홈서비스 게이트웨이 보안 체계에 관한 연구

김 현 철* · 김 시 흥* · 안 성 진** · 정 진 욱* · 유 윤 식***, 전 용 일***

요 약

유무선 통신 기술의 발전에 힘입어 가정 내의 각종 기기를 유선 또는 무선으로 연결하여 정보를 공유하고 제어하는 기술인 홈 네트워크(Home Network)는 서비스 제공자와 사용자, 통신 사업자의 관심 속에 엄청난 발전을 거듭하고 있다. 이러한 홈 네트워크 기술은 홈 네트워크 제어기술, 홈 네트워크 전송기술과 더불어 홈 네트워크의 안전성과 신뢰성을 제공하기 위한 홈 네트워크의 관리 및 보안 기술이 절실히 요구되고 있다. 특히 홈서비스 게이트웨이는 그 특성상 강력한 인증 및 보안 기능이 요구되며 사용자 및 서비스 별로 상이한 인증 및 암호 기능이 요구된다. 본 논문에서는 다양한 네트워크 보안 기술과 암호 기술, 그리고 인증 기술을 기반으로 지속적으로 서비스가 가능한 홈 네트워크 보안 체계 설계를 목적으로 한다.

An Investigation on Survivable Security Schemes of Home Service Gateway

Hyun Cheol Kim* · Si Hung Kim* · Seongjin An**
Jin Wook Jung* · Yoon Sik Ryu*** · Young Il Jun***

ABSTRACT

With the radical improvement of wire and wireless communication technologies, home network which interconnects various home appliances is approaching ripening stage. Digitalization of the home environment will break down the boundaries of information, communications and broadcasting, and enable us to realize many breakthroughs on the home front and connect to our home. In order to enable users to access securely to their home network, we first construct secure home network model which can authorize users using their permission policy. In this paper, we examine various security technique used in home network and propose home network security scheme which can service constantly.

* 성균관대학교 컴퓨터공학과
** 성균관대학교 컴퓨터교육과
*** 한국전자통신연구원

1. 서 론

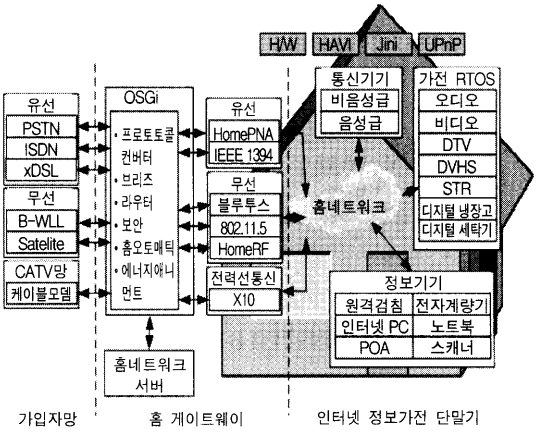
PC(Personal Computer)와 인터넷을 중심으로 한 1990년대 디지털 혁명은 산업현장에 엄청난 영향을 미쳐 모든 기기의 디지털화 및 업무양식을 근본적으로 바꾸어 놓았다. 이와 같은 디지털 물결은 유무선 통신기술의 발달과 더불어 최첨단 정보기기에서 시작하여 산업현장의 각종 기기와 가전제품까지 확산되어가고 있다. 여러 대의 PC를 가진 가정이 늘어나고 인터넷 접속이 가능한 정보가전 기기가 등장하는 등 각각의 장치들을 한데 묶어 서로 연결하고 인터넷 접속을 통해 편리함과 부가가치를 창출하고자 하는 욕구가 증대되고 있다[1-3].

이와 같이 가정 내의 각종 기기를 유선 또는 무선으로 연결하여 하나로 묶어서 정보를 공유하고 제어하는 모든 기술 및 서비스를 홈 네트워크(Home Network)라고 한다. 홈 네트워크를 기반으로 가정에 서비스를 전달하기 위해서는 (그림 1)에서와 같이 가정 내의 홈 네트워크 환경, 서비스를 가정까지 전달해 주는 외부의 네트워크 환경, 그리고 다양한 서비스 및 콘텐츠의 제공 등의 구성요소가 필요하다.

