PKI 기반 홈 네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구

정회원 이 영 구*, 김 정 재*, 김 현 철**°, 전 문 석*

A Study for PKI Based Home Network System Authentication and Access Control Protocol

Young-Gu Lee*, Jung-Jae Kim*, Hyun-Chul Kim**°, Moon-Seog Jun* *Regular Members*

요 약

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. 그래서 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 접근 제어 기술을 이용한 홈 네트워크 보안 프로토콜을 설계하고 제안한다.

Key Words : Home Network, Authentication, Access Control, X.509, Hash

ABSTRACT

A home network system is made up of 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. So, the necessity for a security protocol to protect user asset and personal information within a home network is gradually increasing. Thus, this paper 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.

Ⅰ. 서 론

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 가정 내의 정보화도 가속시키고 있다.

과거 '홈오토메이션 시스템'에서 본격적인 '홈네트워킹 시스템'으로 전환이 시작되었고, 최근에 IT의 화두로 떠오르고 있는 홈 네트워크 시스템은 새로운 기술 발전이었으며 거기에 따른 인간의 편리한 생활을 만들어 줄 것이다[1].

* 숭실대학교 컴퓨터학과(ad3927, arginss, mjun@ssu.ac.kr)
** 한국과학기술정보연구원 정보화전략팀(dmzpolice@kisti.re.kr) (° : 교신저자)
논문번호 : KICS2009-10-483, 접수일자 : 2009년 10월 26일, 최종논문접수일자 : 2010년 3월 31일

하지만 기존 홈 네트워크 시스템에서는 인터넷과 직접적으로 연결되어 있어 언제라도 외부 위협요소로부터 공격에 대상이 되며, 서로 다른 인증방법 및 스니핑, 스푸핑 등의 여러 해킹공격에 대한 취약성으로 인해 디바이스의 다양성과 홈 디바이스의 자원 공유 등으로 인해 고려해야 할 보안요구 사항은 더욱더 복잡해지고 있다.

따라서 본 논문에서는 외부 클라이언트에서 홈 네트워크를 컨트롤 하기위한 사용자 인증방법과 각 사용자마다 그룹을 나누어 디바이스를 제어하고 접근할 수 있는 접근권한 방법을 제안한다.

Ⅱ. 관련연구

2.1 홈 네트워크 구성

아래 그림 1은 홈 네트워크 시스템의 구성도를 보여주고 있으며 이러한 홈 네트워크 시스템은 크게 외부네트워크, 홈 게이트웨이, 내부 네트워크, 홈 미들웨어, 각종 디지털 정보 가전기기 그리고 다양한 응용서비스로 구성된다[2].

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 있으며 그

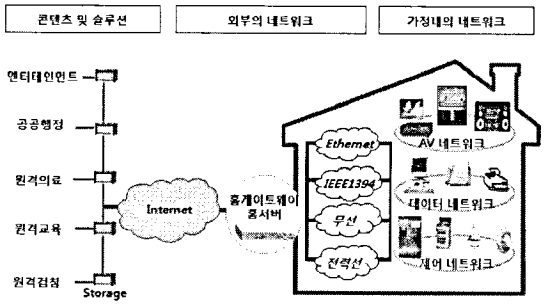


그림 1. 홈 네트워크 시스템 구성도

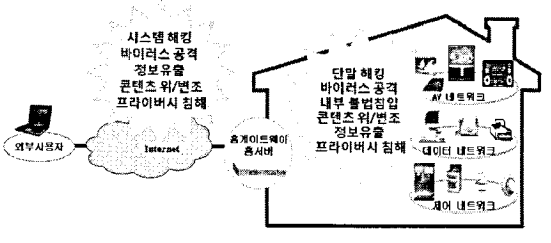


그림 2. 홈 네트워크 보안의 문제점

림 2와 같은 보안상의 문제점이 야기되고 있다.

2.2 홈 네트워크 보안 기술

홈 네트워크에서는 유무선 네트워크와 다양한 프로토콜 등으로 기존의 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야할 보안 취약성이 많이 존재한다. 홈 네트워크의 다양한 디바이스들은 인터넷과 서로 연결되어 공격의 대상이 될 수 있으며, 더욱이 홈 네트워크에서 디바이스의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 보안요구사항이 더욱 복잡해지고 있다. 홈 네트워크에서 보안해야할 사항에 대하여 그림 3과 같이 5가지로 나누어 볼 수 있다[3,4].

