Journal of the Society of Korea Industrial and Systems Engineering
Vol. 34, No. 4, pp.72－81, December 2011.

홈 네트워크에서의 적응적 통합 보안 정책 및 관리 기술

이상준* · 김이강* · 류승완**† · 박유진** · 조충호*

*고려대학교 컴퓨터정보학과
**중앙대학교 경영학부

Adaptive Convergence Security Policy and Management Technology of Home Network

Sang-Joon Lee* · Yi-Kang Kim* · Seungwan Ryu**† · You-Jin Park** · Choong-Ho Cho*

*Department of Computer Information Science, Korea University
**School of Business Administration, Chung-Ang University

In this paper, we propose adaptive convergence security policies and management technologies to improve security assurance in the home networking environment. Many security issues may arise in the home networking environment. Examples of such security issues include the user privacy, the service security, the integrated networking security, the middleware security and the device failure. All these security issues, however, should be fulfilled in phase due to many difficulties including deployment cost and technical complexity. For instance, fundamental security requirements such as authentication, access control and prevention of crime and disaster should be addressed first. Then, supplementary security policies and diverse security management technologies should be fulfilled. In this paper, we classify these requirements into three categories, a service authentication, a user authentication and a device authentication, and propose security policies and management technologies for each requirement. Since the home gateway is responsible for interconnection of many home devices and external network access, a variety of context information could be collected from such devices.

Keywords : Context Aware, Home Network, Access Control, Security, Policy

1. 서 론

최근 신축 아파트에는 기본적으로 홈 네트워크 서비스가 제공되고 있다. 이러한 홈 네트워크 서비스가 점차 보급되면서 향후 사용자의 요구에 따라 다양한 기기들이 서버에 연결되어 편리함을 가져다 줄 것이다. 또한 사용자는 다양한 홈 네트워크 서비스들을 댁내외 어디에서든 이용할 수 있는 원격 제어 서비스를 제공받아 편의성이 증대된 서비스들을 사용하기를 원하게 된다.

그러나 홈 네트워크 서비스의 보급이 확대되고 원격제어 서비스 등이 통신 네트워크를 통해 제공되면서 홈 네트워크 보안 문제가 주요 해결 이슈로 부각되고 있다. 홈 네트워크에서 발생 가능한 주요 보안 문제

논문접수일 : 2011년 10월 10일 게재확정일 : 2011년 10월 28일
† 교신저자 ryu@cau.ac.kr
※ 이 연구는 지식경제부 산업원천기술개발사업의 '고효율 건물에너지 감응형 EMM 플랫폼 기술 개발' 사업(10035142)의 지원을 받아 수행하였습니다.

중에는 다양한 기기들이 서버와 연결됨으로써 발생하는 기기 오작동에 의한 위협과 서버에 침입하여 기기를 불법 제어하는 해커에 의한 위협 등이 존재한다.

본 논문에서는 이러한 홈 네트워크에서 발생하는 보안문제들을 해결하기 위한 방안으로 홈 네트워크의 적응적 통합 보안 정책 및 관리 기술을 제안한다. 본 논문에서 제안하는 보안 정책이란 위협 상황에 따라 변경되는 적응적인 대응방안들을 의미하며, 이러한 보안 정책들은 다양한 모듈로서 구현될 수 있다. 이를 위해 우선 홈 네트워크에서 발생하는 보안 문제를 정의하고 해결하기 위한 각종 보안요구사항들을 정의하였다. 이러한 요구사항은 크게 서비스 요구사항, 기기 요구사항 및 사용자 요구사항으로 분류될 수 있다. 이를 바탕으로 접근제어와 상황인지 정책을 기반으로 하는 홈 네트워크 통합 보안 정책을 제시하였다. 특히 상황인지 기반 보안 서비스 제공을 위해 보안 상황인지 모듈의 구성방법과 보안 상황인지 시나리오를 제시하였다. 이러한 접근제어와 상황인지 기반의 보안 정책이 적용된 모듈들은 월패드(Wall-Pad)와 셋탑박스(Settop-Box)에 내장되는 모듈들로 구현하였다.

본 논문의 구성은 제 2장에서 홈 네트워크의 표준화 동향에 대한 분석을 하고, 제 3장에서 홈 네트워크의 주요 보안 요구사항에 대해 알아본다. 제 4장에서는 제안하는 적응적 통합 보안 정책에 대해 기술하고 제 5장에서는 홈 네트워크 구성 및 구현을 설명하며, 마지막으로 제 6장에서 결론을 맺는다.

2. 홈 네트워크 관련 연구 동향

2.1 국내외 표준화 동향

홈 네트워크 보안에 대한 국내 표준화는 현재까지 ITU-T에서 진행 중인 표준안이 3건이 있으며, 2005년부터 ITU-T에서 진행 중인 표준안들은 Study Group 17의 Question9에서 진행 중이다. Question9는 X-homesec-1, X-homesec-2, X-homesec-3의 세 부분으로 나뉘어 있고, X-homesec-1은 "Framework of security technologies for home network", X-homesec-2는 "Device certificate profile for the home network", X-homesec-1은 "User authentication mechanism for home network service"라는 제목으로 표준화가 진행 중이다. 국외 표준화로는 2005년에 ISO에서 제안한 표준안이 한 건 있다. 이 표준안은 홈 네트워크 보안 전반에 관하여 다룬 표준으로 ISO/IEC에서 홈 네트워크 보안 표준이 2005년 6월에 발표되었고, 크게 보안 요구사항, 댁내 보안 서비스, 댁외 보안 서비스로 나뉘어 표준이 완성되었다. 이 표준에서는 홈 게이트웨이 중심의 홈 네트워크 모델을 정립하여, 해당 모델에 적절한 보안 요구사항 및 댁 내외 보안 서비스들을 정의하였다[9, 13].

<그림 1>은 이 표준안에서 제시하는 댁내외 보안에 대한 개략도이다. 댁내 환경에는 다양한 종류의 기기 및 통신매체들이 있고, 그 중 외부 공격에 대해 안전성이 확보되지 않은 통신매체들도 있기 때문에 SCMP (Security Continuity Management Protocol)를 두어 댁내 보안을 제공한다. 그리고 댁외 환경에는 인터넷을 이용하여 홈 네트워크가 연결되어 있으므로 새로운 프로토콜을 제시하지 않고, 기존의 인터넷 보안 프로토콜을 이용한다. 즉, 네트워크 계층의 보안을 위해서 IPsec을 이용하고, 세션 계층의 보안을 위해서 SSL(Secure Socket Layer) 혹은 TLS(Transport Layer Security)를 이용한다.