이러한 기술들 중에서 홈 네트워크 제어기술과 홈 네트워크 전송기술과 더불어 홈 네트워크의 안전성과 신뢰성을 제공하기 위한 홈 네트워크의 관리 및 보안 기술이 절실히 필요한 실정이다. 특히 홈서비스 게이트웨이는 그 특성상 강력한 인증 및 보안 기능이 요구되며 사용자 및 서비스 별로 상이한 인증 및 암호 기능이 요구된다[4-6].

본 논문에서는 다양한 네트워크 보안 기술과 암호 기술, 그리고 인증 기술을 기반으로 지속적으로 서비스가 가능한 홈 네트워크 보안 체계 설계를 목적으로 한다. 먼저 암호화 알고리즘, 공개키 암호와 PKI(Public Key Infrastructure) 기술, 그리고 서비스 게이트웨이 사용자 인증 기술 등을 살펴보고 SNMPv3를 이용한 서비스 게이트웨이 보안 관리 기술에 대해서 제안한다.

마지막으로 본 논문에서 제안하고 있는 서비스 게이트웨이 보안 구현 기술로서 웹 기반 홈 네트워크 상태 관리, 트래픽 관리, 실시간 상태정보 보고 체계 등을 기술한다.



(그림 1) 홈 네트워크 구조

2. 홈서비스 게이트웨이를 위한 암호 기술 및 인증 기술

2.1 해쉬함수

해쉬함수는 (그림 2)에서와 같이 임의의 길이의 비트스트링을 고정된 길이의 출력 값인 해쉬코드로 압축시키는 함수이다. 해쉬함수는 다음과 같은 몇 가지 특성을 갖는다.

먼저 해쉬함수는 주어진 출력에 대하여 입력값을 구하는 것이 계산상 불가능해야 한다(일방향성). 또한 주어진 입력에 대하여 같은 출력을 내는 또 다른 입력을 찾아내는 것이 계산상 불가능해야 하며 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것 또한 계산상 불가능해야 한다(강한 충돌 회피성)[7].

이러한 특성을 바탕으로 해쉬함수는 데이터

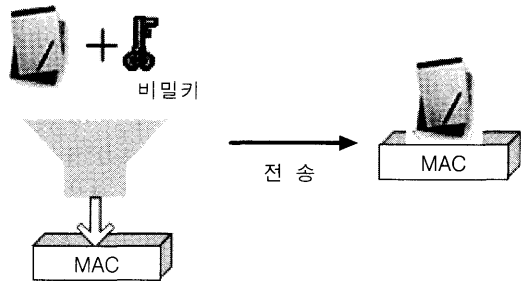
의 무결성, 인증, 부인 방지 등에서 응용되는 중요한 함수 중의 하나이다. 일례로 전자서명의 경우 몇 바이트에서 수 기가바이트에 이르는 다양한 크기의 메시지를 직접 전자서명 프로토콜에서 사용한다는 것은 문제가 있으므로, 메시지를 해쉬코드로 압축하고 이를 이용하여 전자 서명 값을 생성한다. 이때 또 다른 어떤 메시지가 동일한 해쉬코드를 생성한다면 위의 전자 서명 값은 또 다른 메시지에 대한 서명도 되므로 큰 문제가 발생한다. 실제로 이러한 문제가 발생하지 않는 것은 해쉬함수가 강한 충돌회피성을 가지고 있으므로, 이론적으로 동일한 해쉬코드를 가지는 메시지가 무한히 존재함에도 불구하고 현실적으로 동일한 해쉬코드를 가지는 한 쌍의 메시지를 찾을 수는 없기 때문이다.

