情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

홈네트워크에서의 보안 요구사항 분석

정 재 학*

요 약

홈네트워크가 최근 주목을 받으면서 다양한 업계에서 구현되고 있다. 그러나 보안에 대한 고려를 충분히 하지 못한 상태에서 기능 구현에 주로 초점을 맞추고 있으며 최근에 와서야 보안에 대한 관심을 기울이고 있는 상황이다. 홈네트워크는 단일 서비스가 아닌 다양한 서비스의 집합으로서의 성격이 강하므로 보안에 대한 요구사항 또한 다양할 수 밖에 없다. 본 논문에서는 암호, 인증 기술을 기반으로 어떠한 요구사항이 있으며, 이를 위한 보안 대책에 대한 내용을 논의한다.

Ⅰ. 서 론

홈네트워크는 초고속 인터넷의 보급과 케이블 TV의 보급, 디지털 방송의 시작 등을 기반으로 망 사업자, 가전 기기 제조사, 방송 장비 제조사, 방송 및 컨텐츠 제공사, 건설사 등 다수의 사업자가 새로운 시장으로 개척을 시작하고 있는 상황이다. 정보통신부가 추진하고 있는 IT839 정책의 8대 서비스에 포함되어 있으며, 기업들은 컨소시엄을 구성해 홈네트워크 시범 단지를 구축하는 등 최근 활발한 개발이 진행 중이다. 그러나 초기부터 신규 시장으로서 서비스 구현에만 초점을 맞추어왔으며 역기능을 방지하기 위한 보안기능은 최근에 들어서야 관심의 대상이 된 것이 사실이다.

홈네트워크는 생활의 중심에서 편의성을 제공하는 서비스인 만큼 서비스를 제공받는 사용자 입장에서는 편의성만큼이나 그 역기능에 대한 우려가 클 수 밖에 없다. 이러한 역기능은 사생활 침해나 개인 정보의 노출, 개인 정보의 도용 등 많은 문제를 포함하며 다른 서비스에 비해 공격받는 사용자의 피해는 더욱 커질 수 있다. 따라서 서비스가 성공적으로 제공되기 위해서는 초기부터 보안 기능을 적절히 구현하여 이러한 문제를 차단하여야 한다.

또한 우리나라는 초고속 인터넷과 다양한 서비스 뿐 아니라 PKI 분야에서도 세계적인 인프라를 이미 구축하여 활용하고 있으므로 홈네트워크 분야에서도 이를 적극 활용하여 서비스의 안전성 및 활용도를 최대한 높일 수 있을 것으로 기대되는 바이다.

보안에는 침입 차단, 안티바이러스 등 다양한 분야가 있으나 본 논문에서는 암호, 인증 기능을 중심으로 홈네트워크의 각 서비스에 대한 보안 요구사항을 분석하고 이에 대한 보안 방안을 논한다.

Ⅱ. 홈네트워크 서비스

홈네트워크는 특정 망 또는 서비스를 규정하는 것이 아니라 가정을 기반으로 하는 다양한 서비스의 집합이라 할 수 있다. 따라서 서비스의 종류 및 형태는 매우 다양하며 현재 구현을 진행 중인 서비스 이외에도 실제 서비스를 진행하는 동안 새로운 서비스들이 계속 추가될 것이다. 따라서 지금 모든 서비스에 대한 정의를 내리는 것은 어려운 일이며 전형적인 서비스들을 대상으로 보안 요구사항 들을 분석하고 대책을 논의해 보기로 한다.

홈네트워크의 서비스는 크게 다음과 같이 분류될 수 있다.

⊙ 외부에서 내부로의 서비스
⊙ 내부에서 외부로의 서비스
⊙ 기기 메인터넌스 서비스

1. 외부에서 내부로의 서비스

외부에서 내부로의 서비스는 방범, 관제 서비스, 기기

* 소프트포럼 (주) (jhjung@softforum.com)

제어 등의 서비스가 있다. 방범, 관제 서비스는 외부에서 집의 상태를 모니터링하는 서비스로 침입 여부, 방문자 확인, 잠금 설정등의 서비스가 포함되며 기기 제어는 보일러, 에어컨의 작동 및 중지, 가스 및 전원의 차단, 반려동물 케어 등의 서비스가 포함된다. 이러한 서비스는 생활의 편의 및 안전을 고려하여 제공될 것이며 홈네트워크의 대표적인 서비스로 홍보되고 있다.

