Design On Secure Messenger Mechanism Using Elliptic Curve Cryptography and IPSec

Gwang-Mi Choi, Su-Young Park and **Hyeong-Gyun Kim**, *Member, KIMICS*

Abstract—When most of existing instant messengers log on server, they transmit to sever in encoding password to RC5. but RC5 don't be secured because it has been known many of password cracking tools. Also, messengers don't have any protection on the transmitted information with communicating two hosts since loging on, endangering the privacy of the user. As a counter measure, messengers need to provide security service including message encryption. In this paper, we designed a key exchange method of password representing fast, effective and high security degree, using ECC(Elliptic Curve Cryptography) that being known the very stronger than another public key cryptography with same key size. To effectively improve data transmission and its security using IPSec protocol between users, tunnel mode is introduced. Tunnel mode transmits Host-to-Host data through virtual pipelines on the Internet.

Index Terms—IPSec(IP Security), ECC(Elliptic Curve Cryptography), RC5, P2P(Peer-to-Peer)

I. INTRODUCTION

Internet-based e-mail service has ensured many users owing to its powerful functions, convenience and speed as it replaces the conventional postal services. Under such a circumstance, since messenger which began to be used some years ago has integrated conventional services like e-mail, sending files and chatting and additionally and offered services of new types with various new services, its users are increasing.

Messenger is the program which can give and receive a real-time message at any time where internet is available and has the characteristics of quick service, convenience and real time [1-6].

Such characteristics of messenger as sending messages or files like telephone in real time become a great attraction to those who felt the inconvenience in using individual internet service and recently a number of instant messaging program (hereinafter called messenger) service appeared and began to be widely used.

Manuscript received July 22, 2004.

Gwang-Mi Choi is with school of Computer and Internet, Dongkang College, Gwang ju. Korea, (e-mail: iplab@hanmail.net)

Su-Young Park is with school of Computer Science and Statistic, Chosun University, Gwang ju. Korea, (e-mail: swiminpark@hanmail.net)

Hyeong-Gyun Kim is with field of Computer and Internet, Dongkang College, Gwangju, Korea. (e-mail : multikim87@hanmail.net)

Most messengers which are currently used have been operated without the security function of information transmitted. The situation that private information of messenger service users or message transmitted are exposed on network without any security device may contain a potential security risk that the information can be wiretapped by a third person. Therefore, development of secure messenger system which can transmit information safely is needed.

Accordingly, the secure messenger presented in this paper is designed to encode information from two hosts in communication and then transmit it with key exchange method using secure and reliable ECC in wireless internet environment and IPSec Protocol designed for protection of packet delivered through public internet network.

In this paper, chapter 2 examines the basic concept of messenger and standardization work in progress and describes security problems of existing messengers, chapter 3 describes ECC and IPSec, chapter 4 designs secure messenger mechanism and chapter 5 is conclusion.

II. RELATED RESEARCHES

A. Outline

Messenger plays the very important roles in communication between client and client unlike conventional internet service which was communication between client and server. In particular, it has the advantage of reducing load of service with communication between clients.

Messenger can be divided and compared into two types according to its implementation. The first is server dependent type which server locates in the center of messenger and it retrieves logon users and controls user states and message exchange.

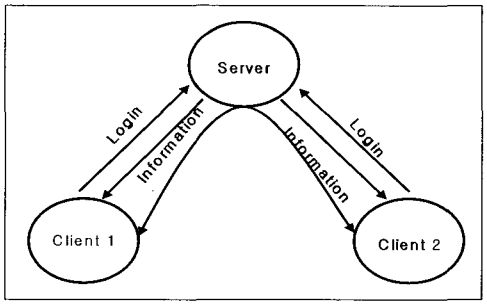

Fig. 1 IM Operation Diagram Via Server

Fig. 1 is operation diagram of server dependent messenger. The second is P2P (Peer-to-Peer) messenger as server independent type and needs no server, doesn't consider communication with server and if homogeneous

program is executed and network resource is available, it can perform messenger functions. Fig. [2] is operation diagram of P2P.

