Secure Mobile IM System Using NTRU

Chilamakuri Manasa #1, M.V.S.N Maheswar #2

#1 Student, PVP Siddhartha Institute of Technology, Kanuru,Vijayawada,Krishna(dt)

#2 Assoc. professor, PVP Siddhartha Institute of Technology, Kanuru,Vijayawada,Krishna(dt)

Abstract: Mirabilis (a pioneer of online chatting that revolutionized communication over the Internet) created the first IM system, dubbed ICQ (I seek you), in 1996 which achieved widespread adoption quickly among netizens. Although other instant messaging (IM) systems have surpassed ICQ in popularity, the medium of IM remains a popular form of technologized communication. The major drawback has been the vulnerabilities associated with IM technology. These vulnerabilities have created several security issues. A hybrid encryption policy using the AES, SHA-1, and RSA algorithms provided by Bouncy Castle encryption library serves as a means of achieving security in IM systems. Implementing a three layered ciphering scheme is a computation and resource over head in IM clients. So we propose to use a single robust ciphering scheme NTRU (Nth degree truncated polynomial ring). The NTRU algorithm is an asymmetric (public/private key) ciphering system that can be used in IM systems. An IM application with NTRU implementation validates the claim.

Keywords: Instant messaging (IM), Nth- Degree Truncated Polynomial Ring Unit (NTRU), Message, Security, Encryption, Decryption.

I INTRODUCTION

In last few years Internet has set the direction of how, where and the way we communicate. E-mail has become a mainstream form of communication and has replaced the traditional letters. In last couple of decades people have started using Internet regularly. The need of live and sensible way of communication over Internet has increased rapidly. The start of Instant Messaging came about in 1996. Instant Messenger is client software that allows person to person interactive communication in real-time provided both users have the same software. Such communication is called ‘chat’. Company named Mirablis, Ltd., introduced ICQ, instant messaging utility. ICQ, in shorthand language is “I seek you”.

Instant messaging (IM) is a real-time communication service which allows a user to send a message, usually based on text, to other users. Nowadays we depend more and more on information from the Internet, and are increasingly not satisfied with accessing the Internet using personal computers or office workstations. Hence, accessing the Internet by portable and wireless devices has been becoming popular.

IM systems are also playing important roles in business communication fields, such as observing the status of staff, real-time chatting, getting business opportunities and so on. The enterprise applications lay more emphasis on the security of the system; therefore, considering the efficiency issue, existing work use the SHA-1 digest algorithm, AES symmetric encryption algorithm, RSA asymmetric encryption algorithm and RSA signature algorithm, with Bouncy Castle Crypto package, to design a security policy to secure the IM system.

In this paper, we propose to use a single robust ciphering scheme NTRU (Nth degree truncated polynomial ring). Instead of implementing a three layered ciphering scheme provided by Bouncy Castle encryption library which is a computation and resource over head in IM clients. To reduce computation and resource overhead especially in resource scarce devices such as mobile devices, NTRU algorithm is implemented. The NTRU algorithm is an asymmetric (public/private key) ciphering system that can be used in IM systems. An IM application with NTRU implementation validates the claim.

II BACK GROUND

A) HOW IM WORKS

Instant messaging works as its name. It delivers the user's message to his desired contact instantly. The message delivery is instant provided users contact person is online. The client software allows user to maintain a list of contacts that he wants to communicate. User can send messages to any of the contacts in his list. Such list is referred to as a buddy list or contact list. This contact list is nothing but e-mail ID of a contact. User can also block a particular contact or everyone who is not on his contact list from sending an instant message. Setting the appropriate privacy settings does this.

When user logs on Instant messenger service he can see the presence of the friends on his contact list and vice versa. User can show his availability via Instant Messenger. Sometimes user is online but is busy and do not wish to respond to any instant messages. In such situations user can change his status to 'Busy' or 'Not available'. This allows the person who is trying to contact user know the reasoning behind the non-availability of user. User can also choose to be invisible while being online. This enables him to watch his contacts without giving his status.

Various communication means are available using instant messaging. User can have an individual chat session or have a conference with multiple users. With use of web camera and voice an interactive web conference can be held using instant messaging.

B) IM Service providers

Among the various vendors for instant messaging, America online (AOL), Yahoo and Microsoft are some of the major vendors in providing instant messaging for consumers.

- MSN Messenger – MSN has about 9 million subscriptions. Besides the subscribers, MSN Messenger can be downloaded free of charge by anyone with an access to Internet.
- Yahoo Instant Messenger – Just like MSN, Yahoo provides the Messenger services free of charge to anyone who wants it. Simply go to their web site and download the Yahoo Messenger. Both Yahoo and MSN support instant text and voice messages, communication face-to-face via web cameras, and affordable PC-to-phone calls anywhere in the world.

III Vulnerabilities of IM

Insecure Communication is the main vulnerability of IM. Businesses are required to protect information related to their customers, vendors and their own trade secret. Several specific issues come up with insecure communications in commercial sector.

