안전한 단문 전송 시스템 설계 및 구현

송기평* · 손홍* · 조인준** · 주영지** · 이달원**

*한국전자통신연구원 표준연구센터, **배재대학교 컴퓨터공학과

The Design and Implementation of Secure Instant Messaging System

Gi-Pyeung Song* · Hong Sohn* · In-June Jo** · Young-ji Ju** · Dal-won Lee**

*ETRI/Protocol Engineering Center, **Graduate School of Paichai University/Department of Computer Engineering

E-mail : gpsong@pec.etri.re.kr, hsohn@pec.etri.re.kr, injune@mail.paichai.ac.kr, going@zamus.com, dunals@chollian.net

요 약

IM(Instant Messenger)은 현재 가장 각광받고 있는 개인 커뮤니케이션 도구이다. 이는 개인에게는 전자우편을 대신할 도구로 기업에게는 사용자 확보의 도구이자 무한한 잠재력을 가진 도구로 평가받고 있다. 하지만, IM은 보안상 여러 문제점을 내포하고 있다. 전송 메시지에 대한 공격에 안전하지 못하다는 점을 비롯하여 여러 취약점들이 보고 되고 있고, 이를 이용한 해킹 도구 들이 개발된 상태이다. 다시 말해, IM을 통해 주고 받는 메시지는 누구든지 엿볼 수 있으며 조작 가능하다는 것이다. 이는 기업의 전략적 도구로의 발전에 큰 걸림돌로 작용하며 개인의 프라이버시에 대한 심각한 문제를 낳을 수 있다.

IETF의 IMPP WG(Working Group)에서는 IM간의 상호 연동을 위한 표준을 준비하고 있으나 가장 많은 IM 사용자를 확보하고 있는 AOL(American On-Line)의 불참으로 관련 표준 제정의 진행이 원만하지 않은 상태이며 전송되는 데이터의 형식에 관한 논의만이 주로 이루어질 뿐 전체적인 보안 서비스에 대한 논의는 미비한 상태이다.

본 논문에서는 이러한 IM의 취약점과 보안상의 문제를 해결하여 안전한 단문 전송 시스템(SIMS : Secure Instant Messaging System)을 설계 및 구현하였다.

ABSTRACT

The Instant Messenger(IM) is the most popular personal communication tool today. IM is a tool that can substitute E-mail for a person, and can secure the user for a company. Further, it is claimed as it has a limitless potential. However, there has been several reports on security issues. It has known that the transmitting message is not secured for the attacks, and hacking tools has been developed. In addition, several reports has been made regards to the vulnerability. In other words, anyone can peep through and manipulate the messages that are sent or received via IM. This is a barrier for the IM to be developed as a corporate's strategic tool, and furthermore, it will create serious personal privacy issue.

IETF IMPP Working Group is preparing a standard mutual relationship between IM. However, it is complicated due to the American On-Lines's absence, whom has ensured the most number of IM users. There was a discussion only about the form of the transmitting data, but it is insufficient state to discuss the security service for general.

In this paper, I design and implement the Secure Instant Messaging System, to solve the IM's vulnerability and the security issue presented above.

Ⅰ. 서 론

국내외 인터넷 사용인구 증가와 함께 개인간 통신 지원 도구 또한 비약적 발전을 거듭하고 있다. 그 중 실시간 메시지 전송을 지원하는 IM은 단기간의 성장에도 불구하고 인터넷 사용인구의 1/3이상이 사용하며, 실시간 개념을 바탕으로 전자우편의 단점을 보완할 도구, 기업간 전략회의 도구 등의 다양한 형태의 서비스로 발전하여 수많은 응용프로그램을 탄생시킬 기반기술로 전망하고 있다.

AOL, YAHOO, Microsoft 등의 대기업뿐만 아니라 사용자를 유치하려는 거의 모든 사이트에서 각 기업에 특화된 형태로 제공되고 있는 IM은 비약적 발전과 함께 여러 문제점이 도출되고 있다. IM 프로그램 사용시 각각의 기업별 전송 정보 형식이 정의되어 호환성이 없는 문제와 더불어 전송 중 메시지 노출 등의 취약한 보안상의 문제를 들 수 있다. 이는 IM이 널리 사용될 수 있는 응용프로그램으로의 발전에 최대 문제점으로 인식되고 있다. 현재 IETF[1]의 IMPP WG[2,3]에서 IM 개발사들의 제안서를 바탕으로 관련 표준화 작업을 진행하고 있으나 가장 많이 사용중인 AIM(AOL Instant Messenger)과 ICQ를 보유한 AOL의 비협조로 아직 적절한 표준안을 마련하지 못하고 있는 실정이다.