국내 홈 네트워크 보안 표준화 작업은 한국정보통신기술협회(Telecommunication Technology Association(TTA))의 정보보호기반 프로젝트 그룹(PG101)과 홈 네트워크 시큐리티 포럼(Homenetwork Security Forum(HNSF))을 중심으로 진행되고 있으며, 2004년 홈 네트워크 사용자 인증 메커니즘에 관한 표준안이 HNSF에 제출된 것을 시작으로 홈 네트워크 보안에 관한 국내 표준화 활동이 시작되었다. 홈 네트워크 사용자 인증 메커니즘에 관한 표준은 검토 회의를 거쳐, 2005년에 TTA와 HNSF에서 표준으로 제정되었다. 2006년에는 홈 네트워크 보안정책 기술 언어에 관한 표준안이 TTA(PG101)와 HNSF에 제출되었고, 2006년 12월 표준으로 제정되었다. 또한, 홈 네트워크를 위한 보안기술 프레임워크에 관한 표준안이 TTA(PG101)에 제출되었고, 역시 2006년 12월 표준으로 제정되었다.

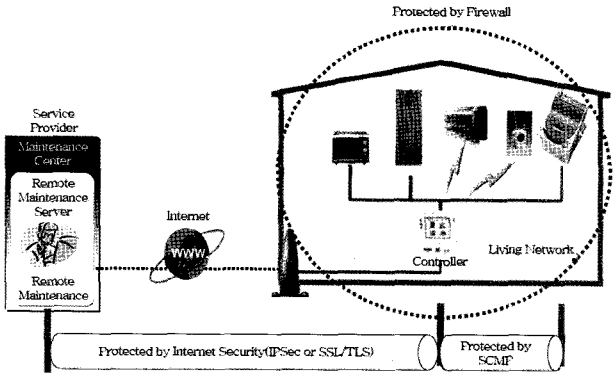
이덕규 외[3]는 안전한 홈 네트워크 서비스 제공을 위해 필요한 사용자 인증 메커니즘과 홈 게이트웨이와 홈 네트워크 사업자 인증서버 간 기기인증 메커니즘에 관하여 정의하였고, 또한 홈 네트워크 서비스를 댁내 기기 제어, 홈 네트워크 사업자 인증 서버가 제공하는 서비스 이용, 댁외에서의 댁내 기기 제어 등의 세 가지로 구분하였으며, 이 서비스 이용에 필요한 사용자 인증 메커니즘을 제시하고 있다. <그림 2>는 사용자 인증메커니즘에 대한 세 가지 경우를 도식화한 것이다.

2.2 국내외 관련 연구 동향

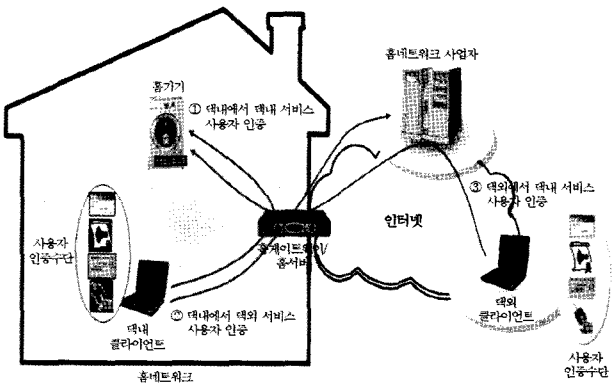
홈 네트워크 시스템이 인터넷에 연결됨에 따라 불법적인 침입자로 인한 도청 및 변조에 대한 대책이 요구되고 있다. 일반적으로 데이터의 보안을 위한 여러 가지 방법 중 암호화하는 방법이 가장 안전한 데

이터 보안 방법으로 사용되고 있다.

국내외 관련 연구로써, 주성호 외[6]와 이정열 외[4]은 전력선 통신(Power Line Communication(PLC))에서 발생하는 데이터 보안 문제를 다루고 있고, 키 교환을 통한 데이터 전송을 사용한다. Kim et al.[10]은 다중 홉 환경의 홈 네트워크에서의 보안을 다루었으며, 이 경우 홉들 간의 데이터 교환 시 키 보안이 중요 기술적 이슈이다. Tseng et al.[11]은 생체정보를 바탕으로 데이터 보안에 대해 다루었고, 박현문 외[1]와 조수형 외[5]는 ZigBee 및 RS-485 기반 무선 센서 네트워크에 대한 보안을 홈 게이트웨이에서 해결방안을 찾고 있다.



<그림 1> 댁내 및 댁외 보안



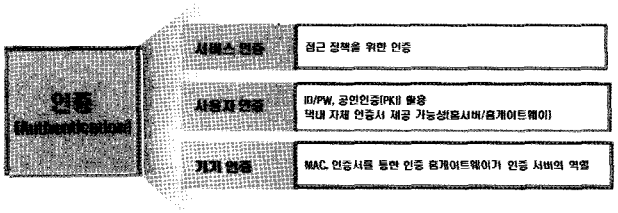
<그림 2> 사용자 인증 메커니즘

그러나 이러한 기존연구들에서는 PDA, PLC, 데이터 보안 등과 같은 특정 상황 및 기기 사용 환경을 가정하고 이에 적합한 제한적으로 최적화된 보안 아이디어를 제시하고 있다. 그러나 홈 네트워크는 다양한 기기들을 연결하여 서비스를 제공하기 위해 각종 인터페이스를 기반으로 통신이 이루어지기 때문에 보다 근본적이고 통합적인 보안정책의 수립 및 관리가 필수적이다. 따라서 본 논문에서는 다양한 기기가 연결되고 댁내외에서 서비스 사용이 가능한 홈 네트워크 환경에서 수집된 다양한 정보를 기반으로 제공되는 상황인지 기반의 적응적이고 통합적인 보안 정책을 제시하고 구현한다.

3. 홈 네트워크 보안 요구사항

홈 네트워크라는 환경은 일상생활과 밀접하게 연관된 정보가전기기들에 내장되어야 하므로 경제적이고 높은 신뢰성을 제공해야 한다. 최근 네트워크 환경은 이동성과 편리성, 보안성이 차지하는 부분이 점차 커짐에 따라 각각의 조직과 사용자의 필요에 따라 네트워크 사용 권한을 부여하는 인증 중심의 통합 보안 솔루션 도입도 고려해야 할 것이다.

홈 네트워크의 보안 요구 사항은 프라이버시, 서비스, 통합 네트워크, 미들웨어, 기기 등의 측면에서 다양하게 존재한다. 다양한 측면에서의 보안 요구사항을 기반으로 홈 네트워크 보안을 구축해야 하지만 개발 초기단계부터 모든 요구사항을 충족시키기는 비용적 측면 및 개발 기간에 비추어 많은 어려움이 있다. 따라서 우선적으로 인증과 접근제어, 방범/방재와 같은 가장 기초적이고 중요한 분야의 보안 정책을 정립한 후 이에 부가하여 다양한 보안정책을 수립하고 제공하는 단계적 접근법이 요구된다. 특히, 홈 네트워크에서의 인증 및 접근 제어는 가장 기본적이면서 중요한 보안 요구사항으로서 <그림 3>에서 제시하는 바와 같이 서비스 인증, 사용자 인증 및 기기 인증으로 구분할 수 있다[2, 7]. 서비스 인증은 접근 정책을 위한 인증을 의미하며, 사용자 인증은 ID/PW, 공인인증서, 댁내 자체 인증서 등을 활용한 홈 서버 및 홈 게이트웨이에서의 사용자 인증이며, 기기인증은 MAC 등을 통한 홈 게이트웨이에서의 다양한 기기 인증을 의미한다.