대표적인 해쉬함수로는 1993년 NSA(National Security Agency)에 의해 설계된 SHA(Secure Hash Algorithm)를 1995년에 수정/보완한 SHA-1이 있다. SHA-1은 160비트의 출력을 가지며 대부분의 공격에 강한 저항성을 갖는다. 그러나 AES(Advanced Encryption Standard)에서 키 길이가 128, 192, 256 비트를 지원함에 따라서 출력 길이가 256, 384, 512 비트인 해쉬함수의 필요하게 되어 현재 SHA-256, SHA-384, SHA-512가 개발 중에 있다. HAS-160은 SHA-1과 MD5(Message Digest 5)의 장점을 취하여 국내 표준 해쉬함수로 개발된 것으로 본 논문에서 제안하는 홈서비스 게이트웨이는 160 비트 이상의 키 길이를 갖는 것을 기본으로 한다.

2.2 MAC 알고리즘

메시지 인증 코드(Message Authentication Code : MAC)는 데이터가 변조(수정, 삭제, 삽입 등)되었는지를 검증할 수 있도록 데이터에 덧붙이는 코드이다. 디지털 데이터인 경우 일부 비트의 변경이나 삽입 또는 삭제에도 흔적이 남지 않기 때문에 이런 문제를 해결하기 위하여 원래의 데이터로만 생성할 수 있는 값을 데이터에 덧붙여서 그 진위 여부를 확인하도록 하는 것이 MAC이다. 이때, 변조된 데이터에 대해서 MAC을 생성하여 MAC도 바꿔치기 할 가능성이 있으므로 MAC의 생성과 검증은 반드시 비밀키를 사용한다.

홈서비스 게이트웨이에서는 MAC 생성함수로 해쉬함수를 이용한 HMAC(Hashed MAC)를 사용한다. HMAC에서는 해쉬함수의 입력으로 사용자의 비밀키와 메시지를 동시에 사용하여 해쉬 코드를 구한다.



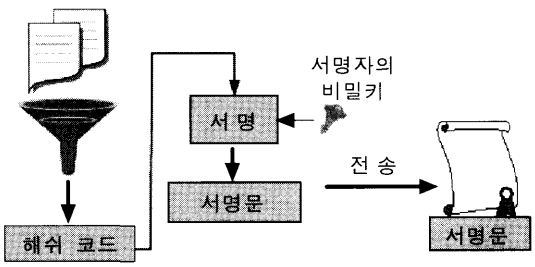
(그림 2) MAC 생성

2.3 전자 서명

서명(Digital Signature)은 데이터의 위조를 막고, 부인 방지를 위한 방법으로 MAC과 같이 데이터의 변조도 검증할 수 있게 한다. 디지털 서명은 각 데이터마다 서로 다른 서명을 생성하고 MAC과는 달리 해당 서명을 누구나 검증할 수 있어야 한다. 따라서 비밀키 방식의 MAC으로는 서명을 생성할 수가 없고 공개키 방식을 사용하게 된다. 공개키 방식을 사용하므로 공개키 암호와 마찬가지로 공개키 기반 구조(PKI)가 필요하다[7].

서명의 생성은 (그림 3)에서와 같이 서명자의 비밀키(서명키)를 사용한다. 이때 서명의 대상이 되는 데이터는 평문 전체가 아니라 평문을 해쉬한 해쉬 값에 대해서 서명을 생성한다. 일반적으

로 공개키 방식은 많은 연산시간을 필요로 할 뿐만 아니라 모든 평문에 대해서 서명을 생성하게 되면 서명의 길이가 그만큼 커지게 된다. 그러나 해쉬함수의 특성을 이용하면 해쉬 값에 대해서만 서명을 생성하여도 평문 전체에 대해서 하는 것과 같은 효과를 얻을 수가 있다.



