情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

홈네트워크 환경에서의 지식기반 서비스를 위한 보안 및 정책 연구

황 지 온*, 엄 윤 식*, 김 용*, 박 세 현**

요 약

기존의 단순한 형태의 장치들이 연결된 물리적 공간을 보다 지능적, 적응적 컴퓨팅 환경으로 변화하는 중심에 홈네트워크가 자리잡고 있으며, 이러한 환경에서는 다양한 종류의 각종 디바이스들이 네트워크로 연결되어 서로 통신하기 때문에, 다양한 상황에서의 보안 문제점들이 발생될 수 있다. 따라서 본 논문에서는 홈네트워크 보안 기술 및 환경 분석을 기반으로 보안 요구사항을 도출한다. 그리고 안전한 홈네트워크의 구축을 위해 홈네트워크 환경을 파악하여, 기존 홈네트워크 관련 요소 기술에 대해서 알아보고, 보안 문제점을 검증한다. 이러한 문제점을 기반으로 홈네트워크 환경에 따른 보안 적용 모델 방안을 제시하여, 홈네트워크의 보안 취약성 분석을 기반으로 홈네트워크 환경에 따른 보안 적용 모델 방안을 마련하고자 한다. 또한 홈네트워크 보안 및 인증 메커니즘의 실용적이고 확장적으로 구성이 가능한 다양한 기술 요소를 검증하고자 한다.

Ⅰ. 서 론

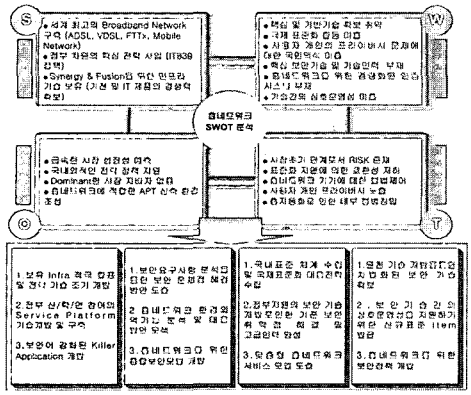
홈네트워크는 현재 가장 주목받고 있는 차세대 IT 기술로써 댁내의 정보가전기기에 대한 제어, 관리, 통합 및 연동을 바탕으로 인터넷과 결합하여 생활의 편리함을 극대화하기 위한 기술의 집합체이다. 이와 같은 홈네트워크는 기술적인 계층에 따라 물리적인 데이터 전송을 위한 하부 네트워크 기술과 상위 응용과의 연동을 위한 미들웨어 기술, 그리고 각각의 가전기기에 적용되는 정보가전 기술로 나누어진다. 현재는 광대역 통신, 무선인터넷, 센서 기술 등과 결합하여 유비쿼터스 컴퓨팅으로 확장되어 가고 있다. 따라서 이러한 추세에 맞추어 시장에서의 성공적인 홈네트워크를 위해서는 사용자 인증과 권한/인가 서비스 개발 및 보안기술이 필수적이다[1].

홈네트워크는 단순히 가정 내에서 통신망을 구축한다는 좁은 의미에 한정되지 않고, 다양한 분야가 결합되어 커다란 시너지를 창출하는 복합 멀티미디어 산업으로서 가정 내의 정보가전 기기가 네트워크로 연결되어 기기·시간·장소에 구애받지 않고 서비스가 제공되는 미래 가정환경인 디지털홈을 구성하는 핵심요소이다. 홈네트워크는 홈 내부에 위치한 어떤 기기 간에도 네트워크가 가능하고, 원격지로부터도 네트워크를 통하여 기기의 제어 및 관리가 가능한 통신 서비스 환경을 구축하기 위한 것이다[2]. 홈네트워크 산업을 활성화시키기 위해서는 이기종 유, 무선 네트워크 망간의 상호 연동 기술은 물론 관리적 측면에서의 기술과 통합 측면에서의 기술 등이 필요하고, 또한 정보의 처리, 전달 및 저장을 안전하게 하기 위해서는 특히 보안기술이 절실하게 요구된다.

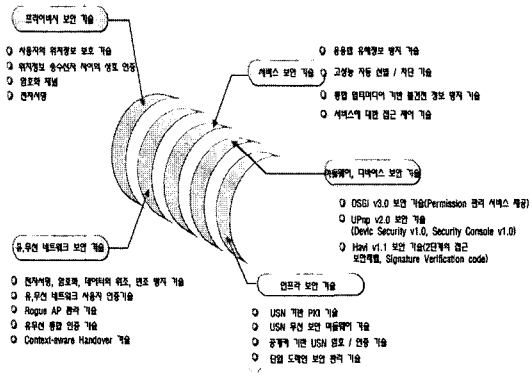
IT의 주도 국가인 미국 또한 국가기관, 유수 대학 연구소, MS/HP/IBM 등의 첨단기업 등을 앞세워 홈네트워크 산업에 투자를 아끼지 않고 있으며, 미국을 비롯해서 일본, 유럽 등 세계 각국 또한 이에 대한 연구를 활발히 진행하고 있다.

[그림 1]에서의 홈네트워크에 대한 SWOT 분석으로부터 홈네트워크에서의 여가가지 취약점들이 산재해 있음을 알 수 있으며 안전한 홈네트워크 환경을 구축

* 중앙대학교 전자전기공학부 홈네트워크 연구센터
** 중앙대학교 전자전기공학부 홈네트워크 연구센터 센터장(shpark@cau.ac.kr)
본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터(중앙대학교 홈네트워크연구센터) 지원사업의 연구결과로 수행되었음.



〔그림 1〕 홈네트워크에 대한 SWOT 분석



〔그림 2〕 홈네트워크 기존 보안기술

하기 위해서는 특히 보안에 대한 대책 마련이 시급함을 알 수 있다.

〔그림 1〕에서 살펴보았듯이 홈네트워크는 무궁한 발전 가능성을 내재함과 동시에 여러 분야의 기술들을 유기적으로 결합하여 사용하기 때문에 기존 보안 문제에 대한 취약성을 그대로 포함하고 있다. 또한 홈네트워크는 요소기술 및 환경 등의 특성으로 인해 홈네트워크 정보기기에 대한 불법적인 공격이 빈번하게 발생할 수 있다. 이러한 공격은 개인의 프라이버시 침해 뿐 아니라 개인의 생명 및 자산까지 직접적인 피해를 줄 수 있어 보안 취약성에 대한 대응책 마련이 매우 시급한 실정이다.

따라서 본 논문에서는 홈네트워크 환경에서의 보안 기술을 살펴보고, 이를 기반으로 보안 요구사항을 도출한다. 또한 홈네트워크에서의 보안 적용 모델을 제시하며, 이를 뒷받침하기 위한 세부 기술로 실시간 웹 무결성 검증 유비쿼터스 홈네트워크 보안 시스템, 보안 미들웨어 적용 생체인증을 위한 워터마킹, 사용자 기반의 지능형 서비스 제공을 위한 보안 기술 및 추론 엔진을 제시한다. 그리고 결론으로 제시된 보안 모델의 추후 진행 사항을 도출하며, 홈네트워크에서의 보안을 정리하고자 한다.

Ⅱ. 홈네트워크 환경에서의 보안기술 및 보안 요구사항

홈네트워크 보안 요구사항 도출에 앞서 홈네트워크 구축 환경 및 기존 홈네트워크 환경에 적합한 여러 보안기술에 관하여 살펴본다.

홈네트워크를 구축하기 위해서는 홈네트워크 기술, 액세스망 기술, 콘텐츠 및 솔루션 기술이 필요하다. 홈네트워크 기술에는 전력선 통신, 전화선 통신, LAN, IEEE1394, 무선랜 등의 유무선 네트워크 기술, 플러그인 앤 플레이 기능을 지원하는 HAVi, Jini, UPnP 등의 미들웨어 기술이 있다. 또한 외부 액세스망에 대해 망 종결과 모뎀 기능을 제공하고, 홈네트워크를 연결하여 망간 연동 기능을 제공하는 가정용 게이트웨이인 홈 게이트웨이 기술과, 원격에서 다중의 서비스들을 액세스망을 거쳐 홈네트워크에 접속된 정보가전 기기에 전달하고 관리하는 서비스 플랫폼 기술이 포함된다〔3〕.

