안전한 메시지 전송을 위한 Secure Messenger System 설계 및 구현

최상수*, 황성하*, 최용준*, 고정호*, 김소연**, 이강수*
(*)한남대학교 컴퓨터공학과
(**)충주대학교 BK21사업단

A Design and Implementation of Secure Messenger System for Secure message transmission

Sang-Su Choi*, Sung-Ha Hwang*, Yong-Joon Choi*, Jeong-Ho Ko*, So-Yeon Kim**, Gang-Soo Lee*
(*)Department of Computer Engineering, Hannam University
(**)BK21 , Chungju National University
E-mail : {gcss09, hsh0408, yong8e, jhko, sykim, gslee}@se.hannam.ac.kr

요 약

최근 인터넷을 기반으로 하는 정보통신 인프라의 발달에 따라 다양한 서비스가 등장하였으며 이들 서비스들을 통합하여 제공하는 인스턴트 메시징 서비스가 등장하여 그 수요가 급증하고 있다. 그러나, 기존의 인스턴트 메시징 서비스들은 전송되는 메시지에 대하여 어떠한 보안장치도 제공되지 않아서 제 3자에 의한 개인정보 유출 및 악용이 문제점으로 부각되고 있다. 따라서 본 논문에서는 기존의 인스턴트 메시징 구조에 사용자 인증 기능 및 암호화 기능을 조합하여 안전한 메시지 전송을 위한 SMS(Secure Messenger System)를 설계하고 개발하였다.

1. 서론

최근 인터넷을 기반으로 하는 정보통신 인프라의 발달에 따라 다양한 서비스가 등장하였고 그 응용분야 또한 광범위하다. 특히, 전자우편 서비스는 기존 우편 서비스를 대체할 수 있을 정도로 강력한 기능 및 편리성과 신속성으로 대중화에 성공하여 많은 사용자들을 확보한 실정이다. 이러한 상황에서, 몇 년 전부터 제공되기 시작한 인스턴트 메시징(Instant Messaging) 서비스는 전자우편, 파일전송 및 채팅 등의 기존 서비스를 통합하고 부가적으로 다양한 최신 서비스들까지 제공하는 새로운 형태의 서비스를 제공하고 있어 그 이용자가 계속 증가하고 있는 실정이다.

인스턴트 메시징 프로그램(메신저)은 TCP/IP 프로토콜을 이용하여 인터넷이 연결된 곳이라면 언제 어디서나 실시간으로 메시지들 주고받을 수 있는 프로그램[1~6]을 의미하며 신속성, 정확성 및 편리성과 실시간성 등의 특징을 갖는다. 전자우편은 사용자가 직접 서버에 접속해 새로운 내용을 확인해야 하는 반면 메신저는 전화와 같이 실시간으로 메시지나 파일 등을 전달할 수 있다. 메신저가 가진 이러한 특징들은 개별적인 인터넷 서비스 이용에 불편함을 느끼고 있던 기존 이용자들에게 큰 매력으로 작용하여 최근 다수의 메신저 서비스가 등장하여 보편적으로 사용되기 시작하였다.

그러나, 기존의 메신저 프로그램의 종류는 매우 다양하며 그 우열을 가리기가 매우 힘들기 때문에 사용자는 한가지 이상의 메신저 프로그램을 동시에 사용해야 하는 상황이며, 이것은 심각한 자원 낭비가 아닐 수 없다. 결국 각종 메신저 프로그램을 통합할 수 있는 새로운 메시징 프로그램이 나오거나 인스턴트 메시징의 표준화가 이루어지는 것이 무엇보다 시급한 일이라 할 수 있을 것이다. 이를 위하여 인스턴트 메시징 서비스를 오픈 소스화 하려는 노력과, 주요 업체들의 지원을 받아 인스턴트 메시징 서비스의 프로토콜을 표준화하려는 작업이 IETF에서 진행중에 있다[2~6].

또한, 현재 제공되고 있는 대부분의 메신저 프로그램은 전송되는 정보가 아무런 보호장치 없이 네트워크를 통해 전송되기 때문에, 다양한 보안 문제점을 가지고 있다. 이것은 전송되는 메시지가 제 3자에게 노출되어 개인 정보가 유출될 수 있다는 것을 의미한다. 따라서 전송되는 메시지를 안전하게 전달할 수 있는 안전한 인스턴트 메시징 프로그램의 개발이 필요하다.

이런 배경에서, 본 논문에서는 네트워크를 통해 전송되는 정보(인스턴트 메시지, 전자우편, 파일 등)의 암호화를 지원하여 안전하게 정보를 전달할 수 있는 안전한 인스턴트 메시징 프로그램을 설계하고 개발한다. 본 시스템은 사용자 등록시 인증서를 발급하여 사용자의 인증을 수행하며 서버와의 통신시 암호를 기본으로 하고 사용자간의 통신시 선택적으로 암호를 지원한다.

