홈 네트워크 보안 정책 프레임워크

김건우* · 김도우, 이준호, 한종욱

*한국전자통신연구원

Security Policy Framework for Home Network

Geon-woo Kim* · Do-woo Kim, Jun-ho Lee, Jong-wook Han

*Electronics and Telecommunications Research Institute

E-mail : kimgw@etri.re.kr

요 약

다양한 이동 기술, 센서 기술 및 원격 제어 기술이 발달하고 생활의 질이 향상됨에 따라, 홈 네트워크에 관한 연구와 개발이 활발히 진행되고 있다. 현재 네트워크 서비스 사업자와 건설 업체를 중심으로 다양한 홈 네트워크 서비스를 제공하려는 노력이 진행되고는 있지만 안전하고 효율적인 보안 서비스를 제공하기에는 아직 미흡한 측면이 있다. 따라서 본 논문에서는 홈 네트워크 서비스를 제공하는데 있어서 안전하고 다양한 사용자 인증 메커니즘을 제공하고 효율적으로 서비스를 제어하기 위한 보안 프레임워크를 제안한다. 즉, 각 호마다 설치되어 동작하는 홈 게이트웨이를 기반으로 호별 보안 정책을 설정하고 수행함으로써 다양한 보안 시나리오를 가능하게 하며, 추후 사업자 서버 및 로컬 서버와의 연동을 통해서 능동적인 홈 네트워크 시스템 보안 서비스를 제공하고자 한다.

ABSTRACT

As various mobile technologies, sensor technologies, and remote control technologies are growing and quality of life is enhanced, researches and developments on home network are actively on going. Currently, some network service providers and construction corporations are going to provide home network service, but neither secure nor efficient, So, in this paper, we propose a security framework for providing various secure user authentication mechanisms and efficiently controlling services in home network. Namely, we are going to provide active home network security services with home gateway-based security policy, which locates on the gateway of each home.

키워드

홈 네트워크 보안, 인증, 접근 제어, 보안 정책

Ⅰ. 서 론

홈 네트워크는 이동통신, 초고속 인터넷 등 유·무선 통신 네트워크를 기반으로 가정 내의 A/V, 데이터통신 및 정보가전 기기들이 네트워크로 상호 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스를 제공받을 수 있는 가정 환경을 구축하여 국민들에게 편리하고, 안전하고, 즐겁고, 윤택한 삶을 제공할 수 있는 새로운 IT 기술 이용 환경이라 할 수 있다[1].

홈 네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버 공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, 서비스 거부 공격, 통신망 도·감청 등에 보안 취약성을 내포하고 있다[2].

따라서 본 논문에서는 이러한 홈 네트워크 상에서 이러한 보안 취약성을 제거하여, 보다 안전하고 효율적인 홈 네트워크 서비스를 제공하기

위한 보안 프레임워크를 제안한다.

II. 본 론

안전하고 효율적인 홈 네트워크 서비스를 제공하기 위해서는 기본적으로 다양한 사용자 인증 메커니즘, 강력하고 효율적인 접근 제어, 및 보안 정책 관리 기능 등이 필요하다. 이러한 보안 서비스를 집행하기 위해서 각 호마다 별도의 홈 게이트웨이를 설치하고, 각 호의 사용자 및 다양한 인증, 홈 네트워크 사업자 서버와의 인터페이스 역할을 수행한다. 따라서 사업자 서버의 오버헤드를 감소시킬 수 있을 뿐 아니라, 각 호별 맞춤형 보안 서비스가 가능하다.

그림 1은 홈 네트워크 보안을 위한 컴포넌트를 도식화한 그림이다.

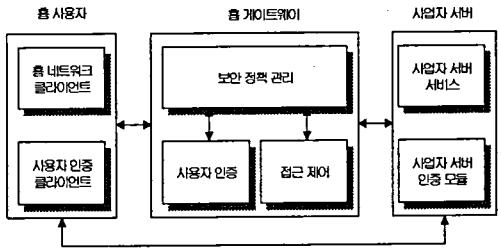

그림 1. 홈 네트워크 보안 컴포넌트

홈 네트워크 사용자는 사업자 서버의 인증 메커니즘과 관련 없이 원하는 인증 메커니즘을 선택해서 사용할 수 있으며, 홈 게이트웨이는 홈 사용자를 대신해서 사업자 서버와 인증한다. 사용자 인증이 끝나면 인증 정보화 서비스를 기반으로 접근 제어를 수행하며, 이는 사업자 서버에 투명성을 보장한다. 보안 정책 관리는 사용자 인증과 접근 제어에 필요한 보안 정책을 수립하고 분배하는 기능을 담당한다.