이에 따라 각 홈네트워크를 구성하는 기술들에 대한 보안 요소를 도출하고 그에 따른 문제점을 분석하고자 한다.

1. 홈네트워크 보안 기술

홈네트워크 보안을 위해서 사용되는 일반적인 보안 요소 기술로는 데이터 기원 인증, 명령 권한 검증, 메시지 무결성 보호, 메시지 재생 방지, 데이터 비밀성, 키 분배 등이 있다. 다음의 〔그림 2〕는 홈네트워크에서 사용되는 기존의 보안 기술들을 프라이버시, 유/무선 네트워크, 인프라, 미들웨어, 서비스, 디바이스의 측면으로 나누어서 정리한 것이다.

1.1 프라이버시

컨버전스 환경으로 발전함에 따라 현재 홈네트워크 환경에서의 개인 프라이버시 침해에 대한 대응책이 미비한 상태이며, 사용자 개인 정보 노출로 인한 프라이버시 침해 가능성은 점점 증가하고 있다. 그러므로 여러 보안상의 문제점을 지니고 있는 환경이지만 향후에

는 이러한 보안상의 문제점에 대한 대책 마련과 함께 기존 기술을 기반으로 더욱 강력한 개인 프라이버시 침해 방지 기술과 환경이 제공되어야 할 것이다[4].

1.1.1. 사용자의 위치정보 보호 기술

차세대 위치기반 보안 인증 서비스에서 중요하게 생각해야할 개인정보보호를 위해서는 개인 프로파일이나 요청에 의한 보호정책이 설정되어야하고, 프로파일 기반 하에 위치 공개 여부, 시간과 날짜, 정확도가 주요한 부분으로 다뤄져야 한다. 또한 요청 기반(언제, 어디서라도 위치 공개 On/Off, 조건부 공개)과 선택사양(필요시마다 허용 요청) 그리고 사전 허용 없이 그 어느 누구도 위치 정보를 획득해서는 안 된다.

위치정보와 사용자정보 사이에서 프라이버시 침해를 최소화 할 수 있는 매핑 단계와 각 Case 별 Identity 정보 공개 및 사용이 가능해야 하며, 위치정보에 대한 송신자의 서명, 위치 정보 자체에 대한 암호화 그리고 위치 정보 전송단에서의 암호화(WTLS, SSL, IPSec, VPN)가 이루어져야 한다.

즉, 사용자의 위치정보 보호를 위해 상호 인증 시스템을 통한 강력한 인증 및 암호화 시스템이 필요하다.

• 인증(Authentication)

개체들 간의 상호 인증 즉, 위치정보 작성자(송신자)와 수신자 사이의 상호인증이 필요하고, 악의적인 송/수신자로부터 개인정보를 보호해야하며, 전송되는 데이터에 대한 변조까지 막을 수 있는 방안이 필요하다. 웹서비스보안기술분석 및 응용 방안 연구 또한 사용자와 위치정보 작성자간에 인증이 이루어진 후 사용자의 개인정보의 전송이 가능해야 하는데, 이는 인증이 이루어지지 않은 경우 제공되는 정보에 대해 신뢰할 수 없으므로 사용자 또는 위치정보 작성자의 정책에 따라 대응할 수 있어야 한다. 따라서 사용자는 인증이 이루어지지 않은 경우 개인정보 전송을 제한할 수 있도록 정책 설정을 해야 할 필요가 있다.

• 암호화 채널

네트워크상의 해킹을 방지하기 위한 암호화 채널을 사용하여 견고한 종단 간 암호화가 필요하고, SSL, WTLS의 사용이 가능하다.

• 전자서명

부인 봉쇄 및 메시지의 변경 방지 기능을 위해, 전자서명 사용이 필요하다.

1.2 유·무선 네트워크

홈네트워크 유·무선 네트워크 보안 기술에는 전자서명, 암호화, 사용자 인증, Rogue AP 관리, 유·무선 통합 인증, 데이터 위·변조 방지 기술 등이 핵심 기술이며, 아래 [표 1]에서는 각 기술들에 관해 간단히 설명하고 있다.

[표 1] 유·무선 네트워크 보안 기술

기본기능	설 명
전자서명	· 서명자가 자신이 서명한 사실을 부인할 수 없음 · 서명한 사용자에 대해 제3자가 확인 가능
암호화	· 서명된 메시지 내용에 무결성 보증
사용자 인증	· 임의의 정보에 접근할 수 있는 주체의 능력이나 자격을 검증 · 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방지
Rogue AP 관리	· 악의적으로 설치된 Rogue AP의 탐지
유·무선 통합 인증	· 각종 유·무선망에서 인증, 보안 인터넷 로밍 보안 등을 · 통합적으로 관리할 수 있는 기술
데이터 위·변조 방지	· 데이터의 정확성은 데이터 위·변조를 막아내는가가 중요 · 원천적으로 데이터 사용을 제한하는 사전 관리 방법 · 나중에 위·변조 여부를 검증하는 사후 관리 방법

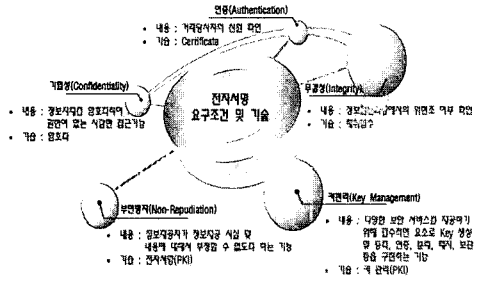
1.2.1 전자서명 기술

현실 세계의 종이문서에 표기되는 수기 서명이나 인장 기능을 전자문서에서 구현한 것이라 할 수 있다. 디지털화된 전자문서는 그 특성상 원본과 사본을 구별하는 것이 불가능하므로 네트워크를 이용한 전자문서 교환에는 전자서명이 필수적이다. 전자문서를 작성한 사람이 누구인지를 확인하는 사용자 인증(User Authentication)과 해당 메시지가 변경되니 않은 원본임을 확인하는 메시지 인증(Message Authentication) 기술로 나누어진다. 전자서명의 기본 기능은 다음 [표 2]와 같다.

[표 2] 전자서명의 기본 기능

기본기능	설 명
사용자 인증	· 서명자가 자신이 서명한 사실을 부인할 수 없음 · 서명한 사용자에 대해 제3자가 확인 가능
메시지 인증	· 서명된 메시지 내용에 무결성 보증

전자서명의 요구조건 및 기술요소에 대해 다음 [그림 3]에서 나타내고 있다.



[그림 3] 전자서명 요구조건 및 기술

1.2.2. 암호화 기술

정보의 수집, 처리, 저장, 검색, 송수신 과정에서 그 정보가 훼손, 변조되거나 불법적으로 유출되는 것을 방지하고, 정보처리 시스템 내에 저장되거나 통신망을 통하여 송수신되는 정보를 각종 위험으로부터 보호하여 시스템의 가용성(Availability)을 보장하기 위한 관리적, 기술적 수단을 말한다. 이러한 정보보호를 제공하기 위해 많은 서비스들이 암호 알고리즘을 바탕으로 구현되고 있으며, 이와 같은 정보보호 서비스는 5대 서비스라 불리며, 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 부인방지(Non-Repudiation), 접근통제(Access Control) 등 5가지로 요약된다. 암호시스템(CryptoSystem)에서는 기밀성과 인증 서비스를 모두 제공하여야 진정한 암호 시스템이며 KMI(Key Management Infrastructure), PKI(Public Key Infrastructure) 이 두 가지를 핵심으로 하여 서비스를 제공한다.

암호를 정보시스템에 적절히 구현하기 위해서는 어떠한 표준을 선택할 것인가, 그리고 하드웨어 암호화 방법을 선택할 것인가 아니면 소프트웨어적인 방법을 선택할 것인가 등 여러 가지를 고려해야 한다. 암호화 구현 시 고려해야 하는 사항은 크게 6가지로 나누어 볼 수 있다.

• 암호화의 표준의 선택

암호의 표준화를 선택할 때는 상호운용성(Interoperability)과 비용효과성(Costeffective), 트랜드(Trend)를 고려해야 한다.