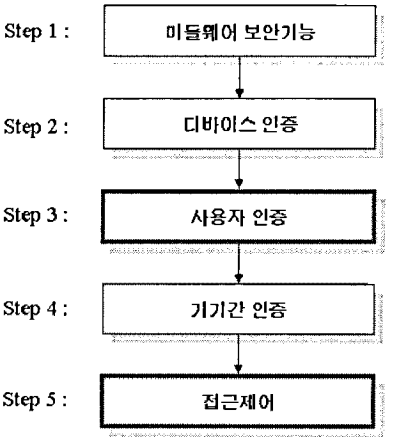


그림 3. 보안 프레임워크

2.2.1 홈 미들웨어 보안

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

2.2.2 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 HAVi의 경우는 디바이스마

표 1. 홈 네트워크 미들웨어에 따른 보안 기술

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

다 고유한 인증서를 발행하여 디바이스를 인증한다[6,8].

2.2.3 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 증명하기 위한 수단으로 사용된다[7].

2.2.4 기기간 인증

원활한 홈서비스 제공을 위해서는 기본적으로 홈 네트워크 구성 요소간의 자원공유를 위한 기기간 상호인증 과정이 이루어져야 한다. 현재 기기간의 상호인증은 미들웨어 레벨에서 제공하는 보안기능에 의존하고 있다. 하지만 미들웨어 레벨에서의 홈 디바이스의 인증은 가장 기본적인 부분에서의 보안 기능만을 제공하기 때문에 다양한 홈 네트워크 환경에 적용하기 위한 기기간의 인증이 필요하다.

2.2.5 접근 제어

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[9].

Ⅲ. 제안하는 시스템

본 논문에서 제안하는 시스템의 사용자 인증은 공개키 암호 알고리즘 기반의 인증서를 통해 이루어진다. 이때 개인의 인증서는 홈 서버로부터 발급받아 관리되며 발급받은 인증서에는 사용자가 사용할 수 있는 가전기기에 대한 접근 권한이 명시되어 있어 허가받지 않은 사용자로부터의 불법적인 시스템 사용을 사전에 방지할 수 있다.

아래 그림 4는 제안하는 시스템의 홈 서버와 홈 클라이언트간의 동작과정을 보여주고 있다.

3.1 인증서 발급

홈 서버에서는 각 사용자의 디바이스에 대한 DID(Device ID)와 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 받으며, 인증서는 인증서버가 가지고 있는 사설 인증서를 이용한다. 발급 시 인증서버는 클라이언트 디바이스에 대한 디바이스 ID와 Key를 생성하여 홈 서버에 저장하고 인증서를 발급한다. 그림 5는 사용자 인증서 발급 과정을 보여주고 있다.

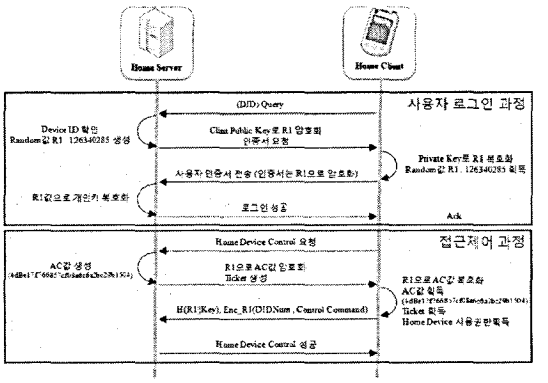


그림 4. 홈 서버와 홈 클라이언트 동작과정

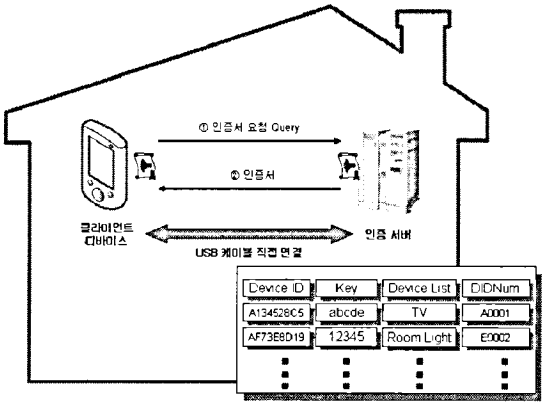


그림 5. 사용자 인증서 발급과정

3.2 사용자 인증

아래 그림 6은 본 논문에서 제안하는 프로토콜의 사용자 인증 과정을 보여주고 있으며 사용자 인증 과정은 아래와 같다.