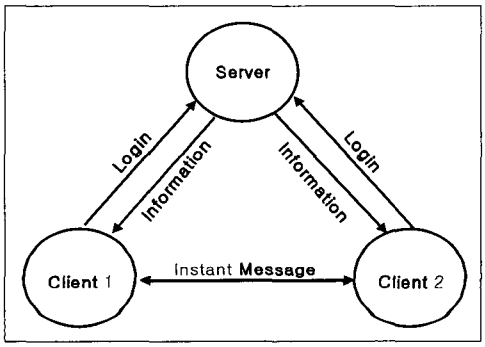

Fig. 2 IM Operation Diagram Via PEP

B. Related Standardization Work

IETF progresses standardization work related to "instant messaging and presence protocol" [3-5]. Standardization work in progress includes RFC document and 3 draft documents and documents related to standardization can be summarized as follows [1-5].

"A Model for Presence and Instant Messaging" (RFC 2778) defines abstract model for presence and instant messaging system. It defines complex and various entities and terms and makes service offered by system outline. In addition, it aims to define common terms for the future works of protocol and markup for presence and instant messaging [1].

"Instant Messaging/Presence Protocol Requirements" (RFC 277) define minimum requirements to meet the purposes of IMPP (to define standard protocol and make independently developed instant messaging or presence application interact on the internet) [2].

"Common Presence and Instant Messaging Message Format" describes message type for protocol following CPIM (Common Profit for Instant Messaging) and 'message/cpim' mime type [3].

"Data and Time on the Internet : Timestamps" are profiles of ISO 8601 standard for expressing date and time used in Gregorian calendar and define date and time modes to be used in internet protocol [4].

C. Security Problems

Convention messenger services send password through encryption to RC5 when logging on to server, but recently password cracking programs were widely known. In addition, since information transmitted between client messengers is transmitted through network without any protection device, a third person wiretaps it or transmitted message may be exposed, security problems of personal information outflow have been addressed.

While conventional messenger service offers blacklist, message rejection and spam message prevention functions, measures against message snipping (sniffing) by evil hacker are helpless. However, researches on strengthening security functions of messengers are wholly lacking abroad, but are in the stage of beginning home [7].

Therefore, this study designed the secure messenger mechanism in order that information can be transmitted securely with the encryption of information transmitted between clients using password key exchange mode and IPSec based on secure and reliable ECC in radio internet environment and the support of user authentication.

III. ECC AND IPSEC

A. Outline of ECC

ECC offers mathematical place where encryption algorithm not a specific encryption algorithm can be implemented and algorithms like RSA, ElGamal, etc are implemented on elliptic hyperbola not on conventional integral space [8].

Elliptic curve on finite field $GF(p)$(decimal $p>3$) is composed of all points (x, y) on $GF(p)$ satisfying Weierstrass equation and virtual point at infinity O. Elliptic curve defined on real number is a set of points (x, y) satisfying elliptic curve equation of Expression 1.

$$y = x^3 + ax + b,\ (x,\ y,\ a,\ b \text{ real number}) \quad (1)$$

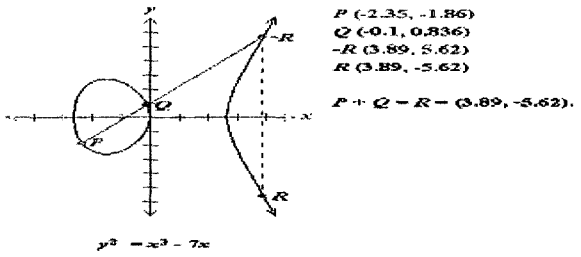

Fig. 3 Example of addition of two different points on elliptic curve of real number

where, if coefficients satisfy this condition, $4a^3 + 27b^2 \neq 0$, this elliptic curve makes a group with point at infinity O non-existent on the elliptic curve. Since elliptic curve defined on real number uses element {0,1} with incorrect calculation due to slow calculation and rounding-off error it is not appropriate for encryption. By this reason, application on real cryptographic applications used binary finite field GF (2^m). Fig. 3 is the example of two different points on elliptic curve of real number.

