

홈 서버에서는 각 사용자의 디바이스에 대한 디바이스 ID와 Key를 생성하여 저장하고 있으며, 사용자 디바이스가 추가/삭제되면 사용자 디바이스는 홈 서버에서 디바이스를 등록하고 디바이스 ID와 Key를 재발급 받는다.

인증서는 사용자가 클라이언트 디바이스를 가지고 홈 네트워크 안에 있는 인증서버에서 직접 USB 케이블을 연결하여 발급 받는다. 발급시 인증서버는 클라이언트 디바이스에 대한 디바이스 ID와 Key를 생성하여 홈 서버에 저장을 하고 인증서를 발급한다.

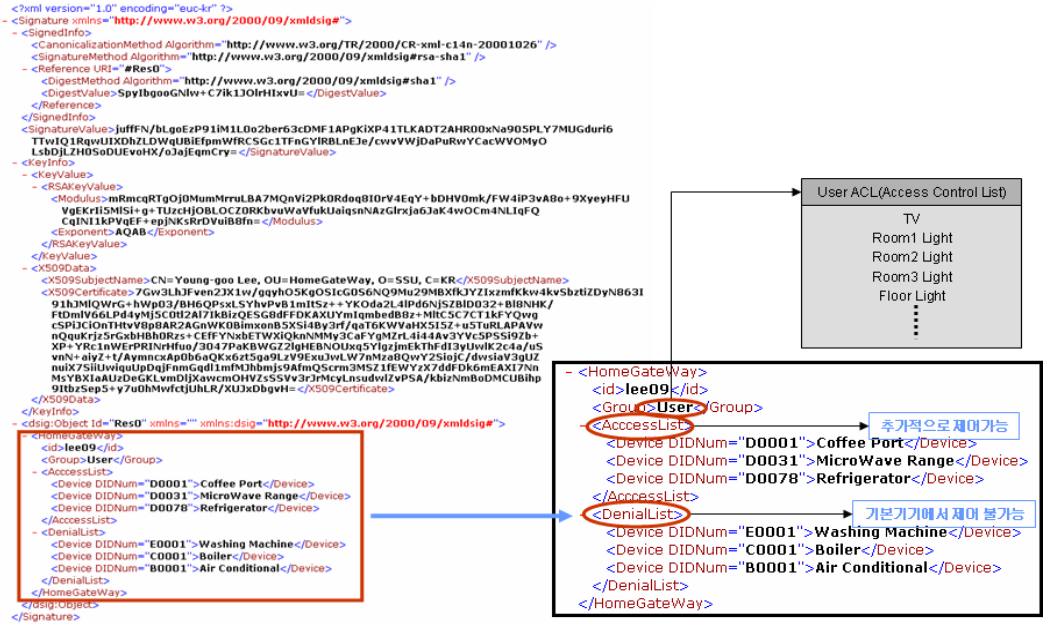


[그림 4] 사용자 인증서 발급과정

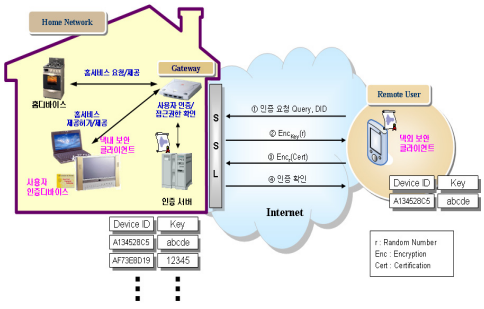
그림 4는 사용자 인증서 발급 과정을 보여주고 있으며 그림 5는 사용자 인증서 정보를 보여주고 있다. 사용자 인증서는 클라이언트 디바이스 ID와 개인키, 홈 디바이스 목록, 홈 디바이스 번호를 포함하고 있다.

