Diffie-Hellman 키 교환 방식을 이용한 안전한 인스턴트 메신저의 구현

정보고[O] 이광수
숙명여자대학교 전산학과
{bgjung, rhee}@cs.sookmyung.ac.kr

Implementation of Secure Instant Messenger using Diffie-Hellman Key Exchange Algorithm

Bogo Jung[O] Gwangsoo Rhee
Dept. of Computer Science, Sookmyung Women's University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보 전달이 일상 생활처럼 되고 있다. 이러한 현상에 맞추어 등장한 인스턴트 메신저는 즉각적인 메시지의 전달이라는 장점으로 인해 국내에서도 사용자가 급속히 늘고 있다. 그러나 현재와 같이 아무런 보호장치 없이 네트워크를 통해 사용자 정보나 메시지가 노출되면 잠재적 보안 위험이 따르게 되며, 따라서 전송되는 정보의 암호화를 포함하는 안전한 인스턴트 메신저 서비스의 필요성이 대두되고 있다. 본 논문에서는 보안 기능이 포함된 안전한 인스턴트 메신저를 설계하고 자바 언어를 이용하여 구현하였으며, 시스템 설계는 일반 사용자도 쉽게 사용할 수 있고 관리가 편리한 시스템에 역점을 두었다.

1. 서론

인스턴트 메신저란 네트워크를 통하여 실시간으로 메시지를 전송할 수 있는 프로그램을 말하며, 부가적인 기능으로 지정된 사용자들의 메신저 서버 접속 상태나 파일 전송, 대화방 등을 함께 제공한다. 전자 우편이 사용자가 메일 서버에 접속하여 편지들을 읽어오는 과정을 요하는데 비해 인스턴트 메신저는 자동적으로 사용자 화면에 메시지를 전달함으로써 보다 간편하고 즉각적인 메시지의 전달을 기대할 수 있다. 이러한 인스턴트 메신저의 장점으로 인해 그 이용자는 빠르게 증가하고 있으며, 인터넷의 가장 보편적인 서비스의 하나로 정착될 것이 전망되고 있다[1].

현재 사용되고 있는 대부분의 인스턴트 메신저 서비스는 전송되는 정보에 대한 보안 기능이 없는 상태로 운영되고 있다. 인스턴트 메신저 서비스 사용자의 개인정보나 전송되는 메시지가 아무런 보호장치 없이 네트워크 상에 노출되어 있는 상황은 서비스 이용의 급격한 확대와 함께 크나큰 잠재적 보안 위험성이 내재되어 있으며, 안전한 인스턴트 메신저 시스템 개발의 필요성이 대두되고 있다.

본 논문에서는 인스턴트 메신저에 요구되는 보안 서비스를 분석하여 안전한 인스턴트 메신저 시스템을 설계하고 구현한다. 안전한 인스턴트 메신저는 자바 언어로 개발되었으며, 통신 기능은 클라이언트-서버 구조에 비해 통신 오버헤드가 경감되는 자바 RMI에 의한 분산 처리 환경을 기반으로 설계되었으며, 사용자 정보 관리는 Oracle 7.3.3과 JDBC 인터페이스를 이용한다. 그리고 인스턴트 메신저의 사용 계층이 특정 컴퓨터 전문가 집단이 아니라 일반 사용자라는 측면을 고려하여, 보안 서비스의 이용자 투명성을 최대한으로 고려하였다. 안전한 인스턴트 메신저 시스템에서 가장 중요한 부분은 서버와 클라이언트 사이 또는 클라이언트들 사이에 전송되는 정보를 암호화이며, 암호화 알고리즘으로는 DES를 사용하고[2], DES 암호 키의 교환은 Diffie-Hellman 키 교환 방식을 선택하였다[3].

본 논문에서는 2장에서 현재 서비스되고 있는 인스턴트 메신저들의 일반적인 기능과 몇몇 주요 제품들의 특징을 살펴본다. 3장에서는 안전한 인스턴트 메신저 설계와 구현에 대해 기술하며, 4장에서는 결론과 향후 연구방향을 기술한다.

2. 인스턴트 메신저 현황

인스턴트 메신저들이 보편적으로 갖추고 있는 기능들은 다음과 같다.

- 메시지 전송 : 상대방에게 메시지를 보낼 수 있고 수신자는 메시지를 읽은 뒤 답장을 할 수 있다.