본 논문에서는 안전한 단문 전송을 지원하는 SIMS의 설계 및 구현에 연구의 목적이 있다. 대칭키 및 공개키 암호 시스템, 축약기술 등의 암호기술을 기반으로 기존 IM의 문제점인 취약한 보안서비스를 보완하여 안전한 단문 전송을 지원하는 SIMS를 설계하고 구현하였다.

Ⅱ. 안전한 단문전송 시스템 설계

이 장에서는 본 논문에서 제안한 안전한 단문 전송 시스템 SIMS를 상세히 기술한다. 본 논문에서 설계 내용을 기술하기 위해 표 1의 표기법을 사용하였다.

표 1. 표기법 기호설명

기호	설명
E	Encryption
D	Decryption
M	암복호화의 대상
KPP_u	사용자 패스프레이즈를 이용한 키
KS	세션키(한 세션 동안에만 사용)
KU_u	사용자의 공개키
KR_u	사용자의 개인키
KU_u1	수신자의 공개키
KR_u1	수신자의 개인키
H	해쉬, 메시지 축약

안전한 단문 전송 시스템 SIMS는 그림 1과 같은 환경에서 동작한다.

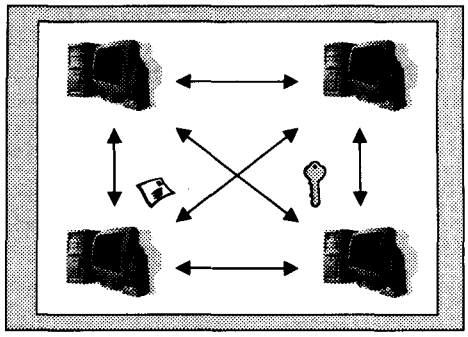

그림 1. SIMS 동작환경

SIMS 설계의 특징은 IM의 기능적 측면 보다는 보안 서비스[4,5,6]에 중점을 두고 설계하였고, 제한된 사용자를 대상으로 별도의 중앙 서버 없이 클라이언트 간의 동작만으로 단문, 키, 상태 정보 등을 송수신한다.

클라이언트의 로컬 시스템에 저장되는 정보는 TripleDES 알고리즘을 이용한 PBE(Password Based Encryption) 암호기술 및 MD5 축약기술을 사용하였고, 송수신 정보에는 RSA, DES 알고리즘을 이용한 암호기술과 MD5 축약기술을 사용하여 여러 보안 서비스를 제공하였다.

2.1 사용자 등록 및 수정

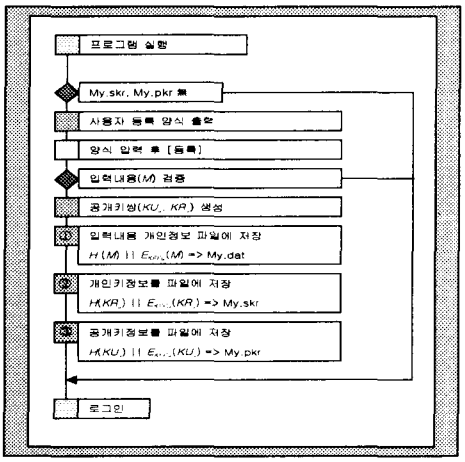

그림 2. 사용자 등록 과정

사용자 개인 정보(M - ID, Name, Email)을 입력받아 처리한다. 사용자 개인 정보의 수정시 사용자 등록에서의 과정과 동일하나 수정입력된 개인 정보를 처리 후 수신자들에게 변경된 정보를 전송하는 차이점이 존재한다.