본 논문의 2장에서는 인스턴트 메시징에 대한 기본 개념과 진행중인 표준화 작업 및 시장동향을 조사하고 기존 메신저들의 보안 문제점들에 대하여 설명하며, 3장에서는 안전한 메시지 전송을 위한 일반적인 보안 요구사항들과 이를 충족시키기 위한 인스턴트 메신저의 설계에 대하여 설명하고, 4장에서는 3장에서 설계한 내용을 바탕으로 SMS(Secure Messenger System) 개발에 대하여 기술하며, 끝으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 개요

인스턴트 메시징 프로그램(메신저)이란 TCP/IP 프로토콜을 이용하여 인터넷이 연결된 곳이라면 언제 어디서나 실시간으로 메시지를 주고받을 수 있는 프로그램을 의미한다[1~6]. 메신저의 주요 기능은 텍스트 메시지를 신속하게 실시간으로 상대방에게 전달하는 것이지만, 1:1 혹은 1:N 간의 다자간 채팅 및 파일 송수신 서비스도 제공할 수 있으며 인터넷폰과 같은 실시간 음성전달이나 화상 데이터 전송 기능 등 다양한 기능들을 포함한 새로운 메신저들이 등장하고 있는 실정이다.

표 1. 두 가지 형태의 메신저 비교

	서버 종속형	서버 독립형
특 징	· 대규모 네트워크에 적합 · 중앙에 서버 존재 · 서버에 의한 작업 통제	· 소규모 네트워크에 적합 · 서버가 필요없음 · 동종 프로그램이 실행되고 네트워크 자원 사용이 가능하다면 기능 수행 가능 · 다양한 프로토콜 이용 가능
장 점	· 안정적 · 효과적인 메시지 작업 가능 · 서버와의 상호작용으로 다양한 서비스 및 기능 제공 · 작은 광고 탑재로 광고효과 · 지역적 제한 없음	· 소규모 단체(학교, 병원, 벤처) 내부에서 신속하고 간단한 메시지 전송
단 점	· 시스템 관리 및 유지보수 난이 · 네트워크 단절로 인한 전체 기능 이용 불가	· 다양한 서비스 제공의 한계 · 지역적 제한
종 류	· 대부분의 메신저	· Win95/98의 WinPopup

메신저는, 기존 인터넷 서비스가 클라이언트와 서버 사이의 통신이라는 것과는 달리 클라이언트와 클라이언트 사이의 통신에서도 아주 중요한 역할을 한다. 특히 클라이언트 사이의 통신으로 서버의 부하를 경감시킬 수 있다는 장점을 가지고 있다.

메신저는 구현 형태에 따라 크게 두 가지로 구분[1]할 수 있는데, 첫 번째 형태는 서버 종속형(Server dependent) 메신저로서 중앙에 서버가 존재하고 이 서버에 로그온해 사용자 검색, 사용자 상태 및 메시지 교환 등의 작업을 서버가 통제하는 형태이다. 두 번째 형태는 서버 독립형(Server independent) 메신저로서 서버가 필요 없으며 서버와의 통신이 고려 대상이 아니며 동종 프로그램이 실행되고 네트워크 자원 사용이 가능하다면 메신저 기능을 수행할 수 있는 형태이다. 두 가지 형태의 메신저를 비교해 보면 <표 1>과 같다.

2.2 관련 표준화 작업

현재 IETF에서는 "인스턴트 메시징 및 프리전스 프로토콜(IMPP : Instant Messaging and Presence Protocol)"과 관련한 표준화 작업을 진행중에 있다[2~6]. 현재 진행중인 표준화 작업으로는 2개의 RFC 문서[2,3]와 3개의 Draft 문서[4,5,6]가 존재하는데 각각의 표준화 관련 문서들을 정리해 보면 다음과 같다.

"A Model for Presence and Instant Messaging" (RFC 2778)은, 프리전스(presence) 및 인스턴트 메시징 시스템을 위한 추상 모델에 대하여 정의하고 있다. 이 문서에서는 복잡하고 다양한 엔티티 및 용어들을 정의하고 시스템에서 제공되는 서비스에 대하여 아웃라인을 잡고 있다. 또한 프리전스 및 인스턴트 메시징을 위한 프로토콜과 마크업에 대한 향후 작업들을 위하여 공통의 용어들을 정의하는 것을 그 목적으로 하고 있다[2].