2.1 사용자 인증

홈 네트워크 사용자는 개인의 기호에 맞는 다양한 인증 메커니즘을 사용할 수 있어야 한다. 즉 모든 가족이 홈 네트워크를 사용할 수 있다면, 개인의 취향과 보안 강도에 따르는 다양한 인증 서비스를 제공해야 한다. 하지만 현재 홈 사업자는 IP/PW와 인증서 방식만을 선별적으로 채택해서 사용하고 있으며, 차세대 인증 방식으로 각광받고 있는 생채 인증 메커니즘이나 RFID와 같은 방식을 사용하기에는 아직 무리가 있는 실정이다. 따라서 사업자 서버가 제공할 수 없는 인증 메커니즘을 각 호마다 별도로 동작하는 홈 게이트웨이에서 수행하게 함으로써 사용자 효율성을 증대시킬 수 있다.

이를 도식화한 그림은 그림 2와 같다.

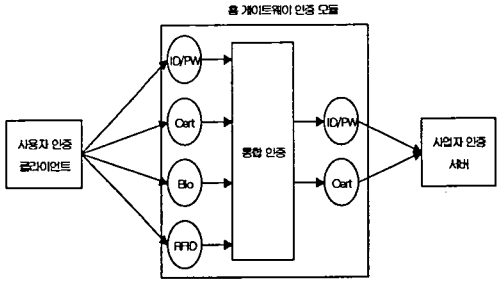

그림 2. 홈 네트워크 인증 모듈

홈 게이트웨이의 인증 모듈은 다양한 인증 메커니즘 간의 연동을 지원해야 하며, 이를 위해서 실시간 매핑 테이블을 구성할 수 있어야 한다. 즉, 사용자와 사업자의 투명한 인증 연동을 지원하고, 인증 메커니즘의 수정, 삭제와 같은 수정 작업이 용이해야 한다.

2.2 접근 제어

효율적인 홈 네트워크 서비스를 제공하기 위해서는 다양한 접근 제어 모듈을 제공해야 한다. 홈 네트워크의 특성을 고려할 때, 다양한 가족의 구성원들이나 손님, 원격 검침원 등 신뢰할 수 없는 사용자들로부터의 홈 디바이스와 서비스를 보호하고 제어하기 위해서는 역할 기반 접근 제어 기능을 제공하는 것이 바람직하다.

홈 네트워크 VoD 서비스를 예로 들면, 컨텐츠 제공자나 사업자 서버의 입장에서는 인증만 성공적으로 수행되면 해당 서비스를 제공하는 것을 목표로 하고 있다. 하지만, 홈 게이트웨이 입장에서는 인증에 성공했을 경우라도 서비스를 차단해야 할 필요가 있다. 중학생 자녀가 성인물 VoD 서비스를 받고자 하는 경우, 홈 게이트웨이에서 별도의 접근 제어를 제공해야 한다. 이러한 보안 정책은 사업자 서버에서 제공하기에는 많은 오버헤드가 발생하기 때문에, 각 가정의 환경에 맞는 맞춤형 접근 제어 정책을 수립하고 수행할 수 있어야 한다.

홈 사용자로부터 서비스 요청이 발생하면, 먼저 해당 인증 메커니즘을 구동해서 사용자 인증 과정을 수행한다. 인증이 성공적으로 마치면, 이 인증 정보와 서비스를 기반으로 접근 제어를 요청한다. 이러한 접근 제어는 미리 설정된 접근 제어 DB에 저장되어 있으며, 이는 보안 정책 관리 모듈에서 관리한다. 접근이 허용되면 해당 홈 디바이스나 서비스를 제공하고, 접근이 허용되지 않으면 해당 사용자에 접근 권한 없음 메시지를 전송한 후 패킷을 제거한다.

그림 3은 접근 제어 모델을 정의한다.

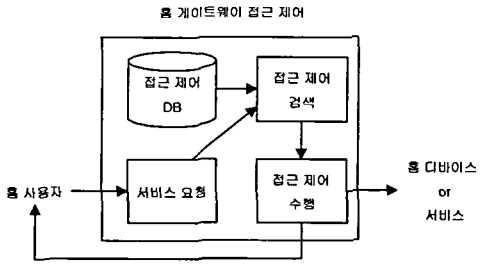

그림 3. 접근 제어 모델

2.3 보안 정책 관리

홈 네트워크 보안을 위한 필수 기능인 사용자 인증과 접근 제어를 상위 레벨에서 관리하고 제어하기 위한 기능이다. 즉, 상위 레벨의 보안 정책을 수립하고 분배하기 위한 기능으로서 다양한 모델에 적용될 수 있어야 한다.

현재 개발되고 있는 홈 게이트웨이는 최소의 처리 기능만을 수행하고 있으며, 이 장비에 사용자 인터페이스를 통한 보안 정책 관리 서버를 운용하는 것은 바람직하지 않을 수도 있다. 따라서 본 논문에서 제안하는 방식은 다양한 홈 게이트웨이 사용과 모델을 공통적으로 적용될 수 있는 확장성 있는 보안 정책 관리 모듈을 제안한다.

그림 4는 보안 정책 프레임워크를 도식화한 그림이다.