2.2 로그인

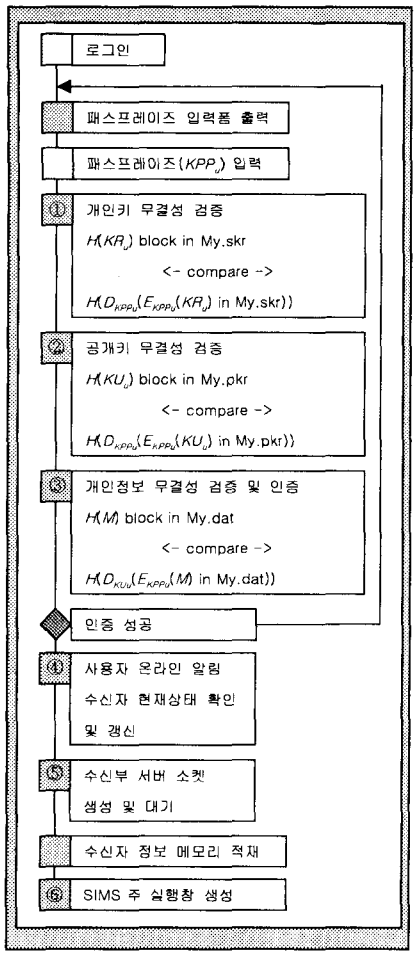

그림 3. 로그인 과정

2.3 수신자 등록 및 삭제

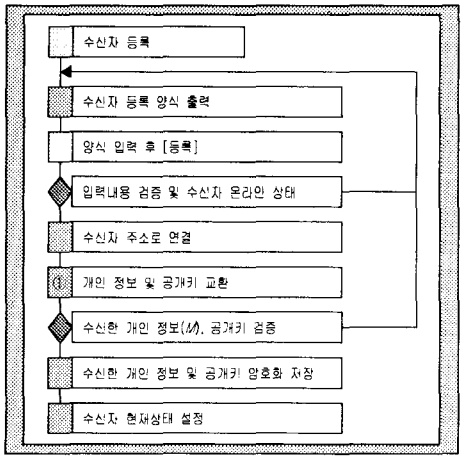

그림 17. 수신자 등록 과정

수신자 개인 정보(M - UIN(고유번호), ID, Name, Email, IP Address, Port Number)을 입력받아 처리한다.

수신자 삭제시에는 삭제될 수신자를 선택 후 수신자 정보(User.dat)를 삭제하고 갱신하며 역시 수신자 공개키 정보(UIN.pkr)을 삭제한다.

2.4 단문전송

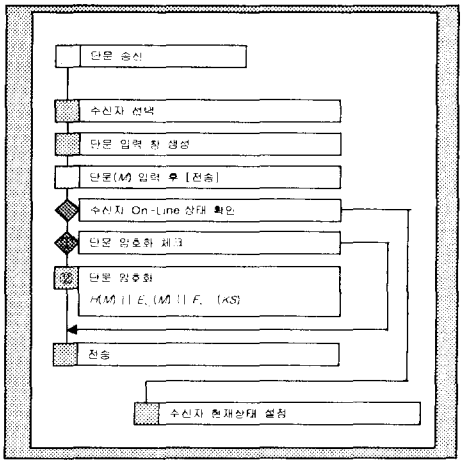

그림 5. 단문전송 과정

2.5 단문수신

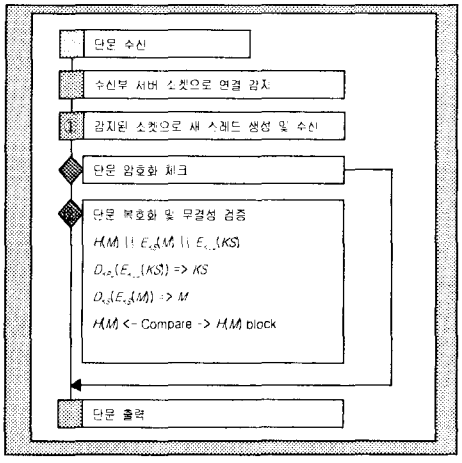

그림 6. 단문수신 과정

III. 안전한 단문전송 시스템 구현

본 논문에서 설계한 안전한 단문 전송 시스템은 운영체제로 Microsoft Windows 2000 Server를 사용하였으며, 구현 언어로 플랫폼 독립적이고

네트워크 관련 지원이 강한 Java[7,8]를 선택, 프로그램 개발키트인 JDK 1.2.2[9,10]와 암호라이브러리인 IAIK JCE(Java Cryptography Extension)[11,12,13]를 사용하여 구현하였다.

안전한 단문 전송 시스템은 그림 7과 같이 9개의 처리기로 구성된다.