이 연구는 1999년도 과학기술부 여자대학교 연구기반 확충사업의 지원으로 수행되었음

- 파일 전송 : 파일을 선택하여 상대방에게 파일을 보낼 수 있고, 송신자는 파일을 받아 저장한다. 파일 전송의 경우 첨부할 메시지를 적어 파일과 함께 보낼 수 있다.
- 일대일 대화 : 상대방을 선택하여 일대일 대화를 할 수 있다.
- 대화방 : 한 명 이상의 상대방과 함께 대화를 할 수 있다.
- 개인정보 및 비밀번호 변경 : 처음 인스턴트 메신저에 등록할 때 입력한 개인정보 및 비밀번호를 변경할 수 있다.
- 친구검색 및 정보보기 : 등록된 사용자 중에서 원하는 사람을 찾기 위해서 키워드를 입력하여 친구로 등록할 수 있고, 검색된 친구의 개인정보를 볼 수 있다.

현재 나와있는 국내외 인스턴트 메신저 제품은 수십 종에 이르며, 이런 제품들은 부가적인 서비스의 종류와 오프라인 상태에 있는 상대와의 통신 지원 여부, 사용자 접근 제한 등에 조금씩 차이를 보인다.

ICQ는 아메리카-온라인(AOL) 사의 제품으로 인스턴트 메신저의 원조이며 상대방이 접속중이 아니더라도 메시지나 파일 전송, 채팅 요구 등이 가능한데, 이는 서버가 통신 요청 내용을 보관해 두었다가 상대방이 접속할 때 처리해주는 방법을 사용한다. 그리고, 다른 사용자의 친구 목록 등록 허용 여부, 패스워드 관리 수준, 메시지 수신 허용 여부 등을 개별 사용자가 정할 수 있는 기능을 제공한다[4].

마이크로소프트사의 MSN 메신저 서비스 역시 자신의 개인 정보나 접속 상황에 대한 접근, 메시지 수신 허용 여부 등에 대한 사용자의 권한을 보장하고 있으며, 또한 자신을 친구 목록에 등재하고 있는 다른 사용자들의 리스트를 볼 수 있고, 사용자 패스워드를 암호화하여 전달한다[5].

디지토사의 소프트메신저는 전용 클라이언트 프로그램이 없어도 웹을 통해 개인정보를 수정할 수 있고, 친구를 찾아 메시지를 보낼 수 있다. 또한 메시지를 전달할 때 서버를 경유하여 보내기를 선택했다면 메시지를 읽는 일도 가능하다[6].

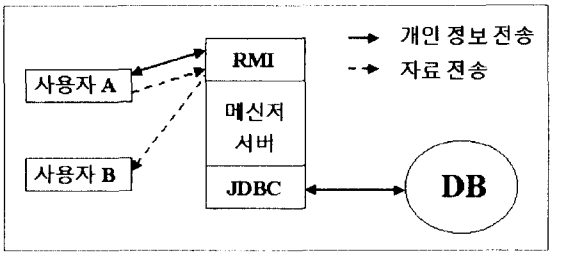
MaXIM(Magic Xecure Instant Messenger)은 (주)드림시큐리티사의 제품으로 인증 서버인 Magic CA 서버와 연계하여 암호화 기능과 인증 기능이 추가된 인스턴트 메신저이다[7]. MaXIM은 전자서명과 전자봉투를 이용하여 정보를 전송함으로 데이터 및 파일에 대한 암호화를 제공하고 있다.

3. 안전한 인스턴트 메신저의 설계와 구현

본 논문에서 구현된 인스턴트 메신저에서는 메시지와 파일 전송, 대화방, 친구 목록 및 검색 등의 일반적인 서비스를 제공하고 있으며, 오프라인 사용자의 처리와 다중 통보 서비스 등이 추가될 예정이다.

3.1 인스턴트 메신저 시스템 모형

본 논문에서 구현된 인스턴트 메신저 시스템의 모형은 그림1의 3-tier 시스템이다. 그림에서 실선이 나타내는 통신은 사용자 등록, 개인 정보의 수정, 사용자 검색이나 친구 목록 작성 등의 서비스에 사용되는 정보의 흐름을 나타내며 주로 클라이언트 시스템과 서버 사이의 통신이다. 점선이 나타내는 통신은 메시지나 파일 전송, 대화방 등에서 사용되는 정보의 흐름을 나타내며, 클라이언트 시스템들 사이의 통신이다.