"Instant Messaging/Presence Protocol Requirements" (RFC 2779)는, IMPP의 목적(표준 프로토콜을 정의하여 독립적으로 개발된 인스턴트 메시징 그리고/또는 프리전스 어플리케이션이 인터넷 상에서 상호작용할 수 있도록 한다)을 충족시키기 위한 최소한의 요구사항들에 대하여 정의하고 있다[3].

"Common Presence and Instant Messaging Message Format "은, CPIM(Common Profile for Instant Messaging) 명세를 따르는 프로토콜을 위한 메시지 형식과 'message/cpim' mime 유형의 정의에 대하여 기술하고 있다[4].

"Date and Time on the Internet: Timestamps"는, 그레고리오력(Gregorian calendar : 현행 태양력)을 사용하는 날짜 및 시간을 표현하기 위한 ISO 8601 표준의 프로파일로써 인터넷 프로토콜에서 사용하기 위한 날짜 및 시간 형식에 대하여 정의하고 있다[5].

"CPIM Presence Information Data Format"은, IMPP 워킹그룹 내에서의 토의를 위하여 프리전스 형식 명세를 제안하고 있으며 지금까지 토의를 가속시켜온 IMPP 메일링 리스트로부터 제안된 문제들에 대한 목록을 포함하고 있다[6].

2.3 메신저의 기본 구조

현재 진행중인 표준화 작업들[2~6]과 서비스중인 메신저 서비스들[7~12]을 살펴보면 공통적으로 <그림 1>과 같은 기본구조를 가지고 있으며, 공통적인 구성요소들을 살펴보면 다음과 같다[1].

- 사용자 : 메신저 사용자
- 클라이언트 프로그램 : 사용자의 메신저 관련 작업을 다른 클라이언트나 서버에 송수신하거나 관련 정보를 저장하는 프로그램
- 접속 서버 : 클라이언트와 접속하여 로드밸런싱에 의해 서비스할 서버에 분산해 주는 서버
- 프리전스 서비스 서버 : 사용자의 프리전스 상태(온라인, 오프라인, 기타 상태)를 관리하고 전달하는 서버
- 인스턴트 메시징 서버 : 인스턴트 메시징를 서비스해주는 서버
- 사용자 데이터베이스 서버 : 등록된 사용자 관련 데이터가 저장되는 데이터베이스 서버
- 기타 서비스 서버 : 웹서버, 메일 서버 등의 메신저 서비스의 기능을 강화시켜주는 기타 서비스를 제공하는 서버

2.4 시장동향

최근 인스턴트 메시징 서비스에 대한 관심의 증가로 외국에서는

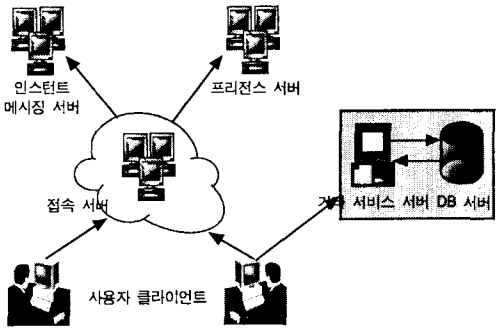

그림 1. 기존 메신저 시스템의 구조 및 구성요소

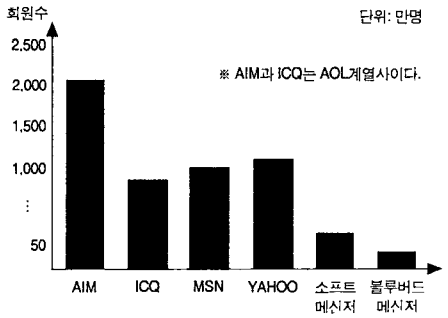

그림 2. 국내·외 메신저 서비스 업체의 회원수 비교(2000. 8)

ICQ[7]를 선두로 다양한 메신저 서비스가 제공되고 있다. 특히 전 세계적으로 가장 많은 사용자를 확보한 메신저 서비스 회사인 AOL의 AIM[8] 및 ICQ와 뒤늦게 메신저 시장에 뛰어든 마이크로소프트의 MSN 메신저[9] 사이의 선두다툼이 치열한 가운데 YAHOO[10] 소프트메신저[11], 블루버드 메신저[12] 등의 다수의 국내·외 업체들이 자사만의 독특한 특징을 내세워 꾸준히 사용자를 늘려나가고 있는 실정이다. 국내외 메신저 서비스 업체들의 회원수를 비교한 결과는 <그림 2>와 같다.

2.5 보안 문제점

기존의 메신저 서비스들은 전송되는 정보가 아무런 보호장치 없이 네트워크를 통해 전송되어 제3자가 이를 도청하거나 전송 메시지가 노출될 수 있으므로 개인정보 유출에 대한 보안 문제점들이 제기되고 있다.