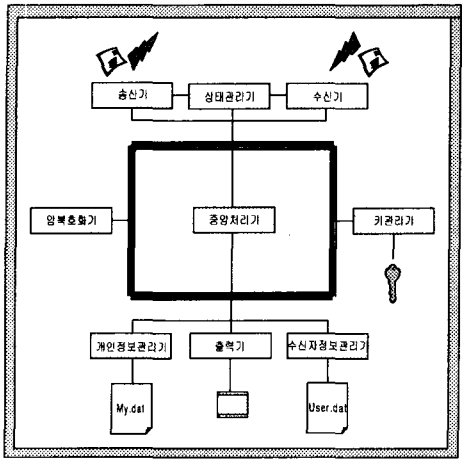

그림 20. SIMS 구성요소

3.1 중앙처리기
① SIMS 시작
② 환경 변수의 정의
③ 각종 화면 구성
각종 정보화면, 로그인/주실행창 구성
④ 수신자 상태 정보 표시
상태관리기 및 수신부와 연계 수신자 상태정보 표시
⑤ 사용자 등록 처리 요청
개인정보관리기에 사용자 등록창 출력 및 등록처리 요청
⑥ 로그인 처리 요청
암복호화기 및 키관리기에 로그인 처리 요청
⑦ 수신부 서버 소켓 생성 요청
수신부에 단문 및 정보 수신을 위한 서버 소켓 생성 요청
⑧ 단문 입력창 출력 요청
송신부에 단문 입력을 위한 입력창 출력 요청
⑨ 단문 수신창 출력 요청
수신한 단문 확인을 위한 수신창 출력 요청

3.2 상태관리기
① 사용자 On Line 및 Off Line 알림
로그인 성공시 중앙처리기의 요청에 의해 수신자들에게 사용자 OnLine 정보 송신 요청
② 사용자 정보 변경 알림
개인정보 변경시 개인정보관리기의 요청에 의해 수신자들에게 변경된 개인 정보 송신 요청

3.3 개인정보관리기
① 개인 정보 등록 및 수정
중앙처리기의 요청에 의해 사용자 등록 화면을 출력하고 중앙처리기, 키관리기, 암복화기와 연계하여 사용자 등록 및 수정에 관한 처리 수행
② 개인 정보 전달
다른 처리기들의 요청에 의해 개인 정보를 다른 처리기에 전달

3.4 수신자정보관리기
① 수신자 정보 등록
수신자 등록 화면을 출력하고 중앙처리기, 키관리기, 암복화기, 송신기 등과 연계하여 수신자 등록 처리
② 수신자 정보 수정
수신기의 요청에 의해 수신된 수신자 정보를 전달 받아 수신자 정보 수정 처리
③ 수신자 정보 전달
다른 처리기의 요청에 의해 수신자 정보를 다른 처리기에 전달

3.5 송신기
① 단문 입력 화면 출력
중앙처리기의 요청에 의해 단문 입력화면 출력
② 단문 전송
키관리기, 암복호화기와 연계하여 입력한 단문을 수신자에게 전송
③ 개인 정보 전송
암복호화기와 연계하여 개인 정보 전송
④ 공개키 전송
키관리기, 암복호화기와 연계하여 공개키 전송
⑤ 사용자 On Line 및 Off Line 알림 전송
상태관리기 요청에 의해 사용자 상태정보 전송

3.6 수신기
① 서버 소켓 생성
중앙처리기 요청 의해 수신담당 서버소켓 생성
② 단문 수신
단문을 수신하여 중앙처리기로 전달
③ 수신자 정보 수신
수신자정보 수신하여 수신자정보관리기로 전달
④ 수신자 공개키 수신
수신자 공개키 수신하여 키관리기로 전달
⑤ 상태 정보 수신
수신자 상태정보 수신하여 중앙처리기로 전달

3.7 출력기
① 단문 확인 화면 출력
중앙처리기 요청에 단문 확인가능 화면 출력
② 단문 입력 요청
답장입력 위해 중앙처리기에 단문 입력화면 출력 요청
③ 수신자 등록 요청 결과 출력
수신자 등록 위해 보낸 요청 결과 출력