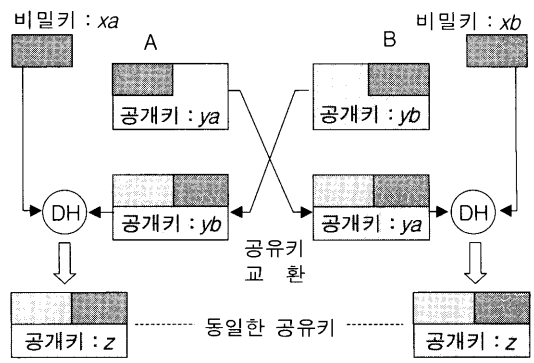
(그림 3) 전자서명 생성

서명의 검증은 서명자의 공개키(검증키)를 사용하여 서명을 검증한다. 수신 데이터를 서명과 메시지를 나누고 서명 값으로는 서명자의 공개키를 사용하여 구한 해쉬 값과 메시지를 해쉬하여 구한 해쉬 값을 비교하여 메시지에 대한 서명을 검증할 수가 있다. 대표적인 서명함수로는 RSA (Rivest, Shamir, Adleman)와 DSS(Digital Signature Standard)가 있다. 홈서비스 게이트웨이에서는 상기한 모든 서명 방식을 지원하여야 한다.

2.4 키 교환 알고리즘

공개키 암호는 수학적으로 풀기 어려운 문제들을 바탕으로 하고 있으므로 암/복호화 연산이 매우 느릴 뿐만 아니라 많은 시스템 자원을 필요로 한다. 한편 홈서비스 게이트웨이의 용량을 고려하여 미리 비밀키를 공유하거나 안전한 통신 채널을 사용하여 세션키를 전송을 하는 것이 효과적일 수 있다.

전자메일과 같은 일방향성 통신이거나 혹은 서버와 클라이언트 환경에서는 송신자나 클라이언트가 일방적으로 사용할 세션키를 설정하여 상대방에게 전송하여도 무방하지만 홈서비스 게이트웨이의 경우에는 (그림 4)에서 나타내고 있는 바와 같이 양쪽에서 각자 생성한 비밀 정보를 사용하여 새로운 세션키를 생성하는 것이 바람직하다. 대부분의 키 교환 알고리즘은 1976년에 발표된 Diffie-Hellman 알고리즘에 기초한다. DH 알고리즘은 유한체의 이산 로그 문제의 어려움에 바탕을 둔 알고리즘이지만 홈서비스 게이트웨이에서는 제안된 메모리와 처리능력을 갖는 무선 인터넷 단말 또한 지원해야 하기 때문에 타원곡선을 사용한 DH 알고리즘도 지원해야 한다.



(그림 4) 양방향 세션키 교환 방식

2.5 공개키 암호화 기술

Diffie와 Hellman은 1976년 발표한 논문 "New directions in Cryptography"에서 기존 암호학의 상식을 뛰어넘는 혁신적인 발상으로 기존의 관용 암호 방식의 문제점으로 지적되던 키 분배 방식을 해결한 암호 방식을 제안하였다. 공개키 암호 방식에서는 키를 두 개로 나누어 하나는 암호화키로 또 하나는 복호화키로 사용한다. 암호화키는 공개 목록에 공개하고 복호화키는 개인이 비밀리에 보관한다. 그러므로 암호화키는 공개키, 복호화키는 비밀키라고도 부른다.

공개키 암호화에서 송신자는 수신자의 공개키로 전달하려는 평문을 암호화하여 수신자에게 암

호문을 전송하면 수신자는 자신의 비밀키로 암호문을 복호화 한다. 따라서 공개키 암호 방식은 관용 암호 방식에서 필요한 키의 사전 분배가 필요 없는 획기적인 방식이다[7].

홈서비스 게이트웨이의 통신 특성상 암호문을 생성한 송신자의 신원을 확인해야 할 경우가 대부분이며 관용 암호 방식으로는 신원 확인이 어렵지만 공개키 암호 방식을 이용 디지털 서명으로 쉽게 수행할 수 있다.

현재 많이 사용되고 있는 공개키 암호 기술에는 RSA와 타원 곡선 암호가 있다. 타원 곡선 암호는 RSA에 비해 상대적으로 작은 키 사이즈를 갖기 때문에 가용 메모리가 적은 스마트카드 등에서 많이 사용되고 있다. 그러나 RSA 공개키 암호의 단점은 암호화 속도가 느리고 키 사이즈가 커야 되는 단점이 있다. 다양한 유무선 인터페이스를 지원해야 하는 홈서비스 게이트웨이는 서비스와 사용자 등급별로 전자 서명을 수행하기 위해 RSA와 타원 곡선 암호 방식을 모두 지원해야 한다.