3.3 사용자 인증

사용자 인증은 클라이언트가 발급받은 인증서를 가지고 사용자가 외부에서 SSL(Secure Sockets Layer)을 통하여 홈 네트워크에 접속을 요청한다. 사용자 인증요청이 전송되면 홈 서버는 난수 r값을 생성하여 클라이언트 디바이스의 개인키로 암호화하여 전송을 하고, 클라이언트는 자신의 개인키로 전송받은 정보를 복호화한 후 다시 자신의 인증서를 난수 r값으로 암호화하여 전송한다. 아래 그림 6은 사용자 인증 과정을 보여주고 있다.



[그림 5] 사용자 인증서 정보



[그림 6] 사용자 인증과정

사용자 인증과정의 세부내용은 다음과 같다.

① 클라이언트는 Query와 DID(클라이언트 디바이스 ID)를 전송을 한다.

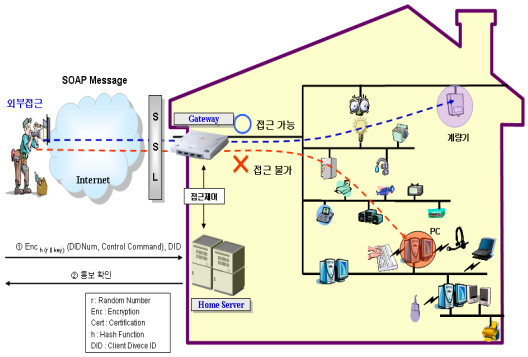
② $Enc_{key}(r)$: 홈 서버는 DID를 비교하고 난수 r값을 생하여 클라이언트의 디바이스의 개인키로 난수 r값을 암호화하여 전송한다. 이때 사용되는 암호화 방법은 비밀키 암호화 방법을 이용한다.

③ $Enc_{r}(Cert)$: 클라이언트는 자신이 가지고 있는 개인키로 복호화하여 난수 r값을 얻어내고, 난수 r값으로 자신의 인증서를 암호화하여 홈 서버에 전송한다.

④ 홈 서버는 인증서를 확인하고 올바른 인증서이면 인증확인 메시지를 전송하고, 클라이언트는 홈 네트워크에 접속해 디바이스를 제어한다.

3.4 디바이스 접근 제어

사용자 인증이 이루어지면 그림 7과 같이 홈 게이트웨이를 통한 각 디바이스 접근이 이루어진다. 외부 클라이언트가 홈 디바이스에 접근 할 때 사용자에 따라 홈 디바이스에 접근권한이 부여되고, 홈 서버는 외부 클라이언트의 인증서를 통해 접근 가능 여부를 판단해 홈 디바이스의 접근을 통제한다.



[그림 7] 디바이스 접근제어

디바이스 접근 제어에 대한 프로세서는 아래와 같다.

① $Enc_{h(r||Key)}(DIDNum, Control\ Command), DID$
- 서버로부터 전송받은 난수 r값과 자신의 키를 연접한 후 해쉬한다.
- 해쉬값과 X.509 기반의 애트리뷰트인 DIDnum와 Control Command 메시지를 암호화한 값과 클라이언드 자신의 DID를 홈서버에 전송한다.

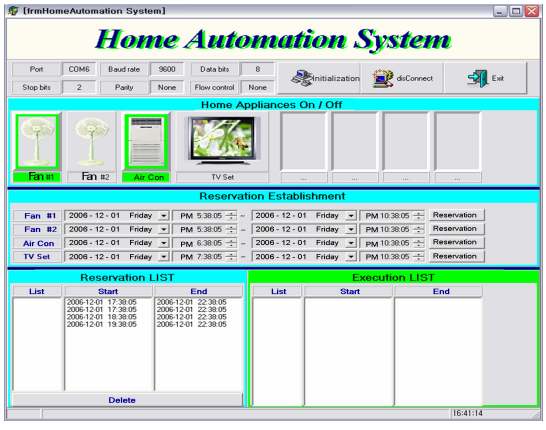
② 홈 서버는 클라이언트의 DID 값을 이용하여 복호화 하여 DIDnum와 Control Command를 확인한 후 사용자에게 장치 사용 여부를 전송한다.

