VPN을 이용한 Embedded 홈 네트워크 시스템 보안

Embedded Home Network System Security using VPN

진선일*, 정진규*, 안광혁*, 유영동*, 홍석교*

* 아주대학교 전자공학과 (전화 : (031)219-2489, 팩스 : (031)212-9531, E-mail : jj3jj@hanmail.net)

Abstract : The home network system of ubiquitous computing concept is changing present our home life as more comfortable and safe. Also, it permits that we can connect the home network system and control the appliance which is linked to the home network system without limitation in time and place. But, as other systems that use the public network like the Internet, remote control/monitoring of the home network system that use the Internet includes problems such as user's access which is not admitted and information changing. This paper presents the efficient solution about the security problem that is recognized to important problem of the home network system. Also this paper implements the security of the home network system based on the UPnP (Universal Plug and Play), adding VPN (Virtual Private Network) router that uses the IPsec to the home network system which is consisted of the ARM9 and the Embedded Linux.

Keyword : Ubiquitous, Home Network System, Embedded system, UPnP, IPsec, VPN

Ⅰ. 서론

가정 내의 디지털 정보 기기들을 기능 공유, 데이터 공유 등을 목적으로 네트워크화 한다는 개념인 홈 네트워크 시스템은 UPnP와 같은 미들웨어를 이용함으로써 사용자로 하여금 홈 네트워크 시스템에 새로운 가전 기기들을 쉽게 추가하고 제거할 수 있게 하고 있다.[1] 또한 PDA, 핸드폰, 노트북 등의 이동식 기기들을 통해 언제 어디에서든 홈 네트워크 시스템에 접속하여, 원하는 기기들을 원격제어 및 감시할 수 있게 됨으로써, 홈 네트워크는 미래의 우리 가정 내 모습을 보다 더 편안하고 윤택하게 해주고 있다.

그러나 인터넷과 같은 공중망을 이용한 홈 네트워크 시스템의 원격제어 및 감시는 인터넷을 이용하는 다른 네트워크 시스템과 마찬가지로 보안적인 측면에서 원치 않는 이용자의 접근 및 정보 조작 등의 문제를 포함하고 있다.[2][3][4] 그러한 문제를 해결하기 위해서는 침입방지 시스템(IPS), 침입탐지시스템(IDS), VPN 등과 같은 보안 개념들이 기존의 홈 네트워크 시스템에 적용되어야 한다.[2]

본 논문에서는 ARM9과 임베디드 리눅스로 구현된 홈 서버에 VPN 라우터를 추가함으로써 강력한 보안 기능이 더해진 홈 네트워크 시스템을 구축하고자 한다.

II. 홈 네트워크 시스템과 VPN

1. 홈 네트워크 시스템

홈 네트워크는 다양한 기능을 가진 가정 내 디지털 정보 기기들을 기능 공유, 데이터 공유, 원격 제어 등을 위해서 하나의 네트워크로 연결한 것을 말한다. 이러한 홈 네트워크는 다양한 정보, 편리한 생활, 사생활 보호, 안전한 가정 생활 등을 제공하면서 가정 내의 삶을 보다 더 편안하게 해주고 있다. 또한 유비쿼터스 개념이 미래의 디지털 정보 사회의 모습으로 대두되면서 언제 어디서나 가정 내 디지털 미디어를 즐길 수 있는 유비쿼터스 개념을 포함한 홈 네트워크 시스템으로 발전하고 있다.

2. UPnP

UPnP는 Universal Plug & Play를 나타내며 홈 네트워크에 사용되는 대표적인 미들웨어 중 하나이다. 미들웨어는 사용자 인터페이스와 제어 디바이스 사이에서 서로를 연결해 주는 소프트웨어이다. 홈 네트워크에 사용되는 미들웨어로는 HAVi (Home Audio/Video Interoperability), JINI (Java Intelligent Network Infrastructure) 등이 있으며, 본 논문에서는 UPnP를 이용하였다.

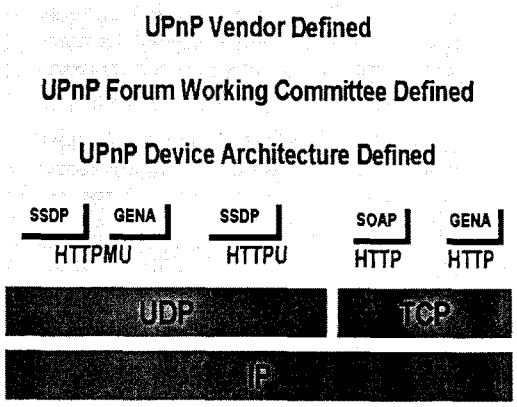

그림1. UPnP 구조

Figure1. UPnP Structure

UPnP는 물리 망이 Ethernet, PLC(Power Line Communication), IEEE1394, Bluetooth 등 어느 것이 되더라도 별도의 configuration 없이 쉽게 각각의 망에 연결되어 있는 기기들을 제어할 수 있게 한다.