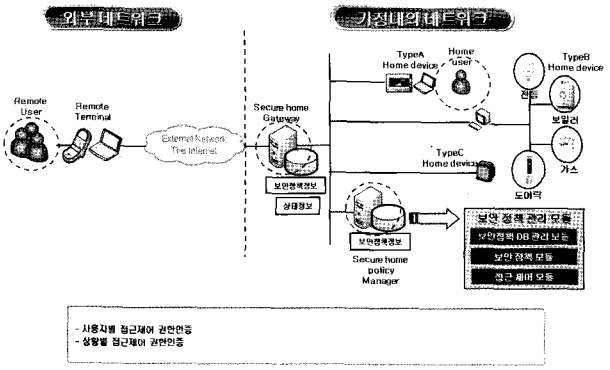


<그림 3> 홈 네트워크 인증 체계

3.1 서비스 인증

제어할 기기와 서비스에 따라 홈 네트워크 자원에 대한 접근권한 제어 기능이 요구된다. 구성원 별로 제

공받을 수 있는 홈 네트워크 기반 서비스의 종류가 다르고, 홈 네트워크 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근제어 기능이 필요하다. 유비쿼터스 컴퓨팅 환경을 고려할 때 접근제어를 위한 ACL(Access Control List)은 단말 기기가 내장하고 있는 것이 효율적이라고 할 수 있지만 안전성 및 편리성 측면에서 일관된 보안정책을 따라 서버에서 접근 권한이 제어되어야 할 것이다. <그림 4>는 서비스 인증의 기본 개념을 나타낸 것이다.



<그림 4> 서비스 인증

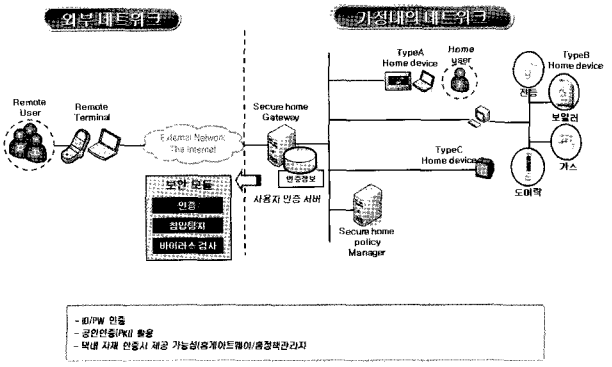
3.2 사용자 인증

사용자 인증 기술은 홈 네트워크 제어를 위한 1차 보안 과정이라 할 수 있다. 또한 홈 네트워크에서 구성원의 의지에 따라 사용자 인증을 요청하는 경우도 있지만, 구성원 의지와 관계없이 구성원 상황에 따라 사용자가 인증되어 구성원에 적합한 서비스가 제공되는 경우도 예상할 수 있다. 예를 들어 중요한 기기나 과금 서비스에 대한 접근이 필요할 때 사용자에게 지문, 홍채 등의 2차 인증을 거치는 방법이다.

본 논문에서 제시한 사용자 인증 환경에서는 ID/PW를 사용하여 댁내/댁외를 구별한 사용자 인증 과정을 거친다. 일반적인 댁외 사용자 인증은 ID/PW 방식을 따르고, 댁내 인증은 PW방식을 따른다. 또한 댁내 보안 상황에 따라서 중요한 기기를 제어할 경우에는 2차적인 인증을 요구한다. <그림 5>는 사용자 인증의 기본 개념을 도식화한 것이다.

3.3 기기 인증

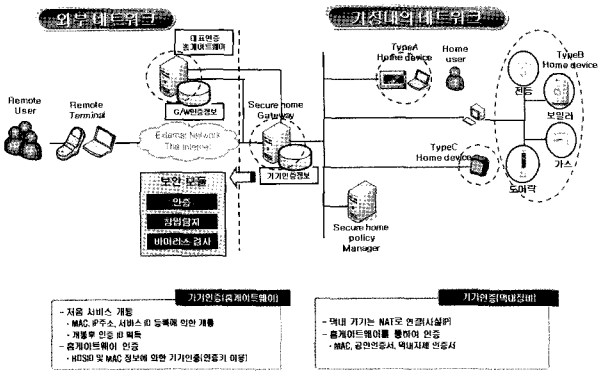
불법 기기의 사용을 방지하기 위해서는 홈 네트워크 구성요소인 기기 자체에 대한 인증 과정이 필요하다. 기기 인증 과정이 없다면, 댁내에서 불법적인 외부 무선기기가 아무런 제약 없이 자유롭게 설치되고,



<그림 5> 사용자 인증

사용되고, 제거될 수 있게 된다.

현재까지 기기 인증은 통합 홈 네트워크 환경에서의 미들웨어 레벨에서 제공되고 있다. 예를 들어, UPnP(Universal Plug and Play) 경우 기기마다 부여된 Security ID로 기기의 홈 네트워크 등록과정에서 기기 인증이 이루어지고 있으며, Havi 경우에는 기기마다 고유한 인증서를 발행하여 기기 인증 수행 시 사용하고 있다. 따라서 향후 기기에 대한 안전하고 다양한 서비스 제공을 위해서는 기기 인증정보에 대한 통일된 발급 및 관리 체계에 대한 기술적, 정책적인 연구가 필요할 것으로 보인다. <그림 6>은 기기 인증의 기본 개념을 나타낸 것이다.



<그림 6> 기기 인증

3.4 기타 인증

앞서 제시한 세 가지 인증 외에도 홈 네트워크 구성요소 간의 자원공유를 위하기 위한 기기 간 인증, 홈 네트워크에 사용되는 다양한 미들웨어를 위한 미들웨어 보안 등이 있다. 홈 네트워크의 활성화를 위해서는 안전성 강화도 중요하지만 사용자 편리성 또한 고려되어야 할 사항 중의 하나이다. 높은 안전성은 사용자 측면의 편리성을 저해할 수 있으며, 이에 반해 높

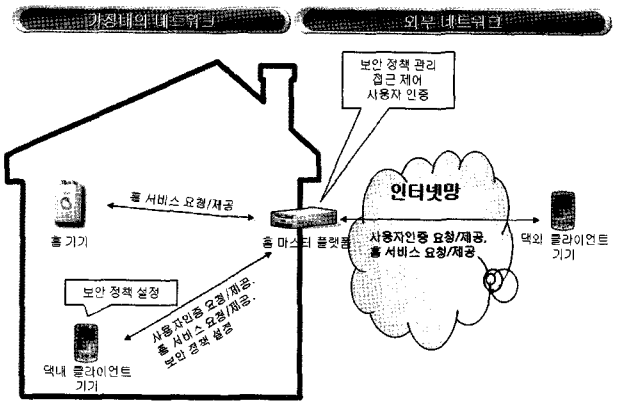
은 사용자 편리성은 홈 네트워크의 보안 안전성에서 취약할 수 있다.

