사용자 중심의 홈네트워크를 위한 키 교환 프로토콜 설계

정민아*

A design of Key Exchange Protocol for User Centered Home Network

Min-A Jeong

요 약

본 논문에서는 편재형 컴퓨팅(pervasive computing)환경을 제공하는 홈네트워크으로서 보다 향상된 사용자 중심의 홈네트워크를 편재형 홈 네트워크라 정의한다. 이를 위해 사용자가 다른 홈네트워크의 장치를 사용하고자 할 경우 이를 직접 제어하고 설정할 필요가 없도록 이동에이전트 개념을 도입하였고, 이러한 홈네트워크 환경에서 이동 에이전트는 다른 홈네트워크로 이동하여 필요한 장치들을 제어할 수 있다. 또한, 이와 같이 제안한 홈네트워크 환경에서 사용자와 원격 홈 네트워크를 접근하는 상대방 홈 서버를 인증하고, 홈 네트워크 사이에 전송되는 텍스트 및 멀티미디어 데이터와 이동 에이전트를 보호하기 위하여 키 교환 프로토콜을 설계하였다. 키 교환 프로토콜은 데이터 종류에 따라 인증 및 데이터 암호화를 수행하기 위하여 본 논문에서 제안한 프로토콜과 IPSec을 선택적으로 사용하는 다중모드를 제공한다.

ABSTRACT

In this paper, we define that pervasive home network, which provides necessary services for user properties and removes distractions to improve the quality of human life. So, user can enjoy home network technology including devices and softwares at any place with no knowledge of networked home, devices, and softwares. In this home network, a mobile agent, called LAFA, can migrate to unfamiliar home network and control the necessary devices. For this environment, we design security management module for authenticating user and home server that access some other home networks, and for protecting text, multimedia data, and mobile agent that are transferred between home networks. The security management module is composed of a key exchange management module and an access control management module. For key exchange management module, we propose a key exchange protocol, which provides multimode of authentication mode and key exchange mode. One of these two modes is selected according to the data type.