Since elliptic curve group defined on GF(2^m) has finite elements and there is no ascending sequence by rounding off, it has been used in binary computer operation. If P and Q are two points of elliptic curve E, the following expression is established. Expression 3-2 is elliptic curve equation on GF (2^m). (Expression 2)

$$y^2 + xy = x^3 + ax^2 + b,\ (a,\ b \in GF(2^m)) \quad (2)$$

[addition algorithm on GF (2^m)]

◎ If P≠Q, P+Q=R(,) and, values of, are as follows.

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a,$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

$$\lambda = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)$$

Security of elliptic curve encryption system is based on complexity of discrete algebra problems on elliptic curve. That is, points P and Q = k · P is given on elliptic curve E(GF(2^m)), it is impossible to get k in an exponential time [9].

Elliptic curve encryption system is mainly calculated by adding point on elliptic curve, P, by x times. That is, addition to get Q=xP

Q = xP is calculated by modular multiplication. Major public key encryption system depends on efficient modular multiplication and since elliptic curve is smaller than systems having different P values, its efficiency is excellent. Security of elliptic curve encryption system depends on discrete algebra problems of elliptic curve and its efficiency depends on rapid calculation of xP. Fig. 4 is the example of inverse element and infinite origin of addition on GF (2^m). Table 2 compares RSA/DSA with the same security to size of domain variables of elliptic curve [15].

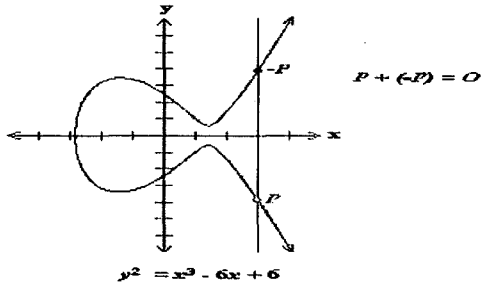

Fig. 4 inverse element and infinite origin of addition

Table 2. Comparison of Domain Variables by the Same Security

Time to break in MIPS year	RSA/DSA (BITS)	ECC (BITS)	RSA vs. ECC key
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

B. Outline of IPSec

IPSec (Internet Protocol Security) is VPN tunneling protocol standardized by IETF (Internet Engineering Task Force), is an extended form of IP and is operated on TCP/IP based network. It is defined as a set of standard protocol for transparent authentication, confidentiality and integrity of data in application program and existing network basis and is also divided into tunnel mode and transport mode according to data areas. Fig. 5 shows header layout and protected areas according each mode. Tunnel mode adds new IP header to transmit information from security gateway to other security gateway securely, encapsulates the whole IP datagram and uses IP address of both security gateways to address field of new IP header. However, host-based tunnel mode extended block transmitting secure information to host-to-host and IP address of host is used for address field of new IP header. Transport mode encapsulates IP payload in order to transmit information to host-to-host securely. While tunnel mode protects all upper layers including IP, transport mode is confined to TCP (or UDP) and its upper layers and its security is lowered, but overload can be reduced [11.12].