향후 이기종의 다양한 유무선 네트워크와 다양한 프로토콜들이 혼재하는 네트워크 환경이 구축되는 추세이므로 이에 따라 기존 인터넷 등에서 발생되던 보안 취약성 외에도 추가적으로 많은 보안 취약성을 고려해야 할 것이다. 따라서 다양한 기기들과 다양한 통신환경이 존재하는 홈 네트워크 환경에서는 사용자의 개입 없이 자동화된 규칙에 의해 적응적으로 보안정책이 제공되고 관리되는 적응적 통합보안 정책기술의 개발이 시급한 실정이다.

4. 적응적 통합 보안 정책

홈 네트워크를 위한 인증 및 접근권한 제어 기술은 서비스 접근 시 사용자 인증 및 접근 권한 검증을 통하여 권한이 있는 사용자만이 서비스를 이용할 수 있도록 함으로써 안전한 홈 네트워크 구축이 가능하도록 한다. 홈 네트워크를 위한 인증 및 접근권한 제어 기술은 보안 정책 관리, 사용자 인증, 접근 제어의 세 가지 기술들로 구성되어 있다. 이들 기술들은 보안 관리자가 보안 정책을 설정한 후 접근 제어 모듈에게 설정된 보안 정책을 넘겨주고 인증 모듈에서 인증을 수행하여 인증 결과를 접근 제어 모듈에게 넘겨주면, 접근 제어 모듈은 인증된 사용자의 특정 장치나 서비스에 대한 접근 권한 검증을 수행하는 것으로 서로 연동된다.

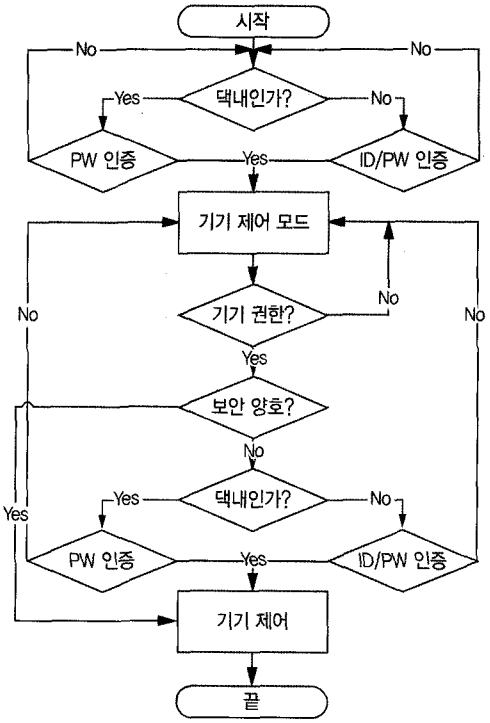
홈 게이트웨이 역할을 하는 셋탑박스와 월패드는 사용자 인증 모듈, 접근 제어 모듈, 보안 정책 관리 모듈이 탑재되어 홈 네트워크를 위한 인증 및 접근권한 제어 서비스가 이루어진다. <그림 7>은 홈 네트워크를 위한 인증 및 접근권한 제어 기술이 적용되는 상황을 개략적으로 나타낸 것이다.



<그림 7> 인증 및 접근권한 제어 기술 적용 사례

4.1 접근 제어(Access Control)

<그림 8>은 본 논문에서 제안하는 접근 제어 방식이다. 우선, 홈 네트워크 서비스 사용자가 댁외나 댁내에서 홈 네트워크 서버에 접근하면 홈 네트워크 서버는 접근한 사용자가 댁내인지 댁외인지 판별하여 다른 방식으로 인증을 요구한다. 댁외일 경우, PC를 사용한 접근이나 모바일 장비를 이용하기 때문에 ID와 PW를 요구하여 인증을 하게 되고, 댁내일 경우, 손으로 간편하게 터치하거나 IPTV를 이용한 리모컨 제어를 할 것이기 때문에 간단하게 PW만으로 인증을 요구하여 사용자가 누구인지 판별한다.



<그림 8> 제안하는 접근 제어 방식

사용자 인증 과정이 끝나면, 기기 제어 모드로 들어가게 되는데, 홈 네트워크 서버는 인증이 완료된 사용자가 누구인지 식별하게 되며, 사용자마다 부여가 기기제어 권한 DB를 기반으로 기기 제어를 하게 된다. 해당 기기에 권한이 있다면 제어가 가능하고, 해당 기기에 권한이 없다면 제어가 불가능하다.

접근제어의 권한에 따른 기기제어 방식에서 더 나아가 현재 홈 네트워크 시스템의 보안 상황에 따른 권한 제약 모듈이 있다. 다시 말하면, 인증된 사용자가 해당 기기에 대한 권한이 있지만, 홈 네트워크 서버가 현재 시스템 보안 상황에 위험 요소가 존재한다고 판단하면 권한이 부여된 기기임에도 불구하고 기기

제어에 제약을 한다. 제약이란 한 번 더 인증을 요구하는 것으로써 한, 두 번의 인증을 더 거친다면, 비로소 기기 제어를 할 수 있을 것이다.

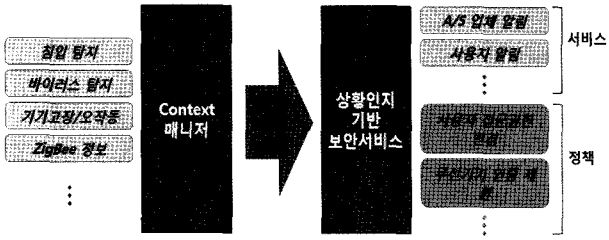
4.2 상황 인지

유비쿼터스 홈의 고도화된 서비스를 제공하기 위해서는 빠른 상황인지 기술, 상황에 따른 정보를 다양한 방법으로 제공하는 기능, 홈 서버로의 지속적인 저장/관리 기술 등이 필요하다.

본 논문에서는 프로파일 정보에 대한 저장, 관리가 가능하고 환경 추론 및 서비스 결정, 정책적 관리에 따른 서비스 제공을 통해 사용자에게 유비쿼터스 홈에 적합한 보안 상황인지 서비스를 제공하고자 한다.

4.2.1 보안 상황인지 서비스 모델

보안 상황인지란 홈 네트워크 시스템에 적용된 다양한 센서 및 탐지 장치들을 통해 탐지된 정보를 토대로 상황을 분석하고, 보안 정책에 따라 보안 등급을 조정하여 홈 네트워크 시스템의 안전성을 확보하는 방법이다. <그림 9>는 보안상황인지의 서비스모델을 나타내고 있다. 센서 및 다양한 탐지 장치들로부터 수집된 침입탐지, 바이러스탐지, 기기고장 및 오작동 등의 정보를 분석하여 상황인지 기반 보안 모듈을 통해 A/S 업체 알림, 사용자 알림 등의 서비스와 사용자 접근권한 변경, 무선기기 인증제한 등의 정책을 실행하게 된다. 보안 상황인지의 주목적은 현재와 과거의 보안위협을 분석하여, 추가적인 위협을 방지하고, 홈 네트워크 시스템의 안정적인 동작을 위함이다.