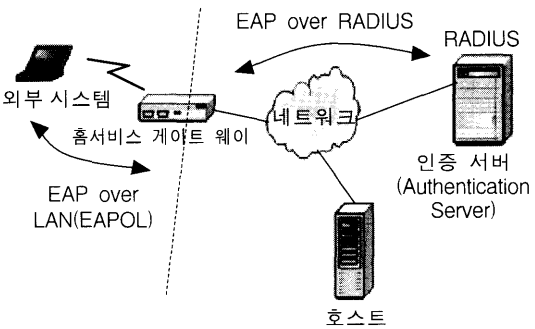
2.6 인증 기술

홈 자동화(HA : Home Automation) 기능을 제공하는 홈서비스 게이트웨이는 다른 암호화 기술을 비롯하여 강력한 인증 기능을 필요로 한다. 그러나 일반 인증 서비스 기능과 달리 홈서비스 게이트웨이는 중소규모의 사용자만을 서비스하기 때문에 RADIUS(Remote Authentication Dial-in User Services)를 이용한 802.1X와 비슷한 형태의 인증 서비스가 적합하다.

RADIUS는 홈서비스 게이트웨이와 인증 서버 사이에서 인증, 서비스 허가, 과금(Accounting)에 관한 정보 전달을 수행하는 프로토콜로써 인증서, DNS(Domain Name System) 정보들과 함께 적절한 사용자 및 서비스 인증을 수행할 수 있다는 장점을 제공한다.

3. 홈서비스 게이트웨이 PKI 기술

PKI에서 인증서는 사용자의 공개키와 사용자 식별자를 연결하는 것이다. 인증서는 기본적으로 인증기관(CA : Certificate Authority)이 부여하는 일련 번호, 인증서에 포함된 서명 방식을 식별하기 위한 서명 알고리즘 확인자, 발행 CA X.500 이름, 인증서의 유효기간, 인증서 소지자의 X.500 이름, 그리고 인증서 소지자의 공개키 등으로 구성된다. 인증서에 포함되는 서명문은 상기한 요소를 해쉬한 후 CA의 서명용 개인키로 서명함으로써 생성된다.



(그림 5) 홈서비스 게이트웨이 인증 요소

PKI에서 사용자의 신분 확인은 CA 또는 CA 기능을 대신하는 등록기관(RA : Registration Authority)에 의하여 수행된다. 인증서는 발행주체에 따라 최종개체를 위한 EE(End Entity) 인증서와 인증기관을 위한 CA 인증서로 구분된다. CA 인증서는 공개키 기반구조 상의 신뢰를 보장하기 위한 상호 인증(Cross Certification)용 인증서로 사용된다.

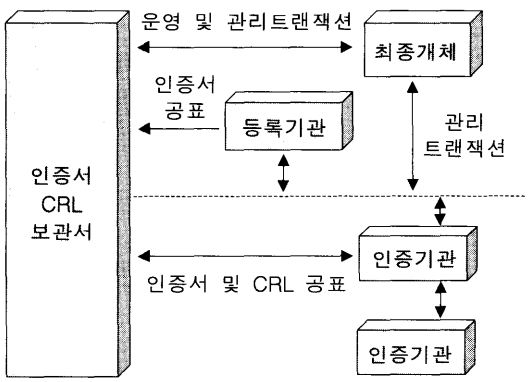
홈서비스 게이트웨이는 인증서를 이용한 다양한 인증 및 공개키 분배를 위해 공개 CA에서 발행한 인증서를 이용할 수 있고 또한 홈서비스 게이트웨이 자체가 인증서를 발행하는 CA의 역할을 수행할 수도 있다.