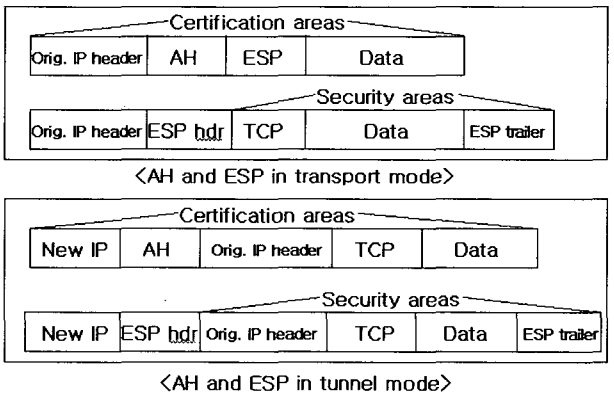

Fig. 5 Header layout and protected areas according to each mode

IPSec includes standard security protocol within each mode in order to offer integrity that message is not modulated or replaced in the process of authentication and transmission of identification between two agencies or users in communication and confidentiality that data transmitted through network are not exposed to others. IPSec security protocols include AH (Authentication Header) protocol for the purpose of authentication, integrity of data and prevention of replay and ESP (Encapsulating Security Payload) protocol for the purpose of authentication, integrity of data, prevention of replay and confidentiality [11, 12]. These two protocols can be used independently according to each requirement level or in a combined form. AH compresses a fixed area according to each mode offered in IPSec through message compression function like HMAC-MD5 or HMAC-SHA like [Fig. 6] and uses its value ICV (Integrity Check Value) as authentication data field value on AH header. It offers generation of sequence number ensuring authentication and integrity of data through this value and function of preventing replay with verification of sequence number [10, 12, 13].

ESP encodes a fixed area to message encryption functions like DES or RSA according to each mode, ensures confidentiality of data and offers replay prevention function like AH through replay prevention function [11].

IPSec procedure is shown in [Fig. 6] and its process is divided into IPSec header generation and message authentication and encryption [12]. IPSec header generation should be located between IP and TCP (or UDP), AH must include authentication value of AH upper layers to authentication field of generated header and ESP must include encryption value of ESP header upper layout to payload field of generated header. Therefore, this study applies IPSec to communication between two hosts and performs transmission of encoded message in the process of transmitting and receiving message mutually

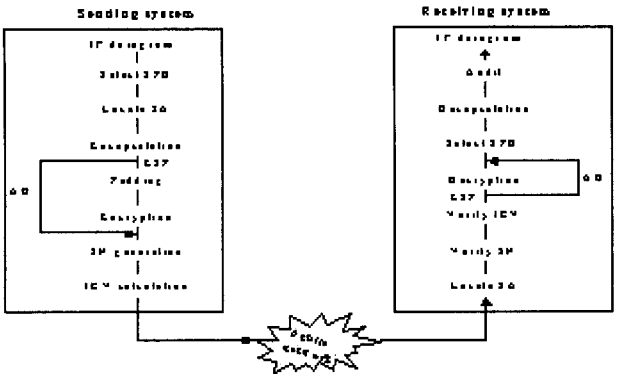

Fig. 6 IPSec Procedure

IV. SUGGESTED MESSENGER MECHANISM

A. Structure

Messenger suggested in this paper consists of four components as follows:

- Messenger Client : functioning communication with server, transmission of messages between users and monitoring of communication with mail server and presence state of users
- Messenger Server : functioning to issue, distribute and manage user information and public key authentication
- Membership Information & History Data : functioning to keep registered information and history of users and keep and send absent users' message
- Mail Server : functioning to send and receive encryption mail between users

Brief system configuration chart is shown in [Fig. 7].

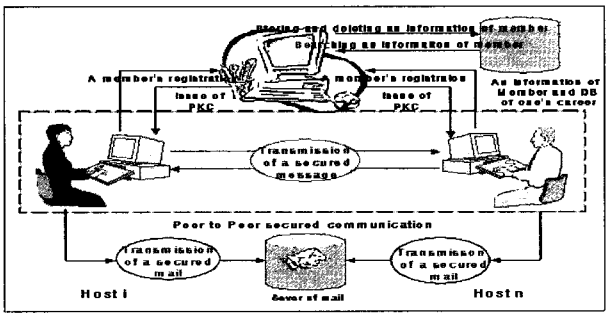

Fig. 7 Structure of Messenger

B. Scenario of Procedures Using Messenger

Scenario sending messages between users using messenger securely follows the following procedures.