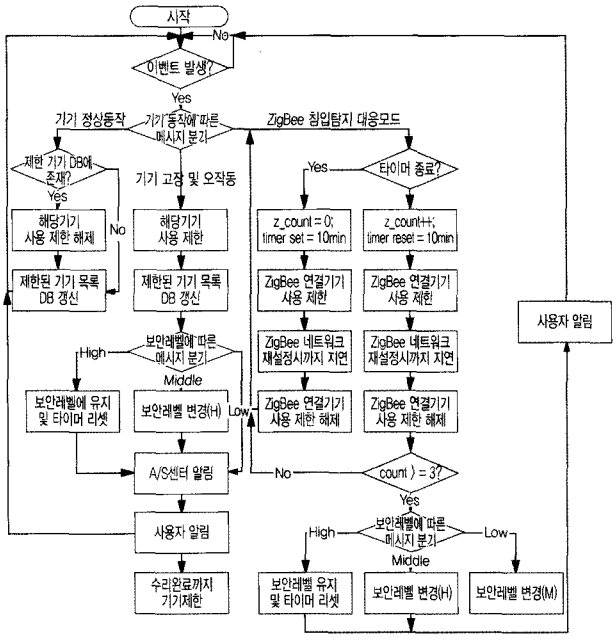
<그림 9> 보안상황인지 서비스 모델

4.2.2 보안 상황인지 모듈

<그림 10>은 보안상황인지 모듈의 동작 메커니즘을 나타낸 것이다. 먼저 보안 상황 이벤트 메시지를 받은 보안상황인지 모듈은 해당 메시지를 판독하여 기기고장, 바이러스, 침입탐지 등의 위협상황과 기기정상동작, 심각한 바이러스 해결 등의 위협상황 해결 메시지로 분류하고, 해당 이벤트를 받는 것을 시작으로 모듈이 동작한다.

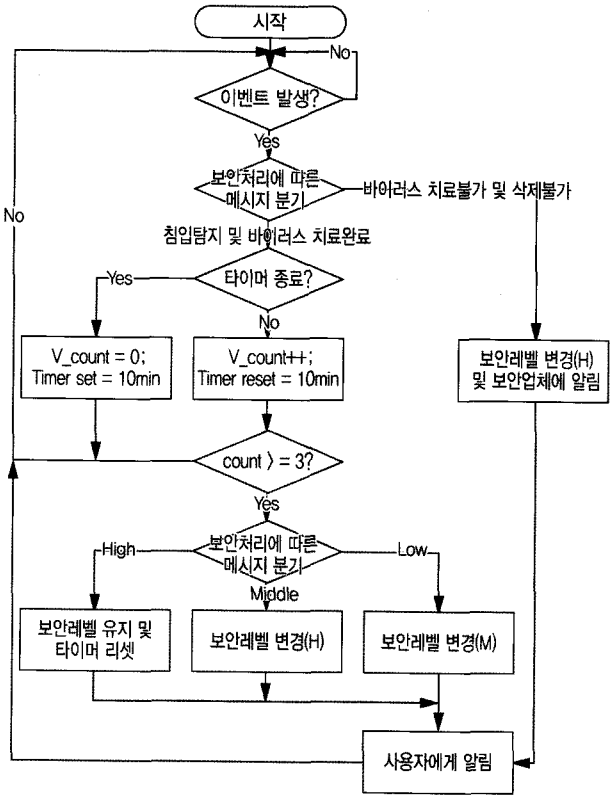
먼저 기기고장 메시지일 경우, 해당기기의 사용을 제한하고, 제한기기 목록을 업데이트 하게 된다. 그리고 추가적인 위협이 있었는지를 확인하기 위해 현재의 보안레벨을 확인하는데, 현재의 보안레벨이 Default(Low)가 아니라면 이전에 보안위협이 있었던 것으로 판단하고, 현재 발생한 기기고장 메시지가 이전의 보안위협에 영향을 받은 것으로 생각할 수 있기 때문에 보안레벨을 수정하게 된다. 그리고 해당기기의 A/S 업체에 알리고, 사용자에게도 기기고장에 대한 것을 알리게 된다. 그리고 해당기기의 사용제한 해제는 해당 기기의 수리가 완료되어 기기 정상동작 메시지가 발생하게 되면 하도록 한다.

다음으로 ZigBee 기기에 대한 해킹이나 기타 침입탐지가 발생하면, ZigBee 자체적으로 대응모드를 수행하게 된다. ZigBee의 침입탐지 대응모드가 실행되면 보안상황인지 모듈은 무선 위협으로부터 홈 네트워크 시스템을 보호하기 위해 보안레벨을 변경하게 되는데, ZigBee 자체의 대응모드가 있기 때문에, 심각한 위협으로 판단하지 않고, 대응모드 발생 즉시 보안레벨을 변경하지 않는다. 보안레벨 변경방법은 먼저 대응모드가 발생하게 되면, 대응모드 발생의 횟수를 저장하게 된다. 동시에 대응모드 발생시간을 측정하여, 일정시간 안에 ZigBee 침입탐지 대응모드가 여러 번 발생하면 악의적인 위협이라고 판단하고 보안레벨을 변경하게 된다. 발생 횟수는 보안레벨이 수시로 변하는 것을 방지하기 위해 사용되며 본 연구에서는 3회의 발생횟수를 사용하였다.



<그림 10> 상황인지 모듈 동작 메커니즘

ZigBee는 홈 기기를 연결하여 무선으로 제어할 수 있도록 하는 장치이므로, 침입탐지 대응모드가 발생하게 되면, ZigBee 기기와 연결된 홈 기기는 사용을 할 수 없게 된다. 따라서 ZigBee 기기와 연결된 홈 기기의 사용을 제한하게 된다. 보안레벨을 변경한 후 현재의 보안위협과 대응상황을 사용자에게 알림으로 ZigBee 침입탐지 대응모드를 완료하게 되고, ZigBee 침입탐지 대응모드가 완료(ZigBee 네트워크 재설정 완료)되었다는 메시지를 확인하면, 사용이 제한되었던 ZigBee 연결 기기의 사용제한을 해제하게 된다.

