Design and Implement of a Secure Instant Messaging Service with IC Card

Chia-Pei Lee
Graduate Institute of Information and Computer Education, National Kaohsiung Normal University
m9453719@stu94.nknu.edu.tw

Chung-Huang Yang
Graduate Institute of Information and Computer Education, National Kaohsiung Normal University
chyang@nknucc.nknu.edu.tw

Abstract

Instant Messaging (IM) is one of the most important Internet applications that enable real-time exchange messages through personal computers. IM allows users to send texts, audio and video files, and other types file. People are using IM both for personal and business reasons. However, most IM systems are not secure. In order to find a solution to secure IM communications, we designed and implemented a Secure Instant Messaging and Presence Protocol (SIMPP) for the three-party (two users and one server) IM communication model. The SIMPP is base on elliptic-curve cryptography. At the same time to enhance the security and convenience. We simplify some process to enter SIMPP with contact and contactless smart card. The proposed IM service is compatible with IETF XMPP (eXtensible Messaging and Presence Protocol) Standard. We chose jabberd2 software to create a SIMPP server on the Linux platform, wherein we used C++ Builder to create a SIMPP client on the Windows platform. This study also introduces the technology of Instant Messaging, SIMPP implementation.

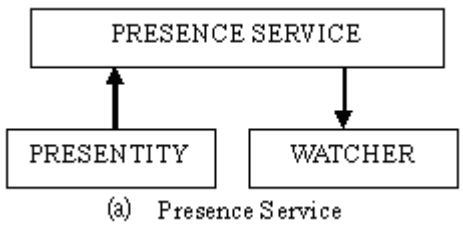
Keywords: Instant Messaging、XMPP、Jabber、IC Card

1 Introduction

Instant Messaging (IM) [2] is one of the most important Internet applications that enable real-time exchange messages. IM allows users to send texts, audio and video files, and other type files. People are using IM both for personal and business reasons.

In year 2000, Internet Engineering Task Force (IETF) released the Request For Comments (RFC) 2778 standard [3] which defines IM systems to be composed of two types of services, Presence Service and Instant Messaging Service, as shown in Figure 1. The Presence Service, shown in Figure 1(a), is responsible for the presence exchange. Through Presence service get presence status each other. The Instant Messaging Service, shown in Figure 1(b), is responsible for the inter-client real-time message exchanges. Through Instant Messaging Service exchange messages each other. Under the IM services models, data communications between any two clients should pass through the server, shown in Figure 2.

IETF defines the requirement Instant Messaging and Presence Protocol (IMPP) in RFC 2779. There are two standard protocols within the IETF for Instant Messaging; SIMPLE and XMPP. SIMPLE and XMPP are in accordance with RFC 2778 and RFC 2779.



(a) Presence Service

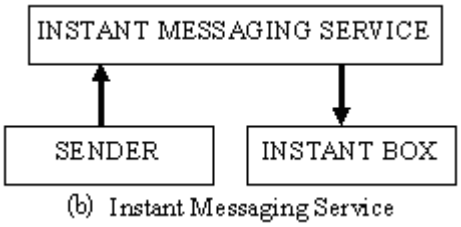


Figure.1 Two types of IM services models defined in RFC 2778

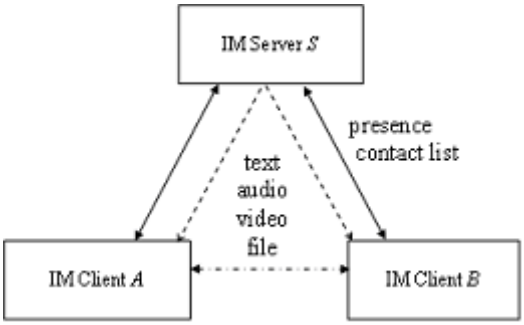


Figure.2 Three-Way communication model

Session Initiation Protocol (SIP) is used to establish and manage multimedia IP sessions. However, it can be used to provide Instant Messaging and Presence service. Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) is an IM protocol based on SIP, using peer-to-peer (P2P) for real-time information exchange, and many multimedia (such as VOIP, video) communications. For security, SAMPLE is followed the standard of SIP.

XMPP is the first protocol for Instant Messaging. It is uses a distributed client-server architecture like email. XMPP [8, 13] exchange data with XML (eXtensible Markup Language) format, and exchange data in Client-Server architecture. XMPP technology from Jabber, in fact, it is the core protocol of the Jabber. Jabber is an open instant messaging technology. For security, Simple Authentication and Security Layer (SASL) and SSL/TLS have been built into the core XMPP/Jabber specifications.

We designed and implemented a secure IM protocol, SIMPP (Secure Instant Messaging and Presence Protocol) enhance the communication security of the IM system. The proposed SIMPP was implemented with the XMPP protocol of RFC 3920-3923 and JEPs (Jabber Enhancement Proposals) while ECC (Elliptic Curve Cryptosystem) was selected to speedup public-key cryptographic functions.