4. 제안한 시스템의 실험 및 평가

4.1 제안하는 시스템의 실험

제안하는 시스템은 홈 서버와 클라이언트 구조로 되어 있으며, 홈 서버를 통해 사용자가 직접 USB케이블을 통하여 미리 발급받은 클라이언트 디바이스의 인증서를 통해 홈 서버에 접속하여 홈 디바이스를 컨트롤 한다. 이때 인증서 발급과정에서 사용자의 권한에 따라 홈 디바이스에 대한 접근제어 리스트를 다르게 생성하여 관리한다.

본 논문에서 제안하는 시스템의 실험 환경은 Intel Pentium-4 CPU 2.80과 1GB의 RAM, 그리고 MS-Windows XP Professional 운영체제를 사용하였다. 또한 구현언어는 Delphi 7.0과 ASP 웹 프로그램을 사용하였고, 데이터베이스는 MS-SQL 2000을 사용하였다. 아래 그림 8은 본 논문에서 제안하는 홈 네트워크 시스템의 서버 인터페이스이다.



[그림 8] 홈 네트워크 시스템 서버

홈 서버는 홈 디바이스의 상태정보와 예약처리 상황을 처리하고, 사용자 등급에 따른 홈 디바이스 접근제어를 수행할 수 있다. 또한 홈 디바이스에 대한 상태 정보를 실시간으로 읽어 드린 후 접속한 클라이언트에게 전송하고 클라이언트는 서버로부터 전송된 홈 디바이스 상태정보를 통해 제어하고자하는 디바이스에 대한 제어를 수행한다. 예약목록은 홈 디바이스 동작 시작 시간에 따라서 우선순위가 정해지며 동일한 디바이스에 대한 예약이 중복되어 발생할 경우 우선순위가 높은 순서에 따라 동작하게 된다.

클라이언트는 자신의 DID 값을 전송하고 인증을 요청한다. 서버는 난수 r값을 생성하여 클라이언트의 Key 값으로 암호화 하여 클라이언트에게 재전송하고 클라이언트는 자신의 Key 값으로 복호화 하여 난수 값 R을 획득한다. 클라이언트는 획득한 난수 R을 이용하여 인증서를 암호화 하여 서버에게 전송하고, 서버는 자신이 가지고 있던 난수 R을 이용하여 전송받은 정보를 복호화하고 인증서를 검사한다. 서버는 인증결과를 클라이언트에게 전송한다.

4.2 비교 분석

표 2는 기존 프로토콜과의 비교 실험을 통하여 연산 횟수, 데이터 송/수신량, Key 개수에 대한 성능 분석을 보여주고 있다.

[표 2] 프로토콜 기능 비교

구분	P사	S사	M사	제안 프로토콜
사용자인증 연산 횟수	4회	4회	6회	4회
hash 연산 횟수	-	-	-	2회
Data 송/수신 량	ID, Key 64+128=192bit	ID, Key 64+128=192bit	ID, Key 64+128=192bit	ID, h(Key‖R) 64+128+64=256bit
암호화횟수	1회	1회	2회	2회
Key 개수	1개	1개	2개	1개

기존의 공개키 기반구조에서 인증서를 이용하고 있는 M사의 경우 인증방법에서 6번의 연산횟수를 거쳐 인증을 하였으나 제안한 프로토콜에서는 4번의 연산횟수를 거쳐 사용자를 인증할 수 있기 때문에 속도가 빠르며 기존의 Key를 이용한 암호화 방법보다 데이터량은 많지만 난수 r값과 Key를 연접하고 해쉬하여 전송하기 때문에 보안적인 면에서 더 안전하다.

5. 결론

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 시간이나 공간에 구애를 받지 않고 다양한 홈서비스를 제공받을 수 있는 디지털 홈 구현을 위한 홈 네트워크에 대한 연구가 활발히 이루어지고 있다.