이 경우 정상적인 목적으로 사용되는 경우 편의 및 안전이 크게 증진될 것으로 기대되지만 반대로 악용될 경우 심각한 문제를 야기할 수 있다. 침입자가 침입을 시도하는 경우를 생각해 본다면 외부에서 집의 문이나 창문을 여는 기능을 제공하지 않더라도 보안 설정을 변경하여 방범 서비스를 해제할 수 있으면 보안 장치가 무용지물이 될 수 있다. 따라서 이러한 서비스는 반드시 사용자 인증이 필요하다. 또한 서비스 제공 회사의 직원의 접근에 대해서도 통제할 필요가 있으므로 권한 관리 또한 요구된다.

권한 관리의 경우 가구별로 접근 권한을 설정해서 관리해야 하는데 이러한 권한을 서비스 제공사의 서버에서 관리하거나 가구별로 설치되어 있는 게이트웨이기기에서 관리할 수 있다. 서버에서 관리하는 경우 서비스 제공사에서 설정을 대행해 주는 것이 용이하므로 편리한 측면이 있으나 서비스 제공사의 내부 직원에 의한 사고 등의 위험을 내포하고 있다. 가구 내에서 관리하는 경우 PC 또는 TV에서 인터페이스를 제공해야 하므로 구현상 어려움이 따르며 이에 대한 관리도 가구 내에서 직접 수행해야 하면 불편함이 수반되는 문제가 있다. 따라서 이러한 사용상의 편의성과 관리의 안전성을 함께 고려하여 서비스를 제공해야 한다.

2. 내부에서 외부로의 서비스

내부에서 외부로의 서비스는 집안에서 외부 서비스 제공자의 서비스를 받는 것으로 PC를 기반으로 서비스를 받는 것도 포함될 수 있으나 이는 홈네트워크의 개념과는 별도로 진행되고 있는 것으로 주로 TV를 기반으로 하는 서비스가 고려의 대상이 된다. 홈네트워크 안에서 또하나의 중요한 채널이 바로 TV를 기반으로 하는 서비스 이며 서비스 제공자의 수익 모델과도 직접적인 관계를 가지므로 상당한 주목을 받고 있다.

PC를 사용한 서비스는 그 대상이 제한된다면 TV를 기반으로 하는 서비스는 대상이 더욱 넓어지므로 그만큼 큰 시장이 될 수 있으며 광고 방송 또는 VOD 등 PC에서 제공하지 못하거나 PC 보다 더 좋은 품질로 제공할 수 있는 서비스를 통해 인터넷을 사용하는 새로운 시장을 열게 될 것이다.

TV를 기반으로 하는 서비스는 T-Commerce, T-Banking, VOD, 게임 등의 서비스와 기존 인터넷 포탈, 메일 서비스 등이 제공될 것이다. T-Commerce의 경우 디지털 방송과 결합하여 TV 시청 도중 상품을 구매하는 서비스가 대표적으로 홍보되고 있다. 그러나 이 경우 방송과 광고에 대한 법적인 문제가 선행되어 정리되어야 하므로 어려움이 따른다. 하지만 홈쇼핑 채널의 경우 방송의 목적이 광고이고 판매이므로 T-Commerce의 일차적인 수혜자가 될 것으로 보인다. 현재는 방송 시청 중에 구매를 위해서는 전화를 걸어 오퍼레이터 또는 ARS를 통해 구매를 신청하고 지불 정보, 배송지 등을 전달하는 방식을 사용하고 있다. 이 경우 T-Commerce와 연결된다면 광고 방송을 보는 중에 리모콘으로 구매를 선택하여 TV에 설치되어 있는 전자지갑을 구동하여 입력되어 있는 지불 정보와 배송지 정보를 전달하면 현재보다 훨씬 편리하고 정확하게 처리할 수 있다.