① 클라이언트는 Query와 DID를 전송하고 사용자 인증을 요청한다.

② 홈 서버는 DID를 비교하고 난수 r을 생성한다. 그 후 클라이언트와 사전에 교환하여 가지고 있는 대칭키 k를 이용하여 난수 r을 암호화한 정보를 클라이언트에게 전송한다.

③ 클라이언트는 대칭키 k로 전송받은 정보를 복호화하여 난수 r을 획득하고 획득한 난수r을 암호화키로 사용하여 자신의 인증서를 암호화하고 홈 서버에게 전송한다.

④ 홈 서버는 자신이 생성한 해당 클라이언트 난수 r을 이용하여 전송받은 정보를 복호화한 후 사용자 인증을 수행하며 수행 결과를 다시 클라이언트에게 전송한다.

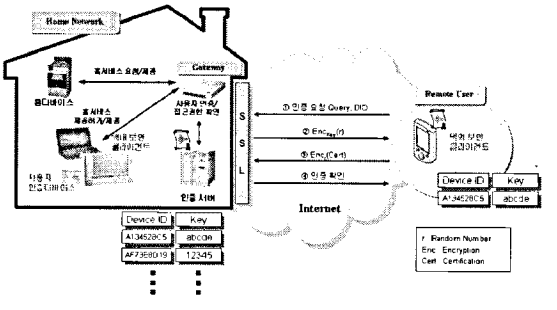


그림 6. 사용자 인증과정

3.3 디바이스 접근 제어

사용자 인증이 이루어지면 그림 7과 같이 홈 게이

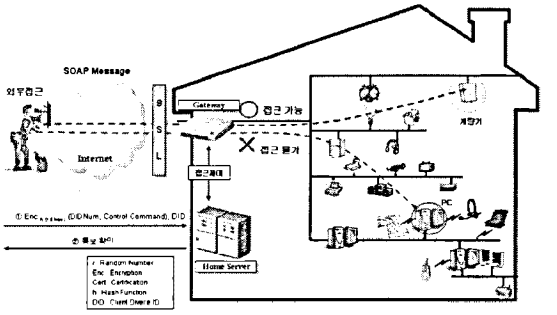


그림 7. 디바이스 접근제어

트웨이를 통한 각 디바이스 접근이 이루어진다. 외부 클라이언트가 홈 디바이스에 접근 할 때 사용자에 따라 홈 디바이스에 접근 권한이 부여되고, 홈 서버는 외부 클라이언트의 인증서를 통해 접근 가능 여부를 판단해 홈 디바이스의 접근을 통제한다.

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 DIDnum과 Control Command 메시지를 암호화 한 값과 클라이언트 자신의 DID를 홈 서버에 전송한다.

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

Ⅳ. 성능평가 및 비교분석

4.1 성능평가

제안하는 프로토콜과 P사의 UPnP, S사의 Jini, M사의 HAVi를 각각 비교하여 기존의 홈 네트워크 시스템이 제공하는 ID/Password 방식과 안전한 통신을 위하여 인증서를 이용한 홈 네트워크 방식을 비교하여 그에 따르는 보안상에 문제점의 발생을 최소화하는 것을 비교분석 하였다.

기존의 ID/Password 기반 인증 프로토콜의 가장 큰 취약점은 공격자의 패스워드 사전 공격이며 컴퓨터의 발전으로 공격자가 오프라인에서 활용할 수 있는 계산 능력이 증가하여 더욱더 위협적이다. 따라서 이를 예방하기 위해서는 정당한 인증 프로토콜 실행 중에 공격자가 도청과 같은 수동적 공격으로 패스워드에 대한 어떠한 정보도 획득할 수 없어야 한다.

또한 패스워드가 검증이나 예측이 가능한 평문 메시지에 대하여 직접적인 암호화키로 사용된다면 평문

과 암호문을 획득한 공격자는 자신이 추측한 패스워드 목록을 반복적으로 키로 사용하여 동일한 암호문이 생성되는지를 확인하는 검증문 공격을 수행할 수 있으므로 이러한 방법도 피해야 한다. 제안한 기법에서는 디바이스의 인증을 위해 직접 인증서를 발급받고 인증서와 난수 r값을 이용하여 SOAP 메시지 전송에 수반되는 문제가 없는지 분석해 보고, 악의적인 사용자들에 의한 스니핑(Sniffing), 스푸핑(Spoofing), 재전송(Replay Attack)등의 공격에 강한 특징은 표 2와 같이 기존 시스템과 비교하여 확인 하였다.