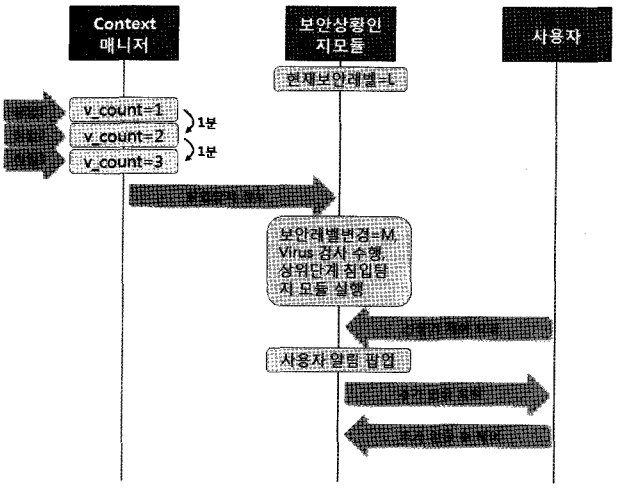


<그림 11> 상황인지 모듈 동작 메커니즘(유선침입 및 바이러스 탐지의 예)

<그림 11>은 홈 네트워크 시스템에서 유선으로의 침입탐지 혹은 바이러스가 발생했을 때의 보안상황인지 모듈의 동작 메커니즘을 제시하고 있다. 먼저 이벤트 메시지는 바이러스 치료 완료 혹은 침입탐지 처리완료 등과 같이 보안위협을 안전하게 해결했다는 메시지와 바이러스 치료불가와 같이 심각한 위협 메시지로 구분하게 된다. 바이러스 치료완료와 같이 추가적인 모듈에서 홈 네트워크 시스템에 영향을 주지 않도록 처리가 된 위협들은 위의 ZigBee 침입탐지 대응모드에서와 동일하게 동작하게 된다. 다음으로 심각한 위협 메시지가 발생하게 되면 홈 네트워크 시스템의 보안상황인지 모듈은 보안레벨을 최상위 단계(High)로 설정하고, 보안업체와 사용자에게 알리게 된다. 일반적으로 보안레벨이 변경이 되었을 경우에는 보안레벨의 하향조정은 일정한 시간을 정하여 시간이 지나면 자동적으로 하향 조정되게 되는데, 심각한 위협 발생 시에는 해당 위협이 처리가 되었다는 메시지를 받았을 때 보안레벨 하향조정이 시작된다. 보안 상황인지 모듈에서 처리한 모든 이벤트와 처리 방법은 로그 데이터베이스에 저장되게 되며, 주기적으로 사용자와 보안업체에 알리게 된다.

4.2.3 보안상황인지 시나리오

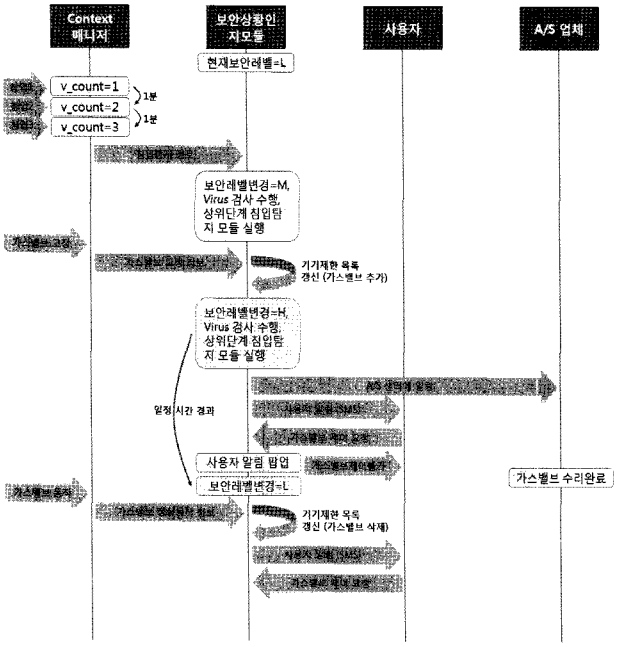
<그림 12>는 단일 보안 위협 발생(침입탐지) 시 보안상황인지 시나리오를 예시적으로 나타내고 있다. <그림 12>의 보안상황인지 시나리오에서는 먼저 침입탐지 메시지가 1분 간격으로 3번 발생을 하게 되면 Context 매니저는 침입탐지 횟수를 저장하고, 홈 네트워크 시스템에 악영향을 미칠 것으로 판단하여 침입탐지 정보를 보안상황인지 모듈에 알린다. 침입탐지 정보를 확인하여 보안상황인지 모듈은 보안레벨을 한 단계 높이게 되고, 높여진 보안레벨을 참조하여 바이러스 검사와 상위단계의 침입탐지 모듈을 동작시키게 된다. 보안레벨이 높아진 상황에서 사용자가 홈 기기 제어를 요청하게 되면 기기 제어 화면에 알림 창으로 사용자에게 현재의 보안상태를 알리게 되고, 보안상황인지 모듈은 사용자에게 추가적인 인증을 요구하고, 사용자는 추가적인 인증 후 홈 기기를 제어할 수 있게 된다.



<그림 12> 단일 위협상황의 보안상황인지 시나리오 예시

<그림 13>은 홈 네트워크 시스템에 보안위협이 복합적으로 발생했을 때의 경우의 보안상황인지 시나리오를 예시적으로 나타내고 있다. 우선 침입탐지 발생 시 홈 네트워크 시스템의 보안상황인지 모듈 동작은 앞의

단일 보안위협 시나리오의 내용과 같다. 보안레벨이 하향 조정되기 전에 다른 보안위협(기기고장 등)이 발생하면, 보안상황인지 모듈은 고장 난 기기의 사용을 제한하고, 보안레벨을 상향조정하게 된다. 상향 조정된 보안레벨을 참조하여 바이러스 검사와 상위단계의 침입탐지 모듈을 동작시키게 된다. 또한, 보안상황인지 모듈에서는 고장난기기의 A/S업체에 수리 요청을 하고, 사용자에게 알리도록 한다. 이때 사용자가 해당 기기를 제어하려고 하면, 제어화면에 현재의 보안 상태를 알리고, 추가적인 인증을 요구하거나 사용제한 메시지를 보여준다. 현재 보안레벨에 따라 원격 제어가 가능한 기기의 기능이 제한되며, 위험도 높은 기기의 경우는 제어가 불가능 할 수도 있다. A/S업체에서 고장 난 기기를 수리하면, 홈 기기는 트랜시버를 통해 홈 네트워크 시스템으로 정상동작 메시지를 보내고, 메시지를 받은 보안상황인지 모듈은 해당기기의 제한을 해제하게 되고, 사용자에게 SMS로 기기 수리가 완료되었음을 알린다. 일정한 시간이 지나면 보안레벨이 하향 조정되게 되는데, 이때 사용자는 정상적으로 기기제어 및 홈 네트워크 시스템의 서비스를 이용할 수 있다.