• 하드웨어/소프트웨어 구현

암호화 방법은 하드웨어적인 암호화 방법과 소프트웨어적인 방법으로 구분되는데, 이들 방법들을 선택할 때 보안 관리자는 그 암호화 방법의 보안성, 비용, 단순성, 효율성과 구현이 용이한지 여부를 테스트해야 한다.

• 키관리

암호키 관리는 암호 보안에 이어 가장 필수적이다. 암호화 알고리즘이 잘 구현되고, 그 암호화 강도가 강할지라도 암호키 관리가 잘 못되어 타인에게 누출 된다면 암호의 보안성은 현저히 감소할 수밖에 없는 것이다. 암호키 관리는 암호키의 생성과 분배, 저장, 입력, 사용, 복구, 파괴 등의 과정을 모두를 말한다.

• 암호화 모듈의 보안

소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합의 모듈로 구현되어진다. 모듈에는 암호화 알고리즘이나 관리 파라미터, 알고리즘에서 사용되는 키의 임시저장소 등이 포함되는데, 이러한 모듈을 변경이나 조작으로부터 보호하는 것은 암호화 구현의 중요 사항 중의 하나이다.

• 네트워크에서의 암호화

네트워크를 따라 전송되는 암호화된 정보나 MAC 값, 디지털 서명들은 통신장비나 소프트웨어에 의해 왜곡되어지지 않아야 한다. 또한 변경이나 왜곡이 되어졌다 하더라도 그 데이터를 암호화 방법을 통하여 탐지 및 복구, 재전송을 요구할 수 있어야 한다.

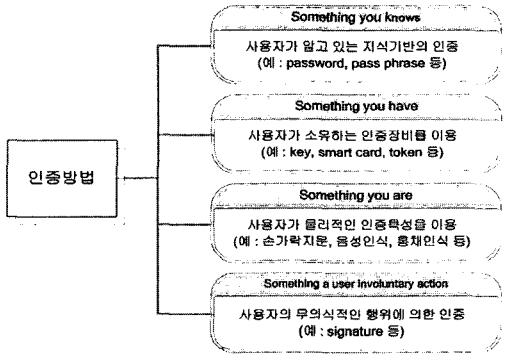
• 암호화 수출

현대의 암호가 개인뿐만 아니라 기업이나 국가의 이익과 직간접적으로 많은 연관이 있기 때문에, 암호를 수출하는 것은 미국에서는 엄격히 규제하고 있다.

1.2.3. 유·무선 네트워크 사용자 인증기술

임의의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는 단계로 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방지해 준다. 사용자 인증에는 허가(Authentication), 책임 추적성(Accountability)이 있다.

허가는 시스템이 사용자, 프로그램 또는 프로세스에게 허가한 권한을 말하는 것이고, 책임 추적성이란 멀티유저, 멀티태스킹이 지원되는 네트워크 환경에서는 누가, 언제, 어떠한 행동을 하였는지 기록하여 필요시 그 행위자를 추적 가능하도록 함으로써 책임소재를 명



〔그림 4〕 인증방식에 의한 분류

확하게 해야 할 필요성이 생기게 되었기 때문에, 시스템의 보호 관점에서도 비인가자 또는 인가된 사용자에 대하여 경각심을 불러 일으켜 컴퓨터의 부정사용을 줄이는 효과를 거둘 수 있어 반드시 보장되어야 할 보안의 중요 요소 중의 하나라 할 수 있다.

1.2.4. Rogue AP 관리 기술

네트워크에서의 공격이로 하면 컴퓨터, 네트워크, 패킷에 침투하려는 모든 시도와 악성 프로그램과 자가 복제 프로그램을 심으려는 모든 시도를 지칭한다. 이러한 공격을 여러 범주로 분류할 수 있는데, 네트워크 공격을 능동형 공격과 수동형 공격으로 분류할 수 있다.

악성 파일 심기, 데이터 변경, 네트워크 방해가 능동형 공격에 해당되고, 이론상으로 볼 때 수동형 공격을 발견하는 것은 매우 어려우며 능동형 공격의 탐지는 비교적 쉽다. 도청과 같은 수동형 공격은 네트워크에 실질적인 해를 가하지 않지만 해커는 도청기법을 사용하여 능동형 공격에 필요한 정보를 획득한다. 네트워크 ID없이 네트워크 외부에서 공격하는 것을 원격공격이라고 하며, 기존에 보유하고 있는 계정을 사용하여 공격하는 것을 로컬 공격이라고 한다. 치고 빠지기 공격은 짧은 시간동안 시스템을 혼란에 빠뜨린다. 이에 반해 지속 공격은 공격이 지속되는 시간만큼 네트워크에 해를 가한다. 로그 AP(rogue AP)는 보안성을 갖추지 않는 무선 AP로써 외부 침입자가 쉽게 접근할 수 있는 곳이다. (로컬 해커들은 로그 AP를 서로 공유한다.)

1.2.5. 유·무선 통합 인증 기술

유무선 상에서 모든 인증 관련 요청 사항과 인증 처리, 사용자 관리, 로그 파일 관리를 데이터베이스 서버의 중복 투자 없이 일괄 처리할 수 있다. 즉, 각종 유무선 망에서 인증, 보안, 인터넷 로밍 보안 등을 통합적으로 할 수 있는 기술로써, 기존의 인터넷 인증서버는 서비스별로 별도 서버를 설치해야할 뿐 아니라 인터넷 로밍을 위한 정용 서버로 추가 마련해야하기 때문에 구축비용 부담이 높았던 반면에, 유무선 통합 인증 기술은 인증 서버 하나로 각종 유무선 인터넷 서비스를 처리할 수 있기 때문에 경제적이며, 공중 무선랜과 휴대인터넷(HPI), 차세대 광대역통합망(BcN)에서도 적용할 수 있다.

1.2.6. 데이터의 위조, 변조 방지 기술

데이터 정확성은 데이터 위변조를 얼마큼 막아낼 수 있는가에 의해 좌우된다. 정확성을 향상시키기 위해서는 원천적으로 데이터 사용을 제한하는 사전 관리 방법과 나중에 데이터 위변조 여부를 검증하는 사후 관리 방법으로 나눠진다. 사전 관리 방법은 사용자를 제한하는 것과 애플리케이션을 제한하는 것으로 분류할 수 있다. 또한 사용자 제한은 사용자에게 적절한 권한을 부여하고 업무 필요성이 있는 사람에게 데이터에 대한 접근 권한을 부여하는 것이다.

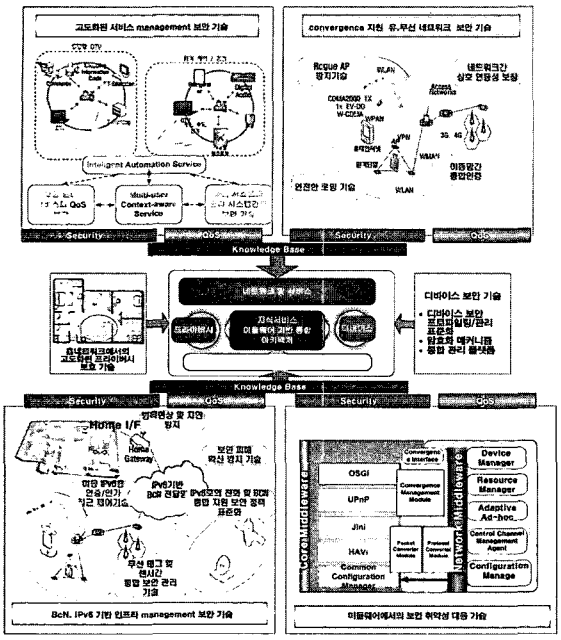
비대칭키 방식을 이용한 PKI는 데이터 기밀의 보존, 전자서명 확인과 본인확인, 위/변조 방지 기능 등으로 전자서명 인증제도에 가장 적합한 모형이다.