현재 인터넷을 통해 카드 결제를 하거나 인터넷 뱅킹으로 이체 거래를 위해서는 공인인증서 기반의 전자서명을 첨부하도록 되어 있다. 홈네트워크도 공중망 인터넷을 사용하므로 동일한 규정이 적용된다고 볼 수 있다. 따라서 T-Commerce, T-Banking을 구현하기 위해서는 공인인증서를 지원할 필요가 있다. 만일 공인인증서를 사용하지 않아도 되도록 적용한다면 PC 등의 다른 플랫폼에서도 TV와 동일한 방식으로 접속할 수 있으므로 기존 서비스에 대한 보안성 침해가 문제가 될 수 있으며 국가적으로 구축한 PKI 기반의 안전한 서비스 제공이라는 측면에서도 공인인증서 지원은 반드시 필요하다. 전자지갑을 구현하는 경우 사용자 인증을 통해 해당 정보에 접근하도록 하여야 하며 지불 정보 등은 암호화하여 저장하여야 한다.

공인인증서 지원을 위해서는 인증서의 이동성 지원이 필수적이다. 현재 공인인증서는 용도별로 1인 1인증서를 기반으로 하기 때문에 TV와 PC에서 동시에 사용하기 위해서는 이동성이 지원되어야 한다. 이를 위해서 TV 또는 셋톱 기기에서 스마트카드, USB 등의 인터페이스를 지원하거나 네트워크를 통해서 인증서를 TV로 이동하는 기능을 지원해야 한다.

VOD, 게임의 경우 역시 지불이 필요하며 이와 함께 사용자 나이에 의한 제한이 함께 고려되어야 한다. 방송의 경우 7세 이상 시청가, 12세 이상 시청가, 15세 이상 시청가, 19세 이상 시청가 등 네 등급으로 나눠지며, 영화 등급은 전체 관람가, 12세 관람가, 15세 관람가, 18

세 관람가, 제한 상영가 등 다섯 등급으로 분류되고 있으므로 사용자의 나이에 따른 제한을 제공하여야 한다. 이를 위해서는 사용자 식별과 인증이 제공되어야 하며 공인인증서를 사용한 본인 확인에 의한 나이 제한 서비스가 제공될 수 있다.

3. 기기 메인터넌스 서비스

서비스를 사용하는 동안 문제가 생기거나 기능의 개선 또는 문제의 보완등의 이유로 모듈을 갱신 또는 추가의 필요성이 생긴다. 이는 모든 서비스에 대해서 동일하게 발생하며 PC의 경우 사용자가 프로그램을 갱신하거나 자동으로 갱신하도록 하고 있다. PC의 경우 사용자가 내용을 확인하고 승인하면 갱신이 이루어진다. 그러나 홈네트워크 기기의 경우 인터페이스와 플랫폼이 상이하므로 PC와 같은 방식을 취할 수는 없다.

홈네트워크 기기는 네트워크에 항상 접속되어 있으므로 네트워크를 통한 자동 갱신이 유력한 방법이 될 수 있다. 하지만 이 경우 공격자가 불법적인 모듈로 갱신을 하거나 스파이웨어, 바이러스 등의 프로그램을 설치할 수 없도록 차단하는 것이 필요하다. 이를 위해서 전자 서명된 모듈을 검증하고 설치 할 수 있는 기능이 요구된다. Windows ActiveX 컨트롤의 경우 Authenticode라고 하는 전자 서명 기반의 코드 서명 기법을 사용하고 있으나 이 경우 프로그램 제조사를 확인시켜 주는 역할만 제공하며 설치 여부는 사용자의 판단에 맡기고 있다. 홈네트워크 기기의 메인터넌스를 위해서는 사용자 인터페이스 없이 자동으로 설치될 필요가 있으며 이를 위해서 기기에 기 등록된 인증서로 서명된 경우에 한해서만 설치되도록 하는 기능이 필요하다. 기기 제조사는 모듈에 대한 충분한 검증 후에 서명한 모듈을 전송해 이를 설치하여야 한다.