홈 네트워크의 정보가전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안기능의 탑재가 어렵기 때문에 사이버 공격에 취약하다는 문제점이 있다. 더욱이 홈 네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 사이버 공격의 대상이 될 수 있어 해킹, 악성코드, 웜 바이러스, DoS(Denial of Service) 공격, 통신망 도청 등 보안취약성을 가지고 있으며, 이로 인하여 사생활 침해, 개인정보의 노출, 개인정보의 도용 등 많은 문제가 발생한다.

제안하는 방식은 사용자가 자신의 클라이언트 디바이스의 인증서를 오프라인에서 홈 서버로부터 직접발급 받으며 발급받은 인증서를 이용하여 사용자 인증과 디바이스 접근제어를 수행한다. 제안한 프로토콜에서의 데이터는 항상 암호화 되어 전송되므로 불법적인 장치가 클라이언트의 개인키와 난수 r값을 모르면 데이터의 정보가 노출될 위험은 없으며, 또한 홈 디바이스 제어 메시지는 해쉬한 값을 다시 암호화 하여 전송하기 때문에, 중간에서 메시지를 가로채더라도 메시지의 내용을 유추하는 것은 불가능 하다는 장점이 있다.

향후 연구과제로는 다양한 홈 디바이스를 제어하는 방법과 연산 수행능력이 떨어지는 휴대용 기기를 이용한 무선에서의 홈 디바이스 접근 및 제어하는 방법에 관한 연구가 필요하며, 기존의 유선망에서 사용하는 안전한 보안 프로토콜과 제안한 방법을 적용하여 보다 안전한 보안 프로토콜에 관한 연구가 필요하다.

참고문헌

[1] 정재학, “홈 네트워크에서의 보안 요구사항 분석”, 한국정보보호학회지 제14권 5호, pp.19-22, 2004.

[2] TTAS.KO-12.0030, “홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘”, 한국정보통신기술협회, 2005.

[3] Car M. Ellison, “Home Network Security”, Intel Technology Journal Vol 6, Issue 4, 2002.

[4] 김정태, “유비쿼터스 홈 서버 보안 요구사항 및 구현방안”, 전자통신동향분석, 제20권 제2호, 2005.04.

[5] 전대식, “Homenetwork Middleware 보안기술 동향 및 업체 동향”, 전자부품연구원 전자정보센터, 2004.11.

[6] 박동준, “홈 네트워크 보안에 관한 연구”, 건국대학교, 2005.

[7] H. Jo, H. Youn, “A Secure User Authentication Protocol Based on One-Time-Password for Home Network”, ICCSA 2005, VOL 3480, p.519, May 2005.

[8] 정용훈, “홈 네트워크 기반의 안전한 콘텐츠 전송에 관한 연구”, 한국산학기술학회논문지, 2007

[9] H.Schulzrinne, X. Wu, and S. Sidiroglou, "Ubiquitous Computing in Home Networks", IEEE comm. Mag. Oct. 2003.

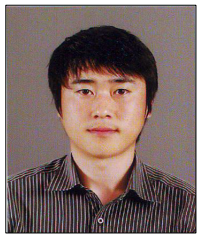
[10] 전병찬, “인터넷 정보가전을 위한 통합 홈 서버 설계 및 구현”, 한국산학기술학회논문지, 2007

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 일반대학원 컴퓨터공학과 (공학석사)
- 2005년 2월 : 숭실대학교 일반대학원 컴퓨터공학과(공학박사)
- 2005년 3월 ~ 현재 : 서일대학교수

<관심분야>
USN, RFID, 영상보안, 홈네트워크

이 영 구(Young-Gu Lee) **[정회원]**



- 2003년 2월 : 숭실대학교 전자계산원(공학사)
- 2006년 2월 : 숭실대학교 대학원 컴퓨터학과(공학석사)
- 2010년 1월 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정

<관심분야>
멀티미디어 보안, PKI, 홈 네트워크 보안, IPTV