Ⅲ. 본 론

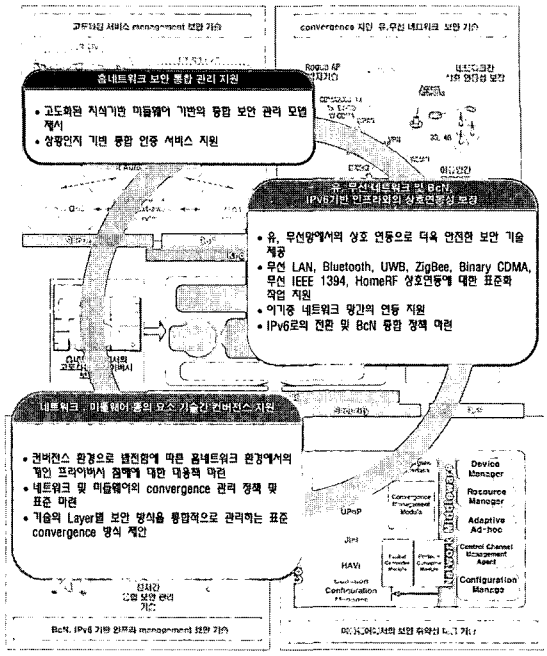
본론에서는 앞서 도출한 보안 요구사항을 기반으로 홈네트워크 환경에서의 적용 가능한 보안 적용 모델을 제시한다. 또한 이러한 모델의 세부 기능 및 구조를 기술하고, 홈네트워크 보안 적용 모델을 뒷받침하기 위한 실시간 웹 무결성 검증 보안 시스템 및 보안 미들웨어 적용 생체 인증을 위한 워터마킹과 보안 기술 및 추론엔진에 대한 세부 내용을 정리하고자 한다. 이를 통해 현재의 홈네트워크에서의 보안적 문제점을 보완할 수 있는 방안을 제시하며, 차세대 보안 모델을 제시하고자 한다.

1. 홈네트워크 환경에 따른 보안 적용 모델

현재의 홈네트워크에서의 보안은 각 기술별 보안의 적용, 또는 기존의 보안 요소기술의 단순한 적용에 그쳐 기존 단순한 인프라에서와는 다른 다양한 인프라와 기기, 사용자에 대한 고려가 이루어지지 않은 상황에



〔그림 5〕 홈네트워크 환경에 따른 보안 적용 모델



〔그림 6〕 본 과제에서 제안한 보안 적용 모델

서의 보안 모델이다.

따라서 본 논문에서는 다양한 인프라와 기기 및 환경에서의 적용이 가능하며 이러한 보안 기술을 통합 관리할 수 있는 보안 모델을 구성하고자 한다. 그러므로 홈네트워크 환경에서 보안을 저해하는 요소에 대한 대응 방안을 제시한다. 또한 홈네트워크에 적용 가능한 보안정책을 마련함과 동시에 홈네트워크 환경에 적합한 통합보안모델을 다음 〔그림 5〕와 같이 제안한다.

〔그림 6〕는 홈네트워크에서의 요소별 취약점에 대한 대응 기술 및 이를 통합 관리하는 지식 기반 미들웨어를 나타내고 있다. 기존의 홈네트워크 보안 기술은 상호연동적인 측면, 컨버전스적 측면, 관리적인 측면에서 취약점을 가지고 있는데 반하여, 제안하고자 하는 모델에서는 요소별 보안 취약점에 대한 대응 기술뿐만 아니라, 기존의 문제점들을 통합하여 관리할 수 있는 고도화된 보안 아키텍처를 제시하고 있다.

1.1 지식기반 미들웨어 기반의 홈네트워크 보안 통합

홈네트워크에서의 보안 모델의 경우, 기존의 단순한 환경에서의 모델과는 달리 다양한 요구사항이 필요하며, 이를 통합, 관리할 수 있는 방안이 제시되어야 한다. 따라서 지식기반 미들웨어의 홈네트워크 환경에서의 보안은 Intelligent Automation Service에 대한 보안 인증 및 서비스의 QoS 보장되어야하며, Multi-user Context-aware Service에 대한 지원으로 다중 사용자 환경에서 발생할 수 있는 conflict에 대한 문제 해결 및 상황인지 기반의 통합 인증 서비스 지원이 이루어져야 한다.

1.2 유, 무선 네트워크 및 BcN, IPv6 기반 인프라와의 상호 연동성 보장

홈네트워크는 지식기반의 사용자 맞춤형 서비스를 제공하는 것을 목적으로 구성되기 때문에 다중 사용자, 다중 환경, 다양한 인프라를 기반으로 한다. 따라서 유, 무선망에서의 상호 연동성을 보장하며 이 기종망 간의 통합 인증에 대한 보안을 지원하고 안전한 로밍에 대한 보안 기술을 제공되어야 한다.

Wireless LAN, Bluetooth, UWB, ZigBee, Binary CDMA, 무선 IEEE1394, HomeRF 등의 상호연동에 대한 표준화 작업을 지원하며, 홈네트워크 환경에서 사용되는 다양한 이기종 네트워크 망간의 연동을 지원함으로써 Seamless한 서비스 지원 및 QoS 보장되어야 한다.

IPv6로의 전환 및 BcN 통합 정책을 마련하여 네트워크에서 발생할 수 있는 병목현상 및 지연에 대한 방지 대책을 수립하고 BcN망으로의 통합 네트워크 환

경에서 더욱 급격하게 퍼질 수 있는 보안 피해에 대한 확산 방지 기술을 제공하고, 각종 무선 태그 및 센서 간 통합 보안 관리 기술 제공이 되어야 한다.

1.3 네트워크, 미들웨어 등의 요소 기술간 컨버전스 지원

컨버전스 환경으로 발전함에 따른 홈네트워크 환경에서의 개인 프라이버시 침해에 대한 대응책이 마련되어야 한다.

또한 네트워크 및 미들웨어의 통합 관리 정책 및 표준이 마련되어야하며, 기술의 Layer별 보안 방식을 통합적으로 관리하는 표준 convergence 방식을 제안하고자 한다.

디바이스 보안 프로파일링 및 관리에 대한 표준화 방안 마련됨과 동시에 강력한 암호화 메커니즘을 제공함으로써 개인의 프라이버시 및 보다 안전한 홈네트워크 서비스 제공을 위한 보안 강화가 요구된다.

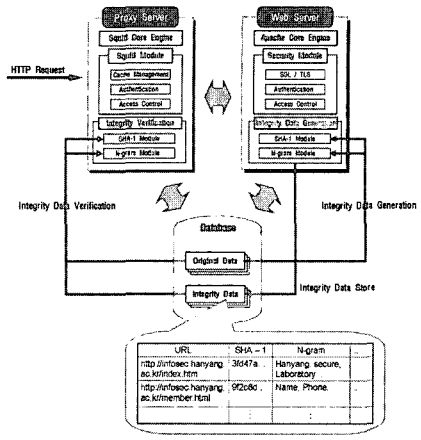
2. 실시간 웹 무결성 검증 유비쿼터스 홈네트워크 보안 시스템

제시된 홈네트워크 보안 모델을 실질적인 적용을 위한 방안의 하나로 웹 무결성의 검증을 통해 외부망에서의 홈네트워크 시스템의 보안성 강화 및 내부 모듈간의 상호 인증을 구성하도록 하는 보안 시스템을 구성한다. 실시간 웹 무결성 검증 홈네트워크 보안 시스템은 아파치 웹 서버에 연동된 무결성 데이터 생성 모듈을 이용하여 DB에 저장된 원본 데이터에 대한 무결성 데이터를 생성하고, 스퀴드 프록시 서버에 연동된 무결성 검증 모듈을 이용하여 원본 데이터와 무결성 데이터를 비교, 데이터의 무결성을 검증하게 된다.

실시간 웹 무결성 검증 홈네트워크 보안 시스템의 구성도 : 실시간 웹 무결성 검증 홈네트워크 보안 시스템은 프록시 서버와 아파치 웹 서버의 연동 보안 기술로, 아파치 웹 서버에는 무결성 데이터 생성 모듈, 스퀴드 프록시 서버에는 무결성 검증 모듈이 각각 연동된다. 무결성 데이터 생성 모듈은 웹 서비스에 이용되는 모든 데이터에 대한 무결성 데이터를 생성하여 DB에 저장하게 되며, 무결성 검증 모듈은 사용자가 웹 서비스 요청 시 원본 데이터와 무결성 데이터를 DB에서 가져와 원본데이터에 대한 무결성을 검증한다.