2001년 6월, 세계에서 가장 많은 사용자를 확보한 ICQ가 해킹을 당한데 이어 MSN도 그 원인이 해킹으로 추정되는 보안사고가 발생하였다. 이는 기존의 메신저 시스템들이 얼마나 해킹에 취약한지를 보여주는 단적인 예라 할 수 있을 것이다. 또한, 국내에서도 종종 메신저 사용 중에 해킹에 의하여 클라이언트 시스템이 다운되는 현상이 발생하였다는 보고를 접할 수 있다.

기존 메신저 서비스에서는 기본적으로 블랙리스트 기능, 메시지 거부 기능 및 스팸 메시지 방지 기능 등을 제공하지만 악의를 가진 해커에 의한 메시지 스니핑 등에 대해서는 속수무책일 수밖에 없다. 그러나, 국외에서는 메신저에 대한 보안기능 강화에 대한 연구는 거의 전무한 실정이며, 국내에서도 시작단계에 불과하다[13].

따라서, 본 논문에서는 전송되는 정보의 암호화 및 사용자 인증을 지원하여 안전하게 정보를 전달할 수 있도록 하는 안전한 메신저를 설계하고 개발하였다.

3. Secure Messenger 설계

본 논문에서는, 2.5절에서 설명한 기존 메신저의 보안문제들을 해결하기 위하여 정보보호의 기본 목표인 비밀성, 무결성 및 가용성을 만족시킬 수 있도록 설계 및 구현되었다.

본 장에서는 정보보호의 기본 목표와 RFC 2779에 명시된 보안 요구사항들을 만족시키는 안전한 메신저를 설계한다.

3.1 안전한 메시지 전송을 위한 보안 요구사항

정보보호를 위한 기본 목표와 이를 충족시키기 위하여 SMS(Secure Messenger System)에서 설계한 내용들은 다음과 같다.

(1) 인증(Authentication)

인증이란 참여하는 각 개체는 서로간에 높은 신뢰도를 가져야 한다는 원칙이며, SMS 메신저에서는 이를 만족시키기 위하여 사용자 인증을 지원한다.

(2) 무결성(Integrity)

무결성이란 허락되지 않는 제 3자에 의해 변경되어서는 안된다는 원칙이며, SMS 메신저에서는 이를 만족시키기 위하여 전송되는 메시지에 대한 서명을 지원한다.

(3) 비밀성(Confidentiality)

비밀성이란 교환되는 각 정보는 제 3의 개체에 알려져서는 안된다는 원칙이며, SMS에서는 이를 만족시키기 위하여 전송되는 메시지에 대한 암호화를 지원한다.

(4) 부인방지(Non-Repudiation)

부인방지란 각 개체는 송수신한 정보를 부인할 수 없어야 한다는 원칙이며, SMS에서는 이를 만족시키기 위하여 인스턴트 메시지와 파일 전송에 서명을 지원하여 송신 부인방지 기능을 제공한다.

3.2 SMS 메신저의 시스템 구조

본 논문에서 제안하는 SMS 메신저는 다음과 같은 네 가지 구성요소로 구성되어 있다.

- 메신저 클라이언트 : 서버와의 통신과 사용자 사이의 메시지 전송을 담당하며 메일 서버와의 통신 및 사용자들의 프리젠스 상태를 모니터링하는 기능을 담당
- 메신저 서버 : 사용자 정보 및 공개키 인증서를 발급 및 배포하고 관리하는 기능을 담당
- 회원정보 및 이력 DB : 사용자의 등록 정보 및 이력을 보관하며 부재중인 사용자의 메시지를 보관하고 전달하는 기능을 담당
- 메일 서버 : 사용자간의 암호메일을 송수신하는 역할을 담당

이상의 네 가지 구성요소들로 이루어진 개략적인 시스템 구조도는 <그림 3>과 같다.

3.3 SMS 메신저의 사용절차 시나리오

SMS 메신저 이용하여 사용자간에 안전하게 메시지를 전송하는 시나리오는 다음과 같은 절차를 따른다.

① 메신저 클라이언트가 공개키 쌍을 생성한 후 메신저 서버에게 신규 등록을 요청한다.