인증서는 유효기간이 만료되기 이전에 여러

가지 이유로 취소될 수 있으며 CA는 취소된 인증서의 목록을 디렉터리에 보관하고 있으며 취소된 인증서 목록을 CRL(Certificate Revocation List)라고 한다. 홈서비스 게이트웨이는 인증서를 받아들이기 전에 반드시 인증서의 상태를 검사해야 하며 자체적으로 CRL 목록을 유지하고 있어야 한다.

3.1 홈서비스 게이트웨이 PKI 구성요소

PKI는 (그림 6)과 같이 인증서를 발급 받는 최종개체(EE), 최종개체에게 인증서를 발급하는 인증기관(CA), 인증기관의 업무 중 신원확인 기능을 수행하는 등록기관(RA), 인증서나 CRL을 보관하기 위한 보관소 등으로 구성된다.



(그림 6) PKI 기본 구성 요소

최종개체는 일반적으로 사용자나 사용자가 사용하는 응용 프로그램을 의미하며 보관소는 인증기관이 발행한 인증서나 CRL을 보관하고 이를 요청하는 여러 사람들이 열람할 수 있도록 하는 시스템을 의미한다. PKI를 이용하는 홈서비스 게이트웨이에서는 인증서와 CRL을 관리하기 위해 LDAP(Light-weight Directory Access Protocol), HTTP, FTP(File Transfer Protocol), X.500 프로토콜을 지원해야 한다.

PKI에서 사용자는 먼저 자신의 인증서를 발급 받기 전에 인증기관과 연결하여 자신과 관련된 X.500 DN(Distinguished Name), 도메인 이름, IP 주소, 그리고 다른 속성 정보의 유효성을 제공받거나 제공하고, 이들의 유효성을 인증기관으로부터 검증 받아야 한다. 인증기관은 사용자에게 자신의 공개키나 공개키 인증서를 신뢰성 있게 제공하며, 사용자는 자신의 공개키/개인키 쌍을 생성할 수 있다. 인증기관이 사용자에게 인증서를 발행하고, 사용자에게 인증서를 전달하며, 보관소에 인증서를 공표한다. 일반적으로 초기화 과정과 인증 과정은 하나의 과정으로 동시에 수행된다.

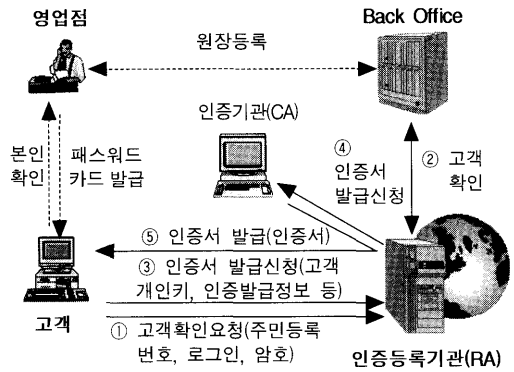
인증기관 또는 홈서비스 게이트웨이에 의하여 생성된 사용자의 개인키와 공개키는 무결성이 보장될 수 있도록 암호화된 형태로 전달되거나 스마트카드와 같은 물리적 토큰을 이용하여 전달되어야 한다.

상호 인증은 하나의 보안 영역과 다른 보안 영역간의 신뢰를 보장하기 위한 기법이다. 상호 인증은 하나의 인증기관이 다른 인증기관에게 발행해주는 상호 인증서를 이용하여 실행된다. 상호 인증서는 하나의 보안 영역에 있는 사용자와 다른 보안 영역에 있는 사용자간의 안전한 정보 교환을 가능케 한다.