키워드

홈네트워크, 이동 에이전트, 키 교환, 인증, IPSec,

*전남대학교 전자통신기술연구소

접수일자 : 2003. 12. 10

Ⅰ. 서 론

홈네트워크에서 사용할 장치에 대한 설정은 HAVi, Jini, and UpnP와 같은 장치 미들웨어들에 의해서 자동적으로 수행된다[1,2,3]. 이러한 미들웨어들은 원격 제어 기능만을 제공하므로 사용자가 자신의 홈네트워크 장치들을 제어할 경우나 사용자가 다른 홈네트워크로 이동할 경우에 친숙하지 않은 다른 홈네트워크에 쉽게 적응할 수 없다. 이러한 문제를 해결하기 위해 본 논문에서는 LAFA(Logical Appliance Flow Agent)라는 이동 에이전트를 사용한다[4]. LAFA는 장치를 자동으로 제어하고 제어흐름을 자동으로 관리함으로써 사용자가 장치를 설정해야 하는 번거로움을 제거하였다. 또한, 사용자가 어플리케이션을 설치해야 하는 어려움을 해결해 주었으며, 어느 홈네트워크에 이동하더라도 쉽게 적응할 수 있도록 한다. 이와 같이 본 논문에서는 사용자의 편리성에 중점을 둔 사용자 중심의 홈네트워크를 편재형 홈네트워크라 정의하였다. 이러한 편재형 홈네트워크 환경은 사용자에게 많은 편리함을 주는 반면, 이러한 환경에서 사용되는 모든 장치들은 서로 네트워크로 연결되어 있으므로 다양한 불법적 접근을 막기 위해 보다 신중한 고려가 필요하다[5,6,7]. 그러므로 본 논문에서 제안한 사용자 중심의 홈네트워크 환경에서는 사용자 또는 다른 홈네트워크를 접근하는 홈서버에 대한 인증이 요구된다. 또한, LAF(Logical Appliance Flow) 수행에 필요한 원격 홈네트워크 간에 이동되는 LAFA나 텍스트 및 멀티미디어 데이터 등 전송되는 각 데이터의 종류에 맞는 적절한 보호가 요구된다. 멀티미디어 데이터나 LAFA가 이동해야 할 경우 세션 시간이 시간이 길어지기 때문에 세션키를 주기적으로 갱신을 해줘야 하며, 짧은 텍스트 데이터인 경우는 세션 시간이 매우 짧기 때문에 전송 중에 세션키를 갱신할 필요가 없다. 그러므로 본 논문에서는 홈네트워크 환경에서 접근하는 사용자에 대한 인증, 각 홈서버 간에 LAF를 실행하기 위해 이동하는 에이전트(LAFA)와 LAF가 실행될 때 발생하는 데이터 및 원격 홈네트워크 사이에 교환되는 데이터에 대한 보호하기 키 교환 프로토콜을 설계한다. 키 교환 프로토콜은 인증 관리 모듈과 암호화 관리 모듈로 구성하였으며, 데이터 종류에 따라서 인증 및 데이터 암호화를 수행하기 위하여 본 논문에서 제안한 프로토콜과 IPSec을 선택적으로 사용하는 다중모드를 지원한다. 텍스트 데이터 전송시 인증 및 데이터 보호는 본 논문에서 제안한 프로토콜의 키 교환 모드로 수행된다. 그리고 LAFA와 멀티미디어 데이터 전송시 인증은 프로토콜의 인증 모드로 수행되고 데이터 보호를 위해서는 IPSec을 사용한다. 본 논문의 구성은 다음과 같다. 2장에서는 키 교환 프로토콜 설계를 위한 관련연구를 기술한다. 3장에서는 본 논문에서 제안한 편재형 홈네트워크 구조와 각 구성요소에 관하여 기술한다. 4장에서는 본 논문에서 제안한 홈네트워크내에서 보안을 유지하기 위해 설계한 키 교환 프로토콜에 관하여 기술한다. 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2. 1 키 교환 프로토콜 특성

키 교환 프로토콜의 주된 기능은 안전한 세션키 생성이다. 안전한 세션키 생성을 위해서 흔히 고려하는 사항은 쌍방 인증, PFS(Perfect Forward Secrecy) 지원, 클로깅(Clogging)이나 재전송 공격(Replay Attack)에 대한 대비 등이다. 이 외에도 키 생성의 효율성이나 다양한 모드로 동작하는 다중모드(multimode) 지원, 세션 키 재 생성의 효율성, 키의 독립성, 프로토콜의 단순성 등도 많이 고려된다.

2.2 기존의 키교환 프로토콜

본 절에서는 네트워크 계층과 응용 계층에서의 기존의 키 교환 프로토콜들을 기술한다.

1) IKE(Internet Key Exchange)

IKE는 보안 조합(Security Association:SA)을 위하여 인증된 키 관련 사항들을 협의하고 제공하기 위한 IPSec의 디폴트 키교환 프로토콜이다[8,9,10]. IKE는 키 교환을 하기 위하여 서로 다른 2단계를 정의하고 있고 각각의 단계에서 설정된 SA를 각각 SA-1, SA-2라 한다. SA-1의 목적은 SA-2를 위하여 안전하고 인증된 채널을 형성하는 것이며, SA-2는 SA-1의 파라미터를 사용하여 사용자 데이터를 암호화하기 위한 파라미터를 협의 하는 것이다. SA-2에서 협의한 파라미터는 추후에 IPSec의 AH(Authentication Header)나 ESP(Encapsulation Security Payload)등의 프로토콜에서 사용한다. 하나의 SA-1으로 다수의 SA-2를 설정할 수 있다.