3. VPN

VPN(Virtual Private Network)은 네트워크 상의 여러 노드들 사이의 통신을 가능하게 하는 Network 특성, 사설 망의 강력한 보안 기능을 그대로 가지는 Private 특성, 기존에 존재하는 공공망인 인터넷 상에 새로운 연결 통로를 만드는 Virtual 특성 등을 가지는 보안 망의 개념이다. 그림2는 VPN을 구현하는 표준 프로토콜을 나타낸다.

	PPTP	L2TP	IPsec	SOCKS V5
표준화	Vendor-specific	RFC 2661	RFC 2401-2410	RFC 1928,1929,1961
OSI 계층	Layer 2	Layer 2	Layer 3	Layer 5
작동 모드	Client/Server	Client/Server	Peer-to-Peer	Client/Server
지원하는 프로토콜	IP,IPX,NETBEUI, etc.	IP,IPX,NETBEUI, etc.	IP	TCP, UDP/IP
터널 서비스	접속당 단일 PPP 터널	접속당 단일 PPP 터널	SA에 기반한 다중 터널	각 세션에 대해서 별도의 터널
사용자 인증	PAP/CHAP	PAP/CHAP	없음	제공됨
데이터 인증/암호	없음	없음	AH/ESP에 의해서 암호화/인증 제공	GSS-API를 이용해서 메시지마다 암호화/인증
키 관리	없음	없음	ISAKMP/IKE	GSS-API/SSL

그림2. VPN 표준

Figure2. VPN Standard

VPN Standard 중에서 IPsec은 IETF에서 설계하고 IPv6에서 기본으로 제공되는 보안 프로토콜로써 현재 많은 VPN 장비에 사용되고 있고, 본 논문에서도 IPsec을 이용하여 VPN을 구현하였다. IPSec은 Internet Protocol을 위한 security architecture로써[4], 컴퓨터들 사이의 안전한 통신과 암호 키 교환을 구현하는 표준 프로토콜들의 집합이다. IPsec은 인증과 암호화를 위해 AH(Authentication Header)[5]와 ESP(Encapsulation Security Payload)[6] 을 사용하며, 암호 키 교환을 위해서는 IKE(Internet Key Exchange)[7]를 사용한다.

Ⅲ. 홈 네트워크 시스템 구현

홈 네트워크 시스템은 크게 Home Server, Appliance, Medium으로 구성된다.

1. Home Server

Home Server는 홈 네트워크 시스템의 외부와의 연결 통로이다. 그림3는 Home Server의 구성을 나타내고, 그림4는 임베디드 홈 서버를 구현하기 위해 사용한 ARM9을 이용한 Target board이다.

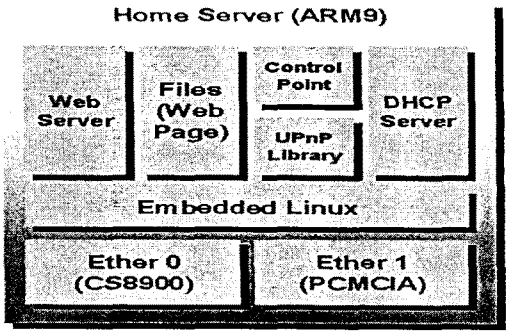

그림3. 홈 서버

Figure3. Home Server

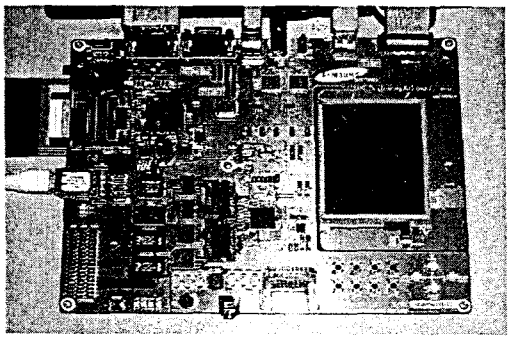

그림4. ARM9 기반의 Target Board

Figure4. Target Board based on the ARM9

홈 서버는 원격지에서의 접속과 홈 네트워크 상에 있는 가전 기기들을 연결해주기 위해서 웹 서버를 포함한다. 또한 홈 서버는 UPnP 관점에서 Control point에 해당하므로 UPnP 라이브러리를 포함하고 있고, 네트워크에 새로이 추가되는 가전 기기들에게 자동으로 IP를 할당하기 위해 DHCP 서버를 포함하고 있다.