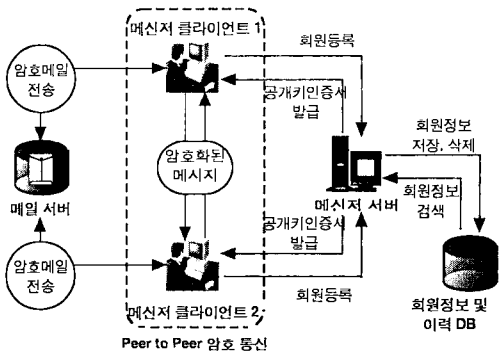

그림 3. SMS의 시스템 구조

표 2. SMS 메신저의 제공 기능

구 분	클라이언트	서버
회원등록 기능	- 키 쌍 생성 - 공개키 인증서 발급 요청 - 회원가입요청	- 회원등록 및 회원정보 관리 - 공개키 인증서 발급 및 관리 - 감사로그 생성
로그인 기능	- 로그인	- ID와 패스워드 검사 - 멤버의 프리젠스 상태 검색 - 저장된 메일 검색 - 감사로그 생성
그룹멤버관리 기능	- 그룹멤버관리 (검색,등록,삭제) 기능 - 공개키 인증서 저장	- 사용자 검색 - 공개키 인증서 배포
대화 기능	- 세션키 생성 - 메시지 암/복호화 - 메시지 송수신	X
메일전송 기능	- 세션키 생성 - 메일 암/복호화 - 메일 송수신	- 메일정보 관리
인스턴트 메시징 기능 (쪽지)	- 세션키 생성 - 메시지 암/복호화 - 쪽지 송수신	X
파일전송 기능	- 세션키 생성 - 파일 암/복호화 - 파일 송수신	X
공개키 인증서 관리 기능	- 그룹멤버의 공개키 인증서 관리	- 사용자 및 서버의 공개키 인증서 관리

② 서버는 사용자 정보를 서버에 저장하고 공개키 인증서를 생성하여 발급하고 DB에 저장한다.

③ 클라이언트 A가 B와의 통신을 위해 B를 서버에서 검색하여 그룹에 등록을 요청한다(B의 허락 요구).

④ B가 A의 그룹 등록 요청을 수락한 후 서버로부터 A의 공개키 인증서 수신한다.

⑤ 서버는 A에게 B의 공개키 인증서를 전송하고 A는 B의 공개키 인증서를 저장한다.

⑥ A가 B의 공개키를 이용하여 B와의 키 분배 후 암호통신 또는 암호파일 전송을 수행한다.

3.4 SMS의 제공 기능

SMS 메신저는 기본적으로 회원등록 기능, 로그인 기능, 그룹멤버관리 기능, 대화 기능, 메일전송 기능, 인스턴트 메시징 기능, 파일전송 기능, 공개키 인증서 관리 기능을 제공한다. 각각의 기능에 대하여 클라이언트와 서버에서 수행하는 작업들은 <표 2>와 같다. 이상과 같은 기본적인 메신저 기능 이외에, 보안 요구사항들을 충족시키기 위하여 SMS 메신저에서 제공하는 보안기능들을 자세히 살펴보면 다음과 같다.

(1) 신규등록 기능

신규등록 기능은 사용자로부터 ID와 패스워드 등의 사용자 정보를 입력받아 신규 사용자 등록 작업을 수행하는 기능으로써, 입력된 ID의 중복 여부를 판단하여 모든 입력이 정확하게 이루어지면 키 쌍을 생성하고 공개키 정보(공개키, 평문, 사용자의 개인키로 평문을 암호화한 암호문)를 서버에 전달하여 검증을 받는다. 이때 서버측에서는 수신된 공개키로 암호문을 복호화하고 평문과 비교하여 공개키를 검증하게 되며, 공개키 검증을 완료하면 수신된 공개키를 이용하여 인증서를 생성하고 클라이언트에 전송하며 클라이언트는 수신된 인증서를 검증하고 개인키와 공개키 인증서를 저장한다. 신규등록 기능을 도식화하면 <그림 4>와 같다.

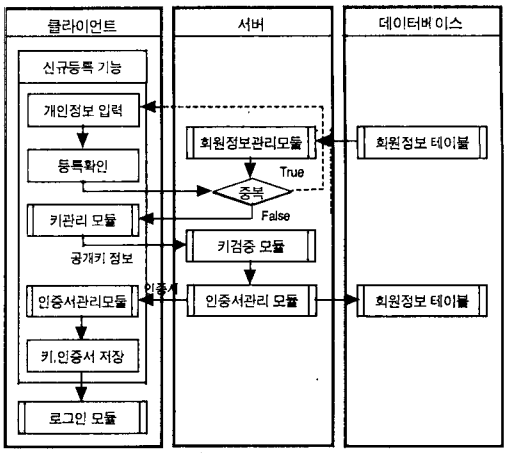

그림 4. 신규등록 기능

(2) 암호화된 대화 기능

암호화된 대화 기능은 온라인 상태에 있는 사용자간의 암호화된 P2P 채팅을 수행하는 기능으로써, 사용자 A가 B에게 채팅을 요청하여 상호간의 메시지 송수신 중에 암호화된 메시지를 전송하는 기능을 수행한다. 이때 제약사항으로는 채팅하는 사용자가 인증서가 배포된 등록된 그룹멤버이어야 한다. 암호화된 대화 기능을 도식화하면 <그림 5>와 같다.