(1) Registration and Connection

When user executes secure messenger first, personal information sent by users' subscription to secure messenger or through connection with messenger should be encoded. Conventional way of sending information with messenger was based on encryption of password with symmetry key encryption technique, but it was not secure due to many password cracking tools. Accordingly, this study uses elliptic curve encryption system which was known as stronger than other encryption systems with the same key size and suggests password key exchange method. Client having verification of serve through registration procedure encodes ID, PWD with public key transmitted from server to elliptic curve encryption algorithm. [Fig. 8] shows the process that client sends ID, PWD to server and [Fig. 9] shows the process of verifying ID, PWD by server. Server searches personal key authentication of client saved on database and decodes it.

Let's open *E and P(∈E) and assume messenger* $M=(ID_x, PWD_y)(\in F_2 \times F_2)$

<When client (messenger user) logs on server>

[Server]

Select real number α randomly

Open *kP* by calculation

[Client]

Select real number *k* randomly

Calculate point *kP* and point $k(aP)=a(kP)=(x, y)$ *if* $x, y \neq 0$, *send (kP, IDx, PWDy) to server.*

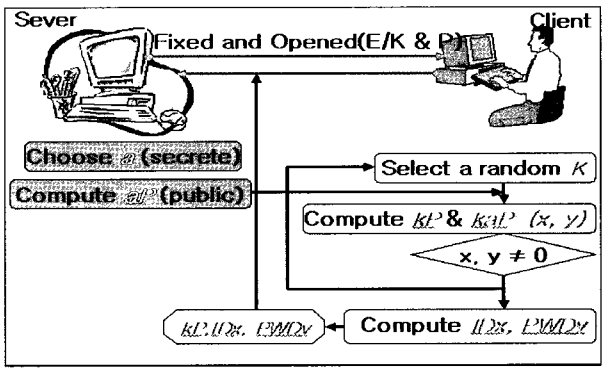

Fig. 8 Process of sending ID, PWD to server by client

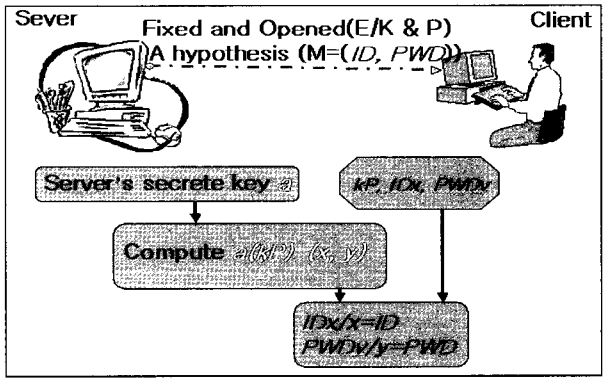

Fig. 9 Process of verifying IP, PWD by server

<(Server) for confirming *ID, PWD*>

1) $a(kP)=(x, y)$

2) $\frac{IDx}{x} = ID, \quad \frac{PWDy}{y} = PWD$

(2) Encoded Dialogue Function

Encoded dialogue function performs encoded host chatting between on-line users. It performs the function of sending encoded messages in the process of sending and receiving message by A's request of chatting to B. Its restrictions are that chatting users should be registered group members of distributed authentication and use IPSec protocol. [Fig. 10] is the example based on tunneling of IPSec protocol environment.

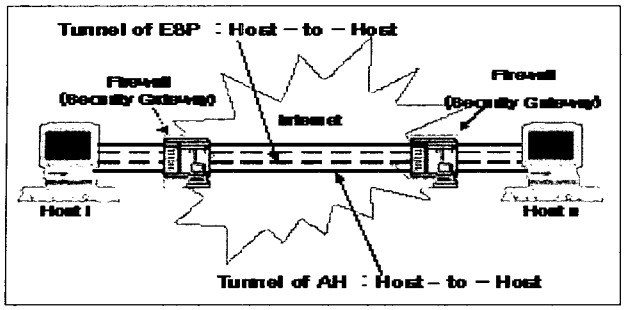

Fig. 10 Message Exchange Mechanism Using Suggested IPSec

When tunnel between two hosts is made, host encapsulates and sends message into ESP. For the protection of datagram from non-authenticated distortion, AH must be used necessarily. The principle of operation to send encapsulated message to AH and ESP is shown in Fig. 11.