2. Appliance and Medium

실제 가전 기기들을 이용하지 않고, 일반 PC 위에 가상으로 가전 기기들을 구현하였다. 가상의 가전 기기들을 구현하기 위해서 Intel에서 제공하는 UPnP Tool을 이용하였다. Medium은 Ethernet을 이용하여 구성하였다.

Ⅳ. VPN 라우터 구현 및 적용

먼저 리눅스를 이용하여 라우터를 만들고, FreeS/WAN [10]을 이용하여 그 라우터 위에 소프트웨어적으로 VPN을 구현하였다. Encryption/Decryption 과정에서 발생하는 시스템 부하를 최소화 하기 위해 Crypto API를 이용하여 인증/암호화 관련 알고리즘을 kernel에 적재하였다. 또한 kernel-2.4.x에서 지원하는 Firewall인 IPTABLE을 이용하여 VPN 라우터에 Firewall기능을 추가하였다.

그림5는 VPN 라우터를 이용하여 구성한 전체 홈 네트워크 시스템을 나타낸다.

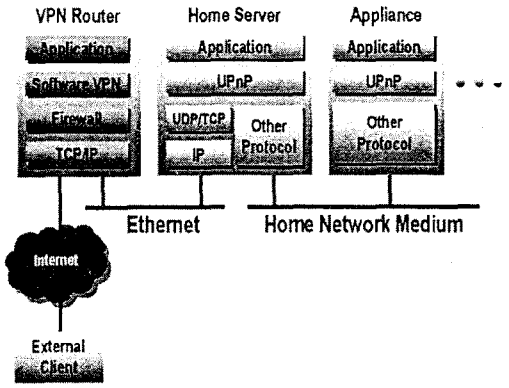

그림5. 전체 시스템 구성도

Figure5. Whole system schematic diagram

V. 결론

본 논문에서는 홈 네트워크 시스템의 외부와의 연결 통로인 홈 서버를 UPnP 기반의 임베디드 시스템으로 구현한 다음, 인터넷과 같은 공중망을 이용한 Remote control/monitoring 시에 발생할 수 있는 보안 상의 문제점을 VPN 라우터를 이용하여 해결하였다. VPN을 이용함으로써, 공중망인 인터넷으로도 안전하게 홈 네트워크 시스템에 접근하여 제어/감시할 수 있고, 또한 VPN의 특성으로써 사무실의 네트워크와 홈 네트워크를 하나의 사설 망과 같이 안전하게 이용할 수도 있다. 그러나 소프트웨어로 구현된 VPN은 데이터의 Encryption & Decryption 시에 많은 연산을 처리해야 하기 때문에, 시스템에 부하를 발생시킬 수 있다. 따라서 소프트웨어로 구현된 VPN시스템을 Hardware Acceleration을 이용한 시스템으로 대체함으로써 이러한 부하 문제를 해결해야 할 것이다. 또한 VPN 라우터와 Home Server를 각각 두지 않고 하나의 시스템으로 통합하게 되면 전체 홈 네트워크 시스템을 보다 간결하게 구성할 수 있을 것이다.

참고 문헌

[1] Michael Jeronimo, Jack Weast, "UPnP Design by Example" Intel, 2003

[2]Carl M. Ellison, Corporate Technology Group, Intel Corporation, "Home Network Security", Intel Technology Journal, vol 06, November 15, 2002

[3] www.certcc.or.kr

[4] 안광혁, "원격 감시를 위한 내장형 소형 웹 서버", 아주대학교, Feb., 2001

[5] Stephen Kent, Randall Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, IETF, Nov., 1998

[6] Stephen Kent, Randall Atkinson, "IP Authentication Header", RFC 2402, IETF Nov., 1998

[7] Stephen Kent, Randall Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, IETF, Nov., 1998

[8] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, IETF, Nov., 1998

[9] Intel, "IP Security : Building Block for the Trusted Virtual Network", Intel Corporation, 1999

[10] www.freeswan.org

[11] Intel, "IPsec Offload Performance and Comparison", Intel Corporation, 2000

[12] Poonam Arora, Prem R. Vemuganti, Praveen Allani, "Comparison of VPN Protocols – Ipsec, PPTP and L2TP", Department of Electrical and Computing Engineering George Mason University, 2001