<그림 13> 다중 위협상황의 보안상황인지 시나리오 예시

5. 홈 네트워크 구성 및 구현

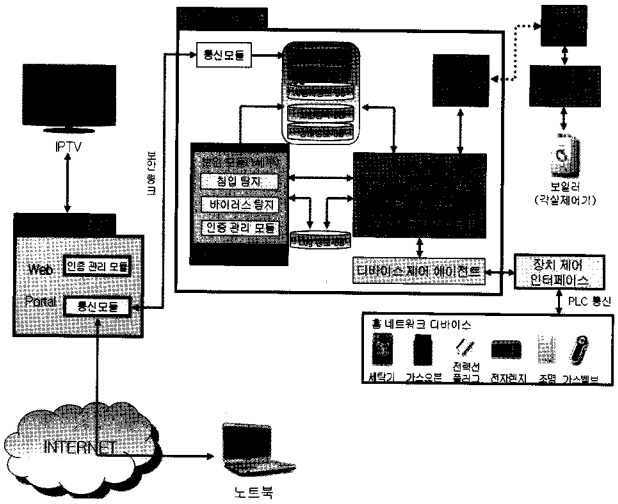
본 논문에서 제안한 홈 네트워크 통합 보안정책을 적용한 홈 네트워크 시스템은 통신 모듈, 보안정책 관리 모듈, 디바이스 제어 에이전트, 보안 모듈, ZigBee 모듈 등으로 구성된다. 이 중 본 논문에서 다루는 모듈은 보안정책 모듈이며, 이 모듈의 주요 기능은 홈 네트워크 시스템의 적응적인 보안을 위해 정책 기반 접근제어 및 접근제어 명령에 따른 상황인지 제공이다. 이를 위해 보안에 영향을 주는 주변 환경 정보들은 통신 모듈 및 보안모듈 등을 통해 수집하며, 이후 판단에 따른 디바이스 제어를 위해 디바이스 제어 에이전트 및 ZigBee 모듈과 통신을 한다. 이 다양한 모듈들로 이루어진 홈 네트워크 시스템을 크게 두 가지로 구성하였다. 하나는 셋탑박스와 월패드로 구성된 시스템으로 신축 건물에 들어가는 홈 네트워크 시스템을 가정하였고, 다른 하나인 셋탑박스만으로 구성된 시스템은 기축 건물에 들어가는 홈 네트워크 시스템을 가정하였다. 셋탑박스는 시스템으로의 접근들을 통제하는 홈 서버 역할이며, 월패드는 보안 정책을 기반으로 홈 네트워크 시스템을 통제하는 역할을 한다. 후자의 경우, 월패드의 보안 모듈들이 셋탑박스 쪽으로 추가되게 된다.

5.1 셋탑박스와 월패드 시스템 구성 및 구현

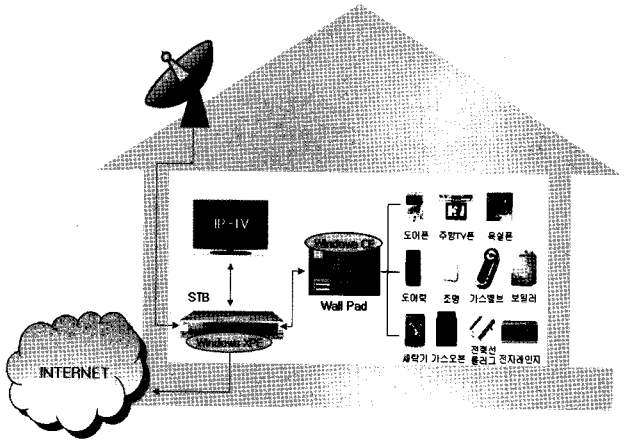
셋탑박스와 월패드가 동시에 존재하는 시스템의 경우, 셋탑박스는 홈 서버 기능을 하며 사용자의 접근을 위해 웹 서버 모듈을 가지고 있고 셋탑박스의 보안 모듈은 인증 관리 모듈, 통신 모듈로 구성된다. 홈 네트워크로의 접근은 월패드를 통한 직접 접근이 가능하며, 또한 인터넷 및 IPTV 등을 이용한 웹 서버 접근 가능하다. 웹 서버를 통해 외부에서 접근하는 사용자가 시스템에 미치는 악영향을 차단하기 위해 인증 관리 모듈이 필요하며, 외부의 사용자 및 사업자 서버, 월패드와 통신을 하기 위한 보안 통신 모듈이 필요하다. 이를 통해 셋탑박스의 보안성을 확보할 수 있고, 월패드에서는 보안모듈에 방화벽을 설치하여 보안 성능을 배가 시킨다. 월패드의 기능인 장치 제어와 보안정책 관리를 수행하게 되면, 이에 해당하는 보안정책 관리 모듈이 정책기반 접근 제어 모듈 및 상황 인지 모듈, 보안정책 DB 관리 모듈을 통해 기능을 수행하여 디바이스 제어 에이전트나 ZigBee 모듈에게 해당 제어 메시지를 전송하여 사용자가 원하는 작동을 하게 도와준다. 보안 모듈과 보안 정책관리 모듈은 모두 기본 설정이 담긴 DB를 기반으로 기능을 수행하게 되며, 해당 DB는 환경설정 DB, 상황인지 DB, 사용자정보 DB, 보안정책 DB, 상태정보 DB로 구성된다. <그림 14>는 셋탑박스와 월패드 모듈별 구성도를 보여준다.

<그림 15>은 셋탑박스와 월패드 시스템 구성도를 나타낸다. 셋탑박스는 컴퓨터와 같이 고성능의 기기가 아니기 때문에 일반적으로 많이 쓰이는 Windows XP 환

경에서 시스템을 구축하지 않고, Windows XP Embedded (이하 XPE) 환경에서 시스템을 구축하였다. XPE는 MS 사가 PC용 OS인 Windows XP를 기초로 개발한 임베디드 시스템용 OS이다. XPE는 모듈화된 각종 기능을 컴포넌트화 하여 필요한 기능만을 통합할 수 있도록 도와준다. 이를 통해 제품에 맞는 시스템 사이즈를 자유롭게 선택할 수 있고, Win32 API를 제공한다. 월패드는 CPU로 ARM 11 Core 667MHz를 사용한다. 셋탑박스보다 한층 경량화된 모델이기 때문에 WinCE 환경에서 시스템을 구축하였다. 이와 같이 XPE 및 WinCE는 시스템을 경량화 할 수 있고, 윈도우즈의 기본 API를 제공하기에 프로그램을 사용하는데 있어서 범용성을 제공하여서 선택하게 되었다. 다만 특성상 설치 이전에 필요한 기능이나 프로그램, 라이브러리 등을 컴포넌트화 하여 이미지로 만들어야 하기 때문에 전체 시스템의 구성에 따라 다른 형태로 구현될 수 있다.