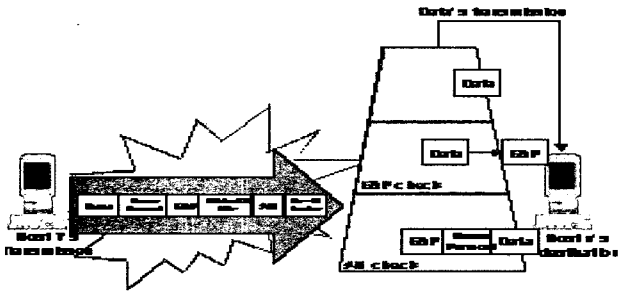

Fig. 11 Suggested Message Transmission Mechanism

IV. CONCLUSIONS

According to IDC report, it was found that 1 hundred million and 3 thousand people have used free messenger service in the world in 2003 and 80 million people have used messenger everyday, and it is expected that use of messenger is increasing. For more activation of messenger, information protection which can ensure security and reliability is needed. This study examines IPSec giving direct packet security which has rapid processing speed and more efficient ECC and network layout than other public system keys and how to apply it to messenger.

This study uses ECC encryption algorithm with fast and stronger processing speed than other encryption systems and logs on server to solve violation of personal privacy. In addition, it sends data with IPSec tunnel and offer authentication and confidentiality service of data. For more development of messenger than the present, it is considered that research toward practical implementation of suggested systems should be conducted.

REFERENCES

[1] RFC 2778("A Model for Presence and Instant Messaging"), http:// www.ietf.org/rfc/rfc2778.txt
[2] RFC 2779("Instant Messaging/Presence Protocol Requirements"), http:// www.ietf.org/rfc/rfc2779.txt
[3] "Common Presence and Instant Messaging Message Format", http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-msgfmt-03.txt.
[4] "Data and Time on the Internet:Timestamps", http://www.ieft.org/internet-drafts/draft-ietf-impp-datetime-04.txt.
[5] "CPIM Presence Information Data Format", http:// www.ieft.org/internet-drafts/draft-ietf-impp-cpim-pidf- 00.txt.
[6] AIM, http://www.aol.com/aim/homenew.adp
[7] A.J Menezes and S. A. Vanstone, "Elliptic Curve Cryptosystems and her mplementation, Journal, on Crytology, PP. 209-224, Autumn, 1993.
[8] ECC Toturial, http://www.certicom.com/resources/ecc_toturial/ecc_toturial.html, 2001.
[9] S. Kent. et. al., "Security architecture for the Internet Protocol", RFC 2401, IETF. 1998.11.
[10] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
[11] S. Kent, R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, November 1998.
[12] C. Madson, R. Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, November 1998.
[13] C. Madson, R. Glenn, "The Use of HMAC-SHA-1 within ESP and AH", RFC 2404, November 1998.
[14] Insoo Lee, "Analysis on Elliptic Curve Public Cryptosystems", KISA, December, 1998.

Gwang-Mi Choi
She received the M.S. and the Ph.D. degrees in the Dept. of Computer Science and Statistic, Chosun University. Her research interests Multimedia, Neural networks, Multimedia contents, Artificial intelligence, Information security, Networks.

Su-Young Park
She received the M.S. degrees in the Dept. of Computer Science and Statistic, Chosun University.
Her research interests Multimedia, Neural networks, Multimedia contents, Artificial intelligence, Information security, Networks.

Hyeong-Gyun Kim
He received the M.S and Ph.D. degrees in the Dept. of Computer Engineering from Chosun University. His research interests include Multimedia, Image processing, Mobile communication, Character recognition.