2) SKEME

SKEME는 주로 IP계층에서의 보안 프로토콜의 키 관리 프로토콜이지만 다른 인터넷상의 보안 응용들의 키 관리 프로토콜로도 사용할 수 있다[11]. 이 프로토콜은 basic, share, pre-shared, 그리고 fast 등의 네가지 모드와, SHARE, EXCH 그리고 AUTH 등의 세 가지 단계를 제공한다.

3) SSL/TLS

이 프로토콜은 TLS Record Protocol 와 TLS Handshake Protocol 등의 두 개의 계층으로 구성된다[9,12,13,14]. TLS Record Protocol에서는 TLS Handshake Protocol 와 같은 다양한 상위 프로토콜들을 캡슐화하여 연결 보안성을 제공한다. TLS Handshake Protocol은 TLS Record Layer 상위에서 동작하면서 세션의 암호화 파라미터들을 협의한다.

4) SKIP(Simple Key-management for Internet Protocol)

SKIP은 네트워크 계층의 보안 프로토콜인 IPSec의 AH나 ESP와 같은 session-less datagram protocol 등과 함께 사용할 수 있도록 설계되었다[13,15]. SKIP은 최초 설계시 기능에는 PFS가 포함되어있지 않다. 그래서 이 기능을 포함시키도록 확장할 수 있지만 그에 따른 상당한 오버헤드가 발생하는 것으로 알려져 있다.

2.3 IPSec

IPSec은 IETF의 IPv6의 보안 프로토콜이며, IPv4에서도 옵션으로 사용할 수 있다[9,10,12]. IPSec은 IP계층에서 인증과 암호화를 위하여 AH(Authentication Header)와 ESP(Encapsulation Security Payload) 두 가지 프로토콜을 가지고 있으며 키 관리를 위하여 디폴트 키관리 프로토콜로 IKE를 사용한다. ESP는 데이터의 기밀성과 무결성을 보장하고 옵션으로 데이터 인증 서비스를 제공한다. AH는 패킷 수준의 데이터의 인증과 무결성을 보장 받기 위하여 사용된다. AH는 ESP와 마찬가지로 데이터 인증 서비스를 제공하지만 인증 범위가 ESP보다 더 넓다. AH와ESP들은 각각 두 가지 모드로 Tunnel과 Transport를 제공한다.

III. 편재형 홈네트워크

본 장에서는 편재형 홈네트워크에 대한 시스템 구조 및 구성요소를 간략히 서술한다. 그림 1은 편재형 홈네트워크에 대한 참조 모델을 나타낸다. 본 장에서는 이러한 여러 구성요소 중 보안 관리 모듈과 관련된 몇가지의 개념에 관하여 기술하고자 한다.

Functional Component Module (FCM)

장치(또는 appliance)의 단위기능을 구현한 모듈로서 어플리케이션에서 호출 가능한 최소단위모듈(Function)이다. 예를 들어 텔레비전은 tuner FCM, display FCM과 clock FCM을 포함한다[R. Lea00].

Logical Appliance (LA)

각 장치들은 대체적으로 기계, 센서, 사용자 인터페이스, 그리고 컨트롤러 등을 포함하는 구성요소들을 포함한다. 만약 이러한 컴포넌트들이 서로 연결되어 통신할 수 있다면 보다 더 유연성있게 장치의 기능들(FCM)을 공유할 수 있다. 특정 기능을 제공하기 위한 이러한 장치 구성요소들(FCM)의 조합의 결과를 'Logical Appliance'라 한다.

Logical Appliance Flow (LAF)

LA를 형성하는 FCM들 간에 수행 순서를 추가한 것을 의미한다. FCM간에 수행순서를 미리 결정해 놓아, 시작 FCM이 사용자의 요구에 의해 시작되면, 수행순서대로 다음 FCM을 거쳐 마지막 FCM까지 자동적으로 수행된다.

Functional Component Table (FCT)

FCM수행에 필요한 정보 및 LAF 구성정보를 포함한다.