- Identity Theft – This is a technological nightmare for an individual who has to live it. In identity theft an individual's identity is stolen and is used by an identity thief to conduct various monetary transactions. The person who's identity has been stolen is not aware of these transactions. By the time an individual becomes aware of such theft bad record in the system is already established. Such crime can be easily committed. Confidential information such as your bank account number, social security number, credit card information should not be shared during IM session.
- Cyber stalking - Crime such as Cyber stalking is becoming very common. In this case stalker

stalks a victim on Internet. Use of E-mail or other forms of electronic communication is used by stalker as means of stalking. Presence is the most popular feature of IM. IM gives away the presence of user. This makes it easier to stalk the person online.

Currently users expect high level of security while doing Instant messaging. Some familiar problems are: data confidentiality while transmitting, data and application access must be controlled, data integrity, loss of device must have limited impact, and non repudiations.

Confidentiality: only the valid communicating users can view the messages.

Integrity: the messages can’t be tampered by the intruders. The system should be able to find out such alteration.

Non-repudiation: no party can deny the receiving or transmitting the data communicating between them.

Authentication: each party has to have the ability to authenticate the other party.

Authorization: it has to be ensured that, a party performing the transaction is entitled to perform that transaction or not.

Security: It is where the messages are encrypted/decrypted using NTRU/PKCS for secure communications

IV RELATION BETWEEN IM AND NTRU

To counter the vulnerabilities of IM as mentioned in section-III, we implement NTRU cryptosystem which mentioned in section-V. Existing work use the SHA-1 digest algorithm, AES symmetric encryption algorithm, RSA asymmetric encryption algorithm and RSA signature algorithm, with Bouncy Castle Crypto package, to design a security policy to secure the IM system. But they are computation and resource over head in IM clients. To reduce computation and resource overhead especially in resource scarce devices such as mobile devices, NTRU algorithm is implemented.

IV NTRU CRYPTOSYSTEM

The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman. NTRU can be used in mobile devices and other mobile applications because of its features of easy generation of keys, high speed and low memory use.

NTRU has 3 integer parameters: N, p, q. N represents the degree of the polynomials at most N-1; p is smaller than q. p and q are small moduli used to reduce the coefficients of the polynomials. They do not have common divisor. We briefly describe the NTRU algorithmas follows.

Key generation

We have to choose two random polynomials x and y in the ring with the restriction that their coefficients are small, usually in {-1, 0, 1}. We import another symbol here: $Z(a_1, a_2)$, which means a set of polynomials with a_1 coefficients are 1, a_2 coefficients are -1 and the rest are 0.

Usually we choose x from $Z_x(a_x, a_{x-1})$ and g from $Z_y(a_y, a_{y-1})$. Then we compute x_p (the inverse of x modulo p) and x_q (the inverse of x modulo q) with the property that

$x * x_p = 1 \pmod p$ and $x * x_q = 1 \pmod q$.

If x doesn’t have these inverses, another x should be chosen. The pair of polynomials x and x_p should be kept as the private key, and the public key K can be computed by

$K= p\, x_q * y \pmod q$.

Both x and x_p are used for private key and K is used for public key.

Let the parameters (N, p, q) have the values N = 11, p = 3 and q = 32 and therefore the polynomials x and y are of degree at most 10. The system parameters (N, p, q) are known to everybody. The polynomials are randomly chosen, so suppose they are represented by

x= -1+X+X2-X4+X6+X9-X10
y= -1+X2+X3+X5-X8-X10

Using the Euclidean algorithm the inverse of x modulo p and modulo q, respectively, is computed So

x_p= 1+2X+2X3+2X4+X5+2X7+X8+2X9 (mod 3)
x_q= 5+ 9X+ 6X2+ 16X3+ 4X4+ 15X5+ 16X6+ 22X7+ 20X8+ 18X9+ 30X10 (mod 32)

Which creates the public key K computing the product K = px_q*y (mod q).

K= 8+ 25X +22X2 +20X3 +12X4 +24x5 +15X6+ 19X7 + 12X8 +19X9 +16X10 (mod 32)

Encryption

The message to be sent can be put into a form of a polynomial $m \epsilon Z_m(a_m, a_m)$ whose degree is at most N-1. Then we randomly choose a blinding polynomial $r \epsilon Z_r(a_r, a_r)$ in the ring. So the encrypted message e should be computed by

e = r*K + m (mod q).