(3) 암호화된 인스턴트 메시징 기능

암호화된 인스턴트 메시징 기능은 온라인 상태에 있는 사용자에게 암호화된 쪽지 보내기를 수행하는 기능으로써, 사용자 A가 문자열의 길이가 제한된 쪽지를 작성하여 메시지를 암호화하고 다시 전자서명을 하여 B에게 전달하는 기능을 수행한다. 이때 제약 사항으로는 쪽지를 송수신하는 사용자가 인증서가 배포된 등록된 그룹멤버이어야 한다.

암호화된 인스턴트 메시징은 사용자의 프리젠스 상태가 오프라인일 경우 서버에 보관되며, 온라인일 경우 사용자에게 직접 전달된다. 암호화된 인스턴트 메시징 기능(직접전달)을 도식화하면 <그림 6>과 같다.

(4) 암호화된 파일전송 기능

암호화된 파일전송 기능은 온라인 상태에 있는 사용자에게 암호화된 파일을 전송하는 기능으로써, 사용자 A가 전송할 파일을 선

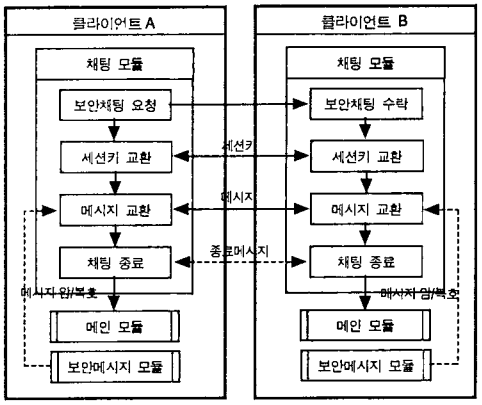

그림 5. 암호화된 대화 기능

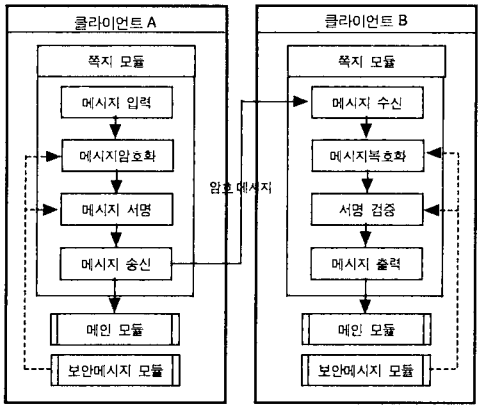

그림 6. 암호화된 인스턴트 메시징 기능

택하면 세션키를 생성하고 파일 및 세션키를 암호화한 후 다시 암호화된 파일에 서명한 후에 B에게 전송하는 기능을 수행한다. 암호화된 파일을 수신한 사용자 B는 세션키 및 파일을 복호화하고 서명을 검증한 후에 파일을 저장한다. 이때 제약사항으로는 암호화된 파일을 송수신하는 사용자가 인증서가 배포된 등록된 그룹멤버이어야 한다. 암호화된 파일전송 기능을 도식화하면 <그림 7>과 같다.

4. SMS 메신저의 구현

4.1 개발환경

본 논문에서 개발한 SMS 메신저 시스템은 Windows 98/2000 환경에서 JDK 1.3을 이용하여 Java로 작성되었으며, 암호알고리즘은 SUN사의 JCE 규격을 따르는 JCSI 패키지[14]를 사용하였다. 또한 데이터베이스는 MySQL 3.23.38을 사용하였으며 개발 도구로는 볼랜드사의 JBuilder 4를 사용하여 개발하였다.

안전한 메시지 전송을 위하여, 안전성이 증명된 기존의 보안 알고리즘들을 사용하였으며 암호 알고리즘으로는 공개키 알고리즘인 RSA와 대칭키 알고리즘인 DES를, 전자서명을 위하여 RSA와 해쉬 알고리즘인 SHA-1을 이용하였다.