또한 기기의 설정 변경 또는 홈 기기 제어 등의 명령을 서비스 제공사가 사용하는 경우에 이로 인한 사고가 발생한다면 이에 따른 책임 여부가 문제가 될 수 있다. 이러한 책임을 밝히기 위한 기초 자료로 전자서명이 사용될 수 있다. 홈네트워크서비스는 단일 회사의 서비스보다는 여러 회사의 공동 서비스 형태로 제공되며 각 회사는 각자의 역할과 책임을 가지고 서비스를 제공하게 되므로 각사의 이해가 상충되는 문제가 발생할 수 있다.

Ⅲ. 관련 연구보안 기술

홈네트워크의 보안요구 사항에 따라 적용하여야 하는 보안 기술에 대해 분석한다.

1. 암호화

데이터의 암호화는 가장 광범위하게 적용되어야 하는 기능이다. 기본적으로 사용자의 사생활 보호라는 측면에서 본다면 거의 모든 데이터는 암호화되어 처리되어야 한다. 홈네트워크는 특성상 많은 가구가 하나의 네트워크에서 분기하여 서비스를 받는다. 이는 회사등의 환경과 가장 큰 차이를 보이는 것으로 회사의 경우 사내망의 경우 대부분 암호화 하지 않으나 홈네트워크의 경우 다른 가구로부터 반드시 보호받아야 하므로 아파트 단지와 같은 경우 단지 내의 트랜잭션에 대한 암호화가 반드시 제공되어야 한다.

2. 식별 및 인증

식별 및 인증을 위해서는 기본적인 ID/비밀번호 방식과 함께 공인인증서, 생체 인증 등이 사용될 수 있다. ID/비밀번호 방식의 경우 구현상 가장 간단하지만 사용자가 ID와 비밀번호를 입력하여야하므로 불편하며 보안성이 낮다는 것이 단점이다. 공인인증서의 경우 인증서 이동성 기능 제공 및 각 플랫폼상에서의 구현 등이 어려우나 비밀번호 만을 입력하며 전자서명, T-Commerce, T-Banking에의 활용과 높은 보안성 제공이 장점이다. 생체인증의 경우 사용자의 입력이 필요없으므로 편리하지만 지문 인식기 등의 장치를 요구하는 점이 단점이다. ID/비밀번호 방식과 지문 인증 방식에서는 사용자 인증 정보의 등록과 저장이 안전하게 구현되어야 한다.

이러한 인증 방식은 각각의 장점에 따라 함께 사용될 수 있다. 예를 들면 현관의 잠금장치는 지문 인증을 사용하고 TV 리모콘에 지문 인식 장치가 포함된 경우 TV 기반 서비스에서 지문 인증을 사용할 수 있으며, T-Commerce, T-Banking에서는 공인인증서 기반의 서비스를 사용하고 외부에서 접근하는 경우 사용자 설정에 따라 제한적으로 ID/비밀번호를 허용하는 등을 선택할 수 있다. 실 서비스에서는 보안성과 함께 편의성을 함께 고려하여야 하므로 사용자에게 선택을 맡기는 것도 필요하다.

3. 전자서명

전자서명은 사용자 인증, 부인 방지 및 코드 서명에도 사용된다. 전자서명을 사용하는 것은 성능 및 자원의 소요가 필요하므로 업무에 따라 적절히 적용하되, 만일의 경우를 대비할 수 있도록 업무의 성격을 충분히 분석하여 설계할 필요가 있다.

코드 서명은 앞장에서도 논한 바와 같이 기기의 모듈을 갱신하거나 추가할 때 기 등록된 인증서로 검증 성공한 모듈만을 설치하도록 하여 불법적인 모듈 또는 바이러스, 스파이웨어 등의 설치를 차단하도록 한다.

인증서는 공인인증서와 사설인증서를 사용할 수 있으며 업무의 성격에 따라 선택하여 사용할 수 있다.