3.8 암복호화기

① 단문의 축약 및 암복호화

키관리기와 연계하여 단문을 축약 및 암복호화 함으로써 안전한 보관송수신 지원

② 개인 및 수신자 정보의 축약 및 암복호화

키관리기와 연계하여 개인 및 수신자 정보를 축약과 암복호화 후 안전한 보관송수신 지원

③ 키정보의 축약 및 암복호화

키관리기와 연계하여 키정보 축약 및 암복호화 후 키 정보의 안전한 보관송신 지원

3.9 키관리기

① 공개키쌍 생성

개인정보관리기 요청에 의해 사용자 공개키쌍 생성전달

② 세션키 생성

각종 정보의 암호화 위해 세션키 생성전달

③ 키 검증

암복호화에 사용되는 각종 키 검증

IV. 타 시스템과의 보안 서비스 비교

본 논문에서 구현한 안전한 단문 전송 시스템은 기존 IM의 보안상 취약점을 대칭키 암호기술, 공개키 암호기술, 그리고 메시지 축약기술을 이용하여 해결함에 따라 안전한 단문 송수신을 지원하였다. 표 2는 기존의 대표적 IM들이 제공하는 보안 서비스와 본 시스템이 제공하는 보안 서비스를 비교한 것이다.

표 2. 타 시스템과의 보안 서비스 비교

보안서비스	SIMS	AIM	ICQ
기밀성	O	X	X
인증	O	X	X
무결성	O	X	X
접근제어	O	X	X

기존 IM은 표 2와 같이 보안 서비스를 전혀 제공하지 못하고 있다. IM은 최상의 보안 서비스를 요구하는 은행 관련 시스템은 아니다. 그러나, IM의 활용도에 대한 다양한 응용 및 발전 가능성과 안전한 단문의 송수신을 위하여 보안 서비스는 반드시 제공되어야 한다.

V. 결 론

본 논문은 안전한 단문 전송 시스템 설계 및 구현에 관한 것이다.

기존 IM은 적절한 보안서비스를 제공하지 못하고 있다. 사용자 로컬 시스템에 저장되는 중요 정보 파일들은 특별한 해킹 도구 없이 그 내용을 파악할 수 있으며 네트워크 상으로 송수신 되는 단문 및 여러 정보는 쉽게 공격 당할 수 있다. 이러한 취약점에 대해 본 시스템은 대칭키 암호기술 및 공개키 암호기술, 메시지 축약기술 등을 이용하여 로컬 시스템에 저장되는 정보 파일 및 송수신 정보에 기밀성, 무결성, 인증 등의 보안 서비스를 제공함으로써 기존 IM의 취약점을 보완하였으며 안전한 환경에서 정보의 보관 및 송수신을 가능하게 하였다.

본 시스템의 특징은 플랫폼 독립적인 Java 언어로 구성되어 실행에 있어 시스템 의존적이지 않다는 점이다.

본 논문은 IM의 여러 기능 중 단문 송수신에 관한 논의가 되었으나 추후 단문 전송 외의 다양한 정보 교환에 관한 논의가 필요하며 추세에 따라 송수신 단문, 사용자 정보, 키 등에 대해 XML을 적용하여 각각의 메시지 포맷에 대한 정의와 이를 이용한 송수신에 대한 논의가 요구된다.

참고문헌

[1] IETF(The Internet Engineering Task Force), http://www.ietf.org.

[2] IETF IMPP Working Group, http://www.imppwg.org.

[3] IETF IMPP Working Group, IMPP Protocol Candidates, http://www.imppwg.org/activities/impp_candidates.html.

[4] Bruce Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons Inc., 1996.

[5] William Stallings, "Cryptography and Network Security: Principles and Practice, Second Edition", Prentice-Hall Inc., 1999.

[6] "정보보호 표준 교재", 한국정보보호센터, 1999.

[7] Jonathan B. Knudsen, "Java Cryptography", O'REILLY, 1998.

[8] Sun Microsystems Inc., 2000, http://java.sun.com.

[9] Java 2 SDK, Standard Edition Documentation Version 1.2.2-001, Sun Microsystems Inc., 1999.

[10] Java 2 SDK, Standard Edition 1.2, Sun Microsystems Inc., 2000,http://java.sun.com/products/jdk/1.2/.

[11] Java Cryptography Extension(JCE) 1.2.1, Sun Microsystems Inc., 2000,http://java.sun.com/products/jce/.

[12] The IAIK Java Cryptography Extension (IAIK-JCE) 2.6.1, the IAIK-Java Group, 2000, http://jcewww.iaik.tu-graz.ac.at/jce/jce.htm.

[13] Cryptix JCE, Cryptix, 2000, http://www.cryptix.com/products/jce.