LAF Execution Engine

LAF 수행 엔진은 각 홈네트워크내에 홈서버에 설치되어 LAF를 관리하고 수행한다. 또한 서로 다른 홈네트워크에 설치되어 있는 LAF 수행 엔진들은 서로 협력하여 장치 등의 자원을 공유하며, LAF가 서로 다른 홈네트워크 사이를 이동할 수 있는 환경을 제공한다.

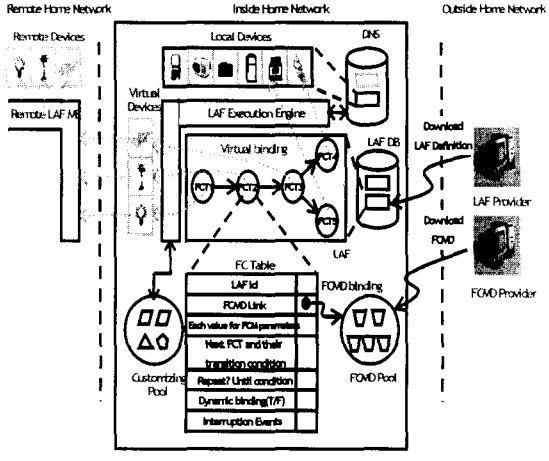

그림 1. 편재형 홈네트워크 구조

IV. 홈네트워크를 위한 보안의 필요성 및 키교환 프로토콜 설계

이 장에서는 홈네트워크 환경에서 발생하는 데이터와 데이터 전송형태를 기술한다. 또한, LAFA와 데이터들을 안전하게 전송하기 위한 보안의 필요성 및 키교환 프로토콜을 제안한다.

홈네트워크 사용자는 LAF를 수행하기 위해 먼저 인증을 받은 후 디폴트 홈네트워크 서버(Default Home Network Server)에게 작업을 지시하고 처리결과를 전달 받는다. 또한 사용자가 지시한 작업을 처리할 때 디폴트 홈네트워크 서버는 필요한 경우 LAFA를 생성하여 사용자가 위치한 홈네트워크나 외부의 다른 홈네트워크로 전송한다. 외부 홈네트워크에 존재하는 사용자에게 자신의 홈네트워크가 아닌 다른 홈네트워크에서 데이터를 전송할 필요가 있는 경우에는 그 사용자의 홈네트워크를 경유하지 않고 그 홈네트워크에서 직접 사용자에게 전송한다. 이러한 환경에서 그림 2에서 제시한 바와 같이 홈네트워크를 접근하는 사용자들에 대한 인증, 인증된 사용자에게 LAF를 접근하는 권한 부여, 원격 홈네트워크에서 LAF를 수행하기 위한 서로 다른 홈서버 간 인증, LAF 수행을 위해 전달되는 이동 에이전트와 데이터, 그리고 LAF가 수행된 후 다른 홈서버 또는 사용자에게 전달되는 데이터에 대한 무결성 및 기밀성을 유지하는 것이 필요하다.