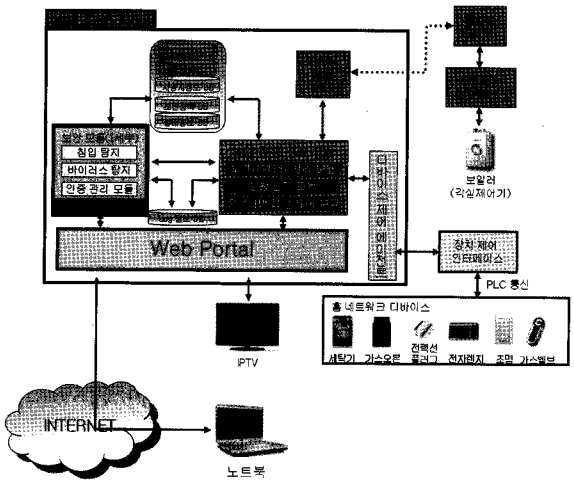
<그림 14> 셋탑박스와 월패드 모듈별 구성도



<그림 15> 셋탑박스와 월패드 시스템 구성도

5.2 셋탑박스 시스템 구성 및 구현

셋탑박스만 존재하는 시스템의 경우에는 기존의 셋탑박스와 월패드로 나누어졌던 기능들이 셋탑박스 측으로 통합된다. 셋탑박스는 홈 서버 기능을 하며 사용자의 접근을 위해 웹 서버 모듈을 가지고 있다. 셋탑박스의 보안 모듈은 인증 관리 모듈, 통신 모듈로 구성되며, 월패드에 구성되어 있던 보안 모듈들이 셋탑박스에 내장되게 된다. 홈 네트워크로의 접근은 월패드를 활용한 직접 접근은 불가능하며, 인터넷 및 IPTV 등을 이용한 웹 서버 접근만이 가능하다. 웹 서버를 통해 외부에서 접근하는 사용자가 시스템에 미치는 악영향 차단하기 위해 인증 관리 모듈이 필요하며, 셋탑박스와 월패드 간 보안에서 요구되었던 보안 통신 모듈은 셋탑박스에 보안 모듈이 통합되면서 필요하지 않게 된다. 통합된 모듈인 장치 제어와 보안정책 관리를 수행하게 되면, 이에 해당하는 보안정책 관리 모듈이 정책기반 접근 제어 모듈 및 상황 인지 모듈, 보안 정책 DB 관리 모듈을 통해 기능을 수행하여 디바이스 제어 에이전트나 ZigBee 모듈에게 해당 제어 메시지를 전송하여 사용자가 원하는 작동을 하게 도와준다. 보안 모듈과 보안 정책관리 모듈은 모두 기본 설정이 담긴 DB를 기반으로 기능을 수행하게 되며, 해당 DB는 환경설정 DB, 상황인지 DB, 사용자정보 DB, 보안정책 DB, 상태정보 DB로 구성된다. <그림 16>는 셋탑박스 모듈별 구성도를 보여준다.

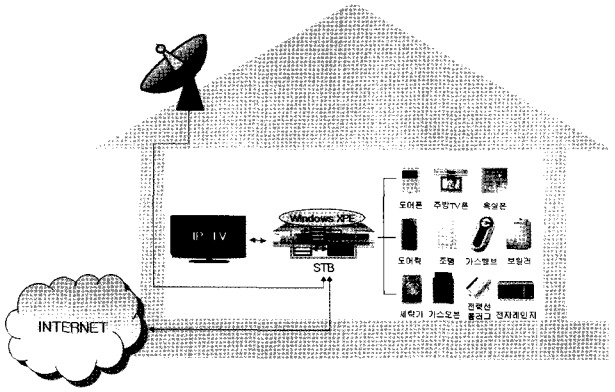


<그림 16> 셋탑박스 모듈별 구성도

<그림 17>은 셋탑박스 시스템 구성도를 나타낸다. 셋탑박스만 존재하는 시스템의 경우에는 기존의 셋탑박스와 월패드로 나누어졌던 기능들이 하나로 통합된다. 시스템 구현 환경은 제 5.1절과 같다.

6. 결 론

향후 홈 네트워크 시스템의 보편화 및 다양한 유무선 서비스의 활용은 사회경제적으로 큰 효과를 기대해도 좋을 것이다. 이를 통한 인터넷 접속 등의 유비쿼터스 홈 네트워크 환경이 점차 실현되면서 홈 네트워크 시스템의 보안 기능이 점점 중요해지고 있지만, 현재 홈 네트워크 시스템의 보안 기술은 연구가 더딘 상황이다. 홈 네트워크의 보편화가 이루어지고 다양한 차세대 네트워크 기술들과 연동을 통한 서비스가 일반화된다면, 큰 사회적 문제가 될 수 있다.



<그림 17> 셋탑박스 시스템 구성도

본 논문에서는 셋탑박스와 월패드를 이용하여, 홈 네트워크 시스템에서 댁내외의 유기적이고, 적응적인 인증을 통해 보다 안전하고 효율적인 홈 네트워크 시스템의 구축 방안을 제시하였다. 제안한 보안 정책 기술이 실제의 홈네트워크 시스템에 적용된다면 홈 네트워크 시스템의 서비스 안전성에 기여할 수 있을 것으로 판단된다. 실제 시스템 구현 상황에서 특정 알고리즘에 대한 정의나 보안 시스템 구성에는 어려움이 있으나 본 논문에서 기술한 요구사항들과 활용 시나리오에서 발생할 수 있는 보안 취약성을 점차 해결하고 관련 기술들을 개발해 나아가야 할 것이다.

참고문헌

[1] 박현문, 박수현, 서해문; "이웃탐지와 ACL을 이용한 ZigBee 기반의 홈 네트워크 보안 시스템 구현", 전자공학회논문지, 46(1) : 35-45, 2009.

[2] 오홍룡, 염홍열; "ITU-TSG17 홈 네트워크 보안 표준화 동향 및 향후 전망", 한국정보보호학회지, 16(6) : 9-18, 2006.

[3] 이덕규, 김도우, 한종욱; "홈 네트워크 보안 기술 및 표준화 동향", 전자통신동향분석, 23(4) : 89-101, 2008.

[4] 이정열, 윤진희, 전해성, 김학범; "고속전력선통신이 적용된 홈 네트워크의 보안취약점 분석", 정보보호학회지, 20(1) : 66-73, 2010.

[5] 조수형, 이상학; "홈 게이트웨이 기반 보안 시스템 개발", 한국정보과학회 2010년 컴퓨터종합학술대회 학술발표논문집, 37(1) : 299-302, 2010.

[6] 주성호, 임용훈, 박병석, 김태완, 김영형, 최문석, 이범석; "Analysis of Security Weakness and Countermeasure in PLC-based Homnetwork," 2006년 전력전자학술대회 논문집, 478-480, 2006.

[7] 진병문, 오홍룡, 염홍열, 강신각; "2006년 ITUT SG17 연구동향", TTA, ITU-T 연구활동보고서, 2006.

[8] HNSF, http://www.hnsf.org.

[9] ITU-T, http://www.itu.int/ITU-T.

[10] Kim, H. S., Lee, J. W., Gupta, S. K. S., and Lee, Y. H.; "Trust-Propagation Based Authentication Protocol in Multihop Wireless Home Networks," *Proc. of Communication System Software and Middleware conference*, 1-5, 2006.

[11] Tseng, P. C., Wang, J. W., and Hwang, W. S.; "Securing Traffic at QoS-aware Residential Gateway Using Biometric Signatures," *IEEE Transactions on Consumer Electronics*, 54(3) : 1148-1156, 2008.

[12] TTA, http://www.tta.or.kr.

[13] Walter, P.; "Home Network Security-Part1 : Security Requirements," ISO/IEC, June. 2005.