<그림 1> 인스턴트 메신저 모형

인스턴트 메신저 시스템에서의 통신은 자바 RMI구조를 이용하였다. 송신자는 정보를 전송하기 위해서는 그 정보를 처리하는 서버의 해당 메쏘드를 호출하며, 서버는 처리 결과를 메쏘드의 리턴값 형태로 전달한다. 수신자가 등록된 다른 사용자일 경우 서버는 수신자의 해당 메쏘드를 호출하는 콜백(callback) 기능을 사용한다.

3.2 인스턴트 메신저의 보안 요구사항

인스턴트 메신저의 표준화 작업을 추진하고 있는 IETF 응용 영역 IMPP (Instant Messaging and Presence Protocol) 그룹에서 만든 RFC 2779 문서에서는 메신저 보안과 관련하여 메시지의 기밀성과 재전송(replay) 공격에 대한 대비, 메시지 부결성 등을 기본 요건으로 규정하고 있다[8]. 본 논문에서는 네트워크를 통해 전달되는 보안을 요하는 모든 정보를 암호화하고, 또 매번 사용되는 암호 키를 통신 당사자들끼리 새로 정하게 함으로써 재전송 공격과 메시지 부결성 문제를 해결한다. 인스턴트 메신저에서 암호화를 요하는 정보는 크게는 다음과 같이 두 종류로 분류된다.

- 서버로 전송되는 개인정보의 보호 : 사용자는 인스턴트 메신저에 등록하기 위하여 개인 신상에 관한 정보 및 인스턴트 메신저에 접속하기 위한 비밀번호를 서버에 전송하게 된다. 또한 개인정보 및 비밀번호를 사용 중에 변경할 수 있다. 만약, 서버로 전송되는 정보들이 암호화되지 않고 네트워크를 통하여 그냥 전송된다면 이는 제3자에 의하여 도청될 수 있다. 이를 예방하기 위해서는 사용자 개인에 대한 정보가 네트워크를 통하여 전송될 경우 암호화되어 전송되어야 한다. 이 경우는 전송되는 정보는 송신자와 서버만이 알고 있는 키로 암호화되어 있어야 한다.
- 사용자간에 전송되는 정보의 암호화 : 사용자가 전송

하는 메시지나 파일이 중요한 내용일 경우 이러한 내용은 수신자 외의 다른 사용자가 해독할 수 없도록 암호화되어 전송되어야 한다. 이 경우는 송신자와 수신자만이 알고 있는 키로 암호화되어 있어야 한다.

3.3 사용된 암호 알고리즘

안전한 인스턴트 메신저에서는 서버와 사용자, 그리고 사용자간에 전송되는 정보를 암호화하기 위하여 대칭형 알고리즘(Symmetric Algorithm)을 사용하였다. 대칭형 알고리즘은 암호화 및 해독을 위해 필요한 비밀키(Secret Key)를 서로 공유해야 하는 단점이 있지만, 비대칭형 알고리즘에 비해 암호화 및 해독에 걸리는 시간이 짧기 때문에 실시간 정보를 교환하는데 적합하다. 대칭형 알고리즘으로는 가장 널리 사용되어 온 DES를 사용하였으나 시스템의 구현은 특정 암호 알고리즘에 종속되어 있지 않으므로 다른 알고리즘으로의 변경이 용이하다. DES 키 교환은 Diffie-Hellman 키 교환 방식을 원형대로 사용하였다. Java 암호 모듈은 Sun JCE 스펙을 따르는 오스트리아 그라쯔 대학에서 제공하는 IAIK-JCE 패키지를 사용하였다[9].

3.4 안전한 인스턴트 메신저의 보안 기능 구현

인스턴트 메신저에서 사용되는 암호화 기능은 통신 참가자의 형태에 따라 키 교환 방식이 달라지므로, 각 경우를 구분하여 구현하였으며, 통신에서 암호화 기능은 강제적인 것은 아니며 사용자가 선택할 수 있도록 하였다.

3.4.1 개인정보의 암호화

사용자가 등록 혹은 수정할 때 입력하는 개인정보는 서버와 공유하는 키를 이용하여 암호화하여 전달된다. 이 경우 사용자는 서버의 데이터베이스에 직접 접근할 수 없고, 암호화된 정보만을 전송한다. 서버는 사용자로부터 암호화된 정보를 받아 사용자와 공유한 키를 이용하여 해독한 뒤 데이터베이스에 저장하게 된다.