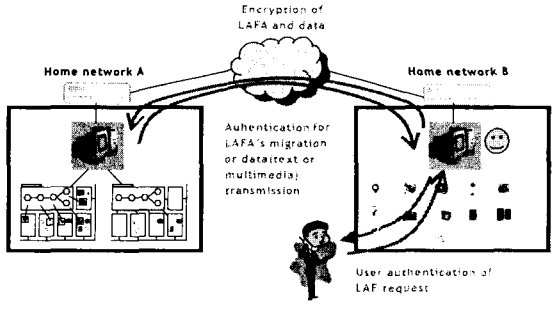

그림 2. 홈네트워크 환경에서의 보안의 필요성

4.1 보안 관리 모듈

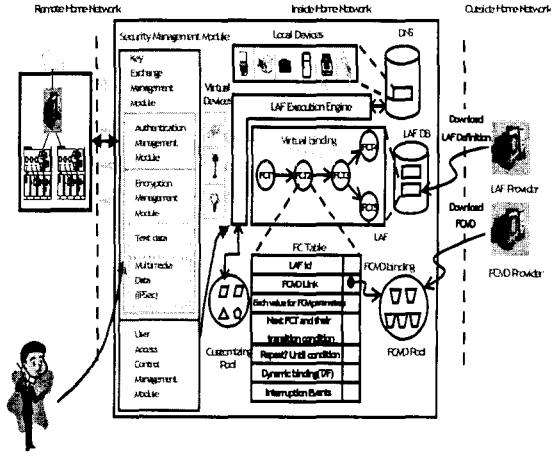

그림 3. 홈네트워크와 보안관리모듈

그림 3은 홈네트워크 환경에서의 보안 관리 모듈의 구조를 나타낸다. 보안 관리 모듈 중 키 교환 관리 모듈은 인증 관리 모듈과 암호화 관리 모듈로 구성하였다. 키 교환 관리 모듈을 위해 데이터 종류에 따라 다른 모드로 수행되는 멀티 모드를 지원하는 제안한 키 교환 프로토콜을 사용한다. 인증 관리 모듈은 홈네트워크를 사용하고자 하는 사용자와 원격 홈네트워크의 홈서버를 인증하기 위한 기능을 제공한다. 또한 암호화 관리 모듈은 서로 다른 홈네트워크 사이에 전송되는 데이터의 종류가 텍스트 데이터인 경우에는 제안한 프로토콜을 수행함으로써 이루어진다. LAFA와 멀티미디어 데이터를 전송할 경우에 홈서버를 인증하는 과정은 제안한 프로토콜의 인증 단계를 수행함으로써 이루어지도록 하고, 전송시간이 오래 걸리기 때문에 세션키를 갱신할 필요성이 있으므로 데이터를

암호화하여 전송하는 과정은 IPSec을 사용하도록 설계하였다. 이러한 모듈들을 지원하기 위해 제안된 키 교환 프로토콜은 다음 절에 기술한다.