4. 플랫폼

홈네트워크는 기존 서비스와는 달리 매우 다양한 기기를 함께 사용 하는 서비스로서 사용되는 플랫폼도 다양하다. 홈 게이트웨이, 셋톱 등의 장비는 Embedded Linux 또는 Windows CE 등을 주 OS로 사용하고 있으며 향후 다양한 Embedded OS가 사용될 수 있다. 또한 방송 셋탑의 경우 ACAP(Advanced Common Application Platform)/OCAP(Open Cable Application Platform)이라는 브라우저에 대응 되는 플랫폼을 사용한다. 또한 외부에서 사용자가 휴대폰을 통한 접속으로 사용할 수 있으며 내부에서 PC를 사용한 제어를 할 수 있다.

이와 같이 현재 사용중인 기기 또는 새롭게 만들어질 기기에서 함께 사용할 수 있어야만 한다. Embedded 기기의 경우 특히 자원 및 성능 상의 제약이 있을 수 있으며 상용화 후에 기능을 보완하는 것은 상당히 제한적이다. 따라서 초기부터 보안에 대한 고려를 충분히 하여 필요한 기능을 분석하고 이를 함께 구현할 필요가 있다.

Ⅳ. 결 론

홈시큐리티 서비스를 위해서는 가구 사용자의 인증과 권한 관리를 통해 접근을 통제하고, 각 접근에 대한 전자서명을 통해 명령에 대한 부인방지 기능을 제공하여야 한다. T-Commerce, T-Banking을 구현하기 위해서는 공인인증서를 지원해야 하며, 코드 서명을 위해 전자서명을 적용해야 한다.

홈네트워크는 다양한 서비스의 집합체인 만큼 각 서비스 별로 서로 다른 요구사항을 가지게 되며 동일한 기준을 모두 획일적으로 적용하기는 어렵다. 그러나 다른 서비스를 고려하지 않고 설계하게 되면 기능상의 충돌 등의 문제가 발생하게 되므로 전체 서비스를 대상으로 설계를 하여야만 한다. 이를 통해 일관성 있고 편리하게 사용할 수 있는 서비스를 제공해야 한다. 보안 기능 구현에서 또 하나 중요한 것은 실제로 사용하는 것이다. 기능은 포함되어 있으나 사용이 불편하여 사용자기 이를 배제하고 사용하게 되면 의미가 없으므로 사용의 편의성을 함께 고려하여야 한다.

공인인증서의 경우 강력하면서도 편리한 보안 기능을 제공할 수 있으며 사용자 인증, 본인 확인, 부인 방지 등 다양한 영역에 적용할 수 있으므로 사용의 편의성만 확보된다면 홈네트워크에서도 강력한 도구로 사용될 수 있을 것이다.

이상과 같이 홈네트워크 서비스는 기존 서비스와는 달리 더욱 다양하고 폭넓은 보안요구사항을 가지고 있으며 초기에 이러한 요구사항에 부합하는 시스템을 설계하여 구현하여야 할 것이다.

참 고 문 헌

[1] Cable Television Laboratories, Inc, "OpenCable Application Platform Specification", 2002

[2] Advanced Television Systems Committee, Inc, "Advanced Common Application Platform(ACAP)", 2004

[3] KISA, "홈네트워크 산업 활성화 정책방향", 최우혁

[4] TTA, "디지털 홈 네트워크 기술 표준개론", 2004. 4.

[5] TTA, "디지털 홈 기술 특집", TTA Journal, 2003. 7~8.

[6] 정보통신부, "지능형 홈네트워크 기획 보고서", 2003. 8.

[7] IITA 주간기술동향 1161호, "Home Network 발전 방향과 연구 개발 동향", 우문균, 2004.

〈著 者 紹 介〉

정 재 학(Jae Hak Jung)

1992년 8월 : 포항공과대학교 수학이학사

1995년 2월 : 서강대학교 대학원 전자계산학과 공학석사

1995년 11월 ~ 1999년 3월 : 미래산업 (주) 부설연구소 소프트포럼

1999년 4월 ~ 현재 : 소프트포럼 (주) 부설연구소 연구소장

〈관심분야〉 정보보호, PKI, 암호/인증 응용