2.1 무결성 데이터 생성 모듈

아파치 웹 서버에 연동된 무결성 데이터 생성 모듈



〔그림 7〕 실시간 웹 무결성 검증 홈네트워크 보안 시스템 모듈의 구성도

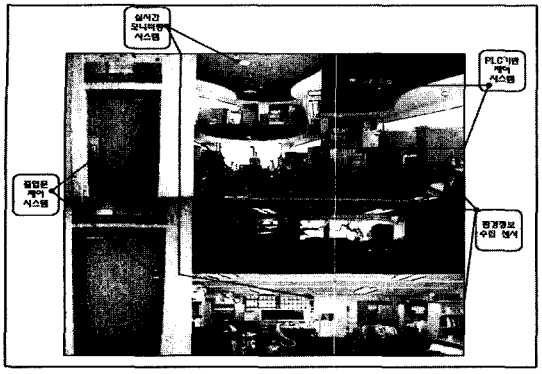
은 SHA-1과 N-gram을 이용하여 해쉬값으로 무결성 데이터를 생성한다. 이미지, 그리고 PHP나 JSP의 웹 스크립트 파일 등은 DB에 있는 원본 데이터를 이용하여 무결성 데이터를 생성, DB에 저장하게 된다. 또한 HTML 문서는 해쉬 값만이 아닌 N-gram을 통해 각 명령어를 추출한 무결성 데이터를 하나 더 만들어 DB에 저장한다. 웹 페이지 업데이트 실시간으로 웹 파일에 대한 무결성 데이터를 바로 생성함으로서 사용자가 원하는 웹 서비스 이용 시 즉각적으로 무결성 검증을 할 수 있도록 한다.

2.2 무결성 검증 모듈

퀴드 프록시 서버에 연동된 무결성 검증 모듈은 원본 데이터와 무결성 데이터를 비교하여 데이터의 무결성을 검증한다. HTML 문서는 해쉬 값과 N-gram 추출 데이터를 이용하여 무결성을 검증하고, 각 웹 페이지에 맞는 이미지 및 웹 스크립트 파일의 원본 데이터와 무결성 데이터를 DB에서 가져와 무결성을 검증한다. 데이터에 이상이 없을 시는 바로 사용자에게 웹 서비스를 제공하며, 데이터가 변조되었다고 판단 시는 웹 서비스에 연결된 원본 데이터 DB를 통해 가져온 원본 데이터로 복구하여 사용자에게 안전한 웹 서비스를 제공하게 된다.

3. 3D 기반의 모니터링 시스템을 통한 사용자 인증 및 사용자 위치 트래킹을 통한 상황인지 서비스

MCU를 통해 1차적인 센싱정보의 Context화를



〔그림 8〕 사용자 인증 및 인식을 위한 implementation

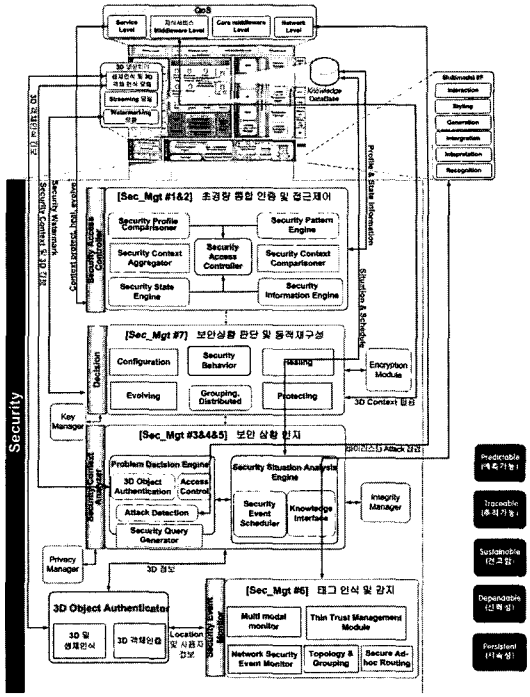
거쳐 홈 서버 및 월패드 등으로 전송하여, 상황인지 기반의 홈 서버에서는 MCU에서 전송된 데이터를 바탕으로 추론을 통한 지능적 홈네트워크 서비스가 가능하다.

MCU는 온도, 습도, 조도와 전력량을 VCM, PLM으로부터 전송 받아 데이터베이스를 구축하여 서버로 전달하고, 데이터 수집과, 전송에 있어서 안정성을 제공하기 위해 최적화된 기능을 포함하고 최대한의 안정성을 제공하는 임베디드 리눅스 기반 플랫폼이다.

매직미러는 홈네트워크 환경에서 상황 인지 서비스를 위해 사용자의 프로파일에 기반한 사용자별 맞춤형 서비스 제공함으로써, 사용자의 위치를 트래킹하여 seamless한 멀티미디어 서비스 제공 사용자의 프로파일과 위치를 파악하여 사용자가 매직미러 앞에 섰을 시에 사용자의 선호 정보를 실시간으로 웹크롤링하여 제공한다.

매직뷰어를 사용하여 홈네트워크 환경에서 상황 인지 서비스를 위해 사용자의 프로파일에 기반한 사용자별 맞춤형 서비스 제공하기 위하여, 카메라를 통한 자동 얼굴 인식을 통해 사용자가 매직미러 앞에 섰을 시에 사용자의 선호 정보를 실시간으로 웹크롤링하여 제공하게 된다.

보안 상황을 지능적으로 적용 가능한 초경량 통합 인증 기술과 전자서명 및 공인인증, 생체 인식, 3D영상, 사운드, 공간정보를 통합적으로 이용하는 지능적 초경량 인증 기술 및 SSO 지원 통합 사용자 인증 및 권한관리 기술을 적용하여 다양한 Home Appliance에 적용 가능한 통합 AAA(Authentication, Authorization, Administration) 기술을 통해 사용자 및 기기의 인증과 권한 관리를 한다. Power 소모를 최소화하면서 보안 강도를 유지시키는 적응적 인증 기술로 콘텐츠 보안(CVP, Content Vectoring



〔그림 9〕 차세대 홈네트워크 보안 미들웨어 아키텍쳐

Protocol) API를 구성한다. 또한 리포팅과 이벤트 정보 분석(LEA, Log Export) API 및 침입 탐지와 차단(SAM, Suspicious Activity Monitoring) 방안을 적용하도록 구성한다.

사용자 이동성 context-awareness 보안 서비스 기술은 사용자 이동에 따른 위치변화, 서비스 종류(realtime, non-realtime), data type, 분산 이동망의 채널 상태, bandwidth, 서비스 그룹의 반경, entity의 통신 능력 등의 감지 및 차등적 보안 기술로 구성하고, 실시간으로 변화하는 사용자의 위치 및 통신 환경에 대응하여 사용자 프로파일링 기술과 최적화된 적응적 보안 QoS 기술을 융합한 보안 classification 제공한다. 또한 사용자의 이동성을 고려한 상황 적응형 thin trust 모델에서는 사용자 이동시에 entity간의 협업 프로토콜 및 보안 미들웨어의 위치인증 기술을 통해 재인증 절차를 획기적으로 줄이는 seamless 보안 서비스를 제공하고, 보안 공격의 능동적 유형(DoS, roque bridge)과 수동적 유형(도청, 감청)에 따른 협업 프로토콜을 이용한 공격자의 위치 감지 및 보안 설정 변경을 통하여 분산 이동망의 신뢰성을 향상 시킨다. 분산 이동 망에서 최적인 적응적 보안 정책을 적용하도록 구성한다.

사운드와 공간정보의 연계로 보안 상황 인지를 통해 특정 지역의 사운드를 감지하여, 보안 및 위급 상황을 판단하여 이를 자동적인 서비스 연계를 위해, 공간정보를 효과적으로 이용할 수 있는 멀티모달 기술과 특정지역에서는 자신의 음성과 위치정보가 matching 되어 상황인지기반의 보안 서비스가 제공된다.

댁내/외에서 홈네트워크에 접속하는 무선 태그 및 센서 인증 메커니즘은 센서 및 태그의 추가/제거 시 Back-end 서버를 통한 인증, 그리고 홈네트워크 센서의 Ad-Hoc 상황에 적합한 안전한 보안 관리를 한다. 센서들의 자원적 제한을 고려한 홈 서버와 센서 및 태그간 안전한 키 분배 및 암호화 기술 그리고 홈서버 및 센서간 제어 메시지에 대한 기밀성, 무결성, 인증을 제공하기 위한 메커니즘을 제공 한다. 또한 태그리더 및 센서들에 대한 DoS 공격 범위 및 피해의 최소화 기술을 구성하기 위해, 센서 및 태그리더에 대한 DoS 공격의 피해를 최소화하는 인증 및 라우팅 프로토콜기술과, 센서에 대한 jamming 및 flooding과 같은 공격을 사용자에게 알려주는 알람 메세징 기술을 적용한다.