표 2. 기존 시스템과 성능 비교

	P사 프로토콜	S사 프로토콜	M사 프로토콜	제안하는 프로토콜
인증방법	ID Password	ID Password	인증서	인증서
디바이스 인증	Y	Y	N	Y
접근제어	Y	N	N	Y
상호인증	N	Y	N	Y
메시지 전송방법	개인키로 암호화 후 전송	개인키로 암호화 후 전송	공개키로 암호화 후 전송	난수 r값과 개인키로 암호화 후 전송
사용자 등급	N	N	N	Y

4.2 비교분석

표 3은 기존 프로토콜과의 연산 횟수, 데이터 송수신량, 사용되는 Key 개수에 대한 비교 실험을 통한 성능 평가를 보여주고 있다.

표 3. 프로토콜 기능 비교

구분	P사	S사	M사	제안 프로토콜
사용자 인증시 프로세스 과정 횟수	4회	4회	6회	4회
hash 연산 횟수	-	-	-	2회
Data 송/수신량	ID, Key 64+128= 192bit	ID, Key 64+128= 192bit	ID, Key 64+128= 192bit	ID, h(Key‖R), Enc_R(DIDNum, Control Command) 64+128+128 =320bit
사용자 인증시 암호화과정 횟수	1회	1회	2회	2회
Key 개수	1개	1개	2개	1개

실험 결과에서 확인 할 수 있듯이 인증서를 이용하고 있는 M사의 경우 사용자 인증 시 6번의 연산을 거쳐 인증을 하였으나 제안한 프로토콜에서는 4번의 연산을 거쳐 사용자를 인증할 수 있기 때문에 속도가 빠르며 기존의 Key를 이용한 암호화 방법보다 처리되는 데이터량이 증가된다는 단점이 있으나 난수 r과 Key를 연접하고 해쉬하여 전송하기 때문에 보안적인 면에서 더 안전하다는 장점이 있다.

4.3 보안성 비교분석

제안 프로토콜이 기존의 프로토콜들과 비교했을 경우 연산횟수에 다소 차이가 있기는 하나 하드웨어 발전의 영향으로 해결 될 것이라 보고, 홈 네트워크 시스템의 구성면에서는 기존의 프로토콜들이 갖고 있는 기능과 같은 기능을 사용하고 추가적으로 다른 기능을 요구하지는 않는다.

보안적인 측면에서는 그림 8과 같이 스푸핑 공격, 스니핑 공격, 재전송 공격과 같은 여러 공격에 안전하다는 것을 알 수 있다.

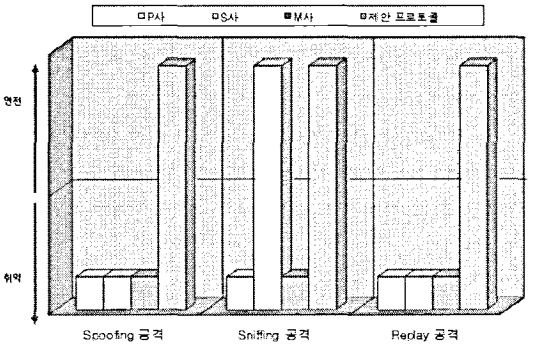


그림 8. 각 프로토콜 보안성 비교 그래프

4.3.1 스니핑 공격

제안하는 방식은 어떠한 방식으로 데이터가 전송되던 간에 데이터는 항상 암호화 되어 전송되므로 불법적인 장치가 키를 가지고 있지 않는 한 데이터 정보가 노출될 위험은 없다. 실제로 사용자 인증과 디바이스 제어과정에 있어서, 홈 서버는 난수 값을 생성하고 생성한 난수 r값과 Key를 연접하고 해쉬하여 데이터를 전송하기 때문에 Key를 유추하는 것이 어렵다. 또한 난수 r값을 클라이언트의 개인키로 암호화하기 때문에 개인키 없이는 난수 r값을 유추할 수 없다.

4.3.2 스푸핑 및 재전송 공격

스푸핑 및 재전송 공격으로부터 안전하기 위하여 전송되는 데이터는 난수를 이용하여 불법적인 사용자

의 접근을 방지하고 있다. 메시지는 난수 r값과 클라이언트 개인키를 연접하여 해쉬한 값으로 전송하기 때문에, 중간에서 메시지를 가로채더라도 실제 메시지의 내용을 유추하는 것은 불가능하며, 매번 메시지의 내용이 변하기 때문에 공격자가 중간에 메시지를 가로채어 재전송 할 수 없다.