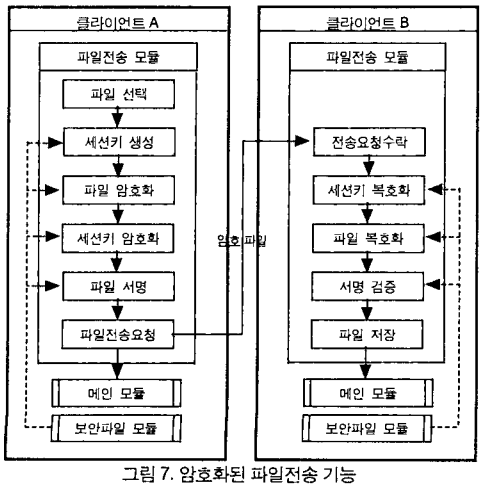

그림 7. 암호화된 파일전송 기능

그림 8. 메신저 클라이언트의 로그인 화면

4.2 개발내용

본 논문에서 설계하고 개발한 SMS 메신저는 크게 메신저 클라이언트와 메신저 서버 프로그램으로 구분할 수 있다. 메신저 클라이언트는 사용자의 컴퓨터에 설치되어 사용자가 메신저 서버에 로그인하고 사용자간의 메시지 전송, 파일 전송 및 인스턴트 메시징 전송 등의 기능을 수행한다. 메신저 서버는 사용자의 프리젠스 상태 및 사용자 정보 관리, 로그인과 인증서 관리를 수행한다.

메신저 클라이언트의 로그인 화면은 <그림 8>과 같다. 로그인 화면에서 신규 사용자는 신규가입을 신청하고 기존 사용자는 ID와 패스워드를 입력하여 서버에 로그인하게 된다. 사용자가 로그인에 성공하면 메신저 클라이언트 메인 화면으로 이동하게 된다.

메신저 클라이언트의 메인 화면은 <그림 9>와 같다. 로그인에 성공한 사용자는 그룹멤버를 설정하거나 그룹멤버에게 채팅, 쪽지 전송 및 파일전송 등의 서비스를 이용할 수 있다.

채팅, 쪽지 및 메일과 파일전송의 일반기능은 기존의 메신저와 유사하며 각 서비스들은 일반/보안으로 구분하여 사용할 수 있다.

보안 채팅 화면은 <그림 10>과 같다. 사용자가 인증서가 배포된 그룹멤버에게 채팅을 요청하고 상호간에 메시지 전송 중에 보안을 요하는 메시지(주민번호, 계좌번호 등) 전송이 필요하면 보안통신 버튼을 클릭하여 <그림 5>의 보안기능을 수행하게 된다. 이때 세션키 교환 및 파일의 암복호는 사용자에게 은닉되어 프로그램 수준에서 자동으로 처리함으로써 사용자 편의성을 제공하였다.

보안 쪽지 화면은 <그림 11>과 같다. 사용자가 그룹멤버에게 쪽

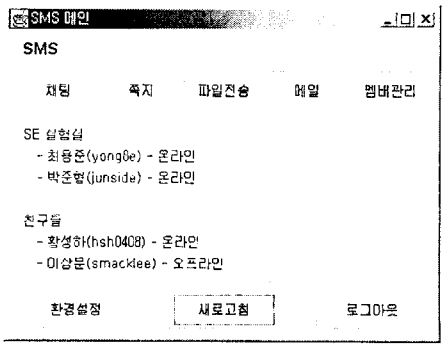

그림 9. 메신저 클라이언트의 메인 화면

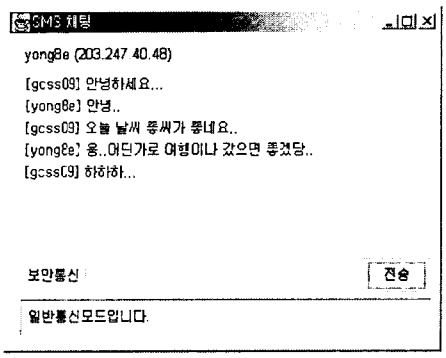

그림 10. 보안 채팅 화면

지전송 버튼을 클릭하고 보안쪽지 기능을 선택하면 <그림 6>의 보안기능을 수행하게 된다. 이때에도 모든 보안관련 작업은 사용자로부터 은닉되어 사용자는 편리하게 보안기능을 수행할 수 있다.

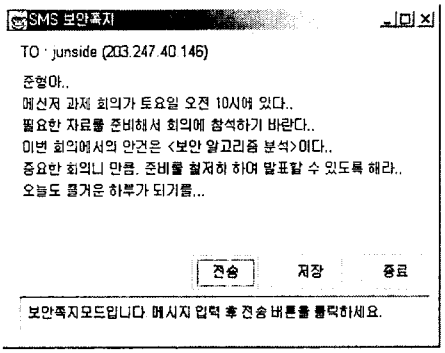

그림 11. 보안 쪽지전송 화면

보안 파일전송 화면은 <그림 12>와 같다. 사용자가 그룹멤버에게 파일전송 버튼을 클릭하고 보안파일 기능을 선택하면 <그림 7>의 보안기능을 수행하게 된다. 이때에도 사용자 편의성을 제공하기 위하여 모든 보안관련 작업들은 사용자로부터 은닉된다.