4. 홈서비스 게이트웨이 보안 체계

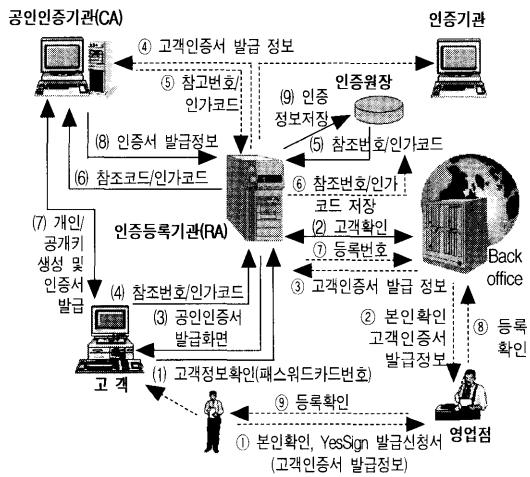
(그림 7)은 다양한 암호 및 인증 서비스를 제공하기 위해 본 논문에서 제안하고 있는 홈서비스 게이트웨이 사설 인증서 발급 방식을 나타내고 있다. 이 경우 CA와 RA는 홈서비스 게이트웨이가 되며 CRL을 저장하는 디렉터리 또한 홈서비스 게이트웨이에서 관리하게 된다. 따라서 CRL을 관리하기 위한 프로토콜과 인증 프로토콜의 선택이 유연하다는 장점이 있지만 SOHO (Small Office Home Office)와 같은 응용의 경우 모든 인증서를 홈서비스 게이트웨이가 관리해야

한다는 단점이 있다.



(그림 7) 홈서비스 게이트웨이 사설 인증서 발급 과정

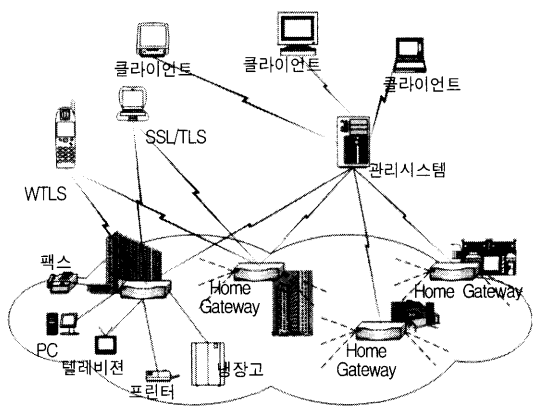
(그림 8)은 공인 인증서를 기반으로 패스워드와 OTPS(One Time Password System) 또는 보안 카드를 이용한 홈서비스 게이트웨이 최상급 보안 체계를 도시하고 있다. 이러한 방식을 이용하여 식별자나 비밀번호를 도용 및 데이터의 감청을 원천적으로 봉쇄할 수 있으며 공인 인증서를 기반으로 한 전자 서명을 사용하여 데이터의 무결성을 확보할 수 있다. 또한 전자 서명을 통하여



(그림 8) 홈서비스 게이트웨이 보안 인증서 발급 과정

홈서비스 게이트웨이 접속 사실에 대한 부인 방지를 수행할 수 있다.

(그림 9)는 홈서비스 게이트웨이 보안 관리 네트워크 구조를 도시하고 있다. 그림에서와 같이 홈서비스 게이트웨이는 관리 시스템에 의해 직접 관리 될 수도 있고 가입자가 유무선 인터페이스를 통해 직접 관리할 수 있기 때문에 이러한 모든 경우를 고려한 관리 인터페이스 및 MIB(Management Information Base) 구조를 갖고 있어야 한다. 대부분의 경우 가입자가 직접 홈서비스 게이트웨이를 관리할 것으로 보이며 무선 인터넷을 통한 안전한 통신채널을 제공하기 위해 홈서비스 게이트웨이는 무선 PKI 및 인증서 처리 기능 또한 제공해야 한다. 무선 구간의 통신 채널은 무선 인증서를 기반으로 WTLS(Wireless Transport Layer Security)를 이용하는 것이 가장 효과적이며 유선 구간은 이와 유사한 TLS(Transport Layer Security)를 이용한다.



(그림 9) 홈서비스 게이트웨이 보안 관리 구조

또한 관리 시스템을 통한 네트워크 관리는 SNM Pv3(Simple Network Management version 3)을 이용한 안전한 통신을 필요로 하기 때문에 홈서비스 게이트웨이의 모든 MIB는 SNM Pv3을 지원하는 형태로 구축이 된다.