4. 사용자 기반의 지능형 서비스 제공을 위한 보안 기술 및 추론 엔진

서비스가 고도화되며 홈네트워크 시스템은 보다 많은 사용자의 정보와 환경의 데이터를 요구한다. 그리고 이것은 정보의 노출 위험 및 사용자에게 잘못된 인증이나 정책의 적용 등의 문제점을 발생시킬 수 있다. 따라서 이러한 컨텍스트를 관리하고 정보에 대한 보안 요소를 강화하는 방안이 필요하다. 그리고 다양한 서비스의 제공에 앞서 사용자 및 서비스에 대한 정책적인 고려사항들이 요구된다. 그러므로 사용자 및 환경에 대한 정보를 관리하고 보안 적용 모델을 구성하며 보안, 인증, 사용자 및 서비스의 우선 순위, 서비스에 대한 권한 등에 대한 다양한 정책적인 요소들을 고려하여 시스템을 구성할 필요가 있다. 그리고 사용자 및 서비스 Priority를 설정하여 동시적인 서비스에 적응할 수 있어야하며, 사용자 별 차등적 서비스 제공의 효율성을 위해 Device Access Level이나 Privilege, Authentication과 같은 정책적 Rule의 구현이 필요하다.

또한 사용자에게 제공될 정보에 대한 Privacy Level을 두어, 그에 따라 동작기기를 달리 적용함으로서 현재의 기본적이고 제한적인 Rule이 가진 한계점을 보완할 필요성이 존재한다.

서비스 제공에 있어서 충돌을 인식할 수 있도록 사용자 및 사용자의 위치, 사용자 주변 기기, 사용자의 우선순위 및 보안 레벨과 사용자가 사용 가능한 서비스 및 서비스에 대한 정보들을 읽어들여 각 관계성에 따라 정보를 추출하고 다른 정책적 룰과의 비교, 검사를 할 수 있는 추론기가 요구된다.

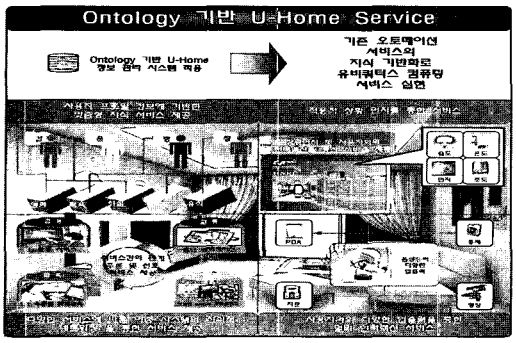
4.1 Ontology정보의 관리

홈네트워크에서는 보다 많고 다양한 컨텍스트가 요구되며 이러한 정보와 그 정보 간의 다양한 관계성을 명시하고 이를 관리하기 위한 방안으로 온톨로지의 개념을 도입하고자 한다. 그리고 온톨로지에서는 다양한 정보 뿐 아니라 보안을 위한 정책적인 요소와 서비스의 관계성을 명시하고 적용하도록 구성한다.

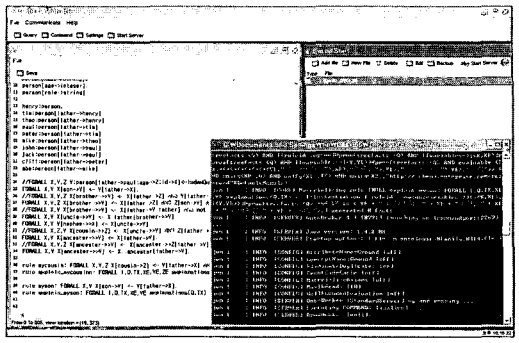
Domain 온톨로지에 정의된 Person, Space, Service, Policy등이 서로 관계성을 맺고 있음을 볼 수 있다. 예를 들어서 Home에 있는 어떠한 공간(Space)의 정보를 설명하려면 그 Space의 소유자(Person) 정보에서부터 어떠한 서비스(Service)가 제공되는 공간인지 등 다양한 정보들이 복합적으로 융합되어 하나의 공간을 나타낼 수 있다. 이렇듯 온톨로지를 통해 명확히 정의된 Domain을 구현하면 필요한 분야라면 어느 분야라도 따로 데이터를 구성하지 않아도 기존 데이터를 재사용할 수 있는 확장성을 제공하는 시스템으로 구성 될 수 있다.

현재의 Web Service를 비롯한 다양한 서비스들은 각각 개별적인 시스템 모델에 의해서 구현되어 다른 시스템과의 상호 정보 공유와 서비스의 융합을 제공하지 못하고 있는 실정이다. 이러한 개별적으로 분리되어 있는 시스템 및 서비스들의 정보 공유가 가능하여 확장성 있는 연동이 가능하다면 이미 구현되어 있는 시스템만을 활용하더라도 보다 더 고도화된 서비스가 가능해질 것이다. 또한 인간의 사고방식을 컴퓨터가 이해할 수 있고, 이러한 인간과 컴퓨터의 의미적인 상호 작용(semantic interaction)이 컴퓨터와 컴퓨터 사이에서도 그대로 반영될 수 있는 기술적 환경이 조성되도록 하는 것은, 차세대 컴퓨터 시스템의 궁극적 목표라고 할 수 있다.

온톨로지는 이러한 차세대 컴퓨터 및 서비스 고도화를 위한 Soft Infra를 구축하기 위한 핵심 기술이자 핵심 구성요소로 자리를 잡아가고 있다.



〔그림 10〕 온톨로지 기반 U-Home Service



〔그림 11〕 온톨로지 및 Rule 편집기와 작동 콘솔

4.2 System 및 Service Rule의 적용

홈네트워크 환경에서 서비스를 제공받고자 하는 경우 사용자가 서비스의 정책을 구성하고 서비스에 대해 요청함으로써 서비스가 시스템으로부터 생성되고 제공되어진다. 따라서 서비스 및 질의에 대한 추론을 위한 룰의 적용 및 온톨로지에 대한 query 결과와의 매칭되어야 하고, 각 룰 간의 우선순위 및 적용에 대한 정책적인 관리와 상황에 따른 적용 검사가 이루어져야 한다.

정적으로 제공되는 패턴화된 서비스에 대한 정의 및 다양한 동적 환경 또는 사용자의 선호환경에 대한 다양한 서비스와 다양한 환경 및 상황에 따른 서비스 구현방안 적용될 필요가 있으며, 이에 따른 정책 및 보안, 우선순위, 충돌에 대한 해결방안, 시간과 공간에 기반한 서비스의 변화 등에 대한 시스템적 룰과 정책적 룰의 구현이 반드시 요구된다.

4.3 추론된 결과에 대한 다양한 Policy 적용 및 정리

홈네트워크 환경에서는 다양한 서비스와 정보의 제공이 가능하다. 그러나 그에 반대급부적으로 홈네트워크에서의 서비스나 정보는 사용자에게 여가없이 제공되거나 또는 잘못된 정책에 의해 제공되는 경우 커다란 보안상의 문제를 초래할 수 있다. 따라서 보안을 위한 모듈의 구성이나 보안 프레임워크를 구성하는 것이 중요하며, 보안의 정책 적용을 위한 방안을 마련하고 이러한 보안 및 인증 정책을 서비스의 제공에 앞서 적용하는 것이 중요하다.

서비스를 제공하기 위해서는 정보의 보안과 사용자의 보안 등급에 대한 검증, 기기에 관련된 사용자 및 상황에서의 권한과 그 권한에 관련된 정책적 요소들, 서비스가 올바르게 적용이 되는 것인지 또는 서비스의 정보 유출이나 보안적 문제점이 있는지를 분석하고 파악하기 위한 다양한 방안이 필요하다.