이와 같이 본 논문에서 구현한 SMS 메신저의 보안 및 일반 기능들을 기존 메신저들과 비교한 결과는 <표 3>과 같다.

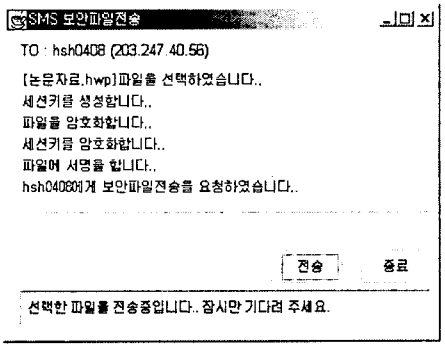

그림 12. 보안 파일전송 화면

표 3. 국내·외 인스턴트 메시징 프로그램의 특징 비교

항목 \ 회사	ICQ	AIM	MSN	YAHOO	소프트 메신저	블루버드 메신저	SMS 메신저
보안기능	×	×	×	×	×	×	○
한글 게시정	◌	○	○	○	○	○	○
등록 방법	고유번호	ID	ID	ID	ID	ID	ID
파일 전송	◌	×	◌	×	◌	◌	○
URL 전송	◌	○	○	×	○	◌	○
한글 채팅	×	○	○	×	○	○	○
음성 채팅	◌	×	◌	×	×	◌	×
즉석 이메일	◌	×	○	×	○	◌	○
인터페이스	쉬운편	쉬운편	쉬운편	쉬운편	쉬운편	쉬운편	쉬운편
특 징	다양한 기능	넷스케이프 홈페이지 버튼과 간편한 사용법	국제전화 기능 강화, 주식정보 확인, 쉬운 연결	자체 야후 e-mail 수신 알림기능,간단한 사용법	파일전송이 빠르고, e-mail 수신 안내기능, 자료실 기능	웹 메신저 기능	사용자 인증 기능 및 암호화기능

5. 결론

본 논문에서는 전송되는 메시지를 암호화하여 안전한 메시지를 전송할 수 있는 안전한 메신저를 설계하고 구현하였다. SMS 메신저는 전송되는 메시지의 암호화와 공개키 인증서를 기반으로 하는 사용자 인증 등의 보안 기능들을 제공함으로써 기존 메신저가 가지고 있는 각종 보안 문제점들을 해결하였다. 따라서 SMS 메신저는 전송되는 메시지의 비밀을 요하는 회사나 국가기관 및 군에서도 안전하게 사용할 수 있다.

본 논문에서 설계하고 구현한 SMS 메신저는 메시지를 전송하기 위하여 암호화 알고리즘과 공개키 인증서를 사용하기 때문에, 생성되는 각종 키 관리에 대한 문제점이 발생될 수 있으므로 이를 해결하기 위하여 사용자가 키를 분실하였을 경우 이를 복구해줄 수 있는 키복구 시스템 개발을 향후 연구과제로 남긴다.

참고문헌

[1] "빠른 세대의 빠른 통신법, 인스턴트 메시징", 마이크로소프트웨어, pp.254-289, 1999년.

[2] RFC 2778("A Model for Presence and Instant Messaging"), *http://www.ietf.org/rfc/rfc2778.txt.*

[3] RFC 2779("Instant Messaging/Presence Protocol Requirements"), *http://www.ietf.org/rfc/rfc2779.txt.*

[4] "Common Presence and Instant Messaging Message Format", *http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-msgfmt-03.txt.*

[5] "Date and Time on the Internet: Timestamps", *http://www.ietf.org/internet-drafts/draft-ietf-impp-datetime-04.txt.*

[6] "CPIM Presence Information Data Format", *http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-00.txt.*

[7] ICQ, *http://web.icq.com/.*

[8] AIM, *http://www.aol.com/aim/homenew.adp.*

[9] MSN 메신저, *http://messenger.msn.com/.*

[10] YAHOO 메신저, *http://messenger.yahoo.com/.*

[11] 소프트 메신저, *http://www.digito.com/.*

[12] 블루버드 메신저, *http://www.bluebirdmessenger.com/.*

[13] 정보고, 이광수, 안전한 인스턴트 메신저의 설계와 구현, 한국정보처리학회 논문지, 8-C권 2호, 2001년 4월.

[14] JCSI-2.0, *http://javatree.web.cern.ch/javatree/share/opt/security/jcsi-2.0/.*