5. 결 론

본 논문은 홈 네트워크의 중심이 되면서 다양한 유무선 인터페이스를 지원하는 홈서비스 게이트웨이의 보안체계에 관한 것이다. 강력한 인증과 암호화를 위해 본 논문에서는 사용자 등급 및 서비스 등급 별로 보안 등급을 분리할 것을 제안하고 있으며 특히 인증서 및 키 관리를 위해 PKI를 기반으로 하는 다양한 방식을 제안하였다.

홈서비스 게이트웨이의 다양한 암호 및 인증 체계는 유연하고 확장성 있는 서비스 시나리오를 보장할 뿐만 아니라 홈서비스 게이트웨이가 SOHO 영역에도 무리 없이 사용될 수 있는 효과적인 플랫폼을 제공한다.

특히 홈서비스 게이트웨이에서 VPN(Virtual Private Network) 서비스 지원은 네트워크에서 제공하는 다양한 보안 솔루션을 홈 네트워크에서 이용하게 할 수 있을 뿐만 아니라 네트워크 사업자로 하여금 서비스를 홈 네트워크 내부에 까지 확장할 수 있는 기반을 제공할 수 있다.

향후 홈서비스 게이트웨이의 용량을 고려한 RADIUS, 인증서 발급 절차, CRL 관리 프로토콜의 소형화가 필요로 할 것이다.

참 고 문 헌

[1] A. Nash, W, Duane, C. Joseph, D. Brink, "PKI Implementing and Managing E-Security", RSA, 2001.

[2] M. A. Hasan, "Power Analysis Attacks And Algorithmic Approaches To Their Countermeasures For Koblitz Curve Crypto-system", 1988.

[3] Dimitar Valtchev, et al., "Service Gateway Architecture for a Smart Home", IEEE Communications Magazine, Apr. 2002.

[4] Francois Bougant, et al., "The User Profile for the Virtual Home Environment", IEEE Communications Magazine, Jan. 2003.

[5] Nathan J. Muller, "SNMP's Remote Monitroing MIB", International Journal of Network Management, WILEY, Vol.6, No.1 1996.

[6] Brent A. Miller, et al. , "Home networking with Universal Plug and Play", IEEE Communications Magazine, Dec. 2001.

[7] 원동호, "현대 암호학", 2001.

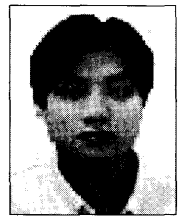
김 현 철

1990년 성균관대학교 정보공학과 (공학사)

1992년 성균관대학교 정보공학과 (공학석사)

1992년~2002년 한국전자통신 연구원 선임연구원

2002년~현재 (주) 아이트로닉스 소장



김 시 흥

2003년 성균관대학교 정보통신 공학부(공학사)

2002년~현재 성균관대학교 컴퓨터공학과 석사과정

안 성 진

1988년 성균관대학교 정보공학과 (공학사)

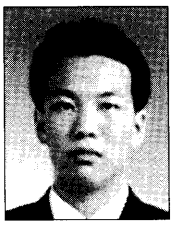
1990년 성균관대학교 정보공학과 (공학석사)

1998년 성균관대학교 전기전자 컴퓨터공학과(공학박사)

1999년~현재 성균관대학교 컴퓨터교육학과 조교수

정 진 욱

1974년 성균관대학교 전기공학과 (공학사)
1979년 성균관대학교 전자공학과 (공학석사)
1991년 서울대학교 전자계산학과 (이학박사)
1973년~1985년 한국과학기술연구소(KIST) 실장
1996년~현재 한국정보처리학회 회장
1996년~현재 정보보호 추진분과위원회 자문위원
1985년~현재 성균관대학교 전기전자 및 컴퓨터 공학부 교수
관심분야 : 네트워크 관리, 망 보안, 컴퓨터교육



유 윤 식

1999년 성균관대학교 전자공학과 (공학사)
2001년 성균관대학교 전기전자 컴퓨터공학부(공학석사)
2001년~현재 한국전자통신연구원 연구원

전 용 일

1981년 고려대학교 전기공학과 (공학사)
1983년 한국과학기술원 전기공학과(공학석사)
1983년~현재 한국전자통신연구원 책임연구원