따라서 같은 하드웨어 구성에서 각 기능을 어떻게 사용하는가에 따라 보안성이 증가되고 하고 감소되기도 한다. 제안하는 시스템은 단계별 진행과정으로 상호인증을 하였는데 각 단계마다 스푸핑 공격과 재전송 공격이 확실하게 차단된다는 장점이 있다.

V. 결 론

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. 현재 홈 네트워크를 구성하고 있는 디지털 정보 가전 기기들은 제한된 용량으로 인해 컴퓨팅 능력이 낮고 보안기능의 탑재가 어려우며 또한 유무선 통신망을 통해 외부 네트워크와 연결되어 있어 사이버 공격의 대상이 될 수 있을 뿐만 아니라 해킹, 악성코드, 웜 바이러스, DoS공격, 통신망 도청 등의 보안 취약성을 가지고 있다. 이로 인해 사생활 침해, 개인정보의 노출, 개인정보의 도용 등 많은 문제가 발생한다. 따라서 본 논문에서는 사용자가 자신의 클라이언트 디바이스의 인증서를 오프라인에서 홈 서버로부터 직접 발급받아 사용자 인증과 디바이스 접근제어를 수행한다. 또한 사용자 인증 데이터 정보는 항상 암호화 되어 전송되므로 불법적인 장치가 클라이언트의 개인키와 난수 r을 모르면 데이터의 정보가 노출될 위험이 없으며 홈 디바이스 제어정보는 해쉬 한 값을 다시 암호화 하여 전송하기 때문에, 중간에서 메시지를 가로채더라도 메시지의 내용을 유추하는 것은 불가능 하다는 장점이 있다.

참 고 문 헌

[1] Freed, Les, Hungry Minds. "Guide to home networking", 2004, G, 89236.

[2] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜", 한국정보과학회, Vol.30, pp.75-81, 2003.

[3] 원태성, "안전한 홈 네트워크의 보안 요구사항 연구", 단국대학교, 2004.

[4] J. Zhuge, and R. Yao, "Security Mechanism for Wireless Home Network", in Proc. of IEEE Global Telecommunications Conference 2003 (GLOBECOM 2003), Vol.3, pp.1527-1531, Dec. 2003.

[5] TTAS.KO-12.0030, "홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘", 한국정보통신기술협회, 2005.

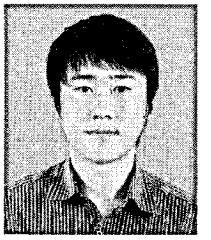
[6] 박동준, "홈 네트워크 보안에 관한 연구", 건국대학교, 2005.

[7] Car M. Ellison, "Home Network Security", Intel Technology Journal Vol 6, Issue 4, 2002.

[8] 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.

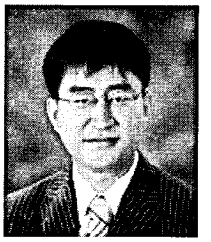
[9] E. Callaway, L. Hester, P. Gorday, "Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks", IEEE Communications Magazine, Vol.40 No.08. 2002.

이 영 구 (Young-Gu Lee) 정회원



2003년 숭실대학교 전자계산원
2006년 숭실대학교 컴퓨터학과 석사
2007년~현재 숭실대학교 컴퓨터학과 박사과정
<관심분야> 인터넷 보안, PKI, DRM

김 정 재 (Jung-Jae Kim) 정회원



1995년 영동대학교 컴퓨터공학과 공학사
1999년 숭실대학교 대학원 컴퓨터학과 공학석사
2005년 숭실대학교 대학원 컴퓨터학과 공학박사
<관심분야> 멀티미디어 보안, DRM, RFID

김 현 철 (Hyun-Chul Kim) 정회원

2003년 인제대학교 정보컴퓨터학부
2005년 경원대학교 전자계산학과 석사
2009년 숭실대학교 컴퓨터학과 공학박사
2009년 5월~현재 한국학기술정보연구원 정보화전략팀 선임연구원

<관심분야> 공전소, DRM, 보안 정책 및 전략

전 문 석 (Moon-Seog Jun) 정회원

1981년 숭실대학교 전산학과
1986년 University of Maryland 전산학 석사
1989년 University of Maryland 전산학 박사
1991년~현재 숭실대학교 컴퓨터학과 교수

<관심분야> Network Security, 정보보호, PKI