4.2 키 교환 프로토콜 설계

본 시스템을 위한 프로토콜을 설계함에 있어서 다음과 같은 사항들은 가정하였다. 첫째, 텍스트 데이터 전송 중에는 세션키를 갱신하지 않는다. 텍스트 데이터들은 사용자의 작업지시나 홈네트워크 간의 정보갱신을 위한 자료들이므로 세션 시간이 짧기 때문이다. 둘째, 이동에이전트나 멀티미디어 데이터 전송 중에는 세션 진행 도중에 세션키를 갱신할 수 있다. 이동에이전트나 멀티미디어 데이터는 비교적 그 크기가 크고 세션 시간도 길기 때문이다.. 셋째, 사용자의 휴대형 단말기에서는 IPSec을 직접지원하지는 않는다. 넷째, 사용자가 디폴트 홈 네트워크에 작업을 지시하기 위해서는 디폴트 홈 네트워크에 본인의 계정(ID)을 가지고 있어야 한다. 다섯째, 사용자 확인은 전자인증서(Digital Certificate:DC)에 포함된 ID를 이용한다. 여섯째, 홈네트워크 간의 상호인증은 홈네트워크들의 대표 ID를 인증서버(Certificate Authority:CA)에 등록한 것으로 보고 인증서버에 등록된 ID를 이용한다. 이와 같은 가정 하에 설계한 키 관리 프로토콜의 특징은 다음과 같다. 첫째, 상호간 인증을 위하여 X.509 전자 인증서를 상호 교환하다. 먼저 Initiator A가 자신의 인증서를 해쉬한 메시지 다이제스트에 서명을 하고 B에게 인증서를 보내면, B는 첨부한 인증서에서 A의 공개키를 얻어서 A임을 확인 하고 A와 동일한 방법으로 B의 인증서를 A에게 보내면 A는 B와 동일한 방법으로 B임을 확인한다. 둘째, 이동에이전트나 대량의 데이터 전송시의 데이터의 비밀성, 무결성 서비스는 IPSec에 위임할 수 있으나 IPSec에서는 사용자 인증 서비스는 제공하지 않으므로 IPSec 상위에서 동작하는 사용자 인증 서비스만을 제공하는 프로토콜이 필요하다. 또한 소량의 데이터 전송을 위하여 데이터의 비밀성, 무결성, 그리고 사용자 인증 모두를 제공하는 프로토콜이 필요하다. 이를 위해 설계한 프로토콜은 USER_AUTH와 KEY_EXCH 두 가지 모드를 지원한다. 본 시스템에서 사용하고자 하는 프로토콜은 키 생성의 안정성과 효율성을 선택의 중요한 요인으로 보고 키 교환 알고리즘이 네트워크 계층에서 수행되는 프로토콜만을 고려하였다. 먼저 IKE는 다량의 멀티미디어 데이터 전송에는 적합하지만 초기 SA설정 오버헤드로 소량의 텍스트를 전송하기엔 부적합 하다. SKEME는 다중 모드를 지원하지만 그 기능이 IKE의 기능에 모두 포함되어 있고 이 역시 세션키 재생성의 효율성을 고려하여 설계하였으므로 최초의 세션키를 생성하기 위한 오버헤드가 상당히 크다. SSL/TSL은 두개의 계층으로 구성되며 사용자 인증 및 키 교환은 응용계층에서 수행되므로 본 시스템의 프로토콜로서는 적합하지 않다. SKIP은 본 시스템에서 반드시 필요로 하는 보안기능인 PFS를 기본 기능으로 제공하지 않는다. 본 시스템에서는 안전한 데이터 전송을 위하여 IPSec을 활용한다. 그러나 IPSec은 데이터 인증과 기밀성 등의 서비스는 제공하지만 단대단 사용자 인증 서비스는 제공하지 않으며, 소량의 텍스트를 전송하기엔 오버헤드가 너무 크다. 그러므로 단대단 사용자 인증과 소량의 텍스트 데이터를 안전하게 전송하기 위하여 새로운 키 교환 프로토콜을 설계한다. 새로이 개발되는 프로토콜은 IPSec의 보완(complement)용으로 사용된다. 다음은 개발된 프로토콜의 논리적인 수행 4단계와 데이터의 종류에 따라 동작하는 다중모드에 대한 설명이다.

1)키 교환 프로토콜의 수행 4 단계

본 키 교환 프로토콜의 수행 절차는 크게 그림 4 같이 4단계로 구분할 수 있다. 제 1단계는 쌍방간에 암호화 파라미터를 협의하는 과정이다. Initiator A은 A가 처리 가능한 여러 가지 파라미터 옵션들을 Hello 메시지에 담아서 보내면, Responder B는 A는 보낸 여러 가지 파라미터 옵션들중에서 B가 처리 가능한 옵션 하나를 선택하여 Hello 메시지에 담아 A에게 보내다. 제 2단계에서는 사용자를 인증한다. A의 전자인증서 Ca에 사전에 협의한 Hash 함수를 사용하여 Message Digest(MD)를 만들고, MD에 A의 개인키 Ra로 암호화(서명)하여, A의 전자인증서 Ca와 함께 B의 공개키 EUb로 암호화한 후 B에게 보낸다. B는 A로부터 받은 메시지의 Ca에서 A를 인증하고 A와 동일한 방법으로 메시지를 만들어 DH(Diffie-Hellman)공개 값 Pb와 함께 B에게 보내다. 제 2단계 일부와 제 3단계는 DH 알고리즘에 의한 세션키 생성을 위한 DH의 공개 값 교환과 키 생성이다. A는 DH 알고리즘을 사용하여 세션 키 SK를 생성하고 랜덤 수 RN을 생성하여 세션 키 SK를 사용하여 RN을 암호화하여 A의 DH 공개 값 Pa 와 함께 B에게 보내다. B는 DH 알고리즘을 사용하여 세션 키 SK를 생성하고 A로부터 받은 메시지를 B의 세션키를 사용하여 복호화한 메시지에 포함된 RN+1을 A에게 보낸다. 제 4단계부터는 실제로 전송할 데이터를 암호화하고 전송하는 단계이다. A는 사전에 협의한 해쉬 함수를 사용하여 전송할 메시지 M의 MD H(M)를 만들고, H(M)과 M을 세션 키 SK로 암호화하여 B