친구정보보기를 통해 전송되는 상대방에 대한 정보 역시 서버와 공유된 키를 이용하여 암호화되어 전송되기 때문에 등록된 사용자에게만 개인정보가 보여질 수 있다.

이 경우 사용되는 키는 일회용이며, 매번 사용자와 서버가 협력하여 새로운 키를 생성하여 사용한다.

3.4.2 사용자간에 전송되는 정보의 암호화

사용자간에 전송되는 정보는 서로 공유하는 키를 이용하여 암호화되어 전송된다. 메시지, 파일, 그리고 일대일 대화를 하게 되는 경우 암호화에 이용되는 키는 사용자만 알 수 있고, 서버는 알 수 없다.

암호화 전송을 위해서는 수신자와 암호 키를 교환하고, 교환된 키는 메시지나 파일 전송의 경우 일회용으로 한 번밖에 사용되지 않는다. 그러나 일대일 대화의 경우는 교환된 키의 수명은 일대일 대화가 종료되기 전까지 계속된다.

메시지나 파일을 암호화하여 보내는 경우는 메시지 상자를 사용하여 수신자에게 암호화된 자료의 도착을 알리고, 일대일 대화의 경우 암호화 전송이 이루어짐을 나타내기 위하여 암호화된 문장과 해독된 문장을 화면에 동시에 표시한다.

3.4.3 대화방에서의 암호화

대화방에서 암호화된 내용을 전송하기 위해서는 두 명 이상의 사용자가 키를 공유해야 한다. 이 경우는 메시지나 파일, 그리고 일대일 대화에서 사용하던 방법과는 다른 방법을 사용하게 된다. 먼저 대화방을 개설하는 사용자가 임의의 암호 키 K를 생성한다. 암호화된 대화방에 참여하고자 하는 다른 사용자는 먼저 개설자에게 확인을 받은 뒤 개설자와 Diffie-Hellman 방법을 이용하여 임시 키를 교환하고, 개설자는 그 임시 키를 이용하여 대화방 키 K를 암호화하여 전달한다. 즉, 그 대화방에 참가하는 사용자들은 서로 다른 임시 키를 받게 되지만 최종적으로 대화방 개설자로부터 수령하는 키는 모두 K이다. 개설자는 사용자의 정보를 확인하고 참여여부를 결정할 수 있다.

4. 결론 및 향후과제

본 논문에서는 인스턴트 메신저를 사용하여 네트워크를 통해 정보 전달을 할 경우에 생기는 문제점을 지적하고, 이를 해결하는 방법으로 암호화 기능이 첨가된 인스턴트 메신저를 제안하였다. 매번 사용되는 암호 키가 통신 참가자의 협력에 의해 새롭게 정해지므로 메시지를 가로채 보관해 두었다가 재전송 하는 공격이 불가능하며, 암호키에 대한 보안만으로 메시지의 변조나 위조가 불가능한 시스템으로 구현하였다.

향후과제로는 통신 상대방이 오프라인 상태에 있어 Diffie-Hellman 키 교환 방식을 적용할 수 없는 상황과 다수 사용자나 사용자 그룹을 대상으로 메시지나 파일을 전송하는 기능이 추가될 때 발생하는 키 분배 문제를 효율적으로 해결하는 방안에 대한 연구 등을 들 수 있다.

5. 참고문헌

[1] PC Week, 4(19):66-67, 1999

[2] Data Encryption Standard(DES). National Bureau of Standards FIPS Publication 46, 1977

[3] W.Diffie and M.E.Hellman. Multiuser cryptographic techniques. AFIPS Conference Proceedings, 45:109-112, 1976

[4] ICQ, http://www.icq.com/

[5] MSN Messenger Service, http://messenger.msn.com

[6] 소프트메신저, http://www.softmessenger.com/

[7] MaXIM, http://www.dreamsecurity.com/html/productinform_1.htm

[8] M.Day, S.Aggarwal, G.Mohr, and J.Vincent, Instant Messaging / Presence Protocol Requirements, RFC 2779, Feb 2000

[9] IAIK-JCE, http://jcewww.iaik.tu-graz.ac.at/