Let m = -1+X3+X4-X8+X9+X10 and r = -1 +X2+X3+X4-X5-X7 then encryption message is denoted as “e”.

e= r*K + m (mod q)
e = 14 + 11X+ 26X2+ 24X3+ 14X4+ 16X5+ 30X6+ 7X7+ 25X8+ 6X9+ 19X10 (mod 32)

Decryption

First, use a part of the private key f to compute polynomial

i = x*e (mod q), then
j = i (mod p), and then

We use the other part of the private key x_p to compute polynomial c = x_p *j (mod p). If this procedure is successful, c will be the original message m. actually, for appropriate parameter values, this probability is extremely high.

i = x*e (mod q)
i = 3-7X-10X2-11X3+10X4+7X5+6X6+7X7+5X8 - 9X9 – 7X10 (mod 32)
j = i (mod p)
j = -X- X2+ X3+ X4+ X5+ X7- X8- X10 (mod 3)
c = x_p*j (mod p)
c = *-1+X3+X4-X8+X9+X10* = *m* (Proved)

V PERFORMANCE

The NTRU crypto system is a new public key cryptography approved in 2009. NTRU cryptosystem is faster and provide stronger security than other traditional cryptosystems. NTRU algorithm performed very well on the mobile devices and there were no negative effects on the mobile devices’ performance due to the small time required for the key generation. NTRU does not require high computing power, which makes it the best alternatives for mobile devices with providing either same or more security facility.

NTRU cryptosystem is gaining more popularity slowly because it’s key size is very small, key generation, encryption speed, decryption speed are much faster and computation power requires very less, Operation speed is very fast, more efficient, consuming less space and more suitable for mobile devices. NTRU is standardized in IEEE 1363.1-2008 and X9.98-2010. Unlike RSA and ECC, NTRU is resistant to quantum computing based on crypto attacks as shown in above table. It is the smallest public key crypto available on market. Unlike RSA and ECC, no successful attack has been recorded to break the security of this algorithm. NTRU encryption and decryption method computational execution timings in secs is shown in table-1.

Let Encryption key size : 51 bits and Decryption key size : 20 bits

Text size	Encryption	Decryption
128 bits	0.0000001	0.0000001
256 bits	0.0000001	0.05490
512 bits	0.05494	0.05490
1K	0.10989	0.05490
2K	0.27472	0.05490
5K	0.65934	0.16484
10K	1.31868	0.36100

Table -1: Encryption and Decryption timings of NTRU

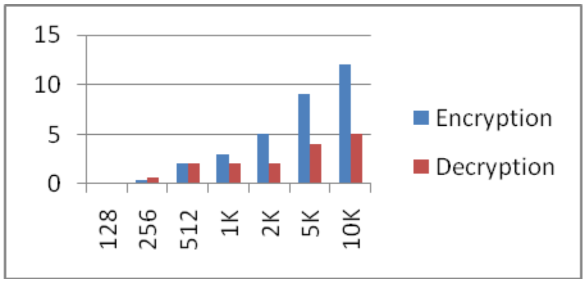

Fig 1: Performance on encryption and decryption timings of NTRU

Method	***AES***	***RSA***	***NTRU***
Approach	*Symmetric*	*Asymmetric*	*Asymmetric*
Encryption	*Faster*	*Slow*	*Fastest*
Decryption	*Fastest*	*Slow*	*Faster*
Key Distribution	*Difficult*	*Easy*	*Easy*
Complexity	*O(LogN)*	*$O(N^3)$*	*O(N LogN)*
Security	*Moderate*	*High*	*Highest*
Nature	*Open*	*Open*	*Open*

Table-2: Comparison between NTRU, DES and RSA

VI CONCLUSION

Instant messaging (IM) is a real-time communication service which allows a user to send a message, usually based on text, to other users. The major drawback has been the vulnerabilities associated with IM technology which creates several security issues. In this paper, we propose to use a single robust ciphering scheme NTRU (Nth degree truncated polynomial ring). The NTRU algorithm is an asymmetric (public/private key) ciphering system that can be used in IM systems. Instead of hybrid encryption policies like AES, SHA-1, and RSA algorithms provided by Bouncy Castle encryption library serves as a means to achieve security. But implementing a three layered ciphering scheme provided by Bouncy Castle encryption library which is a computation and resource over head in IM clients. To reduce computation and resource overhead especially in resource scarce devices such as mobile devices, NTRU algorithm is implemented. NTRU used in mobile devices and other mobile applications because of its features of easy generation of keys, high speed, easy keydistribution and low memory use.

VII REFERENCES

[1] M. Fabri, D. Moore and D. Hobbs, "Empathy and Enjoyment in Instant Messaging," IEEE International Workshop on Human- Computer Interaction, Sept. 2005

[2] Bird, Drew. "Instant Messaging: Corporate Productivity Tool or Cool Toy? ". Intranet Journal, May 1, 2003.

[3] Hallett, Tony. "IM creates 'rampant security risk'". ZDNet UK. February 5, 2003.

[4] Desmond, John. "Report: Secure IM Alternatives Growing". eSecurity Planet: Trends. June 12, 2003.

[5] Bird, Drew "Choosing an Instant Messaging System". Instant Messaging Planet. July 16, 2003.

[6] http://en.wikipedia.org/wiki/NTRUEncrypt

[7] J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, pp. 267-288.

[8] Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam: "Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011.

[9] Xiaoyu Shen; Zhenjun Du; Rong Chen: "Research on NTRU Algorithm for Mobile Java Security", in International Conference Scalable Computing and Communications; Eighth International Conference on Embedded Computing (SCALCOM-EMBEDDEDCOM'09), 2009. page(s): 366 – 369