에게 전송한다.

1단계 : Parameter negotiation
A → B: Hello
B → A: Hello
2단계 : User authentication
A → B: $E_{Ub}(C_a, E_{Ra}(H(C_a)))$
B → A: $E_{Ua}(C_b, E_{Rb}(H(C_b))), P_b$
3단계 : Session Key generation
A → B: Esk(RN), Pa
B → A: Esk(RN+1)
4단계 : Message Encryption and Sending
A → B: Esk(M, H(M))

그림 4. 키 교환 프로토콜

2) 키 교환 프로토콜의 두 가지 모드

본 프로토콜은 USER_AUTH 모드와 KEY_EXCH 모드등 두 가지 모드로 수행시킬 수 있다. USER_AUTH 모드는 사용자의 인증만이 필요한 경우에 사용되는 모드이며, KEY_EXCH 모드 사용자의 인증은 물론 세션키를 생성하여야 하는 경우에 사용하는 모드이다.

USER_AUTH 모드

AUTH 모드는 두 사용자간 사용자 인증 서비스만을 필요로 하는 경우에 사용하는 모드이다. 이 경우는 프로토콜의 1단계와 2단계가 수행되는데 2단계의 두 번째 메시지에서 B의 DH 공개 값 Pb는 Null 값으로 채워서 보낸다. 본 프로토콜의 USER_AUTH 모드 수행이 끝난 후 데이터를 안전하게 전송하기 위해서 IPSec 제어 모듈이 IPSec을 호출한다.

KEY_EXCH mode

EXCH 모드는 두 시스템 간 사용자 인증 서비스뿐만 아니라 데이터의 비밀성, 무결성 서비스를 제공한다. 즉 이 모두는 인증을 거친 사용자 데이터를 암호화할 세션키를 생성하고 전송할 데이터를 암호화하고 전송하는데 사용하는 모드이다. 이 모드에서는 프로토콜의 1단계에서부터 4단계까지 모두 수행이 된다.

V. 결 론

본 논문에서는 사람의 편이성에 중심을 둔 사용자 중심의 홈네트워크를 편재형 컴퓨터라 정의하고 이를 위해 이동 에이전트 개념을 도입하였다. 이에 따라 사용자가 직접 장치를 제어하고 설정해야 하는 번거로움을 제거하였다. 이러한 편재형 홈 네트워크 환경은 사용자에게 편리함을 주는 반면 다양한 보안 문제를 야기 시킬 수 있다. 이러한 보안 문제를 해결하기 위하여 보안 관리 모듈을 설계하였으며, 키 관리 모듈과 접근제어 관리 모듈로 구성하였다. 이를 위해 본 논문에서 제안한 키 관리 프로토콜은 키 관리 모듈에서 수행되며 세션 타임이 짧은 텍스트 데이터에 사용된다. 멀티미디어 데이터나 LAFA의 이동에 사용되는 IKE의 두 단계 SA(security Association)설정을 데이타 전송 중에 세션키를 갱신할 필요가 없는 텍스트 데이터의 전송에 사용하기에는 오버헤드가 너무 크다. 제안한 키 관리 프로토콜의 또 다른 용도는 사용자 인증이다. 사용자는 사람 또는 홈 서버다. IPSec은 데이터 인증 서비스는 제공하지만 단대단(end-to-end) 사용자 인증 서비스는 제공하지 않는다. 본 프로토콜은 IPSec이 제공하지 못하는 단대단 사용자 인증 서비스를 제공한다. 즉, 프로토콜은 데이터를 안전하고 효율적으로 전송하고 사용자를 인증하기 위한 IPSec의 보완(complement)용으로 개발되었다. 그러므로 본 프로토콜이 IPSec을 완전히 대체할 수 있도록 모든 종류의 안전한 데이터 전송에 사용되기 위해서는 PFS의 완화, 더욱 다양한 다중모드 지원, 효율적인 세션키 재생성, 다양한 공격으로부터의 보호 등의 방안을 더욱 연구하고 네트워크 계층의 다른 키 교환 프로토콜과의 성능 비교 평가가 이루어져야 한다.