따라서 Priority 및 Access Level에 대한 fact값과 Priority 적용에 대한 우선순위 및 중복에 대한 처리문제의 Rule이 만들어져야 하고, Conflict 발생시, Priority에 대한 사용자 및 위치, 관련 정보 등에 따른 차등적 적용을 위한 Rule이 필요하다. 또한 Privacy에 대한 사용자 및 Level에 대한 Ontology 적용을 위한 Rule, 보안 및 정보에 대한 보안 레벨의 동적인 관리와 권한 부여 등이 역시 추론된 결과에 대한 다양한 policy 측면에서 고려되어야 할 사항이다.

4.4 Rule에 대한 우선순위 관리 및 적용

실질적으로 구성된 정책에 대해서도 서비스를 검증하기 위해서는 각 정책들 중에서도 어떤 정책을 먼저 검증해야 하는지, 상황에 따라 어떠한 정책이 더 중요한 요소가 되는지가 다르기 때문에 이에 대한 관리가 필요하게 된다. 따라서 다양한 Rule 자체에 대한 우선순위 관리기능(Rule에 대한 우선순위의 적용 및 순위가 동일한 Rule들에 대한 관리기능)이 요구되며, 동일한 Rule에 대한 적용방안을 위한 Rule의 구성 및 우선순위 변경을 위한 update가 되어야 한다.

4.5 추론경과 관리 및 서비스 시스템 전송

서비스가 올바르게 관리되고 시스템에서 정책이 제대로 동작하기 위해서는 추론 또는 보안이나 인증의 결과가 시스템에서 관리되고 서비스에 대한 제공 상황이 정보로써 올바르게 저장되어야 한다. 그러므로 Rule 및 instance를 통한 추론된 결과 값에 대한 의미적 정리 및 관리가 필요하며, 각 Service에 맞도록 요청되는 질의 결과나 추론정보를 각 서비스번들로 전

송 및 Ontology update가 이루어져야 한다.

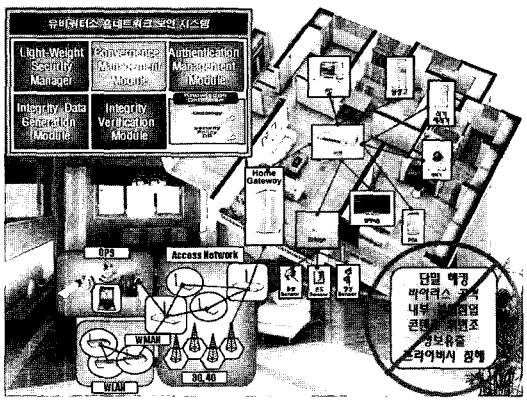
또한 서비스 및 사용자에 관련된 추론정보와 Session, Task, SubTask 사용에 대한 정보 전송이 제공 되어야 한다.

4.6 Rule에 따른 Context에 대한 재추론

서비스가 사용자에게 제공되어지거나 환경이 변경되는 경우 이를 기반으로 보안 및 인증의 유지, 사용자의 위치 변경에 따른 환경 및 서비스의 변화, 보안 체계와 정책에 대한 변동 사항의 관리를 위해서는 새로운 컨텍스트를 관리하고 이를 통해 새로운 정책과 정보를 도출할 필요가 있다. 이는 Rule을 통해 Ontology의 instance들에 대한 보다 세부적인, 또는 일반적인 관계성 정립되어야하고, 부족한 상황정보를 Rule 기반의 재추론 수행을 통해 보완되어야 한다.

Ⅳ. 홈네트워크 적용 모델

1. 홈네트워크 보안 모델 및 세부 모듈의 적용 방안



〔그림 12〕 홈네트워크 보안 모델

Light Weight Security Manager는 사용자 인증 후 홈네트워크망의 차별화된 엑세스를 통해 지정된 디바이스의 엑세스만 허용하고, 해커에 의한 계속적인 피해 방지를 위해, 홈네트워크 망과 외부 망간의 연결을 해제한다. 유무선 네트워크상에서 임의로 접근하는 사용자의 인증 및 허가 기술이 포함된다.

Convergence Management는 유무선 네트워크상에서 모든 이증관련 요청 사항 및 인증 처리, 사용자 관리, 로그 파일 관리를 처리하며, 인증, 보안, data에 관련된 정보보안 작업을 수행한다.

Authentication Management는 네트워크 환경에서인증에 관한 정보 및 사용자의 위치 트래킹을 따라서 사용자의 인증된 정보를 관리한다. 3D 모니터링을 통해 사용자의 인증을 하고, 이 정보를 관리함으로써 사용자에 대한 효율적 인증 처리를 한다. 또한 위치 정보 관리를 통해 사용자의 위치에 따른 서비스 제공 및 인증 체계 구성을 위해 사용한다.

Integrity Data는 DB에 저장된 원본 데이터에 대한 무결성 데이터를 생성함으로써 사용자가 원하는 서비스를 이용하는 경우 즉각적으로 무결성 검증을 한다.

Integrity Verification은 원본 정보와 무결성 정보를 비교하여 데이터의 무결성을 검증하고, 이상이 없는 경우 사용자에게 서비스를 제공하고, 정보가 변조 되었다고 판된 되는 경우에는, 원본 데이터의 복구 및 안전한 서비스의 제공이 이루어진다.

이러한 홈네트워크 보안 모델의 적용은 사용자의 효율적 인증 체계의 구성, 사용자 및 환경 정보의 무결성과 보안 관리, 다양한 네트워크 환경으로부터 체계적인 보안 프레임워크 구성, 사용자에게 맞는 지능형 서비스 제공을 위한 정책적 관리를 가능하게 한다. 또한 홈네트워크 보안 모델 및 전체 시스템을 융합적으로 구성함으로써 분산되어 있고 각 모듈에 따라 구성되어 있던 보안 시스템을 통합 관리가 가능하게끔 한다. 그리고 사용자 및 환경 정보를 관리하고 서비스에 대한 정책적인 요소 기술을 구조적으로 적용함으로써 보다 안정적이고 정확한 서비스를 제공하도록 한다.

Ⅴ. 결 론

홈네트워크는 여러 분야의 기술들을 유기적으로 결합하여 사용하기 때문에 기존 보안 문제에 대한 취약성을 그대로 포함하고 있으며, 요소기술 및 환경 등의 특성으로 인해 홈네트워크 정보기기에 대한 불법적인 공격이 빈번하게 발생할 수 있으므로 정보의 처리, 전달 및 저장을 안전하게 하기 위해서는 특히 보안 기술이 절실하게 요구된다.

기존 홈네트워크에서의 보안 기술은 단지 유무선 네트워크 인프라에서 적용되던 기본적인 보안 구조와 모듈을 활용하는 방안이 주가 되었다. 그러나 실질적인 홈네트워크 환경은 다양한 인프라 구조의 융합과 그 안에서 다양한 정보의 흐름이 이루어진다. 따라서 기존의 기술만으로는 홈네트워크 환경에서의 보안 강화에는 미약하다. 본 논문에서 제시한 새로운 보안 인프

라 구조는 다양한 인프라의 컨버전스 측면과 정보의 보안 및 인증, 정책적인 면에서의 보안을 강조하며 홈 네트워크에 좀 더 적합하도록 구성되었다.

홈네트워크를 구축할 때 가장 먼저 해야 할 일은 각각의 집에 제공할 서비스 레벨을 먼저 정의해야 한다. 예를 들어 가전 기기의 제어만을 지원하는 단순한 홈 오토메이션 수준의 홈 네트워킹을 구현할 것인지, 혹은 댁내에 오디오·비디오 신호의 실시간 전송을 위한 광대역 네트워크를 지원할 것인지에 대해 먼저 결정을 해야 이 서비스를 제공해 줄 수 있는 홈 네트워킹 아키텍처가 정해질 것이기 때문이다. DTV 서비스를 위한 멀티미디어 신호의 전송을 결정한다면 IEEE 1394 기술의 채택이 필수적일 것이며 IEEE 1394 기술을 채택하여 홈네트워크를 구현할 경우 백본 네트워크에 대한 선택이 또한 중요하게 된다.

여기에 특히 고려해야 할 핵심 기술로 홈네트워크를 위한 정보보호 기술의 접목이다. 어떤 사용자의 집안에 있는 가전 기기들을 디지털화하고 이들을 홈네트워크로 연결하려면 네트워크의 전문 지식이 없는 일반 사용자들을 고려하여 Plug and Play 기능은 필수적이지만 만일 그 사용자의 집에 다니러 온 모든 외부인들조차 아무런 인증 절차 없이 모든 정보를 노출시킬 수는 없기 때문이다.