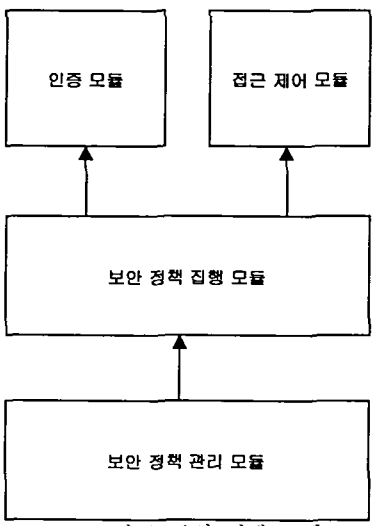

그림 4. 보안 정책 모델

홈 네트워크 보안 정책은 크게 보안 정책을 생성하고 분배하는 기능을 수행하는 보안 정책 관리 모듈과, 설정된 보안 정책을 수행하는 보안 정책 집행 모듈로 구성된다. 이 두 모듈이 물리적으로 한 장비에 설치될 필요는 없지만, 보안 정책 집행 모듈은 반드시 홈 게이트웨이 상에서 구동해야 한다.

보안 정책 관리 모듈은 사용자 직관적인 인터페이스를 제공해야 하며, 이는 가정 내 관리자에 의해서 설정될 수 있어야 한다.

모든 경우를 고려해야 복잡한 보안 정책을 수립해야 하는 것은 홈 네트워크를 관리하는 입장에서 난감한 일이 아닐 수 없다. 따라서 이 시스템은 기본 설정을 포함하고 있어야 하며, 관리자로 하여금 특정 보안 정책만을 생성하면, 자동적으로 보안 정책을 수립할 수 있어야 한다.

그림 5는 보안 정책 모듈을 세분화한 그림이다.

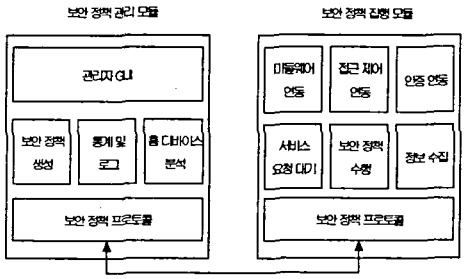

그림 5. 보안 정책 수행

보안 정책 관리 모듈은 크게 보안 정책을 생성하는 기능, 통계 및 로그 처리 기능, 홈 디바이스 분석 기능, 관리자 GUI, 및 안전하게 보안 정책을 분배하기 위한 보안 정책 프로토콜로 구성된다. 관리자 GUI는 보안 정책 관리 모듈이 설치되는 장비의 특성을 고려해서 개발되어야 하며, 관리자 편이성을 위해서 자동으로 홈 디바이스를 인식하고 등록할 수 있어야 한다.

보안 정책 집행 모듈은 미들웨어 연동 기능, 접근 제어 연동, 인증 연동, 서비스 요청 대기, 보안 정책 수행, 및 사용자 정보 수집 기능으로 구성된다.

이러한 기능은 안전하고 효율적인 홈 네트워크 서비스를 제공하기 위해서 필요한 기능으로, 구체적인 구현 방식은 환경에 따라 달라질 수 있다.

III. 결 론

홈 네트워크는 다양한 기기와 사용자에게 안전하고 효율적인 서비스를 제공하기 위한 환경을 지원한다. 따라서 다양한 홈 네트워크 서비스를 구성하는 것도 중요하지만, 내·외부의 불법 접근으로부터 홈 디바이스와 서비스를 안전하기 보호하기 위한 홈 네트워크 보안 서비스가 중요한 이슈로 부각되고 있다.

따라서 본 논문에서는, 안전하고 효율적인 홈 네트워크 보안 서비스를 제공하기 위해서 필요한 보안 프레임워크를 정의하고 각 모듈 및 연동 모델을 제시한다.

다양한 사용자 인증 메커니즘을 제공하기 위한 통합 인증 모듈, 사용자별, 홈 디바이스별, 홈 네트워크 서비스별로 다양한 접근을 제어하기 위한 접근 제어 모듈, 전체 홈 네트워크의 보안 파라다임을 설정하기 위한 보안 정책 모듈로 구성된다.

홈 네트워크는 통합 인증 모듈, 접근 제어 모듈, 및 보안 정책 모듈 간 유기적인 연동을 통해서 홈 네트워크 사용자에게 보다 안전하고 편리한 서비스를 제공할 수 있다.

또한 사업자 서버의 오버헤드를 줄일 수 있으며, 추후 사업자 서버와 로컬 서버에 동일하게 적용할 수 있는 확장성을 제공한다.

참고문헌

[1] 김정원, 정보통신부, "홈 네트워크 산업 활성화 정책 방향", 정보과학회지, 2004, 09, 제 22권 제 9호 통권 제 184호

[2] 한종욱, 김도우, 주홍일, 한국전자통신연구원, "홈 네트워크 보안 프레이워크 구축을 위한 고려사항", 정보과학회지 2004, 09, 제 22권 제 9호 통권 제 184호