참고문헌

[1] R. Gupta, S. Talwar, and D. Agrawal, "Jini home networking: a step toward pervasive computing," IEEE Computer, Vol. 35, Issue 8, pp. 34-40, Aug. 2002.

[2] R. Lea, S. Gibbs, A. Dara-Abrams, and E. Eytchison, "Networking home entertainment devices with HAVi," IEEE Computer, Vol. 33, Issue 7, pp. 35-43, Sep. 2000.

[3] B. Miller, T. Nixon, C. Tai, and M. Wood, "Home networking with Universal Plug and Play," IEEE Communications magazine, Vol. 39, Issue 12, pp. 104-109, Dec. 2001.

[4] J. Yoo, D. Lee, "Pervasive Home Network for User Centered environment," Technical Report of KJIST, KJIST-DIC-TR-2002-001, 2002.

[5] L. Kagal, T. Finin, and A. Joshi, "Trust-based security in pervasive computing environments," IEEE Computer, Vol. 34 Issue 12, pp. 154-157, Dec. 2001.
[6] F. Stajano and R. Anderson, "The Resurrecting Duckling: security issues for ubiquitous computing," IEEE Computer, Vol. 35 Issue 4, pp. 122-126, Apr. 2002.
[7] S. Ungar, "Home network security," In Proc. IEEE 4th Int. Workshop on Networked Appliances, pp. 41-48, 2002.
[8] D. Harkins, D. Carrel, "The Internet Key Exchange," RFC 2409, Nov. 1998.
[9] H. X. Mel, D. Baker, Cryptography Decrypted, Addison-Wesley, 2001.
[10] C. R. Davis, IPSec: Securing VPNs, McGraw-Hill, 2001.
[11] H. Krawczyk, "SKEME: a versatile secure key exchange mechanism for Internet," IEEE Proc. of the Symposium on Network and Distributed System Security, 1996.
[12] W. Stallings, Cryptography and Network Security, 2nd Edition, Prentice-Hall, 1999.
[13] G. Caronni, H. Lubich, A. Aziz, T. markson, R. Skrenta, "SKIP-Securing the Internet," Proc. of the Fifth Workshop on Enabling Technologies, (WET ICE '96), IEEE Computer Society Press, 1996.
[14] B. Schneier, Applied Cryptography Decrypted, Wiley, 1996.
[15] A. Aziz, T. markson, H. Prafullchandra, "Simple Key-management for Internet Protocols," http://www.skip-vpn.org/spec/SKIP.html, Apr. 1997.

저자소개

정민아(Min-A Jeong)

1992년 전남대학교 전산통계학과(학사)
1994년 전남대학교 대학원 전산통계학과(이학석사)
2002년 전남대학교 대학원 전산통계학과(이학박사)
2002년 ~ 2003년 광주과학기술원 정보통신학과 Post-Doc.
2003년 ~ 현 재 전남대학교 전자통신기술연구소 Post-Doc.
※관심분야 : 정보보호, 데이터마이닝, 생물정보학, 데이터베이스,