본 홈네트워크 환경에서의 지식기반 서비스를 위한 보안 및 정책 연구에서는 안전한 홈네트워크 환경 구축을 위한 환경을 살펴보았고 운영상의 다양한 유형별 특성 및 보안 현황에 대해 분석을 하였다.

실시간 웹 무결성 검증 유비쿼터스 홈네트워크 보안 시스템을 통해 방화벽, SSL/TLS 등 기존의 보안 시스템에 실시간 웹 무결성 검증 홈네트워크 보안 시스템을 포함하여, 더욱 더 강건한 보안 서비스를 구축함으로서 정부기관이나 기업들의 웹 서버 데이터를 삭제, 또는 변조하거나 웹 페이지의 링크를 바꾸는 등 홈페이지에 대한 직접적인 공격을 방어할 수 있다. 아울러 OSGi를 이용한 웹 기반 무결성 홈네트워크 보안 서비스를 구축하여 사용자에게 집안의 상태 정보 등을 안전하게 서비스함으로서 더욱 안전한 홈네트워크 보안기술 개발에 도움이 될 것이라 생각한다.

사용자 기반의 지능형 서비스 제공을 위한 보안 기술 및 추론 엔진의 연구를 통해 Priority 및 Privacy의 고려를 통해 서비스의 Conflict 문제나 다중 사용자에 대한 문제점을 보완하여 다양한 정적 패턴의 서비스가 필요한 공간이나 위치인식에 따른 서비스 제공을 위한 부분에서 기반기술로써 이용될 것으로 기대할 수 있다.

유비쿼터스 환경에서의 홈네트워크는 사용자 적응적 서비스 제공을 위한 추론엔진을 통해 지능적 서비스 제공이 가능하다. 이는 다중 사용자로 시스템을 확장할 때 발생할 수 있는 Conflict 문제를 해결할 수 있으므로 유비쿼터스 사회 구현에 큰 부가가치 창출 가능성이 있다.

그러나 이러한 전체 홈네트워크 보안 시스템의 구성 및 모델의 제안은 실제적인 적용 방안과 시스템의 검증 방안이 요구된다. 그리고 기존의 보안 시스템과 통합 모델을 전체적으로 관리하기 위한 다양한 방향의 접근이 모색되어야 할 것이다.

참 고 문 헌

[1] Warren Webb, "Harmony at Home", http://www.edn.com 2004. 5.

[2] 이전우, 배창석, "디지털 홈 기술동향", 한국전자통신연구원, 2003.8.

[3] 손 홍, 장종표, "홈네트워크 표준화 로드맵", HN Focus, Vol. 05, 한국홈네트워크산업협회, 2005. 5.

[4] 이성몽, "유비쿼터스 컴퓨팅 환경에서 개인정보 보호 방법", IITA 기술정책정보단, 2005. 5.

[5] Theodore B. Zahariadis, "Home Networking Technologies and Standards", 2003.

[6] 박준희, 손영성, "홈네트워크 미들웨어 기술 및 표준화 동향", 전자통신동향분석 제19권 제 5호, 2004. 10.

[7] 맹혜선, 한탁돈, 김신덕, "멀티 매니징 기법을 이용한 웹기반 분산 병렬 컴퓨팅 환경", 정보처리학회 논문집 Vol. 6, No.7 1999. 7.

[8] N. Davies and H.W. Gellersen, "Beyond Prototypes: Challenges in Deploying Ubiquitous Systems," IEEE Pervasive Computing, vol. 1, no. 1, 2002, pp. 26-35.

[9] M. Román et al, "A Middleware Infrastructure for Active Spaces," IEEE Pervasive Computing, vol. 1, no. 4, 2002, pp. 74-83.

[10] W.Y. Lum and F.C.M. Lau, "A Context-Aware Decision Engine for

Content Adaptation," IEEE Pervasive Computing, vol. 1, no. 3, 2002, pp. 41-49.

[11] S. Yau et al., "Reconfigurable Context-Sensitive Middleware for Pervasive Computing," IEEE Pervasive Computing, vol. 1, no. 3, 2002, pp. 33-40.

[12] H. Chen et al., "An Ontology for Context-Aware Pervasive Computing Environments," Proc. IJCAI 03 Workshop Ontologies and Distributed Systems, IJCAI Press, 2003.

[13] Lee, J., Kim, S., Kim, D., Shin, J., Paik, J.K.: Feature fusion-based multiple people tracking. In: PCM (1). (2005) 843 - 853

[14] Mathew Laibowitz, "Parasitic mobility for pervasive sensor networks," In: Pervasive, 2005. Volume 3468 of Lecture Notes in Computer Science., Springer (2005) 255-278.

[15] Biegel, G., Cahill, "A framework for developing mobile, context-aware applications." In: PerCom. (2004) 361-365.

[16] Lee, M., Kim, J., Park, S., Lee, J., Lee, S., "A secure web services for location based services in wireless networks". In: NETWORKING 2004. Volume 3042 of Lecture Notes in Computer Science., Springer (2004) 332-344.

[17] Jeffrey Hightower, "Learning and recognizing the places we go. In: Ubicomp 2005. (Lecture Notes in Computer Science) 159-176

[18] Consolvo, S., Roessler, P., Shelton, B.E., "The carenet display: Lessons learned from an in home evaluation of an ambient display." In: Ubicomp. (2004) 1-17.

[19] Junhaeng Lee, "Feature fusion-based multiple people tracking." In: PCM (1). Volume 3767 of Lecture Notes in Computer Science., Springer (2005) 843-853.

[20] Leelasantitham, A.; Pattaramalai, S.; Chamnongthai, K.; Thipakorn, B.; "Inspection of water mark on currency note by using correlation mapping and neural network." Circuits and Systems, 1998. IEEE APCCAS 1998. The 1998 IEEE Asia-Pacific Conference on 24-27 Nov. 1998 Page(s):403-406.

[21] Kountchev, R.; Milanova, M.; Ford, C.; Rubin, S.; "Multimedia watermarking with complex Hadamard transform in the inverse pyramid decomposition." Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on 2003 Page(s):305-310.

[22] Minsoo Lee, Yong Kim, Yoonsik Uhm, Zion Hwang, Gwanyeon Kim, Sehyun Park and Ohyoung Song, "Location-Aware Multi-Agent based Intelligent Services in Home Networks," Lecture Notes in Artificial Intelligence, vol. 4203, Sept. 2006, pp. 178-187, Proc. ISMIS 2006, The 16th International Symposium on Methodologies for Intelligent Systems, Bari, Italy, September 27-29, 2006.

[23] Yong Kim, Yoonsik Uhm, Zion Hwang, Minsoo Lee, Gwanyeon Kim, Ohyoung Song and Sehyun Park, "A Context-Aware Multi-Agent Service System for Assistive Home Applications", Lecture Notes in Computer Science, vol. 4159, Sept. 2006, pp. 736-745, Proc. UIC-06, The 3rd International Conference on Ubiquitous Intelligence and Computing, China, September 3-6, 2006.

〈著者紹介〉

황 지 온 (Zion Hwang)

2003년 2월 : 중앙대학교 정보시스템학과 졸업
2005년 2월 : 중앙대학교 전자전기공학부 석사
2005년 9월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크, 지식기반 서비스 아키텍처 등

엄 윤 식 (Yoonsik Uhm)

2004년 2월 : 중앙대학교 전자전기공학부 졸업
2006년 2월 : 중앙대학교 전자전기공학부 석사
2006년 3월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크 미들웨어, 지식기반 서비스 아키텍처, 홈네트워크 보안 등

김 용 (Yong Kim)

2004년 2월 : 중앙대학교 전자전기공학부 졸업
2006년 2월 : 중앙대학교 전자전기공학부 석사
2006년 3월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크, 유비쿼터스 상황인지, 홈네트워크 보안 등

박 세 현 (Sehyun Park)
정회원
1999년 3월~현재 : 중앙대학교 부교수
2004년 8월~현재 : 홈네트워크 연구센터 센터장
관심분야 : 홈네트워크, 유비쿼터스 컴퓨팅, 인터넷 보안 및 정책 관리 등