IC (integrated circuit) card or smart card is a pocket-sized card with embedded IC. Smart card can be used for identification, strong authentication and data storage. We can distinguish smart card into contact smart card and contactless smart card. Contact smart card has to contact with card reader for transmitting data. The standard for contact card communication is defined in ISO/IEC 7816. We can find the application of contact card in daily day, such as ATM card、SIM card (GSM) or credit card. Contactless smart card transmits data from remote retrieval by coil.

Contactless smart card communicates with card reader trough RFID. The standard for contactless card communication is defined in ISO/IEC 14443. It defines two types of contactless card “A” and “B”. Contactless smart card often used for public transportation and other electronic purse applications. We simplify some process to enter SIMPP with contact and contactless smart card, to enhance the security and convenience of SIMPP.

The security of Instant Messaging will be introduced in the section 2. To improve SIMPP with contact and contactless smart card in the section 3, and introduce the system in the section 4. The conclusion is given in section 5.

2 Secure Instant Messaging

The section will be introduced the secure rules of origin in IM protocol. In addition to display some software used in IM secures. RFC2779 lists the security considerations for

IMPP. SIMPLE and XMPP protocols have some different rules in security, too.

2.1 SIMPLE Security

No special security rules have been developed focusing on SIMPLE. SIMPLE have been developed based on the SIP. SIMPLE follow SIP about the rules of security. SIP protects data with TLS and S/MIME (Secure/Multipurpose Internet Mail Extensions). About these are described in RFC3428.

2.2 XMPP Security

XMPP includes a method for securing the stream from tampering and eavesdropping. This channel encryption method makes use of the Transport Layer Security (TLS) protocol, along with a "STARTTLS" extension that is modeled after similar extensions for the IMAP, POP3 [POP3], and ACAP protocols [10].The SASL is proposed as a method for adding pluggable authentication support in XMPP. Using STARTTLS shown as Client-to-Server example Figure 3.

Step 3: Server sends the STARTTLS extension to client along with authentication mechanisms and any other stream features:

```
<stream:features>
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'>
    <required/>
  </starttls>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
  </mechanisms>
</stream:features>
```

Step 4: Client sends the STARTTLS command to server:

```
<starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5: Server informs client that it is allowed to proceed:

```
<proceed xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5 (alt): Server informs client that TLS negotiation has failed and closes both stream and TCP connection:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
</stream:stream>
```

Step 6: Client and server attempt to complete TLS negotiation over the existing TCP connection.

Figure.3 Begin a TLS negotiation to secure the stream.

2.3 Existing Security Solutions

There are two main kinds of secure IM system. The first is password protected. Users register a username and password for their new account. The user-chosen password is often weak. The second is third-party solutions. The kinds of software always designed for some one IM system (such as MSN Messenger, AIM, Yahoo! Messenger) and usually build the channel of secure between two clients (such as IMSecure、SimpLite). The disadvantage of this software is that it needs to be installed in two clients.

2.4 SIMPP

Under the IM service models, data communications between two clients should pass through the server. At the same time, messages may not be encrypted when they pass through a server. We designed and implemented a secure IM protocol, SIMPP improve the communication security between client-client of the IM system.

The main objective of the proposed secure IM design is to reduce computational overhead imposed on an IM system due to security enhancement. Since security does not come from free and additional computational time is required to perform security functions, therefore, we revised the IMKE protocol to get a more efficient IM system, while still maintaining its security. The proposed Secure Instant Messaging and Presence Protocol (SIMPP) contain three phases: (1) registration, (2) client-server communications, and (3) client-client communications.

In addition to improve the security and convenience, we increases the way of input password with contact and contactless smart card in login process.

Contact smart card has to contact with card reader for transmitting data. Contactless smart card transmits data from remote retrieval by coil. Contactless smart card communicates with card

reader trough RFID. For a number of reasons contactless technology is believed to be less secure than contact technology.

This study aim is using the smart card the security, portable, the convenience; simplify some process to enter SIMPP with contact and contactless smart card.

3 Design Secure Instant Messaging System

This study aimed to strengthen SIMPP (Secure Instant Messaging & Presence Protocol) on the use of the safety and convenience. Use contact and contactless smart card to enhance convenience during login SIMPP system.

3.1 Smart Card

This study implements the secure instant messaging system with Java Card and MIFARE Card. Java Card is a kind of contact smart card. It is a framework for execution of application in contact smart card developed by Sun. The advantages of Java Card program is security and portable.

MIFARE is the most widely contactless smart card. It is developed by Philips. MIFARE is the NXP Semiconductors-owned trademark now. NXP is a leading semiconductor company founded by Philips. MIFARE card with the ISO/IEC 14443A standard, signal frequency is 13.56MHz, Induction in the range of about 0~10 cm.

3.2 Register and Login

There are three kinds of ways to login SIMPP. Enter password through keyboard, Enter Java card's PIN code get account and password from Java card or through card reader get account and password from MIFARE Card. When he/she wants to login SIMPP with Java card or MIFARE card, he/she has to create a new account and set password with the same type.

3.2.1 Normal

When he/she creates a new account, user has to setup password. User has to enter password through keyboard login SIMPP.

3.2.2 Java Card

When he/she creates a new account with Java card, user must reset PIN code of Java card. At the same time, SIMPP will create password and record into Java Card. User has to enter Java Card's PIN card to get password entry SIMPP.

3.2.3 MIFARE Card

When he/she creates a new account with MIFARE card, user has to create new account and to setup password. After create a new account, SIMPP will be record account and password into MIFARE card. Through card reader user can entry SIMPP.

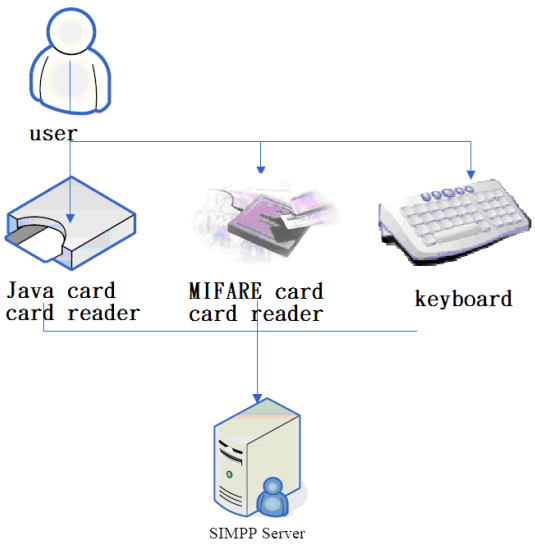


Figure.4 SIMPP Register and Login

4 System Implementation

The same as Google Talk, this study to choose XMPP/Jabber [10, 11, 12] to implement SIMPP. Client and Server used TCP port 5222 (used TCP port 5223 with SSL), this study Client interface shown in Figure 5.

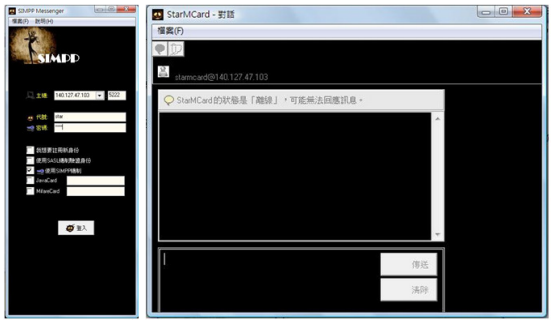


Figure.5 Secure IM client software with SIMPP

This study enhances SIMPP (Secure Instant Messaging & Presence Protocol) security and convenience.

5 Conclusion

Instant messaging has become popular. However, most IM systems are not secured. We designed and implemented a Secure Instant Messaging and Presence Protocol (SIMPP) base on elliptic-curve cryptography. This study enhances SIMPP (Secure Instant Messaging & Presence Protocol) security in login process. We simplified some process to enter SIMPP with contact and contactless smart card and implemented in IM client. We increased register and login in IM client software.

Reference:

1. Berson, T. "SKYPE Security Evaluation," Oct. 2005, http://www.anagram.com/berson/skyeval.pdf
2. Chatterjee, S. and Abhichandani, T. and Haiqing, B. and TuIu, and Jongbok, B. "Instant messaging and presence technologies for college campuses," IEEE Network, Vol. 19, No. 3, May-June 2005, pp. 4 - 13.
3. Day, M. and Rosenberg, J. and Suugano, H. "A Model for Presence and Instant Messaging," IETF RFC 2778, Feb. 2000.
4. Hankerson, D. and Menezes, A. and Vanstone, S. Guide to Elliptic Curve Cryptography, Springer, 2004.
5. Kikuchi, H. and Tada, M. and Nakanishi, S. "Secure Instant Messaging Protocol Preserving Confidentiality against Administrator," Proc. 18th Int'l Conf. Advanced Information Networking and Applications (AINA), 2004, Vol. 2, pp. 27–30.
6. Mannan M. and Van Oorschot, P.C. "A Protocol for Secure Public Instant Messaging," Financial Cryptography and Data Security 2006 (FC'06), 2006. http://www.scs.carleton.ca/research/tech_reports/2006/download/TR-06-01.pdf
7. MSN Sniffer, http://www.effetech.com/msn-sniffer/
8. NXP (formerly Philips), MF1ICS50 Functional Specification. Jan 29, 2008.
9. Rittinghouse J. and Ransome, J. Instant Messaging Security, Elsevier Digital Press, 2005.
10. Saint-Andre, P. "Extensible Messaging and Presence Protocol (XMPP): Core," IETF RFC 3920, Oct. 2004.
11. Saint-Andre, P. "Streaming XML with Jabber/XMPP," IEEE Internet Computing, Vol. 9, No. 5, Sep./Oct. 2005, pp. 82-89.
12. Shiegoka, I. Instant Messaging in Java: The Jabber Protocols, Manning Publications, 2002.
13. Sun Microsystems, Inc. http://java.sun.com/javacard/specs.html
14. Wireshark, http://www.wireshark.org/